Faculdades Integradas de Taquara - Faccat
Av. Oscar Martins Rangel, 4.500
Taquara, RS, CEP 95600-000

Curso de Sistemas de Informação

SOFTWARE PARA APLICABILIDADE DAS NORMAS NBR ISO/IEC 27001 E NBR ISO/IEC 27002 E APOIO À TOMADA DE DECISÕES EM SEGURANÇA DE TI

Eliéser Prichua
Faculdades Integradas de Taquara – Faccat – Taquara – RS – Brasil
elieser@faccat.br

Everton Luís Berz
Professor Orientador
Faculdades Integradas de Taquara – Faccat – Taquara – RS – Brasil
everton@faccat.br

Resumo

Este artigo apresenta os resultados de uma pesquisa experimental que teve por finalidade desenvolver um software, denominado SASiso. Este software tem como finalidade integrar as funções do gerente de TI com as do auditor de segurança da informação na aplicabilidade das normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002 resolvendo alguns possíveis problemas na aplicação de normas ISO em geral. O software se atém a apresentar um conjunto gráfico de resultados e classificar a organização no âmbito da segurança da informação, usando para isso, a matriz de análise SWOT. As informações são classificadas de tal forma que podem ser usadas para apoio à tomada de decisão, tanto estrutural como de negócios, na organização.

Palavras-chave: SASiso, TI, segurança da informação, NBR ISO/IEC 27001, NBR ISO/IEC 27002

SOFTWARE TO APPLY THE STANDARDS NBR ISO/IEC 27001 AND NBR ISO/IEC 27002 AND SUPPORT DECISION MAKING ON SAFETY OF IT

Abstract

This article presents the results of an experimental study that aimed to develop a software, called SASiso. This software aims to integrate the functions of the IT manager with the auditor's information security in the applicability of NBR ISO/IEC 27001 and NBR ISO/IEC 27002 resolving some possible problems in implementing ISO standards in general. The software adheres to present a set of graphical results and classify the organization within the information security, using it for the SWOT analysis matrix. The information is sorted so that can be used to support decision-making, both structurally and business organization.

Key-words: *SASiso, IT, information security, NBR ISO/IEC 27001, NBR ISO/IEC 27002*

1. Introdução

A segurança da informação é, muitas vezes, um ente desprezado nas organizações. A informação é considerada um ativo e, dependendo da organização, pode ser considerado o ativo de maior valia que sustenta toda a estrutura e negócios da empresa (CARUSSO e STEFFEN, 1999).

A busca pela proteção da informação é um fator que, quando considerado, estudado e monitorado, não apenas proteje os ativos da organização, mas provê competitividade e ganho de negócio.

A informação é um ativo que requer atenção e cuidados. Algumas dificuldades encontradas nas organizações que desejam melhorar seus padrões de segurança através das NBR ISO/IEC 27001 (2005) e NBR ISO/IEC 27002 (2006) são: (i) gastos com segurança são altos e provar à alta diretoria que investimentos precisam ser feitos é difícil; (ii) aplicação de ISO é lenta; (iii) acompanhamento do plano de implantação da ISO é dificultoso, pois muitas vezes é difícil levantar o que foi cumprido e o que precisa ser feito; (iv) tempo do gestor de TI é escasso, sendo comum a contratação de gestor de SI (Segurança da Informação) para acompanhamento do projeto; (v) relacionamento entre gestor de TI e auditor pode ser conflitante.

Netto e Silveira (2007) classificaram a segurança em três camadas: física, lógica e humana, provando que a humana é o elo mais fraco e propenso à corrupção. Conciso a isto, a Pesquisa Global de Segurança da Informação 2012 (PWC, 2012) conduzida entre fevereiro e abril de 2011, engloba mais de 9600 participantes da área de TI e segurança da informação em 138 paises relaciona que as fontes mais prováveis de incidentes de informação são originadas do funcionário ou ex-funcionário, seguido pelo hacker ou terrorista. Isso evidencia que é possível ter dispositivos físicos e técnicas modernas na organização, mas se não possuir pessoal consciente e treinando para diversas situações, os esforços para manter as informações seguras podem se tornar em vão.

Para manter as informações protegidas é necessária uma política de segurança maciça. Não existe um modelo considerado certo de política de segurança de informação a ser seguido, sendo que cada organização deve ter uma solução adequada a seu uso (CARUSO e STEFFEN, 2007). No entanto, existem diretrizes às boas práticas de segurança da informação, é o caso das normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005) voltadas para a gestão e controle. A organização de um SGSI[1] que esteja de acordo com as normas citadas é árdua e extensa e, na maioria das vezes, requer agente especializado, de preferência um auditor de segurança da informação.

[1] SGSI: Sistema de Gestão de Segurança da Informação

A aplicação de padrões ISO normalmente é lenta, sendo pré-condição tratá-la como um projeto à parte para instituí-la corretamente Kosutic (2011a). Logo, levantar informações de quais etapas da ISO foram ou não cumpridas não é uma tarefa tão simples.

O mercado carece de ferramenta que auxilie na integração CIO[2], CSO[3] e auditor efetiva e sem conflitos de interesse, que não comprometa nem engesse a organização e que sirva de apoio na aplicação das normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005).

Conforme Kosutic (2011b), a ISO 27001 é voltada para a gestão, enquanto a NBR ISO/IEC 27002 (2005) é voltada para o controle. A primeira fornece um modelo para planejar, implementar, monitorar, analisar e aperfeiçoar um SGSI. A segunda fornece detalhamentos dos controles a serem tomados e suas diretrizes para que sejam implantados.

Este artigo apresenta os resultados do desenvolvimento de um aplicativo web objetivado em integrar a gestão de TI e a auditoria em segurança da informação, facilitando a aplicação das normas de segurança NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005). O *software* é capaz de apresentar os pontos fracos e fortes da organização no âmbito da segurança da informação e abrir margem ao apoio à decisão de negócio.

Este artigo divide-se da seguinte forma: na seção 2 é apresentado os trabalhos e pesquisadores que tratam sobre os temas relacionados à segurança da informação; a seção 3 mostra a metodologia usada no desenvolvimento do trabalho e do *software*; na seção 4 é apresentado os detalhes de como o *software* foi implementado; na seção 5 é mostrado o resultado da aplicação do *software*; e, na seção 6, apresenta-se a conclusão do trabalho realizado.

2. Referencial Teórico

2.1 Segurança da Informação

Conforme Lago e Guimarães (2011) a Segurança da Informação tem sua origem na era Egípcia a mais de cinco milênios atrás onde o homem, em virtude de sua criatividade e engenhosidade, escondia e mascarava as informações restringindo o acesso delas à pessoas específicas. Com a evolução dos tempos e a chegada da "era digital", modo com que Gil (2000) caracteriza as últimas três décadas, esta proteção se acentua se fazendo mais necessária, tornando-se muitas vezes vital para a existência da própria organização. A NBR ISO/IEC 27002 (2005) afirma que em virtude dos ataques cada vez mais comuns, se faz jus um sistema de segurança da

[2] CIO: Chief Information Officer ou Chefe do Escritório de Informação
[3] CSO: Chief Security Officer ou Chefe do Escritório de Segurança

informação para que a organização permaneça competitiva, lucrativa, zelando por sua imagem junto ao mercado.

A NBR ISO/IEC 27002 (2005) define a segurança da informação como um ativo, que como qualquer outro, precisa ser protegido e para que os objetivos de segurança da informação sejam atendidos, é necessário que os controles também sejam atendidos, implementados, melhorados e acompanhados.

Conforme Caruso e Steffen (2007) e Fontes (2011) a segurança da informação serve para proteger as informações consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização, já que o ativo mais importante da organização nem sempre são os ativos tangíveis, mas muitas vezes são os intangíveis que geram valor (inovação e capital intelectual) ou proteção de valor (segurança da informação propriamente dita).

2.2 ISO

Conforme Cecchetto *et al.* (2000), as primeiras normas foram elaboradas pela *International Organization for Standardization* (Organização Internacional de Padronização) fundada em 1947 em Genebra na Suíça. A Organização Internacional de Padronização conta hoje com 160 países participantes, entre eles o Brasil. A sigla ISO faz referência à palavra grega ISO, que significa igualdade. As normas precursoras foram as da série 9000, normas estas que tratam de sistemas para gestão e garantia da qualidade nas empresas. A versão brasileira da norma é a NBR ISO 9001, sendo de responsabilidade da ABNT (Associação Brasileira de Normas Técnicas) representar o Brasil nas entidades internacionais de normalização técnica (MARCON, 2011).

As normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005) são voltadas à segurança da informação e fornecem padrões internacionais que possibilitam às organizações aplicar boas práticas na Gestão da Segurança da Informação, levando ao nível máximo de excelência neste quesito.

2.2.1 NBR ISO/IEC 27001

A NBR ISO/IEC 27001 (2006) é uma evolução da norma BS 7799 criada pela indústria britânica em 1993, sendo editada para o português em 2006. Sua metodologia é estruturada para a adoção das melhores práticas na segurança da informação buscando melhoria contínua (VANZOLINI, 2011). A norma NBR ISO/IEC 27001 (2006) especifica requisitos para um SGSI, sendo preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar,

manter e melhorar um SGSI (NBR ISO/IEC 27001). É baseada no ciclo PDCA[4] também conhecido como ciclo de Deming, visto na Figura 1, a seguir.

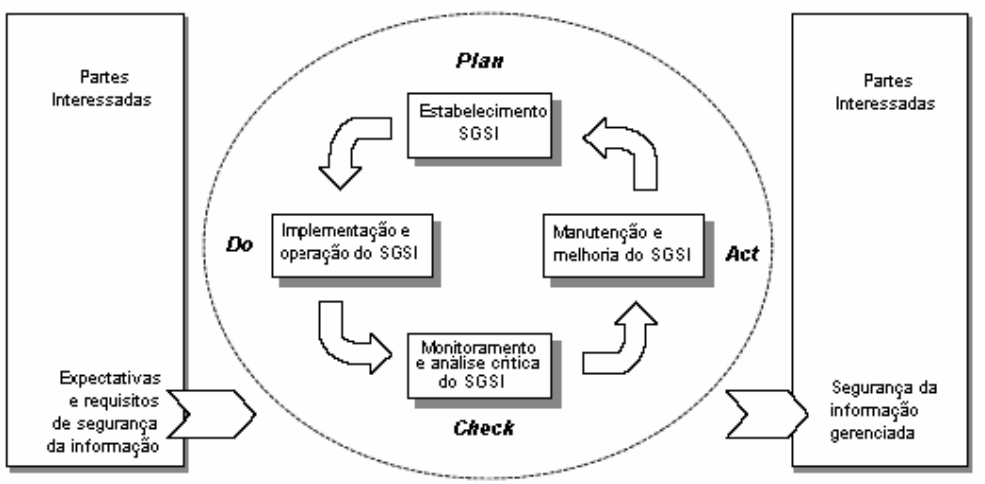

Figura 1 - Modelo PDCA aplicado aos processos do SGSI
Fonte: NBR ISO/IEC 27001 (2006, p. VI)

Kosutic (2011b) caracteriza a ISO 27001 como voltada para a organização e a ISO 27002 voltada ao indivíduo. Isto significa que a organização pode obter certificação na ISO 27001 e, em contrapartida, o indivíduo interessado em certificar-se em normas de segurança, pode certificar-se na ISO 27002. A ISO 27001 tem caráter normativo e informativo, ou seja, para a organização obter tal certificação necessita atender todos os elementos, considerando as particularidades da empresa, descritos na seção normativa (NBR ISO/IEC 27001, 2006). Esta norma é compatível e integrável com as normas ISO 9000 e ISO 14001 (FERNANDES e ABREU, 2008).

A ISO 27001 fornece apenas uma curta definição de um controle, enquanto a ISO 27002 fornece diretrizes detalhadas sobre como implementar o controle, servindo como um guia prático para desenvolver os procedimentos de segurança da informação (FERNANDES e ABREU, 2008).

2.2.2 NBR ISO/IEC 27002

A ISO 27002 não requer que todos seus controles e diretrizes sejam aplicados, devidamente ao fato de respeitar a particularidade de cada organização e, permite inclusive, que controles adicionais sejam acrescentados conforme o perfil da empresa (NBR ISO/IEC 27002, 2005).

Cada norma que compõe a ISO é dividida em três seções: (i) objetivo, que explana o objetivo geral do controle; (ii) controle, que especifica o tipo de controle a ser tomado; e (iii) diretrizes para implantação, que explana as considerações necessárias para o controle ser implementado.

[4] *Plan, Do, Check, Act*: Planejar, Realizar, Verificar, Melhorar

Quanto a sua formação, é dividida em 11 seções, sendo elas: (i) Política de Segurança da Informação; (ii) Organização e Segurança da Informação; (iii) Gestão de Ativos; (iv) Segurança em Recursos Humanos; (v) Segurança Física do Ambiente; (vi) Gestão de Operações e Comunicação; (vii) Controle de Acesso; (viii) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação; (ix) Gestão de Incidentes da Segurança da Informação; (x) Gestão de Continuidade de Negócio; (xi) Conformidade.

Conforme Faria (2011) e Kosutic (2011b), a ISO 27002 é indispensável para uma boa aplicação da ISO 27001, em face da ISO 27001 fornecer apenas uma curta definição de um controle, enquanto a ISO 27002 fornece diretrizes detalhadas sobre como implementar o controle. Logo, para se obter uma política de segurança séria e efetiva buscando a proteção das informações da organização que se estenda aos clientes, fornecedores e terceiros, requer-se que ambas as normas estejam em consonância. Essa colocação pode sugerir que exista apenas uma norma completa que complemente as diretrizes de ambas as normas ao invés de possuir duas normas distintas. No entanto, conforme Kosutic (2011b), a norma se tornaria extensa prejudicando sua implantação e uso prático.

2.3 Sistema de Gestão de Segurança da Informação (SGSI)

SGSI ou ISMS (*Information Security Management System*) é definido por Goyn (2011) como um sistema de gestão desenvolvido para a segurança da informação de uma organização, baseado em uma abordagem de riscos do negócio. Ou seja, é um conjunto de processos, diretrizes e políticas embasadas na análise de risco com o intuito de identificar e corrigir ameaças e pontos fracos do sistema de informação.

Para que um SGSI seja passível de ser certificado tem de obedecer a um conjunto de requisitos definidos na NBR ISO/IEC 27001 (2006), sendo alguns obrigatórios e outros seletivos. Entre os obrigatórios, cita-se: (i) gestão de âmbito; (ii) gestão de inventário; (iii) gestão do risco; (iv) gestão de formação e de ações de sensibilização de segurança; (v) gestão de registros de incidentes; (vi) auditorias internas; e (vii) ações preventivas e corretivas. Já os seletivos é a aplicação dos 136 controles presentes no Anexo A da NBR ISO/IEC 27001 (2006), cujos quais a organização deve implantar os controles de acordo com sua tolerância a riscos e regra de negócios (COELHO, 2011).

Calder e Watkings (2008) justificam a necessidade de um SGSI devido às ameaças à integridade, disponibilidade e confidencialidade das informações serem cada vez maior, gerando maiores perdas financeiras.

Além das perdas financeiras serem cada vez maiores, a Figura 2, a seguir, revela que os investimentos em segurança da informação tendem a aumentar.

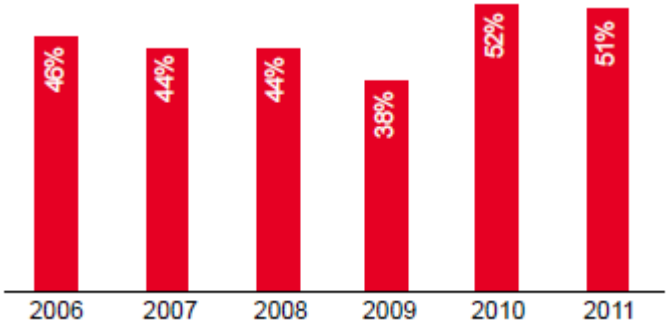

Figura 2 - Percentual dos respondentes para os quais os gastos com a segurança da informação aumentarão nos próximos 12 meses
Fonte: PWC (2012, p. 17)

2.4 Auditoria

A auditoria tem seus primórdios no século XIV, onde, na Inglaterra, criou-se o cargo de auditor do tesouro, em 1314. As primeiras auditorias eram aplicadas com intuito de verificar fraudes e a honestidade do administrador. No entanto, foi em 1934 que a profissão de auditor toma ressalto. As empresas americanas, preocupadas com sua credibilidade da bolsa, foram obrigadas a recrutar serviços de auditores. Ressalta-se que o setor contábil é o setor pioneiro da auditoria, logo a auditoria como especialização em informática e segurança da informação é uma área consideravelmente recente, sendo motivada pelo advento da era digital (GIL, 2000).

Conforme Attie (2000), a auditoria tem finalidade de examinar, corrigir, ajustar e certificar as organizações. Gil (2000) coloca o auditor como responsável tanto pela segurança física de equipamentos, pessoal, suprimentos e instalações, quanto pela segurança lógica e confidencialidade de sistemas, arquivos e informações. No entanto, o auditor não concebe a solução sozinho e não as realiza de fato, apenas propõe ao auditado as soluções e possibilidades, cabendo a este realizá-las ou não.

Entre alguns procedimentos a serem realizados pela equipe de auditoria, Gil (2000) destaca: (i) compreensão do ambiente a ser auditado, realizando análise de riscos; (ii) definição de escopo de teste, especificando os resultados a serem alcançados; (iii) realização de simulação em laboratório ou em campo visando comprovar a efetividade dos possíveis resultados auditados; (iv) emissão de opinião bem como recomendações a respeito do ambiente auditado; (v) debate com profissionais para analise de viabilidade e escolha das alternativas mais adequadas; (vi) acompanhamento e melhoramento das soluções propostas.

Voltada à área de auditoria de TI e segurança da informação, existem duas certificações oficiais nesta área: CISA[5] e CISM[6], ambas reguladas pelo órgão internacional ISACA, o que confere qualidade e integridade nas certificações. Como pré-requisito para o CISA, o órgão regulamentador requer atuação comprovada do candidato de no mínimo cinco anos na área de auditoria e processos e, para o CISM, treinamento anual de 120 horas pós certificação.

2.5 Análise Swot

SWOT é um termo formado pela combinação de quatro palavras em inglês: *strengths* (forças), *weaknesses* (fraquezas), *opportunities* (oportunidades) e *threats* (ameaças) criado por Albert Humphrey, que liderou o projeto de pesquisa na universidade de Stanford nas décadas de 60 e 70. Conforme Daychouw (2007) a análise SWOT não foi desenvolvida para ser aplicada sobre um domínio em específico, logo ela permite ser aplicada sobre qualquer cenário, sendo dividida entre ambiente interno (forças e fraquezas) e ambiente externo (oportunidades e ameaças).

O ambiente interno pode ser controlado pelos membros da própria organização, sendo seu resultado dado pelas decisões de negócio tomadas.

O ambiente externo está fora do controle da organização, mas é dever da mesma conhecê-lo e trabalhar para monitorá-lo, buscando evitar as ameaças e aproveitar as oportunidades. Um evento que possa afetar uma organização provindo externamente seria, por exemplo, a alteração de uma legislação. A Figura 3 mostra como a análise SWOT se organiza.

SWOT	AJUDA (Na conquista de objetivos)	ATRAPALHA (Na conquista de objetivos)
AMBIENTE INTERNO (Atributos da organização)	Forças	Fraquezas
AMBIENTE EXTERNO (Atributos do ambiente)	Oportunidades	Ameaças

Figura 3 – Modelo Esquemático da Análise SWOT
Fonte: (DAYCHOUW, 2007, p. 8)

[5] CISA: *Certified Information Systems Auditor* (Certificação em Auditoria em Segurança da Informação).
[6] CISM: *Certified Information Security Manager* (Certificação em Gerenciamento em Segurança da Informação)

3. Metodologia

Este artigo classifica-se como uma pesquisa de natureza aplicada, tendo objetivo exploratório, abordagem quantitativa e teve como base a metodologia experimental (JUNG, 2011).

O método de desenvolvimento escolhido seguiu a modelagem prescritiva de *software* usando o modelo incremental. Segundo Pressman (2006), o modelo incremental possibilita que, após uma entrega parcial contendo o núcleo do *software* (conjunto de atividades principais), desenvolva-se um novo plano para o próximo incremento embasado no resultado de uso e avaliação do usuário. As etapas do modelo incremental, conforme a Figura X, são: (i) comunicação; (ii) planejamento; (iii) modelagem; (iv) construção; e (v) implantação.

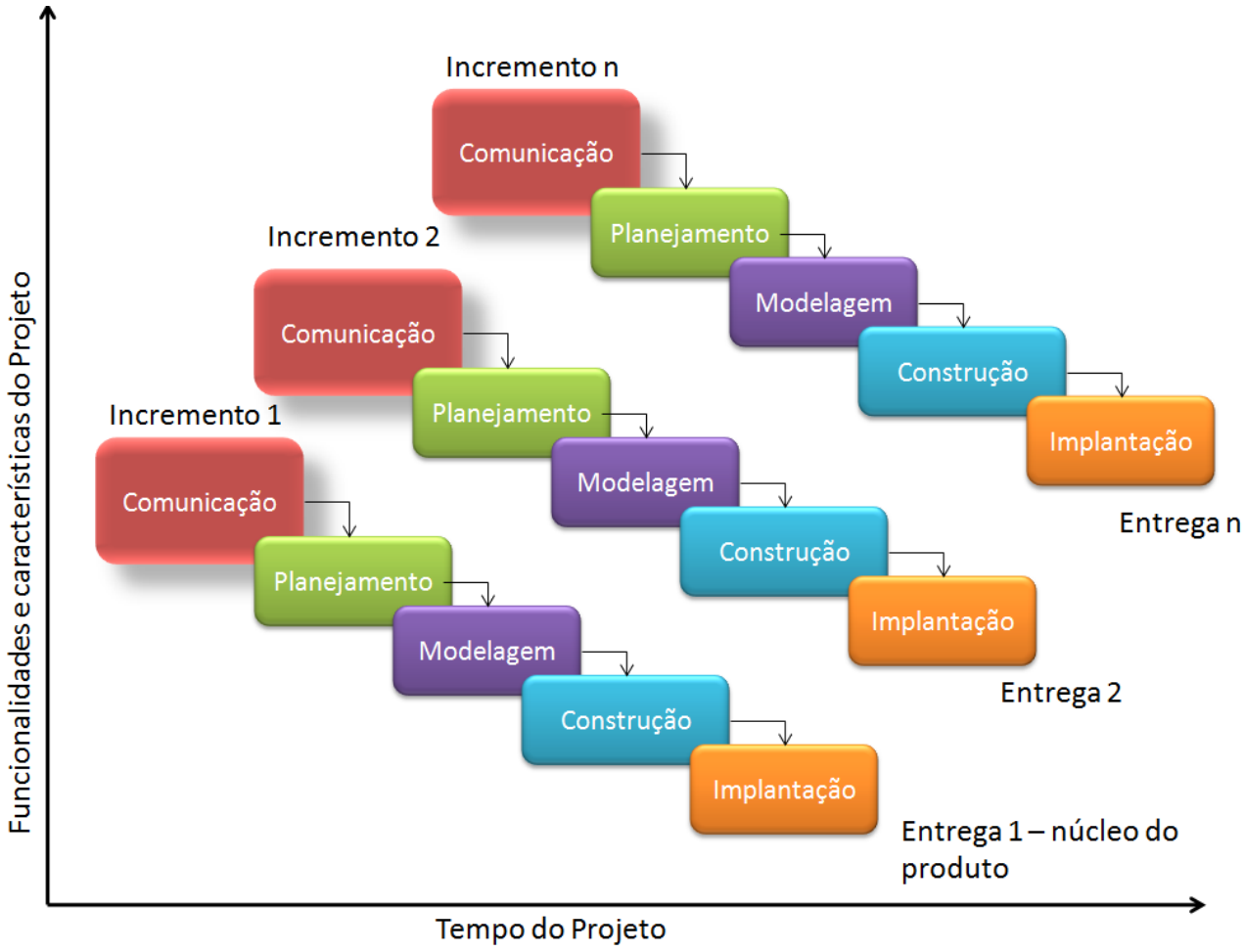

Figura 4: modelo incremental
Fonte: adaptado de Pressman (2006, p. 40)

Tal modelo foi escolhido devido se ter os requisitos iniciais bem definidos, mas possibilitasse a entrega gradual de forma que o cliente utilizasse suas funcionalidades antes do aplicativo estar integralmente concluido.

A partir da problematização e análise das ferramentas desenvolveu-se um sistema web, denominado SASiso, que será elucidado nas seções seguintes.

3.1 Análise de requisitos

A análise de requisitos é uma das atividades realizadas na fase de comunicação do modelo incremental. Segundo Pressman (2006) é uma etapa que permite obter informações que resultam em especificações das características operacionais da aplicação, teve início na identificação da carência de ferramentas no mercado que auxiliem no gerenciamento da segurança da informação nas organizações. Através de pesquisa bibliográfica, persebeu-se que as normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005) são os alicerces do regimento às boas bráticas da segurança da informação nas organizações brasileiras. O estudo teve como objetivo idenficar a estrutura das normas, como elas são compostas e como devem ser implantadas. Esta etapa foi o alicerce para a viabilidade do *software*, que tem como intuito agir no acompanhamento da implantação das normas citadas.

É possível identificar os seguintes requisitos funcionais para o sistema desenvolvido: (i) o sistema deve disponibilizar o acesso a dois atuantes no sistema (auditor de segurança e o gestor de TI); (ii) será utilizado para aplicar as normas de segurança ISO 27001 e ISO 27002; (iii) as seções das normas serão pontuadas através da atribuição de pesos, o que será utilizado para classificar a organização quanto à segurança da informação; (iv) deve ser possível consultar uma matriz de forças e fraquezas na organização, tal como matriz SWOT; (v) para uma visão gerencial deverá ser possível consultar gráficos que mostrem o nível de proteção das informações na organização; (vi) deverá possuir um relatório que contenha informações relevantes para análise do auditor.

Para que o sistema funcione como desejado, faz-se necessário a identificação dos seguintes requisitos não-funcionais: (i) o acesso de cada usuário (gestor e auditor) é realizado com login e senha pessoais e instransferíveis, ficando garantido que o acesso só seja realizado pelos entes identificados; (ii) a disponibilidade do sistema seja efetiva de forma que os serviços que garantem a funcionalidade do sistema estejam disponiveis; (iii) o sistema funcione em tempo hábil e tenha uma performance satisfatória no sentido que não gere insatisfação do usuário; (iv) a usabilidade esteja assegurada de forma que o usuário tenha uma boa perspectiva do sistema, no que se refere às cores e disponibilidade dos menus e ferramentas, e que o sistema seja autoexplicativo.

É importante salientar que o sistema funcionará numa estrutura cliente/servidor. No servidor haverá o banco de dados e a aplicação devidamente configurados e, o cliente, utilizará qualquer *browser*[7] para acesso ao sistema. O acesso poderá ser tanto local como externo, pois sua funcionalidade deve ficar garantida independente da estrutura de conexão escolhida.

[7] *Browser:* aplicativo para navegação na internet (Internet Explorer, Chrome, Fiferox, Opera, entre outros).

3.2 Modelagem do *software*

A modelagem do software foi realizada utilizando linguagem UML[8] que, conforme a OMG (2012), unifica todas as etapas de desenvolvimento e integração de modelagem de negócios. Para a construção dos diagramas e demonstração da análise e funcionamento do software, usou-se o software Astah (CHANGE VISION, 2012) na versão *freeware*[9].

A Figura 4 mostra o diagrama de caso de uso do sistema que, segundo Pressmann (2006), explana como um ator específico ou usuário interage com o sistema, constando as interações possíveis entre produtores e consumidores de informação e o sistema. O diagrama de caso de uso tem, como principal finalidade descrever o sistema do ponto de vista do usuário. A seguir podem ser visualizadas as funções dos dois papeis atuantes do sistema.

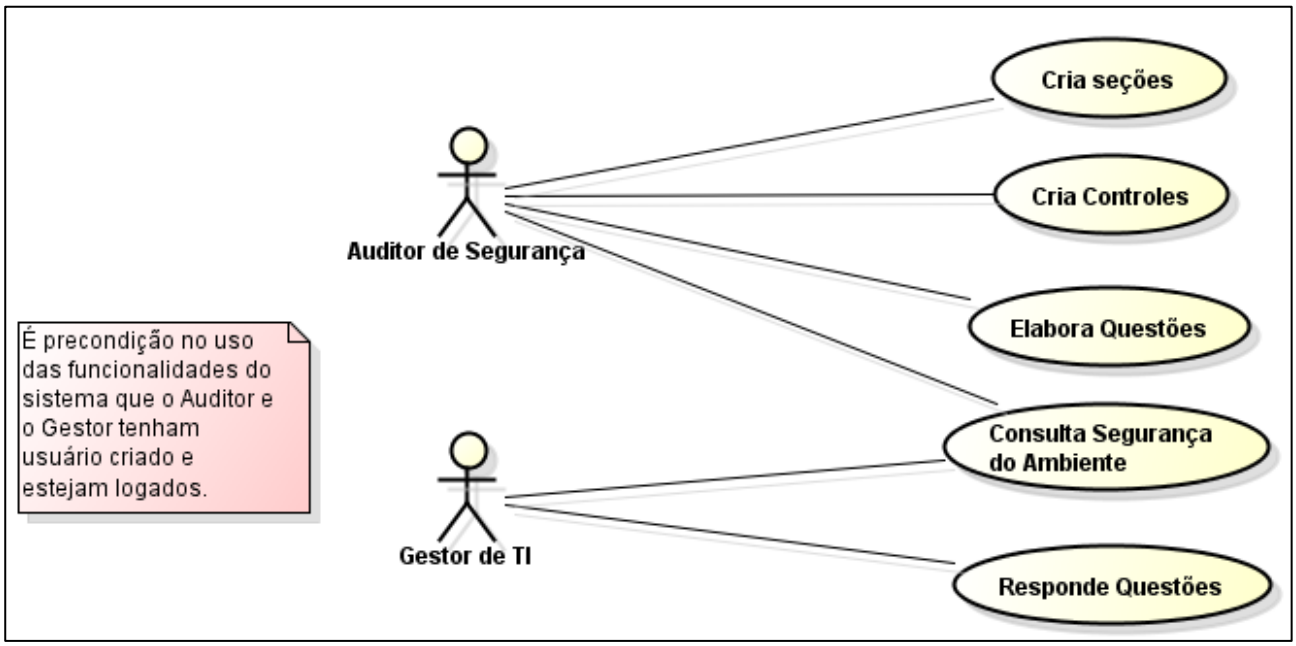

Figura 5: Diagrama de Casos de Uso

No diagrama demonstrado, percebe-se a existência de dois atores: (i) "Auditor de Segurança" e o (ii) "Gestor de TI". O auditor de segurança fica responsável pelo mapeamento das normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005). Os casos de uso "Cria seções" e "Cria Controles" são a transformação das seções e a interpretação dos controles presentes nas normas. Após ter sido realizado este mapeamento, o auditor também fica responsável pela elaboração das questões, representado pelo caso de uso "Elabora Questões", onde, em segundo momento, serão respondidas pelo gestor de TI, expressado pelo caso de uso "Responde Questões". Exemplos e detalhes deste funcionamento podem ser vistos na seção 4.1.1. Após terem sido

[8] UML: *Unified Modeling Language* ou Linguagem de Modelagem Unificada.
[9] *Freeware*: utilização livre, não requer pagamento de obtenção de licença.

respondidas as questões será possível consultar a classificação da organização quanto à segurança da informação, representado pelo caso de uso “Consulta Segurança do Ambiente”. Esta consulta pode ser realizada tanto pelo auditor quanto pelo gestor de TI.

Para representar o funcionamento do sistema num nível mais específico construiu-se o diagrama de classes, conforme pode ser visto na Figura 5. Segundo Fowler (2000) o diagrama de classes é um elemento abstrato que representa um conjunto de objetos que tem como características atributos e métodos (ações e comportamentos), abrangendo a definição de todas as classes no problema a ser resolvido.

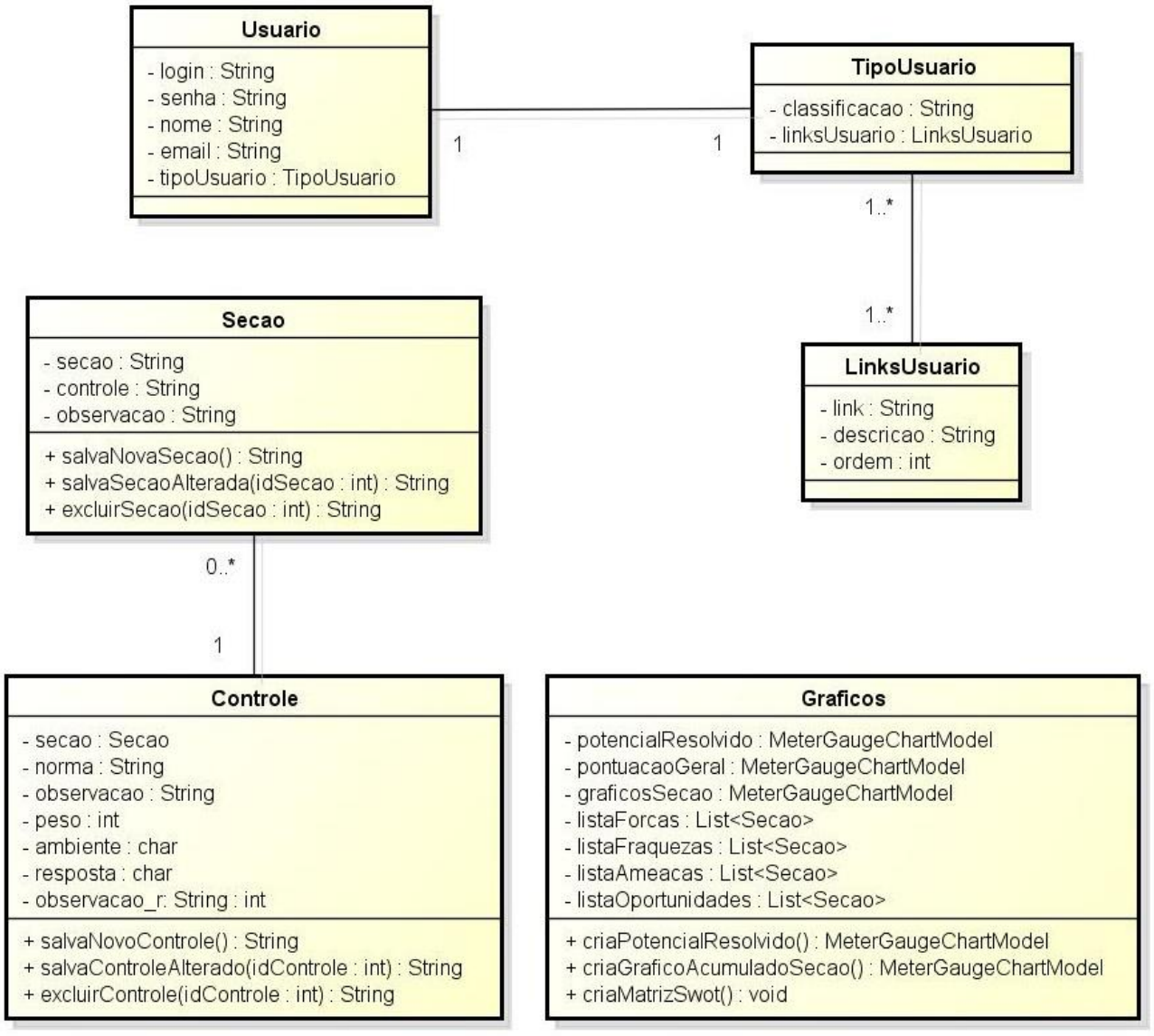

Figura 6: Diagrama de Classes

A classe “Secao” representa alguma seção da norma NBR ISO/IEC 27001 (2006) e a classe “Controle” representa um controle na mesma norma. O relacionamento indica que, para que exista

um controle cadastrado, é necessário que exista uma seção cadastrada. A classe "Graficos" é responsável pelo gerenciamento dos gráficos que conferem a classificação da organização no âmbito da segurança da informação, gráficos estes, que englobam a pontuação por seção, pontuação geral e matriz SWOT , sendo melhor apresentados na seção Desenvolvimento. As classes "Usuario", "TipoUsuario" e "LinksUsuario" correspondem ao tratamento de login e às restrições de acesso para cada usuário.

3.3 Desenvolvimento

O desenvolvimento do sistema faz parte da etapa de "construção" do modelo incremental e foi realizado utilizando a linguagem de programação Java (ORACLE, 2012a). O Java surgiu em 1991 num projeto realizado pela Sun Microsystems, cujo desde 2009 é mantida pela Oracle. Tem como característica ser livremente distribuido e de usufruir do paradigma de orientação a objetos, o que gera facilidades para o programador principalmente no que confere ao reaproveitamento de código. A interface utilização para escrever o código e desenhar o leiaute do SASiso foi o Netbeans (ORACLE, 2012a), sendo optado por tal devido sua facilidade de uso e ganho de produtividade, já que muitos componentes já vem prontos. Igualmente ao Java, o Netbeans é gratuito, o que diminui o gasto com licenças para o desenvolvimento de software. Usou-se o *framework*[10] Hibernate (HIBERNATE, 2012) para mapeamento de objeto relacional. O Hibernate tem como principais características a transformação das classes em Java para tabelas do banco de dados e ser portável para qualquer banco de dados SQL[11].

Para uma maior produtividade e *design* aprimorado, usou-se o *framework* JSF 2.0 (ORACLE, 2012b) e o Primefaces (PRIMEFACES, 2012) que é considerado uma especialização do JSF. O JSF é um *framework* MVC[12] para desenvolvimento Java sendo escolhido para o desenvolvimento devido fornecer uma baixa curva de aprendizagem aliada a várias ferramentas adicionais (SANTOS, 2008). O MVC é um padrão de projeto que surgiu pela comunidade Smalltalk (SMALLTALK, 2012) em 1979 tendo como característica dividir um projeto em três camadas, sendo elas: *Model*, compõe a estrutura lógica dos dados; *View*, coleção de classes que dá suporte ao usuário; e *Controller*, realiza a comunicação entre o modelo e a visualização. Sua característica é a de separar a lógica de negócios (*model*) da interface do usuário (*view*) e do fluxo de aplicação (*controller*), ou seja, separar a informação da apresentação. O Primefaces trata-se de uma

[10] *Framework:* em desenvolvimento de software é uma abstração que une código comuns e provê uma funcionalidade genérica.
[11] Structured Query Language, ou Linguagem de Consulta Estruturada.
[12] MVC: *Model, View, Controller* (Modelo, Visão e Controle).

especialização do JSF tendo como diferencial ao JSF a presença de um conjunto especial de ferramentas, com caracteristicas melhoradas.

Para gerenciamento do banco de dados utilizou-se o SGBD[13] Postgre SQL (POSTGRE, 2012) e para o servidor de aplicação usou-se o Tomcat (APACHE, 2012). O Postgre é um banco de dados relacional multiplataforma e facilmente escalável, tendo como principal atrativo seu desempenho satisfatório e confiabilidade. O Tomcat é um servidor específico para aplicações Java Servlets e, por não atender outras plataformas, é um *container* rápido e eficiente. Ambos, Postgre e Tomcat, são gratuitos, não exigindo gasto financeiro para obtenção dos direitos de uso.

Optou-se por essas tecnologias por serem de conhecimento do programador e oferecer facilidade de uso, organização e produtividade.

4. Implementação

Nessa seção é descrito os detalhes da implementação do sistema, como é realizado o processamento para a construção da matriz SWOT e as funções de cada atuante no sistema.

4.1 Auditor de Segurança da Informação

O auditor de segurança da informação não precisa se restringir aos controles expostos nas normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005), podendo agregar outro conhecimento que as complemente e que acredite poder aperfeiçoar a segurança na organização. Ao realizar o mapeamento, o auditor atribuirá pesos diferentes a cada controle mapeado, com base na sua experiência e no critério de importância que considere necessário para aquele controle. Os pesos serão classificados de 1 a 5 conforme a impactação que a falha de um controle possa oferecer à organização. Serão associados a 1 quando o impacto for muito baixo e a 5 quando o impacto for muito alto.

4.1.1 ATUAÇÃO DO AUDITOR

Cada seção possui diversos controles que devem ser mapeados para o sistema. Tomando como exemplo o controle da norma NBR ISO/IEC 27002 (2005): “5.1.1 Documento de Política da

[13] SGBD: Sistema de Gerenciamento de Banco de Dados.

Segurança da Informação", diz: "Convém que um documento de política de segurança da informação seja aprovado pela direção publicado e comunicado para todos os funcionários e partes externas relevantes".

Um possível mapeamento do auditor a respeito do controle citado seria: "Existe uma PSI homologada pela direção e de aceite de todos os clientes internos e externos?". Resposta "Sim" ou "Não". Possível impacto atribuído pelo auditor: "3 (médio)". Infere em ambiente "Interno" ou "Externo".

O exemplo citado explana um possível mapeamento ao controle 5.1.1 da NBR ISO/IEC 27002 (2005), onde o peso de impacto atribuído ao não cumprimento desse controle é três. Caso a resposta seja positiva, soma-se três pontos, caso seja negativa, a organização deixa de contabilizar três pontos. Obviamente, quanto maior o número de pontos, mais bem consolidada quanto à segurança da informação a organização se encontrará. Observe, também, que o auditor necessita especificar o mapeamento como de responsabilidade interna ou externa à organização, pois sendo interno, o controle contabilizará para as forças e fraquezas e, sendo externo, contabilizará para ameaças e oportunidades. A indicação do controle ao ambiente interno ou externo é essencial para que seja possível a construção da matriz SWOT.

4.2 Gestor de TI ou SI

Tendo sido alimentado o sistema pelo auditor, a função do gestor é a de responder aos questionamentos levantados de acordo com sua organização. As possíveis respostas são "sim" ou "não". Caso o gestor ache que algum levantamento questionado pelo auditor não se aplique à sua organização, poderá não responder e acrescentar uma observação explicando o porquê do questionamento não se aplicar. Desta forma, o auditor analisára as respostas não respondidas e poderá eliminar o controle inválido, pois somente ele tem permissões para cadastrar e excluir os dados que alimentou.

4.3 Pontuação

A qualquer momento, tanto o gestor quanto o auditor, poderão consultar a matriz SWOT, que apresentará o resultado dos controles observados pelo auditor e cumpridos ou não pela organização. Em cada seção será aplicado a Equação 1 para, desta forma, classificar cada seção na

matriz SWOT. Tendo a seção atingido uma pontuação acima ou igual a 50% será classificada como força ou oportunidade e, atingindo abaixo de 50%, será classificada como fraqueza ou ameaça.

$$S_1 = \frac{\sum_{i=1}^{a} T_i}{\sum_{i=i}^{n} S_i} \; x\,100$$

Equação 1: pontuação individual por seção

Na Equação 1 o S_1 representa o porcentual atingido na seção 1; T_i representa a pontuação total atingida na seção 1; S_i representa a pontuação total possível de se atingir na seção 1. Logo, a porcentagem que expressa a pontuação da primeira seção é: a divisão do somatório de pontos atingidos em todos os controles da seção 1, dividido pelo somatório máximo possível de se atingir nesta seção, multiplicado por 100.

Após se ter a classificação e porcentagem de cada seção é possível computar a pontuação geral da organização através da Equação 2.

$$P_{total} = \sum_{i=S_1}^{S_c} \frac{Ts_1}{N_s} \; x\,100$$

Equação 2: pontuação geral da organização

Na Equação 2 P_{total} é a porcentagem que representa a pontuação total no âmbito da organização; Ts_1 representa o total de pontos atingidos em todas as seções; N_s representa o total de pontos possíveis de serem atingidos em todas as seções. Logo, a porcentagem que expressa e classifica a pontuação da organização em todo o âmbito de segurança da informação é: o somatório de todos os pontos atingidos da seção 1 à seção 11, dividido pelo somatório de todos os pontos possíveis de se atingir da seção 1 à seção 11, multiplicados por 100.

4.4 Pesos

A construção da matriz SWOT só é possível devido ao peso e ao ambiente atribuído a cada questão pelo auditor. Neste momento apresenta-se o porquê do processo de pontuação escolhido.

A explicação provém do campo da gerência de projetos, especificamente da análise quantitativa de riscos, que segundo o PMBOK (2004) nada mais é uma quantificação numérica dos riscos que podem afetar potencialmente e significativamente um projeto, ou analogamente neste

caso, uma organização. A classificação dos riscos se justifica devido ao impacto que o mesmo pode acarretar caso o risco possa de fato ocorrer.

Conforme o PMBOK (2004) a organização pode classificar o risco por objetivo e desenvolver maneiras de realizar uma classificação geral aos riscos. Logo, neste software, foi aplicada uma pontuação que representa a forma comumente adotada na prática da análise quantitativa de riscos: o uso do impacto apresentado numa matriz probabilidade x impacto, conforme o Quadro 1.

Probabilidade	**Ameaças**					**Oportunidades**				
0,90	0,05	0,09	0,18	0,36	0,72	0,72	0,36	0,18	0,09	0,05
0,70	0,04	0,07	0,14	0,28	0,56	0,56	0,28	0,14	0,07	0,04
0,50	0,03	0,05	0,10	0,20	0,40	0,40	0,20	0,10	0,05	0,03
0,30	0,02	0,03	0,06	0,12	0,24	0,24	0,12	0,06	0,03	0,02
0,10	0,01	0,01	0,02	0,04	0,08	0,08	0,04	0,02	0,01	0,01
Impacto	0,05	0,10	0,20	0,40	0,80	0,80	0,40	0,20	0,10	0,05

QUADRO 1: Matriz probabilidade x impacto
Fonte: adaptado do PMBOK (2004)

Percebe-se, no Quadro 1, uma multiplicidade de cinco fatores de probabilidade (0,10; 0,30; 0,50; 0,70 e 0,90) e outros cinco fatores de impacto (0,05; 0,10; 0,20; 0,40 e 0,80).

A pontuação atribuida à cada questão elaborada pelo auditor no aplicativo é classificada considerando o impacto que o não cumprimento do controle pode acarretar à organização, ou seja, foi considerado apenas o fator impacto da matriz probabilidade x impacto.

Embasado na situação apresentada, desenvolveu-se uma maneira mais direta para classificar os riscos de um controle das normas ISO utilizadas neste trabalho, conforme visto na Tabela 1.

TABELA 1: Classificação de Pesos

Impacto	**Peso**
Muito baixo	1
Baixo	2
Médio	3
Alto	4
Muito alto	5

5. Resultados

Nesta seção são apresentados os resultados do software desenvolvido, contemplando os pontos mais relevantes ao funcionamento do sistema.

A Figura 6 apresenta a visão do auditor no momento do cadastro das questões, ou seja, é o mapeamento dos controles presentes nas normas ISO na forma de perguntas que visam avaliar a segurança da informação no ambiente. Tais perguntas serão respondidas posteriormente pelo gestor de TI ou encarregado interno de segurança da informação.

Figura 7: tela de cadastro dos controles (visão do auditor)

Os campos informados pelo auditor são os seguintes, mas não necessariamente nesta ordem: (i) seção, refere-se à qual seção, pré-cadastrada anteriormente, corresponde o questionamento que está sendo construindo; (ii) norma, corresponde à pergunta propriamente dita, referente ao mapaeamento da ISO interpretada pelo auditor; (iii) observação, alguma informação relevante à norma e que esclareça sobre o questionamento levantado; (iv) peso, corresponde à escolha do impacto que o não cumprimento da norma pode trazer à organização; (v) ambiente, especifica se o controle implica no ambiente interno ou externo, o que será usado em seguida para a construção dos gráficos, pontuação e matriz SWOT.

A Figura 7, a seguir, demostra os questionamentos construidos pelo auditor, conforme ilustrado na Figura 6. No exemplo da Figura 7 são exibidos seis questionamentos, onde, em cada questionamento é exibido (i) título: a qual controle das normas ISO o questionamento se aplica; (ii) pergunta: o questionamento realizado pelo auditor; (iii) observação do auditor: refere-se à observação realizada pelo auditor para auxiliar a compreensão do questionamento; (iv) resposta: correponde às respostas possíveis pelas quais o gestor pode optar, neste caso "sim" ou "não"; (v) observação do gestor: local reservado ao gestor explicitar alguma observação que julgue importante quanto ao questionamento realizado e à resposta concedida. Observe que não é exibido nos questionamentos se o controle implica no ambiente interno ou externo à organização. Neste momento essa informação não é importante ao gestor sendo útil somente para a construção da matriz SWOT.

Figura 8: tela de resposta aos questionamentos (visão do gestor)

Após serem respondidas as questões, faz-se necessário salvar as informações. O botão "salvar", presente na parte superior e inferior da grade de questões, realizará essa função quando clicado. As respostas podem ser salvas uma só vez, ao final da operação, ou a cada resposta realizada.

A tela ilustrada pela Figura 8, a seguir, trata-se de um painel que exibe o resultado geral da organização no âmbito de segurança da informação. Este painel é exibido automaticamente após o gestor ou o auditor acessarem o sistema.

Figura 9: tela de visualização dos resultados e matriz SWOT

Os primeiros gráficos, em forma de odômetro, exibem a porcentagem de pontuação geral, onde foi aplicado a Equação 2 (descrito na seção Pontuação), e a porcentagem de questões respondidas, respectivamente.

O segundo grupo de gráficos exibe a porcentagem de pontuação específica de cada seção das normas ISO utilizadas, onde, em cada seção foi aplicado a Equação 1 (descrito na seção Pontuação).

A terceira parte exibe a matriz SWOT, classificando cada seção da norma em força ou fraqueza, quando referem-se ao ambiente interno, ou em oportunidade ou ameaça, quando referem-se ao ambiente externo.

O painel ilustrado pela Figura 8, quando apresentado à alta diretoria, pode servir como apoio à tomada de decisão. Os gastos com a segurança e com TI normalmente são altos e provar que investimentos precisam ser realizados nesta área nem sempre é fácil. Com a apresentação dos resultados na forma que o software relaciona, poder-se-á solidificar os argumentos a fim de facilitar o investimento para melhorar o valor da TI e segurança da informação, o que, provavelmente, resultará numa série de benefícios à organização.

6. Conclusão

A segurança da informação, muitas vezes, é um ente desconsiderado nas organizações, mesmo que estas tenham como principal agente gerador de valor os ativos intangíveis. A busca pela proteção da informação é um fator que, quando considerado, estudado e monitorado, não apenas proteje os ativos da organização, mas provê competitividade e ganho de negócio. No entanto, para desenvolver e manter um ambiente seguro, se requer investimentos. Apresentar a alta diretoria um plano de segurança da informação como investimento a ser realizado nem sempre é fácil.

Não existe um modelo certo de proteção à informação, sendo permitido que cada organização possua a sua. Todavia, as normas NBR ISO/IEC 27001 (2006) e NBR ISO 27002 (2005) são consideradas alicerces às boas práticas de segurança da informação para as organizações. A NBR ISO/IEC 27001 (2006) é voltada para a gestão, tem caráter normativo e informativo e é baseada no modelo PDCA. Já a NBR ISO/IEC 27002 (2005) é voltada para o controle, sendo dividida em 11 seções com diretrizes detalhadas sobre como implantá-las. Para se obter uma política de segurança séria e efetiva, buscando a proteção das informações da organização, estendendo-se aos clientes, fornecedores e terceiros, requer-se que ambas as normas estejam em consonância. No entanto, a aplicação de normas ISO podem ser lentas e auferir as etapas cumpridas e faltantes pode tornar-se complexo e tedioso.

Neste artigo apresentou-se o desenvolvimento de um aplicativo *web* denominado SASiso. O aplicativo tem como objetivo ntegrar a gestão de TI de qualquer organização com a equipe de auditoria em segurança da informação, que trabalham juntas para aplicar as normas NBR ISO/IEC 27001 (2006) e NBR ISO/IEC 27002 (2005). O SASiso é capaz de apresentar os pontos fortes e fracos da organização no âmbito da segurança da informação e abrir margem ao apoio à decisão, tanto estrutural como de negócio.

O software foi desenvolvido em Java dentro do paradigma orientado a objetos, usando o padrão de projeto MVC, o que conferiu agilidade e organização no desenvolvimento. Para facilitar algumas etapas, como o gerenciamento de dados e o gerenciamento da interface, usou-se o Hibernate e o JSF com a especialização Primefaces.

O resultado final gerado pelo software é a apresentação de uma série de gráficos e de uma matriz SWOT, representando a posição da organização quanto à segurança da informação. A análise SWOT não foi desenvolvida para ser aplicada sobre um domínio em específico, logo, ela permite ser aplicada sobre qualquer cenário. O SASiso concatena todas as seções das normas ISO utilizadas e as classifica na matriz SWOT como forças, fraquezas, oportunidades ou ameaças.

Foi possível identificar que as organizações que valorizam seus ativos intangíveis e se preocupam com sua proteção possuem diferencial no mercado. Possuir uma ferramenta que facilite

a aplicação das normas de segurança ISO e que apresente como resultado um conjunto de informações de interesse à alta direção pode servir como apoio a decisão de negócio e, provavelmente, pode resultar uma série de benefícios à organização.

Pretende-se para trabalhos futuros, acrescentar um relatório com os gráficos e a matriz SWOT, facilitando, assim, a apresentação dos resultados à alta direção. Para atingir um maior nível de detalhamento, pretende-se desenvolver uma matriz SWOT onde seja possível visualizar não somente as normas, mas também cada controle contido na norma.

Referências

APACHE. **Apache Tomcat**. Disponível em: <http://tomcat.apache.org/>. Acesso em 6/out/2012.

ATTIE, William. **Auditoria, Conceitos e Aplicações**. São Paulo: Atlas, 2000.

CALDER, Alan; WATKINS, Steve. **IT governance: A Manager's Guido to Data Security and ISO 27001/ISO 27002** - 4ª ed. Filadélfia – Estados Unidos. Editora Kogan Page, 2008.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny**. Segurança em Informática e de Informações** – 2ª Ed. São Paulo: Senac, 1999.

CECCHETTO, José; SILVA, Francisco; COSTA, Rita. **Qualidade** (2000). Monografia apresentada no curso de Organização, Sistemas e Métodos das Faculdades Integradas Campos Salles. Disponível em: <http://www.maurolaruccia.adm.br/trabalhos/qualidade.htm> Acesso em 18/out/2011.

CHANGE VISION. **Astah Community**. 2011. Disponível em: <http://astah.net> Acesso em 15/set/2012.

COELHO, Paulo. **Requisitos de um SGSI – Sistema de Gestão de Segurança da Informação**. Disponível em: <http://ismspt.blogspot.com/2006/09/requisitos-de-um-sgsi-sistema-de-gesto.html> Acesso em 31/out/2011.

DAYCHOUW, Merhi **40 Ferramentas e Técnicas de Gerenciamento**. Rio de Janeiro: Brasport, 2007.

FARIA, Aléxia Lage. **Conheça a NBR ISO/IEC 27002 – Parte 1**. Disponível em: <http://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-1/> Acesso em 19/out/2011.

FONTES, Edison. **Segurança: um ativo intangível que protege valor!**.Disponível em: <http://informationweek.itweb.com.br/blogs/seguranca-um-ativo-intangivel-que-protege-valor/> Acesso em 26/out/ 2011.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz. **Implantanto a Governança de TI – da Estratégia à Gestão dos Processos e Serviços** - 2ª Ed. Rio de Janeiro: Brasport, 2008.

FOWLER, Martin. **UML essencial: um breve guia para a linguagem – padrão de modelagem de objetos** – 3ª Ed. Porto Alegre: Bookman, 2005.

GIL, Antonio de Loureiro. **Auditoria de Computadores –** 5ª Ed. São Paulo: Atlas, 2000.

GOYN, Pedro. **Segurança em 2010**. Disponível em: <http://www.baguete.com.br/artigos/732/pedro-goyn/09/12/2009/seguranca-em-2010> Acesso em 31/out/2011.

HIBERNATE. **Why Hibernate**. Disponível em: <http://www.hibernate.org/about/why-hibernate> Acesso em 6/out/2012.

JUNG, Carlos Fernando; AMARAL, Fernando Gonçalves. **Elaboração de artigos científicos**. Porto Alegre: PPGEP/UFRGS, 2011.

KOSUTIC, Dejan. **Dilemas com os auditores internos das normas ISO 27001 e BS 25999-2**. Disponível em: <http://blog.iso27001standard.com/pt-br/2010/12/16/dilemas-com-os-auditores-internos-das-normas-iso-27001-e-bs-25999-2/#> Acesso em 13/out/2011a.

KOSUTIC, Dejan. **Semelhanças e diferenças entre a ISO 27001 e a ISO 27002**. Disponível em <http://blog.iso27001standard.com/pt-br/2010/12/19/iso-27001-vs-iso-27002-4/> acessado em agosto de 2011b.

LAGO, Davi Guimarães; GUIMARÃES, Enio Benfica. **Segurança da Informação e sua História**. Disponível em <http://www.viajus.com.br/viajus.php?pagina=artigos&id=2202> acessado em 26 de outubro de 2011.

MARCON, Anderson. **O que é ISO?** Disponível em <http://portaldoconsumidor.wordpress.com/2010/09/20/o-que-e-iso/> acessado em 18 de outubro de 2011.

NBR ISO/IEC 27001 – **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos**, ABNT –Associação Brasileira de Normas e Técnicas. Brasil, 2006.

NBR ISO/IEC 27002 – **Tecnologia da informação – Técnicas de segurança – Código de Prática para a gestão da segurança da informação**, ABNT – Associação Brasileira de Normas e Técnicas. Brasil, 2005.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro. **Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas** – Revista de Gestão da Tecnologia e Sistemas de Informação – Universidade Municipal de São Caetano do Sul – IMES. Brasil, 2007.

OMG, **Unified Modeling Language**. Disponível em <http://www.uml.org/> acessado em 13 de outubro de 2012.

ORACLE. **Java SE downloads**. Disponível em <http://www.oracle.com/technetwork/java/javase/downloads/index.html> acessado em 6 de outubro de 2012a.

ORACLE. **Java Server Faces**. Disponível em <http://www.oracle.com/technetwork/java/javaee/javaserverfaces-139869.html> acessado em 6 de outubro de 2012b.

PMBOK. **Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos**. 3ª ed. Pensilvania, EUA: Project Management Institute, 2004.

POSTGRE SQL. **Sobre o PostgreSQL**. Disponível em <http://www.postgresql.org.br/sobre> acessado em 6 de outubro de 2012.

PRESSMAN, Roger S. **Engenharia de software.** 6ª ed. Rio de Janeiro: McGraw-Hill, 2006.

PRIMEFACES. **Why Primefaces**. Disponível em < http://primefaces.org/whyprimefaces.html> acessado em 6 de outubro de 2012.

SANTOS, Gustavo P. **Aplicação do Padrão de Projeto MVC com JSF.** Monografia apresentada à disciplina Trabalho de Graduação III, do Curso de Ciência da Computação da Faculdade de Jaguariúna, sob a orientação do Prof. Ms. Peter Jandl Jr. Jaguariúna, 2008.

SMALLTALK. **The History of Smalltalk**. Disponível em: < http://www.smalltalk.org/smalltalk/history.html> Acesso em 28/ago/2012.

VANZOLINI, Carlos Alberto. **Manual de Comunicação com o Cliente: NBR ISO/IEC 27001**. Elaborada pela Diretoria de Certificação da Fundação Vanzolini. USP – SP, 2011.