Métricas e Artefatos para a Priorização de Investimentos no Ajuste de Conformidade à Norma ISO 17799

Reinaldo de B. Correia, André H. I. de Azevedo, Luiz F. Rust da C. Carmo

Núcleo de Computação Eletrônica – Universidade Federal do Rio de Janeiro (UFRJ)
Caixa Postal 2324 – 20.010-974 – Rio de Janeiro – RJ – Brasil

{reinaldo, andre, rust}@nce.ufrj.br

Abstract *One of the great challenges of information security area concerns the development of methods and models to assist mitigation of the risks which current systems are submitted, consequence of the great diversity/complexity of those systems, and the wide gamma of vulnerabilities and potential attacks. This paper deals with the development of new metrics and models to assist the process of a compliance adjustment to the ISO 17799 standard. Basically, we have investigated different forms to characterize compliance (and compliance sensitivity to its controls) to be used in a prioritization process of the required controls.*

Resumo. *Um dos grandes desafios da área de segurança é estabelecer métodos e modelos para se aferir e planejar a mitigação dos riscos existentes, dado a grande diversidade e complexidade dos sistemas atuais e da larga gama de vulnerabilidades e potenciais ataques. Este artigo propõe o desenvolvimento de novas métricas e modelos específicos que auxiliem o processo de ajuste de conformidade à norma ISO 17799. Basicamente, investigam-se diferentes formas de expressar a conformidade* (*e sensibilidade desta conformidade aos respectivos controles), gerando subsídios para um processo de priorização da implementação dos controles necessários.*

1. Introdução

Nos últimos anos, observa-se uma crescente preocupação com a Segurança da Informação (SI) nas organizações em todo mundo. As empresas começam a perceber que a segurança é mais do que proteção dos dados, da informação ou dos sistemas de um negócio. É a proteção do próprio negócio em si [Solms 2005]. A identificação dos possíveis riscos a que uma empresa está exposta se tornou uma atividade essencial no cenário atual. Além da identificação destes riscos, a organização precisa tomar medidas de controle que os eliminem ou os reduzam ao nível considerado “aceitável”.

Um dos maiores desafios encontrados está na dificuldade em mensurar o custo-benefício das medidas de controles mais apropriadas para a mitigação dos riscos, aliadas ao fato de que a grande maioria das empresas possui recursos escassos para investimento em SI. Logo, identificar e analisar os riscos mais críticos ao negócio fim da organização e escolher a melhor estratégia de mitigação de riscos tornaram-se processos por demais complexos.

Neste contexto, grandes empresas, agências governamentais e instituições internacionais têm trabalhado para estabelecer padrões e normas que reflitam as melhores práticas de mercado relacionadas à segurança dos sistemas e informações. Uma das primeiras normas sobre o assunto foi criada pelo *British Standards Institute* (BSI) e foi catalogada como BS 7799 [BSI 2002]. Após um trabalho intenso de consulta pública e internacionalização, em

primeiro de dezembro de 2000, a BS 7799 foi aceita como padrão internacional pelos países membros da *International Standards Organization* (ISO), sendo então denominada ISO/IEC 17799 [ISO/IEC 2005]. No ano 2001, a norma foi traduzida e adotada pela Associação Brasileira de Normas Técnicas (ABNT) como NBR 17799 - Código de Prática para a Gestão da Segurança da Informação. A norma define 127 controles que podem compor o escopo do sistema de gerência de segurança (*Information Security Management System* - ISMS), enfocando o processo sob o ponto de vista do negócio da empresa. A conformidade dos processos corporativos com a norma ISO 17799 permite que as empresas demonstrem aos seus parceiros de negócio e clientes o seu comprometimento com a Confidencialidade, a Integridade e a Disponibilidade das informações por elas manipuladas. Para definir o escopo do ISMS e os controles apropriados para a empresa, a norma exige que seja realizado um processo de análise de riscos que vai determinar a necessidade, a viabilidade e a melhor relação custo-benefício para a implantação desses controles. Além disso, é possível obter uma certificação desse ISMS, através de uma auditoria realizada por uma certificadora, de forma similar aos processos bastante conhecidos de ISO 9000.

A análise de conformidade é utilizada para comparar o nível atual da segurança da informação com relação à norma 17799, e pode ser aplicada a um departamento, a um processo de negócio ou a uma empresa como um todo. A implantação de suas recomendações permite obter um maior grau de conformidade à norma e, eventualmente, uma certificação perante os órgãos competentes.

O projeto AGRIS[1] [Carmo 2005] (Análise e Gerência de Riscos em Segurança), desenvolvido através do programa FRIDA, tem como principal objetivo o desenvolvimento de ferramentas focadas às práticas organizacionais latino-americanas (enfatizando as brasileiras), levando em conta nossas particularidades culturais e restrições de recursos, mas respeitando integralmente às recentes normas e padrões internacionais correlatos. O ambiente AGRIS incorpora ferramentas de apoio à análise de decisão de investimentos em Segurança da Informação. Mais especificamente, através de sua utilização, o gestor pode avaliar quais domínios da ISO/IEC 17799, e os respectivos controles, são relevantes para que a organização fique com seus processos em conformidade com esta norma (Análise de Conformidade).

A primeira versão dessa ferramenta de análise de conformidade tem como entradas: o orçamento global destinado a Segurança da Informação, a relevância do domínio, o grau de conformidade e o custo de cada controle do domínio. Na saída, a ferramenta gera uma lista de priorização dos investimentos por domínio, mediante os seguintes passos: (i) a informação de relevância atribuída pelo gestor de SI é usada para fazer um rateio do orçamento pelos domínios; (ii) o gestor determina o grau de conformidade atual e o grau de conformidade desejado de cada controle do domínio (denominado *gap* do controle); (iii) o orçamento de um domínio é rateado entre os controles, considerando como fator de peso a razão entre o *gap* do controle e o somatório de todos os *gaps*.

Apesar de bastante útil, a estratégia descrita acima parte da premissa que o gestor é capaz de estimar o grau de conformidade desejado. Uma informação errada do gestor pode comprometer completamente a distribuição do orçamento, deixando de maximizar a "conformidade" em si.

---

[1] *Projeto financiado pelo Programa FRIDA - Fundo Regional para a Inovação Digital na América Latina e Caribe*

O principal objetivo da proposta apresentada neste artigo é apresentar uma alternativa para a modelagem do cálculo da conformidade de um sistema de forma a permitir estudos complementares de maximização do retorno dos investimentos em vista de um desejável aumento desta conformidade. Isto é feito sem que o gestor de segurança precise então arbitrar o grau de conformidade desejado para cada controle.

Em suma, este artigo define um conjunto de métricas e artefatos, para o equacionamento do cálculo da conformidade, que quantificam o estado dos controles e a importância dos diversos requisitos de segurança ao negócio específico da instituição sob análise. Em seguida, após serem apresentadas e definidas, duas formas alternativas para modelagem da conformidade são submetidas a uma análise comparativa e conclusiva em face dos requisitos levantados. Por último, o modelo de conformidade exponencial é aplicado em alguns casos hipotéticos para análise da sensibilidade da conformidade frente aos diferentes controles.

2. Trabalhos relacionados

A condução de uma análise do tipo custo-benefício direcionada aos ativos de segurança da informação é reconhecidamente um trabalho de extrema dificuldade que vem suscitando diferentes propostas na literatura. Abordagens unindo modelos baseados em estimativas de riscos são relativamente recentes e visam à redução das vulnerabilidades de uma forma gradual e interativa.

As melhores práticas atuais que versam sobre Gestão de Riscos (CobiT [IT Governance Institute 2007], ITIL [BS ISO/IEC 2005], OCTAVE [Alberts e Dorofee 2002]) não incorporam o custo de implementação das contramedidas, uma vez que adotam modelos cujos objetivos primordiais são a criação de *frameworks* que auxiliem o gestor de riscos para que este melhor identifique, trate e controle os riscos existentes nas organizações.

Uma novidade da abordagem apresentada neste artigo é a realização de uma análise de custo-benefício sob o prisma da análise de conformidade. A maioria das abordagens usa métricas de aferição para capturar e estimar riscos. Na proposta apresentada, considera-se a norma ISO 17799 como referência de fato, e procura-se maximizar os investimentos para alcançar esta referência. Ou seja, considera-se que os riscos são indiretamente mitigados com essa aproximação aos procedimentos normativos. O custo-benefício é extraído de uma análise de conformidade e não de uma análise de riscos.

[Cum et al. 2003] propõe um processo analítico hierárquico para consolidação da análise de risco tendo em vista os critérios introduzidos pela BS7799. O grande mérito desta proposta é reconhecer e aproveitar o enorme trabalho de convergência realizado pelos especialistas na elaboração desta norma. Porém, não faz nenhuma proposta de avaliação de custo-benefício.

[Butler 2002] propõe uma metodologia, denominada SAEM (*Security Attrubute Evaluation Method*), para análise de custo-benefício em investimentos de segurança. Basicamente, essa metodologia insere uma etapa de avaliação dos investimentos após uma etapa de análise de riscos. Cada uma destas etapas é feita através de uma análise multiatributos de forma a aprimorar o processo de estimativas: (i) análise de risco - tipo de perdas, freqüência e peso; (ii) avaliação de investimentos - benefício, eficiência, cobertura e custo. Esta proposta tenta contornar o caráter subjetivo das diversas aferições necessárias através de uma rígida estruturação metodológica.

[Arora 2004] também propõe uma metodologia estruturada de forma a realizar uma avaliação de retorno de investimentos atrelada a um processo de análise/mitigação de riscos.

Uma peculiaridade desta proposta é que o problema da subjetividade dos parâmetros envolvidos é minimizado através da prerrogativa inicial de uma extensa base de dados correlacionando incidentes e prejuízos causados.

Apesar de não oferecerem diretamente uma avaliação de custo-benefício, [Jung et al. 1999] e [Liao e Song 2003] exploram uma vertente diferente, baseada no uso de reconhecimento de padrões, para o desenvolvimento de um sistema de análise de riscos assistido (estes sistemas podem ser facilmente estendidos para também considerar também o retorno de investimentos). A partir de uma estrutura padrão de classificação para os eventos passados, o sistema pode inferir o grau de similaridade do evento atual. Apesar de estes sistemas serem capazes de proporcionar sugestões úteis baseadas nas experiências anteriores, é necessário um tempo considerável para a criação de um conjunto significativo de casos conhecidos. Ainda, se um novo caso acontecesse sem casos similares no passado, o resultado gerado em quase nada ajudaria no processo de análise de riscos.

3.Métricas e Artefatos

3.1 Métricas de Aferição

As métricas de aferição identificadas no presente trabalho são os *graus de conformidade e de impacto* que estão associados a cada um dos controles que constituem um domínio. Segundo a norma ISO/IEC 17799, o conjunto de domínios define todos os aspectos de segurança que devem ser considerados junto aos sistemas de informação.

Os *graus de conformidade* dos controles, que normalmente são quantificados pelos usuários do sistema de informação, exprimem (dentro de uma escala) o quanto um determinado controle está concluído (implementado), ou seja, espelham o nível de suficiência (acabamento) de determinado controle. O grau de conformidade independe de qualquer outra consideração, não estando, por exemplo, relacionado à importância ou ao peso do controle a que está associado.

Os *graus de impacto* são comumente valorados por especialistas da área de segurança (também dentro de uma escala) e determinam a importância ou relevância de determinado controle no atendimento aos requisitos de segurança do domínio. Não denotam prioridade de um controle em relação a outro, uma vez que procuram expressar o fato de que certos aspectos de segurança (controles) quando não contemplados parcial ou integralmente tornam os sistemas de informação mais vulneráveis a ataques do que outros controles associados ao mesmo domínio.

Um artefato importante no desenvolvimento do modelo proposto neste artigo é o de *perfil*. O *perfil* pode ser de dois tipos: de *conformidade* e de *impacto*. O *perfil de conformidade* é o conjunto dos graus de *conformidade* de todos os controles de um domínio. Pode ser visualizado como um vetor, sendo cada elemento um grau de normalidade do controle correspondente a sua posição no vetor. Logo, a dimensão do perfil ou vetor de conformidade é igual ao número de controles do domínio.

O *perfil de impacto* é análogo ao *perfil de conformidade*, constituindo-se, entretanto, dos graus de impacto dos controles de um domínio. A dimensão do vetor ou perfil de impacto também é igual ao número de controles do domínio e, portanto, igual ao do vetor de conformidade. Os aspectos de segurança de um domínio são, portanto, caracterizados pelos perfis ou vetores de conformidade e de impacto que guardam os valores das métricas de aferição, graus de conformidade e de impacto.

Outra métrica importante é o *grau de impacto de domínio*, cujos valores são também atribuídos por especialistas da área de segurança da informação. Essa métrica tem natureza idêntica à métrica grau *de impacto*, diferenciando-se apenas por estar associada aos domínios e não aos controles dos domínios. O conjunto de *graus de impacto de domínio* constitui o perfil ou vetor de impacto do sistema de informação, possuindo dimensão igual ao número de domínios necessários para caracterizar os aspectos de segurança do sistema de informação.

3.2 Artefatos

Os artefatos utilizados são: a *conformidade de domínio*, a *conformidade do sistema de informação*, a *sensibilidade de domínio* e a *sensibilidade do sistema de informação*. O artefato *conformidade de domínio* informa, utilizando-se de uma escala normalizada, o quanto o sistema de informação, está conforme com a norma ISO/IEC 17799, considerando somente os aspectos de segurança atendidos pelo domínio em questão. Ao contrário das métricas de aferição, os valores do artefato *conformidade de domínio*, assim como todos os outros artefatos, são obtidos através de modelos matemáticos e não por atribuição pelo usuário do sistema ou pelo especialista de segurança. O modelo matemático estabelece a dependência entre a *conformidade de domínio* e as métricas de aferição *graus de conformidade e de impacto*, retratando que os controles produzem impactos diferentes no sistema de informação. Esses impactos diferenciados surgem devido, em maior grau, às características técnicas de segurança e, em menor grau, ao tipo de negócio alvo e os objetivos das instituições detentoras desses sistemas de informações.

Para a completa caracterização dos aspectos de segurança de todo um sistema de informação (definindo melhor o artefato *conformidade do sistema de informação*) faz-se necessário introduzir os artefatos de *perfis de conformidade e de impacto do sistema de informação*. O perfil de conformidade do sistema é um vetor que reúne todos os valores da métrica de conformidade de domínio, enquanto que o perfil de impacto do sistema de informação agrega os valores da métrica de aferição grau de impacto de domínio. Esses valores, tanto de conformidade quanto de impacto estão associados a cada um dos domínios. As dimensões desses perfis ou vetores são iguais ao número de domínios do sistema de informação. O conceito desses perfis, que exprimem globalmente os aspectos de segurança do sistema de informação em função da norma e da natureza do negócio da instituição, é similar ao conceito de perfil de domínio e de impacto, que refletem a mesma idéia, mas restringindo-se ao domínio.

A *conformidade do sistema de informação* possui caráter idêntico ao da *conformidade de domínio*. Entretanto, enquanto a primeira possui significado global ao sistema de informação, a segunda somente possui significado local, ou seja, informa o grau de atendimento à norma referente a um só domínio. Assim, a conformidade do sistema de informação é uma métrica, com valor numérico adimensional não superior que a unidade, destinada a informar o quão um determinado sistema de informação está de acordo com a norma e, portanto o seu grau de segurança. Presume-se, desta forma, que quanto mais conforme o sistema de informação (a conformidade do sistema de informação tendendo a 1) estiver com a norma, ou seja, quanto mais controles previstos na norma estiverem implementados e domínios plenamente implementados, mais seguro o sistema será. A conformidade do sistema de informação é calculada utilizando-se um modelo matemático semelhante àquele utilizado para a conformidade de domínio. Esse modelo assume que a conformidade do sistema de informação é função dos graus de conformidade de domínio (perfil de conformidade do sistema de

informação) e também dos graus de impactos de domínio (perfil de impacto do sistema de informação) associados a todos os domínios.

O artefato *sensibilidade de domínio* quantifica as variações da conformidade de domínio em função das variações produzidas nos graus de conformidade dos controles do domínio. Esse artefato pode ser utilizado para estabelecer critérios de prioridades de controles, uma vez que ele é capaz de identificar os controles, que tendo seus respectivos graus de conformidade, por exemplo, acrescidos, geram um maior aumento na conformidade do domínio. A priorização de controles está relacionada à criação de um esquema racional de aplicação de recursos na segurança dos Sistemas de Informação. Esse esquema visa tornar o sistema de informação o mais seguro possível a partir de um orçamento fixo e limitado.

O artefato *sensibilidade do sistema de informação* quantifica as variações da conformidade do sistema de informação considerando as variações das conformidades dos domínios. Este artefato é conceitualmente similar ao artefato sensibilidade de domínio, tendo, entretanto, como foco todo o sistema de informação e não somente um domínio. Possui também o importante papel de estabelecer prioridades. Mas, neste caso, em relação aos domínios e não aos controles.

4. Modelos e Análise dos artefatos

4.1. Premissas básicas

Os modelos matemáticos e a análise comportamental dos artefatos foram elaborados assumindo-se algumas premissas descritas a seguir.

A primeira premissa é referente aos valores máximos e mínimos das métricas de aferição e auxiliares. As métricas de aferição estão limitadas a valores máximos, denominados fundo de escala, que podem ser diferentes para cada uma dessas métricas (FE_{GC}: fundo de escala do grau de conformidade, FE_{GIC}: fundo de escala do grau de impacto do controle e FE_{GID}: fundo de escala do impacto de domínio). Neste trabalho, adotou-se um fundo de escala único e igual a 5 (cinco) para todas as métricas de aferição ($FE_{GC} = FE_{GIC} = FE_{GID} = 5$). Os artefatos sendo todos normalizados assumem o valor máximo igual à unidade.

A segunda premissa diz respeito aos valores intermediários que as métricas podem assumir entre os valores máximos e mínimos ($0 \leq V_{\text{métrica aferição}} \leq FE_X$, onde FE_X é o fundo de escala da métrica em questão). Para as de aferição, incluindo o zero, somente valores inteiros e discretos podem ser atribuídos ($Cv = \{0, 1, 2, \ldots, FE_X\}$, onde *Cv* é o conjunto de valores possíveis). Como o fundo de escala é cinco para todas as métricas, o conjunto dos valores possíveis ficou limitado a seis valores ($Cv = \{0, 1, 2, 3, 4, 5\}$). Essa simplificação, por um lado visa limitar a abrangência do problema, facilitando a análise do comportamento dos artefatos diante das métricas de aferição e, por outro, retratar mais fielmente a realidade de campo. É razoável admitir que os avaliadores, sendo eles usuários dos sistemas de informação (para grau de normalidade) ou especialistas em segurança (para impacto de controle e de domínio), provavelmente não possuem capacidade para discernir graus com precisão melhor que a unidade. Os artefatos podem assumir qualquer valor real entre zero e a unidade ($0 \leq V_{\text{artefato}} \leq 1$).

A terceira premissa trata do universo de análise na adoção do modelo mais adequado para o cálculo dos artefatos. Esse universo foi limitado a domínios de 3 a 5 controles, dependendo do foco da análise de que se está tratando. Considerando que o número de perfis aumenta exponencialmente em função do número de controles ($n_{Perfil} = (D[Cv])^{nctr}$, onde n_{Perfil} é o número de perfis, *D[Cv]* é a dimensão de *Cv*, ou seja, o número de valores discretos que

a métrica pode assumir e *nctrl* é o número de controles do domínio), é necessário limitar esse número para facilitar a análise, a coleta e a diagramação dos dados. Assim, o número de perfis ficou limitado entre 216 ($n_{Perfil} = 6^3$) e 7776 ($n_{Perfil} = 6^5$), presumindo-se que os resultados e conclusões são extensíveis a universos de domínios com número de controles quaisquer.

4.2. Requisitos

Antes de iniciar diretamente a análise dos dois modelos, é necessário identificar as características desejáveis da métrica conformidade de domínio para que ela cumpra seu objetivo de quantificar, de forma mais fiel possível, o quanto um sistema de informação atende aos requisitos de segurança discriminados na norma ISO/IEC 17799.

De imediato, é fácil perceber que a **primeira característica** dessa métrica é a de apresentar valores diferentes para perfis de conformidade distintos. Isto significa que, para conjuntos diferentes de graus de conformidade, esperam-se valores de conformidades de domínio distintos associados a cada um deles. É claro que os valores de conformidade de domínio estão associados ao mesmo perfil de impacto, ou, de outra forma, um determinado perfil de conformidade possui valores diferentes de conformidade de domínio para perfis de impacto também diferentes.

A segunda característica corresponde à necessidade de a métrica respeitar as condições de contorno, conforme formulado anteriormente, ou seja, os valores que essa métrica precisa assumir nas condições de contorno. Logo é preciso que, quando o sistema de informação esteja completamente desconforme, o modelo garanta que essa métrica seja igual a 0 (zero). Opostamente, quando for atribuído o valor máximo (FE_{GC}) aos graus de conformidade de todos os controles do domínio, o modelo deve atribuir o valor 1 (um) a essa métrica, indicando que o sistema de informação está plenamente conforme.

A **terceira característica**, a mais difícil de ser identificada, está relacionada à capacidade do modelo de refletir, no valor numérico calculado para a conformidade de domínio, as notas de valor zero atribuídas aos graus de conformidade. Essa capacidade é importante principalmente pelo fato de que alguns controles quando não implementados expõem o sistema de informação a um alto risco de ataque.

4.3. Modelos para a Conformidade de Domínio

O dois modelos analisados neste trabalho são, em ordem de complexidade, os modelos do produto normalizado, e o de modelo exponencial. A tabela 1 apresenta as expressões matemáticas que representam os respectivos modelos.

O modelo do produto normalizado apresenta uma expressão composta de dois termos. O primeiro calcula o somatório dos produtos dos graus de conformidade dos controles do domínio pelos respectivos impactos. O segundo termo é o fator de normalização, que divide o primeiro pelo maior valor possível que pode assumir o somatório, isto é, o produto do fundo de escala do grau de conformidade (FE_{GC}) pelo fundo de escala do grau de impacto de domínio (FE_{GIC}) e número de controles do domínio. O maior valor possível ocorre na situação em que todos os controles são valorados com o valor máximo tanto para o grau de conformidade (FE_{GC}) quanto para o grau de impacto (FE_{GIC}).

Assim, neste caso, o maior valor possível para a conformidade de domínio é um, atendendo a condição de contorno superior comentada anteriormente. A condição de contorno inferior também é satisfeita, pois caso os graus de conformidade forem zero para todos os

controles, todos os termos da soma será zero, tornando o resultado e, conseqüentemente, a conformidade nula. A principal falha desse modelo está na impossibilidade de dotar a métrica com a primeira e a terceira características. Em relação à primeira, pode-se afirmar que obter conformidades de domínio diferentes para todos os perfis de conformidade em relação a um perfil de impacto não é tarefa trivial, devido à existência de perfis de conformidade equivalentes.

Tabela 1. Expressões Matemáticas dos dois Modelos.

Modelo do Produto Normalizado ($CONFD_p$)	Termo 1 $\sum_{i=1}^{nctr} GC_i \times GIC_i \times \frac{1}{nctr \times (FE_{GC} \times FE_{GIC})}$
Modelo exponencial ($CONFD_e$)	$\left(1 - a^{\left(-k \sum_{i=1}^{nctr} GC_i\right)}\right) \times \zeta^{-\lambda \sum_{i=1}^{nctr} \left(GIC_i \times (FE_{GC} - GC_i) \times \alpha^{-GC_i}\right)}$ Termo 3 Termo 2

GC ---------- Grau de Conformidade de Controle
GIC --------- Grau de Impacto de controle
FE_{GC} ------- Fundo de escala do Grau de Conformidade
FE_{GIC} -------Fundo de escala do Grau de Impacto
$nctr$ ---------- Número de controles no domínio
ζ, λ, α, a e k -------- constantes

Por definição, perfis equivalentes são os perfis de conformidade diferentes que apresentam valores de conformidade de domínio iguais para um mesmo perfil de impacto. A equivalência pode ser de dois tipos, tipo 1 e tipo 2, que surgem por causa de dois fatores. A equivalência do tipo 1, ou equivalência natural, está associada a perfis de impacto com pelo menos dois controles com graus de impacto iguais. Isto pode ser facilmente constatado no diagrama da Figura 1.

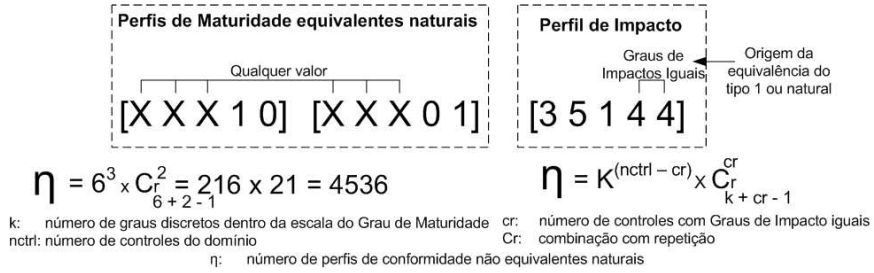

Figura 1. Equivalência natural ou do Tipo 1

O diagrama da Figura 1 mostra, para um domínio de dimensão 5 (número de controles igual a 5), um exemplo de dois perfis de conformidade equivalentes naturais em que a equivalência é produzida por dois controles com graus de impacto iguais a 4. Os dois perfis de conformidade equivalentes usados como ilustração mostram que graus de conformidade atribuídos de forma invertida nos dois controles com graus de impacto iguais produzem graus de conformidades iguais, apesar de os perfis de conformidade serem diferentes. A expressão apresentada na Figura 2 calcula o número de perfis de conformidade que não são equivalentes naturais (Tipo 1), não significando que esses não possam ser equivalentes do Tipo 2, como está descrito mais a diante. Do total dos 7776 perfis de conformidade (6^5) possíveis em um domínio com 5 controles, 3240 (41,7%) são perfis equivalentes naturais (Tipo 1), podendo os 4.536 (58,3%) restantes serem perfis equivalentes do Tipo 2 ou não equivalentes. A equivalência natural não é eliminada nos dois modelos propostos, ou qualquer modelo que venha a ser concebido devido à natureza das métricas envolvidas e ao esquema adotado na aferição da conformidade dos sistemas de informação. Para se conseguir tal efei-

to, algum tipo de atributo exclusivo de controle deveria ser criado. Esse atributo deveria possuir valor único para cada um dos controles, por exemplo, o uso da posição no perfil de controle seria uma forma de estabelecer prioridades para o controle.

Entretanto, isso não retrata a semântica desejada para a *prioridade*, que é intimamente atrelada à complexidade de implementação do controle, ao custo de implementação do controle e sua sensibilidade em relação à conformidade do domínio, conforme será visto mais adiante. O ponto importante sobre os perfis equivalentes naturais é o cuidado que se deve ter para desconsiderá-los nas simulações por introduzirem distorções nos respectivos resultados.

O outro tipo de equivalência, do Tipo 2 ou induzida, tem origem na baixa complexidade do modelo utilizado para o cálculo da conformidade do domínio e, também, no pequeno número de graus diferentes de normalidade e de impacto. Esse tipo de equivalência pode ser compreendido imaginando-se, por exemplo, dois ou mais perfis de conformidade diferentes com uma combinação de graus de conformidade tal que, ao aplicar o modelo, obtêm-se conformidades de domínio iguais. Esses perfis de conformidade se estiverem associados a um mesmo perfil de impacto sem graus de impacto iguais, garante-se que a equivalência envolvida é a induzida ou do tipo 2. No caso contrário, quando os perfis de conformidade estão associados a um perfil de impacto com graus de impacto iguais, deve-se tomar o cuidado de verificar se os perfis de conformidade pertencem ao conjunto de perfis de conformidade não equivalentes naturais, conforme detalhado anteriormente. A Figura 2 além de mostrar, em um domínio de dimensão 3 (com 3 controles), um grupo de dois perfis de conformidade possuindo equivalência induzida (o Perfil de conformidade não possui graus de impacto iguais, garantindo a inexistência de equivalências naturais), salienta que o modelo do produto normalizado não apresenta a característica 3, pois não gera valores de conformidade diferentes entre os perfis com e sem grau de conformidade zero.

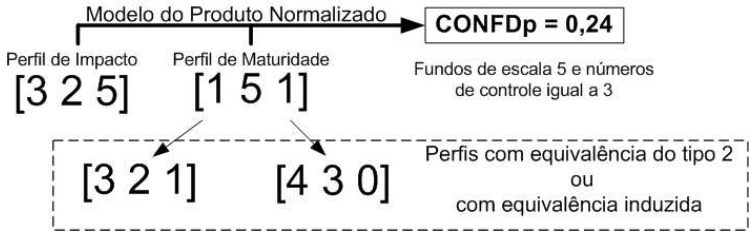

Figura 2. Equivalência induzida ou do tipo 2

Para contornar ou amenizar os problemas identificados no modelo do produto, foi concebido o modelo exponencial. A razão inicial pela escolha de um modelo que envolve funções exponenciais é que essas funções, para valores positivos da variável independente (expoente), têm valores compreendidos no intervalo $0 < a^{-x} \leq 1$, tornando a métrica conformidade de domínio naturalmente normalizada. Outra razão é o fato dessa função reproduzir comportamentos com maior complexidade do que somas e produtos, que são as operações usadas no modelo do produto. Essa maior complexidade visa amenizar, em relação ao modelo anterior, o problema da equivalência induzida de perfis de conformidade.

É possível compreender o modelo exponencial identificando-se na função, apresentada na Tabela 1, o papel dos diversos termos (destacados na tabela por elipses) que a compõem. O Termo 1, chamado de termo de conformação, tem como função garantir a condição de contorno inferior que determina como sendo zero o valor da conformidade de domínio quando o perfil de conformidade é zero (todos os controles possuindo graus de conformidade zero) e, ao mesmo tempo, ter contribuição nula no cálculo do valor da conformidade do do-

mínio para perfis de conformidade diferentes de zero (pelo menos um dos controles com grau de Normalidade diferente de zero). É fácil verificar que a exponencial da constante *a* torna-se 1 quando o somatório dos graus de Normalidade de seu expoente é igual a zero, fazendo com que o Termo 1 assuma o valor zero. Também, pode-se constatar que, considerando valores elevados para as constantes *a* e *k*, o resultado dessa exponencial é muito pequeno mesmo quando, no pior caso, o somatório dos graus de conformidade é igual a 1 (para o perfil de conformidade com um grau de conformidade 1 e os graus restantes com valor zero), tornando o valor do Termo 1 muito próximo da unidade.

Passando à análise do expoente da exponencial da constante zeta (ζ), observa-se que o somatório calcula a soma dos produtos de três termos. Esse somatório terá tantos produto-membros quantos forem os controles do domínio. O Termo 3, conforme indicado pela elipse na Tabela 1, garante que quando for atribuído o valor máximo aos graus de conformidade de todos os controles do domínio o expoente torne-se zero, assegurando assim a condição de contorno superior para a conformidade de domínio, isto é, quando todos os graus de conformidade do domínio são máximos, a conformidade de tal domínio deve ser 1 (exponencial da constante zeta (ζ) igual a 1), sinalizando que o domínio está plenamente conforme com a norma.

O Termo 2, também destacado na Tabela 1 por uma elipse, é um fator redutor do grau de impacto que tem como função dotar o modelo com a terceira característica descrita anteriormente. Assim o Termo 2 penaliza exponencialmente os perfis de conformidade que possuam controles com graus de conformidade de valores zero. Este efeito é alcançado reduzindo o valor do grau de impacto do controle para graus de conformidade crescentes diferentes de zero, sendo a maior redução correspondente ao grau de conformidade igual ao fundo de escala do grau de conformidade (α^{-FEGC}). A exponencial de base α é igual a um quando o grau de conformidade for zero, não contribuindo no valor do produto-membro e, conseqüentemente, no valor final do somatório. Salienta-se que haverá tantos produto-membros com a exponencial de base α igual a 1 quantos forem o número de graus de conformidade de valor zero no perfil de conformidade, penalizando mais intensamente os perfis de conformidade com maior número de controles com grau de conformidade zero. Notar também que neste caso o valor do expoente de zeta (ζ) é maior, tornando o valor da respectiva exponencial menor, o que reduz o valor final da função e conseqüentemente da conformidade de domínio.

4.4. Análise comparativa dos modelos propostos

Os dois modelos foram comparados utilizando-se dois critérios: a equivalência induzida de perfis de conformidade e a equivalência de perfis parcialmente nulos. A equivalência induzida reflete a capacidade do modelo em gerar o maior número de graus de conformidade de domínio diferentes para o maior número possível de perfis de conformidade. Já a equivalência de perfis parcialmente nulos demonstra a habilidade do modelo em não permitir que perfis de conformidade parcialmente nulos não tenham valores de grau de conformidade de domínio iguais a perfis de normalidade não nulos. Recapitulando, os perfis de conformidade nulos são aqueles que possuem todos os controles do domínio com graus de conformidade iguais a zero, enquanto os não nulos possuem graus de conformidade de todos os controles diferentes de zero. Os parcialmente nulos contêm pelo menos um dos controles com grau de normalidade igual a zero.

Como é natural que essa diferenciação tenha que se refletir em valores de conformidade de domínio diferentes, as simulações visaram o cálculo desses valores diante de diversas combinações de perfis de conformidade e de impacto. Para os dois critérios, realizaram-

se simulações com as seguintes constantes para o segundo modelo: a = 100, k = 10, ζ = 1,5, λ = 1/8 e α = 2. Esses valores foram estabelecidos empiricamente por intermédio de simulações prévias, procurando-se gerar valores de conformidades os mais homogêneos possíveis para a faixa de dimensão de domínios escolhida ($3 \leq D[D] \leq 7$). Nos dois modelos, os fundos de escala dos graus de conformidade e de impacto foram iguais a 5, sendo possível atribuir a ambos os graus somente valores discretos e inteiros, incluindo o zero

A idéia básica das simulações referentes ao critério da equivalência induzida foi a de contabilizar, para diversos perfis de impacto, o número de perfis de conformidade que geravam valores de conformidade diferentes, sem considerar a equivalência natural. Na simulação foram usados perfis de impacto com graus de impacto distintos para cada um dos controles do domínio. A Tabela 2 apresenta os resultados obtidos para duas dimensões de domínio e perfis de impacto.

Tabela 2. – Número de perfis com Equivalência Natural.

Modelo	Perfis de Impacto					
	[213]	[543]	[125]	[1253]	[5243]	[2314]
Produto Normalizado	185	159	175	1240	2227	1245
Exponencial	66	44	52	822	722	853
Total de Perfis	216			1296		

Pelos resultados, constata-se um número sensivelmente menor de perfis com equivalência induzida para o modelo exponencial do que para o modelo do produto normalizado, confirmando a necessidade de funções com maior grau de complexidade. A Figura 3 mostra o gráfico de conformidade de domínio (CONFD) x Perfis de Conformidade (PC) para os dois modelos considerando um perfil de impacto fixo ([543]). Os perfis de conformidade foram marcados no eixo das abscissas em ordem crescente de graus de conformidade, sendo a origem o perfil zero ([0,0, ...,0,0]). A primeira marca corresponde ao segundo perfil imediatamente superior ([0,0, ...,0,1]) e assim sucessivamente até o último perfil ([5,5, ...,5,5]). Cada uma das três colunas da Figura 5 contém os gráficos das três dimensões de domínio simuladas. Os gráficos inferiores são continuações dos gráficos superiores. Reparar que a origem dos gráficos inferiores corresponde a perfis diferentes de zero.

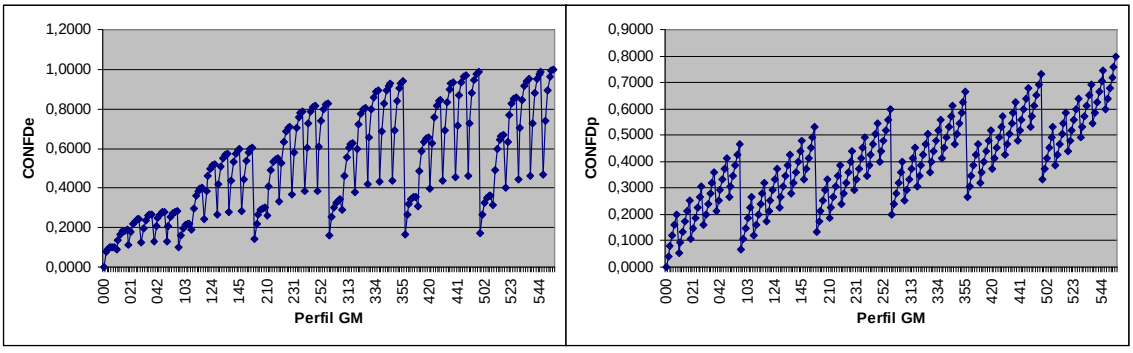

Figura 3. Gráficos Conformidade de Domínio x Perfis de Conformidade.

Esses gráficos mostram claramente o comportamento da conformidade calculada pelos dois modelos. Traçando-se uma linha paralela ao eixo das abscissas e excursionando essa linha ao longo do eixo das ordenadas fica evidente a ocorrência da redundância induzida, bastando para tal verificar se a reta intercepta os gráficos (do modelo de produto e exponencial) em mais de um ponto do mesmo gráfico. Após uma rápida análise gráfica por meio dessa reta, verifica-se que o modelo exponencial é mais apropriado para o cálculo da métrica conformidade de domínio por apresentar um menor número de perfis de conformidade com

equivalência induzida (menor número de pontos de cruzamento da reta com o gráfico do modelo exponencial).

Para o segundo critério de comparação, equivalência de perfis parcialmente nulos, as simulações foram concebidas de forma similar à anterior, só que neste caso computando os números de perfis de conformidade com pelo menos um controle com grau de conformidade zero que possuem o mesmo valor de conformidade de domínio de qualquer perfil de conformidade não nulo. Os resultados mostraram que o desempenho do modelo exponencial é semelhante ao do obtido no teste anterior, demonstrando o efeito do termo exponencial da constante α na composição do grau de conformidade do domínio para perfis de conformidade com graus de conformidade de valores zero.

5. Uso do modelo exponencial para cálculo da sensibilidade

Conforme definido anteriormente, o artefato *sensibilidade de domínio* exprime a influência de um determinado controle na conformidade de domínio, ou, em outras palavras, revela a capacidade de um controle em produzir alterações na conformidade de domínio a partir de variações geradas no grau de conformidade do referido controle em função de um Perfil de impacto fixo. Sua notação é S^k_d onde d é número do domínio e k o do controle. O seu cálculo pode ser expresso por $S^k_d = (CONFD(Ref) - CONFD(Cor)) / CONFD (Ref)$..... (1), onde CONFD (Ref) é o grau de conformidade do domínio referência e CONFD(Cor) a conformidade do domínio corrente, ou seja, após ser realizado o incremento no grau de conformidade do domínio referência.

Com o intuito de analisar o uso do modelo exponencial em (1) foram executadas simulações para diversas configurações de domínio e de perfil de impacto. As configurações consistem em estabelecer as dimensões do domínio, os perfis de conformidade a partir dos quais se efetuaram os aumentos sucessivos do grau de conformidade, os números de controles em que foram realizados simultaneamente os aumentos, os perfis de impacto e modelo usado. A Tabela 3 mostra os itens das três configurações selecionadas nas simulações.

Tabela 3 – Configurações das simulações

Dimensão do Domínio	3	5	8
Perfis de Impacto	[315]	[13524]	[32114532]
Perfis de Conformidade	[122]	[10231]	[22031243]
Nº de ctrls c/ alterações simultâneas	1	1	1
Intensidade de incremento	1, 2, 3, 4 e 5	1, 2, 3, 4 e 5	1, 2, 3, 4 e 5
Controles utilizados	Todos	Todos	Todos
Modelo usado	Exponencial	Exponencial	Exponencial

As Tabelas 4, 5 e 6 apresentam os valores da sensibilidade e da intensidade de aumento produzidos separadamente no grau de conformidade para cada um dos controles do domínio. Cada coluna dessas tabelas se refere a cada um dos controles numerados em relação ao perfil de impacto do menor ao maior índice (da esquerda para direita ou de cima para baixo no vetor).

Tabela 4. Sensibilidade x Intensidade p/ PI = [315] e PC = [122]

Intensidade	Ctrl1 (GC=2)	Ctrl2 (GC= 2)	Ctrl 3 (GC=1)
1	0,1351	0,0257	0,2093
2	0,1903	0,0355	0,3048
3	0,2093	0,0387	0,3426
4			0,3554

Observa-se pelos resultados obtidos que a sensibilidade é dependente do perfil de impacto, da dimensão do domínio, dos valores dos graus de conformidade - a partir dos quais

se produzem as variações nesses graus de conformidade, da intensidade dessas variações e, também, do número de controles que tenham seus graus de conformidade alterados simultaneamente. Um perfil de impacto que apresenta um grau de impacto de valor alto para um determinado controle tende a tornar a sensibilidade referente a esse controle maior que outro que possui um grau de impacto baixo. É fácil perceber que domínios de dimensões elevadas (grande número de controles) fazem com que cada controle individualmente tenha menos participação na composição do grau de conformidade de domínio, possuindo, portanto, cada um dos controles sensibilidades menores do que aqueles pertencentes a domínios de dimensão baixa (poucos controles). A intensidade da alteração também pode ter influência, pois a intensidade das variações obtidas na sensibilidade pode não seguir um padrão linear.

Tabela 5. Sensibilidade x Intensidade p/ PI = [13524] e PC = [10231]

Intensidade	Ctrl 1 (GC=1)	Ctrl 2 (GC=3)	Ctrl 3 (GC=2)	Ctrl 4 (GC=0)	Ctrl 5 (GC=1)
1	0,2884	0,0192	0,1351	0,5780	0,0654
2	0,4259	0,0257	0,1903	0,9083	0,0927
3	0,4811		0,2093	1,0590	0,1032
4	0,5000			1,1186	0,1067
5				1,1388	

Tabela 6. Sensibilidade x Intensidade p/ PI = [32114532] e PC = [22031243]

Intensidade	Ctrl 1 (GC=3)	Ctrl 2 (GC=4)	Ctrl 3 (GC=2)	Ctrl 4 (GC=1)	Ctrl 5 (GC=3)	Ctrl 6 (GC=0)	Ctrl 7 (GC=2)	Ctrl 8 (GC=2)
1	0,0192	0,0095	0,1351	0,2884	0,0095	0,1642	0,052	0,079
2	0,0257		0,1903	0,4259	0,0128	0,2404	0,0722	0,1102
3			0,2093	0,4811		0,2722	0,079	0,1208
4				0,5		0,2843		
5						0,2884		

6. Conclusão

A priorização de investimentos no ambiente empresarial torna-se cada dia mais importante considerando a atual escassez de recursos e a necessidade de se obter o maior retorno da aplicação desses recursos. Um dos maiores desafios encontrados atualmente pelos gestores de segurança da informação é determinar o custo-benefício das medidas de controles mais apropriadas para a mitigação dos riscos de segurança.

Uma novidade da abordagem apresentada neste artigo é a proposta de uma análise de custo/benefício sob o prisma da análise de conformidade, diferentemente da maioria das abordagens, que usam técnicas de modelagem do risco sobre um conjunto de métricas de aferição extremamente difíceis de serem estimadas. Na proposta apresentada, considera-se a norma ISO 17799 como referência de fato, e procura-se maximizar os investimentos para alcançar esta referência. Ou seja, considera-se que os riscos são indiretamente mitigados com essa aproximação aos procedimentos normativos. O custo/benefício é extraído de uma análise de conformidade e não de uma análise de riscos.

A partir da definição de duas métricas de aferição - conformidade e grau de impacto de um controle a um certo domínio - investigou-se dois diferentes modelos matemáticos para expressar a conformidade do sistema e também a sensibilidade da *conformidade* a um controle específico, gerando subsídios para um processo de priorização da implementação dos controles necessários. Pelos resultados obtidos através de simulações, verifica-se uma maior adequação do modelo exponencial para o cálculo da conformidade de um domínio, por este apresentar um menor número de perfis de conformidade com equivalência induzida. Este modelo exponencial foi em seguida aplicado em alguns casos selecionados, de forma a permitir uma análise da sensibilidade da conformidade frente aos diferentes controles.

Como trabalho futuro, pretende-se investigar a necessidade de incluir novos parâmetros para a concepção de um modelo de priorização mais preciso, como por exemplo: a complexidade de implementação do controle. A complexidade reflete a dificuldade de se obter os recursos materiais e humanos para que um determinado controle seja implementado (não diz respeito ao custo, pois independentemente do custo de implementação, para se concluir tal tarefa podem ser necessários equipamentos ou recursos humanos não facilmente disponíveis no momento).

7. Referências

Solms, B. V, Solms, R. V. (2005). From information security to business security?, Computers & Security, 24, pp. 271-273.

BSI. (2002). BS 7799 - Information Security Management – Part 2: Specification for Information Security Management System.

ISO/IEC. (2005). FDIS 17799:2005 - Information techniques – Security techniques – Code of pratice for information security management.

IT Governance Institute. (2007).COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2. edição, ISACA.

Alberts, Christopher e Dorofee, Audrey. (2002). Managing Information Security Risks: The OCTAVE Approach, Ed. Addison-Wesley.

Cum, B., Lo, C., Wong, P., Hwong, J. (2003). Evaluation of information security related risks of an organization: the application of the multicriteria decision-making method, Anais do IEEE 37th Annual 2003 International Carnahan Conference on Security Technology.

Butler, S.A. (2002). Security Attribute Evaluation Method: A Cost-Benefit Approach, Anais do ICSE'02 - International Conference on Software Engineering, EUA.

Arora, A., Hall D., Pinto, C.A., Ramsey, D., Telang, R. (2004) Measuring the Risk-Based Value of IT Security Solutions, IT Professional, vol. 06/6, pp.35-42, Nov/Dez.

Liao, G., Song, C. (2003). Design of a Computer-Aided System for Risk Assessment on Information Systems, Anais do IEEE 37th International Carnahan Conference on Security Technology.

C. Jung, I. Han; and B. Suh. (1999). Risk Analysis for Electronic Commerce Using Case-Based Reasoning, International Journal of Intelligent Systems in Accounting, Financial & Management, vol. 8, pp. 61-73.

Carmo, L.F.R.C., Alves, G.A.A., Costa, R.B.C., Reis Junior, C.A. (2005). Estratégias de mitigação de riscos de segurança de segurança do ambiente AGRIS. Anais do SSI'2005 - 7º Simpósio Segurança em Informática.

Zhao, D., Wang, J., Wu, J., Ma, J. (2005). Using Fuzzy Logic and Entropy Theory to Risk Assessment of The Information Security. Anais do Fourth International Conference on Machine Learning and Cybernetics, Guangzhou.

He, Q., Otto, P., Antón A.I., Jones, L. (2006). Ensuring Compliance between Policies, Requirements and Software Design: A Case Study. Anais do Fourth IEEE International Workshop on Information Assurance (IWIA'06).