José Maria Cardoso Salgado Mexia Alves

Análise do Risco dos Sistemas Informáticos de Suporte à área Financeira

Número: 200600191

Fevereiro 2010

Universidade de Coimbra

Faculdade de Economia da
Universidade de Coimbra

Mestrado em Economia Financeira

Análise do Risco dos Sistemas Informáticos de Suporte à área Financeira

José Maria Cardoso Salgado Mexia Alves

Relatório de Estágio orientado por:
Professor Doutor Pedro Godinho

Fevereiro 2011

Resumo: O presente trabalho descreve a experiência do estagiário ao longo de dezanove semanas na equipa de "Information Technology Risk and Assurance" da empresa Ernst & Young e a sua participação no projecto de apoio à Auditoria Financeira a um banco que por razões de confidencialidade será designado por BGE (Banco Genérico de Estudo).

Este projecto consistiu na avaliação dos ITGCs (Information Technology General Controls), ou seja, na avaliação dos controlos de seguranças dos sistemas informáticos no âmbito da Auditoria Financeira, passando pela análise dos controlos de Gestão de Alterações (GA), Gestão de Acessos Lógicos (GAL) e Operações (O).

Ao longo do estágio foram detectados pontos onde poderia ser acrescentado valor, tais como a criação de um padrão que permita apoiar as decisões de considerar a segurança de um sistema eficaz ou não ou o uso de um método de quantificação que forneça ao cliente uma visão simplificada sobre o estado de segurança dos seus sistemas.

Para estes efeitos foi utilizada uma adaptação do método AHP (Analytic Hierarchy Process) criado por Satty, 2001.

Através desta adaptação e do uso de cenários de sistemas cuja segurança é considerada eficaz e não eficaz foi possível chegar um modelo que permite a criação de um padrão que pode servir de apoio à atribuição das avaliações.

Ainda a partir da adaptação do método AHP chegou-se a um método que permite quantificar a segurança dos sistemas informáticos de modo a fornecer ao cliente uma primeira impressão sucinta do estado de segurança dos seus sistemas.

Palavras-chave: Apoio à Auditoria Financeira, ITGC, GA, GAL, O, AHP.

Abstract: The present work describes the experience of the intern throughout nineteen weeks in the team of "Information Technology Risk and Assurance" of the company Ernst & Young and his participation in the Financial Audit support to a bank that for confidential reason will be named as BGE (Banco Genérico de Estudo).

This project consisted in the evaluation of the ITGCs (Information Technology General Controls), in other words, it consisted in the evaluation of the Information Systems security con-

trol in the scope of Financial Audit, passing through the analysis of the Gestão de Alterações (GA), Gestão de Acessos Lógicos (GAL) and Operações (O) controls.

Throughout the internship period there were detected some points where there could be added value, such as the creation of a standard which would be able to support in the decision of considering the security of a system effective or not or the use of a quantifying method which would give the client a simple view of his systems security.

For this purposes it was used an adaptation of Satty's, 2001 AHP (Analytic Hierarchy Process) method.

Making use of this adaptation and using scenarios of systems which security was considered effective and ineffective it was possible to arrive to a model that enables the creation of a standard which can support the evaluations.

Still from the AHP method adaptation it was constructed a method which permits to quantify the security of the information systems in a way that makes it possible for the client to have a first impression about the security of his systems.

Keywords: Financial Audit support, ITGC, GA, GAL, O, AHP.

Agradecimentos

Agradeço à Ernst & Young por me ter permitido fazer este estágio e por me ter facilitado as ausências necessárias para assistir às aulas de Seminário de Investigação e reunir com o orientador. Aos meus colegas que me ajudaram sempre que os solicitei e especialmente ao meu tutor David Oliveira que me apoiou ao longo todo o processo fornecendo aconselhamentos e respondendo às minha questões.

Agradeço de modo particular ao meu orientador de estágio, Professor Pedro Godinho, que sempre se mostrou disponível para me ajudar a fazer um trabalho melhor e sem o qual não teria sido possível a sua concretização.

Para a Professora Maria Adelaide Duarte vão os meus agradecimentos porque, através das aulas de Seminário de Investigação, me ajudou e facilitou a concepção deste relatório de estágio.

A ambos os Professores agradeço o encorajamento que sempre me deram tentando demonstrar que estaria a fazer um bom trabalho.

Por último, agradeço aos meus Pais o apoio que me deram na revisão do texto de modo a evitar eventuais falhas na sua escrita.

Sumário

Análise do Risco dos Sistemas Informáticos de Suporte à área Financeira

1. Introdução

Os sistemas informáticos são, hoje em dia, imprescindíveis a praticamente todas as empresas.

Os benefícios da utilização destes sistemas são múltiplos e variados, nomeadamente, permitindo às empresas terem um sistema de acesso central ao dados, manter facilmente um *backup* da informação, distribuírem informação de um modo mais fácil, prepararem os impostos de um modo simplificado, identificarem características dos clientes, terem ganhos de eficiência e reduzir custos no uso de papel e armazenamento de informação.

No entanto será necessário ter em conta que o uso de sistemas de informação também apresenta alguns riscos que são muitas vezes negligenciados por parte das empresas.

Se a nível pessoal essa negligência pode não ter grande impacto, ao nível empresarial pode trazer perdas de valor enormes devido ao extravio, falta de integridade, falta de autenticidade ou indisponibilidade da informação.

Com o objectivo de compreender como as empresas lidam e devem lidar com este risco foram integrados os trabalhos da equipa de "Information Technology Risk and Assurance" (ITRA) de apoio à auditoria da empresa Ernst & Young.

Durante o período de estudo[1] foram efectuados trabalhos num banco, que será denominado como Banco Genérico de Estudo (BGE) por razões de confidencialidade, com o objectivo principal de avaliar a segurança e integridade dos dados financeiros relevantes de modo a aferir se a equipa de auditoria pode confiar neles ou não. Além do objectivo principal os trabalhos desenvolvidos também pretendem fornecer aconselhamento à empresa (BGE) em relação ao modo como podem gerir os seus sistemas informáticos de forma a assegurar que não existem perdas de valor por esse meio.

[1] Componente do estágio de José Maria Mexia Alves no quadro do 2º ciclo do Curso de Economia da Faculdade de Economia Universidade de Coimbra, realizado entre Setembro de 2010 e Março de 2011 na empresa *Ernst &Young*.

Com este fim são analisados os "Information Technology General Controls" (ITGC's) nos aspectos que referem à gestão de alterações (GA – de Gestão de Alterações), aos acessos lógicos (GAL – de Gestão de Acessos Lógicos) e Operações (O – Operações). Ao longo do texto será explicado mais aprofundadamente o que incorpora cada uma destas categorias.

Como resultado desta análise é decidido se os controlos em prática são ou não eficazes (*effective* ou *ineffective*), sendo este um ponto onde o presente trabalho pretende fazer uma melhoria ao desenvolver um método que permita suportar a decisão de atribuir o resultado *effective* ou *ineffective* e quantificar em que medida os controlos são eficazes ou não.

Os resultados produzidos pelo trabalho têm dois objectivos:

O primeiro é suportar, com base no estabelecimento de um padrão, a decisão de considerar se o risco de violações aos dados financeiros produzidos ou armazenados nos sistemas informáticos se encontrou devidamente mitigado durante o período de auditoria em causa.

O segundo destinar-se-ia a fornecer ao cliente, através da quantificação, uma visão simplificada do risco a que está sujeito, incentivando-o a melhorar os controlos nos casos em que o risco seja elevado.

Para atingir os objectivos é utilizada uma adaptação do método AHP de Satty, 2001 que é descrito na secção 2.

De seguida, no ponto 3.1 é descrito o trabalho efectuado pelo estagiário na empresa Ernst & Young e que serve de base para o estudo efectuado.

Na secção 3 é descrito todo o trabalho realizado para atingir os objectivos propostos, passando pela aplicação do método AHP ao caso em estudo (3.2.1), pela construção de cenários que nos permitem criar o padrão referido no primeiro objectivo (3.2.2) e pela aplicação prática ao resultado obtidos a partir da análise efectuada para o BGE ao longo do período de estágio (3.2.3).

Para finalizar as conclusões são apresentadas na secção 4.

2 - Revisão da Literatura: Metodologia a utilizar[2]

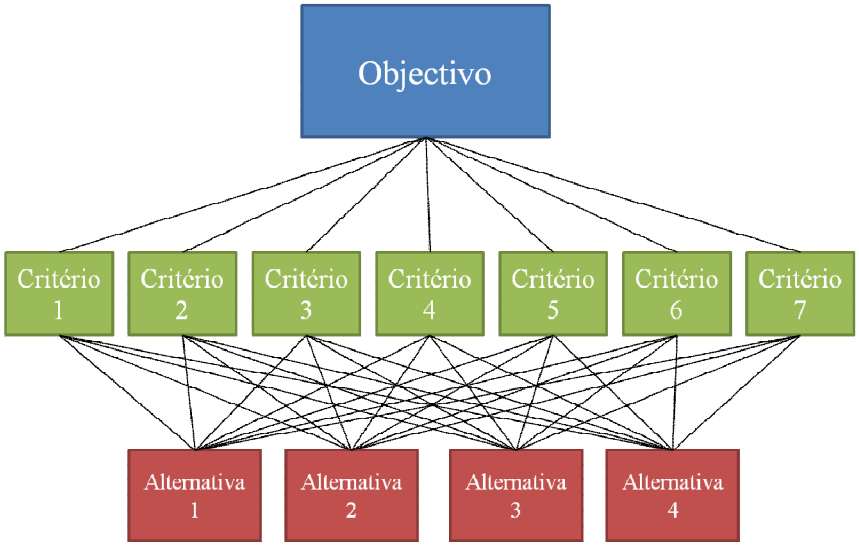
Para quantificar o risco associado aos sistemas de informação optou-se, de entre um vasto conjunto de métodos, pelo método Analytic Hierarchy Process (AHP).

De modo a possibilitar uma mais fácil compreensão da sua aplicação é feita, de seguida, uma descrição sucinta do método.

O método AHP baseia-se na construção de uma hierarquia de critérios em que o topo é o critério de síntese (o objectivo) e os níveis inferiores são os critérios que influenciam ou têm impacto nalgum critério de nível superior.

Após construída esta hierarquia, os critérios são comparados par-a-par, permitindo atribuir-lhes uma prioridade, ou importância, numérica.

Ilustração 1 - Árvore de Hierarquias



Fonte: Adaptação de (Satty & Vargas, 2001)

Segundo Saaty, autor do método, a avaliação deverá ser composta de acordo com a seguinte escala semântica, dados dois elementos i,j:

a_{ij} = 1 se i e j são igualmente prioritários

3 se i é fracamente mais prioritário do que j

5 se i é fortemente mais prioritário do que j

7 se i é demonstravelmente mais prioritário do que j

[2] Para esta secção são seguidos os textos de (Dias, 2002), (Dias, Almeida, & Clímaco, 1997) e (Satty & Vargas, 2001)

9 se i é absolutamente mais prioritário do que j

A partir desta avaliação constrói-se uma matriz de comparação A tendo em conta a reciprocidade $a_{ij} = 1/a_{ij}$ para qualquer par (i,j) e que $a_{ii} = 1$ o que leva a que sejam necessárias apenas n(n-1)/2 comparações.

Considerem-se λ_{max} o maior valor próprio de A, $w = (w_1,\ldots,w_n)$ o vector próprio correspondente e n o número de elementos em comparação. Se as avaliações feitas forem perfeitamente coerentes entre si, verifica-se que $\lambda_{max} = n$ e $a_{ij} = w_i/w_j$.

O Índice de Consistência (IC) é calculado a partir da expressão:

Equação 1 - Índice de Consistência

$$IC = \frac{|\lambda_{max} - n\ |}{n-1}, \text{com } \lambda_{max} = \frac{1}{n}\sum_{i=1}^{n}\frac{[Aw]_i}{w_i}$$

Depois de calculado este valor deve ser calculado o Rácio de Consistência (RC) que é obtido através da comparação do IC com uma tabela que contém IC obtidos através de uma amostra de matrizes recíprocas geradas aleatoriamente usando a escala 1/9, 1/8, …, 8,9.

Tabela 1 – Average Random Consistency Index (RI)

n	1	2	3	4	5	6	7	8	9	10
Random Consistency Index (RI)	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Para que as avaliações feitas sejam consideradas consistentes, Satty (Satty & Vargas, 2001) afirma que, o valor do RC não deverá ser maior que 0,1 uma vez que nesse caso se estaria demasiado próximo de ter atribuído avaliações aleatórias aos critérios.

Quando isso acontece o problema deve ser novamente analisado e as avaliações atribuídas devem ser revistas.

Uma vez que a determinação exacta do vector próprio w pode ser demorada, Saaty (Satty & Vargas, 2001) sugere alguns métodos de aproximação, dos quais se destacam os seguintes:

1º método – Divide-se cada elemento de A pela soma dos elementos da coluna em que se encontra e considera-se provisoriamente w_i igual à média aritmética da i-ésima linha da matriz obtida. Caso $\sum_{i=1}^{n} w_i = 1$ termina o processo, caso contrário divide-se cada elemento de w por $\sum_{i=1}^{n} w_i$.

2º método – Considera-se provisoriamente w_i igual à média geométrica dos elementos da i-ésima linha da matriz obtida. Caso $\sum_{i=1}^{n} w_i = 1$ termina o processo, caso contrário divide-se cada elemento de w por $\sum_{i=1}^{n} w_i$.

Após a determinação dos vectores próprios de todos os critérios e subcritérios, são obtidos, através da sua combinação, os coeficientes de ponderação. Para terminar constrói-se uma matriz por cada nível e multiplicam-se as matrizes resultantes do nível mais baixo para o topo de modo a obter a importância de cada alternativa em relação ao objectivo global.

Além do método AHP foram analisados os métodos ELECTRE (*ELimination Et Choix Traduisant la RÉalité*) (ver, por exemplo, Dias, 2002; Dias, Almeida, & Clímaco, 1997) dando especial atenção para a sua variante ELECTRE TRI, uma vez que seria o mais orientado ao tipo de problema em análise.

O método ELECTRE TRI afecta conjuntos de acções a categorias pré-definidas e ordenadas, com base em múltiplos critérios (Dias, 2002) . Para definir as categorias são limitadas inferiormente e superiormente por acções de referência. O objectivo deste método é avaliar cada acção, afectando-a a uma categoria.

No entanto, ao analisar este método chegou-se à conclusão que, embora pudesse ser útil no que diz respeito ao primeiro objectivo, não seria o mais adequado para atingir o objecto de quantificação, uma vez que o resultado não se traduz num número, mas sim num intervalo limitado pelas acções de referência.

Deste modo foi escolhido o AHP por se ter considerado ser o mais adequado e próximo de ambos os objectivos, permitindo tanto a criação do padrão referido como a quantificação do risco.

3. Trabalho Desenvolvido

3.1. Trabalho efectuado na empresa: objectivos, metodologia e práticas [3]

Como foi referido anteriormente, ao longo do período de estágio foi desenvolvido um projecto para um banco que por razões de confidencialidade passará a ser designado ao longo do texto como BGE (Banco Genérico de Estudo).

O objectivo dos trabalhos foi avaliar o risco associado aos Sistemas de Informação do BGE de modo a poder aferir se a equipa de auditoria pode confiar, ou não, na documentação aí existente, assim como fornecer ao banco aconselhamento no sentido de melhorar a protecção dos seus dados.

A metodologia utilizada pela Ernst & Young para levar a cabo as suas auditorias é a metodologia GAM (Global Audit Methodology) que se encontra dividida nas etapas Planeamento e Identificação de Riscos, Estratégia e Avaliação do Risco, Execução e, finalmente, Conclusão e Relatório.

O processo de avaliação dos *"Information Technology General Controls"* (ITGC's) encontra-se inserido, sobretudo, na segunda etapa da metodologia (Estratégia e Avaliação do Risco)

Este processo encontra-se dividido em três passos:

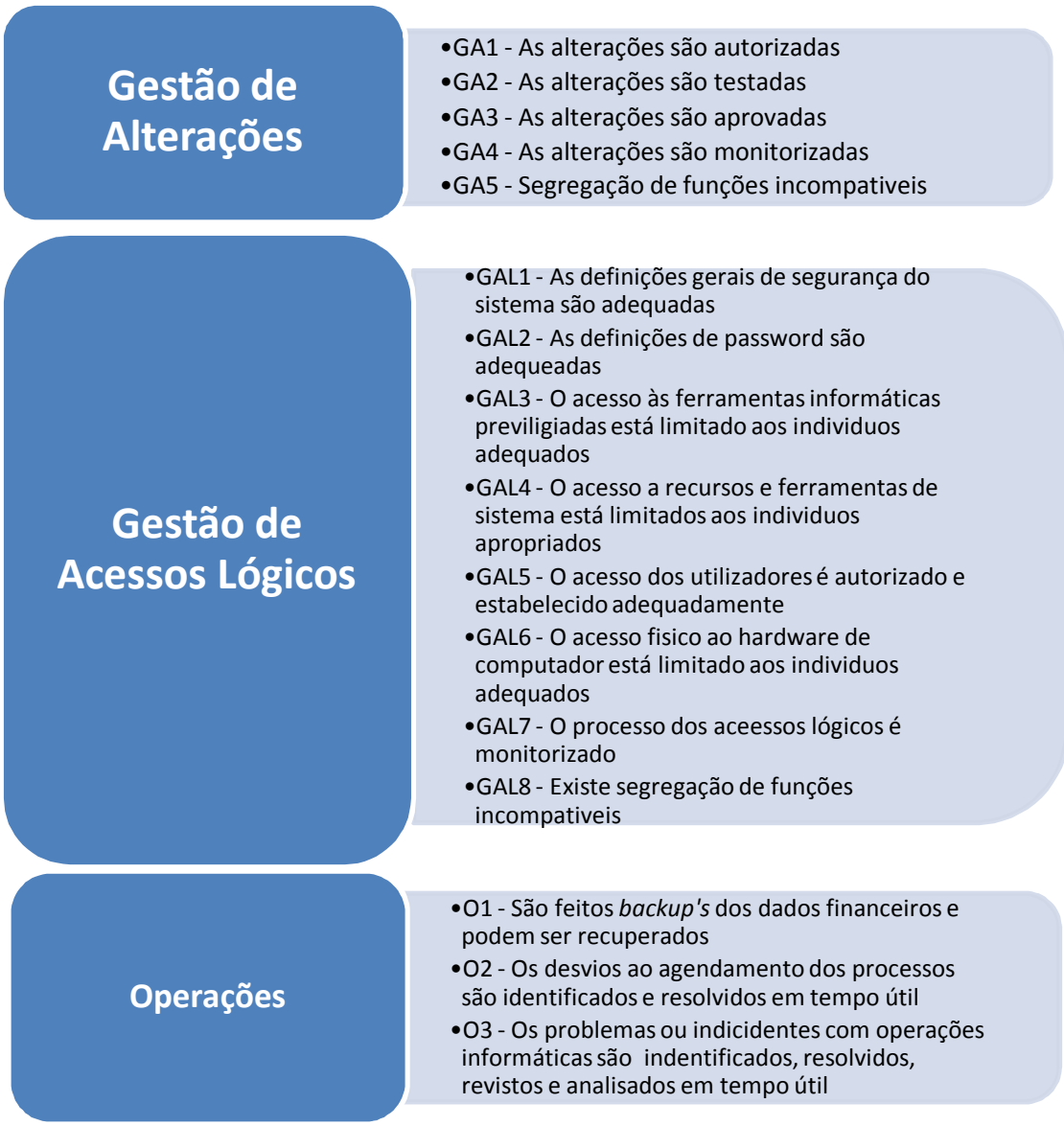
- Compreender os ITGC's da empresa
- Desenvolver e executar testes aos ITGC's da empresa
- Avaliar os ITCG's da empresa

Para sistematizar o processo destes três passos existe uma categorização que será aprofundada ao longo do texto.

De modo a facilitar a sua compreensão é apresentado o seguinte esquema:

[3] Para este ponto o estagiário apoiou-se num documento das Ernst & Young que descreve a metodologia utilizar. (Ernst & Young Global Audit Methodology and Suplemental Audit Guidance, 2010)

Quadro 1



A categoria Gestão de Alterações tem o objectivo de certificar que só alterações autorizadas, testadas e aprovadas são feitas às aplicações, interfaces, bases de dados e sistemas operativos.

A Gestão de Acessos Lógicos pretende verificar se apenas pessoas autorizadas têm acesso aos dados e aplicações e se as funções a que têm acesso estão limitadas às suas necessidades (executar, actualizar, alterar, etc.)

Os objectivos da categoria Operações prendem-se com a realização de backup's aos dados que contêm informação financeira de modo a que possam ser recuperados correctamente na sua totalidade no caso de se verificarem problemas com o sistema. Além disso também têm o objectivo de assegurar que problemas e incidentes que tenham ocorrido nos sistemas informáticos foram identificados, resolvidos, revistos e analisados em tempo útil.

Ao longo do processo vai sendo elaborado um documento (*walkthrough)* que contém o entendimento sobre os controlos das aplicações retirado das reuniões e políticas, normas, manuais ou outra documentação da empresa, assim como o registo e resultado dos testes efectuados.

Este documento encontra-se estruturado da seguinte forma:

1. Gestão de Alterações
    a. Aplicação 1
    b. Aplicação2
    c. Aplicação 3
    d. Etc…
2. Gestão de Acessos Lógicos
    a. Aplicação 1
    b. Aplicação 2
    c. Aplicação 3
    d. Etc…
3. Operações
    a. Aplicação 1
    b. Aplicação 2
    c. Aplicação3
    d. Etc…

O primeiro passo deste processo será compreender os ITGC's. Com este fim são realizadas reuniões com os administradores e responsáveis das aplicações e áreas relevantes. Nestas reuniões são pedidas informações com base na categorização indicada no Quadro 1.

Além das reuniões é analisada a documentação referida anteriormente de modo a perceber que controlos existem e o modo como devem ser aplicados.

Depois de feitas as reuniões e de compreendidos os ITGC's são elaborados e executados testes com base na documentação obtida de forma a perceber se o entendimento retirado das reuniões é seguido de forma adequada.

Esta documentação é normalmente obtida através de *scripts* (programas que são enviados ao cliente para os correr no sistema a ser analisado e que devolvem um ficheiros com os resultados), *screen shots* de configurações do sistema e documentação comprovativa de que as acções tomadas seguiram o procedimento adequado.

Para alguns testes, como os da categoria Gestão de Alterações e o da categoria Gestão de Acessos Lógicos GAL5 (O acesso dos utilizadores é autorizado e estabelecido adequadamen-

te), pode ser necessário realizar testes mais aprofundados como será descrito nos pontos seguintes.

Para os testes de Gestão de Alterações é obtida uma lista das alterações feitas às componentes relevantes das várias aplicações desde o início do período de auditoria até à data do teste.

A partir desta lista é seleccionada aleatoriamente uma ocorrência para a qual é pedida a documentação que comprova que as alterações seguiram o procedimento adequado, ou seja, que permita verificar que as alterações foram autorizadas (GA1), testadas (GA2) e aprovadas (GA3), que são monitorizadas (GA4) e que existiu segregação de funções (GA5).

A segregação de funções implica que, tanto organizacionalmente como logicamente, as seguintes tarefas sejam executadas por indivíduos diferentes:

- Pedido/aprovação de desenvolvimento ou alteração do programa
- Desenvolvimento do programa
- Pôr ou tirar o programa do ambiente de produção (por ambiente de produção entende-se o uso efectivo do programa pelos utilizadores)
- Monitorização do desenvolvimento e alterações do programa

Para cada um dos GA é atribuída a classificação *effective* ou *ineffective* consoante sejam, ou não, eficazes e é documentado no *walkthrough*.

No caso destes testes serem *effective*, é necessário efectuar testes mais aprofundados fazendo o processo descrito acima para uma amostra de ocorrências que é feita com base no número de alteração efectuadas aos sistemas no período de auditoria em análise.

Para verificar a Gestão dos Acessos Lógicos são analisados os resultados dos *scripts, screen shots* e outra documentação fornecida pelos responsáveis pela aplicação em análise.

Esta informação contém dados como os utilizadores do sistema, os perfis de utilizador existentes, as configurações de *passwords*, etc., tanto para o sistema operativo como para a base de dados de suporte à aplicação.

Cada uma das características (GAL) dos Gestão de Acessos Lógicos pode ter vários pontos que devem ser, ou analisados individualmente, ou tendo em conta resultados de outros pontos.

Estes pontos variam consoante se está a analisar a base de dados ou o sistema operativo, assim como para sistemas operativos (Linux, Windows, AS/400,etc.) e bases de dados diferentes (DB2, SQL Server, etc.).

O procedimento dos testes é o seguinte:

GAL1 – Determinar que as configurações genéricas de segurança do sistema são apropriadas tendo por base as linhas orientadoras mínimas.

GAL2 – Verificar que estão definidos apropriadamente os seguintes pontos: tamanho mínimo da *password*, a password tem de ser alterada após o primeiro log-on, a composição da password obedece a regras pré-definidas, frequência de alteração de password obrigatória, número de tentativas de log-on antes do acesso ser bloqueado, número de passwords que têm de ser usado antes de se poder voltar a usar a mesma, tempo de inactividade até ser necessário fazer login de novo e registo tentativa de login mal sucedidas.

GAL3 – Certificar que a lista de utilizadores com direitos privilegiados está completa, se o número é adequado e se o acesso privilegiado de cada utilizador é apropriado tendo em conta a função que desempenha.

GAL4 – Analisar o acesso aos recursos do sistemas associados a aplicações que podem afectar a exactidão dos dados financeiros e verificar que este é apropriado.

GAL5 – A partir da lista de utilizadores criados/alterados escolher um para a qual será pedida a documentação que permita certificar que foi feito o pedido de criação/alteração, que foi indicada a função e que foi dada uma autorização pelo chefe de área.

GAL6 – Determinar se a lista de empregados com a acesso ao *data center* está completa e rever se estes acessos são adequados. Confirmar que existem controlos para restringir o acesso apenas aqueles indivíduos.

GAL7 – Verificar se existe um processo de monitorização regular dos acessos lógicos.

GAL8 – Verificar que existe segregação de funções

Para cada ponto é decidido se o controlo é, ou não, eficaz sendo depois feita uma agregação ao nível de cada caracteristica GAL. A análise efectuada e o seu resultado são registados no *walkthrough*.

Em alguns casos, como o do GAL5, quando o teste descrito é considerado *effective* procede-se à realização de testes mais aprofundados fazendo a análise descrita para uma amostra de utilizadores, de modo semelhante ao indicado para a categoria Gestão de Alterações.

Com o fim de testar os Operações são verificados três controlos:

O1 – Com base nos *logs* fornecidos pelo cliente determinar, através de uma amostra, que os *backups* estão a funcionar correctamente e que qualquer falha é resolvida em tempo útil. Rever os procedimentos que garantem que periodicamente é testada a recuperação dos *backups*.

O2 – Certificar que apenas pessoal autorizado pode fazer alterações ao agendamento de trabalhos e verificar, através de uma amostra de erros no processo de produção, que houve um acompanhamento e resolução apropriados.

O3 – Através de documentação recolhida junto do cliente, verificar que problemas ou incidentes relacionados com operações informáticas foram identificados, resolvidos, revisto e analisados em tempo útil.

Após feitos os testes, é atribuído um resultado a cada uma das categorias, agregando os resultados das características tendo em conta a importância de cada uma.

Por último, é feita a avaliação agregada dos ITGC's. Esta avaliação é feita para cada aplicação a partir da agregação da avaliação das categorias.

Relatório

Para finalizar o trabalho é efectuado o Relatório onde se regista a maturidade dos controlos aos sistemas de informação tal como sugerido pelo (IT Governance Institute, 2008) (guia de boas práticas de gestão das tecnologias de informação) e se elaboram recomendações de melhoria.

Este Relatório é posteriormente entregue à equipa de Auditoria Financeira que o entregará ao cliente.

O estagiário participou em todas as fases do processo aqui descrito, tendo estado presente nas reuniões com os clientes, contribuído na elaboração do *walktrough*, feito e documentado os testes aos sistemas (exceptuando o O1 e O2) e participado na avaliação final.

Esta participação permitiu perceber a importância da segurança dos sistemas de informação para as empresas, sobretudo para os bancos (por serem instituições financeiras), no que se refere a proteger os seus dados financeiros.

E relação especificamente ao projecto do BGE o estagiário não participou na criação do Relatório. No entanto, teve essa oportunidade em projectos que se seguiram com o mesmo âmbito.

O desenvolvimento do Relatório foi, no entanto, muito importante, uma vez que é este o relatório onde poderá ser integrada a proposta feita neste relatório de estágio.

O estágio permitiu também adquirir conhecimento da estrutura e desenvolvimento do negócio de empresas de várias indústrias, tais como bancos, farmacêuticas, retalho e energéticas.

Ao longo do estágio foi ainda possível desenvolver a sua capacidade de relacionamento com o cliente, tornando-se cada vez mais natural a proximidade com este de modo a esclarecer pontos que não tenham ficado claros nas reuniões iniciais.

Este estágio teve um papel fundamental no crescimento pessoal do estagiário e na sua proximidade ao mundo do trabalho tendo levado ao desenvolvimento do aspecto crítico em relação ao trabalho efectuado e a uma maior facilidade de questionar os colegas de forma proactiva, fornecendo sempre uma proposta de resolução para o problema em causa.

3.2 Hipóteses de inovação

3.2.1- Aplicação da Metodologia

De modo a aplicar a metodologia ao caso de estudo foi necessário fazer algumas adaptações ao método AHP original de Satty (Satty & Vargas, 2001).

Do método AHP original manteve-se o modo como são calculados os ponderadores e o Rácio de Consistência. No entanto, uma vez que este trabalho se destina, não a uma comparação de alternativas mas sim a determinar se os sistemas informáticos relevantes para a Auditoria Financeira são ou não suficientemente seguros foi necessário considerar categorias identificadoras dos riscos, cada uma com suas características, deixando assim de parte a noção de alternativas. Deste modo, a árvore que descreve o processo de decisão, não será a apresentada aquando da descrição do método, que considerava as alternativas e estabelecia o seu desempenho em relação a cada uma das características de modo a chegar à alternativa mais adequada, mas sim a que se encontra representada abaixo:

Ilustração 2 – Árvore do processo de decisão

É, no entanto, mantida a comparação de importância par-a-par entre as características de cada categoria, assim como a comparação de importância das mesmas.

Após efectuada a comparação referida[4], atribuindo valores conforme sugerido por Satty (Satty & Vargas, 2001), foram obtidas as seguintes matrizes, onde está estabelecida a importância das características ou categorias indicadas nas linhas sobre as indicadas nas colunas:

Tabela 2- Gestão de Alterações

	GA1-As alterações são autorizadas	GA2-As alterações são testadas	GA3-As alterações são aprovadas	GA4-As alterações são monitorizadas	GA5-Segregação de funções incompativeis
GA1-As alterações são autorizadas	1	1/3	1/3	5	1
GA2-As alterações são testadas	3	1	1/3	7	3
GA3-As alterações são aprovadas	3	3	1	9	5
GA4-As alterações são monitorizadas	1/5	1/7	1/9	1	1/5
GA5-Segregação de funções	1	1/3	1/5	5	1

[4] A comparação referida e os respectivo cálculos foram elaborados pela autor numa aplicação de folhas de cálculo seguindo de perto os exemplos dados em (Kunz, 2010).

Tabela 3 - Gestão de Acessos Lógicos

	GAL1-As definições gerais de segurança do sistema são adequadas	GAL2-As definições de password são adequeadas	GAL3-O acesso às ferramentas informáticas previligiadas está limitado aos individuos adequados	GAL4-O acesso a recursos e ferramentas de sistema está limitados aos individuos apropriados	GAL5-O acesso dos utilizadores é autorizado e estabelecido adequadamente	GAL6-O acesso fisico ao hardware de computador está limitado aos individuos adequados	GAL7-- O processo dos acessos lógicos é monitorizado	GAL8-Existe segregação de funções incompativeis
GAL1-As definições gerais de segurança do sistema são adequadas	1	1/3	1/7	1/7	1/7	1/3	1	1/5
GAL2-As definições de password são adequeadas	3	1	1/5	1/5	1/5	1	3	1/5
GAL3-O acesso às ferramentas informáticas previligiadas está limitado aos individuos adequados	7	5	1	1	1/3	5	7	5
GAL4-O acesso a recursos e ferramentas de sistema está limitados aos individuos apropriados	7	5	1	1	1/3	5	7	5
GAL5-O acesso dos utilizadores é autorizado e estabelecido adequadamente	7	5	3	3	1	7	9	5
GAL6-O acesso fisico ao hardware de computador está limitado aos individuos adequados	3	1	1/5	1/5	1/7	1	3	1
GAL7-- O processo dos acessos lógicos é monitorizado	1	1/3	1/7	1/7	1/9	1/3	1	1/3
GAL8-Existe segregação de funções incompativeis	5	5	1/5	1/5	1/5	1	3	1

Tabela 4 - Operações

	O1-São feitos backup's dos dados financeiros e podem ser recuperados	O2-Os desvios ao agendamento dos processos são identificados e resolvidos em tempo útil	O3-Os problemas ou indicidentes com operações informáticas são indentificados, resolvidos, revistos e analisados em tempo útil
O1-São feitos backup's dos dados financeiros e podem ser recuperados	1	3	1/3
O2-Os desvios ao agendamento dos processos são identificados e resolvidos em tempo útil	1/3	1	1/7
O3-Os problemas ou indicidentes com operações informáticas são indentificados, resolvidos, revistos e analisados em tempo útil	3	7	1

Tabela 5 - Categorias

	Gestão de Acessos (GA)	Gestão de Acessos Lógicos (GAL)	Operações (O)
Gestão de Acessos (GA)	1	1/3	5
Gestão de Acessos Lógicos (GAL)	3	1	7
Operações (O)	1/5	1/7	1

Tomado como exemplo o último quadro apresentado (Tabela 5 - Categorias), a categoria Gestão de Alterações foi considerada fracamente menos prioritária que a categoria Gestão de Acessos Lógicos (1/3) e fortemente mais prioritária que a categoria Operações (5). Por sua vez a categoria Gestão de Acessos Lógicos foi considerada fracamente mais prioritária que a categoria Gestão de Alterações (3) e demonstravelmente mais prioritária que a categoria Operações (7). Finalmente a categoria Operações foi considerada fortemente menos prioritária que a categoria Gestão de Alterações (1/5) e demosntravelmente menos prioritária que a categoria Gestão de Acessos Lógicos (1/7). Tal como referido na secção 2, as avaliações são recíprocas, ou seja, se a categoria Gestão de Alterações é fracamente menos prioritária que a categoria Gestão de Acessos Lógicos, sendo atribuído ao valor 1/3 a esta comparação, então a categoria Gestão de Acessos Lógicos será fracamente mais prioritária que a categoria Gestão de Alterações, comparação à qual foi atribuído o valor 3 inverso ao anterior.

Neste caso foi atribuída uma prioridade maior à categoria Gestão de Acessos Lógicos por se tratar do ponto mais sensível, uma vez que caso existam acessos indevidos existe um risco muito elevado de segurança para os dados financeiro. A categoria Gestão de Alterações tem uma prioridade um pouco abaixo da Gestão de Acessos Lógicos por ser ainda muito importante na segurança mas onde existe menos ocorrências uma vez que as alterações aos sistemas ocorrem com muito menos frequência que a atribuição de acessos. Por fim a categoria Operações é a menos importante desde grupo por se tratar da categoria que gere os *backups* e a resposta a incidentes com os sistemas informáticos, não deixando, no entanto, de ter um papel forte na segurança dos sistemas, pois é esta categoria que permite salvaguardar que a infor-

mação não é perdida em caso de falha dos sistemas e que todos os incidentes que ocorram são resolvidos em tempo útil.

De modo a obter os ponderadores para cada característica e categoria foram efectuados os cálculos de aproximação dos vectores próprios das matrizes através do 2º método indicado no capítulo 3.2.1. Estes cálculos, assim como todos os que se apresentem daqui em diante no trabalho, foram efectuados com recurso a uma aplicação de folhas de cálculo como demonstrado em (Kunz, 2010).

Na referida aplicação procedeu-se ao cálculo da média geométrica das linhas das matrizes que posteriormente se dividiu pela sua soma obtendo, assim, os seguintes ponderadores:

Tabela 6 – Ponderadores Gestão de Alterações

GA1-As alterações são autorizadas	GA2-As alterações são testadas	GA3-As alterações são aprovadas	GA4-As alterações são monitorizadas	GA5-Segregação de funções incompativeis
0,126	0,260	0,469	0,032	0,113

Tabela 7 – Ponderadores Gestão de Acessos Lógicos

GAL1-As definições gerais de segurança do sistema são adequadas	GAL2-As definições de password são adequeadas	GAL3-O acesso às ferramentas informáticas previligiadas está limitado aos individuos adequados	GAL4-O acesso a recursos e ferramentas de sistema está limitados aos individuos apropriados	GAL5-O acesso dos utilizadores é autorizado e estabelecido adequadamente	GAL6-O acesso fisico ao hardware de computador está limitado aos individuos adequados	GAL7-- O processo dos acessos lógicos é monitorizado	GAL8-Existe segregação de funções incompativeis
0,025	0,048	0,212	0,212	0,345	0,056	0,025	0,077

Tabela 8 – Ponderadores Operações

O1-São feitos backup's dos dados financeiros e podem ser recuperados	O2-Os desvios ao agendamento dos processos são identificados e resolvidos em tempo útil	O3-Os problemas ou indicidentes com operações informáticas são indentificados, resolvidos, revistos e analisados em tempo útil
0,243	0,088	0,669

Tabela 9 – Ponderadores das Categorias

Gestão de Acessos (GA)	Gestão de Acessos Lógicos (GAL)	Operações (O)
0,279	0,649	0,072

Com o objectivo de conferir a consistência das avaliações de importância atribuídas aos parâmetros de cada matriz foi calculado o Rácio de Consistência segundo indicado no método AHP original de Satty (Satty & Vargas, 2001).

Para a obtenção deste rácio foi necessário calcular o Índice de Consistência de acordo com a Equação 1 e dividi-lo pelo valor correspondente ao número de colunas da matriz na Tabela 1.

Os valores de Rácio de Consistência obtidos para as matrizes indicadas foram os seguintes:

Tabela 10 – Rácios de Consistência

GAs	GALs	Os	Categorias
0,053	0,067	0,006	0,056

Qualquer destes valores se encontra bastante abaixo do limite de 0,1 indicado por Satty, permitindo, assim, concluir que as comparações par-a-par efectuadas apresentam consistência aceitável.

Neste momento, está-se em condições de efectuar a avaliação do sistema.

Para isso é atribuído o valor 0 se a analise revelar que a característica é *ineffective* e 1 se esta for *effective*. Estes valores devem ser multiplicados pelos valores das respectivas características e posteriormente somados categoria a categoria obtendo um resultado para cada uma destas. Finalmente, estes resultados obtidos para as categorias devem ser multiplicados pelos respectivos ponderadores e somados de modo a obter o resultado final do sistema. Este resultado representa uma quantificação da eficácia do sistema.

A ilustração abaixo demonstra de forma sucinta um exemplo de todo o processo.

Ilustração 3 - Exemplo de cálculo do resultado de um sistema

Resultado																
Valor de entrada x Ponderador																
Titulo das Categorias																
Ponderador (Valor Próprio)																
Resultado	0,405					0,769								0,757		
Valor de entrada x Ponderador	0,000	0,260	0,000	0,032	0,113	0,000	0,000	0,212	0,212	0,345	0,000	0,000	0,000	0,000	0,088	0,669
Titulo das Características	GA1	GA2	GA3	GA4	GA5	GAL1	GAL2	GAL3	GAL4	GAL5	GAL6	GAL7	GAL8	O1	O2	O3
Ponderador (Valor Próprio)	0,126	0,260	0,469	0,032	0,113	0,025	0,048	0,212	0,212	0,345	0,056	0,025	0,077	0,243	0,088	0,669
Valor de Entrada 1 (*Effective*) ou 0 (*Ineffective*)	0	1	0	1	1	0	0	1	1	1	0	0	0	0	1	1

0,667			
0,113	0,499	0,054	
GA	GAL	O	
0,279	0,649	0,072	

3.2.2- Definição de limiares de eficácia

O resultado obtido no exemplo do ponto anterior quantifica a eficácia do sistema. Este resultado pode ser útil para se perceber de um modo geral a qualidade e eficácia dos controlos implementados para mitigar o risco, dando ao cliente uma ideia da necessidade de efectuar melhorias.

No entanto no que concerne ao objectivo de fornecer apoio à auditoria financeira esta análise demonstra-se insuficiente. Para este objectivo é necessário estabelecer a partir de que nível de eficácia encontrado se pode considerar que os controlos são eficazes.

Este ponto é importante, pois o estabelecimento dos níveis de eficácia poderá permitir uma mais fácil atribuição dos resultados para os caso em que seja claro, além de fornecer uma base que permite eliminar alguma subjectividade existente no processo.

Com este objectivo foram construídos cenários exemplificativos de diversas categorias e sistemas. Alguns destes cenários foram definidos por construção do autor, e outros foram gerados aleatoriamente. Para todos estes cenários foi feita uma análise no sentido de perceber se um analista os qualificaria como *effective* ou *ineffective*. Foi depois aplicado o método descrito no ponto anterior, por forma a verificar quais as pontuações obtidas por cada um. Os cenários definidos para a categoria Gestão de Acessos Lógicos, as pontuações calculadas e a qualificação *effective/ineffective* que se assume que um analista lhes atribuiria são apresentados nos quadros seguintes. Os cenários, valores e resultados relativos às restantes categorias e ao sistema como um todo encontram-se nos Anexos 2 a 6.

Tabela 11 - Exemplo de Cenários

Cenários Construídos										
	Logical Access								Resultado	*Effective/Ineffective*
	GAL1	GAL2	GAL3	GAL4	GAL5	GAL6	GAL7	GAL8		
Cenário 1	1	1	1	1	1	0	0	1	0,918	Effective
Cenário 2	1	0	0	0	0	1	1	1	0,183	Ineffective
Cenário 3	0	1	1	1	1	0	0	0	0,817	Effective
Cenário 4	1	1	0	0	0	1	1	1	0,231	Ineffective
Cenário 5	0	0	0	0	1	1	1	1	0,503	Ineffective
Cenário 6	1	0	1	0	1	0	1	0	0,607	Effective
Cenário 7	1	1	1	1	1	0	0	0	0,841	Effective
Cenário 8	0	1	1	0	0	1	1	0	0,342	Ineffective
Cenário 9	1	1	0	0	0	1	1	0	0,154	Ineffective
Cenário 10	1	1	1	1	0	0	0	0	0,497	Ineffective
Cenário 11	1	1	1	1	0	1	1	1	0,655	Effective

Cenários Aleatórios										
	Logical Access								Resultado	*Effective/Ineffective*
	GAL1	GAL2	GAL3	GAL4	GAL5	GAL6	GAL7	GAL8		
Cenário 1	0	0	0	0	1	1	1	0	0,426	Ineffective
Cenário 2	0	1	1	1	1	0	1	1	0,919	Effective
Cenário 3	1	0	1	1	0	0	1	0	0,474	Ineffective
Cenário 4	1	1	0	0	0	1	0	0	0,129	Ineffective
Cenário 5	0	0	1	0	1	0	1	0	0,582	Ineffective
Cenário 6	1	1	1	0	0	1	1	1	0,443	Ineffective
Cenário 7	0	1	1	0	0	0	1	1	0,362	Ineffective
Cenário 8	1	1	1	1	1	0	0	0	0,841	Effective
Cenário 9	1	1	0	1	1	0	1	0	0,655	Effective
Cenário 10	1	0	0	1	0	0	0	1	0,313	Ineffective
Cenário 11	0	1	1	1	1	0	1	0	0,842	Effective
Cenário 12	1	1	1	0	1	1	0	1	0,763	Effective
Cenário 13	0	1	0	1	1	1	1	1	0,763	Effective
Cenário 14	1	1	1	1	1	0	1	1	0,944	Effective
Cenário 15	1	0	0	1	0	0	1	0	0,262	Ineffective
Cenário 16	0	0	1	0	0	1	0	0	0,269	Ineffective
Cenário 17	1	1	1	0	0	1	1	1	0,443	Ineffective
Cenário 18	1	0	1	1	0	1	0	1	0,582	Ineffective
Cenário 19	1	0	1	0	0	1	1	0	0,318	Ineffective
Cenário 20	0	0	0	0	1	1	1	0	0,426	Ineffective
Cenário 21	0	0	1	1	1	0	0	0	0,769	Effective

Esta análise permitiu aferir de algum modo a consistência do modelo aqui apresentado ao confirmar a adequação das pontuações existentes à avaliação pré-estabelecida para os cenários, demonstrando que não existe nenhum que seja *ineffective* e tenha uma pontuação demasiado elevada e vice-versa.

Após a análise destas tabelas chegou-se à conclusão que os seguintes valores constituiriam limiares de eficácia (LE) adequados:

Tabela 12 - Limiar de Eficácia das Categorias

	GA	GAL	O
Limiar de Eficácia	Inef. < 0,7 < Ind.< 0,8 < Ef.	Inef. < 0,6 < Ind. < 0,65 < Ef.	Inef. < 0,7 < Ind. < 0,75 < Ef.

A partir da tabela anterior é possível verificar que, por exemplo, para a categoria GA um resultado abaixo de 0,7 seria considerado *ineffective*, acima de 0,8 seria *effective* e entre estes

dois valores suscitaria algumas dúvidas, sendo necessária uma melhor ponderação com base no caso em análise.

Além dos Limiares de Eficácia para as categorias foram estabelecidos dois LEs para os sistemas.

A razão para terem sido calculados os LE dos sistemas de duas formas distintas tem a ver com o duplo objectivo deste trabalho: por um lado o objectivo de apoio à auditoria financeira (objectivo 1) para o qual a cada patamar da árvore hierárquica se um ponto é considerado *ineffective* deve ser atribuído o valor "0" e se é considerado *effective* deve ser atribuído o valor "1", uma vez que neste caso apenas importa se é ou não eficaz e não se é mais ou menos eficaz, por outro lado o objectivo de consultoria de fornecer ao cliente uma visão global da segurança dos seus sistemas (objectivo 2) para o qual é usado o valor a que se chegou no patamar anterior da árvore hierárquica, pois neste caso poderá ser útil ao cliente saber qual o grau ineficácia de modo a perceber o esforço que teria de realizar para o tornar eficaz.

Assim para o primeiro objectivo usaremos como cenários para calcular o LE a tabela seguinte:

Tabela 13 - Cenários Sistemas (Objectivo 1)

Cenários Construídos					
	Categorias			Resultado	*Effective/Ineffective*
	GA	GAL	O		
Cenário 1	1	1	0	0,928	Effective
Cenário 2	1	0	0	0,279	Ineffective
Cenário 3	1	0	1	0,351	Ineffective
Cenário 4	0	0	1	0,072	Ineffective
Cenário 5	0	1	0	0,649	Ineffective
Cenário 6	0	1	1	0,721	Effective

Obtendo o seguinte Limiares de Eficácia:

Tabela 14 - Limiares de Eficácia para os Sistemas (Objectivo 1)

Limiar de Eficácia	Inef. < 0,65 < Ind. < 0,7 < Ef.

Enquanto para calcular o LE para o objectivo 2 consideraremos como cenário os valores mínimos e máximos dos LEs das categorias como se pode ver na tabela seguinte:

Tabela 15 - Cenário Sistemas (Objectivo 2)

	Valores de Entrada			Resultado
	GA	GAL	O	
Valor mínimo dos Limiares de Indecisão	0,7	0,6	0,7	0,635
Valor máximo dos Limiares de Indecisão	0,8	0,65	0,75	0,699

Resultando o seguinte Limiares de Eficácia:

Tabela 16 - Limiares de Eficácia para os Sistemas (Objectivo 2)

Limiar de Eficácia	Inef. < 0,63 < Ind. <0,7 < Ef.

Objectivo 1

De modo a fornecer apoio à auditoria foi calculado o Limiares de Eficácia substituindo o valor de cada categoria por 0 se *ineffective* (caso em que a pontuação obtida se situa abaixo do LE) e por 1 se *effective* (caso em que a pontuação obtida se situa acima do LE) como exemplificado na tabela 13, uma vez que será este o método a utilizar para avaliar os sistemas visto que neste caso nos interessa apenas decidir se podemos confiar no sistema ou não, e não tanto o grau de qualidade da sua segurança ou perceber pontos a melhorar.

Posteriormente estes valores são multiplicados pelos ponderadores de cada categoria de modo a obter o resultado do sistema. Neste ponto se o resultado se situar acima do LE indicado na tabela 14 o sistema deverá ser considerado *effective* e a auditoria poderá confiar nos sistemas, caso se situe abaixo do LE deverá ser considerado *ineffective* e a auditoria não deverá confiar nos sistemas, caso se situe dentro do LE a atribuição do resultado deverá ser ponderada com mais cuidado.

Objectivo 2

Para o objectivo de fornecer uma visão geral do estado de segurança dos sistemas ao cliente deve ser usado o LE da tabela 16 uma vez que o modo de obtenção do resultado do sistema é calculado através da multiplicação directa do resultado obtido para o patamar anterior da árvore hierárquica pelos respectivos ponderadores.

Neste caso o LE serve apenas indicador que fornecer ao cliente uma noção da importância de fazer melhorias aos controlos dos sistemas, ou seja, serve para dar uma noção da pontuação que o sistema deveria ter atingido para ser considerado seguro.

3.2.3- Resultado da Aplicação do método ao caso do BGE

Com o fim de perceber a utilidade prática da utilização deste método de quantificação foi feita a sua aplicação ao caso do BGE referido no ponto 3.1.

Assim, os valores de entrada da análise serão os observados para as diversas características das categorias aquando da análise dos sistemas.

Estes valores de entrada foram introduzidos numa árvore como a da Ilustração 2 para cada um dos sistemas.

Os Resultados obtidos para o BGE foram os seguintes:

Tabela 17 - Resultados do BGE

Sistemas	Categoria	Resultado da Categoria (Objectivo 2)	Resultado da Categoria (Objectivo 1)	Resultado da Aplicação (Objectivo 2)	Resultado da Aplicação (Objectivo 1)
Sistemas Centrais	GA	0,968	1	0,975	1,000
	GAL	0,975	1		
	O	1,000	1		
A1	GA	0,968	1	0,943	1,000
	GAL	0,927	1		
	O	1,000	1		
A2	GA	0,968	1	0,975	1,000
	GAL	0,975	1		
	O	1,000	1		
A3	GA	0,968	1	0,943	1,000
	GAL	0,927	1		
	O	1,000	1		
A4	GA	0,968	1	0,943	1,000
	GAL	0,927	1		
	O	1,000	1		
A5	GA	0,968	1	0,532	0,351
	GAL	0,293	0		
	O	1,000	1		
A6	GA	0,968	1	0,975	1,000
	GAL	0,975	1		
	O	1,000	1		
A7	GA	1,000	1	0,984	1,000
	GAL	0,975	1		
	O	1,000	1		
A8	GA	1,000	1	0,984	1,000
	GAL	0,975	1		
	O	1,000	1		
A9	GA	0,968	1	0,943	1,000
	GAL	0,927	1		
	O	1,000	1		
A10	GA	0,968	1	0,943	1,000
	GAL	0,927	1		
	O	1,000	1		

Através destes resultados conclui-se que a equipa de auditoria poderá confiar em todos os sistemas menos no "A5" que obteve um resultado de 0,35 claramente abaixo do LE 0,65

estabelecido através dos cenários. É também possível perceber que a categoria GAL foi a responsável pelo fraco resultado.

Por seu lado, o cliente poderia concluir que os seus sistemas se encontram seguros tirando o "A5". Ser-lhe-ia fácil perceber que deve efectuar melhorias para esse sistema ao nível dos acessos lógicos. No entanto, a análise feita especificamente para o cliente permite-lhe perceber que os seus controlos para GAL já são cerca de trinta por cento eficazes dando-lhe assim uma ideia do esforço necessário para os melhorar, o que não aconteceria se olhasse para os resultados que serviram de apoio à auditoria.

4- Conclusões

Após a realização do estágio, concluiu-se que existe na Ernst & Young um método bem definido que permite avaliar de forma adequada a segurança dos sistemas de informação que suportam os dados financeiros relevantes à Auditoria.

Foram, no entanto, detectados pontos onde pode ser melhorada a base científica dessa avaliação, assim como explorar melhor o uso dos resultados obtidos no que se refere a fornecer aconselhamento sobre o modo como as empresas podem gerir a segurança dos seus sistemas de informação.

Estes pontos foram abordados ao longo do trabalho sendo possível concluir que tanto o objectivo de criação de um modelo padrão que permita simplificar as decisões no apoio à auditoria como o objectivo de fornecer uma visão mais simplificada do estado da segurança dos sistemas ao cliente são exequíveis, podendo trazer ganhos tanto na justificação das avaliações atribuídas aos sistemas como na forma como o cliente olha para a informação que lhe é apresentada

Assim sendo, foi possível, com base numa adaptação do método AHP de Satty (Satty & Vargas, 2001), estabelecer um novo método, que faz uso da consideração de cenários de sistemas eficazes e não eficazes, para a criação de um modelo que permita apoiar as decisões tomadas aquando da avaliação da segurança dos sistemas informáticos das empresas auditadas.

No que se refere a fornecer uma visão global do estado da segurança dos sistemas ao cliente, foi criada, também com base no método AHP, uma forma de quantificar a segurança de cada sistema, fornecendo ao cliente uma primeira noção simplificada do estado dos seus sistemas, permitindo, assim, que este se aperceba mais facilmente da necessidade de intervir para a sua melhoria.

Para ambos os objectivos poder-se-ia ir mais ao pormenor, estendendo a análise a uma hierarquia abaixo, considerando os parâmetros de cada uma das características.

De modo semelhante, seria também possível para o segundo objectivo (para o primeiro não seria relevante) efectuar uma agregação do conjunto dos sistemas. Para isso bastaria considerar um nível superior na hierarquia para o qual se obteria, com base em ponderadores para os sistemas de modo semelhante ao feito para as categorias e critérios, a avaliação da segurança dos sistemas informáticos da empresa no geral.

De modo a pôr em prática a utilização destes modelos de apoio à avaliação e de quantificação, seria necessária a discussão por profissionais mais experientes sobre a importância dos parâmetros usados para atribuir os ponderadores, assim como a reflexão sobre os cenários usados.

Espera-se que o trabalho aqui apresentado possa revestir-se de utilidade quer para a Ernst & Young, quer para outras Auditoras ou Consultoras.

Bibliography

Coyle, G. (2004). *The Analytic Hierarchy Process.* Pearson Education Limited.

Dias, L. M. (2002). *Apontamentos de Análise de Decisão: Como Considerar Múltiplos Critérios.* Coimbra: Faculdade de Economia da Universidade de Coimbra.

Dias, L. M., Almeida, L. M., & Clímaco, J. C. (1997). *Apoio Multicritério à Decisão: Métodos e software dedicádos à avaliação de um conjunto discreto de alternativas.* Coimbra: Faculdade de Economia da Universidade de Coimbra.

Ernst & Young Global Audit Methodology and Suplemental Audit Guidance. (2010, 10 25). E&Y.

IT Governance Institute. (2008). Cobit 4.1. *Cobit 4.1* . Rolling Meadows, IL, USA: ISACA & ITGI,Val IT,CGEIT Exam Resources.

Kunz, J. (2010, February/March). The Analytic Hierarchy Process (AHP). Eagle City Hall Location Options Task Force.

Satty, T. L., & Vargas, L. G. (2001). *Models, Methods Aplications of the Analytic Hierarchy Process.* Massachusetts: Kluwer's International Series.

Anexos

Anexo 1 – Exemplo de cálculo do Rácio de Consistência

	GA1-As alterações são autorizadas	GA2-As alterações são testadas	GA3-As alterações são aprovadas	GA4-As alterações são monitorizadas	GA5-Segregação de funções incompatíveis
GA1-As alterações são autorizadas	1	1/3	1/3	5	1
GA2-As alterações são testadas	3	1	1/3	7	3
GA3-As alterações são aprovadas	3	3	1	9	5
GA4-As alterações são monitorizadas	1/5	1/7	1/9	1	1/5
GA5-Segregação de funções	1	1/3	1/5	5	1

	Média Geométrica	Vector Próprio (Ponderador)	n= 5
GA1-As alterações são autorizadas	0,889	0,126	Soma Média Geométrica= 7,08
GA2-As alterações são testadas	1,838	0,260	
GA3-As alterações são aprovadas	3,323	0,469	
GA4-As alterações são monitorizadas	0,229	0,032	
GA5-Segregação de funções	0,803	0,113	

Soma	8,200	4,810	1,978	27,000	10,200
Vector Próprio	0,126	0,260	0,469	0,032	0,113
Soma*ponderador	1,029	1,248	0,928	0,874	1,156
Lambda max	5,236				
CI	0,059		RI		
CR	0,053		1,120		

Anexo 2 -Cenários Gestão de Alterações

Cenários Construídos							
	Gestão de Alterações					Resultado	*Effective/Ineffective*
	GA1	GA2	GA3	GA4	GA5		
Cenário 1	1	1	1	1	0	0,887	Effective
Cenário 2	0	1	1	1	1	0,874	Effective
Cenário 3	0	0	0	1	1	0,146	Ineffective
Cenário 4	1	1	1	0	0	0,854	Effective
Cenário 5	0	1	1	0	1	0,842	Effective
Cenário 6	0	1	1	1	0	0,761	Ineffective
Cenário 7	0	0	1	1	1	0,615	Ineffective
Cenário 8	0	1	1	0	0	0,729	Ineffective
Cenário 9	1	1	0	0	0	0,385	Ineffective
Cenário 10	1	0	1	1	0	0,627	Ineffective
Cenário 11	1	1	0	1	0	0,418	Ineffective

Cenários Aleatórios							
	Gestão de Alterações					Resultado	*Effective/Ineffective*
	GA1	GA2	GA3	GA4	GA5		
Cenário 1	0	0	0	1	0	0,032	Ineffective
Cenário 2	0	1	0	1	0	0,292	Ineffective
Cenário 3	0	0	0	1	1	0,146	Ineffective
Cenário 4	1	1	1	0	0	0,854	Effective
Cenário 5	1	0	1	0	0	0,595	Ineffective
Cenário 6	0	0	0	0	1	0,113	Ineffective
Cenário 7	0	1	1	1	1	0,874	Effective
Cenário 8	1	1	0	0	1	0,498	Ineffective
Cenário 9	0	1	1	1	1	0,874	Effective
Cenário 10	0	0	0	0	0	0,000	Ineffective
Cenário 11	1	0	0	1	1	0,271	Ineffective
Cenário 12	1	1	1	1	0	0,887	Effective
Cenário 13	0	1	1	1	1	0,874	Effective
Cenário 14	1	0	1	0	1	0,708	Effective
Cenário 15	1	1	1	0	0	0,854	Effective
Cenário 16	1	0	1	0	0	0,595	Ineffective
Cenário 17	1	0	0	1	0	0,158	Ineffective
Cenário 18	1	0	0	1	0	0,158	Ineffective
Cenário 19	0	0	1	1	0	0,502	Ineffective
Cenário 20	0	1	0	1	1	0,405	Ineffective
Cenário 21	1	0	0	0	1	0,239	Ineffective

Limiar de Eficácia	Inef. < 0,7 < Ind. < 0,8 < Ef.

Anexo 3 - Cenários Gestão de Acessos Lógicos

Cenários Construídos

	Gestão de Acessos Lógicos								Resultado	*Effective/Ineffective*
	GAL1	GAL2	GAL3	GAL4	GAL5	GAL6	GAL7	GAL8		
Cenário 1	1	1	1	1	1	0	0	1	0,918	Effective
Cenário 2	1	0	0	0	0	1	1	1	0,183	Ineffective
Cenário 3	0	1	1	1	1	0	0	0	0,817	Effective
Cenário 4	1	1	0	0	0	1	1	1	0,231	Ineffective
Cenário 5	0	0	0	0	1	1	1	1	0,503	Ineffective
Cenário 6	1	0	1	0	1	0	1	0	0,607	Effective
Cenário 7	1	1	1	1	1	0	0	0	0,841	Effective
Cenário 8	0	1	1	0	0	1	1	0	0,342	Ineffective
Cenário 9	1	1	0	0	0	1	1	0	0,154	Ineffective
Cenário 10	1	1	1	1	0	0	0	0	0,497	Ineffective
Cenário 11	1	1	1	1	0	1	1	1	0,655	Effective

Cenários Aleatórios

	Gestão de Acessos Lógicos								Resultado	*Effective/Ineffective*
	GAL1	GAL2	GAL3	GAL4	GAL5	GAL6	GAL7	GAL8		
Cenário 1	0	0	0	0	1	1	1	0	0,426	Ineffective
Cenário 2	0	1	1	1	1	0	1	1	0,919	Effective
Cenário 3	1	0	1	1	0	0	1	0	0,474	Ineffective
Cenário 4	1	1	0	0	0	1	0	0	0,129	Ineffective
Cenário 5	0	0	1	0	1	0	1	0	0,582	Ineffective
Cenário 6	1	1	1	0	0	1	1	1	0,443	Ineffective
Cenário 7	0	1	1	0	0	0	1	1	0,362	Ineffective
Cenário 8	1	1	1	1	1	0	0	0	0,841	Effective
Cenário 9	1	1	0	1	1	0	1	0	0,655	Effective
Cenário 10	1	0	0	1	0	0	0	1	0,313	Ineffective
Cenário 11	0	1	1	1	1	0	1	0	0,842	Effective
Cenário 12	1	1	1	0	1	1	0	1	0,763	Effective
Cenário 13	0	1	0	1	1	1	1	1	0,763	Effective
Cenário 14	1	1	1	1	1	0	1	1	0,944	Effective
Cenário 15	1	0	0	1	0	0	1	0	0,262	Ineffective
Cenário 16	0	0	1	0	0	1	0	0	0,269	Ineffective
Cenário 17	1	1	1	0	0	1	1	1	0,443	Ineffective
Cenário 18	1	0	1	1	0	1	0	1	0,582	Ineffective
Cenário 19	1	0	1	0	0	1	1	0	0,318	Ineffective
Cenário 20	0	0	0	0	1	1	1	0	0,426	Ineffective
Cenário 21	0	0	1	1	1	0	0	0	0,769	Effective

Limiar de Eficácia	Inef. < 0,6 < Ind. < 0,65 < Ef.

Anexo 4 - Cenários Operações

Cenários Construídos					
	Operações			Resultado	*Effective/Ineffective*
	O1	O2	O3		
Cenário 1	1	1	0	0,331	Ineffective
Cenário 2	1	0	0	0,243	Ineffective
Cenário 3	1	0	1	0,912	Effective
Cenário 4	0	0	1	0,669	Ineffective
Cenário 5	0	1	0	0,088	Ineffective
Cenário 6	0	1	1	0,757	Effective

Limiar de Eficácia	Inef. < 0,7 < Ind. < 0,75 < Ef.

Anexo 5 - Cenários Sistemas (Objectivo 1)

Cenários Construídos					
	Categorias			Resultado	*Effective/Ineffective*
	GA	GAL	O		
Cenário 1	1	1	0	0,928	Effective
Cenário 2	1	0	0	0,279	Ineffective
Cenário 3	1	0	1	0,351	Ineffective
Cenário 4	0	0	1	0,072	Ineffective
Cenário 5	0	1	0	0,649	Ineffective
Cenário 6	0	1	1	0,721	Effective

Limiar de Eficácia	Inef. < 0,65 < Ind. < 0,7 < Ef.

Anexo 6 - Cenários Sistemas (Objectivo 2)

	Valores de Entrada			Ponderadores das Categorias			Valores multiplicados pela ponderação da Categoria			Soma dos Valores
	GA	GAL	O	GA	GAL	O	GA	GAL	O	
Valor mínimo dos Limiares de Indecisão	0,700	0,600	0,700	0,279	0,649	0,072	0,195	0,389	0,050	0,635
Valor máximo dos Limiares de Indecisão	0,800	0,650	0,750	0,279	0,649	0,072	0,223	0,422	0,054	0,699

Limiar de Eficácia	Inef. < 0,63 < Ind. <0,7 < Ef.