INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA

AUDITORIA DOS SISTEMAS DE INFORMAÇÃO DAS INSTITUIÇÕES FINANCEIRAS

Ivan Martins

Lisboa, Julho de 2013

INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

AUDITORIA DOS SISTEMAS DE INFORMAÇÃO DAS INSTITUIÇÕES FINANCEIRAS

Ivan Martins

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Contabilidade e Gestão de Instituições Financeiras, realizada sob a orientação científica do Mestre Jorge Sequeira, Professor Adjunto na área da Ciências da Informação e Comunicação.

Constituição do Júri:
Presidente: Mestre Carlos Caldeira
Arguente: Mestre Rui Vieira
Vogal: Mestre Jorge Sequeira (Orientador)

Lisboa, Julho de 2013

Declaro ser o autor desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido (no seu todo ou qualquer das suas partes) a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas. Mais acrescento que tenho a consciência de que o plágio – a utilização de elementos alheios sem referência ao seu autor – constitui uma grande falta de ética, que poderá resultar na anulação da presente dissertação.

Agradecimentos

A minha família por todo o apoio e suporte dado durante a elaboração deste trabalho.

A minha namorada Luísa pela força e garra que me transmitiu no sentido de completar a dissertação.

Ao meu colega e amigo Filipe Silva por todo o auxílio que me prestou no sentido de completar o melhor possível a parte pratica.

Ao meu orientador Dr. Jorge Sequeira pelo apoio prestado na elaboração desta dissertação.

A todos os meus amigos que me transmitiram força e vontade para terminar este trabalho.

Resumo

O presente trabalho tem como objetivo a análise dos métodos e processos existentes, na elaboração de auditorias aos sistemas de informação, em particular nas instituições de carácter financeiro.

A globalização das plataformas informáticas e os seus benefícios em termos de partilha de informação e simplificação de tarefas teve como consequência a adoção por parte da grande maioria das empresas deste tipo de serviços, o que tornou a preocupação com os sistemas informáticos e os seus riscos de utilização um assunto de bastante relevo.

As instituições financeiras dada a natureza do seu negócio são das entidades que mais se encontram dependentes de toda a sua plataforma informática, visto que as transações, transferências e informações presentes nos seus servidores são de vital importância para o seu funcionamento ou até para a sua sobrevivência.

Este trabalho procurará mostrar a verdadeira função da auditoria de sistemas de informação em instituições financeiras nos dias de hoje e a sua vital importância. Este trabalho começa com uma breve descrição da evolução sofrida ao longo do tempo pela auditoria até à formação da auditoria a sistemas de informação e da sua função e processos, sendo que posteriormente serão apresentados os *frameworks* usados para regulamentar ou auxiliar no controlo e avaliação da plataforma informatizada da empresa. Serão igualmente demonstrados que tipos de testes ou pesquisas podem ser efetuados aquando de uma auditoria com especial foco no controlo dos riscos e avaliação dos controlos implementados culminando com a apresentação de casos práticos de auditorias a sistemas de informatização elaborados em instituições financeiras.

Palavras-chave: Sistemas de informação, auditoria e controlo.

Abstract

The present work aims at analyzing the existing methods and processes for the preparation of audits of information systems, particularly in the institutions of a financial nature. The globalization of computing platforms and its benefits in terms of sharing information and simplification of tasks resulted in the adoption by the vast majority of companies for such services, which became a concern with computer systems and their risks use a very matter of relief. Financial institutions given the nature of your business are the entities that are more dependent on its entire platform, since the transactions, transfers and present information on their servers are vital to its functioning or even to their survival. This paper will seek to show the true function of the audit of information systems in financial institutions today and its importance. This paper begins with a brief description of the evolution over time suffered by the audit until the formation of the audit of information systems and their function and processes, and then will present the frameworks used to regulate or assist in monitoring and evaluation platform computer company. Will also be shown what types of tests or surveys may be conducted during an audit with a special focus on risk control and evaluation of controls implemented culminating in the presentation of case studies of audits of computerized systems designed for financial institutions

Keywords: Information systems, audit and control.

Índice

Índice de figuras

Lista de abreviaturas

CCTA	Control computing and telecommunication Agency
Cobit	Control Objectives for Information and related Technology
IEC	International Eletrotechnical Comission
IFAC	International Federation of Accountants
IGAE	Intervencion General de la Administracion del Estado
INTOSAI	International Organization of Supreme Audit Institutions
ISACA	Information Systems Audit and Control Association
ISO	International organization for Standardization
ITIL	Information Technology Infrastructure Library
ITSMF	IT Service Management Forum
MOF	Microsoft Operations Framework
PDCA	Plan, Do, Check, Act
PME	Pequenas e Médias Empresas
POC	Plano Oficial de Contas
SEI	Software Engineering Institute
SGSI	Sistema de Gestão de Segurança de Informação
SI	Sistemas de Informação
SNC	Sistema de Normalização Contabilística
TI	Tecnologia de informação
TIC	Tecnologias de Informação e Comunicação
USGAO	United States Government Accountability Office

1. Introdução

Com o avançar do tempo, a auditoria como a conhecemos foi sofrendo algumas alterações, quer com a mudança de conceitos e objetivos que foram conseguidos com a alteração do POC para SNC e o avanço das plataformas informáticas, quer também em termos de técnicas e métodos com a elaboração de novos testes e analise de forma a fazer face ao desenvolvimento e aparecimento de novos problemas. Um dos grandes impulsionadores destas alterações foi o aparecimento dos sistemas de informação que, com o passar do tempo, conquistaram, junto dos gestores das empresas uma importância vital na sustentabilidade das mesmas. As empresas no mundo atual encontram-se em constante metamorfose e necessitam aceder a todo o tipo de informações, como financeiras, industriais e sociais, quase instantaneamente, de forma a poderem competir num mercado cada vez mais competitivo. Esta situação só é conseguida através da utilização de equipamentos informáticos que facilitem o acesso às informações necessárias em qualquer ponto do mundo. Estas alterações culminaram com a alteração completa do "*modus operandi*" da maioria das empresas, passando elas próprias, como indica Carneiro (2009:1), «de sociedades de indústria para sociedades de informação», mas não foram elas próprias as únicas a sofrerem alterações, tendo indiretamente influenciando várias empresas interligadas, entre as quais, as sociedades de auditoria. Derivado de todas estas alterações ocorridas, Oliveira (2006:14) defende que «A auditoria a sistemas de informação não é hoje em dia apenas uma simples extensão da auditoria tradicional», pois dada a importância que as plataformas informáticas detêm atualmente na empresa, necessitam de ser controladas e verificadas. Oliveira (2006:15) defende que «Os dados processados e os programas utilizados pelos sistemas informáticos são invisíveis e intangíveis, sendo acessíveis ou modificáveis e sem deixar vestígios. Por isso, os responsáveis e os auditores devem tomar medidas especiais que garantam a fiabilidade, integridade e confidencialidade de qualquer dado obtido do sistema informático». É de salientar que atualmente, a auditoria aos sistemas de informação é imprescindível na elaboração de uma certificação legal de contas dada a quantidade de informação que apenas é elaborada eletronicamente. A utilização destas ferramentas está sempre dependente de vários fatores que podem influenciar todo o desenrolar da atividade empresarial. A dificuldade dos colaboradores em assimilar as competências para laborar com as plataformas, a utilização de materiais informáticos mais obsoletos, algo bastante

comum, dada a velocidade em que uma novidade informática hoje, amanha já é considerada obsoleta, a falta de planeamento, por parte da gestão, dos parâmetros necessários ao bom funcionamento da plataforma são exemplos de situações que não irão transmitir uma imagem real e apropriada do estado da empresa. Carneiro (2009:2) defende que «A auditoria informática trouxe soluções para estes problemas». O grande problema deste tipo de auditoria atualmente é que apenas as grandes empresas de auditoria a praticam, sendo que grande parte das empresas do mercado nacional não sofrem qualquer tipo de controlo ou verificação dos seus dados digitais. Carneiro (2009:2) defende «Por diversas razões e devido ao desenvolvimento das TIC no tecido empresarial, este tipo de auditoria tem sido valorizado e a sua aplicação pode ser realizada também em PME's. Por gerar informação sobre o controlo interno e as condições de segurança dos recursos informacionais existentes, a auditoria informática rege-se pela adoção de métodos e procedimentos de controlo de SI que são válidos para uma empresa de qualquer dimensão». É uma realidade á qual qualquer empresa pode aceder, pois como existem programas informáticos que se adaptam ao tamanho e volume de negócio de uma empresa, a auditoria informática também é ajustada consoante a necessidade de trabalho a desenvolver e a complexidade do sistema informático da empresa. No âmbito do trabalho, as instituições financeiras, a necessidade e dependência das plataformas informáticas é uma das principais vantagens e também um dos maiores riscos que as mesmas possuem, fazendo com que a auditoria aos seus sistemas de informação seja uma obrigação determinante para um correto funcionamento de toda a estrutura das empresas. O mercado financeiro não foi exceção, a todas as alterações que aconteceram no mundo com o passar dos anos, visto que até ao ano de 2004 a maioria do mercado bancário era composto por bancos nacionais de cada país. Não existiam grandes transações entre instituições europeias, mas a grande mudança deu-se a partir dessa altura. Os bancos começaram a investir fora dos seus locais de conforto, começaram a efetuar aquisições de outros bancos ou a financiarem instituições fora dos seus países. Os investimentos estrageiros foram das ações mais praticadas, e segundo a *European Confederation of Institutes of Internal Auditing* (2009:13), no ano de 2006 o mercado europeu era composto por um total de oito mil quatrocentos e quarenta e uma instituições de crédito e duzentas e doze mil agencias bancarias com um total de ativos de trinta e seis mil oitocentos e vinte biliões de euros em que quarenta e cinco mil eram grupos bancários que funcionavam fora do seu país de origem. O mercado bancário com a abertura de fronteiras a bancos estrangeiros começou a

conter uma característica que até ao ano de 2004 não possuía, a competitividade. Regra geral o banco nacional detinha todo o monopólio. Com o aparecimento de bancos privados esse monopólio foi sendo diluído. A existência de concorrentes, com outro tipo de propostas e serviços, aliada a uma forte ajuda vinda da casa-mãe fez com que todo o funcionamento do ambiente financeiro se alterasse. O sistema de informação das instituições financeiras foi uma das peças mais importantes para a evolução que ocorreu neste mercado. A sua constante evolução, com os desenvolvimentos sofridos em termos de processamento de informação, criação de análises e comunicação entre diferentes pontos do globo ajudou a criar a plataforma perfeita para que as organizações financeiras se desenvolvessem e começassem a aspirar a novos objetivos que até ao momento não seriam possíveis. Dada esta dependência criada em torno dos sistemas de informação a necessidade de fiscalizar, controlar e analisar todos os prismas das instituições financeiras tornou-se obrigatória. A auditoria a estas entidades é uma obrigação, um bem essencial para o bom funcionamento das mesmas visto que laboram num ambiente onde o risco operacional e a possibilidade de uma falha pode despoletar uma crise mundial.

2. Evolução da auditoria a sistemas de informação

2.1 Evolução histórica da auditoria aos sistemas de informação

Num trabalho onde o tema principal é a auditoria praticada em sistema de informação é necessário antes de mais explicar e apresentar como surgiu a sua base, a auditoria propriamente dita. Segundo estudos antropológicos já no ano de 3.000 a.C. existiam atividades relacionadas com a auditoria, mas o seu conceito foi definido historicamente, no tempo do império romano, visto os imperadores romanos para controlarem melhor as diversas e extensas províncias, por si dominadas, faziam deslocar às mesmas funcionários, com conhecimentos específicos, da sua confiança, para avaliar os lucros e gastos dessas mesmas terras. A auditoria foi sofrendo várias alterações e desenvolvimentos durante o desenrolar da evolução social que ocorreu no mundo, sendo que apenas na segunda metade do século XIX é que a mesma foi adotada pelas empresas, muito devido á revolução industrial ocorrida na Grã-Bretanha. O desenrolar da revolução veio trazer à industria um desenvolvimento desenfreado de tecnologias, quer em novos equipamentos mais avançados, quer em novas técnicas de produção em massa e utilizações de muitos componentes que na época eram topo de gama. A novidade representava o caminho a seguir, mas com um problema que poderia funcionar como um despoletar de falências devido ao elevado custo que representavam. Com todas as alterações sofridas pelas empresas, quer em termos de ferramentas de trabalho como na sua génese, dado a própria denominação de empresa ter-se alterado assistindo-se ao desenvolvimento das sociedades anónimas, os responsáveis pelas empresas não conseguiam obter um controlo interno sobre as ações desenvolvidas e igualmente manter o foco do seu trabalho de gestão, situação que levou a criação de técnicos especializados em controlo e em contabilidade, que foram apelidados de auditores. O crescimento desta prática deveu-se principalmente à colonização da América do Norte, mais concretamente, Estados Unidos e Canada, por parte da Inglaterra, acontecimento que permitiu um elevado desenvolvimento dos países em questão e ao aperfeiçoamento da prática da auditoria. Com o constante desenvolvimento das grandes empresas americanas, o objetivo das mesmas passou a ser a internacionalização, situação que permitiu uma transmissão de *know-how*, o que ajudou a implementar a prática da auditoria em vários países que ainda não a praticavam. Na

Europa, a prática da auditoria nunca foi muito desenvolvida tendo como exceção dessa situação países mais desenvolvidos como a França, Noruega ou mesmo o Reino Unido. Este cenário de subdesenvolvimento começou a sofrer profundas alterações com a criação da união europeia e a sua tentativa de uniformizar as leis e práticas de controlo empresarial, levando a que fosse necessário investimento na criação de uma nova profissão, a de auditor; técnico externo às empresas que praticava diversos tipos de peritagem e analises às contas financeiras das empresas. A crescente procura por parte das empresas levou a que empresas especializadas nesta área se desenvolvessem culminando na situação que se verifica nos dias de hoje, formada por um conjunto de multinacionais de auditoria espalhadas por vários países com uma vasta área de abrangência nos diversos sectores das empresas. Os sistemas de informação utilizados pelas empresas no início dos anos 60 até sensivelmente aos anos 90, segundo Pearlson e Saunders (2009:47), eram apenas direcionados para o uso interno da empresa, primeiro pela necessidade de diminuir os custos da mesma com processos mais baratos, depois como suporte para os gestores dada a sua possibilidade de registar e analisar toda a informação da organização, sendo que os sistemas ajudavam na reprogramação de alguns processos produtivos das empresas. Com o avançar dos tempos, com o desenvolvimento dos mercados, os sistemas de informação foram-se desenvolvendo, ganharam uma importância não exclusivamente na avaliação interna da empresa, mas também na avaliação do meio envolvente onde esta está inserida e na avaliação dos seus concorrentes. Dado o crescimento da influência, no seio da empresa, a auditoria não poderia deixar de acompanhar todos os novos processos elaborados nos sistemas implementados.

2.2 Governança dos Sistemas de informação

Existem bastantes indicadores que demonstram as vantagens em implementar sistemas de informação numa empresa, alguns dos riscos também, mas para uma correta passagem para o processamento de dados em estado virtual a mudança tem e deve ser corretamente definida e elaborada, com o risco de que se algo não é perfeitamente parametrizado, dificilmente a empresa irá usufruir das máximas potencialidades das suas capacidades operacionais. De acordo com o ISACA (2010:9) a governança de sistemas de informação é definida como «o processo que garante que a tecnologia de informação se alinhe com a estratégia de negócio e promova com eficácia os objetivos organizacionais». O

departamento responsável pela implementação desta tecnologia de informação trabalha em função de atingir certos objetivos que permitam á firma efetuar uma correta governança dos mesmos, sendo que o mais flagrante e reconhecido é o de proporcionar à empresa uma correta programação das plataformas informáticas para que a mesma possa usufruir de um *upgrade* em termos de processamento de informação, quer em termos de rapidez como de avaliação, tudo bases para o cumprimento dos objetivos comerciais definidos pela chefia. O departamento responsável pela implementação dos sistemas de informação ainda possui dois objetivos importantes a cumprir, podem não ser tão vitais como o anteriormente apontado, mas não podem ser deixados de parte, que são o controlo de custos e a garantia de continuidade do negócio. Com a adoção do processo informático, os custos com a aquisição de *hardware* por parte da instituição vão diminuir assim como o custo com a eletricidade. Os benefícios alcançados com esta aquisição não se cingem apenas ao controlo de custos, sendo que com esta ferramenta de virtualização de dados, a governança deve ser capaz de permitir a continuidade da empresa no tempo com a adaptação do sistema informático da empresa a novas realidades e novos nichos de mercado que a empresa pode tentar entrar, sem grande alteração do núcleo geral, mas sim apenas dotando a empresa de simples mas eficazes soluções para que os novos desafios sejam facilmente ultrapassados. Os responsáveis pelo departamento de gestão dos sistemas informáticos vão deparar-se com alguns riscos de grau elevado que podem fazer ruir todo o processo instalado na empresa. Para o cumprimento dos seus objetivos, o departamento deve encontrar-se munido de colaboradores que possuam elevados conhecimentos de informática e grande experiência na implementação e gestão diária de todas as possíveis ocorrências provenientes da atividade operacional da empresa. Neste ponto surge o primeiro problema, pois embora a informática seja atualmente do conhecimento geral de todos os colaboradores de várias empresas, a organização pode ter dificuldade em obter para o departamento responsável pela gestão dos mesmo, pessoas com os conhecimentos suficientes para que se consiga, através do uso dos seus avanços tecnológicos, alcançar os seus objetivos operacionais. Indiretamente com o primeiro risco surge o segundo como consequência do anterior, tudo relacionado como a empresa controlava, no passado, as suas tecnologias de informação. As organizações anteriormente faziam distinções entre os vários componentes informáticos que detinham, isto é, os antivírus, o *hardware*, o *software*, as redes internas eram verificadas separadamente, situação que com o surgimento da virtualização se modificou por completo, dada a impossibilidade de efetuar esta

separação, muito por culpa do desaparecimento dos terminais físicos como pela existência de uma rede de trabalho totalmente interligada e virtual, do qual é praticamente impossível tratar os bens de formas separadas e é por causa desta especificidade que a empresa incorre num risco, visto que é necessário uma forte e desenvolvida base de suporte deste sistema para que seja possível obter total acesso as suas potencialidades.

2.3 Ligação entre auditoria financeira e a auditoria de sistemas de informação

Com o desenvolvimento das organizações foi também desenvolvido, no seu seio, a necessidade de as próprias serem alvo de análises e avaliações internas e externas, com o objetivo de as auxiliar no alcançar o máximo das suas capacidades e qualidades, sendo esta a base para a criação da chamada auditoria. A IFAC, entidade criada em Outubro de 1977 através de um acordo assinado por 63 associações de profissionais da área da contabilidade e auditoria com o objetivo de desenvolver e emitir normas geralmente aceites para desenvolver a pratica da auditoria e criar conteúdos de relatórios gerais de auditoria que servissem padrões a nível mundial, criou uma base de auditoria apelidada de ISA /NIR, ou seja, normas internacionais de auditoria e onde define o objetivo essencial da auditoria como sendo o de aumentar o grau de confiança dos utilizadores das demonstrações financeiras de determinada empresa, e isto é alcançado pela emissão de uma opinião por parte de um auditor independente e qualificado, com base em normas técnicas no qual indica que todas as demonstrações estão corretamente elaboradas de acordo com as leis em vigor e que as mesmas apresentam uma imagem verdadeira e apropriada da posição financeira e do resultado operacional da entidade. A base do trabalho do auditor são as demonstrações financeiras desenvolvidas pela organização, sendo que o recurso essencial para esse desenvolvimento é o registo de toda a informação das atividades desenvolvidas no ano do exercício em causa, e no seguimento da importância que a mesma tem para a empresa. A forma como é recolhida, tratada e posteriormente armazenada deve ser alvo de cuidados elevados, especialmente ao nível do registo de quem tem acesso à mesma, quando teve acesso, onde se encontra armazenada e por quem. Estes controlos internos mantêm a informação livre de riscos de adulteração, situação que pode dar azo a problemas graves para o futuro e continuidade da empresa. Anteriormente ao aparecimento dos

computadores e dos avanços tecnológicos todo o suporte existente acerca das informações sobre a empresa existia em formado documental, em papel, o que do ponto de vista da auditoria era de fácil verificação e avaliação dos controlos internos, se os mesmos estariam a funcionar corretamente ou mesmo se estariam devidamente elaborados, visto que o procedimento de registo de informação passava por uma ou mais pessoas. Havia uma segregação de funções e procedimentos a desenvolver pelas diferentes áreas da empresa. O auditor para desempenhar corretamente a sua análise e avaliação deve, segundo Pedro (1992:12) desempenhar quatro etapas no trabalho de auditoria:

1) Avaliação global do controlo interno que determinará o grau de confiança a atribuir ao sistema de informação. Desta avaliação resultará a natureza, oportunidade e extensão dos procedimentos de substanciação a executar posteriormente;
2) Compreensão do sistema contabilístico e exame com vista á determinação dos seus pontos fracos;
3) Verificação da conformidade que permite avaliar o grau de confiança do controlo interno em pontos nevrálgicos do sistema de informação;
4) Substanciação para obter evidência sobre a integralidade, exatidão e validade dos dados.

Com o avanço tecnológico todo o processo foi sofrendo alterações significativas, o acesso aos dados foi tornado mais rápido mas ao mesmo tempo mais complexo, o processo de registo da informação sofreu grandes modificações sendo que a auditoria informática não pode agora ser vista como um prolongamento da auditoria tradicional. Segundo Pedro (1992:13) «Num ambiente informatizado, as funções que antes estavam convenientemente segregadas por um conjunto de pessoas, podem estar agora aglutinadas num único programa cuja descrição funcional ou orgânica nunca foi escrita» e também que num ambiente virtual «o que anteriormente podia ser visto sem óculos, exige agora o conhecimento de sofisticados instrumentos de observação» tudo porque algumas das transações agora desenvolvidas por estas ferramentas não possuem o mínimo de suporte visível, sendo apenas descoberto o resultado final de tais movimentos, sem saber quais os passos que foram tomados para chegar à conclusão final. Quando comparado com a auditoria a elementos físicos em termos de objetivos, a diferença é inexistente, ambas servem para verificar o funcionamento dos controlos internos e se as contas da empresa

refletem o seu estado fidedignamente. A grande diferença é verificada nos métodos a utilizar para alcançar tais objetivos, em questões mais concretas como o controlo da própria plataforma de trabalho utilizada pela entidade que vai alterar o planeamento da auditoria a elaborar. Na opinião de Pedro (1992:13) o auditor financeiro, por exemplo, para cumprir as quatro etapas da auditoria, necessita de um conjunto de informação complementar sobre:

- A conceção global do sistema de informação;
- A organização e gestão do serviço de informática;
- A arquitetura física e lógica da informática compreendendo o equipamento, *software*, comunicações e dados;
- Os controlos relativos à operação dos computadores e do *software* de sistema;
- Os procedimentos de conceção de *software* e de segurança relativos às diversas aplicações;
- Os procedimentos de entrada e saída de dados nas aplicações relevantes;
- A evolução prevista do sistema de tratamento da informação;

O auditor informático necessita de obter um grande conhecimento em áreas até aqui dispensáveis para a emissão da sua opinião, sendo que tem de desenvolver e dominar uma enorme quantidade de valias que lhe permitam trabalhar no novo meio onde se encontra e emitir o seu parecer com base num trabalho isento de erros e possíveis riscos.

2.4 Instituições financeiras e a auditoria aos sistemas de informação

As instituições financeiras fazem parte de um mercado específico que engloba todas as empresas que de alguma maneira conseguem obter recursos financeiros ou fiduciários e os investem a determinada taxa de forma a alcançar um retorno financeiro. O mercado financeiro divide-se em dois grandes sectores diferentes. Um é **o sector bancário**, que é composto por instituições de crédito, empresas de locação financeira e de factoring entre outras, que têm como objetivo de negócio a receção de depósitos por parte do público e das empresas com o intuito de os aplicar por sua vontade mediante o recebimento de um valor com base numa taxa de jura previamente discutida. O outro é o **sector segurador** que é composto maioritariamente pelas companhias de seguro, entidades que têm como negocio o assumir de certos tipos de riscos que podem afetar o dia-a-dia da população em geral ou

empresas, em troca de um pagamento apelidado de prémio de seguro, valor esse composto pelo cálculo da probabilidade de o sinistro segurado acontecer incrementado por comissões de gestão de todo o processo. De acordo com Rodrigues (2010:5) «as instituições financeiras têm como objetivo a obtenção e aplicação de recursos financeiros, sendo o mais sofisticado, mas também o mais vulnerável segmento de uma economia de mercado». As sociedades de crédito e seguradoras formam um núcleo que labora de forma bastante eficaz, com grande controlo nos seus dados e processos mas que dada a sua forma de funcionamento sofre de uma enorme interdependência entre as várias organizações que compõem o dito mercado. Ao utilizarem os depósitos e poupanças recebidos para financiar outras entidades por intermédio da cedência de créditos, vão assumir um risco com montantes que não são sua propriedade, apenas tendo como contra partida o pagamento de uma taxa de juro, situação que só é possível através da existência do bem mais necessário em todo este mercado, a confiança. Uma instituição financeira ou mesmo uma pessoa em nome individual que veja perdida a confiança que os restantes parceiros detêm nela já não irá conseguir nenhum tipo de apoio financeiro ou financiamento. A forte dependência e interligação entre as organizações financeiras é por si só um grande risco no mercado, as baixas margens praticadas pelo negócio financeiro ainda aumentam mais a possibilidade de acontecimento de um desastre. Os depósitos efetuados pelos clientes necessitam de ser remunerados a uma taxa previamente definida e são esses valores que vão possibilitar aos bancos emprestarem a terceiros quantias pelas quais vão ser ressarcidos de uma percentagem do total do empréstimo a multiplicar por uma taxa de juro. No momento em que exista uma grave crise financeira por falha de algum dos parceiros, o sistema bancário não possui a capacidade financeira ou a liquidez necessária para proceder a estabilização e equilíbrio das perdas e graças a interdependência das instituições vai ter um efeito catastrófico no mundo financeiro. Todos estes riscos decorrentes do funcionamento normal do mercado financeiro levaram a que os responsáveis pelo supervisionamento do mesmo decretassem o aumento de toda a vigilância para com as transações, assim como a criação de legislação mais apertada e regulamentação com critérios mais rígidos de forma a combater possíveis falhas. Nos últimos anos temos assistido a várias crises nas instituições financeiras que culminaram com grandes perdas como é o caso da crise financeira que o mundo atravessa nesta altura, resultado direto de uma atividade normal das instituições bancárias que não foi prevenida corretamente. Estatisticamente a grande maioria dos problemas do sector resultam de situações que não são programadas, de acontecimentos

que não são previstos pelos responsáveis ou pelos sistemas de informação, situações essas que não permitem, por parte das entidades, um combate eficaz na mitigação dos problemas que vão decorrer do mesmo. Os sistemas de informação das instituições financeiras não foram o causador desta ultima crise mas no passado já existiram alguns problemas muito graves devido a falta de supervisão e controlo nos sistemas de informação das empresas, como por exemplo a crise do bug do milénio, onde se acreditava que com o passar de ano de 1999 para o ano 2000 um possível erro informático iria causar o *crash* de todas os sistemas fazendo com que se perdesse toda a informação e bases de dados mundiais, levando a um evento quase catastrófico para população mundial. O regulador através da avaliação de todos estes problemas passados e dada a necessidade de fazer face ao risco operacional que a própria atividade financeira pressupõe concluiu que era necessário implementar mais controlo e segurança nos sistemas de informação das instituições financeiras, que deviam ser regulamentados os tipos de controlo a implementar. Foi criado em Basileia, no ano de 2004, um acordo que tem como pressuposto dotar as instituições financeiras, mais concretamente as sociedades bancárias, de um conjunto de regras no sentido de fortalecer a sua resistência à crise e ao risco operacional, tentando desta forma impedir a formação de novos períodos de crise. O acordo denominado Basileia II assenta as suas ideias em três pilares bastante distintos e que são a determinação dos requisitos mínimos de fundos próprios, o processo de avaliação pela autoridade de supervisão e a disciplina de mercado. O pilar que é mais importante focar na elaboração deste trabalho é o segundo, o do processo de avaliação pela autoridade de supervisão, sendo que segundo este pilar as instituições financeiras são obrigadas a criar e deter sistemas de informação que possibilitem uma correta avaliação dos riscos operacionais que a entidade corre a avaliar o capital interno de forma a tomar conhecimento e controlo sobre a possibilidade de fazer frente a uma possível crise, e permitir através desses mesmos sistemas a consequente avaliação do funcionamento dos mesmos por parte dos agentes de supervisão para que este garanta a legalidade de todo o processo de controlo interno presente na instituição. Com todas as alterações que decorreram nas instituições financeiras com o passar dos anos, com todo o avanço tecnológico que aconteceu e consequente dependência dos sistemas de informação, a necessidade de uma auditoria independente aos mesmos é enorme, nem sempre só para validar e verificar se os prossupostos decididos em Basileia se encontram corretamente inseridos, mas também para validar os controlos internos que ajudam na gestão da instituição e se a instalação e o *update* das plataformas de trabalho foram bem

efetuados, sendo um dos principais obstáculos á utilização total das capacidades de um sistema informático a má instalação e programação do mesmo. Com um mercado bastante competitivo, com margens diminutas em que cada cliente ou cada depósito pode fazer a diferença, uma instituição que detenha um sistema de informação a funcionar corretamente consegue obter uma grande vantagem sobre as suas concorrentes, em termos de produtos que pode oferecer, resposta a problemas ou até mesmo resposta a produtos concorrentes. Atualmente um os processos mais em uso pelas instituições financeiras com o auxilio dos seus sistemas de informação é o chamado *"Home Banking"* que oferece uma maior flexibilidade aos seus parceiros, visto que atualmente é mais fácil aceder às plataformas informáticas das instituições do que uma deslocação física a uma agência.

3. A função da auditoria aos sistemas de informação e os seus processos

3.1 Conceitos fundamentais e finalidades – Objetivos e funções do auditor de sistemas de informação;

O conceito atribuído á auditoria de S.I. não difere muito do atribuído á dita auditoria tradicional. Ron Weber (1999) define a auditoria a um S.I. como o processo de recolha e avaliação de evidência para determinar se um sistema computorizado salvaguarda os bens, mantem a integridade dos dados e permite atingir os objetivos da organização de forma eficaz e eficiente. A definição que melhor demonstra o significado de uma auditoria a um S.I e que melhor foca as principais características é da autoria da *Intevencion General de la Administración del Estado*, uma entidade espanhola mais conhecida como IGAE e que é responsável pela autoridade de auditoria na península ibérica, em coordenação com a inspeção-geral das finanças de Portugal. Defende que uma auditoria a um S.I é a revisão dos sistemas de informação, para verificar se realizam as funções e operações para os quais foram criados, assim como comprovar se os dados e demais informações contidos correspondem aos princípios de fiabilidade, integridade, precisão e disponibilidade. A auditoria informática foi desenvolvida muito por necessidade de controlar os processos de registo e tratamento da totalidade das transações das empresas como também validar as demonstrações financeiras emitidas pelas mesmas, e para isso ocorrer, foi necessário, segundo Ron Weber (1999) a utilização de quatro disciplinas que juntas formaram a base de todo o processo:

- **Auditoria tradicional** – Forneceu á auditoria informática o seu Know-how e experiência em avaliação de controlos internos que foram utilizados para a elaboração dos seus próprios manuais de auditoria assim como na elaboração de testes e controlos a utilizar nas plataformas informáticas. Foi também através desta auditoria que foram aprendidos os métodos de captação e avaliação da informação;
- **Gestões de sistemas de informação –** Ao longo dos anos os investigadores preocuparam-se em definir qual a melhor maneira de implementar um sistema de informação numa organização, e com a melhoria alcançada nas técnicas de gestão de projetos, de registo de documentação, orçamentos e outros esse mesmo objetivo

foi alcançado. Estes avanços interagem com a auditoria a sistemas de informação porque são processos que alteram a integridade dos dados, a salvaguarda dos bens e a eficácia e eficiência do alcance dos objetivos por parte da entidade;

- **Ciências do comportamento –** A utilização dos suportes informáticos por parte dos colaboradores da empresa podem levar a falhas que os programadores não anteverão, como por exemplo a resistência das pessoas com mais idade em trabalhar com este tipo de plataformas pode muitas vezes culminar com erros considerados graves e que minam toda a informação dependente do desenvolver dos seus trabalhos. Os auditores devem prestar atenção a estas situações comportamentais que podem levar a falhas graves no sistema;
- **Ciência informática –** Esta ciência tanto produz benefícios para a empresa como também riscos, visto que embora não seja necessário duvidar da fiabilidade dos dados provenientes dos equipamentos informáticos, a verdade é que podem ser manipulados de maneira errada, situação que o auditor pode ter dificuldade em descortinar.

Os desenvolvimentos ocorridos no ambiente empresarial ao nível dos avanços das plataformas informáticas modificaram toda a génese das operações mercantis, visto que a revolução que ocorreu mudou todo o core das transações entre as empresas. Oliveira (2006:18) defende que «Os novos modelos de negócio vão ser constituídos por milhões de transações diárias, feitas com uma intervenção humana mínima ou mesmo nula, que necessitam de ser capturadas e registadas por processos que tenham atingido um nível de automação equivalente». São estas alterações que vão trazer aos auditores novos desafios para ultrapassar visto ser necessário e mesmo obrigatório o domínio e conhecimento das novas tecnologias de informação, assim como deter a perfeita noção de que estas mesmas ferramentas podem transmitir informações financeiras falsas e manipuladas quando utilizadas negligentemente. As modificações elaboradas nestes dois pontos, no mercado e na auditoria, vão fazer uma terceira peça importante ganhar importância que até aqui não possuía, que é o controlo interno do sistema informático. Dado o aumento das transações e a perde de suporte físico da maioria dos registos, a confiança num correto funcionamento dos controlos internos assim como na correta parametrização de todos os dados gerais é extremamente necessário quer para o auditor quer para a parte responsável pela empresa.

3.1.1. Objetivos de uma auditoria de sistemas de informação

A atualidade empresarial está bastante dependente da sua componente informática, sendo através da mesma que toda a informação essencial é processada, onde todos os dados são armazenados e filtrados para proporcionar uma correta avaliação do estado geral da empresa. Ao perceber esta dependência e aceitando a importância dos sistemas de informação, a empresa pretende que os dados provenientes destas bases sejam fiáveis e que apresentem uma imagem real e fidedigna da mesma, além de que sejam capazes de detetar e prever, no futuro, possíveis falhas no desenvolver da atividade operacional, de forma a poderem ser colocados em prática medidas de melhoramento da estrutura e de mitigação dessas mesmas falhas. Com o surgir desta nova realidade, os auditores tiveram que se adaptar e alterar o sentido do trabalho a desenvolver aquando da avaliação das contas e controlos internos das empresas, tendo sido desenvolvido um novo conjunto de objetivos já focados na nova plataforma a ser analisada. Foram analisados dois pontos de vista em termos do que são os objetivos da auditoria informática, e segundo Oliveira (2006:23), os objetivos a cumprir numa auditoria de sistemas de informação são:

- Verificar a existência de medidas de controlo interno aplicáveis, com caracter generalizado, a qualquer sistema de informação da instituição, ente, organismo ou qualquer outro objeto da auditoria;
- Avaliar a adequação do sistema de informação às diretrizes básicas de uma boa gestão informática;
- Oferecer uma descrição do sistema de informação com base nas suas especificações funcionais e nos resultados que proporciona;
- Verificar se o sistema de informação cumpre os normativos legais aplicáveis;
- Verificar se a informação proporcionada pelo sistema de informação é fiável, integra e precisa;
- Determinar se o sistema de informação atinge os objetivos para os quais foi desenhado, de forma eficaz e eficiente;
- Propor as recomendações oportunas para que o sistema de informação se adapte às diretrizes consideradas como essenciais para o seu bom funcionamento;

Na ótica de Carneiro (2009:29), os auditores devem prestar a devida atenção aos sistemas de informação, mais concretamente na sua avaliação e inspeção, com os seguintes objetivos:

- Proteger as suas atividades e recursos;
- Verificar se as suas atividades se desenvolvem eficientemente e de acordo com as normas informáticas e gerais;
- Confirmar se o *hardware* e o software que se pretende adquirir corresponde inteiramente às necessidades de todo o sistema;
- Garantir o controlo da função informática;
- Analisar a eficiência dos sistemas informáticos que comporta;
- Avaliar a adequação e a eficácia dos procedimentos de controlo;
- Verificar as condições em que ocorre a exploração dos procedimentos de controlo e os processos de segurança inerentes, no que respeita a *hardware*, *software*, dados, informações e até o próprio pessoal;
- Preparar e executar a análise técnica das fases de desenvolvimento, implementação e exploração de uma dada aplicação informática;
- Verificar o cumprimento das normas gerais da empresa no que se refere à função informática;
- Rever a eficácia da gestão dos recursos materiais e humanos que pertencem a essa função;

O auditor não é apenas um individuo que se desloca a uma empresa e verifica se as contas financeiras da mesma estão de acordo com todos os normativos legais. Com o passar dos tempos o auditor começou a desenvolver uma atividade mais abrangente junto dos seus clientes, tendo lentamente passado a desenvolver quase atividades de consultor, ajudando as empresas a melhorar quer em termos de controlo interno quer de registo dos seus dados contabilísticos. As duas indicações dos objetivos da auditoria que apresentei aqui são bastante similares em diversos pontos, e eu não poderia deixar de concordar com ambas. A auditoria informática tem por função avaliar, rever e recomendar com o intuito de se proceder a um melhoramento dos controlos internos da empresa assim como analisar e avaliar a utilização de todos os recursos disponíveis na empresa, humanos, materiais e tecnológicos utilizados no âmbito operacional e estratégico. O auditor na elaboração da sua profissão deve garantir a integridade dos dados registados pelo sistema de maneira a que as transações elaboradas sejam de confiança quer para utilização interna quer para a

atribuição de uma imagem verdadeira para o exterior. Deve também avaliar a veracidade das próprias transações presentes no sistema e assim evitar que existem erros que podem induzir em erro os utilizadores de tal informação. O sistema informativo como suporte principal de toda a atividade da organização deve garantir que funciona na sua totalidade e cabe ao auditor documentar a sua disponibilidade, auditabilidade, versatilidade e correta manutenção, ou seja, o auditor deve estudar profundamente o sistema implementado na empresa em questão e verificar se a programação dos sistemas informáticos da mesma estão vocacionados para o cumprimento dos objetivos propostos pela gestão. Deve garantir o registo de todas as transações, quer operacionais quer financeiras no sistema e que as mesmas possam ser acedidas futuramente para posteriores verificações. Deve assegurar que o sistema é de fácil acesso e utilização aos dados quer visualmente quer na extração de ficheiros necessários à elaboração da auditoria e por ultimo analisar e testar os procedimentos operacionais em relação aos controlos internos, tais como testes para que o sistema funcione corretamente ao longo dos anos e que seja possível mitigar o risco de contaminação dos dados.

3.2 Tipos de auditoria a sistemas de informação

No âmbito desta dissertação foi indicado que iria abordar o tema da auditoria a sistemas de informação, mas a verdade é que não existe só um tema geral, ou seja, a auditoria a este tipo de plataforma é muito específica, e pode ser classificada consoante o objetivo que a mesma se propõe alcançar. Segundo Oliveira (2006:23), existem 5 critérios com os quais a auditoria a sistemas de informação pode ser diferenciada:

- O objetivo da auditoria;
- A posição de quem realiza a auditoria;
- A amplitude da auditoria;
- A periodicidade da auditoria;
- A extensão e profundidade da auditoria;

Uma auditoria pode ser definida consoante o seu objetivo final em dois tipos distintos. Uma com **objetivos de confirmação** e outra com **objetivos de gestão**. Uma auditoria com objetivos de confirmação é vocacionada para a validação da veracidade e fiabilidade de toda a informação registada e apresentada pela empresa enquanto uma auditoria com objetivos de gestão é mais abrangente, visto que além de englobar os mesmos objetivos da

de confirmação é também vocacionada para a avaliação da eficácia e eficiência dos sistemas de informação que existem na organização. No âmbito da posição de quem realiza a auditoria ela pode ser divida entre **auditoria externa** ou **interna.** Externa, como a própria palavra indica, é o desenvolver do trabalho por parte de uma equipa independente da empresa a ser auditada, e interna é geralmente uma auditoria desenvolvida por uma equipa com ligações a organização que vai avaliar todos os processos de acordo com as indicações dadas pela gestão. A auditoria classificada em termos de amplitude do trabalho desenvolvido pode ser separada em **auditoria geral**, que como o nome indica tem como objetivo verificar o estado global da empresa, e **auditoria parcial**, que visa analisar e avaliar apenas algumas áreas ou departamentos do todo da empresa. Quanto á periocidade a auditoria de sistemas de informação divide-se em três tipos, as **permanentes**, as **ocasionais** e as de **fim de exercício.** As auditorias permanentes são as que se realizam de uma forma bastante regular durante um período específico, ou seja, durante um período definido decorrem diversas vezes. As auditorias ocasionais apenas têm lugar quando surge algum acontecimento que não estava previsto. Só em casos de ações imprevistas, de forma a conseguir corrigir ou mitigar o problema. Por fim temos a auditoria de fim de exercício que é a prática mais comum em Portugal, que consiste na verificação anual ou semestral que tem como finalidade analisar e verificar se os resultados e informações apresentadas pela entidade espelham o seu verdadeiro estado e se apresentam uma imagem real e apropriada do valor financeiro da organização. Por fim as auditorias podem ser definidas com base na sua extensão e profundidade, dividindo-se neste caso em **integrais ou completas** e **por provas ou sondagens.** Uma auditoria integral é composta pela completa análise de todas as informações registadas pela empresa durante um espaço temporal previamente definido, podendo ser integrada numa auditoria geral ou mesmo parcial, ou seja, podem existir numa mesma auditoria classificações diferentes. Uma auditoria parcial é o que o próprio nome indica neste caso, é a análise de uma certa quantidade de registos escolhidos aleatoriamente que vão depois ser extrapolados para o todo, ou seja, é uma amostra que ao ser analisada e verificada a sua veracidade irá ser extrapolada como a imagem da empresa no seu todo. Como podemos observar pela indicação dada na descrição apresentada na auditoria integral, uma auditoria pode deter em si varias definições, desde que o objetivo da mesma seja passível de escolha entre estas cinco características, a auditoria pode muito bem possuir mais do que um critério classificativo.

4. Frameworks de referência na auditoria a sistemas de informação

A informação gerada no interior de uma empresa serve como elo de ligação entre os vários sectores e tem como objetivo juntar os vários departamentos de forma a criar um conjunto que se foque no alcançar do objetivo principal, a sustentabilidade da empresa. Para isso é bastante importante registar toda a informação sobre a totalidade dos procedimentos efetuados no decorrer da atividade da empresa no sentido de desenvolver um conhecimento real e concreto do estado geral da mesma. No decorrer deste trabalho foram identificados grandes qualidades acerca dos sistemas de informação e também enumeradas as vantagens obtidas com os mesmos, mas foi referenciado que uma errada programação ou gestão dos mesmos poderia ter consequências catastróficas para a empresa. Os responsáveis pela gestão da plataforma informática enfrentam muitas vezes um problema para o qual não existe solução, e o risco de propagação para a totalidade da empresa é elevado. O risco mencionado é o que tem origem na constante evolução dos sistemas informáticos, dado existir sempre a probabilidade de a informação sofrer alterações, seja por causa das constantes evoluções das plataformas, seja por possíveis ataques informáticos. Será então a utilização de sistemas de informação mais um risco do que uma vantagem? Segundo o ISACA (2009:7), «a gestão dos sistemas de informação é da responsabilidade dos executivos e da alta gestão, consistindo em aspetos de liderança, estrutura organizacional e processos que garantam que a área de tecnologias de informação da organização suporte e aprimore os objetivos e estratégias da organização». A gestão dos sistemas de informação depende em dois sentidos das plataformas. Em primeiro lugar, e dado que no mercado atualmente todos os processos são controlados informaticamente, é necessário garantir que os sistemas de informação estão bem implementados com as politicas e procedimentos da empresa por forma a alcançarem os objetivos propostos e evitar que existam acontecimentos que ponham em causa esses mesmos objetivos e em caso de existirem que a plataforma os combata. Em segundo lugar na necessidade de obtenção de informação cada vez mais precisa que ajude a desenvolver novas estratégias de mercado que irão servir de base para novos investimentos ou entradas em diferentes segmentos de mercado. Para conseguir desenvolver todo o sistema de forma a alcançar este tipo de informação é necessário a implementação de metodologias de sistema de informação, *frameworks* de boas práticas de sistemas que vão permitir à gestão dominar os recursos presentes na

empresa e manipula-los na forma que mais convém à instituição. No âmbito do trabalho iremos desenvolver mais detalhadamente o Cobit e o ITIL no âmbito das metodologias e a ISO 27001 no âmbito da segurança dos sistemas de informação.

4.1 Cobit

Para uma empresa obter um aproveitamento total das ferramentas que possui a gerência precisa de desenvolver mecanismos que lhe possibilitem controlar todo o sistema de informação. Necessita de garantir a correta ligação dos mesmos com a área de negócio em que se encontra, organizar as tarefas a desenvolver pela plataforma segundo diretrizes globalmente aceites pelos empregados da organização. Deve também escolher dentro da plataforma quais os sistemas de informação mais importantes para o alcance dos objetivos e desenvolver esses mesmos e, não menos importante, deve desenvolver e decidir quais as finalidades a atingir com os controlos que vão ser implementados. Neste sentido uma das metodologias que pode ser adotada e que cobre estes quatro pontos é o Modelo Cobit. O ISACA (2009:11) definiu a missão do Modelo Cobit em «pesquisar, desenvolver, publicar e promover um modelo de controlo para a governança de tecnologias de informação atualizado e internacionalmente reconhecido para ser adotado por organizações e utilizado no dia-a-dia por gestores de negócios, profissionais de tecnologias de informação e profissionais de avaliação». Como já foi indicado anteriormente a direção das instituições e a gestão das tecnologias de informação necessita que as mesmas sejam direcionadas para o atingir dos objetivos da organização, que possuam resistência para fazer face aos obstáculos que poderão encontrar e que ganhem a flexibilidade necessária para aprender com esses mesmos obstáculos. Devem também conseguir detetar e gerir os riscos e acima de tudo usando toda a informação processada descubram oportunidades de negócio para a entidade. Estas situações não são possíveis sem a implementação de boas práticas nas tecnologias de informação no que diz respeito á área de controlo e gestão. O que são boas práticas para o Modelo Cobit? A crescente complexidade dos mercados, o aumento dos custos com as plataformas informáticas, a necessidade de fazer face aos requisitos de regulação impostos por Basileia II acerca do controlo de qualidade, segurança e proteção dos seus registos informativos, o aumento do risco operacional e consequente probabilidade de acontecimentos negativos para as empresas e a necessidade de comparação de empresas, mais concretamente entre a própria e as suas concorrentes

levaram a que fossem desenvolvidos processos que têm como grande trunfo serem globalmente aceites por todas as empresas e que definem regras e controlos para mitigar todas as situações negativas descritas e que são originárias da atividade normal da instituição. Um dos modelos criados para tal situação foi o Cobit, que tem como principais características:

- Ser focado no negócio;
- Ser orientado a processos;
- Ser baseado em controlos;
- Orientado a medições;

Figura 1 - Princípios básicos do Cobit (ISACA, 2009:12)

4.1.1 Focalização no negócio

A focalização no negócio é a base de todo o modelo Cobit porque visa criar uma interligação entre os objetivos de negócio da empresa e os objetivos presentes no sistema de informação e essa situação passa por uma gestão dos sistemas com os corretos critérios e parâmetros de controlo que cumpram todas as necessidades em termos de qualidade e segurança. Foi definido com base nas necessidades acima indicadas sete critérios que a informação proveniente dos sistemas deve possuir para que a mesma possa ser usada por parte da gestão (ISACA, 2009):

- **Efetividade** – A informação deve ser importante para o processo de negócio e deve ser passível de utilização por parte da gestão da instituição;
- **Eficiência** – Obtenção e entrega da informação com a utilização da menor quantidade de recursos disponíveis;
- **Confidencialidade** – As informações produzidas podem ser bastante importantes para a continuidade da empresa, situação que obriga a que ninguém tenha conhecimento das mesmas além do seu destinatário;
- **Integridade** – Deve ser fiável e na obtenção da mesma deve ser disponibilizado toda a informação acerca dos objetivos propostos;
- **Disponibilidade** – Deve ser passível de ser distribuída quando for solicitada. Sendo pedida para hoje ou no futuro, deve ser sempre passível de obtenção;
- **Conformidade** – Deve estar de acordo com a legislação em vigor a que a empresa se encontra sujeita;
- **Confiabilidade** – Deve ser de confiança para a tomada de decisão por parte do núcleo responsável pela gestão da empresa;

Os critérios de informação indicados formam a base para a elaboração dos objetivos de negócio, visto a informação ser processada e avaliada pelos órgãos de gestão das instituições com o intuito de definir o futuro e como ele irá ser alcançado. Para conseguir elaborar os serviços para apresentar ao seu segmento de mercado, a gestão deve alem de definir os objetivos, definir também os processos a desenvolver, os atos a serem elaborados para que seja concluído o objetivo final. Para uma entidade conseguir desenvolver o seu processo de negócio precisa de usufruir da plenitude dos seus sistemas de informação e aqui é que é necessário definir os objetivos dos mesmos como sendo os que foram definidos para o da empresa em geral. Concluída esta fase de definição de objetivos, quer para o negócio quer para os sistemas de informação, é preciso definir um processo que fique responsável para avaliar e controlar os processos informáticos e se os objetivos estão a ser alcançados pelas plataformas. Para conseguir que os objetivos da empresa sejam atingidos não basta apenas proceder a uma elaboração de objetivos a implementar nos sistemas de informação, é essencial proceder á avaliação dos recursos existentes na empresa e se for concluído que é necessário a existência de mais plataformas informáticas devem ser investidos recursos financeiros no melhoramento desse aspeto para que as necessidades de negócios sejam atingidas sendo com isso concretizados os objetivos finais

da empresa. Os recursos de tecnologias de informação que o Cobit refere são (ISACA, 2009):

- **Aplicativos** – São programas automáticos para a utilização por parte das pessoas responsáveis e são também os programas que processam as informações registadas;
- **Informações** – São dados disponibilizadas pelos sistemas de informações referente a todos os processos elaborados pelos mesmos;
- **Infraestrutura** – Conjunto dos recursos que permitem a existência dos aplicativos, como por exemplo, sistema operativo, *hardware*, redes, servidor, entre outros.
- **Pessoas** – São os responsáveis pela gestão e utilização de todas as plataformas informáticas de uma instituição;

A focalização como a imagem indica é um processo cíclico que vai ajudando a empresa na elaboração do seu sentido de existência, no concretizar do seu objetivo através da utilização de sistemas de informação corretamente programados e controlados.

4.1.2 Orientação para processos

O modelo Cobit facilita a gestão das tecnologias de informação dado implementar um modelo operacional de fácil acesso e visualização para todos os colaboradores da empresa. Este processo permite a qualquer colaborador da empresa, em qualquer área da mesma, facilmente ajudar na verificação do desempenho dos sistemas implementados. Segundo o ISACA (2009:14) o Cobit «fornece uma metodologia para medir e monitorizar a performance das tecnologias de informação, comunicação com prestadores de serviços e integração das melhores práticas de gestão». A adoção do modelo de processos por parte da instituição ajuda na motivação dos seus colaboradores, em especial dos responsáveis pelas várias áreas dos processos, pois permite o distribuir de responsabilidades. As responsabilidades nas tecnologias de informação são geralmente definidas por quatro domínios sendo eles o planeamento, a construção, o processamento e a monitorização. As referências no modelo Cobit assumem outras denominações, sendo elas: Planeamento e Organização, Aquisição e Implementação, Entrega e Suporte e por fim Monitorização e Avaliação. A primeira indicada, **Planeamento e Organização** é responsável pela criação das estratégias e orientações a implementar nos sistemas de informação de maneira a que os próprios contribuam da melhor maneira possível no alcançar dos objetivos de negócio. A **Aquisição e Implementação** vai fazer face às necessidades que surgiram do domínio

anterior. Para conseguir elaborar o que foi definido no planeamento, no que respeita a tecnologias de informação, é necessário verificar os recursos disponíveis na empresa. Em caso de falta dos mesmos devem ser identificados os que são necessários, analisar as ofertas existentes no mercado e adquirir as melhores soluções para a necessidade da organização. Não basta apenas proceder à aquisição pois já foi referida mais de uma vez a importância de uma correta implementação das tecnologias de informação de forma a ser extraído das mesmas as suas maiores potencialidades e assim aumentar a sua contribuição para o alcançar do objetivo da instituição. O processo de **Entrega e Suporte** fica responsável pelo controlo das entregas dos produtos e serviços pedidos relativos aos sistemas de informação, nos quais dizem respeito os prazos de entrega dos serviços, o suporte informático a disponibilizar às pessoas que vão trabalhar com o mesmo em termos de formação ou resolução de problemas que não eram esperados e também o suporte em termos de assistência técnica sempre que um das plataformas sofra qualquer tipo de avaria técnica ou de *hardware*. A **Monitorização e Avaliação** vai proceder à corrente análise e verificação dos sistemas implementados, ao longo do tempo de vida útil dos mesmos, de forma a assegurar que são cumpridos requisitos indicados em Basileia II em termos de segurança de informação, tais como os critérios de qualidade que são necessários respeitar no que reporta às informações provenientes deste tipo de plataformas. Este domínio das tecnologias de informação fica encarregue de avaliar a elaboração geral do trabalho desenvolvido pelos sistemas, se o controlo interno está a funcionar corretamente e também avaliar a gestão em termos gerais de todos os processos informáticos.

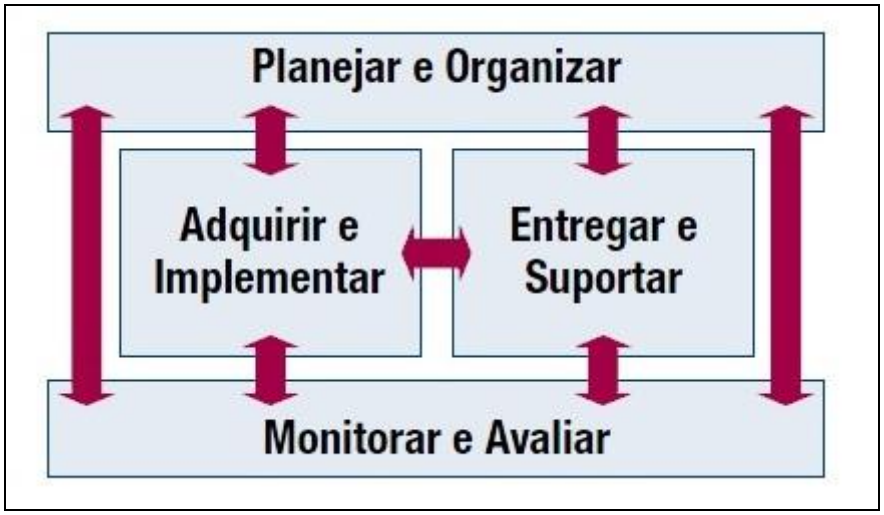

Figura 2- Os quatro domínios do Modelo Cobit (ISACA, 2009:14)

4.1.3 Baseado em controlos

O Cobit disponibiliza uma vasta gama de processos que podem ser, consoante a necessidade, conjugados para fazer face às necessidades da empresa no que respeita à correta utilização das plataformas informáticas. Todas as instituições, ou quase todas, definem as responsabilidades dos seus sistemas de informação de acordo com o geralmente definido como *standard*, através dos 4 domínios gerais, planeamento, construção, processamento e por fim a monitorização, mas dentro destes existe a possibilidade de optar por 34 processos que podem ser adaptados isoladamente, ou mesmo agregados entre eles para fazer face às necessidades da empresa. O modelo Cobit define a necessidade de existência de controlos para todos os processos de forma a aumentar o seu grau de implementação no processo geral da empresa e que se consiga reduzir o risco de falha sendo que os controlos também auxiliam a chefia na verificação da direção correta tomada pelos sistemas de informação na obtenção dos objetivos propostos pela administração das instituições e na prevenção da ocorrência de eventos indesejados. Em caso de deteção dos mesmos, ajuda na elaboração de medidas que permitam mitigar essas mesmas ocorrências. O ISACA (2009:15) define o controlo como «politicas, procedimentos, praticas e estruturas organizacionais criadas para prover uma razoável garantia de que os objetivos de negócio serão atingidos e que eventos indesejáveis serão evitados ou detetados e corrigidos». As instituições para implementar esta ferramenta seguem um processo cíclico, ou seja, devem escolher o processo ou processos que melhor correspondam as necessidades dos sistemas de informação, devem proceder a sua implementação e quando se encontrarem implementadas e a funcionar o foco da empresa deve ser na mitigação dos riscos que podem ocorrer por terem sido colocados processos de parte que poderiam ter sido aplicados pela empresa. O modo como o Cobit foi elaborado em termos de implementação dos processos é uma grande ajuda para a instituição, visto o método utilizar uma base geral com todos os processos geralmente detetados nas tecnologias de informação e é de fácil compreensão e utilização por parte dos colaboradores responsáveis pela gestão das operações nos vários departamentos. Para que a empresa consiga usufruir de todas as capacidades das tecnologias é necessário os gestores implementarem controlos nesses mesmos processos para assegurar que o caminho que se pretende percorrer está corretamente planeado e a ser seguido. O modelo Cobit possui também, para cada processo anteriormente delineado, controlos que vão auxiliar a gestão operacional a desempenhar a sua função. Segundo o ISACA (2009:16) os controlos são definidos através dos domínios

que existem ou seja, cada domínio, dos quatro apresentados, possuem controlos especificamente desenhados para os objetivos dos mesmos mas o Cobit possui ainda controlos gerais de processos que têm que ser tidos em conta, são eles:

- **PC1 Metas e Objetivos do Processo** – Define e comunica as metas e objetivos específicos, mensuráveis, acionáveis, realísticos, orientados a resultados e no tempo apropriado para a efetiva execução de cada processo de TI. Assegura que eles estão ligados aos objetivos de negócio e que são suportados por métricas apropriadas;
- **PC2 Propriedade dos Processos** - Designa um proprietário para cada processo de TI e claramente define os papéis e responsabilidades de cada proprietário de processo. Inclui, por exemplo, a responsabilidade pela elaboração do processo, interação com outros processos, responsabilidade pelos resultados finais, medidas de performance do processo e a identificação de oportunidades de melhorias;
- **PC 3 Repetibilidade dos Processos** – Elabora e estabelece cada processo-chave dos TI de maneira a que possa ser repetido e produzir de maneira consistente os resultados esperados. Fornece uma sequência logica mas flexível das atividades que levarão ao resultado desejado, senão ágil o suficiente para lidar com exceções e emergências. Usa processos consistentes, quando possível, e processos personalizados quando é inevitável;
- **PC 4 Papeis e Responsabilidades** – Define as atividades-chave e as entregas do processo. Designa e comunica os papéis e responsabilidades para uma efetiva e eficiente execução das atividades e a sua documentação bem como a responsabilização pelo processo e as suas entregas;
- **PC 5 Politicas Planos e Procedimentos** – Define e comunica com todas as politicas, planos e procedimentos que direcionam os processos de tecnologias de informação que são documentados, revistos, mantidos, aprovados, armazenados, comunicados e utilizados para treinar. Designa responsabilidades para cada uma dessas atividades e em momentos apropriados verifica se elas são executadas corretamente. Assegura que as políticas, planos e procedimentos sejam acessíveis, corretos, entendidos e atualizados;
- **PC 6 Melhoria do Processo de Performance –** Identifica um conjunto de métricas que fornecem diretrizes para os resultados e performance dos processos. Estabelece metas que refletem nos objetivos dos processos os indicadores de performance que permitem atingir os objetivos dos processos. Definem como os dados são obtidos. Compara as métricas reais com as metas e toma medidas

quanto aos desvios quando necessário. Alinha métricas, metas e métodos com o enfoque de monitorização de performance geral de TI.

Estes são os controlos básicos que o Cobit indica serem obrigatoriamente implementados num ambiente em que os sistemas de informação se encontram a funcionar visto reduzirem o aparecimento de situações não programadas e o risco, e aumentarem a eficácia e eficiência dos recursos disponibilizados como a qualidade do produto ou serviço final. Os processos definidos pelo Cobit não são de utilização já pré-definida, ou seja, são dadas instruções que posteriormente serão adaptadas da melhor forma por parte dos responsáveis pelas áreas em que vai ser utilizado tal modelo. Para uma correta gestão de todo o sistema informático da empresa, o Cobit possui uma ferramenta chamada **RACI** que vai definir três aspetos bastante importantes para o funcionamento desses mesmos processos e dos controlos que a eles diz respeito. Os três aspetos indicados são o de Responsabilizado, de Consultado e o de Informado, sendo que o primeiro diz respeito á atribuição de responsabilidade ao colaborador encarregue de orientar e indicar as atividades a serem desenvolvidas, ou seja, responsabiliza um colaborador, muitas vezes o chefe da secção operacional em questão, pela execução de determinada atividade, enquanto os outros dois termos dizem respeito á utilização e consequente informação de que todos os ativos que necessitem ser usados serão usados no âmbito de suporte da atividade que precisa de ser elaborada. Os controlos apresentados anteriormente são definidos e programados segundo os termos da gestão administrativa da instituição. São considerados controlos gerais das tecnologias de informação sendo que também existem controlos que são elaborados pelos colaboradores das áreas específicas, chegando então a conclusão que os controlos implementados numa instituição se dividem em dois tipos, **controlos gerais dos sistemas de informação** e os **controlos de aplicativos**. Os primeiros são mais direcionados para a resposta a mudanças que aconteçam no negócio ou na empresa, para a evolução de sistemas de informação e para a segurança global de toda a empresa. Os segundos são controlos que se encontram anexados aos processos e que ajudam na sua aplicação, responsáveis pelo controlo da veracidade das informações, validade, totalidade e autorizações que são precisas para o desenrolar de uma atividade. Os controlos de aplicativos podem ser automatizados ou então manuais. O Cobit defende que o desenvolvimento de tais controlos de aplicativos deve ser inserido na responsabilidade do domínio de Aquisição e Implementação e definido juntamente com os restantes controlos e

processos pela parte administrativa da instituição, mas a gestão dos mesmos controlos e a responsabilidade pelo seu correto funcionamento não são do âmbito da gestão de sistemas de informação, mas sim da pessoa definida aquando da elaboração do RACI, ou seja, aquando da delegação de responsabilidade a um colaborador especifico responsável pelo executar de tal controlo. Como sucedeu com os processos, o Cobit (ISACA, 2009) possui também um conjunto recomendado de objetivos de controlo de aplicativos, sendo eles:

- **AC1 Preparação e Autorização de Dados Originais** – Assegura que os documentos fonte sejam preparados por pessoal autorizado e qualificado seguindo os procedimentos estabelecidos, levando em consideração uma adequada segregação de funções relacionadas com a criação e aprovação desses documentos. Erros e omissões podem ser minimizados através do bom desenho de formulário para entrada de informação, permitindo que erros e irregularidades detetados sejam reportados e corrigidos;
- **AC2 Entrada e Coleta de Dados Fontes** – Estabelece que a entrada de dados seja executada de maneira apropriada por pessoal autorizado e qualificado. A correção e o reenvio de dados que foram erroneamente inseridos devem ser executados sem comprometer o nível de autorização da transação original. Quando apropriado para a reconstrução, os documentos originais devem ser guardados por um período adequado;
- **AC3 Testes de Veracidade, Totalidade e Autenticidade** – Assegura que as transações sejam exatas, completas e válidas. Valida os dados que foram inseridos e editados ou enviados de volta para correção o mais próximo possível do ponto onde foram originados;
- **AC4 Processamento Íntegro e Válido** – Mantem a integridade e validade dos dados no ciclo de processamento. A deteção de transações erróneas não interrompe o processamento de transações válidas;
- **AC5 Revisão das Saídas, Reconciliação e Manuseio de Erros** – Estabelece procedimentos e responsabilidades associadas para assegurar que as saídas sejam manuseadas de uma forma autorizada, entregues aos destinatários corretos e protegidas durante a transmissão. Garante que ocorre a verificação, deteção e correção da exatidão das saídas e que a informação provida pela mesma é usada;
- **AC 6 Autenticação e Integridade das Transações –** Antes de transportar os dados das transações entre os aplicativos e as funções de negócios/operacionais (internas ou externas à organização), verifica endereçamento adequado, autenticidade da

origem e integridade do conteúdo. Mantém a autenticidade e integridade durante a transmissão ou transporte.

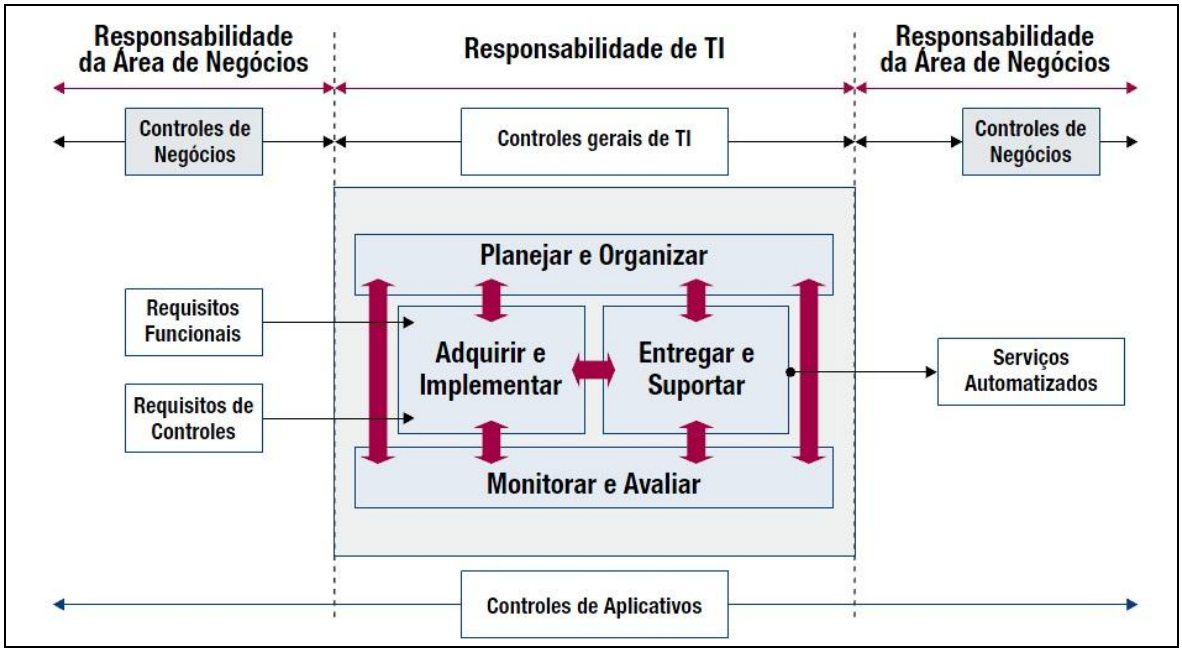

Figura 3 - Controlos gerais e de aplicativos do Modelo Cobit (ISACA, 2009:18)

4.1.4 Orientado a Medições

Uma empresa sente a necessidade de avaliar e verificar o estado dos seus sistemas de informação e analisar, em sintonia com os objetivos a alcançar, qual a melhor gestão e controlo sobre as plataformas que necessita implementar. Este tipo de análise ao potencial operacional da instituição não é de fácil elaboração. É preciso analisar os recursos informáticos disponíveis na empresa e verificar onde é necessário elaborar um melhoramento dos mesmos e assim definir como vão ser instalados tais acréscimos de forma a obter o máximo proveito de toda a capacidade das plataformas adquiridas. O Cobit ajuda nesses aspetos com os seguintes processos (ISACA, 2009):

- Modelos de maturidade que permitem fazer comparações e identificar os necessários aprimoramentos de capacidades;
- Objetivos de performance e métricas para os processos de TI, demonstrando como os processos atingem os objetivos de negócio e das TI;
- Objetivo de atividades para habilitar o efetivo desempenho do processo;

As administrações, dado o aumento da importância na elaboração dos planos e objetivos anuais das empresas por parte dos sistemas de informação, são cada vez mais chamadas a verificar a correta parametrização dos mesmos. Os gestores das instituições possuem vários prismas a analisar aquando da elaboração dos objetivos e como os poderão alcançar. A preocupação com a concorrência direta, o melhorar dos métodos operacionais para elaborar os produtos de maneira mais eficiente e eficaz, como extrair a máxima capacidade dos seus sistemas de informação, processos a adotar e os melhores controlos a implementar. Embora seja de difícil elaboração esta análise global, os processos das TI vão desempenhar um importante serviço de maximização operacional, e para isso, a gestão dos sistemas de informação precisa de efetuar diversas avaliações. O objetivo das avaliações é o de detetar possíveis situações passíveis de melhoramento para permitir à empresa maximizar a sua capacidade de produção usando o mínimo de recurso possíveis. Esta avaliação de processos é elaborada pelo responsável pelos processos implementados em cada área operacional, sendo que devem ser atendidas três necessidades (ISACA,2009):

1. Medidas relativas ao estado em que a empresa se encontra;
2. Maneira de eficientemente decidir para onde a empresa pretende ir;
3. Ferramenta para avaliação do progresso em relação às metas;

Um método para proceder a verificação e avaliação da empresa é a utilização do modelo de maturidade para a gestão dos sistemas de informação. Este modelo é composto por uma escala que vai avaliar a maturidade do desenvolvimento dos TI, sendo que vai do grau zero, que é apelidado de inexistente, ao grau cinco, que diz respeito a um sistema de informação otimizado. A escala é derivada da original que foi elaborada pelo *Software Engineering Institute* (SEI) como método para avaliar a maturidade relativa á elaboração de software, mas que no Cobit funciona de maneira ligeiramente diferente. Os graus de maturidade no modelo Cobit funcionam como uma espécie de análise ao processo das tecnologias de informação, que após a respetiva verificação irá indicar onde se deve focar a gestão com mais atenção, de forma a potenciar as prioridades anteriormente detetadas. Os 34 processos de TI, que o Cobit tem, possuem os seus próprios modelos de maturidade que podem auxiliar à gestão desses mesmos processos. Podem ajudar a descortinar o atual estado da performance operacional da instituição, ajudar na verificação da exata quota de mercado detida pela empresa no mercado alvo, na avaliação e indicação dos locais onde a

instituição se poderia focar no sentido de maximizar os processos por ela própria escolhidos e mais importante ainda, processa as informações sobre as alterações a elaborar para que a instituição evolua o máximo possível. O modelo Cobit tem como uma das suas principais vantagens a inclusão de toda a empresa na ajuda ao controlo dos sistemas de informação e consegue este processo através da fácil comunicação e explicação dos métodos que utiliza, situação também usada com o método de maturidade dos processos através da elaboração de um gráfico que tem por base os graus definidos anteriormente. Os graus encontram-se distribuídos entre zero e cinco, sendo que cada um diz respeito ao seguinte (ISACA,2009):

0. **Inexistente** – Inexistência de um processo, sendo que para a própria empresa não existe nenhuma situação a ser elaborada;
1. **Inicial / *Ad Hoc*** – Existem evidências que a empresa reconheceu situações anómalas e que precisam de ser trabalhadas. No entanto, não existe um processo padronizado de ação, os problemas são resolvidos caso-a-caso;
2. **Repetível, porém intuitivo** – Os processos evoluíram para um estágio onde procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe uma formação ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixada com o individuo. Há um alto grau de confiança no conhecimento do individuo e consequentemente podem acontecer erros;
3. **Processo definido** – Procedimentos foram padronizados, documentados e comunicados através de formação específica. É obrigatório que estes processos sejam seguidos; no entanto, é possíveis existir falha nas deteções de desvios. Os procedimentos não são sofisticados mas existe formalização das práticas existentes;
4. **Gerenciado e Mensurável** – A gestão monitoriza e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar a funcionar corretamente. Os processos estão debaixo de uma constante melhoria e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada;
5. **Otimizado** – Os processos foram refinados a um nível de boas práticas, baseado no resultado de uma contínua melhoria e maturidade. As tecnologias de informação são utilizadas como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rápida nas adaptações.

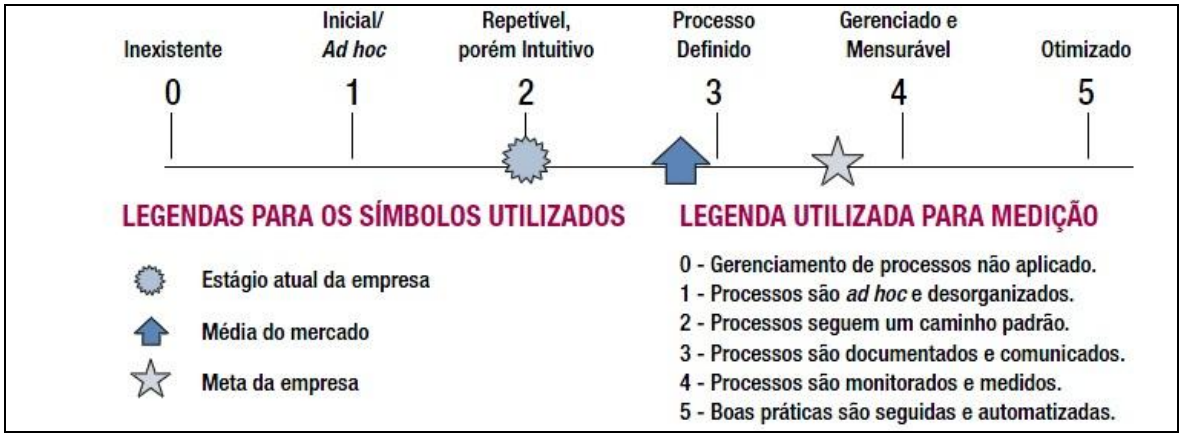

Figura 4 - Representação gráfica dos modelos de maturidade (ISACA,2009:20)

O modelo de maturidade é uma ferramenta bastante importante para as instituições pois irá permitir que os colaboradores que trabalham diretamente com os processos expliquem aos gestores administrativos onde existem as falhas no sistema de informação da empresa, mais concretamente nos processos e que sejam trabalhadas soluções para corrigir tais erros de forma que os objetivos propostos sejam atingidos.

Em jeito de conclusão, os modelos de maturidade disponibilizam à empresa um template geral que as instituições podem usar para desenvolver uma correta gestão e controlo dos seus sistemas de informação. O template é composto por vários pressupostos: (ISACA,2009):

- Um conjunto de requisitos e aspetos que habilitam os diferentes níveis de maturidade;
- Uma escala onde a diferença pode ser facilmente medida;
- Uma escala que pode ser utilizada para comparações pragmáticas;
- Uma base para definir as posições de partida e de como pretende ficar no futuro;
- Suporte para a análise de deficiências a fim de determinar o que precisa ser feito para atingir o nível escolhido;
- Considerada no conjunto, uma visão de como a área de TI é gerida na organização.

4.2 ISO 27001

A ISO 27001 é uma norma que surgiu através da atualização e melhoramento de outras duas normas, a BS779 e a BS779-2, e tem como principal objetivo servir de referência global em matéria de gestão da segurança de informação elaborada por empresas. A norma

foi desenvolvida pela *International Organization for Standardization* (ISO), organização que possui a sua sede na Suíça e que é a responsável mundial pela criação de normalizações referentes a diversos assuntos de variadas áreas. A norma tem vindo a sofrer alterações significativas desde a data de 1995, ainda sobre a denominação de *British Standard* 7799, que foi a primeira norma prática utilizada para a gestão da segurança. É usada a denominação de *British Standard* visto ser no Reino Unido, e muito graças à revolução industrial, que foram e são elaborados os códigos e normas com as melhores praticas a desenvolver. Um grupo constituído pelo ISO e pelo *International Eletrotechnical Comission* (IEC) ficou responsável pela elaboração das revisões necessárias efetuar com base no estudo das varias impressões conseguidas nas visitas elaboradas a diversos países, onde foram avaliados as práticas de segurança, com a junção de várias ideias que os membros do grupo iam conseguindo obter, tudo no sentido de efetuar um upgrade da norma em si. A primeira versão da norma, já com a denominação atual, foi tornada publica no ano de 2005, mais concretamente no primeiro semestre. A norma tem como objetivo a recetividade por parte das instituições de um conjunto de regras juntamente com a aceitação de processos e controlos desenvolvidos com o intuito de combaterem e gerirem os riscos que a empresa incorre relativos à sua informação. «A norma foi preparada para prover um modelo para estabelecer, implementar, operar, monitorizar, analisar criticamente, manter e melhorar um sistema de gestão de segurança de informação (SGSI)» (ISO,2005). A organização precisa para o seu correto funcionamento de gerir corretamente todas as suas atividades, e para isso necessita de transformar os seus recursos de entrada da melhor maneira de forma a desenvolver as saídas com a máxima eficiência. Este processo deve ser delineado pela gestão da instituição com todo o cuidado e deve ser controlado de forma que todo o plano seja cumprido. Para elaborar um processo de controlo que consiga gerir corretamente o sistema de informação de uma instituição, a ISO 27001 aconselha que os seus colaboradores dediquem uma atenção específica em alguns pontos, sendo eles:

- Desenvolvimento de uma identidade em relação às necessidades de segurança da informação da instituição e da elaboração de objetivos específicos para o sistema de informação;
- Elaboração e operacionalização de controlos de apoio à gestão dos sistemas de informação em termos de segurança com o intuito de controlar o cumprimento dos objetivos e o risco decorrente do negócio;
- Verificação e avaliação do trabalho desenvolvido pelo SGSI da organização;

- Proceder a um desenvolvimento, em termos de capacidades e regras do SGSI, de forma que o mesmo se mantenha atualizado com o passar dos tempos;

O modelo utilizado para um melhor controlo e elaboração do SGSI por parte da norma é o modelo apelidado de "*Plan-Do-Check-Act*" (PDCA), que é definido da seguinte maneira:

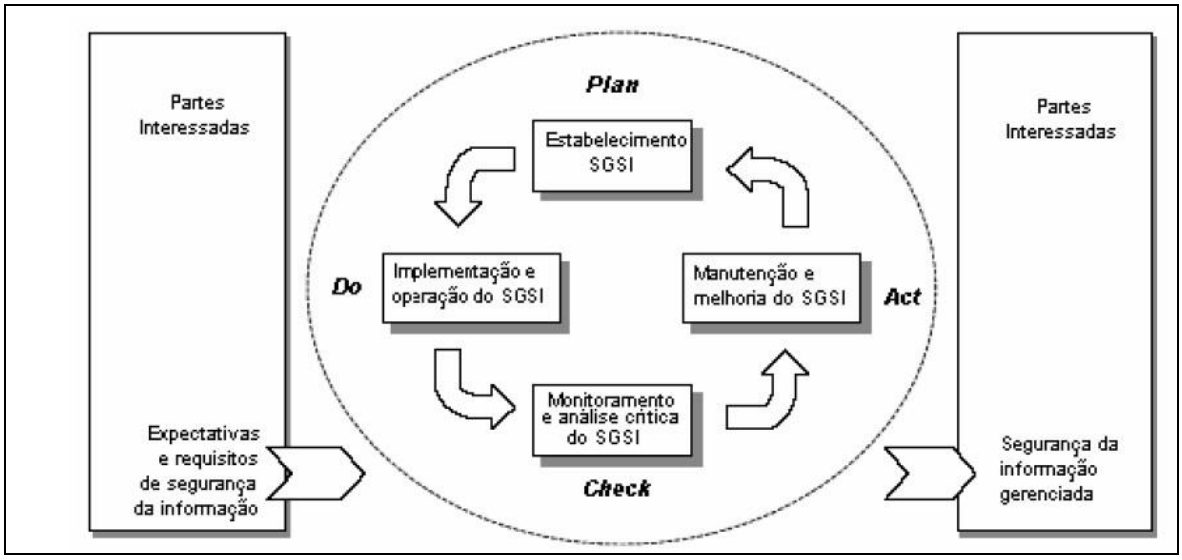

Figura 5 - Modelo PDCA (ISO, 2005:6)

***Plan* (Planear)** **(Estabelecer o SGSI)**	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as politicas e objetivos globais de uma organização.
***Do* (Fazer)** **(Implementar e Operar o SGSI)**	Implementar e operar a política, controlos, processos e procedimentos do SGSI.
***Check* (Verificar)** **(Monitorizar e analisar criticamente o SGSI)**	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiencia prática do SGSI e apresentar os resultados para a análise crítica pela direção.
***Act* (Agir) (Manter e melhorar o SGSI)**	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Tabela 1 - Modelo PDCA (ISO, 2005:6)

Os pressupostos indicados pela ISO 27001 são elaborados tendo em conta uma visão global. Não são critérios específicos e foram criados para que fosse possível a sua adaptação a qualquer tipo de instituição, sendo irrelevante as áreas onde atua ou mesmo a sua dimensão. A norma é composta por cinco componentes, que são:

- Sistema de gestão de segurança da informação;
- Responsabilidade da direção;
- Auditorias Internas do SGSI;
- Análise crítica do SGSI pela direção;
- Melhoria do SGSI;

Estas componentes são a base sobre a qual a organização deve implementar o seu sistema de segurança, utilizando as características que ambas possuem da forma mais conveniente, mas a exclusão ou a não implementação de uma ou mais indicações presentes em um dos

cinco componentes não valia o uso da ISO 27001 por parte da empresa, porque exclusões apenas são aceites quando existe a possibilidade de a empresa segurar corretamente a sua informação e que, mesmo sem utilizar algum dos pontos da norma, consiga cumprir todos os requisitos legais assumidos como base em termos de segurança. No primeiro componente apelidado de **Sistema de gestão de segurança de informação** a empresa necessita de elaborar e definir as bases sobre as quais irá ser criado o SGSI, e para que tal aconteça deve ser analisado e avaliado várias variantes que fazem parte do habitat da mesma. O negócio onde ela se movimenta, o seu enquadramento geográfico, os recursos disponíveis e mais importante, a tecnologias de informação que possui são tudo bases para a criação do SGSI. A constituição de um grupo que defina os objetivos a alcançar por parte da empresa é essencial, e que consequentemente crie um caminho a seguir usando as bases legais em que a empresa opera, os critérios de segurança ao qual a empresa pertence, os métodos de negócio desenvolvidos para fazer face ao risco operacional, e alem do mais, os pressupostos utilizados pela gestão sobre que acontecimentos podem derivar em riscos para a instituição. O risco é um dos principais problemas para um instituição e o alvo a combater para o SGSI, dado ser a principal arma que existe ao serviço da instituição para a sua mitigação, combate e controlo. No que respeito ao mercado que este trabalho se encontra inserido, o mercado financeiro, as instituições estão sobre um enorme risco operacional, podendo mesmo extrapolar esta situação para o mercado que sofre mais pressão do risco operacional, dado ser uma das principais variáveis aquando da elaboração de investimentos financeiros. É verdade que quanto maior o risco, maior o lucro mas acresce também a probabilidade de perda, e isso é uma das situações a evitar por parte das empresas deste sector. Numa área que depende da confiança, como a área financeira, a elaboração de controlos para combater o risco são as melhores ferramentas que uma instituição bancária pode usufruir, desde que usadas corretamente. São bastantes os riscos que uma instituição financeira pode sofrer, **variações das taxas de juro**, que pode diminuir os lucros das empresas fazendo com que o seu resultado seja menor, ou mesmo negativo se a quantidade de passivos for superior ao lucro, risco de mercado, **o risco de crédito** que é noticia na atualidade visto as famílias não possuírem capacidade de fazer face aos créditos por elas criados, fazendo com que as instituições bancárias não recebem a contrapartida de terem emprestado capital, o **risco de câmbio** que pode transformar um empréstimo em outra moeda num determinado montante durante um determinado tempo num valor bastante menor no prazo de maturidade por a taxa de cambio ter diminuído. São

apenas algumas situações que provam que o SGSI deve possuir na sua programação vários tipos de informação de como funciona o mercado, as diferentes taxas de câmbio de diferentes áreas do globo, assim como muitas das situações que podem culminar em riscos para a instituição. Para ser possível responder a tais riscos, a instituição deve implementar algumas ferramentas para permitir ao SGSI analisar o negócio, verificar as variáveis e emitir um parecer sobre se a situação vai acarretar uma tomada de riscos por parte da empresa. No início, o SGSI deve ser pensado com base na maneira de funcionar da organização, deve conseguir analisar todos os processos de elaboração de saídas da entidade e com essa análise e com a ajuda dos controlos nele implementado indicar se o risco operacional é elevado ou se é passível de ser suportado na totalidade. O SGSI deverá ser capaz de detetar os riscos corretamente, se representam alguma ameaça à empresa, se irão colocar a entidade numa exposição demasiado perigosa e deverá concluir se o prejuízo proveniente desses mesmos riscos poderá culminar com o encerramento da instituição. A simples identificação do perigo não é suficiente, é preciso proceder a uma correta avaliação do problema em si. Primeiro deve ser verificado se o risco é suportável, se a falha que ocorrer proveniente da fuga de informação ou da informação incorreta é viável mesmo acarretando alguns prejuízos, e se não coloca em causa a continuidade de empresa. Passado a primeira indicação, é necessário calcular a possibilidade real de tal risco acontecer e os danos que poderá causar. Avaliar se as falhas de segurança que possam acontecer levarão a que os ativos da empresa não sejam suficientes para fazer face ao problema, e quando as variáveis se encontrarem totalmente avaliadas e a verificação concluir tudo o que poderá ser imputado à empresa, caso o risco se torne real, devem ser avaliadas as proteções que existem no SGSI para mitigar o problema, ou seja, para o correto planeamento de um sistema é necessário que o sistema detete todos os riscos e a sua probabilidade de ocorrer para posteriormente implementar os controlos que o mitiguem o máximo possível. A grande maioria das empresas usa um tipo de gestão de risco bastante comum: a transferência do mesmo para seguradoras. Esta situação no mercado em que se encontra o âmbito do trabalho é impossível, dado as seguradoras serem uma parte integrante do mercado financeiro. Então como podem elas gerir o risco? A pergunta tem resposta quando pensamos no SGSI, tudo no mercado financeiro se resume a confiança, avaliação, controlo e informação e não existe melhor maneira de uma instituição financeira conseguir obter um correto controlo dos seus riscos se não por um correto e bem implementado sistema de controlo de segurança de informação. O SGSI para funcionar corretamente deve ser

implementado com especial atenção aos controlos que a instituição financeira mais precisa, com o intuito de mitigar riscos específicos relativos ao tipo de negócio que a mesma elabora. Um banco não precisa de ter os mesmos controlos específicos que uma seguradora pois os seus outputs são de diferentes naturezas. A organização deve ter sempre em atenção e desenvolver um método de funcionamento que defina corretamente que tipo de ação deve o SGSI desenvolver para combater um determinado tipo de risco à segurança da informação e programar o sistema de maneira a que os controlos sejam capazes de analisar, verificar e atuar rapidamente em situações que o risco de falha de segurança seja bastante real. Para o correto funcionamento do SGSI é necessário que a instituição proceda a um acompanhamento e a uma verificação constante no sentido de detetar possíveis erros na elaboração de todo o processo. Detetar se existiram tentativas de invasão no sistema de segurança e essas mesmas foram bem-sucedidas ou corretamente debeladas. Um dado a ter em conta por parte da instituição é que não pode deixar de analisar todo o processo em termos de eficácia no combate às ameaças pois com o passar do tempo e sem uma adequada manutenção, o SGSI torna-se obsoleto e a proteção por ele desenvolvida perderá o seu valor total. Com o avanço dos sistemas de informação, com o desenvolvimento e crescimento da internet juntamente com o estilo de vida da sociedade atual, as instituições financeiras começaram a desenvolver plataformas que necessitam de uma segurança bastante apurada em termos de defesa de informações confidenciais e para que tal seja possível é necessário manter uma melhoria contínua dos seus processos, controlos e programação no combate e prevenção de riscos. De forma a facilitar o controlo por parte da empresa e especificamente auxiliar o papel das auditorias aos sistemas, a norma defende que seja criado um *dossier* documental referente a todas as ações tomadas pelo SGSI, desde o seu desenvolvimento e implementação, passando pela formalização dos objetivos da empresa e as direções operacionais a seguir, os processos e controlos implementados no sistema, os relatórios provenientes das análises elaboradas periodicamente com o intuito de verificar riscos. Todos os passos devem ser registados e guardados, sendo que deve ser prestada especial atenção aos documentos antigos que já se encontram desatualizados e aos documentos provenientes de fontes externas à empresa. A norma aponta também princípios que precisam de ser seguidos de modo a permitir à empresa corresponder a todas as características da ISO 27001. As direções das instituições financeiras são um dos cinco componentes mais importantes, visto serem elas que definem e planeiam tudo o que tiver diretamente relacionado com o sistema. Para satisfazer os requisitos da ISO ela deve

guardar o registo da sua intervenção nos vários passos do SGSI, como a elaboração, definição de processos e controlos, implementação, validação e avaliação com a consequente melhoria das capacidades de análise e controlo. É importante também que a gestão consiga delinear e disponibilizar os recursos necessários para a correta elaboração de todo o sistema, quer em termos legais com a implementação das normas em vigor no seu sector de mercado, quer em termos de definição de controlos de risco assentes na sua aceção do que é um risco para a empresa e muito importante a disponibilização de colaboradores corretamente formados e com competências para a elaboração de todo o tipo de trabalhos que envolvam o SGSI, como forma de analisar se o processo decorre como inicialmente planeado e se as ações são corretamente efetuadas. Sobre a alçada da direção existem outros dois componentes que se conjugam entre si e que proporcionam a elaboração de um sistema de segurança mais robusto e com melhores resultados. Deve ser elaborado uma análise bastante minuciosa e acima de tudo critica para que sejam detetados possíveis falhas em todo o processo e consoante os problemas encontrados elaborar um relatório sobre os aspetos a melhorar e alterar. Com base neste relatório vai ser elaborada uma melhoria global do sistema, quer no uso de diferentes controlos de risco, quer pela implementação de processos de correção de segurança ou outro tipo de ação para mitigar as falhas anteriormente reconhecidas. A melhoria deve ser contínua de forma a criar um SGSI á prova do maior número de riscos existentes no ambiente onde a empresa se localiza para que o futuro ocorra sem sobressaltos. O último componente que é vital também para o correto funcionamento da plataforma é mais vocacionado para o âmbito da validação do correto funcionamento dos processos, controlos e do trabalho desenvolvido no sentido de cumprir com os objetivos anteriormente definidos. A empresa necessita de proceder periodicamente a auditorias internas que permitam validar a utilização de todas as variáveis que compõem o sistema, quer em termos legais, normativos, legislativos, de controlo, de segurança e descortinar se o todo criado pela junção das várias partes processuais vai em sentido do cumprimento de todos os pontos definidos como os melhores para a instituição.

4.3 ITIL

O ITIL é uma *framework*, pública, que indica as melhores ferramentas e ações no que aos serviços de tecnologias de informação diz respeito. É composto por um conjunto de processos que prestam especial atenção á melhoria contínua dos sistemas, quer em termos

de processos quer em termos de qualidade do resultado final dos serviços provenientes dos mesmos. As instituições que adotaram o ITIL podem beneficiar de varias vantagens, como por exemplo a satisfação com o correto funcionamento dos sistemas de informação quer por parte dos clientes quer por parte dos colaboradores, vantagens em termos de lucros e benefícios que a empresa alcançara por possuir uma plataforma informática corretamente implementada e da qual consegue extrair todas as suas potencialidades, a vantagem de conseguir uma poupança em termos de recursos, quer em horas de trabalho gastas quer em termos de consumo de materiais, levando a que os processos sejam desenvolvido com a máxima eficiência e eficácia. As organizações vão poder também criar mais serviços em menor espaço de tempo e com qualidade melhorada dado o controlo dos riscos conseguido com a utilização do ITIL. O ITIL foi criado no Reino Unido a pedido do governo Britânico, mais concretamente pela mão da *Central Computing and Telecommunication Agency* (CCTA), que no ano de 1989 publicou um conjunto de livros que continham na altura as melhores práticas no que às tecnologias de informação diz respeito elaborada em conjunto com alguns especialistas da época. A situação foi modificada aquando da saída da versão dois, onde as práticas foram revistas e foram criados processos que se complementavam. A interligação era maior e foram editados sete livros com essas indicações. Uma das mais fortes vantagens para a atualização e consequente aceitação do ITIL, por parte das empresas, foi o seu método de elaboração ser desenvolvido com base nas opiniões emitidas pelos responsáveis pelas tecnologias de informação de empresas de todo o mundo no fórum da *IT Service Management Fórum* (ITSMF). Os responsáveis expõem os seus problemas com os sistemas de informação das suas empresas, as suas opiniões acerca de possíveis soluções, as praticas que mais utilizam na sua instituição, possíveis melhorias a desenvolver nos processos já existentes, tudo matéria-prima para o constante melhoramento da plataforma em si e uma solução para garantir o foco na solução dos problemas que existem especificamente nas organizações. A segunda versão do ITIL foi a que alcançou a aceitação mundial. Várias empresas começaram a adaptar o modelo recomendado nos livros publicados e o ponto máximo desta situação chegou no ano de 2000, quando a Microsoft, empresa líder e pioneira no desenvolvimento de ferramentas e sistemas de informação, usou as bases criadas pelo ITIL para desenvolver o *Microsoft Operations Framework* (MOF), uma base que contem as boas práticas e recomendações no que diz respeito a negócios, metodologias de mercado e gestão de sistemas de informação. No ano de 2007 foi lançada a terceira versão do ITIL que segregou ainda mais a ligação

entre as várias práticas, e que culminou com o lançamento de cinco livros que definem as cinco novas bases da correta gestão das plataformas de informação. O modelo definido nesta terceira versão é apelidado de **ciclo de vida**, e ganhou este nome em função aos períodos de vida que acompanham os serviços elaborados pela componente informática das instituições. Antes de mais, convém referenciar uma alteração implementada pelo ITIL relativo ao que o sistema de informação cria, geralmente o que as comuns plataformas definem como produto, no ITIL essa definição foi alterada. O produto é algo físico, com existência sólida, tangível, que pode ser colocado em *stock* e valorizado consoante a vontade do seu proprietário, mas para isso agora foi alterado, o que é criado pelas tecnologias de informação é sim um serviço, dado que o mesmo só existe quando é disponibilizado ao seu requisitante, não possui forma física, é intangível. Outra das modificações efetuadas foi a diferenciação entre os termos cliente e utilizador. O **cliente** é indicado como o responsável pela definição do serviço em si, quem controla e adquire o serviço e quem suporta todo o tipo de custos do mesmo, sendo que o **utilizador** é quem usufrui do serviço em si, é o consumidor final. O objetivo principal e o foco geral do ITIL é a gestão de toda a plataforma informática da instituição, desde a correta implementação do mesmo até ao fornecimento dos serviços saídos do sistema, tudo com o intuito de permitir desenvolver um serviço com a máxima qualidade e rigor, mas ao mesmo tempo permitir uma redução de custos dos seus clientes com os recursos informáticos da instituição. O novo e melhorado ITIL assenta a sua base no modelo de ciclo de vida, que é composto por três conceitos que ajudam a explicar como é elaborado a gestão dos serviços de tecnologias de informação (ITSMF, 2007):

Figura 6 - Modelo do Ciclo de vida (ITSMF, 2007)

- **Gestão de serviços** – É um conjunto especializado de capacidades organizacionais para proporcionar valor aos clientes na forma de serviços;

- **Serviço** – É um meio de entregar valor aos clientes, facilitando o alcance dos resultados que são pretendidos sem a existência de custos ou perdas especificas. Mais-valias são possíveis de alcançar por intermédio de processos mas estes são limitados por um conjunto de restrições. Os serviços aumentam o desempenho da performance e reduzem a inibição efetuada pelas restrições, melhorando assim a performance geral, possibilitando o cumprimento dos objetivos propostos.

- **Valor** – O valor é o núcleo do conceito de serviço. A partir do ponto de vista do cliente ele é composto por dois componentes, a utilidade e a garantia, utilidade provém do que o cliente recebe e que serve para suprir uma necessidade, a garantia é a promessa de que o serviço funciona como o cliente deseja.

O método do ciclo de vida de um serviço é o ponto de partida para a implementação da gestão dos sistemas de informação, visto este tipo de modelo permitir que seja corretamente verificado o modo como a gestão das TI está estruturada, o modo como os processos se interligam e interagem entre si, o impacto que uma alteração em determinado componente irá desencadear nos restantes, ou seja, permite uma visão abrangente e completa de todas as partes mais importantes da plataforma informática.

O modelo do ciclo de vida é composto por cinco fases que se encontram interligadas entre si, são elas (ITSMF, 2007):

1. Estratégia de serviço
2. Desenho de serviço
3. Transição de serviço
4. Operação de serviço
5. Melhoria de serviço continuada

Dentro destas cinco fases, a mais importante e que vai influenciar o futuro das outras quatro é a fase da estratégia de serviço, visto ser a fase onde grande parte, senão a totalidade, das decisões vão ser tomadas, são definidos os objetivos a alcançar pela instituição e o modo como eles irão ser alcançados. As três fases seguintes, desenho de serviços, transição de serviços e operação de serviços vão desenvolver as suas competências mas sempre debaixo das indicações provenientes da fase principal, visto ter sido nessa fase que todo o caminho a trilhar pela empresa foi definido. A fase de melhoria de serviço continuada é uma fase independente das outras quatro e que serve para analisar os processos utilizados nas outras quatro fases, verificar o seu funcionamento e os resultados elaborados pelos mesmos e proceder ao desenvolvimento de medidas que visem melhorar os pontos fracos do processo da empresa, de forma a proceder a um aumento da qualidade geral da instituição. E como pode a fase de desenvolvimento de estratégias planear e controlar o que se irá passar nas restantes fases? Pois bem, esta fase é composta por um conjunto de processos e atividades que são de importância crítica na definição e implementação de uma estratégia correta para o cumprimento das metas definidas, sendo eles (ITSMF, 2007):

- **Gestão Financeira** – Uma componente integrante da gestão de serviços. Antecipa a informação da gestão essencial em termos financeiros, o que é necessário para que a prestação de serviços seja eficiente e de baixo custo;
- **Gestão da procura** – A gestão dos serviços deve prestar a devida atenção se a procura e a oferta estão corretamente balanceados. O objetivo da gestão da procura é de prever, com a maior precisão possível a compra de produtos, e sempre que foi possível, equilibrar a procura com os recursos que possui;
- **Carteira de *Service Management* (SPM) –** Processo de gestão de todos os investimentos em serviços de gestão em termos de valor de negócio. O objetivo da SPM é conseguir a criação do máximo valor possível, ao mesmo tempo que gere da melhor maneira os riscos dos processos e os custos;

Em termos de atividades, existem quatro fatores que é preciso definir ou dominar para que toda a elaboração das estratégias da empresa saia corretamente delineada. As atividades da estratégia de serviço são (ITSMF, 2007):

- **Definição do mercado** – Deve ser possível entender a relação entre os serviços e estratégias, entender os clientes e as oportunidades bem como classificar e visualizar os serviços;
- **Desenvolvimento da oferta** – Proceder á criação de uma base de dados de serviços para fazer face às oportunidades que surjam, para que possa ser prestado um determinado serviço com rapidez de forma a fazer face às necessidades dos clientes e do mercado;
- **Desenvolvimento de ativos estratégicos** – Define a rede de valor e melhora as capacidades e os recursos para aumentar o potencial de serviço e desempenho;
- **Preparação para a execução** – Avaliação estratégica, definição de objetivos, definição de fatores críticos de sucesso e definição prioritária de investimentos.

Esta definição de processos ocorre no princípio de todo o processo de gestão das plataformas de informação, mas depois deste patamar, é necessário que a fase de Estratégia dos serviços transforme estas atividades e processos em objetivos concretos, e para isso vai ter que definir funções para que as outras fases existentes no ciclo de vida funcionem de

maneira a que se consigo alcançar os objetivos traçados. Um serviço é promovido à fase dois, estratégia de design quando é recém-criado, ou seja, quando a empresa pretende elaborar um novo serviço para entrar numa nova área de mercado ou quando um serviço precisa de ser melhorado para satisfazer a procura que se verifica. A estratégia de serviços vai facultar á fase de design todos os serviços existentes na base de dados da empresa para auxiliar na elaboração dos novos serviços. A transição de serviço é usada para que o risco de falha de um serviço seja mitigado o máximo possível. Todas as alterações estratégicas definidas na primeira fase vão obrigatoriamente passar na fase três, transição de serviço, de forma a facilitar a sua implementação na empresa. As alterações vão ser analisadas ao pormenor, verificadas as suas qualidades e defeitos, avaliados e por fim decidir se as alterações vão ser tidas em conta e implementadas. Nesta fase a estratégia vai alimentar a fase de transição ao disponibilizar as ferramentas como a base de dados dos serviços, os mapas de elaborações de serviços, a estrutura implementada na instituição e as políticas gerais de conduta para determinar, com base nas informações disponibilizadas pela estratégia, se podem ser implementadas as mudanças. A quarta fase corresponde a etapa final da elaboração da estratégia, dada a necessidade de que a estratégia que é escolhida para implementação esteja dentro das possibilidades de elaboração das operações e recursos disponíveis na instituição. A fase de melhoria contínua é um pouco externa às quatro anteriores, mas mesmo assim a estratégia vai influenciar esta ultima fase. Dada a natureza do mercado da sociedade atual, sempre à procura e a evoluir, tudo está em constante mudança, sendo que as estratégias a implementar não fogem a essa situação, e é através dela que a empresa se adapta a situações em que o seu habitat se modificou. As estratégias depois de implementadas necessitam de ser analisadas, melhoradas, avaliadas, dai ser necessário manter uma qualidade de topo no processo de melhoria continua, para permitir ganhos em relação a mudanças de estratégia que irão culminar com vantagens poderosas quer em termos de qualidade dos serviços prestados, confiança por parte dos clientes ou mesmo de mitigação de possíveis riscos que possam surgir.

4.3.1 Problemas na implementação do ITIL

Na implementação deste tipo de sistemas existem certos processos ou aspetos que não podem ser descurados sobre a ameaça de fazer ruir todo o planeamento e estratégia para o correto funcionamento da instituição. Dada a complexidade da instalação de serviços de

informação algumas empresas não estão disponíveis para elaborar essa mudança, e se não tiverem a capacidade de detetar as possíveis consequências a longo prazo, das suas ações, se não tiverem capacidade para constantemente se atualizarem as situações hoje verificadas como soluções serão, no futuro, o seu principal problema. Alem desta situação, de as empresas não pretenderem, nem serem capazes, de mudar os seus hábitos, a própria gestão pode constituir um problema, se as decisões forem tomadas sem a devida ponderação. Sem o devido tempo e atenção na avaliação de todos os ângulos possíveis pode levar a que erradamente seja escolhido um caminho a seguir que no curto ou médio prazo possa trazer prejuízo à empresa. A fase estratégica de implementação necessita de avaliar o modo como a empresa funciona internamente com já foi indicado anteriormente, para prevenir que a ligação entre os vários departamentos não permita que existam falhas, visto vários serviços necessitarem do trabalho de vários departamentos e caso existam conflitos entre os mesmos a empresa poderá correr o risco de o serviço não ser corretamente elaborado. Outra situação que deve ser verificada é se existe, em cada departamento, um responsável, pois cada processo deve ser elaborado sobre as ordens de um colaborador direto de forma a ser corretamente implementado e gerido, sendo que para isso a administração geral da instituição necessita de atribuir a cada colaborador as suas ordens de trabalho. Tal leva-nos a outra possível falha na implementação do ITIL, pois geralmente é prestada mais atenção à criação dos mapas com os processos, que se descura o mais importante, que é elaborar manuais de operação para que quem instale o processo na parte operacional saiba o que deve fazer e como deve desenvolver o seu trabalho.

O âmbito do trabalho reporta especificamente às instituições financeiras, e o ITIL é neste caso uma ferramenta poderosa que pode auxiliar, e bastante, este tipo de empresas no que a melhoria operacional e financeira diz respeito. A situação que seguidamente será apresentada diz respeito a uma seguradora, que é apresentada de forma anónima por motivos de confidencialidade, que foi apelidada de ABC, SA. Este caso foi usado como exemplo de implementação do ITIL pela Sinfic – sistemas de informação industriais e consultoria, empresa certificada no ramo das tecnologias de informação e formação como indicação de que este tipo de plataforma pode ser implementada em instituições financeiras, e com bastante sucesso. A ABC começou por utilizar o ITIL no ano de 2005, ou melhor, a tentar a sua implementação e tudo porque a empresa não possuía o mínimo de controlo sobre a sua plataforma de informação, chegando a situação a um ponto tão extremo que as falhas que o seu sistema tinha só eram do seu conhecimento quando eram

efetuadas queixas por parte dos seus clientes de que o mesmo não se encontrava em funcionamento. A gestão de tecnologias de informação não detinha maneira de saber da existência dessas falhas, nem mesmo tinha maneira de detetar antecipadamente as mesmas. Nos dias que correm a empresa já possui as ferramentas necessárias para antecipar os problemas e resolver as situações antes que ocorram, mas foi preciso uma seria mudança de processos e mentalidades. A gestão das TI seguiu todos os passos definidos nos livros de boas práticas, sendo que o primeiro passo foi o mais complicado de elaborar. Proceder a uma análise global de toda a plataforma e recursos de informação, à elaboração de um *Check Up* e discutir entre todos os processos que se encontravam errados e definir estratégias de correção. O responsável pelo departamento de TI afirmou mesmo que "Tivemos que mostrar a nossa roupa suja, (…), isto é o que é, e estamos a trabalhar para melhorar". A instituição é de grande dimensão, empregando cerca de trinta mil colaboradores, onde no departamento de tecnologias de informação trabalham, no total, três mil colaboradores, e tendo um nível de faturação na ordem dos milhares de milhão de euros. Mesmo assim, com um sistema a funcionar num estado tão mau como o descrito, o potencial de crescimento da empresa é bastante elevado. O responsável pela implementação e gestão do ITIL indicou que " Todos estavam a trabalhar arduamente, mas o trabalho que estavam a fazer não estava a obter o nível de qualidade que precisávamos proporcionar aos nossos clientes", a situação estava identificada, seguindo-se a definição de estratégias, a fase um do ciclo de vida do ITIL. A situação melhorou, mas foi necessário um ano para focar o serviço de tecnologias de informação no negócio e nos clientes. A empresa não possuía qualquer informação sobre o trabalho que se encontrava a ser desenvolvido pela equipa dos sistemas de informação, nem sobre o processo de criação de serviços e isso foi o segundo passo a desenvolver: a criação de métricas que permitissem analisar, controlar e avaliar o método de criação dos serviços a disponibilizar aos clientes. " A primeira coisa é mostrar que se pode ter controlo, depois, pode-se tentar controlar o que está a originar os números", indicou o diretor de tecnologias de informação da ABC, e a verdade é que ao fim de dois anos já é possível validar cerca de vinte e cinco por cento dos sistemas de informação da instituição, com especial foco nos que têm mais impacto junto dos clientes, e também já é possível proceder ao controlo dos riscos com a antecipação necessária para proceder a correções se necessário. Atualmente, o gestor da ABC ainda possui colaboradores que não aceitam a nova plataforma e a forma como se alterou o processo mesmo com as vantagens que se verificaram, mostrando que na empresa

também existiram resistências a implementação do ITIL do mesmo género que foram indicados acima quando foram enumeradas algumas possíveis práticas que iriam culminar com a falha da implementação dos processos. As pessoas e consequentemente os departamentos que vão ser a base da criação dos serviços da instituição não aceitaram a interligação entre departamentos e mesmo as próprias pessoas mostraram renitência em alterar a sua maneira de trabalhar pois viam-se a sim próprias como especialistas da área de TI, colocando a suposta mais-valia pessoal a frente dos interesses da empresa. O processo acabou por ser bem implementado porque os departamentos e a gestão de TI, em reunião, chegaram a um acordo de bom funcionamento sobre o que cada departamento iria desenvolver na elaboração do produto final, e foi tudo colocado por escrito e assinado pelos responsáveis de cada departamento. Como foi verificado, esta instituição seguiu os passos indicados e trabalhou para mitigar as situações que podiam minar a aceitação do ITIL, e os resultados alcançados não podiam ser mais animadores.

4.4 Certificação

O mercado financeiro é um dos mais importantes espaços negociais do globo, dado a sua natureza de negócio, o movimento de toda a riqueza e divisas do mundo inteiro torna-o a base de todo o desenvolvimento mundial, visto para que tal aconteça é necessário obter financiamento. Dada a importância do mercado em que as instituições financeiras se encontram inseridas, a preocupação com possíveis falhas e a necessidade de controlo do risco operacional fizeram com que fossem adotadas normas de qualidade para proceder a uma correta elaboração de processos que permitam dominar, dentro do possível, todas as manobras de construção dos serviços de forma a conseguir mitigar as possíveis falhas que possam surgir. As normas de qualidade que desempenham um importante trabalho nas instituições financeiras são a ISO 9001, que define como implementar um sistema de gestão de qualidade na organização, e a ISO 27001, que define como implementar uma gestão de segurança, procedimentos que para uma empresa constantemente exposta ao risco e que trabalha com dados confidenciais são essenciais a um correto funcionamento da mesma. Uma certificação é o processo de avaliação, por intermédio de uma empresa exterior à organização, dos processos e serviços da instituição e que, em caso de concordância com os requisitos das normas internacionalmente aceites, é-lhe atribuído um certificado que prova essa mesma concordância. A empresa que desenvolve essas

avaliações tem que ser exterior à entidade de forma que a avaliação seja independente, que não sofra pressões por ter algum tipo de relação com a avaliada, e deve ser reconhecida como entidade de certificação oficial, sendo que em Portugal é o IPAC – Instituto Português de Acreditação que define quais as empresas com capacidade de certificar outras instituições. As certificações obtidas nas ISOs indicadas permitem às instituições financeiras obter vantagens bastante importantes quer ao nível interior da empresa quer no exterior. A ISO 9001 é a base para a implementação de um sistema que vai gerir a qualidade de todos os processos da organização, e no mercado atualmente é uma das principais ferramentas em termos de aumento de produtividade e da competitividade em relação a empresas exteriores e mais importante ainda, representa um aumento da qualidade de processos da própria empresa. Esta norma já se encontra na sua quarta versão, que data de 2008 e possui varias diretrizes de como pode uma empresa desenvolver os seus serviços corretamente para aumentar a satisfação dos clientes que deles usufruem. Indica também como pode, a empresa, desenvolver uma capacidade de melhoria contínua, de criação dos seus serviços com respeito pelas bases legais em vigor e desenvolver os requisitos regulamentares adequados para a sua atividade operacional de forma a obter o mínimo de desperdícios. A empresa ao conseguir implementar estes requisitos consegue obter uma certificação do sistema de gestão de qualidade e comprova que os seus procedimentos estão de acordo com as normas internacionais e que lhe é possível produzir produtos qualificados para os seus clientes. E quais as vantagens que uma empresa ganha em ser certificada pela ISO 9001? Uma correta implementação desta norma vai permitir às empresas possuir um leque enorme de vantagens, quer interiores quer exteriores. Desde já consegue requisitos para tentar a sua entrada em mercados nos quais ainda não se encontra. As empresas ganham um incremento na sua reputação e imagem. A certificação funciona como uma nova ferramenta em termos de marketing, permite obter uma vantagem competitiva em relação aos concorrentes diretos, quer em termos de qualidade dos produtos como em termos de satisfação e reputação junto aos clientes. No âmbito das vantagens internas, convém realçar duas que são bastante importantes, e que são a melhoria na elaboração das funções da empresa, quer em termos de eficiência quer em termos de eficácia no consumo de recursos, e a melhoria da produtividade dos vários departamentos, o que permite elaborar escalas de funcionalidade onde se podem distribuir responsabilidades aos colaboradores diretos assim como implementar uma cultura no seio da instituição com vista à busca da melhoria continua. No que à ISO 27001 diz respeito,

ela já foi abordada anteriormente neste trabalho como um dos *frameworks* de segurança a implementar numa instituição, e a certificação da instituição nesta norma permite também a obtenção de várias vantagens, entre as quais e desde já a credibilidade em termos de mercado, ou seja, o facto de a empresa possuir esta certificação vai ser reconhecido como tendo a vantagem de possuir uma correta proteção em termos de segurança dos seus dados e serviços fazendo com que os clientes se sintam mais protegidos se foram clientes da mesma. A empresa consegue implementar, com esta certificação, uma boa ferramenta de controlo de custos e pode argumentar junto das suas seguradoras que o sistema de controlo de risco que possui é bastante apurado e certificado por instâncias internacionais e pode assim baixar o custo anual do mesmo. Em caso de uma possível falha de segurança os custos que acarretaria para a empresa sem procedimentos rigorosos e certificados seriam astronómicos, podendo mesmo levar ao encerramento da mesma, mas com a certificação da ISO 27001 a instituição está salvaguardada de possíveis erros de segurança provenientes de fonte interna, não correndo o risco de existir a falha de segurança. A instituição consegue ainda demonstrar, em termos de avaliação, junto das autoridades de fiscalização que se encontra a cumprir todas as leis e regras às quais o seu tipo de mercado está sujeito, ou seja, quer em termos de leis nacionais como em termos de leis de mercado. Por fim, a mais importante vantagem para os clientes e para a própria empresa é a redução dos riscos com a segurança. A certificação vai disponibilizar à instituição um conhecimento sobre todos os aspetos ligados aos recursos informáticos: as falhas, como proteger essas mesmas falhas e como implementar as correções ideais, levando a uma proteção bastante fiável contra os riscos provenientes da sua atividade operacional. Resumindo, a certificação permite à empresa que a implementa o alcançar um desenvolvimento global com o intuito de proceder a uma constante evolução e melhoria, em termos de prestígio e marca, com a possibilidade de entrada em novos tipos de mercado, com uma sensação de segurança para os colaboradores da empresa em geral e clientes e permite otimizar todos os processos operacionais de forma a retirar o máximo das instituições. Permite também uma melhoria na eficácia de elaboração de serviços com a redução dos custos em geral e também imprimir uma dinâmica de melhoria continua. Visto a certificação ser uma ferramenta temporária, é necessário manter os padrões que levaram a empresa a ser certificada, pois as avaliações irão decorrer periodicamente, não podendo a empresa descurar os seus procedimentos.

5. Estrutura de uma auditoria a sistemas de informação em instituições financeiras

A importância da análise, controlo e avaliação nos sistemas de informação das instituições financeiras já foi discutida ao longo do trabalho, sendo que neste capítulo vai ser abordado a parte prática referente a elaboração de uma auditoria propriamente dita nas instituições financeiras. Serão também abordados os testes que se podem e devem elaborar para conseguir validar a parte mais importante numa instituição bancaria ou numa seguradora, o seu **controlo interno** que, segundo o Tribunal de Contas Europeu, é a totalidade das políticas e procedimentos concebidos e postos em prática pelos órgãos de gestão de uma entidade para garantir (Oliveira,2006):

- Realização eficiente e eficaz dos objetivos da entidade;
- Adesão a normas externas e a políticas de gestão;
- Salvaguarda de bens e informações;
- Prevenção e deteção de fraudes e erros;
- Qualidade dos registos contabilísticos e a elaboração atempada de informações financeiras e de gestão fiáveis;

A elaboração de uma auditoria aos SI não difere muito em relação ao processo de uma auditoria normal financeira visto que a necessidade de avaliação e certificação dos processos de registo e elaboração de informação é sempre o objetivo a alcançar, tendo por base de trabalho documentos de suporte físico ou digital. O processo de auditoria pode ser desenvolvido por intermédio de duas vertentes, por **diligência externa**, em que a mesma vai ser elaborada por um auditor externo à entidade, com total independência da empresa auditada, sendo que o planeamento neste caso funciona de diferente maneira visto ser necessário que o responsável pelo trabalho tome conhecimento do núcleo da empresa, do seu negócio, maneira de funcionar, estrutura e objetivos propostos a alcançar. A outra vertente é a **auditoria interna**, por determinação da própria gestão e processada pelo departamento de gestão de sistemas de informação. O elaborar do trabalho nesta vertente possui uma grande vantagem sobre a vertente externa no que diz respeito ao tempo e ao custo da mesma, pois não ser necessário proceder a uma aprendizagem relativa a todo o funcionamento da instituição. Possui duas grandes desvantagens, pois embora permita que a empresa tome conhecimento e avalie todo o seu processo informático, apenas é utilizável

internamente, ou seja, não vai permitir a obtenção de certificação dos seus sistemas, por falta de parecer de uma entidade certificadora, pecando também pela falta de independência que pode ocorrer nestes casos de auditorias internas. A auditoria a sistemas de informação segue um padrão geral, um conjunto de regras e testes que disponibilizam um leque de opções bastante alargado ao auditor e que o próprio vai ter de adaptar à empresa em questão. O auditor vai ter de «selecionar os itens ou questões apropriados à auditoria em causa, a partir de uma *checklist* genérica, expandindo o nível de detalhe e adicionando questões e tópicos necessários» (Oliveira, 2006). Cada área de mercado possui os seus riscos e diferentes áreas de especial atenção. O auditor deve programar o seu trabalho com essa situação sempre presente. Usando o tema específico da dissertação, as instituições financeiras, a existência das mesmas e do seu habitat negocial vai fazer com que o auditor não desenvolva um processo com as mesmas áreas de incidência como as que usaria numa auditoria a uma empresa de outro tipo de mercado alvo. O mercado financeiro é conhecido pela forte necessidade de segurança e acima de tudo confiança nos parceiros e nas instituições. É onde ocorrem enormes quantidades de transações eletrónicas de quantidades de divisa e ativos, onde se movimentam bens de valor incalculável, tudo razões que levam à necessidade de implementação por parte das instituições financeiras de controlos internos bastante apertados e sempre atualizados. O auditor ao deter o conhecimento deste pormenor, deve focar o seu trabalho na análise e validação desta área específica das instituições financeiras. O processo de auditoria a sistemas de informação divide-se em quatro fases, todas elas bastante importantes para o resultado final da mesma:

1. **Planeamento da auditoria** – Ponto em que é elaborada a estratégia a utilizar aquando da verificação da instituição financeira, tudo com base no estudo da natureza da mesma, nos objetivos e áreas mais importantes, no seu modo de funcionamento e em tudo o que constitui a organização;
2. **Validação do controlo interno** – São elaborados testes, previamente definidos, para proceder á avaliação e consequente validação dos controlos internos implementados pela instituição;
3. **Testes substantivos** – Elaboração de testes no sentido de validar a informação proveniente dos sistemas de informação, mas geralmente usados apenas na presença de falhas na validação dos controlos internos da instituição;
4. **Relatório final** – Método de apresentação dos resultados alcançados na elaboração da auditoria, uma maneira clara e bastante produtiva de apresentar os resultados.

5.1 Planeamento

Para que seja elaborado corretamente todo o processo de auditoria aos sistemas de informação é necessário, antes de tudo, proceder a um cuidadoso e pormenorizado planeamento com o objetivo de analisar e verificar todas as áreas com maior incidência de risco operacional. Existem duas definições que explicam na perfeição o que o planeamento significa para a auditoria em geral, uma delas foi elaborada pela INTOSAI, e que diz «O auditor deve planear a auditoria de modo a assegurar a execução de uma auditoria de elevada qualidade, de uma forma económica, eficiente e eficaz e num período de tempo adequado», sendo que o USGAO define o planeamento como «a chave para a qualidade da auditoria». É no planeamento que o auditor define as melhores ferramentas de maneira a proceder de forma eficaz e eficiente à avaliação completa da instituição e para a apresentação de um parecer livre de falhas. Este processo diz apenas respeito à elaboração de uma base de sustentação do processo que se encontra a iniciar. Visto que não é um dado fixo, as decisões tomadas neste momento podem e devem ser modificadas no futuro, se necessário, para que a auditoria se adapte a acontecimentos que não estavam previstos no primeiro planeamento. Existem certos procedimentos que o auditor deve implementar para que no fim a auditoria atinga o seu objetivo final (Oliveira, 2006):

- **Conhecimento das operações da entidade** – A base informática da instituição, todo o processo operacional, o modo de a organização funcionar e as operações elaboradas devem ser alvo de um estudo aprofundado para que seja possível ao auditor desenvolver um conhecimento extensivo de toda a organização. É na obtenção do conhecimento da empresa que vão ser detetadas os sistemas específicos que serão analisados com especial atenção.
- **Formação necessária do pessoal** - A equipa que vai ser destacada para proceder a elaboração da auditoria deve possuir membros com uma mescla de valências bastante diversificada, pois a auditoria a sistemas de informação é composta por varias disciplinas, tais como auditoria financeira e informática. A equipa também deve ser montada com base na avaliação primária da instituição e das suas áreas a analisar juntamente com os objetivos do trabalho da auditoria. Com a evolução constante das áreas da informática devem ser constantemente elaboradas ações de formação para os colaboradores das empresas de auditoria para que a competência do seu trabalho detenha uma qualidade acima da média, visto que atualmente os

sistemas de informação exercem influência sobre todos os controlos das instituições.

- **Verificação dos riscos da empresa –** O auditor vai desempenhar a sua função com base nas informações que lhe foram disponibilizadas pela instituição, sendo que a mesma se encontra suscetível a riscos inerentes do seu negócio ou a riscos de controlos, que ocorrem quando os controlos implementados não funcionam corretamente, situação que vai desencadear o chamado risco de auditoria. O risco de auditoria é o risco de o auditor retirar conclusões incorretas relativas aos dados analisados, ou seja, validar dados que no fundo contêm erros materialmente importantes e é com base na avaliação destes três riscos que o planeamento vai definir os testes a desenvolver para que a opinião final seja isenta de erros materialmente significativos.
- **Avaliação primária dos controlos internos –** O auditor deve marcar reuniões com os colaboradores da instituição financeira, proceder a verificações dos procedimentos dos trabalhadores nos sistemas de informação e analisar os métodos e políticas de trabalho, tudo com vista a uma validação superficial dos controlos internos que a empresa possui instalados. Esta primeira avaliação possibilita ao auditor gerir da melhor maneira o consumo do seu tempo e fluxo de trabalho, pois vai demonstrar os controlos que funcionam corretamente e os que não é preciso elaborar analises mais pormenorizadas e que deve ser logo alvo de testes substantivos.
- **Determinação dos controlos a avaliar –** tendo como principio base os dois pontos anteriores, ou seja, a verificação de riscos da empresa e a avaliação primaria dos controlos internos, o auditor deve elaborar um plano para validar e detetar os controlos da empresa que realmente se encontram a funcionar corretamente e que devido a essa situação deveriam ser submetidos a exames para validar a sua eficiência e eficácia.

No termino da quinta fase do planeamento, o auditor já deve conseguir elaborar um processo onde vai definir as vertentes da empresa a analisar, criar um grupo de analise bastante qualificado com o intuito de elaborar uma auditoria de qualidade e muito importante, deve proceder à criação de uma agenda para a elaboração da auditoria para que

seja possível controlar as varias fases da mesma para avaliar se o trabalho se encontra a ser elaborado de forma eficiente e eficaz por parte da equipa.

5.2 Análise do controlo interno da instituição

O controlo interno da uma instituição é o conjunto de ferramentas que a mesma possui para assegurar o correto funcionamento de todos os departamentos da organização. É uma maneira de certificar que a informação obtida é correta, que os dados registados são fidedignos, que os bens se encontram protegidos contra ameaças internas e externas e acima de tudo que os processos são desenvolvidos de maneira eficaz e eficiente sempre com o intuito de reduzir custos e o consumo de recursos por parte da empresa. Segundo as normas de auditoria da INTOSAI, «quando a contabilidade ou outros sistemas de informação estão informatizados, o auditor deve verificar se o controlo interno funciona corretamente, de modo a garantir a exatidão, fiabilidade e integridade dos dados» (Oliveira, 2006). Para proceder a uma validação dos controlos internos, o auditor, antes de mais, deve pedir os dados existentes sobre os mesmos, quais se encontram em vigor, como funcionam e deve proceder à sua avaliação para concluir se os mesmos conseguem garantir a veracidade e integridade de toda a informação produzida pela instituição, e provar que a mesma é fidedigna e que pode ser creditada. Para que isto aconteça, o trabalho a desenvolver é dividido em duas fases diferentes, a validação dos controlos gerais da instituição e posteriormente a validação das aplicações informáticas.

5.3 Avaliação dos controlos gerais das instituições financeiras

O controlo geral é como o próprio nome indica o habitat onde toda a plataforma de informação desenvolve o seu trabalho, onde são elaborados todos os processos informatizados da empresa e isso acontece para que seja possível orientar o sistema de informação para que funcione de acordo com os objetivos da empresa. «Os controlos gerais são a estrutura, políticas e procedimentos que se aplicam á generalidade das operações informatizadas de uma entidade» (Oliveira, 2006), sendo que a IGAE define controlos gerais como a «estrutura organizativa e os métodos e procedimentos estabelecidos para regular a relação dos SI com os restantes elementos ou componentes da entidade». No desenrolar de uma auditoria é de extrema importância que o auditor foque a

sua atenção na avaliação dos controlos internos, pois se os mesmos desempenharem a sua função corretamente, os controlos das aplicações, ou seja, a segunda fase da avaliação do controlo interno, deverá desempenhar a sua função corretamente, visto se encontrar blindada a ataques exteriores. No caso de os controlos gerais serem de fraca prestação, os controlos de aplicações vão estar desprotegidos e à mercê de alterações que vão influenciar negativamente todas as plataformas de informação e adulterar qualquer tipo de dados fornecidos pela empresa. No sentido de verificar todos os controlos gerais da instituição, os mesmos foram separados em dez categorias, sendo elas: Gestão de sistemas de informação, Planeamento e gestão de segurança de toda a entidade, Controlo de acesso, Segurança física, Seleção e implementação de aplicações informáticas, Desenvolvimento e alteração de aplicações informáticas, Software de sistema, Segregação de funções, Continuidade do serviço e Internet (Oliveira, 2006).

5.3.1 Gestão dos sistemas de informação

«A estrutura do departamento de sistemas de informação deve gerir racionalmente os recursos informáticos da organização, de modo a suprir as necessidades de informação de forma eficiente e económica» (Oliveira, 2006). Esta definição é a que melhor exemplifica o que o departamento responsável pela gestão do sistema deve fazer em termos de auxiliar a instituição a atingir os objetivos propostos. O auditor quando elabora o seu trabalho de análise deve prestar, neste primeiro patamar, atenção a um conjunto de regras e procedimentos que devem estar implementados na organização como boas práticas a desempenhar:

- Deve existir sempre um colaborador responsável pela gestão dos sistemas de informação, com experiencia e capacidade formativa suficiente para comandar um departamento completo;
- A equipa que gere a plataforma informática deve conter colaboradores de elevada formação técnica, quer em sistemas de informação que na área de negócio onde a empresa se encontra inserida. Deve ter implementada uma cadeia de comando claramente definida e instaurada uma separação de funções consoante as áreas específicas dos colaboradores em questão;

No âmbito da validação propriamente dita dos controlos internos desta área, o auditor deve verificar se estão a ser implementadas plataformas que visam assegurar:

- Os processos a desenvolver pelos SI encontram-se bem documentados, com mapas de tarefas e com uma estratégia bem definida e planeada;
- As plataformas de informação implementadas na instituição servem para o negócio em causa e colaboram na obtenção de mais-valias no cumprimento dos objetivos gerais da entidade;
- Todos os possíveis, em termos de recursos e de orçamentos, estão a ser elaborados no sentido de permitir ao sistema de informação auxiliar a empresa na obtenção dos seus objetivos;
- A gestão verifica constantemente se os sistemas de informação continuam alinhados operacionalmente com os objetivos da instituição, quer em termos de eficiência, quer em termos de segurança e eficácia. Deve-se também analisar e verificar a utilização dos orçamentos com os gastos reais para que não existam desvios sobre o que foi inicialmente planeado.

Caso prático

Foram disponibilizados testes efetuados por empresas de auditoria a instituições financeiras para que a teoria tivesse uma aplicação pratica na vida real, e no que diz respeito ao processo de controlo e gestão de sistemas de informação foi disponibilizada informação específica de uma seguradora de renome que vai ser mantida sobre o anonimato dada a confidencialidade neste tipo de trabalhos. Como pode ser verificado no anexo 1 foram verificados vários dos patamares da gestão dos sistemas de informação, aos quais foram dados o nome de *Control Environment*. O primeiro teste a desenvolver (Anexo 1 ref.1) foi investigar se a instituição financeira possuía um plano diretor de SI que estivesse focado no objetivos da mesma, tendo para isso entrevistado o responsável pela gestão dos sistemas de informação, que indicou que o sistema se encontrava instalado na empresa desde 2003, mas que nunca tinha sido alterado desde então, situação que representa uma grave falha do controlo interno da empresa, visto não se encontrar atualizado. Foi ainda reportado pelo responsável da instituição que o mesmo já não se adequava aos objetivos propostos pela administração, pois a diferença temporal era muito grande, ficando então prevista uma atualização para que esta falha grave fosse resolvida. Outro dos pontos analisados foi a existência de um orçamento específico para a área de

sistemas de informação (Anexo 1 ref.2), situação confirmada pelo diretor das tecnologias de informação, onde estão delineados os limites máximos de recursos financeiras a gastar com as diferentes atividades do sistema de informação. Segundo o analisado na auditoria (Anexo 1 ref. 3 e 4) existe uma estrutura representada no organigrama da empresa para o departamento de tecnologias de informação e que as funções a desempenhar por todos os colaboradores da empresa estão descritas num documento apelidado de "Estrutura da direção informática" e que anualmente esse documento é validado consoante a entrada de colaboradores na estrutura. Dos pontos analisados entendem-se que foram cobertos pela auditoria os pontos mais importantes a validar.

5.3.2 Planeamento e gestão do programa de segurança da instituição

No planeamento e gestão do programa de segurança da entidade é onde vão ser elaboradas as bases para a criação de uma plataforma que proceda à implementação de controlos e segurança com o intuito de avaliar os riscos aos quais a instituição se encontra sujeita e combater os mesmos até à sua mitigação. Este processo deve ser elaborado juntamente com a gestão de topo da organização para que sejam detetados todos os riscos em que a empresa possa incorrer. Para um bom funcionamento deste patamar dos controlos internos gerais, o auditor, quando elabora o seu trabalho, necessita de validar se os cinco princípios para a gestão de risco estão a funcionar corretamente, deve assim:

- Antes de tudo, verificar se existe um processo implementado que proceda a avaliação de todos os tipos de risco, interno e externo, a que a empresa se encontre exposta, identificando possíveis ameaças e pontos fracos.
- Verificar se a instituição possui um programa de segurança e se nele estão definidas as práticas e processos a desempenhar em caso de ameaças, sendo também de máxima prioridade manter esse mesmo programa atualizado até à data de validação feita pelo auditor;
- Verificar se a gestão da instituição, tem uma plataforma que proceda à organização de um programa de segurança para a totalidade da empresa. Na elaboração do mesmo devem ficar definidos os responsáveis pelo desenvolvimento, implementação e melhoramento do próprio programa de segurança e controlo;
- Verificar se os colaboradores contratados pela empresa possuem formação profissional e ética para desempenharem os seus cargos na instituição, de forma a

evitar possíveis riscos de falha de manuseamento dos sistemas ou mesmo potenciais sabotagens propositadas de maneira a fazer a instituição incorrer em sérios prejuízos e perdas de credibilidade.

- Verificar se todo o processo de gestão de risco é alvo de análise no sentido de garantir que se encontra a funcionar corretamente e que os seus objetivos estão a ser alcançados na totalidade, de forma eficaz e eficiente.

Caso prático

Em relação á validação da gestão da segurança dos sistemas de informação e do seu planeamento, foi verificado como se pode observar pelo Anexo 4 referência 1 onde se encontra indicado que existe na empresa política de segurança, disponível na intranet da empresa em questão, de forma a dar conhecimento à totalidade dos colaboradores. O responsável pela empresa indicou posteriormente que se encontram a desenvolver esforços no sentido de atualizar todas as políticas de segurança da instituição. A auditoria, tendo em conta também a gestão do risco, questionou o responsável pelo departamento dos sistemas de informação, como podemos verificar no Anexo 1 referência 6, sobre a existência da análise dos riscos aos quais a empresa se encontra sujeita, sendo a resposta afirmativa por parte do gestor, visto existir um grupo que é responsável pelo acompanhamento dos sistemas de informação quer em termos de funcionamento no alcance dos objetivos quer no que diz respeito aos riscos a que a empresa se encontra sujeita. No Anexo 6 podemos analisar outro documento referente à gestão da segurança dos sistemas de informação mas num prisma diferente. O documento em questão refere-se aos procedimentos a elaborar aquando de um desastre no sistema de informação, em que se encontram definidos e estritamente planeados todos os passos a desenvolver sempre que exista uma situação deste tipo na instituição financeira. Estão definidos os responsáveis que podem acionar todo o programa de resgate, os processos a desenvolver para recuperar o sistema e ainda os números dos colaboradores a reenviar todos os dados para que os mesmos não corram o risco de desaparecer.

5.3.3 Controlo de acessos

A função principal do controlo de acesso é o de permitir à instituição segurar, dentro do possível, as redes de informação da mesma, como bases de dados, *hardwares*, programas, aplicações informáticas, ou seja, tudo o que regula e faz funcionar a empresa. A segurança

é aplicada com o intuito de mitigar possíveis tentativas de destruição, alterações, modificações ou até perdas propositadas de dados importantes ou impedir danos físicos nos recursos tangíveis da instituição. Os controlos a implementar devem ser de duas naturezas: **lógicos**, para impedir tentativas por meio virtual e **físicos** para salvaguardar os recursos informáticos da instituição que possuem forma tangível e manter a integridade e fiabilidade de toda a informação elaborada pela mesma. O auditor deve proceder à analise dos processos desenvolvidos pela empresa no âmbito da:

- Elaboração de políticas e processos no que dizem respeito à elaboração de uma listagem de autorizações de acesso dependendo do tipo de trabalho a desenvolver pelos colaboradores autorizados. Os serviços de manutenção apenas precisam de aceder fisicamente aos locais com uma periodicidade reduzida, sendo que o pessoal que trabalha diariamente com os dados do sistema necessita de diferente nível de acesso. Deve existir implementado uma diferenciação entre utilizadores e acessos;
- Proceder à diferenciação do tipo de informação e qual a sua importância para a empresa e consoante o resultado, implementar os níveis de segurança aconselhada em termos de complexidade e grau. Informações mais sensíveis devem possuir uma segurança mais reforçada;
- Implementação de uma segurança correta e eficaz através do desenvolvimento de um misto de controlos digitais e controlos físicos no sentido de proteger toda a plataforma informática da instituição; quer aplicações quer componentes físicas;
- Verificação da existência de um programa informático que detete a tentativa de intrusão de pessoas não autorizadas e se essas mesmas serão apresentadas à gestão de sistemas de informação para que sejam tomadas as devidas diligencias no sentido de descobrir quem ou o que tentou entrar no sistema da instituição;

Este tipo de controlo pode ser bastante eficaz no mitigação do risco de adulteração ou destruição da informação, dos dados ou dos recursos físicos da organização, mas para tal deve ser constantemente atualizado com os dados que necessita, quer com a listagem de colaboradores com acesso, quer com alterações de dados de segurança informática periodicamente como palavras-chave ou pins ou com a elaboração de reportes a dar conta do estado do sistema em geral.

Caso prático

Este controlo é um dos mais importantes para a salvaguarda dos dados produzidos e detidos pela empresa pois restringe o acesso aos sistemas de informação. No desenrolar da auditoria à instituição financeira foram elaborados diversos testes, quer manuais quer automáticos no sentido de avaliar o seu correto funcionamento. No âmbito dos controlos manuais foi verificado a existência de processos de restrição de acessos as plataformas sempre de acordo com as políticas da empresa, existindo, sempre que se verifica a necessidade, a criação de novos utilizadores, a alteração de acessos consoante a modificação de funções ou competências, a eliminação de permissões de antigos colaboradores, a comunicação do acesso ao colaborador para tomada de conhecimento do seu nível e a definição dos responsáveis quer de atribuição como de autorização dos níveis dos colaboradores. Como pode ser verificado no Anexo 4 referencias 2 e 3, o teste consistiu no pedido ao departamento de sistemas de informação de uma lista com todas as alterações do ano a auditar, com os novos colaboradores, com os dados dos utilizadores apagados, com as modificações de acesso, para posteriormente selecionar aleatoriamente um número de dados e testar no sistema se foram modificados os colaboradores que deviam de ter sido e se foram mesmo removidos os antigos funcionários. O resultado dos testes elaborados foram satisfatórios em termos de novos colaboradores ou modificações de credenciais, visto terem sido analisados cinco colaboradores sem nenhuma falha de controlo. No que diz respeito à validação dos colaboradores que abandonaram a instituição foi verificada uma falha, sendo que o colaborador detém ainda acesso aos seus dados. Existe neste caso uma falha grave que deve constar no relatório final. A equipa de auditoria procedeu também à avaliação das instruções existentes em relação a revisões periódicas dos acessos disponibilizados e se os mesmos correspondem ao perfil de trabalhador e ao seu papel na empresa. O resultado obtido foi bastante satisfatório dado ter sido iniciado, à data da auditoria, um processo de revisão de acessos, e que os colaboradores analisados continham os seus acessos de acordo com as necessidades das suas funções. No que respeita a testes lógicos foi analisado pela auditora qual o comprimento, prazo e regras de composição para as palavras-chave, o histórico das mesmas e o número de tentativas que são permitidas até que a conta bloqueie, como se pode analisar no Anexo 5 referência 1. Os objetivos neste ponto do controlo foram corretamente alcançados, visto que depois de aceder aos relatórios de valores de sistema e perfis de utilizadores e analisar as configurações de segurança presentes no relatório de valores foi verificado que cada

palavra-chave possui oito caracteres no mínimo, com uma validade de trinta dias, sendo que guarda as ultimas sete palavras-chave. A plataforma de segurança permite apenas três tentativas antes de bloquear a conta. Ainda no anexo 5 podemos verificar que foram analisados vários controlos automáticos de acessos, especialmente vocacionados para a existência de controlos focados na limitação da utilização do sistema em níveis que não fazem parte das necessidades básicas dos colaboradores, e a conclusão a que chegou a auditoria é de que os controlos estão corretamente elaborados, na parte da administração e operacional só tem acesso quem efetivamente faz parte dos grupos que trabalham nessas áreas especificamente.

5.3.4 Segurança física

A criação de barreiras com o intuito de restringir o acesso aos recursos físicos de informação como servidores ou computadores e as informações que as mesmas guardam é o grande objetivo da segurança física. Com a utilização de certo tipo de aparelhos como portas com blindagem, leitores de cartões magnéticos, portas corta-fogo, sensores de pressão entre outras, o acesso a este tipo de áreas torna-se bastante restrito, permitindo apenas o acesso a colaboradores com autorização prévia. O auditor no sentido de validar a segurança física das instituições deve analisar os seguintes processos:

- Verificar a localização dos recursos físicos da instituição e analisar se na proximidade da mesma existem possíveis fontes de risco, como materiais de fácil combustão ou existência de tanques com água, potenciais catalisadores de uma falha de sistema;
- Analisar o ambiente no interior da sala dos recursos informáticos e detetar se o mesmo se encontra dentro das regras de manutenção deste tipo de espaço. O local deve conter principalmente ar condicionado para auxiliar no arrefecimento das máquinas, a inibição de utilização de produtos líquidos e a utilização de soalhos falsos preenchidos com espuma para reduzir o risco de incêndio;
- Verificar o tipo de alimentação energética de segurança que as instituições possuem instalados para fazer face a uma súbita falta de energia elétrica. Podem ir desde a existência de uma *Uninterruptible Power Suply* (UPS) ate a utilização de geradores de segurança, tudo para manter o sistema de informação da instituição a funcionar corretamente e sem interrupções.

Caso prático

O local onde são guardados os componentes físicos do sistema de informação deve cumprir determinados requisitos de forma a salvaguardar os mesmos e diminuir o risco de acidentes. No caso da instituição financeira auditada foi verificado que os componentes de *hardware* se encontravam em ótima condições físicas e ambientais. No anexo 4 referência 7 mostra corretamente o processo a desenvolver pelo auditor, que consiste em verificar as condições físicas e ambientais da sala apelidada de *"Datacenter"*, nomeadamente se continha sistema de ar-condicionado, equipamento de deteção e combate a incêndios, equipamentos de deteção de inundações, *UPS's* e geradores, chão falso, materiais de fácil combustão e camaras de vigilância. O objetivo era também verificar os controlos de acesso ao local visto ser uma área bastante sensível, o "coração" da instituição. A equipa de auditoria foi juntamente com o responsável pelo departamento verificar a sala em questão, e registou a existência de sistemas de combate a incêndios com a utilização de gás, medidor de temperatura conectado ao sistema central de alarme para proceder ao alerta em caso de aumento exponencial de temperatura, sistema de deteção e combate a inundações, com um sistema de escoamento de água instalado debaixo do piso falso, sistema de ar-condicionado com sensor de temperatura, duas *UPS's* que consoante o número de aplicações ligadas duram trinta minutos, gerador de energia e ainda extintores no interior e exterior da sala. Em termos de controlo de questões ambientais esta instituição é um exemplo a seguir, estando preparada para qualquer emergência possível. O controlo físico da sala dos computadores é composto por um ponto de acesso único, que possui duas portas, para aceder ao mesmo é preciso a utilização de um cartão com autorização específica mais a inserção de um código pin, sendo que para aceder ao local, pessoas externas à instituição bancária necessitam do acompanhamento de um técnico interno. No fim existem ainda duas camaras de vigilância que gravam tudo vinte e quatro horas sobre vinte e quatro horas sobre a monitorização de um segurança. As componentes físicas da instituição bancaria são um exemplo de todos os passos que deveriam ser implementados nas diversas entidades para um correto funcionamento dos controlos internos.

5.3.5 Desenvolvimento e modificação de aplicações informáticas

O pedido de alteração das aplicações da instituição, sejam elas de manutenção, melhoramento ou mesmo substituição total de recursos informáticos, deve ser uma decisão

bastante pensada e estudada pela gestão, pois são procedimentos que acarretam para a empresa custos, não só de aquisição, como de paragem do sistema anterior, montagem do novo e certificação de que as potencialidades e funcionalidades da nova aplicação funcionam corretamente. Deve existir ainda a definição de critérios de escolha para as aplicações que evidenciem necessidades de melhoramento de forma a não tornar a empresa frágil em termos de controlos nem em termos de situação financeira dado todo este processo ser financeiramente dispendioso. No momento em que a instituição concluir que é necessário proceder ao melhoramento ou substituição de aplicações financeiras, o auditor deve elaborar um apertado controlo, avaliando se os procedimentos adaptados pela empresa para a elaboração desta alteração se encontram dentro dos padrões de segurança e em concordância com os controlos implementados, e isso diz respeito a validar que:

- Existe por parte da gestão das operações uma autorização prévia para a implementação das modificações, visto serem os gestores que vão verificar a operacionalidade das alterações implementadas;
- Foram unicamente implementadas alterações autorizadas sendo que deve ser elaborada uma bateria de testes para mitigar a existência de alterações não ordenadas pela gestão;
- É mantido um conjunto de registos que permita aos colaboradores da empresa controlar as aplicações que foram aprovadas, as que se encontram em processo de melhoramento, as que ainda se encontram a serem testadas na sua operacionalidade de modo a evitar perturbações de maior. Estes registos devem estar interditos à grande maioria dos trabalhadores da instituição, apenas acessíveis à gestão e devem ser implementados controlos apertados no que diz respeito ao acesso aos programas no sentido de impedir contaminações de sistemas diferentes.

Caso prático

Para proceder a modificações ou alterações totais de componentes do sistema de informação da empresa é necessário desenvolver uma ponderada analise e verificar se o custo/benefício dessa mesma modificação vai ser vantajoso para a instituição. No caso especifico da instituição financeira que se está a analisar, a mesma foi alvo de determinadas análises referentes aos métodos de preparação e implementação de modificações na sua estrutura. O grupo de auditoria começou por analisar se existia no banco procedimentos base para o pedido de alteração e se os mesmos eram registados e

controlados pela gestão dos sistemas de informação. Como se pode verificar no Anexo 3 referências 1 e 2, no que aos procedimentos *standard* e formais diz respeito não existe nenhuma metodologia implementada, não existe uma base geral para efetuar o pedido de alteração mas no que diz respeito ao registo e controlo dos pedidos elaborados foi verificado, junto do responsável pela área em questão, a existência de três pedidos de alteração, e um cancelamento de pedido, sendo que estas informações são registadas num programa próprio de modo a ser desenvolvido um controlo sobre as áreas que se encontram em análise. O auditor depois desta primeira fase, focou o seu trabalho no essencial deste controlo, como se pode verificar no Anexo 3 referencia 3. A aceitação da elaboração da modificação depois de efetuada uma avaliação completa à estrutura, em termos técnicos e de impacto, foi feita e para isso foram disponibilizados, pela gestão da plataforma informática, todas as trocas de informação entre as partes responsáveis pelos testes e analises tendo-se chegado á conclusão que ambos os pedidos existentes foram alvos de detalhada e cuidada análise técnica e posteriormente aprovados pela administração da instituição.

5.3.6 Seleção e implementação de aplicações financeiras

Quando existe uma necessidade em termos de aplicações informáticas, a instituição tem de adquirir os mesmos no sentido de suprimir essa necessidade, mas dentro sempre dos requisitos definidos para a manutenção da fiabilidade e segurança das informações produzidas pela mesma. Deve assim:

- Analisar se os produtos são adquiridos a fornecedores com certificação de comercialização deste tipo de produtos e se os mesmos são testados antes de proceder à instalação. Outro ponto onde é necessário prestar a devida atenção é na qualidade das garantias fornecidas no caso de as aplicações informáticas avariarem;
- Definir antecipadamente o conjunto de aplicações que necessitam de serem atualizadas para a elaboração de um conjunto específico de requisitos com o intuito de escolher as novas aplicações com iguais características para que a empresa não se ressinta em termos de segurança, controlo e produção de informação de qualidade;
- Proceder à elaboração de manuais específicos para a nova aplicação com o intuito de facilitar o manuseamento do mesmo por parte dos colaboradores da empresa;

- Verificar a existência de um processo de atualizações junto do fornecedor para manter a aplicação informática o mais avançada e segura possível no processamento operacional e no combate ao risco.

Caso prático

A instituição financeira, sobre a qual incidiram os casos práticos que estão a ser avaliados neste ponto, ficou um bocado aquém das espectativas visto que dos controlos que foram indicados acima apenas foi analisado a temática relacionada com os fornecedores, como se pode verificar no Anexo 1 referência 5, tendo este controlo pecado pela falta de detalhe desenvolvido nos outros pontos em questão. Foi verificado pelo auditor se os contratos com os fornecedores especializados da instituição se encontravam em vigor e atualizados à data da elaboração do trabalho, situação que se veio a verificar estar implementados. A auditoria não focou nenhum dos outros três pontos assinalados, não sendo possível desenvolver opinião acerca do resultado deste controlo interno. Contudo é uma situação que se pode verificar que não funciona corretamente, dado a sua falta do foco nos pontos em questão. Dada a faltas de um procedimento implementado na empresa sobre o pedido de alterações nas aplicações informáticas, é de todo impossível desempenhar uma função preventiva de todo o tipo de modificações a fazer, ficando assim o sistema à mercê de problemas que surjam para dar relevo à necessidade de obtenção de melhoramentos. Relativo á elaboração de manuais não existe nenhuma indicação de que sejam elaborados para facilitar o trabalho desenvolvido pelos colaboradores neste ponto específico do seu trabalho. Este controlo encontra-se bastante fraco e a área em questão vai ser incluída no relatório final e testes subsequentes vão ser desenvolvidos para analisar a veracidade da informação proveniente deste controlo.

5.3.7 *Software* de sistemas

O *software* de sistemas de informação é composto por um agregado de programas e procedimentos elaborados pela instituição com o objetivo de gerir e orientar todos os processos desempenhados pela plataforma informática. A importância desta ferramenta no seio da organização é enorme. Dela estão dependentes a quase totalidade dos processos operacionais de uma instituição, como processamentos de salários, gestão da base de dados, toda a elaboração de registos. Um ponto que a empresa não pode descurar que é o controlo sobre o mesmo, não permitindo a terceiros o acesso e alteração das bases já

programadas com o risco de catástrofe se tal acontecesse. O auditor deve então proceder a análise da entidade nos seguintes pontos de controlo e verificar se existem:

- Procedimentos de proteção do acesso ao *software* com a utilização de vários tipos de controlo, para que seja mantida a fiabilidade de todo o sistema de informação;
- Instalação de um método de verificação dos acessos ao *software*, ou seja, elaboração de um programa que permita verificar quem acedeu ao sistema e que alterações e modificações elaboraram, para que seja possível a entidade detetar e punir situações consideradas inapropriadas ou forma das normas estabelecidas;
- Registo de todas as alterações elaboradas no *software* do sistema para proceder com maior facilidade ao seu controlo e avaliação, visto apenas serem aceites alterações que já tenham sido testadas com sucesso, e se não for esse o caso, se o registo permite uma fácil mitigação do processo errado;

Caso prático

O *software* de uma instituição financeira é a base operacional de toda a plataforma informática da mesma. Todo o processo da organização é suportado pelo *software* que funciona como ligação entre as operações que são necessárias desenvolver e as componentes físicas do sistema de informação. Para que tudo seja corretamente elaborado, depois de efetuada a programação, o *software* deve possuir controlos de defesa para que seja impossível proceder a alterações indesejadas e não planeadas pela administração. O trabalho a desenvolver pelo auditor nesta área é o de validar a existência desses controlos de acesso e se os mesmos se encontram a funcionar corretamente. Na auditoria desenvolvida a uma instituição financeira, foram efetuados três testes diferentes nesta área, como se pode observar pelo anexo 7. No primeiro foram analisadas as defesas lógicas de acesso ao sistema operativo, as politicas de segurança implementadas e avaliadas essas mesmas politicas para assegurar que a amplitude das medidas é suficiente para salvaguardar a instituição. Após uma reunião com o responsável pelo departamento de sistemas de informação foi verificado que existe um sistema de palavra-chave de seis caracteres com um prazo de validade de noventa dias para aceder ao sistema operativo, que é guardado no sistema as ultimas seis palavras usadas para aceder ao mesmo, que o número de tentativas falhadas permitidas para acesso ao sistema é de três tentativas antes de bloqueio de conta do colaborador. Mas verifica-se a existência de uma grave falha de segurança, pois encontra-se acionada a opção de nunca expirar uma palavra-chave, levando

o prazo de noventa dias a não efetuar a sua finalidade, e mesmo que ao fim de noventa dias seja obrigatório mudar a palavra ela continua ativa para proceder ao acesso do sistema operativo. Esta situação deve ser inserida no relatório final e deve ser alvo de retificação o mais rapidamente possível. No fim desta análise principal foram verificados, mais detalhadamente, dois controlos que devem ser implementados neste tipo de segurança, e que são: a autorização de acessos à administração do *software* apenas a pessoas especializadas e identificadas pela instituição e a instalação de uma aplicação informática que regista as tentativas de entrada no sistema de informação e todas as alterações desenvolvidas de forma a permitir um apertado controlo de todos os processos elaborados. Em relação ao primeiro ponto foi pedido ao departamento de sistemas de informação uma lista de utilizadores com acesso ao nível administrativo do sistema operativo. Foram analisadas todas as contas e verificado se de acordo com as competências dos indivíduos dentro da instituição fazia sentido possuírem acessos administrativos ao sistema. O resultado final foi bom, dado não ter existido qualquer mal funcionamento no controlo, mesmo com a empresa a ser gerida entre dois países diferentes, todos os administradores estão corretamente definidos. No caso da existência de registos de alterações os mecanismos encontram-se a funcionar corretamente, as entradas ou tentativas de entradas e alterações são registadas num programa de auditoria, com a exceção de um programa especifico chamado *"Kerbers"*, que além do controlo que desenvolve na rede interna da empresa mais nenhuma segurança disponibiliza à instituição, tornando-se algo limitado na sua função. Esta situação deve ser reportada em relatório final, mas como um aspeto a melhorar no futuro e nunca como uma falha de segurança, pois o programa diminui o risco de acesso mesmo sendo limitado o seu campo de ação.

5.3.8 Segregação de funções

A existência de segregação de funções nas instituições tem como objetivo diminuir o potencial de risco de falhas graves, seja por questões involuntárias seja por situações propositadas. O primeiro passo na elaboração de um departamento de sistemas de informação é desenvolver a sua hierarquia e os processos que cada colaborador vai praticar, existindo já neste ponto a divisão do controlo e responsabilidade pelos vários profissionais no sentido de diminuir o risco potencial. A empresa ao elaborar esta divisão de tarefas vai proceder à mitigação da probabilidade de ocorrência de erros, dado que o trabalho de cada pessoa vai ser utilizado e consequentemente analisado por outra no

desenvolvimento do seu próprio trabalho, não permitindo a existência de ações fraudulentas ou não autorizadas. A validação desta área de controlo significa analisar se a empresa:

- Possui nos diferentes núcleos do departamento de sistemas de informação uma estrutura organizacional bem desenvolvida, com os objetivos a alcançar corretamente planeadas e o caminho para chegar aos mesmos. Se os níveis hierárquicos se encontram devidamente instaurados, se cada colaborador tem conhecimento das suas responsabilidades e do trabalho a desenvolver e se existem delineadas as competências técnicas necessárias para o desenvolvimento das funções na empresa;
- Procede à análise dos procedimentos operacionais da mesma e elabora a segregação das funções que são incompatíveis;
- Implementa controlos de acesso de forma a certificar que as segregações que foram definidas estão efetivamente a serem cumpridas pelos colaboradores;
- Procede à verificação de toda a atividade desenvolvida pelos colaboradores da instituição, de forma a controlar o acesso às plataformas informáticas e à mitigação de erros de processamento de funções;

Casos práticos

Os departamentos de sistemas de informação possuem sempre uma pirâmide hierárquica para melhor controlar o desempenho das atividades e dos colaboradores, mas a segregação de funções deve existir sempre de modo a diminuir o risco de falhas graves aquando do desenvolvimento de ações incompatíveis entre si, pelo mesmo colaborador. A instituição financeira foi alvo de verificação da existência de segregação de funções no processo de elaboração de alterações no sistema de informação, dada a importância e o risco que este processo representa para a empresa. O auditor pediu ao responsável uma listagem com as alterações efetuadas ou as que se encontram em fase de desenvolvimento na instituição para verificar se existiam evidências que demonstrassem uma segregação ativa e corretamente efetuada ao longo do processo. Após análise foi verificada que existia de facto uma correta separação de funções dado que as alterações ao sistema são efetuadas por uma entidade externa à empresa, como pode ser analisado no Anexo 3 referências 6 e 7, não existindo acesso por parte dos colaboradores internos. No que toca aos ambientes de desenvolvimento de processos, de teste dos mesmos e da produção da empresa, os mesmos

encontram-se igualmente segregados dado os programadores apenas acederem ao ambiente de desenvolvimento, o ambiente de teste só ser acedido por utilizadores finais devidamente autorizados e o processo de transferência de teste para produção ser realizado por um colaborador independente da pessoa que o desenvolveu. A política da organização no que diz respeito ao controlo de separação de funções é exemplar pois não deixa nenhum aspeto por validar e tem implementado todos os processos corretos no que a este controlo diz respeito.

5.3.9 Continuidade de serviço

A continuidade do serviço é composta pelos procedimentos que a mesma possui para proteger os seus dados e combater com a maior eficácia possível o risco de interrupções não previstas. No caso da mitigação da ameaça falhar, a empresa deve possuir um plano de recuperação de todos os processos mais importantes no sentido de permitir a continuidade do funcionamento normal da mesma. Quando a empresa elabora um plano deste género é de capital importância prestar atenção às funções que devem em primeira instancia serem restabelecidas, deve proceder-se a identificação de todas as plataformas informáticas que a mesma possui para que não fique uma unidade desativada sendo o mais importante a elaboração das regras gerais a praticar para que o processo operacional da empresa se desenrole normalmente ate á recuperação dos sistemas de informação mais importantes. Para assegurar a fiabilidade do controlo, o auditor deve verificar se:

- Existe por parte da gestão uma diferenciação entre os processos mais importantes para a empresa e os recursos que esses processos necessitam, para que em caso de tragedia, a empresa recuperar convenientemente;
- Proceder à implementação de ações que visam prever e diminuir a existência de problemas resultantes de acontecimentos imprevistos, como a elaboração de *backups* das bases de dados ou informações importantes e guardá-los em locais diferentes, se estão implementados sistemas de controlo de eventos ambientais como inundações ou incêndios, se existem outras instalações que sirvam de sede enquanto não funcionar a principal. Devem também ser implementados nos seus colaboradores os procedimentos a executar em situações problemáticas;
- Criar documentos com as ações a desenvolver para reiniciar as aplicações informáticas depois de um acontecimento imprevisto;

- Se são efetuados testes e exames com uma periodicidade aceitável com o intuito de manter os planos o mais atualizado possível para que em caso de serem necessários os mesmos funcionem como é expectável. Os testes servem para detetar fraquezas e realizar as correspondentes melhorias estruturais nos mesmos.

Casos práticos

Todos os controlos existentes numa empresa visam a salvaguarda dos processos e a tentativa de mitigação dos riscos que a empresa corre, mas este controlo nem sempre é cem por cento eficaz, e se a catástrofe ocorrer a empresa necessita de estar preparada e ter mecanismos que a façam recuperar todos os seus processos, dados e sistemas. No processo de validação deste controlo da instituição, o auditor deve prestar atenção na elaboração de *backups* das informações, nos processos de recuperação de desastre e se existem ferramentas para acionar os registos quando necessário. No caso real da auditoria a uma instituição financeira, como pode ser verificado no anexo 2, foram efetuados testes específicos aos controlos de continuidade da empresa, em primeiro lugar, e após reunião com o responsável do departamento, foi pedido o manual de procedimentos relativo aos *backups* e quais os processos de segurança em vigor na empresa, para ser efetuada uma análise relativa à sua amplitude, existência e abrangência. Foi detetado que o sistema implementado na empresa se encontrava inadequado pois apenas disponibilizava a informação sobre a frequência, o tipo e o tempo de armazenamento do *backup*, mas a empresa que foi contratada para a implementação do sistema de informação da instituição possuía um backup de todo o sistema. No sentido de analisar a periodicidade com que são elaborados os *backups*, se diários, semanais ou mensais, foram pedidos os *log's* dos mesmos para proceder à verificação da sua concordância com as políticas da instituição, e o resultado obtido foi satisfatório, dado que os registos são elaborados automaticamente pelo programa AS400, embora não exista informação sobre a sua periodicidade. Para que exista um correto controlo dos processos de armazenamento dos registos é necessário elaborar uma revisão periódica e criar as condições para a elaboração de testes de reposição/recuperação desses registos mais importantes de forma que quando forem realmente necessários o processo não contenha falhas e funcione corretamente. O auditor, como pode ser verificado no anexo 2 referências 6 e 7, pediu as evidências que demonstrassem uma revisão dos *log's* realizados pela entidade e para proceder à avaliação dos testes de recuperação pediu acesso ao planeamento e resultados dos últimos testes

efetuados. O resultado dos testes efetuados foi satisfatório no que diz respeito às revisões efetuadas aos registos dado a instituição financeira elaborar um ficheiro de controlo onde são registadas as falhas existentes nos mesmos e onde é possível também descortinar que, pelo menos mensalmente, são elaborados os testes. No caso dos testes de recuperação foi detetada uma falha grave para a instituição dado não se encontrar implementada a realização de ensaios dos registos mais importantes, ficando a organização sem saber se em caso de necessidade os controlos implementados irão funcionar. Esta situação deve ser descrita em relatório como uma imperfeição grave no caso de acidente, dado não ser possível assegurar a correta recuperação de todos os dados. A localização dos registos deve obedecer também a determinadas regras e a auditoria aos sistemas de informação necessita de efetuar a avaliação desse patamar de segurança, para indicar se os mesmos se encontram corretamente guardados, em local seguro, e se em caso de transporte a sua locomoção é efetuada de forma segura. Foi concluído pela auditoria que as bases de dados são armazenadas num cofre, em local seguro e existe uma ficha de controlo que identifica os registos que se encontram fora do perímetro da entidade. Não existe indicação de como é elaborado o transporte dessas *tapes* que se encontram fora do espaço da empresa, mas é uma melhoria que deve ser descrita no relatório final com o intuito de a instituição a adotar o mais rápido possível. Para assegurar a continuidade de uma instituição financeira não é necessário apenas guardar o registo de toda a informação da mesma; é preciso possuir planos de recuperação de catástrofes e de continuidade de serviços, e devem ser ambos testados periodicamente no sentido de ser confirmado o seu correto funcionamento quando for indispensável ativar o plano. O auditor necessita de verificar a existência de estes planos e se eles se encontram implementados na organização, se é revisto e atualizado para que as alterações sofridas ao longo dos anos pela organização sejam repercutidas no próprio plano. Como pode ser verificado no anexo 2 referencias 9 e 10, existem os processos em causa, mas com um gravíssimo problema, não são atualizados desde Novembro de 2004, o que significa que se encontram bastante desatualizados. Dado ser uma situação bastante grave é obrigatório a sua inclusão no relatório final com a indicação de resolução do problema com a ameaça de não emissão de opinião favorável à certificação legal da instituição. Os testes que periodicamente deviam ser elaborados para a aprovação dos mesmos, relativos ao plano de recuperação e continuidade, também não são efetuados, situação que vem do que anteriormente foi referido. Este controlo encontra-se com falhas bastante graves, sendo mesmo inútil para a instituição financeira, necessitando

o auditor de desenvolver testes subsequentes para confirmar o correto funcionamento dos registos.

5.3.10 Internet

No mundo atual a internet é um dos locais mais importantes para qualquer empresa ou negocio, tudo devido à facilidade de chegar a todo o lado em qualquer lugar. Uma instituição financeira pode utilizar a internet de duas maneiras, como **cliente**, quando a utiliza para aceder a varias plataformas existentes, como *emails*, sites da especialidade e pode utilizar a internet como **servidor** quando procede à disponibilização de serviços *e-commerce* como os sites de acesso aos serviços da empresa. Embora a internet seja um dos locais que mais pode fazer a instituição crescer em termos de negócio e importância para os seus clientes, é um mundo que acarreta bastantes riscos, e são esses mesmos riscos que a empresa tem que calcular e concluir se as vantagens provenientes de trabalhar num ambiente deste estilo representam um ganho ou se os prejuízos que vai trazer para a empresa são superiores aos potenciais ganhos. Para mitigar esse mesmo risco existem certos processos que a empresa pode adotar, como a verificação da utilização da internet e a consequente avaliação das tentativas de intrusão por parte de pessoas exteriores à instituição, utilização de aplicações informáticas como antivírus para verificação de anexos recebidos por fontes externas da empresa de modo a analisar a presença de ameaças, formação especifica aos colaboradores para a utilização e navegação na internet, proceder à distribuição de documentos a explicar aos funcionários as alterações que existam na rede interna da empresa e dos acessos a informações *online* exteriores e muito importante, utilização de mecanismos de proteção de informações sempre que for disponibilizada informação para o exterior da empresa. Para avaliar os controlos implementados pela instituição no âmbito de salvaguardar as informações no que à internet diz respeito, o auditor tem que verificar a eficácia dos seguintes processos:

- Implementação de controlos em relação aos acessos à internet, com a instauração de várias aplicações informáticas como *proxys* ou *firewalls* com o intuito de impedir o acesso aos computadores por entidades externas à empresa, aplicações que registem os sítios acedidos pelos colaboradores de forma a verificar se os mesmos estão a aceder a informações ou localizações não autorizadas pela empresa e que colocam em risco a segurança da mesma e ainda verificam se é

disponibilizada informação confidencial por parte desse mesmo colaborador a instituições ou pessoas singulares exteriores.

- Desenvolvimento por parte do departamento responsável de políticas de controlo dos correios eletrónicos e a elaboração de procedimentos de boas práticas no uso dos mesmos, pois os correios eletrónicos são armazenados em servidores e se não existir uma política de controlo pode existir o extravio dos mesmos, situação que pode ter graves consequências para a empresa;
- Existência de uma proteção contra utilizadores externos à empresa no sítio da mesma para impedir o acesso a páginas de elevada importância ou restritas, certificar que apenas possuem autorização para navegar no servidor público e nas páginas que contêm apenas informações autorizadas e proceder à verificação de tentativas de alterações desenvolvidas e elaboradas por *hackers* ou programadores de outras entidades;
- Criação de aplicações informáticas para combater a tentativa dos *hackers* de ultrapassarem as falhas da segurança;
- Elaboração de um processo de transmissão de informação sensível de modo seguro através da internet, quando necessário;
- Criar políticas de sensibilização para a existência de vírus e *spywares* e os seus riscos provenientes do acesso a sítios não autorizados;
- Elaboração de processos seguros de transações financeiras que permitam salvaguardar os dados confidenciais dos seus clientes;

Casos práticos

A expansão que a internet sofreu desde a sua criação foi enorme e atualmente é um local onde muitas empresas desenvolvem os seus negócios dada a facilidade de contacto com entidades locais e estrangeiras, mas nem tudo neste mundo virtual, na *world wide web* é vantajoso para uma empresa, e exemplo disso são as propagações de vírus e *spywares* através de correio eletrónico ou sítios específicos que contaminam os terminais de trabalho de quem acede a estas informações sem a devida proteção. Neste sentido é necessário as instituições financeiras implementarem ferramentas informáticas para impedir esses ataques às suas aplicações informáticas. De acordo com o anexo 4, referencias 4 e 5 podem ser verificadas as análises efetuadas pelo auditor relativas às atualizações dos antivírus dos

servidores e computadores, aos terminais de trabalho dos colaboradores, às configurações dos antivírus assim como a verificação se todos os terminais se encontravam totalmente protegidos e atualizados. A avaliação foi bastante positiva pois os antivírus entravam-se atualizados em todos os terminais de trabalho e as atualizações são instaladas diariamente e automaticamente sempre que existem novas versões disponíveis. No caso do acesso à internet, o auditor necessitou de verificar se a *firewall* se encontrava devidamente programada com as restrições a sítios de conteúdo não autorizado para não permitir o acesso aos mesmos, situação também validada positivamente através de uma reunião com o responsável pelo departamento e posterior analise dos terminais do impedimento de acesso a determinados sítios não autorizados no sentido de proteger os conteúdos da empresa. No controlo da internet, a instituição possui uma excelente segurança relativa a ameaças exteriores.

5.4 Avaliação dos controlos aplicacionais

A avaliação aos controlos operacionais foi executada para proceder a um ato de prevenção, deteção e correção de problemas e erros ocorridos ao longo do processo operacional do sistema de informação. A avaliação é focada essencialmente na informação, na fiabilidade e integridade dos dados a colocar no sistema, na correta conversão da totalidade da informação e dos dados externos para impedir a existência de erros aquando da sua utilização. O foco incide também na certificação do processamento total das informações em tempo útil e sempre de acordo com as politicas implementadas na empresa e no fim o de proteger sempre a informação elaborada de tentativas de modificações e alterações que façam a mesma perder a sua credibilidade. Para a elaboração deste controlo de aplicações existem certas técnicas e processos que o auditor pode e deve utilizar no sentido de validar as proteções das empresas (Oliveira, 2006):

- Observação do funcionamento e execução dos controlos;
- Análise da documentação relacionada com os controlos das aplicações;
- Discussão dos controlos com os funcionários;
- Questionários, inquéritos e inspeções;

Este tipo de controlo incide em três aspetos básicos do tratamento da informação por parte da empresa, sendo eles, a receção primária da informação, o seu processamento e a

disponibilização de informação criadas pela instituição, e comparando com os processos do controlo geral apresentado anteriormente existem diferenças assinaláveis:

- Os processos de controlo são desempenhados automaticamente e não manualmente como nos controlos gerais;
- Os alvos dos testes são as bases de dados e os processos informáticos e não as políticas da empresa, os processos operacionais ou o desenvolvimento de estruturas;
- Os controlos implementados focam-se nos resultados financeiros obtidos em cada aplicação informática, ou seja, uma relação entre o benefício e o custo da existência do mesmo em cada uma das aplicações enquanto nos controlos gerais é analisada este prisma mas numa visão global de todos os controlos de aplicações informáticas.
- Focam-se especialmente na garantia dos dados elaborados pela instituição, na manutenção da fiabilidade e integralidade dos mesmos e acima de tudo na segurança, para evitar a sua modificação ou destruição.

Todo o processo de controlo de aplicações é composto por um conjunto de seis classes, sendo elas os controlos de fronteiras, organização e documentação, *input*, processamento, integridade dos dados e *output* (oliveira, 2006), sendo que o nosso foco vai ser nos três processamentos mais importantes, **input, processamento** e **output,** dado os outros três já serem abordados no controlo geral de uma instituição.

5.4.1 Input

Os elementos que constituem o *input* de uma aplicação informática são os componentes que permitem o transporte das bases de dados e dos processos a desenvolver para o interior das mesmas. As informações podem ser registadas de várias formas nas aplicações informáticas mas a maneira como é efetuado esse processo vai implicar uma adaptação do controlo a implementar por parte da instituição, para que nunca seja posta em causa a segurança e integridade dos mesmos. Os controlos nesta área existem com o objetivo de validar todo o processo e limitar a existência de erros de programação ou absorção de informação e mitigar o risco de tal acontecimento, tendo como exemplo que quanto maior forem os processos manuais despenhados pelos colaboradores na inserção de dados no sistema, maior será a probabilidade de os mesmo possuírem erros. O auditor deve avaliar todos os processos em especial os controlos aplicados nesta fase:

- Registo apenas de dados previamente autorizados por despachos da gestão de topo no sentido de permitir a sua implementação;
- Implementação de registo numérico nos dados a inserir para que seja elaborado um controlo das informações já registadas;
- Proteção dos dados já existentes e previamente autorizados e limitar poucos colaboradores o acesso urgente de alteração de dados;
- Implementação de processos que garantam a exatidão do registo da informação, fazendo a mesma cumprir os requisitos propostos pelo sistema, como em relação a dimensão dos campos, se as margens estão dentro do limite do programa, se não existe registos errados referentes ao mesmo ponto e se a informação se encontra registada de maneira coerente.

5.4.2 Processamento

O processamento é o patamar do processo de transformação de informação que é responsável pelo manuseamento das bases de dados introduzidas nos sistemas de informação que procedendo posteriormente à analise, tratamento, organização e classificação dos mesmos. Nesta fase de tratamento de dados existem duas vertentes diferenciadas pela obtenção da informação a processar, seja ela proveniente de fontes externas à empresa e que tenham sido inseridas no sistema no exato momento ou então dados que já se encontravam nas aplicações. Os controlos implementados neste ponto visam garantir o completo processamento de todos os dados, com exatidão e que a manipulação e classificação ocorram da melhor maneira possível, culminando no fim com o registo de todos os dados elaborados. Para avaliar tal processo, o auditor deve validar com sucesso os seguintes controlos:

- Realização de testes para certificar a logica dos resultados alcançados;
- Elaboração de conjuntos de dados para possibilitar aos colaboradores responsáveis proceder à avaliação dos resultados finais;
- Elaborar um *cross-check* dos dados obtidos manualmente com os obtidos automaticamente com uma periodicidade curta de forma a validar os resultados obtidos;
- Manter os dados processados seguros e acessíveis para que seja possível efetuar, no futuro, testes subsequentes para elaboração de análises de tendências;

- Utilização de registos secundários das operações que ainda se encontram incompletas, para assegurar que são guardados todos os processos elaborados no processamento da informação;
- Proceder à avaliação e controlo de todas as atividades referentes à organização de dados, processos de término de exercício, elaboração de relatórios e outros processos de fecho do processamento de informação no sentido de validar o seu correto funcionamento.

5.4.3 Output

Os controlos de avaliação da informação elaborada pela instituição visam garantir que a mesma é disponibilizada apenas aos colaboradores e a pessoas específicas externas á empresa que possuem autorização para as receber e que a informação disponibilizada seja verdadeira, precisa e completa. Todas as aplicações informáticas possuem sistemas de output para permitir uma correta disponibilização das informações elaboradas pelas instituições, e para esse processo correr da melhor maneira existem certos componentes que são essenciais para o atingir do objetivo, como os equipamentos usados para processar toda a informação, os programas que escolhem as informações a serem processadas e por fim os colaboradores e recursos físicos da instituição que procedem ao encaminhamento do output. Existem dois tipos de output, o ***offline*** **output** e o ***online*** **output.** O *offline* output é criado através do processamento de informação que é disponibilizada pelo registo da mesma, sendo que a análise *online* output a proveniência de toda a informação é de plataformas terminais informáticas. É de extrema importância que as instituições procedam a elaboração de controlos que validem a criação e disponibilização da informação para que o output possa ser entregue o mais rapidamente possível às pessoas credenciadas para tal e sempre com qualidade, exatidão e totalidade. A forma de o auditor validar o correto funcionamento deste patamar de controlo da empresa é testar os seguintes controlos que o compõem:

- Garantir a exatidão e totalidade da informação disponibilizada independentemente do modelo de apresentação;
- Proceder a constante atualização dos recetores das informações;
- Destruir todos os outputs que não tenham destinatários definidos;
- Aplicação de todo o tipo de normas de segurança utilizada pela instituição de forma a tornar os outputs protegidos e confidenciais;

- Proceder a criação de uma numeração sequencial de forma a ser fácil de localizar e controlas as informações disponibilizadas;
- Elaborar cross-checks entre as listagens numéricas das informações e o inventário da empresa e analisar com urgência as diferenças detetadas.

5.5 Elaboração de testes substantivos

As instituições com o desenvolvimento das plataformas informáticas foram adaptando as mesmas para melhorarem as suas performances operacionais em termos de processamento de dados, anotação de processos, melhoramento de procedimentos e distribuição de informação. As vantagens não são apenas para as empresas, dado que ao existir este tipo de recurso, a auditoria tem acesso mais facilmente a todo o tipo de informação que necessita para efetuar o seu trabalho, tudo graças as características dos sistemas (Oliveira, 2006):

- **Centralização** – a informação encontra-se depositada normalmente num número muito pequeno de sistemas informáticos instalados num único edifício;
- **Volume** – o volume de informação é normalmente muito elevado;
- **Suporte *standard*** – o suporte informático onde é mantida a informação é constituído normalmente por bases de dados relacionais que se encontram em discos e cd's;
- **Acesso concorrencial à informação** – a informação mantida nos sistemas informáticos é utilizada, em simultâneo, por vários utilizadores e aplicações;
- **Formato** – o formato dado à informação é uniforme e permite a interligação entre diferentes tipos de informação.

Como já foi apontado varias vezes ao longo do trabalho, os sistemas de informação não trazem apenas vantagens às empresas, o risco foi um dos problemas que foi implementado aquando da aceitação deste tipo de plataformas no seio das instituições. As quantidades enormes de informação que processam e controlam, as diferenças que existem entre as quantidades inseridas em sistema e o que na realidade existem e a obrigatoriedade de existir sempre a necessidade de mão humana para funcionar criam uma rede de problemas que a empresa precisa solucionar. Visto existirem estes riscos o auditor deve desconfiar sempre dos dados provenientes dos sistemas de informação, pois o seu objetivo de trabalho é proceder a sua validação e para isso vai precisar saber utilizar os dados do sistema e posteriormente analisar e validar os mesmos.

5.5.1 Condição para a utilização de dados

O primeiro passo a tomar referente a utilização dos dados do sistema é verificar o que já foi validado até ao momento, isto é, se os controlos gerais e os das aplicações foram suficientemente bons para que os processos fossem validados e os dados sejam considerados exatos e poderem ser usados como amostra no relatório final, se os controlos forem fracos e os dados se tornarem o principal alvo e objeto da auditoria vai ser preciso validar os mesmo e o sistema de informação. No caso de se verificar que os dados não são fiáveis deve ser elaborado um conjunto de processos alternativos como obtenção de dados de outros locais mais fiáveis, proceder a uma restruturação do objetivo geral de forma a eliminar os dados com problema, proceder á avaliação dos dados com problemas mas fazendo sempre referencia a essa situação e indicar a impossibilidade de emissão de opinião sendo que no caso de todos estas reformulações forem insuficientes o auditor deve cancelar a pratica da auditoria.

5.5.2 Apreciação da fiabilidade dos dados

O passo a seguir depois de conseguir aceder aos dados que necessita, o auditor deve proceder a avaliação dos dados, determinar se os sistema de informação elaboram corretamente os dados em que a empresa se baseia para desempenhar as suas operações. Este processo deve ser planeado com todo o cuidado e a estratégia a adotar deve ter em conta todos os elementos que constituem os dados da organização, pois um incorreto planeamento pode fazer a equipa de auditoria desperdiçar recursos em situações que os controlos implementados conseguem validar grande parte da informação, ou uma situação que não foi devidamente alvo de foco e que no futuro pode trazer sérios problemas a instituição. Existem dois métodos para a avaliação da fiabilidade dos dados dos sistemas de informação (Oliveira, 2006):

- **Completa** – Proceder ao teste e avaliação, com profundidade, de todos os controlos de um sistema de informação, incluindo as aplicações e os produtos. Tem como defeito necessitar de muito tempo para desempenhar um correto trabalho, mas permite um melhor entendimento da utilidade e funcionamento de todo o sistema da instituição;
- **Limitada** – foca o seu trabalho especificamente nos dados da instituição, não desempenha uma análise muito detalhada dos controlos e aplicações. Os testes

efetuados aos controlos são os essenciais para que a integridade dos dados seja comprovada;

Este processo não conclui a auditoria em si, visto ainda ficar a faltar o relatório final, mas o desenvolver do trabalho no terreno tem a sua conclusão na validação da fiabilidade dos dados, que é o objetivo principal de uma auditoria, o de assegurar que as informações desenvolvidas pelas instituições, especialmente as financeiras, são exatas, seguras, fiáveis e que demonstram o que realmente se passa no processo operacional da empresa, uma imagem verdadeira da organização.

5.6 Relatório final

No fim de cada auditoria a equipa responsável tem como obrigação a elaboração de um relatório de fim de auditoria, que deve conter determinadas informações padronizadas, como a data de início e fim da auditoria, todos os processos desenvolvidos ao longo do trabalho, as pessoas alvo de entrevista, os testes elaborados, as conclusões a que chegaram os auditores e possíveis alterações a desenvolver para melhorar o processo implementado na instituição. São abordados pelo relatório os seguintes pontos (Carneiro, 2009):

- **Introdução** – deve ser apresentada os objetivos propostos a alcançar com a auditoria a sistemas e identificar possíveis alterações se as mesmas tiverem sido efetuadas.
- **Âmbito e os objetivos da auditoria –** devem mostrar a extensão e profundidade da análise e o que se pretendia com a avaliação.
- **Áreas auditadas** – áreas que foram alvo de análise e validação, mais especificamente a estrutura orgânica e funcional da área de informática.
- **Apresentação dos indicadores de qualidade usados** – apresentação das técnicas utilizadas na auditoria, dos processos de medidas usados e a comparação com as de anos anteriores.
- **Situação atual** – identificação da situação em que se encontra a instituição, em relação ao hardware, software e o sistema de controlo interno.
- **Problemas encontrados** – descrição dos problemas detetados, dos pontos fracos e das eventuais ameaças.
- **Recomendações** – apresentação de orientações a seguir pela instituição para resolver situações menos corretas e que a entidade deve melhorar.
- **Avaliação final** – avaliação global do ambiente auditado.

O relatório de auditoria é para as instituições financeiras e restantes uma prova da sua qualidade, a sua confirmação de avaliação por parte de entidades certificadas que atesta a competência operacional da empresa. Este tipo de documento é uma arma potente para angariar clientes, pois a confiança que advém da certificação é uma das mais fortes campanhas de marketing que podem ser elaboradas. No corpo do relatório existem também, se disso for necessário, certas recomendações ou alertas de melhorias que podem ser implementadas na empresa, no sentido de ficar em concordância com a legislação local ou simplesmente otimizar os processos internos, que segundo os técnicos, não estão a atingir o máximo das suas potencialidades. Dependendo da sua substância, os relatórios podem ser classificados como preliminares ou finais, sendo que os primeiros são elaborados ao longo das diversas fases da auditoria, são de simples elaboração e contêm a opinião do auditor sobre os vários processos analisados, enquanto o relatório final deve demonstrar a totalidade dos processos e dados avaliados, indicar com o relevo necessário todas as deficiências encontradas e sugerir melhorias a efetuar para os problemas encontrados aquando da elaboração do trabalho.

6. Conclusão

No mundo financeiro atual, com a necessidade de satisfazer as necessidades e vontades dos clientes, a mínima vantagem pode significar uma melhoria considerável no que ao aumento de lucros diz respeito. O desenvolvimento informático facultou às instituições ferramentas bastante poderosas que permitem otimizar procedimentos internos e desenvolver produtos cada vez mais específicos e disponibiliza-los em qualquer parte do mundo. Foi referenciado ao longo desta dissertação as várias vantagens alcançadas com a implementação dos sistemas de informação por parte das entidades financeiras, mas ao mesmo tempo, as mesmas sofrem a pressão de riscos o que faz com que a implementação de controlos de segurança e risco sejam bastante importantes assim como o seu correto funcionamento. Na área da auditoria, quer em multinacionais como em revisoras oficiais de contas, a auditoria aos sistemas de informação das empresas em geral, e no âmbito deste trabalho, nas instituições financeiras em particular apenas é desenvolvido pelas grandes empresas da área da auditoria, seja por causa da aglutinação das grandes organizações financeiras na sua carteira de clientes seja por as empresas mais pequenas não possuírem recursos humanos especializados ou recursos financeiros para proceder a sua formação. As empresas que possuem instituições financeiras na sua carteira de clientes podem, com a pesquisa e o trabalho de formação correto, obter uma base para a elaboração de uma avaliação concreta dos controlos implementados na empresa auditada. As bases para a elaboração de uma auditoria a sistemas de informação encontram-se referenciadas nesta dissertação, o alcance à informação correta é bastante fácil, por exemplo, o ISACA possui um sítio na internet que disponibiliza as normas de auditoria que devem ser seguidas e muito mais informação relativa a *frameworks* de segurança e o ITIL concentra toda a informação necessária para o desenvolver de uma auditoria séria e específica, sendo que o auditor pode facilmente desenvolver o conhecimento necessário sobre os sistemas das instituições. O processo mais prático da pesquisa referente á elaboração concreta da auditoria permitiu identificar um padrão a seguir e que pode ser aplicado a qualquer validação de sistemas de qualquer empresa dada a sua generalidade. Os passos a desenrolar são idênticos, em termos teóricos, às auditorias financeiras sendo que a especial atenção é desenvolvida na avaliação dos controlos através de questionários e análises práticas dos métodos de segurança da empresa. O processo de auditoria a sistemas de informação de

instituições financeiras é um processo de difícil implementação, quer em termos de recursos humanos como de horas gastas, mas que depois de corretamente planeado e com o conhecimento correto da empresa é de extrema importância nos tempos atuais, tanto em termos de mercado como em termos de continuidade financeira da mesma.

7. Bibliografia

ABNT – Associação brasileira de normas técnicas – *ISO/IEC 27001:2006*. [em linha]. (Março 2006). [Consult. 26 Abr. 2012]. Disponível em: http://pt.scribd.com/doc/26489075/ABNT-NBR-ISO-IEC-27001.

CARNEIRO, Alberto – **Auditoria e controlo de sistemas de informação**. Lisboa: FCA, 2009. ISBN 978-972-722-407-4.

CARTLIDGE, Alison; HANNA, Ashley; RUDD, Colin; MACFARLANE, Ivor; WINDEBANK, John; RANCE, Stuart – **An introductory overview of ITIL v3**. UK chapter of the itSMF, 2007. ISBN 0-9551245-8-1.

CARVALHO, António A. Silva – Auditoria interna e sistemas de informáticos. Revista de economia, finanças e contabilidade. ISSN 0870-2241. 326(1992) 269-272.

CHAMPLAIN, Jack J. – **Auditing information systems - a comprehensive reference guide**. New Jersey: John Wiley & Sons, Inc, 1998. ISBN 0-471-16890-4.

ECIIA – EUROPEAN CONFEDERATION OF INSTITUTES OF INTERNAL AUDITING – **Banking internal auditing in Europe overview and recommendations by the banking advisory group**. Berlin: Erich Schmidt Verlag, 2009. ISBN 978-3-503-110-377.

ESTEVES, Rui Jorge Ferreira – *A implementação de boas práticas ITIL na administração pública – um estudo de caso*. [em linha]. (Setembro 2008) [Consult. 10 Mai. 2012]. Disponível em: http://repositorio-iul.iscte.pt/bitstream/10071/1973/1/A%20Implementa%C3%A7%C3%A3o%20das%20Boas%20Pr%C3%A1ticas%20ITIL%20na%20Administra%C3%A7%C3%A3o%20P%C3%BAblica%20%E2%80%93%20Um%20Estudo%20de%20Caso.pdf.

GONÇALVES, Rui Alexandre Henriques – *Sistemas de informação para a gestão de risco operacional em instituições financeiras*. [em linha]. (Abril 2011) [Consult. 24 Mai.2012]. Disponível em: https://www.repository.utl.pt/bitstream/10400.5/4264/1/TD-RAHG-2011.pdf.

GORGULHO, José Manuel António – *As melhores práticas de gestão de serviços tecnologias da informação – ITIL*. [em linha]. (2007) [Consult. 10 Mai. 2012]. Disponível em: http://comum.rcaap.pt/bitstream/123456789/1213/1/IESM2007_Jos%C3%A9%20Gorgulho.pdf.

IFAC – Auditoria num sistema computorizado. *Revista do órgão da associação portuguesa de contabilistas*. 26(1983) 7-10.

ISACA – *Cobit 4.1 Português*. [em linha]. 2007. [Consult. 06 Jan.2012]. Disponível em: http://www.isaca.org/Knowledge-Center/cobit/Documents/cobit41-portuguese.pdf.

ISACA – *Como o auditor de TI pode fazer contribuições substantivas para uma auditoria financeira*. [em linha]. 2011. [Consult. 27 Mar.2012]. Disponível em: http://www.isaca.org/Journal/Past-Issues/2011/Volume-1/Pages/How-the-IT-Auditor-Can-Make-Substantive-Contributions-to-a-Financial-Audit-Portuguese.aspx.

ISACA – *Padrão de auditoria de SI: Planeamento*. [em linha]. (Janeiro 2005). [Consult. 23 Fev.2012]. Disponível em: http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-IT-Portugese-S5.pdf.

ISACA – *Virtualização: Benefícios e desafios*. [em linha]. (Março 2011). [Consult. 15 Fev.2012]. Disponível em: http://www.isaca.org/Knowledge-Center/Research/Documents/Virtualization-WP-PT-BR-24March2011.pdf.

ITSMF INTERNATIONAL – **IT service management based on ITIL v3 – a pocket guide**. Van Haren Publishing, 2007. ISBN 978-90-8753-102-7.

MILLS, Annie – **Essential strategies for financial service compliance**. New Jersey: John Wiley & Sons, Ltd, 2008.ISBN 978-0-470-51907-2.

OLIVEIRA, José António – **Método de auditoria a sistemas de informação.** Porto: Porto Editora, 2006. ISBN 978-972-0-45021-0.

PEARLSON, Keri; SAUNDERS, Carol – **Strategic management of information systems**. New Jersey: John Wiley & Sons, Inc, 2009. ISBN 978-0-470-40024-1.

PEDRO, José Maria – A auditoria informática e a formação do auditor. *Boletim inspecção-geral das finanças*. 38/39 (1992) 9-21.

PEDRO, José Maria – Insegurança nos métodos de trabalho em auditoria decorrentes das diferenças entre os ficheiros de cartolina e os magnéticos. *Jornal de Contabilidade*. ISSN 0870-8789. 183 (1992) 142-146.

SANTOS, Pedro, FAIM, Carlos; SILVA, Pedro; MONTEIRO, Rui – *Auditoria em sistemas de informação*. [em linha]. [Consult. 08 Jan.2012]. Disponível em: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CE0QFjAB&url=http%3A%2F%2Fsubversion.assembla.com%2Fsvn%2FGSIDEI%2FAudit.pdf&ei=bNQ0UI-9JY6IhQev2oHYAw&usg=AFQjCNH9fLaorp5TYOPyb2dDJ5FErf0T3g.

SILVA, Pedro Manuel Gomes – *A função auditoria de sistemas de informação: Modelo funcional e de competências*. [em linha]. (Setembro 2007) [Consult. 28 Jan. 2012]. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/8058/1/Pedro%20Gomes%20Silva_A%20Funcao%20Auditoria%20de%20SI.pdf.

SINFIC - *Dez Razões Porque a Implementação do ITIL Falha nas Organizações*. [em linha]. (Novembro 2006) [Consult. 23 Abr. 2012]. Disponível na Internet em: http://www.sinfic.pt/SinficNewsletter/sinfic/Newsletter88/Dossier5.html

SINFIC - *Implementação do ITIL Numa Empresa de Seguros* [em linha]. (Janeiro 2007) [Consult. 18 Abr. 2012]. Disponível na Internet em: http://www.sinfic.pt/SinficNewsletter/sinfic/Newsletter98/Caso.html

WARREN JR, Donald; EDELSON, Lynn; PARKER, Xenia – **Handbook of IT auditing**. New York: Warren, Borham & Lament, 2000. ISBN 0-7913-3243-8.

8. Anexos

Todos os dados apresentados nos anexos são fictícios, dada a política de confidencialidade da empresa auditada.

8.1 Anexo1

1000 - Understand, evaluate and validate control components other than control activities - IT								
Ref.:	**Subprocesso**	**Actividade de Controlo**	**Preventivo ou detectivo**	**Automático / Manual**	**Frequencia**	**Deficiência de desenho identificada?**	**Procedimento de Teste**	**Resultado do Teste**
1	Control Environment - IT Governance	Existe um Plano Director dos Sistemas de Informação (ex:. Plano Estratégico) da Instituição (objectivos de médio e longo prazo) ajustado face aos seus objectivos globais.	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar a existência de um Plano Director dos Sistemas de Informação (ex:. Plano Estratégico) da Instituição (objectivos de médio e longo prazo) ajustado face aos seus objectivos globais.	No dia 08/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que existe um plano diretor para o departamento de IT, que se mantém inalterado desde 2003. De acordo com o Dr. Joaquim Henriques o plano já não reflecte a realidade da Companhia. Está prevista o desenvolvimento de um novo plano estratégico para a area de SI. **Com excepção** (Relatório -> 1.1)
2	Control Environment - IT Governance	Existe um Orçamento afecto à Área dos Sistemas de Informação (perspectiva de curto prazo).	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar a existência de um Orçamento afecto à Área dos Sistemas de Informação (perspectiva de curto prazo);	No dia 08/09/2010, verificámos junto da informação enviada pelo Dr. Joaquim Henriques (Director de IT) que existe Orçamento de custos sobre gestão para 2010 que define os limites máximos de recursos financeiros a alocar às diferentes actividades. Sem excepção
3	Control Environment - IT Roles and Competences	Existe uma Direcção/Departamento responsável pela gestão dos sistemas de informação da Instituição, encontrando-se formalizada a sua estrutura, sendo actualizada periodicamente pela área responsável.	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar a existência de um documento (organigrama) formal e completo que represente a Direcção/Departamento responsável pela gestão dos sistemas de informação da Instituição.	No dia 08/09/2010, verificámos com o Dr. Joaquim Henriques (Director de IT) que existe um organigrama, que representa a área de IT. Sem excepção
4	Control Environment - Human Resources	As funções e responsabilidades dos colaboradores das áreas de TI, internos e externos, encontram-se formalmente definidas, sendo actualizadas periodicamente pela área responsável.	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar se as funções e responsabilidades dos colaboradores das áreas de TI, internos, se encontram formalmente definidas.	No dia 08/09/2010, verificámos com o Dr. Joaquim Henriques (Director de IT) que existe um documento que descreve as responsabiliades e respectivas funções afectas a cada colaborador, verificámos também que este documento se mantém inalterado desde a data da última auditoria realizado. Tal facto deve-se a não terem ocorrido alterações na estrutura colaborativa da DSI da organização. Sem excepção
5	Risk Assessment - IT Objectives and Risks	Estão definidos contratos com todas as entidades externas que prestam serviços na área dos sistemas de informação, encontrando-se estes actualizados.	P	Manual	N/A	Não	Universo: Contratos existentes (total de 3) Amostra: Todos os contratos existentes Método: Examinar 1) Verificar se estão definidos contratos com todas as entidades externas que prestam serviços na área dos sistemas de informação, encontrando-se estes actualizados;	No dia 08/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que a Eurovida possui contratos com a IBM, Compta e Microsoft, que prestam serviços na área de SI. Obtivemos os contratos e constatamos que os contratos estavam: IBM - vigente e assinado I2S - vigente e assinado Sem excepções
6	Risk Assessment - Managing Changes in IT Risks	Existe um orgão (por ex: Comité de TI, composto pelos responsáveis das áreas dos sistemas de informação e áreas de negócio) que reúne periodicamente para efectuar um ponto de situação sobre os projectos dos Sistemas de Informação, e efectuar uma avaliação dos riscos existentes.	D	Manual	Semanal	Não	Universo: Actas das reuniões de 2010 Amostra: 5 ultimas actas das reuniões do periodo de 2010 Método: Examinar 1) Verificar a existência de um orgão (por ex: Comité de TI, composto pelos responsáveis das áreas dos sistemas de informação e áreas de negócio) que reúne periodicamente para efectuar um ponto de situação sobre os projectos dos Sistemas de Informação.	No dia 08/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que a Eurovida guarda um registo das reuniões de um comité de negócio que incorpora as funções de acompanhamento das áreas dos sistemas de informação. Este registo é efectuado sobre a forma de acta e atesta a realização das reuniões. Verificamos que se encontram formalizadas as actas referentes aos meses: 04-2010; 05-2010; 06-2010; 07-2010; 08-2010; Sem excepção

8.2 Anexo

3000- Computer Operations

Ref.:	Subprocesso	Actividade de Controlo	Preventivo ou detectivo	Automático / Manual / Ambos	Frequencia	Deficiência de desenho identificada?	Procedimento de Teste	Resultado do Teste
1	Overall management of computer operations activities	Estão definidos procedimentos formais de operações completos e detalhados, que são geridos de forma centralizada e actualizados sempre que ocorrem alterações nos sistemas.	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar se estão definidos procedimentos formais de operações completos e detalhados, e que são geridos de forma centralizada e actualizados sempre que ocorram alterações nos sistemas.	No dia 14/09/2010, verificamos junto da informação enviadao pelo Dr. Joaquim Henriques (Director de IT) que estão definidos procedimentos de operações completos e detalhados. Obtivemos um conjjunto de documentos que na sua totalidade compõem o manual de o
3	Batch scheduling and processing	Existe um procedimento formal para os processos "batch" que contempla: - o planeamento dos processos batch e respectiva actualização é realizada por colaboradores devidamente autorizados; - a documentação completa e detalhada relativa a resolução de "can	P	Manual	N/A	Não	Universo:N/A Amostra:N/A Método: Examinar 1) Obter o procedimento formal para o planeamento e execução dos processos batch.; 2) Verificar a existência de *checklists* de operações que permitam a avaliação dos controlos realizados na execução dos processo	No dia 14/09/2010, verificamos junto da informação enviada pelo Dr. Joaquim Henriques (Director de IT) que estão definidos os processos batch a correr na Eurovida, tal como o seu planeamento e execução. Esta informação esta incoporada no ficheiro "Procedi
4	Backup and Problem Management	Os dados e aplicações encontram-se adequadamente salvaguardados pela existência de uma política e procedimentos efectivos de backup, que descreva: - frequência dos mesmos; - abrangência (totais/incrementais, dados/aplicações, etc.); - procedimentos de rot	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter a Política Formal de Backups e os respectivos procedimentos actualmente em vigor na empresa; 2) Verificar se a documentação existente é suficiente, analisando nomeadamente a sua abrangência em relaçã	No dia 14/09/2010, verificamos junto da informação enviada pelo Dr. Joaquim Henriques (Director de IT) que está definida uma política formal de backups que não sofreu alterações desde a última auditoria. Mantendo-se assim o procedimento inadequado, uma v
5	Backup and Problem Management	São efectuados backups diários, semanais, mensais e anuais ao sistema GIS (produção).	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter a Política Formal de Backups e os respectivos procedimentos actualmente em vigor na empresa; 2) Analisar os logs dos backups seleccionados e verificar se estes estão em conformidade com as orientações	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques(Director de IT) que os backups são executados automaticamente via schedule do AS400 e Wintel. Obtivemos e consultamos os schedules, constatamos que os mesmos estavam devidamente parametrizados par
6	Backup and Problem Management	Existe uma revisão periódica dos logs de backup dos vários sistemas.	D	Manual	Diário	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter uma lista com todas as revisões realizadas aos logs de backups dos vários sistemas; 2) Obter evidências que garantam que uma efectiva de revisão de logs é periodicamente realizada na instituição.	No dia 14/09/2010, verificámos junto da informação enviada pelo Dr. Joaquim Henriques (Director de TI) a existência de um documento em excel onde são registados os resultados dos backups. Obtivemos dois ficheiros, um relativo aos Backups do Wintel e outro
7	Backup and Problem Management	Periodicamente são realizados testes de reposição/recuperação de backups aos sistemas mais importantes da entidade, sendo mandatória a participação activa dos utilizadores finais e a respectiva aprovação dos testes.	D	Ambos	N/A	Não	Universo:N/A Amostra: N/A Método: Examinar 1) Obter o planeamento e resultados dos últimos testes de reposição de backups realizados; 2) Analisar a extensão, adequadibilidade e documentação dos testes realizados.	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que não são realizados testes de reposição/recuperação de backups periodicamente aos sistemas mais importantes. **Com excepções** (Relatório -> 3.1)

2

3000- Computer Operations								
Ref.:	**Subprocesso**	**Actividade de Controlo**	**Preventivo ou detectivo**	**Automático / Manual / Ambos**	**Frequencia**	**Deficiência de desenho identificada**	**Procedimento de Teste**	**Resultado do Teste**
8	Backup and Problem Management	As tapes dos backups efectuados aos sistemas mais importantes da Entidade, são armazenadas em local próprio e seguro, inclusive num local relativamente distante das instalações principais (Armazenamento remoto)	P	Manual	N/A	Não	Universo:N/A Amostra: N/A Método: Inquirir e Examinar 1) Inquiri os responsáveis sobre o local onde são armazenadas as tapes de Backup (Internamente e externamente) 2) Verificar se, internamente, as tapes são guardadas em local próprio e seguro n(e.g.:	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT), que as tapes são guardadas em local próprio e seguro (i.e cofre). Adicionalmente verificamos a existência de uma folha de controlo onde são assinaladas quais as tapes que são ar
9	Disaster Recovery	Um Plano de Recuperação de Desaste (DRP - Disaster Recovery Plan) está definido e implementado na entidade, sendo revisto e actualizado periodicamente, de forma a reflectir as alterações ocorridas nos equipamentos da empresa.	P	Manual	N/A	**Sim**	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar a existência de um Plano de Recuperação de Desaste (DRP - Disaster Recovery Plan) definido e implementado na instituição, e se este é revisto e actualizado periodicamente, de forma a reflectir as	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) a existência de um DRP formalizado dentro do BCP. No entanto, verificamos que não foram efectuadas alterações ao plano existente desde Novembro de 2004 e com as alterações que a S
10	Disaster Recovery	Um Plano de Continuidade de Negócio está definido e implementado na instituição, sendo revisto e actualizado periodicamente, de forma a reflectir as alterações ocorridas na empresa.	P	Manual	N/A	**Sim**	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar a existência de um Plano de Continuidade de Negócio definido e implementado na instituição, e se este é revisto e actualizado periodicamente, de forma a reflectir as alterações ocorridas na empres	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) a existência de um BCP formalizado. No entanto, verificamos que não foram efectuadas alterações ao plano existente desde Novembro de 2004. **Com excepções** (Relatório -> 3.3)
11	Disaster Recovery	Periodicamente, são realizados testes ao Plano de Recuperação de Desastre, nos quais são realizados testes que requerem a participação activa dos utilizadores finais e a respectiva aprovação dos testes.	P	Manual	N/A	**Sim**	Universo: Relatório de testes ao Plano de Recuperação de Desastre Amostra: Último relatório de testes ao Plano de Recuperação de Desastre Método: Examinar 1) Obter as evidências dos últimos testes realizados ao Plano de Recuperação de Desastre; 2) Anali	No dia 14/09/2010,verificamos com o Dr. Joaquim Henriques (Director de IT) que não são realizados testes ao Plano de Recuperação de Desastre. **Com excepções** (Relatório -> 3.2)
12	Disaster Recovery	Periodicamente, são realizados testes ao Plano de Continuidade de Negócio, nos quais são realizados testes que requerem a participação activa dos utilizadores finais e a respectiva aprovação dos testes.	P	Manual	N/A	**Sim**	Universo: Relatório de testes ao Plano de Continuidade de Negócio Amostra: Último relatório de testes ao Plano de Continuidade de Negócio Método: Examinar 1) Obter as evidências dos últimos testes realizados ao Plano de Continuidade de Negócio; 2) Anali	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que não são realizados testes ao Plano de Continuidade de Negócio. **Com excepções** (Relatório -> 3.3)

8.3 Anexo 3

1500 - Program Changes and Program Developments								
Ref.:	**Subprocesso**	**Actividade de Controlo**	**Preventivo ou detectivo**	**Automático / Manual / Ambos**	**Frequencia**	**Deficiência de desenho identificada ?**	**Procedimento de Teste**	**Resultado do Teste**
1	Management of Maintenance Activities	Está definida uma metodologia standard e formal de desenvolvimento e alteração a sistemas.	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter a Metodologia de Gestão de Alterações e/ou Desenvolvimentos existente na empresa e verificar se a mesma contempla todas as fases do ciclo de desenvolvimento de sistemas.	No dia 15/09/2010, verificamos com o Dr. Joaquim Henriques (Director de Informática) que no âmbito do processo de gestão de alterações não esta definida uma metodologia formal de suporte ao processo. **Projecto Upgrade GIS** A instituição no que diz respeito ao projecto de upgrade do GIS possui um cronograma que contempla o procedimento a ser seguido para implementação das actualizações a serem efectuadas no sistema GIS. Obtivemos o cronograma de 2009 dado que até à data ainda não se realizou um upgrade em 2010 e constatamos que o mesmo contemplava devidamente os passos a serem efectuados para implementação da actualização que ocorreu em 2009. **Com excepções.** (Relatório -> 2.1)
2	Specification, Authorisation and Tracking of Change Requests	Existe uma formalização, registo e acompanhamento do pedido de alterações às aplicações.	P	Manual	N/A	Não	Universo: Pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total de 4) e o projecto de upgrade ao GIS em 2009 Amostra: Todos os pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total 4) e o projecto de upgrade ao GIS em 2009 Método: Examinar 1) Obter a Metodologia de Gestão de Alterações e/ou Desenvolvimentos existente na empresa; 2) Analisar a existência de uma formalização dos pedidos de alteração; 3) Verificar se os técnicos dos Sistemas de Informação encarregues registam e acompanham o estado do pedido.	No dia 15/09/2010, obtivemos com o Dr. Joaquim Henriques (Director de Informática) a lista de pedidos de alterações ao sistema GIS. Dos 4 pedidos contatamos que um tinha sido cancelado. Desta forma a amostra de pedidos de alteração ficou reduzida a 3 pedidos. Os pedidos de alteração ficam registados numa ferramenta propria verificamos o registo formal dos pedido de alteração na ferramenta CSU.net. Sem excepção **Projecto Upgrade GIS** No âmbito do projecto de Upgrade do GIS a existência de um pedido de alteração não é aplicavel dado que este upgrade esta previsto nos termos do contrato estabelecido entre a instituição e a I2S. Sem excepção
3	Specification, Authorisation and Tracking of Change Requests	Antes da alteração ser efectuada, existe uma avaliação funcional, técnica e/ou de impacto, bem como a respectiva aprovação formal.	P	Manual	N/A	Não	Universo: Pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total de 4) e o projecto de upgrade ao GIS em 2009 Amostra: Todos os pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total 4) e o projecto de upgrade ao GIS em 2009 Método: Examinar 1) Verificar a existência de uma análise funcional, técnica e/ou de impacto para cada um dos pedidos aleatoriamente seleccionados, e verificar se estes se encontram formalmente aprovados.	No dia 15/09/2010, obtivemos com o Dr. Joaquim Henriques (Director de Informática) a lista de pedidos de alterações ao sistema GIS. Dos 4 pedidos contatamos que um tinha sido cancelado. Desta forma a amostra de pedidos de alteração ficou reduzida a 3 pedidos. A ferramenta CSU.net para alem de premitir e registar os pedidos de alteração, suporta também trocas de informação entre os intervenietes, tal como uma ferramenta de gestão de alterações, podemos constatar que foi efectuada uma análise da situação para os casos em que se justifica, dada a natureza dos pedidos de alteração. Sem excepção **Projecto Upgrade GIS** A Popular Seguros no que diz respeito ao projecto de upgrade do GIS possui documentação técnica e funcional fornecida pela I2S de modo a suportar o processo de upgrade à aplicação. Sem excepção

4	Testing and Quality Assurance	Realização, manutenção e registo da aceitação dos testes efectuados pelos utilizadores finais/key-users.	P	Manual	N/A	Não	Universo: Pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total de 4) e o projecto de upgrade ao GIS em 2009 Amostra: Todos os pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total 4) e o projecto de upgrade ao GIS em 2009 Método: Examinar 1) Obter o resultado dos testes efectuados pelos utilizadores finais ou *key-user* ; 2) Verificar se os resultados dos testes foram aprovados pelo utilizador/*key-user* que requereu a alteração/ desenvolvimento.	No dia 15/09/2010, obtivemos com o Dr. Joaquim Henriques (Director de Informática) a lista de pedidos de alterações ao sistema GIS. Dos 4 pedidos contatamos que um tinha sido cancelado. Desta forma a amostra de pedidos de alteração ficou reduzida a 3 pedidos. A ferramenta CSU.net para alem de premitir e registar os pedidos de alteração, suporta também trocas de informação entre os intervenietes, tal como uma ferramenta de gestão de alterações, podemos constatar que foi efectuada uma análise da situação para os casos em que se justifica, dada a natureza dos pedidos de alteração. Sem excepção Projecto Upgrade GIS A instituição no que diz respeito ao projecto de upgrade do GIS verificamos a existência de trocas de emails confirmando a realização de testes, adicionalmente verificámos a existência de baterias de testes tal como os resultados dos testes efectuados aos diferentes módulos da aplicação GIS. Sem excepção
5	Program Implementation	As alterações/desenvolvimentos são aprovadas formalmente pelos responsáveis (key-user, área dos SI, etc.) antes do seu transporte para Produção.	P	Manual	N/A	Não	Universo: Pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total de 4) e o projecto de upgrade ao GIS em 2009 Amostra: Todos os pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total 4) e o projecto de upgrade ao GIS em 2009 Método: Examinar 1) Verificar se a aprovação da passagem para produção das alterações se encontra devidamente aprovada e documentada.	No dia 15/09/2010, obtivemos com o Dr. Joaquim Henriques (Director de Informática) a lista de pedidos de alterações ao sistema GIS. Dos 4 pedidos contatamos que um tinha sido cancelado. Desta forma a amostra de pedidos de alteração ficou reduzida a 3 pedidos. A ferramenta CSU.net para alem de premitir e registar os pedidos de alteração, suporta também trocas de informação entre os intervenietes, tal como uma ferramenta de gestão de alterações, podemos constatar que foi efectuada uma aprovação da passagem para produção. Sem excepção **Projecto Upgrade GIS** A instituição no que diz respeito ao projecto de upgrade do GIS possui documentada a aprovação da passagem para produção Sem excepção
6	Segregation of Duties	As responsabilidades relacionadas com o processo de gestão de alterações estão segregadas da seguinte forma: - Os programadores apenas acedem ao ambiente de Desenvolvimento; - O ambiente de teste apenas é acedido pelos utilizadores finais no período de teste; - O transporte de alterações entre os ambientes de Teste e Produção é realizado por pessoa independente de quem realiza o desenvolvimento.	P	Manual	N/A	Não	Universo: Pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total de 4) Amostra: Todos os pedidos de alteração e/ou desenvolvimento ocorridos em 2010(total 4) Método: Inquirir ou observar ou examinar 1) Verificar a existência de evidências que garantam que existe uma adequada segregação de funções ao longo do processo de gestão de alterações.	No dia 15/09/2010, verificamos via indagação e observação com o Dr. Joaquim Henriques que existe uma adequada segregação de funções uma vez que as alterações ao sistema GIS implementadas na instituição são efetuadas externamente, pela I2S. Esta segregação de funções no processo é evidênciada no documento em anexo "Pedidos de alteracao 2010.pdf", e pelo contrato com o fornecedor I2S; Sem excepções
7	Segregation of Duties	Os ambientes de desenvolvimento, de testes e o ambiente de produção estão separados lógica e/ou fisicamente e são tecnicamente idênticos ou muito semelhantes.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Observar 1) Verificar se os ambientes de desenvolvimento, de testes e o ambiente de produção estão separados lógica e/ou fisicamente e são tecnicamente idênticos ou muito semelhantes.	No dia 15/09/2010, verificamos com o Dr. Joaquim Henriques (Director de Informática) que existem três ambientes segregados, sendo eles: - GIVEUV = Produção - GIVEUT = Testes (utilizado para testes de negócio) - GIVEUU = Upgrade (utilizado para testes de upgrade) Consultamos cada ambiente e constatamos que os mesmos estavam devidamente segregados. Sem excepções

8.4 Anexo 4

5000 - Access to Programs and Data								
Ref.:	**Subprocesso**	**Actividade de Controlo**	**Preventivo ou detectivo**	**Automático / Manual / Ambos**	**Frequencia**	**Deficiência de desenho identificada?**	**Procedimento de Teste**	**Resultado do Teste**
1	Management of security activities	Está definida uma Política de Segurança formal, documentada e divulgada a todos os colaboradores da empresa.	P	Manual	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter a política de segurança actualmente em vigor na instituição; 2) Verificar se esta se encontra direccionada, tanto para os utilizadores finais, como para utilizadores de administração, e se contempla to	No dia 14/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que existe uma política de segurança formalizada, que se encontra disponível na intranet da instituição para acesso e conhecimento de todos. Adicionalmente verificamos que está a
2	Security Administration	A gestão de acessos de utilizadores é adequadamente realizada e de acordo com a política e procedimentos formais em vigor na entidade. A gestão de acessos inclui: - a criação de novos utilizadores, eliminação de utilizadores e alteração de funções e comp	P	Manual	N/A	Não	Universo: Novos utilizadores dos sistemas AS400/windows, utilizadores que viram os seus acessos alterados e utilizadores com acessos removidos (total de 15 entradas e 1 saída) Amostra: 5 entradas aleatórias e todos os utilizadores removidos (total de 1)	Verificamos em 14/09/2010 com o Dr. Joaquim Henriques(Director de TI), que a gestão de utilizadores é efectuada pela área de TI com base nas solicitações do RH. Para o teste de novos acessos, selecionamos aleatoriamente 5 casos e constatamos que todos for
3	Security Administration	Existe uma revisão periódica dos utilizadores com "perfis poderosos" definidos nos sistemas em análise, que garante que estes estão atribuídos, ao longo do tempo, de acordo com as funções desempenhadas pelos colaboradores. E efectuado um análise periódico	D	N/A	N/A	Não	Universo:N/A Amostra: N/A. Método: Examinar 1) Obter uma lista com todas as revisões de acessos ocorridas no período em análise. 2) Analisar uma amostra de relatórios de revisão periódica de acessos e verificar os procedimentos adoptados e o trabalho rea	Verificamos em 14/09/2010, com o Dr. Joaquim Henriques, que foi iniciado um processo de revisão de revisão periódica do acesso dos utilizadores ao sistema GIS nomeadamente Este processo está a cargo de auditoria interna e é efectuado numa base semestral. Como evidência do procesos de revisão de acessos e tal como acordado na reunião de Kick-off obtivémos evidência de Revisão periódica dos perfis e acessos de utilizadores aos Sistemas de Informação -um caso de documento final com assinaturas. Sem excepção

4	Data Security	O sistema de anti-virús instalado nos servidores e estações de trabalho da empresa encontra-se actualizado com a versão mais recente.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter e analisar o procedimento de actualização do anti-virús nos servidores e nas estações de trabalho; 2) Obter a configuração do sistema de anti-virús em todas estações de trabalho seleccionadas aleatoria	No dia 15/09/2010, verificamos junto do Dr. José Ferreira (Infra-estrutura) que se encontra instalado na instituição o antivírus Trend Micro. O antivírus está presente em todos os workstations com sistema operativo windows. Verificámos que existe um servidor que acede directamente a internet numa base diária e verifica se existem actualizações disponíveis. Caso existam, este procede à actualização do antivírus e replica as actualizações para as diversas workstations. Verificámos através da consola de gestão de antivírus que para todas as workstations (excepto uma, devido à colaboradora estar de férias) o antivírus encontrava-se instalado e devidamente actualizado. Sem excepção
5	Network Security	São utilizados firewalls para controlo de tráfego nas ligações à internet. As regras de firewall definidas abrangem protocolos críticos e restringem a sua utilização, de acordo com os interesses de segurança da entidade.	P	Automático	N/A	Não	Universo:N/A Amostra:N/A Método: Examinar 1) Obter as regras de acesso na firewall e verificar a adequadibilidade das mesmas;	No dia 15/09/2010, verificamos junto da informação cedida pelo Dr. Joaquim Henriques (Director de IT) que existem mecanismos de firewall activos com regras especificas configuradas. Sem excepção
6	Network Security	Existe um IDS (Intrusion Detection System) OU IPS (Intrusion Prevention System) para monitorizar/alertar sobre acessos indevidos no website da empresa a partir da Internet.	D	Automático	N/A	Não	Universo:Relatórios do sistema IDS Amostra: Último relatórios do sistema IDS. Método: Examinar 1) Obter e verificar a configuração do IDS; 2) Verificar os relatórios gerados pelo IDS para um dia seleccionado aleatoriamente e analisar a actividade gerada	No dia 15/09/2010, verificamos junto do Dr. José Ferreira (Infra-estrutura) que se encontra instalado e activo um sistema de IDS, o fornecedor da tecnologia é a IBM, e apresenta-se sobe forma de software e de hardware. Sem excepção
7	Physical Security	As condições físicas e ambientais são adequadas.	P	Ambos	N/A	Não	Universo: N/A Amostra: N/A Método: Observar 1) Verificar as condições físicas e ambientais do Datacenter, nomeadamente: - Sistema de Ar-Condicionado; Equipamentos de detecção e extinção de incêndios; Equipamentos de Detecção de inundação; UPS's e/ou Ger	No dia 15/09/2010, visitamos o Datacenter junto do Dr. Joaquim Henriques, e verificamos que as condições físicas e ambientais se encontravam adequadas. Foi possivel detectar: Controlo de segurança ambiental e fisica do Datacenter Piso falso, O mecanismo de medição de temperatura está ligado ao sistema central de alarme que em casos da temperatura atingir níveis elevados despoleta um sinal de alarme para a central. Sistema de detecção de inundação e um sistema de escoamento de água debaixo do piso falso; Sistema de detecção de incêndio; Sistema de extinção de fogo através de gás; Sistema de detecção de sismos; Sistema de ar-condicionado redundante, com alarme de temperatura (e.g.no caso da temperatura subir acima da temperatura estabelecida, é disparado um alarme, que é verificado pela DMM e pela segurança do edifício); 2 UPSs de 320 Watts e com autonomia total de 1/2 horas mediante o consumo energético a que são submetidas; Gerador do edifício (900 * 2 Watts). Extintor dentro e fora da sala. um ponto de acesso único ao Datacenter; O acesso ao Datacenter é restrito via utilização de um cartão previamente autorizado e combinado com a utilização obrigatória de um PIN. Os cartões são controlados pela DMM (Direcção de Manutenção e Materiais). O acesso ao Datacenter por entidades externas, só é permitido quando acompanhado de um técnico do Banco - Politica de Controled Visitors Access; Dead man door (2 portas de acesso); Duas câmaras (Dentro e fora da Sala) de vigilância que funcionam 24h por 24h, que são monitorizadas pela segurança; Sem excepção

8.5 Anexo 5

OS/400								
Ref.:	**Subprocesso**	**Actividade de Controlo**	**Preventivo ou detectivo**	**Automático / Manual / Ambos**	**Frequencia**	**Deficiência de desenho identificada?**	**Procedimento de Teste**	**Resultado do Teste**
1	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	As seguintes configurações de segurança lógica estão adequadamente implementadas ao nível do OS/400: 1) Comprimento mínimo da password; 2) Prazo de expiração da password; 3) Composição das Passwords; 4) Histórico de passwords; 5) Número de tentativas fal	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Perfis de administração (SECOFR e SECADM). Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar quais as contas de utilizadores activas que têm os perfis SECOFR ou SECADM e verificar se os mesmos estão correctamente atribuídos.	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos os seguintes utilizadores ativos com perfil SECOFR: CMARQUES; EFRANCO; IROLAO; I2SHC; I2SJO; I2SPR; JFIGUEIRED; MMENDONCA; PSCORE; QSECOFR; REMOTO;SYSUSR; Identificamos um utilizador com o perfil SECADM: I2SARO Com excepção (Relatório -> 4.4)
2	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	Os perfis de administração definidos no sistema OS/400 (SECOFR e SECADM) estão restritos a elementos autorizados.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Utilizadores da área de desenvolvimento. Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar se existem programadores activos com acesso ao ambiente de produção, analisando os utilizadores com perfil PGMR (campo UPUSCL) e o o campo UPTEXT (descrição do utilizador); 4) Analisar as autoridades especiais (campo UPSPAU) e verificar se estão correctamente atribuídas.	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos 63 utilizadores ativos com perfil PGMR, destes 63 59 correspondem a colaboradores da I2S, incluindo uma conta de utilizador com a seguinte descrição genérica:"I2___USR"; **Com excepção** (Relatório -> 4.4)
3	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	No ambiente de produção, perfis poderosos e autoridades especiais alargadas não estão atribuídos a programadores.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Utilizadores da área de desenvolvimento. Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar se existem programadores activos com acesso ao ambiente de produção, analisando os utilizadores com perfil PGMR (campo UPUSCL) e o o campo UPTEXT (descrição do utilizador); 4) Analisar as autoridades especiais (campo UPSPAU) e verificar se estão correctamente atribuídas.	No dia 15/09/2010 , obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos apenas o utilizador de sistema QSYSOPR com perfil SYSOPR. Sem excepção

4	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	O perfil SYSOPR está apenas atribuído a elementos que necessitem dos seus privilégios, nomeadamente aqueles pertencentes à área de Operações.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Utilizadores com perfil SYSOPR. Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar quais as contas de utilizadores activas com o perfil SYSOPR atribuído (campo UPUSCL); 4) Verificar se estas contas estão atribuídas a elementos da área de operações.	No dia 15/09/2010 , obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos apenas o utilizador de sistema QSYSOPR com perfil SYSOPR. Sem excepção
5	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	As autoridades especiais alargadas apenas estão atribuídas aqueles utilizadores que delas necessitam especificamente para realizarem as suas funções.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Utilizadores activos com autoridades especiais (campo UPSPAU diferente de *NONE). Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar quais os utilizadores activos com o campo UPSPAU diferente de *NONE; 4) Verificar se as autoridades especiais estão adequadamente atribuídas.	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos 111 utilizadores ativos com perfil UPSPAU diferente de NONE. Neste universo 102 utilizadores possuem premissões *ALLOBJ. **Com excepção** (Relatório -> 4.4)
6	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	O acesso à linha de comandos está restrito aqueles utilizadores que necessitam especificamente dessa permissão para realizarem as suas tarefas.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles) e valores de sistema (System Values). Amostra: Utilizadores activos com acesso à linha de comandos (campo UPLTCP igual a *NO), com acesso ao menu MAIN (campo UPINMN igual a MAIN) e/ou acesso ao programa ASSIST (valor sistema QATNPGM diferente de *ASSIST). Método: Examinar 1) Obter os relatórios de Valores de Sistema (System Values) e Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar quais as contas de utilizadores activos que podem aceder à linha de comandos (campo UPLTCP igual a *NO); 4) Verificar quais são as contas de utilizadores que têm menú inicial MAIN (campo UPINMN igual a MAIN) 5) Verificar se o parâmetro de segurança QATNPGM (valor de sistema) está definido para que o programa ASSIST (IBM Operational Assistant) não seja chamado cada vez que um utilizador do sistema utiliza a attention key (valor dwe sistema QATNPGM diferente de *ASSIST). No entanto, somente se o utilizador possuir o valor QCMD ou QCL no campo UPATPG é que o menu será o inicial, caso contrário o acesso é limitado ao perfil do utilizador."	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos 66 utilizadores com acesso à linda de comandos. Deste 74 utilizadores existem 74 com acesso ao menu inicial (MAIN). No entanto nenhum dos utilizador possuir o valor QCMD ou QCL no campo UPATPG logo o acesso é limitado ao perfil do utilizador. Consultamos o valor do sistema QATNPGM e constatamos que o mesmo não está diferente de *ASSIST. Sem excepção

7	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	Não existem contas activas adormecidas no sistema OS/400, e as que existem estão apropriadamente justificadas.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Utilizadores activos (campo UPPSOD não preenchido/em branco). Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar se existem contas de utilizadores que nunca se autenticaram no sistema OS/400 (campo UPPSOD não preenchido/em branco)	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos 17 utilizadores adormecidos no sistema, ou seja, que nunca se autenticaram no sistema. **Com excepção** (Relatório -> 4.4)
8	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	Os utilizadores de sistema criados por defeito estão inactivos. As excepções estão devidamente justificadas.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Contas de utilizadores que vêm por defeito com o OS/400. Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar quais as contas de utilizadores de sistema (que vêm por defeito com o OS/400) que estão activas e com password atribuída.	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos 3 utilizadores de sistema (que vêm por defeito com o OS/400) que estão activas e com password atribuída), estes são os seguintes: QPGMR QSRVBAS QSYSOPR **Com excepção** (Relatório -> 4.4)
9	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	Todos os utilizadores têm o menú inicial "SIGNOFF". As excepções estão devidamente justificadas.	P	Automático	N/A	Não	Universo:Relatório dos perfis de utilizadores (User Profiles). Amostra: Utilizadores activos com acesso ao Menu SIGNOFF (campo UPINMN diferente de *SIGNOFF). Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 2) Verificar quais as contas de utilizadores activas que têm um menú inicial igual a *SIGNOFF (campo UPINMN igual de *SIGNOFF); 3) Verificar se existem excepções e se estas estão devidamente justificadas.	No dia 15/09/2010, obtivemos o relatório com os perfis de utilizadores AS/400 com o Dr. Joaquim Henriques (Director de IT) e identificamos 78 utilizadores ativos com menu inicial diferente de SIGNOFF e 68 com o valor de STRMNA (menu inicial padrão). **Com excepção** (Relatório -> 4.4)
10	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	Existem os seguintes procedimentos de controlo: _As contas de utilizadores definidas no sistema são criadas tendo por base perfis pré-definidos de grupos de utilizadores. _Não existem contas genéricas ou com descrição genérica activas no sistema. A existirem, essas contas deverão estar formalmente justificadas e aprovadas. _Não se encontram activas contas de utilizadores pertencentes a colaboradores que já abandonaram a instituição.	P	Automático	N/A	Não	Universo: Perfis de utilizadores (User Profiles). Amostra: Contas de utilizadores activas Método: Examinar 1) Obter o relatório de Perfis de Utilizadores (User Profiles); 2) Seleccionar todos os utilizadores activos (campo UPPSTAT = *ENABLED) e com password atribuída (campo UPPWON =*NO), realizando a análise apenas sobre utilizadores que têm a possibilidade de se autenticar no sistema operativo; 3) Verificar a existência de contas de utilizadores, genéricos ou com descrição genérica, definidas no sistema; 4) Avaliar a adequabilidade e a necessidade de existirem contas genéricas. 5) Verificar se se encontram activas contas de utilizadores pertencentes a colaboradores que já abandonaram a instituição.	No dia 15/09/2010 verificamos, a existência de contas com descrição genérica no sistema. Alguns exemplos dessas contas são: - EGISUSR; - EXPLORA; - GUEST; - I2CTLUSR; - LUSODATA; - REMOTO; - etc.. Verificamos que se se encontram activas contas de utilizadores pertencentes a colaboradores que já abandonaram a instituição: ex: Nuno Ferreira **Com excepção** (Relatório -> 4.4)

11	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	O sistema encontra-se a registar num log/jornal de auditoria eventos previamente definidos.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter evidência do registo de um journal que regista os eventos criticos definidos para o sistema;	No dia 15/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que o log de auditoria está activo para os eventos considerados críticos para a Companhia. Consultamos a configuração do sistema AS400 e constatamos que os logs estavam activos para o módulo de apólices, sinistros e contabilidade. O log regista todos os dados das alterações efectuadas, desde utilizador, data e hora, até dado anterior e dado posterior a alteração. Verificamos que estão registados os logs relativos aos meses de Janeiro a Agosto de 2010. Sem excepção
12	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	Existe uma revisão periódica dos logs de auditoria pelos elementos responsáveis pela administração do sistema operativo.	D	Manual	N/A	Sim	Universo:Logs de auditoria e relatório de monitorização. Amostra: Logs de auditoria e relatório de monitorização XXXX (a preencher) Método: Examinar 1) Verificar se os logs gerados são formalmente verificados e se esta análise é documentada.	No dia 15/09/2010, verificamos com o Dr. Joaquim Henriques (Director de IT) que não existe monitorização dos logs de auditoria do AS400. **Com excepção** (Relatório -> 4.3)
13	Segurança do Sistema Operativo - **OS/400 - Obrigatório**	As ferramentas e funcionalidades poderosas do sistema, como DFU (Data File Utility) e SEU (Source Entry Utility), estão disponíveis apenas para colaboradores devidamente autorizados.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter e verificar a adequabilidade dos acessos aos seguintes programas e funcionalidades sensíveis do sistema como, por exemplo: - SST (System Service Tools) - DFU (Data File Utility) - Query/400 (STRQRY/WRKQRY); - SEU (Source Entry Utility). 2) Analisar quais as contas de utilizadores com acesso ao comando CHGDSTPWD, verificando que as autoridades específicas "ALL" e "CHANGE" estão atribuídas exclusivamente a colaboradores devidamente autorizados.	No dia 15/09/2010, verificamos a adequabilidade dos acessos aos seguintes programas e funcionalidades sensíveis do sistema do AS/400 junto da informação cedida pelo Dr. Joaquim Henriques (Director de IT) e verificamos os seguintes atributos: DFU (Data File Utility): *PUBLIC tem *USE, pelo que todos os utilizadores com acesso à linha de comandos podem executar este programa. QSYS tem autoridade especifica *ALL sobre o objecto. SEU(Source Entry Utility): *PUBLIC tem *USE, pelo que todos os utilizadores com acesso à linha de comandos podem executar este programa. Query/400: STRQRY *PUBLIC tem *USE, pelo que todos os utilizadores com acesso à linha de comandos podem executar este programa. QSYS tem autoridade especifica *ALL sobre o objecto. WRKQRY *PUBLIC tem *USE, pelo que todos os utilizadores com acesso à linha de comandos podem executar este programa. SST *PUBLIC tem *EXCLUDE, pelo que todos os utilizadores com acesso à linha de comandos não podem executar este programa. *QSYS tem autoridade especifica *ALL sobre o objecto. *QSRV tem *USE sobre o objecto. Acesso ao comando CHGDSTPWD *PUBLIC tem *USE, pelo que todos os utilizadores com acesso à linha de comandos podem executar este programa.
14	Segurança do Sistema Operativo - **OS/400**	Os atributos de rede "Job action network attribute" (JOBACN) e "DDM Request access network attribute" (DDMACC) estão adequadamente configurados, garantindo uma maior segurança dos acessos remotos ao sistema.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Obter o relatório "Network Attributes" (NETA); 2) Verificar se o parâmetro "Job action" (JOBACN) está configurado com o valor *REJECT. Caso não esteja, avaliar se o valor definido está de acordo com as necessidades da empresa; 3) Verificar se o parâmetro "DDM request access" (DDMACC) está configurado com o valor *OBJAUT (acessos remotos são controlados através das autoridades sobre os objectos no sistema). Caso não esteja, avaliar se o valor definido está de acordo com as necessidades da empresa.	No dia 15/09/2010, obtivemos o relatório com os atributos de rede do AS/400 junto do Dr. Joaquim Henriques (Director de IT) e verificamos os seguintes atributos: JOBACN - *FILE (de acordo com necessidades da empresa); DDMACC - *OBJAUT. Sem excepção

8.6 Anexo 6

PLANO DE RECUPERAÇÃO DE DESASTRE

DESCRIÇÃO DO PLANO DE RECUPERAÇÃO DE DESASTRE DE UMA SEGURADORA

Informação de versão

Versão	Alteração	Responsável	Data
0.1	Draft Inicial	Tiago Cascais	3-Out-2008
0.2	Inclusão de IP's dos servidores remotos	Tiago Cascais	14-Nov-2008
0.3	Revisão da lista de linhas a reenviar	Tiago Cascais	23-Set-2009
0.4	Revisão da lista de linhas a reenviar; alteração de contactos da PT	Tiago Cascais	20-Set-2010

Uma cópia Online do servidor de Base de Dados será mantida, juntamente com um Terminal Server, no CS da instituição.

Em caso de desastre, irá ser solicitada à Portugal Telecom o reenvio de todas as chamadas dirigidas à instituição para o Contact Center do grupo e será activada a cópia Online do servidor de Base de Dados. Isto permitirá que através de sessões de terminal no Contact Center do grupo, se continue a trabalhar na aplicação de negócio.

Objectivos deste Documento

1) Definir o que pode ser considerado uma situação de desastre;

2) Definir quem tem poderes para activar o Plano de Recuperação de Desastre;

3) Descrever os passos de activação do plano.

Definição de Situação de Desastre

Para efeitos deste documento, é definida como situação de desastre toda a conjuntura que implique paragem total das instalações da instituição por período de duração superior ou igual a uma hora.

> Em caso de desconhecimento da duração da paragem deverá ser usada uma estimativa.

Quem pode activar o Plano de Recuperação de Desastre

O Plano de Recuperação de Desastre pode ser activado pelas seguintes pessoas:

1) Sérgio Penim – sergio.penim@instituição.pt;

2) Zélia Martins – zelia.martins@ instituição.pt;

3) Tiago Cascais – tiago.cascais@ instituição.pt.

Plano de Recuperação de Desastre

Solicitação de reenvio das linhas de entrada da Portugal Telecom

Contactos para efectuar pedido de reenvio

4) David Nunes – david.g.nunes@telecom.pt – 92 740 13 40 / 21 500 06 63;

5) PT Centro de Suporte a Clientes – Grupo da instituição

Procedimento de colocação em produção do servidor em Standby

Descrição dos Servidores no site remoto

Servidor	Papéis	IP	Sistema Operativo	Software	Hardware
EAP-BCM	Servidor de Base de Dados Oracle e Virtual Server	10.100.148.187	Windows Server 2003 R2 Standard 64-Bit	Oracle Server; Virtual Server 2005 R2 Enterprise	HP Proliant DL320 G5p; 1 Intel Xeon Quad-Core 2.2 GHz; 4GB Ram; 2 * 500GB SATA Raid1 HD
EAP-BCMTS	Terminal Server	10.100.148.188	Windows Server 2000 Standard	PIE96, Microsoft Office 2002	Servidor Virtual; 1 Core, 1GB Ram, 16GB HD

Passos para activação da Base de Dados em Stand-By

6) Fazer login no EAP-BCM com o utilizador local Administrator;

7) Aguardar até pararem as *scheduled tasks* "Aplicar Logs" e "Apagar Logs Antigos", e fazer-lhes *disable*;

8) Na linha de comando iniciar a base de dados com os seguintes comandos a serem corridos numa janela de *command prompt*:

9) sqlplus / as sysdba

10) alter database open resetlogs;

Em "C:\migracoes" existem scripts e documentos, assim como os logs das *scheduled tasks*.

Após estes passos, a BD fica aberta no servidor EAP-BCM e disponível para ser acedida através das sessões de terminal no EAP-BCMTS.

Anexo I – Lista de linhas da PT a reenviar

Nº SERVIÇO	TIPO DE NS	PRINCIPAL	ÁREA DE CENTRAL	NOME CLIENTE
LINK'S SAÍDA				
21 727 91 31	AP		01LX01	LINK OUT

21 726 91 71	AP		01LX01	LINK OUT
LINK'S ENTRADA				
21 380 17 00 - 99	AP C/ 106 DDI	S	01LX01	LINK DDI IN (engloba 6 antigos analógicos)
21 370 31 00 - 99	AP C/ 100 DDI	S	01LX01	LINK DDI CLIENTES IN
21 383 55 00 - 99	AP C/ 100 DDI	S	01LX01	LINK DDI CLIENTES IN
21 384 80 00 - 99	AP C/ 100 DDI	S	01LX01	LINK DDI CLIENTES IN
21 380 81 00 - 99	AP C/ 100 DDI	S	01LX01	LINK DDI CLIENTES IN
21 725 23 00 - 99	AP C/ 100 DDI	S	01LX01	LINK DDI CLIENTES IN/OUT
21 722 51 00 - 29 + 21 722 55 00 - 99	AP C/ 143 DDI	S	01LX01	LINK DDI CLIENTES IN (engloba 13 antigos analógicos)
21 720 21 90 - 99	AP C/ 10 DDI	S	01LX01	LINK TELEASSISTÊNCIA
ANTIGOS ANALÓGICOS REENCAMINHADOS PARA DDI'S				
21 385 55 60		21 722 51 00		BES Seguros
21 385 87 07		21 722 51 00		Sagres
21 386 00 35		21 722 51 00		Generali
21 386 00 76		21 722 51 00		BES - Cartões
21 386 01 19		21 722 51 00		Unicre
21 386 02 28		21 722 51 00		BES - Contas Correntes
21 386 33 22		21 722 51 00		Tranquilidade
21 388 47 18		21 722 51 00		BSCH Banco Santander
21 388 47 27		21 722 51 00		Inter-Atlântico
21 388 49 67		21 722 51 00		Mitsubishi
21 388 53 88		21 722 51 00		Victória Assistência - CGU
21 388 55 79		21 722 51 00		Daewoo
21 386 00 03		21 380 17 00		Geral Atendimento
21 386 02 13		21 380 17 00		Directo MGI
21 386 03 08		21 380 17 00		Fax Geral DC
21 386 33 14		21 380 17 00		RightFax - Geral In
21 387 33 23		21 380 17 00		Fax MGI
21 388 62 82		21 380 17 00		Geral Assistência - Prod. Individual
SERVIÇOS ESPECIAIS - VERDES, AZUIS, ÚNICOS E ESPECIAIS				

800 20 0005	Nº VERDE	21 383 55 10		FIDIS FLEET SERVICES
800 20 0095	Nº VERDE	21 384 80 50		PEUGEOT ASSISTÊNCIA
800 20 0111	Nº VERDE	21 384 80 84		BANCO BEST
800 20 0113	Nº VERDE	21 383 55 28		FERRARI
800 20 0228	Nº VERDE	21 384 80 98		RENAULT USADOS
800 20 0433	Nº VERDE	21 383 55 29		MASERATI
800 20 1998	Nº VERDE	21 370 31 34		Verde Médicos
800 20 2271	Nº VERDE	21 370 31 31		BES CONTAS CORRENTES
800 20 2281	Nº VERDE	21 386 00 76		BES CARTÕES
800 20 2291	Nº VERDE	21 383 55 55		BES 360
800 20 2445	Nº VERDE	21 370 31 97		EA Brasil
800 20 2666	Nº VERDE	21 370 31 98		EA Argentina
800 20 2958	Nº VERDE	21 380 81 23		LEASE PLAN
800 20 3030	Nº VERDE	21 384 80 16		LEXUS
800 20 3387	Nº VERDE	21 388 62 82		PRODUTO INDIVIDUAL
800 20 4034	Nº VERDE	21 383 55 31		ALFA ROMEO ASSISTÊNCIA
800 20 6456	Nº VERDE	21 383 55 15		DAEWOO
800 20 6600	Nº VERDE	21 384 80 56		TOYOTA EUROCARE
800 20 6676	Nº VERDE	21 370 31 15		GE FLEET SERVICES
800 20 6678	Nº VERDE	21 370 31 14		MILENIUM BCP RENTING
808 20 1011	Nº AZUL	21 383 55 60		MITSUBISHI EXTENSÃO GARANTIA
808 20 1250	Nº AZUL	21 383 55 68		SUZUKI EXTENSÃO GARANTIA
808 20 1449	Nº AZUL	21 383 55 40		BANCO BEST/BIC
808 20 2201	Nº AZUL	21 383 55 74		KIA ASSISTÊNCIA
808 20 2383	Nº AZUL	21 383 55 83		SAAB APOIO A CLIENTES
808 20 1000	Nº AZUL	21 383 55 85		PRODUTO INDIVIDUAL COMERCIAL
707 28 3149	Nº ÚNICO	21 720 21 98		TELEASSISTÊNCIA
12764	Nº ESPECIAL			
FAXES				
21 386 0308		21 380 17 00		Fax Geral DC
21 386 3314		21 380 17 00		RightFax - Geral In

21 387 3323		21 380 17 00		Fax MGI 11º Piso
21 380 1703		21 380 17 00		RightFax - Sinpat In
21 380 1704		21 380 17 00		RightFax - Veic. Constutores In
21 380 1708		21 380 17 00		RightFax - Veic. Portugal In
21 380 1738		21 380 17 00		RightFax - Frotas In
21 380 1739		21 380 17 00		Fax Plateau Ricoh 4000 - Veículos/CAT
21 380 1742		21 380 17 00		Fax Fornecedores
21 380 1743		21 380 17 00		Fax Comercial
21 380 1745		21 380 17 00		Fax DAF - Gestão de Frotas
21 380 1746		21 380 17 00		Fax Informática
21 380 1747		21 380 17 00		Fax Plateau Ricoh 4500 - Sinpat/Frotas
21 380 1749		21 380 17 00		RightFax - GSD In
21 380 1754		21 380 17 00		RightFax - Juridicos In
21 380 1759		21 380 17 00		RightFax - Médicos
21 380 1770		21 380 17 00		Fax DC - Geral
21 380 1777		21 380 17 00		RightFax - Pruebas
21 380 1786		21 380 17 00		RightFax - Veic. Subst. In
21 380 1787		21 380 17 00		Fax Plateau Ricoh 3045 - Veículos/Jurídicos
21 380 1788		21 380 17 00		Fax DAF
21 380 1789		21 380 17 00		RightFax - Generali
21 380 1793		21 380 17 00		Fax DAFi 11º andar
21 380 1794		21 380 17 00		RightFax - Médicos In
21 383 5532		21 383 55 00		Fax GS Poupular Seguros ==> e-mail
21 383 5551		21 383 55 00		RightFax - Gsinistros In
OUTROS				
21 382 9820	AB S/ DDI		01LX01	VIDEOCONFERÊNCIA
21 382 9824	AB S/ DDI		01LX01	VIDEOCONFERÊNCIA
21 382 9825	AB S/ DDI		01LX01	VIDEOCONFERÊNCIA

8.7 Anexo 7

AIX								
Ref.:	**Subprocesso**	**Actividade de Controlo**	**Preventivo ou detectivo**	**Automático / Manual / Ambos**	**Frequencia**	**Deficiência de desenho identificada?**	**Procedimento de Teste**	**Resultado do Teste**
1	Segurança do Sistema Operativo - **AIX - Obrigatório**	As seguintes configurações de segurança lógica estão adequadamente implementadas ao nível do sistema operativo AIX (de acordo com a politica estabelecida na Entidade): 1) Comprimento mínimo da password (MINLEN); 2) Prazo de expiração da password (MAXAGE); 3) Número de tentativas falhadas permitidas (LOGINRETRIES); 4) Histórico de passwords (HISTSIZE); 5) Existência de caracteres especiais (non - alphabetic) (MINOTHER).	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Solicitar o ficheiro /etc/security/user; 2) Para o utilizador *default* e para os super users (GUID = 0) analisar os seguintes parâmetros: - Comprimento mínimo da password (MINLEN); - Prazo de expiração da password (MAXAGE); - Número de tentativas falhadas permitidas (LOGINRETRIES); - Histórico de passwords (HISTSIZE); - Existência de caracteres especiais (non - alphabetic) (MINOTHER).	Verificámos junto da informação cedida pelo Dr. Henrique Guapo que estão implementadas as seguintes configurações de segurança lógica ao nível do sistema AIX implementado na instituição: 1) Comprimento mínimo da password : 8 caracteres para a maioria dos utilizadores, no entanto estão definidos utilizadores cujo comprimento minimo da password esta por default, isto é, 0 caracteres; 2) Prazo de expiração da password : não esta definido para a maioria dos utilizadores, no entanto para alguns do utilizadores do sistema está definido um prazo de expiração de password de 13 dias; 3) Histórico de passwords: 0 ultimas passswords; 4) Número de tentativas falhadas permitidas: 3 tentativas de login permitidas, no entanto estão definidos utilizadores cujo numero de tentativas de login esta definido por default, isto é, tentativas ilimitadas; 5) A password cumpre requisitos de complexidade : a password não cumpre os requisitos de complexidade (MINOTHER = 0) **Com excepção** **ver ponto 3.6 do relatório de CI**
2	Segurança do Sistema Operativo - **AIX - Obrigatório**	As contas de "super user" (UID = 0) do sistema operativo AIX estão atribuídas a colaboradores devidamente autorizados e identificados que, para a realização das suas tarefas, necessitam de uma conta com tais características.	P	Automático	N/A	Não	Universo: Lista de contas de utilizadores do sistema operativo AIX. Amostra: Contas "super user" do sistema Método: Examinar 1) Solicitar o ficheiro /etc/passwd; 2) Verificar as contas de utilizadores com o UID = 0; 3) Verificar se estão atribuidas a colaboradores devidamente autorizados e identificados.	Verificámos junto da informação cedida pelo Dr. Henrique Guapo que apenas existe uma conta de utilizador com o UID = 0, denominada por ROOT. As contas de "super user" (UID = 0) do sistema operativo AIX estão assim atribuídas de forma adequada no que diz respeito a níveis de acesso. Vide evidência no anexo auditoria externa.pdf Anexo C Sem excepção
3	Segurança do Sistema Operativo - **AIX - Obrigatório**	Todas as contas de utilizadores têm passwords atribuídas.	P	Automático	N/A	Não	Universo: Lista de contas de utilizadores do sistema operativo AIX. Amostra: N/A Método: Examinar 1) Solicitar o ficheiro /etc/passwd; 2) Para todas as contas verificar as que não têm password atribuida (campo de password (segundo campo) em branco).	Verificamos junto da informação cedida pelo Dr. Henrique Guapo que não existem contas de utilizador sem password atribuida. Sem excepção

4	Segurança do Sistema Operativo - **AIX - Obrigatório**	O serviço tftp encontra-se desactivado, uma vez que, apesar de ter a possibilidade de aceder aos dados, não oferece qualquer método de autenticação.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Solicitar o ficheiro /etc/inetd.conf; 2) Verificar se o serviço tftp encontra-se desactivado (com #).	Verificmos junto da informação cedida pelo Dr. Henrique Guapo que o serviço tftp encontra-se desactivado (com #). Sem excepção
5	Segurança do Sistema Operativo - **AIX - Obrigatório**	O sistema regista num log as tentativas incorrectas de acesso ao sistema operativo e as mensagens de segurança das diversas facilidades.	P	Automático	N/A	Não	Universo: N/A Amostra: N/A Método: Examinar 1) Verificar a existência e solicitar os ficheiros syslog.conf e failedlogin; 2) Para o ficheiro syslog.cong verificar quais os niveis de segurança (debug, err, info, notice, warning, alert e emerg) de algumas das seguintes facilidades: -mail; -auth; -kernel; -lpr; -etc. 2.1) Verificar onde estas mensagens são registadas (ex.: dev/console 3) Verificar se no ficheiro failedlogin se são registadas as tentativas falhadas de login.	Verificámos junto da informação cedida pelo Dr. Henrique Guapo que estão implementadas as seguintes configurações ao nivel do sistema de logging implementado no sistema AIX: *.INFO;MAIL.NONE;AUTHPRIV.NONE;CRON.NONE /VAR/LOG/MESSAGES