INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

VICTOR MANUEL DA SILVA ALVES

GOVERNÂNCIA DAS TECNOLOGIAS DE INFORMAÇÃO – UM ESTUDO DE CASO "APLICABILIDADE DO ITIL E DO COBIT NUMA INSTITUIÇÃO DE ENSINO PRIVADO"

Nome do Curso de Mestrado

MESTRADO EM TECNOLOGIA E GESTÃO DE SISTEMAS DE INFORMAÇÃO

Trabalho efectuado sob a orientação do

Professor Doutor Rui Manuel da Silva Gomes
Professor Mestre Jorge Manuel Ferreira Barbosa Ribeiro

Janeiro de 2011

AGRADECIMENTOS

Ao Mestre Jorge Manuel Ferreira Barbosa Ribeiro Professor e ao Doutor Rui Manuel Silva Gomes pela orientação, disponibilidade, profissionalismo e motivação para realizar este trabalho de investigação.

À Marcita e ao Martim que, com muito carinho e apoio, não mediram esforços para que eu chegasse até esta etapa de minha vida.

RESUMO

Nos dias de hoje, as organizações movem-se pela necessidade de apresentar elevadas taxas de rentabilidade, pela satisfação dos seus clientes, dos parceiros ou dos colaboradores, e pela manutenção de elevados níveis de competitividade que lhes permita fazer face à concorrência e garantir-lhes a sua sobrevivência. Para alcançarem estes fins, torna-se necessário que os serviços sejam cada vez mais eficientes e eficazes, devendo estar alinhados com as estratégias das organizações. Com a evolução das características das Tecnologias de Informação (TI), cada vez mais as organizações assentam as suas tarefas e operações em Sistemas de Informação (SI) cada vez mais robustos, quer em termos de funcionalidades disponibilizadas, quer em termos do aumento do desempenho computacional. Torna-se cada vez mais evidente a dependência das organizações em relação a estes sistemas e tecnologias, sendo necessário utilizar mecanismos eficientes no sentido de assegurar o controlo, a gestão e a disponibilidade destes sistemas, assim como a sua governância.

Ao longo das últimas décadas, foram apresentados diversos referenciais orientados para a gestão e controlo de determinadas áreas das TI, como por exemplo, o COSO - *Committee of Sponsoring Organizations*, o PMBook - *Project Management Body of Knowledge*, o CMM - *Capability Maturity Model*, a família de normas ISO (ex. ISO 27001 – Segurança Informática), o Six Sigma, entre outros. Por outro lado, o ITIL - *Information Technology Infrastructure Library* e o COBIT - *Control Objectives for Information and Technology* são duas orientações de elevada importância direccionados para as boas práticas e para o controlo dos Sistemas e Tecnologias de Informação, tendo vindo nos últimos anos a serem reconhecidos pelo seu sucesso em termos de orientação e de aplicabilidade para o controlo e gestão dos SI e das TI. O COBIT corresponde a uma estrutura que abrange todas as actividades relacionadas com a "informática" para a Governância das TI, enquanto o ITIL auxilia na definição dos processos associados aos serviços das TI complementando a iniciativa de processos de negócios. Em geral, procura por meio de boas

práticas, assegurar a entrega e suporte dos serviços de TI. Sendo que, estas duas orientações (ou referenciais) são amplamente reconhecidas pela sua complementaridade para a Governância das TI.

Por outro lado, tal como nas organizações, as Instituições de ensino público e privado tem como ambição a disponibilização aos seus clientes (neste caso alunos), um conjunto de serviços educativos de qualidade que lhes permitam estudar, aprender e aplicar o conhecimento adquirido na sua vida pessoal e profissional. Nos últimos anos, face à necessidade de reorganizar, melhorar e assegurar um melhor de serviço de qualidade, muitas destas organizações implementaram mecanismos internos para alcançar este fim, nomeadamente através da implementação dos Sistemas de Gestão da Qualidade, em especial a certificação da norma ISO 9001. Apesar da utilidade das orientações associadas a esta norma, o facto é que ela é abrangente a várias áreas de actividade das organizações, não estando especialmente orientada para a gestão dos SI e das TI, tornando-se necessário seguir orientações que permitam controlar e gerir a dependência da organização face aos SI e TI.

Neste contexto, após a aplicabilidade da certificação de serviços de qualidade em particular (norma ISO 9001), numa Escola Privada do ensino básico e secundário, este trabalho centrou-se no estudo e implementação da utilização dos referenciais ITIL e COBIT, no sentido de gerir e controlar as TI e assim, assegurar a governância das TI nesta instituição. A implementação desses referenciais na instituição possibilitou a gestão e controlo dos SI/TI, trazendo vantagens em termos de desempenho e eficiência da qualidade dos serviços, assim como na monitorização e controlo mais eficiente da infra-estrutura tecnológica, nomeadamente através da redução do tempo de execução de tarefas em cerca de 23%; na redução do número de incidentes resolvidos e concluídos pelos diversos serviços de informática em 25%, assim como na redução do número de incidentes reabertos em 10%.

Em suma, através deste trabalho foi possível estudar e aplicar as orientações de dois referenciais especialmente orientados para a governância das TI, tirando partido de uma base documental e processual assente na implementação da norma ISSO 9001. Com a realização deste trabalho a

Instituição melhorou o desempenho dos serviços, como a gestão e controlo dos SI e TI, ficando aberto o caminho para uma futura aplicabilidade de outras normas, em particular as orientadas para a segurança informática, nomeadamente a norma ISO 27001.

ABSTRACT

Nowadays organizations are driven by the need to present high rates of profitability, by the satisfaction of their clients, partners and workers and by the maintenance of high levels of competitiveness that allow them to face the competition and ensure their survival. In order to achieve these goals it is necessary to have efficient and effective services aligned with the strategies of the organizations. With the evolution of the characteristics of the Information Technology (IT) more and more the organisations are basing their tasks and operations on Information Systems (IS) that are more and more robust in terms of the available functionalities, as well as in terms of the improvement in the computational performance. The dependence of the organizations in relation to these systems and technologies is becoming more and more evident, being necessary to use efficient mechanisms in order to ensure the control, the management and the availability of these systems, as well as their governance.

Throughout the last decades several frameworks oriented for the management and control of certain areas of the IT have been presented, as it is the example of COSO – Committee of Sponsoring Organizations, the PMBook – Project Management Body of Knowledge, the CMM – Capability Maturity Model, the ISO family of standards (e.g. ISO 27001 – Computer Security), the Six Sigma, among others. On the other hand, the ITIL – Information Technology Infrastructure Library and the COBIT – Control Objectives for Information Technology are two frameworks of great importance which are oriented to best practices and to the control of the Information Systems and Technologies, and in these last years they have been being recognised by their success in terms of orientation and applicability for the control and management of the IS and the IT. The COBIT corresponds to a structure that embraces all the activities related t o the "informatics" for the Governance of the IT, while the ITIL helps in the definition of the processes associated to the services of the IT, complementing the initiative of businesses processes. In general, it searches by means of best practices to ensure the delivery and support of the IT services. Being the case that, these two frameworks (or referentials) are largely recognised by their complementarity for the Governance of the IT.

On the other hand, just like in the organizations the institutions of public and private teaching have as an ambition to put at the disposal of their clients (in this case, students) a range of quality educational services that will allow them to study, learn and apply the knowledge acquired in their personal and professional lives. During these last years and facing the need of reorganizing, improving and ensuring a better quality service, many of these organizations implemented internal mechanisms in order to achieve this goal, namely through the implementation of Quality Management Systems, in special, the certification

of the ISO 9001 standard. Despite the usefulness of the frameworks associated to this standard, the fact is that it is extensive to several areas of activity of the organizations, not being specially oriented for the management of the IS and the IT, therefore it becomes necessary to follow frameworks that allow us to control and manage the dependence of the organization in relation to the IS and IT.

In this context, after the applicability of the certification of quality services in particular (ISO 9001 standard), in a Portuguese Private School of the basic and secondary levels, this work was centered in the study and implementation of the use of the ITIL and COBIT frameworks, with the purpose of managing and controlling the IT and this way, ensuring the governance of the IT in this institution. The implementation of these frameworks in the institution made the management and control of the IT and IS possible, bringing advantages in terms of performance and efficiency of the quality of the services, as well as in the monitoring and more efficient control of the technological infrastructure, namely through the reduction of the number of time spent on the accomplishment of tasks in about 23%; in the reduction of the number of incidents that were solved and closed by the several information technology services in 25 %, as well as in the reduction of the number of reopened incidents in 10 %.

Summing up, through this work it was possible to study and apply the orientations of the two frameworks specially oriented for the governance of the IT, benefiting from a documental and processual base settled in the implementation of the ISO 9001 standard. With the accomplishment of this work the institution improved the performance of its services, as the management and control of the IS and IT, letting the door open to a future applicability of other standards, in particular those oriented for the security in the information technology, namely the ISO 27001 standard.

INDICE

LISTA DE TABELAS

LISTA FIGURAS

Capítulo 1

INTRODUÇÃO

1.1 ENQUADRAMENTO

Actualmente é impossível imaginar uma organização sem uma forte componente na área dos Sistemas de Informação (SI) ou sem uma área de Tecnologias de Informação (TI), uma vez que estes Sistemas asseguram a gestão operacional e estratégica das organizações. As organizações movimentam-se pela necessidade de produzir altas taxas de rentabilidade, pela satisfação de seus clientes, parceiros ou colaboradores, e pela manutenção de elevados níveis de competitividade que lhes permitem enfrentar a concorrência e garantir a sua sobrevivência. A aplicabilidade de orientações que asseguram a qualidade dos serviços nas organizações tornam-se extremamente úteis e necessárias no sentido de garantir elevados níveis de qualidade no serviço. Por outro lado, com a evolução dos SI e TI, cada vez mais as organizações tem como alicerce das suas actividades sistemas e tecnologias mais robustos e eficientes, tornando-se, de um modo geral [RG2009] vitais para garantir um bom desempenho e eficiência para a organização. Emerge claramente a importância da gestão e de controlo da organização, tornando-se necessário seguir e aplicar linhas orientadoras para assegurar a gestão e controlo

(governação)[1] dessas TI [RG2009]. Neste sentido existem algumas questões que devem ser respondidas para atingir essa governância, nomeadamente: Quais as orientações que devemos seguir para gerir as TI? Quais os indicadores que podemos especificar para medir a gestão da TI? Quais as ferramentas que podemos usar para medir a maturidade da Governância das TI?. Muitos referenciais [2] [IOS2005] [DRS2006] [OGC2007] [COSOWEB] [PMBWEB] [COB2007] [ITIWEB] têm sido desenvolvidos nos últimos anos para gerir e controlar as TI, bem como modelos [JPSM2007] e ferramentas [LPA2006] [JP2008] para avaliar a maturidade da Governância das TI, em particular quando aplicados numa organização, no sentido de assegurar os seus objectivos estratégicos. Apesar das vantagens destas orientações, duas das mais reconhecidas [ES2008] para a Governância das TI é o COBIT - *Control Objectives for Information and Related Technology* [COB2007] e o ITIL – *Information Technology Infrastructure Library.*

De uma forma genérica, esta dissertação centra-se no estudo e aplicabilidade do COBIT e do ITIL numa instituição do ensino privado. A instituição alvo do estudo é uma instituição de ensino básico e secundário denominada por Sociedade de Ensino de Campos – SEC, em que o seu objecto social centra-se unicamente no ensino básico e secundário. Trata-se de uma instituição de ensino totalmente gratuito para os alunos, sendo as receitas provenientes do Ministério da Educação e dos quadros comunitários. Actualmente a instituição é composta por 43 docentes, 19 funcionários (não docentes) sendo o número de alunos cerca de 400.

Em 2009 foram deliberadas estratégias orientadas para o Sistema de Gestão de Qualidade (SGQ) o qual culminou com a obtenção da certificação ISO9001 (NP EN ISO 9001:2008). Com a implementação dos procedimentos e linhas orientadoras da norma, a instituição foi capaz de reorganizar, e melhorar o serviço prestado à comunidade académica, nomeadamente aos alunos,

[1]Governar Trata-se de um conjunto de estruturas e processos que visa garantir que as TI suportam e maximizam adequadamente os objectivos e estratégias de negócio da organização, adicionando valores aos serviços entregues, balanceando os riscos e obtendo o retorno sobre os investimentos em TI.

[2] Referenciais: refere-se a normas ou *frameworks* que apresentam linhas orientadoras para gerir, controlar e/ou melhorar a eficiência de uma área (ex: sistemas de Gestão de Qualidade, Segurança Informática, etc.

docentes e funcionários. Contudo, no sentido de servir com melhor eficiência os serviços, a instituição dispõe de um conjunto de componentes associados dos Sistemas e Tecnologias de Informação que necessitam de ser geridos e controlados de uma forma mais eficiente do que o actual.

Neste contexto, tendo como base a estrutura documental e processual da implementação da norma ISO 9001, este trabalho enquadra-se na problemática da Governância das TI, em especial no estudo e aplicabilidade das linhas orientadas do ITIL e do COBIT numa instituição de ensino, no sentido de tentar melhorar a eficiência da gestão e controlo dos SI e TI, de modo a aumentar a qualidade dos serviços (assentes em SI e TI) a disponibilizar à comunidade académica.

1.2 Motivação

A certificação ISO 9001 veio permitir à instituição SEC implementar um conjunto de orientações que permitiram estabelecer um modelo de gestão da qualidade mais eficiente em toda a organização, em especial, ao nível dos serviços. Estas orientações estabelecem requisitos que permitem auxiliar a melhoria dos processos internos, a maior capacitação dos colaboradores, a monitorização do ambiente de trabalho, a verificação da satisfação dos clientes, colaboradores e fornecedores, num processo contínuo de melhoria do sistema de gestão da qualidade. Em termos gerais, a adopção destas linhas orientadoras foram vantajosas para a instituição, uma vez que lhe permitiu conferir uma maior organização, produtividade e credibilidade, no sentido de reorganizar processos internos e assim, agilizar mecanismos orientados para a melhoria dos serviços prestados.

Contudo com a operacionalização prática da norma ISO 9001, detectaram-se algumas limitações e dificuldades sobre a forma como estava a ser efectuada a gestão e controlo das TI, em especial, na gestão da infra-estrutura, a qual não estava a ser eficiente, existindo várias lacunas em termos de organização, especialmente na infra-estrutura de rede, na gestão do acesso aos sistemas,

na dificuldade no acompanhamento dos serviços prestados, na dificuldade em controlar os *backups*, entre outras. Neste sentido a implementação da norma ISO 9001 na área das TI não foi prevista. Constatou-se que a implementação da norma ISO 9001 deveria ter seguido duas orientações: por um lado assegurar a certificação ISO 9001, e por outro, desenvolver formas de trabalho para gerir e controlar as TI, de modo a proporcionar mecanismos que possam garantir a certificação de outros referenciais, como por exemplo, a norma de segurança ISO 27000 [ISO2010].

Neste contexto a motivação deste trabalho advém do facto de ser identificada esta ausência da Governância das TI, tornando-se necessário estudar e aplicar referenciais amplamente reconhecidos e aplicados nas organizações quando orientados para o controlo e gestão das TI. Por sua vez, uma outra motivação centra-se em preparar trabalho para uma futura certificação na área das TI em particular a ISO 27001.

1.3 OBJECTIVOS

Em termos gerais pretendeu-se que este trabalho fosse centrado no estudo, na exploração e aplicabilidade de conceitos e orientações associadas à Governância das TI. Desta forma o objectivo primário desta dissertação foi prover uma maior Governância nas Tecnologias de Informação numa Instituição de Ensino Privado, aplicando os referenciais do ITIL e o COBIT.

Os objectivos secundários deste estudo foi detectar o estado em que se encontram os sistemas e tecnologias de informação da instituição, quanto à sua gestão e segurança, assim como, propor, no caso de ser necessário, uma solução que estando alinhada com a estratégia da organização e sendo viável, em termos de custos financeiros, proporcionar uma melhor qualidade na gestão e segurança desses sistemas. Adicionalmente, também se pretendeu proceder à monitorização da sua aplicabilidade recorrendo a indicadores que permitam verificar os resultados da implementação destes referenciais.

1.4 METODOLOGIA

O método experimental que se utilizou para a realização desta dissertação teve como sustentação os passos metodológicos que se iniciaram, pela identificação do problema, no sentido de formalizar um objectivo, sobre o qual, o mesmo foi desenvolvido. Subsequentemente, a informação foi recompilada organizada e analisada continuadamente, construindo uma proposta para resolver o problema identificado (Secção 3). Finalmente, foram elaboradas conclusões que reflectiram os resultados obtidos na avaliação da operacionalização. Neste sentido este trabalho foi desenvolvido em quatro fases:

1. Revisão da literatura existente sobre os paradigmas utilizados - i.e. tornou-se essencial apresentar os conceitos metodologias e referencias que sustentaram este estudo, a revisão e resumo da bibliografia, assim como dos mais recentes trabalhos que abordam a área do saber deste trabalho, nomeadamente: a Governância dos SI, o ITIL, o COBIT, ISO 9001 e a família 27000.

2. Levantamento dos requisitos (ou Análise dos procedimentos) – após uma análise profunda dos conhecimentos adquiridos na fase anterior efectuou-se um levantamento de toda a estrutura e procedimentos das TI/SI, de forma a verificar o que existe e em que estado é que se encontram.

3. Aplicabilidade do ITIL e COBIT – esta fase de índole mais prática permitiu materializar as ideias conceptualizadas na primeira fase com o contexto organizacional obtido na segunda fase.

4. Avaliação – para verificar que o objectivo de melhorar a Governância do SI foi alcançado foram aplicados indicadores que permitiam monitorizar de forma quantitativa os resultados da aplicabilidade dos referenciais em estudo.

A seguinte tabela (Tabela 1) identifica o cronograma das fases de execução deste trabalho.

FASE	Mês								
	F	M	A	M	J	J	A	S	O
1. Revisão da literatura existente sobre os paradigmas utilizados	X	X	X						
2. Levantamento dos requisitos / Análise dos procedimentos			X	X					
3. Aplicabilidade do ITIL e COBIT				X	X	X	X		
4. Avaliação						X	X	X	X
5. Escrita do documento do projecto de Mestrado.							X	X	X

Tabela 1 - Organização cronológica das fases da dissertação.

O trabalho foi desenvolvido em cerca de dez meses, nos primeiros cinco meses foram centrados na revisão de literatura existente, assim como no levantamento dos requisitos. Nos cinco meses finais foram realizadas as tarefas de aplicação do COBIT, do ITIL e da sua avaliação. Por fim, nos últimos três meses foram destinados para a escrita deste documento.

1.5 Estrutura do Documento

Este documento está estruturado em quatro capítulos. No capítulo um apresentamos o enquadramento, a metodologia e os objectivos deste estudo. No capítulo dois centramo-nos na apresentação dos conceitos teóricos associados à governância das Tecnologias da Informação. O capítulo três é especialmente orientado para a aplicabilidade das orientações do COBIT e do ITIL numa instituição de ensino privado. Finalmente no capitulo quatro apresentam-se as conclusões e trabalho futuro.

Capítulo 2

A GOVERNÂNCIA DAS TECNOLOGIAS DE INFORMAÇÃO

2.1 INTRODUÇÃO

Nos dias de hoje, as organizações movem-se pela necessidade de apresentar elevadas taxas de rentabilidade, pela satisfação dos seus clientes, dos seus parceiros ou dos colaboradores, e pela manutenção de elevados níveis de competitividade que lhes permita fazer face à concorrência e garantir-lhes a sua sobrevivência. Os gestores necessitam cada vez de mais informação sobre as várias actividades de negócio das suas organizações, no sentido de tomarem decisões estratégicas com base em toda a informação das várias vertentes de negócio. Actualmente, é impossível imaginar uma organização sem um forte componente de SI ou sem uma área de TI, para gerir as informações operacionais e fornecer informação de gestão aos executivos necessária para a tomada de decisão. Por esta razão, e por causa da dependência dos SI e TI no suporte à gestão operacional e estratégica das organizações, os SI necessitam de ser geridos e controlados de forma eficiente [WHG2004] e constantemente monitorizados.

Tendo em consideração esta dependência dos Sistemas e Tecnologias de Informação, a Governância das Tecnologias da Informação [KK2001] corresponde a um conjunto de estruturas e processos para garantir que a TI suporte e maximize adequadamente os objectivos e estratégias da organização, agregando valor aos serviços prestados, minimizando os riscos e obtendo um

retorno no investimento em TI [ISACA2005]. Por outro lado, a Governância das TI é parte integrante de uma Governância Corporativa [WR2004] e abrange: os princípios de Governância das TI: Direcção e Controlo, Responsabilidade, Apresentação dos Resultados e Actividades; Governância de Stakeholders e uma Framework na Governância das TI no âmbito da TI. Este último princípio pode ser caracterizado por áreas de intervenção: Alinhamento Estratégico, a entrega do valor, Gestão de Riscos, Gestão de Recursos Humanos e monitorização de desempenho. A Governância corporativa é geralmente caracterizado por múltiplos níveis (Figura 1) operacional (estratégico, operacional e administrativo), assim como, as estratégias de orientações implementadas pelo Conselho de Administração e Direcção Executiva e a execução destas orientações estão fora da gestão das TI e dos negócios.

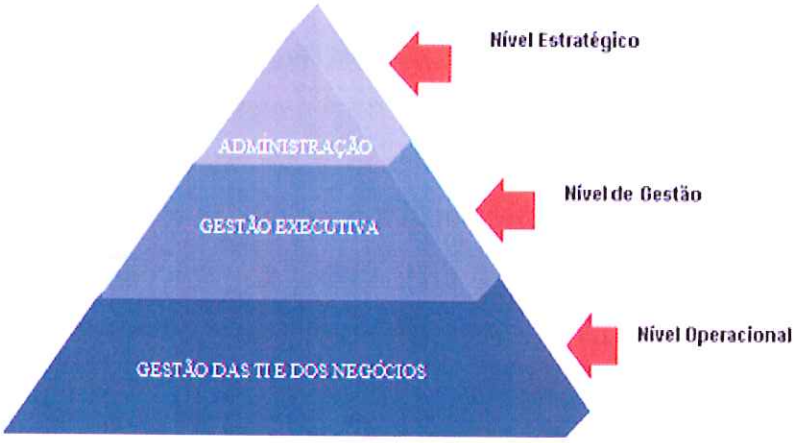


Figura 1 – Níveis Operacionais da Governância Corporativa [IBG2004].

A Governância Corporativa pode ser definida como [IBG2004] "o sistema pelo qual as sociedades são dirigidas e monitorizadas, envolvendo os relacionamentos entre accionistas, Administração, órgãos de chefia, Auditoria Independente e Serviços Financeiros. As boas práticas de Governância corporativa têm a finalidade de aumentar o valor da sociedade, facilitar o acesso ao capital e contribuir para a sua perenidade."

A Governância das TI é essencial para garantir melhorias eficazes e eficientes nos processos da empresa. Fornece uma estrutura que liga os processos de TI, os recursos de TI e as informações às estratégias e objectivos da empresa. Por outro lado, obter uma Governância das TI significa assegurar que as informações da empresa e a tecnologia aplicada suportam os objectivos do negócio permitindo, dessa forma, que a organização rentabilizasse as informações, maximizando benefícios, capitalizando em oportunidades e adquirindo vantagem competitiva [MC2008].

2.2 FERRAMENTAS E FRAMEWORKS

Tradicionalmente, as organizações encararam a Governância das TI como uma abordagem *ad-hoc*, através da criação dos seus próprios referenciais, baseados na experiência existente na organização ou, em alternativa, adoptaram normas internacionais que foram desenvolvidas e aperfeiçoadas recorrendo à experiência acumulada ao longo de anos, por um conjunto alargado de organizações e de profissionais que se tentam posicionar na vanguarda dos SI. Esta última opção é apresentada e defendida por *Rees etal* [RBS2003] como sendo a mais adequada. Para estes autores, existem benefícios na adopção de referenciais pois estes têm as seguintes características:

- Já existentes - poderão não existir vantagens em investir tempo e esforço no desenvolvimento de um "Framework de Governância das TI" metodológico próprio baseado na experiência e no conhecimento limitado de uma só organização quando já existem normas internacionais de SI disponíveis;
- Estruturados - as normas internacionais de SI habitualmente incorporam modelos estruturados que facilitam a compreensão das normas e a sua adaptação pelas organizações Para além disso, o facto de serem estruturados permite que todas as partes interessadas nos SI (*stakeholders*) tenham uma referência que é comum e que permite perceber aquilo que podem esperar dos SI;

- Incorporam as melhores práticas - as normas vão sendo construídas e melhoradas progressivamente ao longo dos anos, passando por um processo de avaliação por inúmeras organizações e profissionais de SI. Esta experiência acumulada de melhores práticas não é possível de alcançar com o esforço de uma só organização;
- Permitem a partilha de conhecimento adoptando normas globalmente aceites para os SI, as organizações podem beneficiar da partilha de conhecimento e de ideias (exemplos: grupos de utilizadores, websites, revistas, livros, etc.). Os referenciais próprios de uma só organização não beneficiam desta partilha;
- Auditáveis - sem a existência de normas de Gestão de SI, a missão da Auditoria de SI é dificultada ou, pelo menos, não fica tão facilitada para ser executada de um modo mais eficaz. Isto significa que, para além da Gestão de SI dever utilizar estas normas, os próprios Auditores de SI deverão também utilizá-las, em vez das habituais práticas *ad-hoc* de Auditoria.

Ainda de acordo com R*ees etal* [SG2003], não existe uma resposta pré-determinada para a questão: Qual o melhor "*Framework*" a seleccionar para a de Governância das TI? Torna-se importante, mais do que seleccionar um "Framework de Governância de TI", as organizações devem ser capazes de ter uma visão apreciativa sobre os diversos referenciais de SI existentes e planificar a implementação de uma "Framework de Governância de TI" sem que combine/integre as melhores práticas de entre os vários referenciais conhecidos, no sentido de assegurar a compatibilidade com as necessidades da organização [RBS2003].

Como referimos, cada vez mais há uma necessidade de desenvolver mecanismos para assegurar o controlo e gestão das TI. Essa preocupação tem sido ao longo dos anos materializada através da apresentação de várias referências [IOS2005] [DRS2006] [OGC2007] [COSOWEB] [PMBWEB] [COB2007], as quais especialmente orientadas para assegurar o controlo e gestão em sectores específicos associados ao SI e TI. Por sua vez, a norma ISO 9000 [TWW2000] corresponde a uma família de normas que especificam

linhas orientadas para os sistemas de gestão da qualidade de uma organização. Trata-se de um conjunto amplo de requisitos, directrizes e outros documentos de suporte que, juntos, podem disponibilizar um conjunto de ferramentas com as quais os gestores das organização podem gerir e melhorar a eficiência dos seus serviços. Apesar de abranger todas as áreas de actividade da organização, incluindo os campos das TI e SI, estas directrizes não fornecem orientações para o controlo e gestão dos Sistemas de Informação a serem implementados numa maioria de casos nesta área, em particular, na disponibilização de serviços aos clientes e funcionários de uma organização.

O ITIL (*Information Technology Infrastructure Library*) [OGC2007] [ITIWEB] é uma biblioteca que apresenta um conjunto de melhores práticas para gerir serviços das TI. Está centrado em "como" devem ser os serviços e processos das TI, ou por outras palavras, incide sobre a prestação de serviços e suporte, considerando os aspectos técnicos de acompanhamento do processo. Trata-se de uma série de manuais de formação que expõe e explicam as práticas que mais benéficas para os serviços das TI que uma organização deve adoptar. O seu objectivo principal é fornecer aos gestores meios de gestão de elevados padrões de qualidade no sentido de obter mais valor[3] usando as TI das suas organizações. Entre as vantagens [NIT2007] do ITIL estão focadas em linhas orientadoras para o uso das melhores práticas de TI, permitindo uma maior rapidez na análise dos resultados de monitorização das TI, fornecendo aos gestores uma visão mais clara dos resultados das TI. Contudo o ITIL tem a particularidade de ser "forte" em orientações para as TI, mas limitado no desenvolvimento e sistemas de segurança.

A norma ISO 17799 [ISOWEB] - "Boas práticas de Segurança da Informação", fornece recomendações para a gestão de segurança da informação, estando especialmente direccionada para os responsáveis pela introdução, implementação ou manutenção da segurança nas organizações, em particularmente na segurança dos SI. Por outro lado, a norma ISO 27000 [CB2006], visa estabelecer os procedimentos para fazer a gestão da segurança de Sistemas de Informação. Historicamente, a ISO 17799 foi originalmente

[3] Valor – melhoria dos serviços prestados pelos SI e TI.

preparada pelo *British Standards Institute* [CB2006] (BS7799) e posteriormente aprovada pela ISO/IEC (i.e. *International Standards Organization/International Electronic Comition*) [IOS2005]. Nos dias de hoje a família de normas ISO 2700x é um padrão aceite para a gestão da segurança da informação no que respeita à definição de linhas de execução do código de conduta estabelecidas na norma ISO 17799.

O CMM (*Capability Maturity Model*) [BSIWEB] [CMMWEB] corresponde a um conjunto de modelos de maturidade orientados para a Governância dos SI. São especialmente usados para o controlo das TI (em especial os processos de software), o qual fornece um método eficiente para classificar o nível em que se encontram as TI na organização. Tem a particularidade de estar direccionado na implementação para "entrega" de software e controlo de processos. Trata-se de uma abordagem derivada do modelo de maturidade para desenvolvimento de software SW-CMM (*Capability Maturity Model for Software*) [MCB1995] proposto pelo SEI (*Software Engineering Institute*) [SEIWEB]. Este modelo é caracterizado por permitir ajudar as organizações no sentido de melhorar os seus processos de entrega de software e controlo de processo.

Por sua vez, o COSO (*Committee of Sponsoring Organizations*) [RM2007] é um padrão aceite para o estabelecimento de controlos internos nas organizações. Permite determinar sua eficácia e eficiência, podendo ser aplicadas na área das TI, assim como em qualquer outra área da organização. O COSO apresenta que o controlo interno é um processo estabelecido pelo Conselho de Administração, gestores e outros destinados a fornecer uma garantia razoável quanto à realização dos objectivos. Em geral, trata-se de um quadro de procedimentos de auditoria aplicados nas organizações. Por outro lado como o COBIT [COB2007], que iremos apresentar seguidamente, fornece um guia detalhado para as TI. A principal diferença entre o COBIT e COSO é que o COSO é genérico, podendo ser usado em qualquer actividade da empresa, enquanto que o COBIT é dedicado exclusivamente à área das TI.

Numa outra vertente da área das TI, o PMBOK [PMI2008], definido pelo *Project Management Institute*, corresponde a uma colecção de processos em áreas de

conhecimento, em particular, como os princípios de boas práticas para a gestão de projectos (incluindo projectos nas áreas de TI).

O BSC (*Balanced Scorecard*) [KN2004] corresponde a um acrónimo que significa indicadores balanceados para o desempenho. Trata-se de uma metodologia centrada na gestão estratégica das empresas, a qual foi criada por *Robert Kaplan* e *David Norton*, em 1992. O *Balanced Scorecard* tem a particularidade de ser uma abordagem que permite a operacionalização da estratégia, facilitando a comunicação e a compreensão dos objectivos estratégicos aos vários níveis da organização. Através do *Balanced Scorecard* os gestores das organizações têm uma visão integrada do negócio, assim como um processo contínuo de monitorização do seu desempenho através da análise de vários indicadores.

O *Six Sigma* [PL2001] corresponde a uma metodologia inovadora, focada na eliminação dos defeitos nos processos dentro de uma organização que visa disponibilizar aos seus clientes um produto ou serviço, com um elevado nível de qualidade.

O COBIT (*Control Objectives for Information and Technology*) [COB2007] [GJC2004], foi desenvolvido pelo IT *Governance Institute* em 1996 [ITGWEB] sendo promovido pelo ISACA - *Information Systems Audit Control Association* [ISACWEB]. Esta *framework* fornece uma estrutura que abrange todas as actividades das TI, em particular o controlo e segurança. O âmbito principal do COBIT é o desenvolvimento de políticas claras e boas práticas de segurança e controlo, estando especialmente focado em simultâneo no controlo dos processos e no controlo estratégico da organização. Neste sentido, tem como objectivo principal desenvolver os objectivos de controlo de acordo com os objectivos e necessidades das organizações.

O SOX (*Sarbanes-Oxley*) corresponde a uma lei aprovada em 2002 pelo governo americano voltada principalmente para organizações de capital aberto (caracterizadas por terem acções na bolsa de valores ou com negociação na *Nasdaq*), tendo como objectivo acabar (ou minimizar a ocorrência) com os processos fraudulentos. Esta lei é composta por 11 secções direccionadas

essencialmente à responsabilidade penal dos órgãos de gestão das organizações. As secções 302 e 404 desta lei apresentam a responsabilidade corporativa através da avaliação da veracidade dos conteúdo dos relatórios financeiros produzidos, assim como, pela área das TI , em termos da avaliação dos controlos internos [SS2005] [SOXWEB].

Em geral, as organizações consideram e usam uma variedade de modelos de TI, padrões e melhores práticas. Contudo, esta panóplia de utilização de várias normas deve ser entendido na forma como eles podem ser utilizados em conjunto, devendo o COBIT actuar como um elemento integrador.

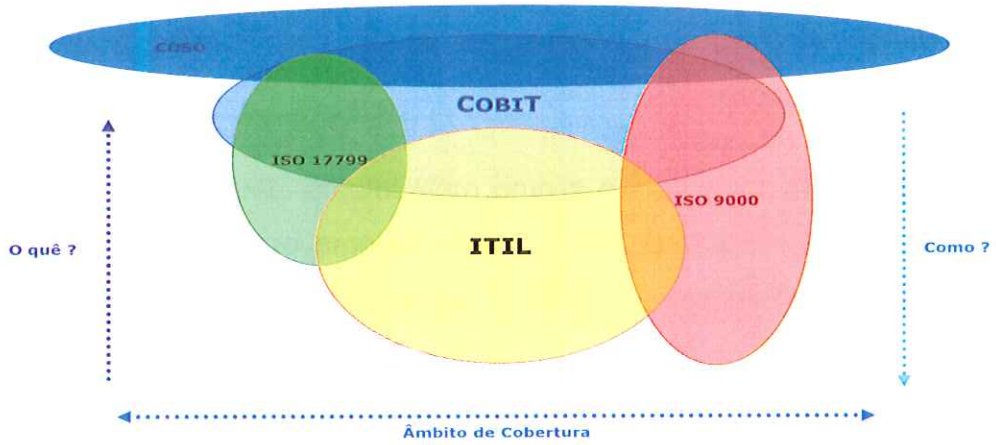


Figura 2 – Relacionamento entre diversos referenciais [ITGWEB].

Na figura 2, ilustra-se o relacionamento entre diferentes referencias, em particular o COBIT, o ITIL, a ISO 17799, a ISO 9000 e o COSO. Podemos verificar que o COBIT integra todos os referenciais apresentados na figura 2, seguido, imediatamente pelo ITIL que unicamente não se integra com o COSO. Os restantes referenciais apresentados são mais específicos, logo menos abrangentes relativos á áreas de TI.

2.3 AUDITORIA NA ÁREA DAS TECNOLOGIAS DA INFORMAÇÃO

Actualmente, numa sociedade em mudança continua, complexa e influenciada pelos SI, as organizações actuais tem a necessidade que a Informação e os Sistemas que a suportam devam ser cada vez mais controlados [SP2007]. A

alta velocidade com que as transacções são processadas, os sistemas de gestão de bases de dados, as redes globais de telecomunicações, o processamento de dados distribuídos, a comunicação através da Internet, e muitos outros factores, têm originado em qualquer organização, sem excepção, que as informações e os dados que as suportam sejam cada vez mais importantes. Por outro lado, as estratégias de gestão, as políticas de segurança, a segregação de funções; o impacto das falhas, o acesso não autorizado, a divulgação da informação, a continuidade do normal processamento dos dados; a adequação dos sistemas informações, e outras questões decorrentes da aplicação de tecnologias inovadoras têm vindo a ter um maior impacto na organização do que alguns anos atrás, surgindo assim uma necessidade de ter um controlo macro adequado [CA2004]. Por estas razões, para muitas organizações a informação e a tecnologia que a suporta, passaram a serem considerados os activos mais valiosos. De acordo com este cenário, começou-se a reconhecer os potenciais benefícios que as ferramentas tecnológicas podem proporcionar, no entanto, também compreendeu-se a importância de conhecer e gerir os riscos associados à implementação de novas tecnologias [CA2004].

Neste sentido, estas mudanças tem e continuarão tendo profundas repercussões nas estruturas de controlo dos SI/TI. A automatização das funções organizacionais está a determinar a incorporação de mecanismos de controlo com maiores potencialidades nos SI, nos sistemas operativos, nas redes e no hardware.

Por outro lado, cada vez mais, as organizações constatavam que a segurança dos seus SI tem de ser seguros e controlados de tal forma que, inicialmente, muitas delas criaram uma função interna de Auditoria Informática, com a responsabilidade de verificar a segurança [SP2007]. Actualmente a função auditoria nas organizações, onde se inclui a Auditoria de SI, tem evoluído no seu estatuto, estando ser encarada como uma actividade de suporte ao negócio (por oposição a uma actividade de inspecção), assim como tendo um carácter pró-activo ou preventivo (por oposição a um carácter reactivo). Segundo este novo paradigma, a auditoria deve ter a sua preocupação

centrada nos processos de negócio e nos SI que os suportam, baseando-se numa abordagem ao risco [DC2007].

Na literatura corrente, o paradigma actual da função auditoria é caracterizado por três factores principais que são:

- A visão holística da Auditoria, ao definir um carácter multi-dimensional quanto ao seu âmbito (visão COSO);
- Auditoria baseada no risco (de passiva, reactiva e baseada em controlos, passou para activa, proactiva e baseada em riscos);
- Dessa forma, a auditoria contribui para a implementação de soluções de melhoria contínua (no sentido de melhorias preventivas e não apenas soluções correctivas) [CA2004].

Em termos gerais a missão da Auditoria dos SI é avaliar e potenciar a melhoria contínua dos níveis de controlo dos SI e uma adequada gestão dos seus riscos por parte da organização. O desempenho de actividades secundárias pelo Auditor de SI (exemplo: consultoria interna) é um importante contributo para promover uma cultura de controlo na organização, assim como permitir aumentar o conhecimento especializado e prático em SI por parte do Auditor. Neste sentido como boas práticas, a Auditoria de SI é uma função especializada que deveria estar inserida num departamento de Auditoria e Gestão de Risco, coexistindo com a função de Auditoria de Processos de Negócio (função semelhante mas mais abrangente e generalista) assim como contemplar função de Gestão de Risco (função complementar pois ajuda os Gestores de SI a identificar e a gerir os seus riscos). Para garantir esta independência, o departamento de Auditoria e Gestão de Risco deverá reportar ao Comité de Auditoria e Gestão de Risco e, por via deste, ao CEO (*Chief Executive Officer*) no âmbito das suas responsabilidades de supervisão [DC2007].

Os principais factores que determinam o universo da Auditoria de SI são [CA2004]: os Processos de Negócio (entre os quais os de Gestão dos SI); os Recursos de SI (incluindo pessoas, aplicações, tecnologias, etc.); e a Informação (critérios de confidencialidade, integridade, disponibilidade,

conformidade e fiabilidade). Neste sentido, os principais factores centram-se no relacionamento entre os processos de negócio, recursos de SI e informação.

Dos referenciais mencionados no ponto 2.2 e das vantagens da sua escolha, o COBIT é reconhecido como o referencial que possui mais actividades directamente relacionadas e específicas orientadas para Auditoria de SI. Por outro lado apesar do COBIT apresentar controlos na área de segurança, a norma ISO 27000 está mais vocacionada para actividades de Auditoria dos SI relacionados com a conformidade da segurança da informação [ISACWEB], podendo ser complementada com os controlos do COBIT.

2.4 O ITIL

O ITIL tem como orientação principal, a operacionalização e a gestão da infra-estrutura da tecnologia numa organização, incluindo todo o que é de relevante no fornecimento dos serviços das TI. Nesse contexto, o ITIL considera que um serviço de TI é a descrição de um conjunto de recursos das TI. Os serviços de suporte do ITIL auxiliam no atendimento de uma ou mais necessidades do cliente, apoiando, desta forma, os seus objectivos de negócio. O princípio básico do ITIL é a gestão da infra-estrutura das TI. O ITIL descreve os processos que são necessários para dar suporte à utilização e à gestão da infra-estrutura das TI. Outro dos princípios fundamentais do ITIL corresponde ao fornecimento de qualidade de serviço aos clientes das TI, assente em custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia e como estes incorporam valor estratégico ao negócio. O interesse nesta área deve-se ao facto de que, através de metodologias (processos) padronizadas de gestão de TI, é possível obter uma relação adequada entre custos e níveis de serviços prestados pela área das TI [SSC2004].

O ITIL é um quadro de referência reconhecido por apresentar as melhores práticas para a gestão de serviços de TI. As melhores práticas, segundo o ITIL, correspondem a "actividades ou processos que comprovadamente obtiveram sucesso quando usados em várias organizações" [OGCA 2007]. A primeira compilação das melhores práticas ITIL foi realizada nos anos 80 e 90, a pedido

do governo Britânico, em particular pela *Central Computer and Telecommunications Agency*, actual *Office of Government Commerce* (OGC), tendo como resultado a sua primeira versão. Desde então, o ITIL foi actualizado duas vezes, entre 2000 e 2002 para a versão 2, e em 2007 para a versão 3 em vigor, estando actualmente em preparação uma actualização à versão 3 (ITIL V3).

Este quadro de referência é caracterizado por aplicar o princípio "*do what works*" [OGCB 2007], sendo muito menos um conjunto de teorias sobre a gestão de serviços de TI do que o destilar das práticas encontradas nas melhores e maiores organizações de TI. O ITIL é uma *framework* (ou conjunto de bibliotecas) não proprietários (embora o Governo Britânico mantenha direitos sobre ele), não prescritivo, compilando as melhores práticas na área da gestão de serviços de TI.

No sentido de compreender o ITIL torna-se no nosso entender, necessário definir os conceitos fundamentais desta abordagem, i.e., serviços, gestão de serviços e valor [JV2009]: a gestão de serviços consiste num conjunto de habilidades (*capabilities*) e recursos organizacionais destinados a fornecer valor aos clientes na forma de serviços; os serviços são um meio de disponibilizar valor aos clientes, facilitando-lhes atingir os resultados (*outcomes*) que pretendem sem que se responsabilizem por custos e riscos específicos. Neste contexto valor deve ser entendido como melhores serviços e/ou serviços de melhor qualidade. Os resultados podem ser atingidos através do desempenho de tarefas, podendo estar sujeitos a um conjunto de restrições. Na realidade, os serviços melhoram o desempenho das tarefas e reduzem o impacto das restrições, assim como aumentando a probabilidade de se atingirem os resultados desejados.

Na perspectiva do cliente, a criação de valor corresponde a uma combinação dos efeitos da utilidade e da garantia (*warranty*). A utilidade está relacionada com as funcionalidades oferecidas pelo produto ou serviço e com o conceito de adequação ao propósito (*fitness for purpose*). Por outro lado, a garantia corresponde a promessa do produto ou serviço funcionar como esperado, i.e., cumprindo os requisitos acordados. Este conceito é também conhecido como

adequação ao uso (*fitness for use*). Em suma, a utilidade corresponde ao que o cliente recebe, enquanto que a garantia é a forma como o recebe.

Em termos de estrutura, o ITIL V3 é composto por 27 processos, dividindo-se em cinco fases: estratégia de serviço (*service strategy*), desenho de serviço (*service design*), transição de serviço (*service transition*), operação de serviço (*service operation*) e melhoria contínua de serviço (*continual service improvement*). Esta nova versão do ITIL inclui todos os processos da versão ITIL V2, complementando-os com 12 novos processos e integrando-os num ciclo de *feedback* contínuo, denominado ciclo de vida do ITIL V3.

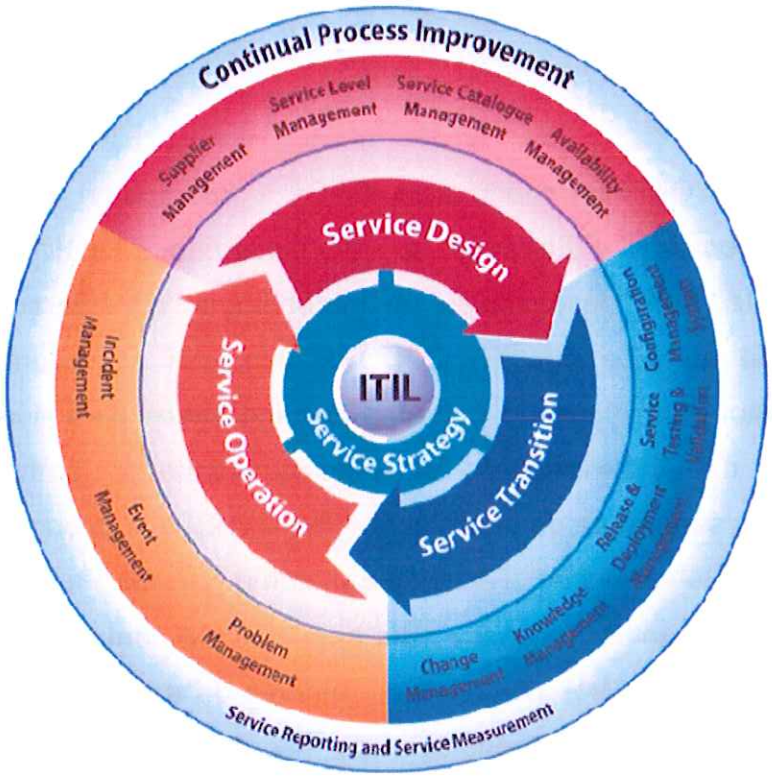


Figura 3 – Modelo do ciclo de vida do ITIL V3 [ITIL 2005].

Tal como representado na Figura 3, a perspectiva de ciclo de vida especificada pelo ITIL V3 sugere uma evolução circular e iterativa dos serviços, permitindo que estes se adaptem melhor ao ambiente de negócio da organização, o qual está em permanente modificação. Em torno da estratégia de serviço, encontra-se o ciclo de desenho, a transição e a operação de serviço. Envolvendo este

ciclo encontra-se a melhoria contínua de serviço, que ajuda a estabelecer e dar prioridade a programas e projectos de melhoria com base nos objectivos estratégicos. Na fase de desenho, as intenções definidas na estratégia são codificadas em serviços que suportem os resultados pretendidos. Na fase de transição decorre a implementação do serviço de acordo com o desenho. Após um serviço ser colocado em produção, entra-se na fase de operação. Na fase de melhoria contínua, que na realidade ocorre em simultâneo com as restantes fases do ciclo de vida, analisam-se métricas e indicadores definidos na fase de desenho e propõem-se as necessárias melhorias ao serviço. Finalmente, as propostas aprovadas são englobadas numa nova iteração do ciclo.

2.5 O COBIT

O referencial COBIT foi criado pelo ISACA – *Information Systems Audit and Control Association* – através do *IT Governance Institute*, organização independente que desenvolveu a metodologia considerada a base da Governância na área das TI. O COBIT funciona como uma entidade de padronização, estabelecendo métodos documentados para orientar a área de tecnológica das organizações, incluindo qualidade de software, níveis de maturidade e segurança da informação [ISACWEB]. Os documentos do COBIT definem a Governância Tecnológica como sendo "uma estrutura de relacionamentos entre processos para direccionar e controlar uma empresa de modo a atingir objectivos corporativos, através da agregação de valor e risco controlado pelo uso da tecnologia da informação e de seus processos" [ISACWEB].

2.5.1 Estrutura

Conforme se ilustra na figura 4, o referencial do COBIT está estruturado [COB2007] em três partes: i) critérios de informação (ou requisitos de negócios): para satisfazer os objectivos de negócio, as informações precisam estar em conformidade com os critérios chamados requisitos de negócio: os

requisitos de qualidade (qualidade, custo, entrega), os requisitos de confiança (eficácia e eficiência das operações, confiabilidade das informações, cumprimento das leis e regulamentos), requisitos de segurança (confidencialidade, integridade, disponibilidade); ii) os recursos das TI: os recursos são geridos pelos processos das TI para fornecer informações que a organização precisa para alcançar os seus objectivos. Esses recursos incluem: aplicações, informações, infra-estrutura e pessoas); iii) os procedimentos de TI: nestes casos estão reunidas as principais actividades das TI num modelo de processos, facilitando a gestão das TI para satisfazer as necessidades do negócio.

Os processos das TI são definidos e classificados em 4 domínios [COB2007] [ISACWEB], com 34 procedimentos. Esses processos estão apresentados e definidos em actividades e tarefas na organização. A estrutura do COBIT está agrupada em quatro domínios (figura 4): planear e organizar, adquirir e implementar, entregar e suportar, controlar e avaliar. Além disso, o COBIT apresenta um conjunto de indicadores a serem monitorizados de forma eficaz para garantir que o controlo e monitorização da SI e TI.

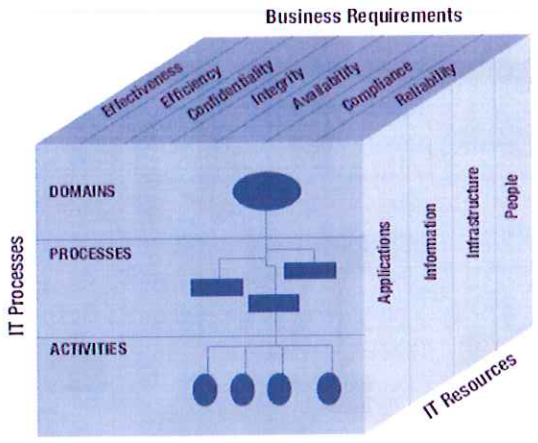


Figura 4 - Dimensões do "cubo do COBIT" [COB2007].

Seguidamente passamos a explicar cada um dos domínios do COBIT (Figura 5). O primeiro domínio, Planeamento e Organização (PO), abrange estratégias e tácticas, procurando a identificação de como pode contribuir para melhorar a realização dos Objectivos organizacionais. Além disso, a realização da visão estratégica precisa ser planeada, comunicada e administrada para as

diferentes perspectivas, sendo composto por 10 Objectivos de controlo; o segundo é a Aquisição e implementação (AI), define que as soluções de TI precisam ser identificadas, desenvolvidas ou adquiridas, como também implementadas e integradas no processo empresarial. As mudanças e manutenções de sistemas existentes são cobertas por esse domínio, isso para ter certeza que o ciclo de vida é assegurado para esses sistemas, sendo composto por 7 objectivos de controlo; o terceiro domínio, Entrega e Suporte (ES), trata da entrega dos serviços requeridos pelo negócio. Para entregar serviços devem ser montados os processos de apoio necessários, estando composto por 13 objectivos de controlo; o quarto domínio, Monitorização e Avaliação, indica que todo o processamento precisa de ser avaliado regularmente para assegurar a qualidade e conformidade dos controlos requeridos. Esse domínio trata da administração do processo de controlo da organização de TI e da garantia de independência provida pela auditoria interna e externa ou obtida por meio de fontes alternativas, estando composto por 4 objectivos de controlo [COB2007].

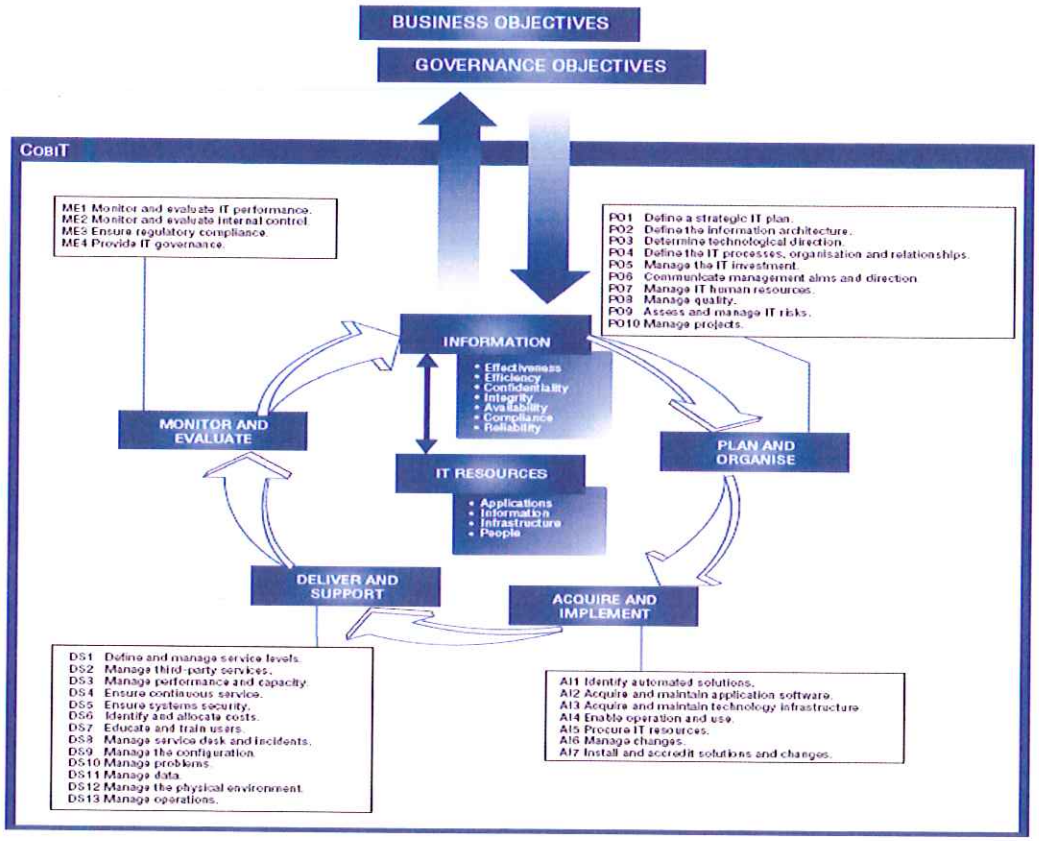


Figura 5 - Domínios do COBIT [COB2007].

Além dos quatro domínios principais que guiam o bom uso da tecnologia da informação na organização, existe também a questão de auditoria que permite verificar, através de relatórios de avaliação, o nível de maturidade dos processos da organização. O método de auditoria segue o modelo do CMM que estabelece os seguintes níveis:

- Inexistente: significa que o processo de gestão não foi implementado;
- Inicial: o processo é realizado sem organização, de modo não planeado;
- Repetível: o processo é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido;
- Definido: o processo é realizado, documentado e comunicado na organização;
- Gerido: existem métricas de desempenho das actividades, o processo é monitorizado e constantemente avaliado;
- Optimizado: as melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos.

O resultado do relatório identifica o grau de evolução dos processos na organização que é avaliada, de modo concreto, com base em relatórios confiáveis de auditoria e parâmetros de mercado. O sumário executivo do relatório traz as seguintes informações: se existe um método estabelecido para o processo, como o método é definido e estabelecido, quais os controlos mínimos para a verificação do desempenho do método, como pode ser feita a auditoria no método, quais as ferramentas utilizadas no método e o que avaliar no método para sua melhoria. A partir de então, a organização define as metas, isto é, os objectivos de controlo a serem atingidos.

2.5.2 VANTAGENS

As vantagens que nos podem proporcionar a implementação deste referencial são diversas, das quais, conforme o próprio guia do referencial indica [COB2007], podemos destacar as seguintes: está alinhado com outros padrões e com as melhores práticas; suporta e é suportado pelas melhores práticas,

provendo assim um ambiente de TI bem gerido e flexível; está orientado para a melhoria da Governância das TI das organizações e na redução dos riscos operacionais; gere e controla as actividades de TI; proporciona um ambiente de controlo responsável em garantir as necessidades de negócio; disponibiliza ferramentas para auxiliar na gestão e no controlo das actividades de TI; garante que as funções corporativas ocorram de forma sistemática para o alcance dos objectivos do negócio; cria uma linguagem comum para todos os envolvidos nos controlos dos processos; Mapeia os objectivos de TI com os objectivos do negócio e *vice-versa;* Mapeia os maiores padrões e *frameworks* de mercado como: ITIL, ISO 20000, ISO 27001 ,entre outras; permite um melhor alinhamento, baseado no negócio; Continuamente em desenvolvimento; provê um ambiente de controlo que é responsável em garantir as necessidades de negócio e servir para funções de gestão e auditoria, a partir de suas responsabilidades de controlo; Aceito internacionalmente como *framework* de modelo para Governância de TI portanto é exigido e reconhecido pela maior parte das empresas de TI; além de todas estas vantagens nos agrega conhecimento.

2.5.3 Pontos Fracos

O "guia" COBIT apresenta algumas desvantagens que o referencial COBIT detêm, dessas desvantagens *Hussain* e *Siddiqui* [HS2005] salientam as seguintes: que o referencial não reconhece a relativa importância de todas as áreas de processo. A natureza genérica do modelo impossibilita executá-lo em todo o ambiente das TI; sendo esta é uma das principais imperfeições do modelo COBIT. A razão identificada por *Hussain* e *Siddiqui* [HS2005]é que o modelo fornece as ferramentas para controlar, mas não dá o poder de medir o impacto do modelo. Consequentemente, revelou-se que o modelo é muito vago e que não existe nenhuma maneira de avaliar o impacto quantitativo. Uma dificuldade do guia COBIT é a maior ênfase dada ao controlo e à mitigação do risco do que à oportunidade de performance, sendo assim um inconveniente para a gestão.

Por fim, a linguagem de controlo do guia COBIT geralmente não é bem compreendida pelas organizações que não possuem conceitos de auditoria ou controlos financeiros [ISA2005]. Apesar de se poder aplicar o COBIT a todos os sectores de uma organização, verificamos que apresenta algum défice quando passamos a observa-lo para além dos processos. Analisando de uma forma genérica, é possível verificar que é deficitário na área operacional (a qual o ITIL cobre), devido à sua orientação estar mais focada para os nível estratégico e táctico.

2.6 Exemplos de Aplicação

Este estudo centra-se na análise e investigação da sua aplicabilidade do COBIT e ITIL, em organizações especialmente orientadas para o ensino. Constatou-se que em Portugal, a aplicabilidade do COBIT e do ITIL é recente nas organizações, sendo conhecidas apenas algumas aplicabilidades pontuais na área das instituições de ensino.

À escala mundial verificou-se que o modelo ITIL tem sido um referencial largamente utilizado em diversas instituições do ensino superior. Nos Estados Unidos, de acordo com o [REM2010], existem 18 universidades com implementações de processos de ITIL. Fazem parte desse conjunto as seguintes universidades: *California State at Sacramento*, *Duke*, *Georgia Tech*, *Harvard*, *Marquette*, *Michigan State*, *Notre Dame*, *NYU*, *Purdue* e *Yale*. O *University* ITSM funciona como um repositório em linha de boas práticas usadas no contexto académico para a gestão de serviços de TI. Em Portugal verificamos que a Fundação para a Computação Cientifica Nacional FCCN e a Instituto Universitário de Lisboa (ISCTE-IUL) tem procurado dinamizar a colaboração com outras universidades nesta área. Contudo só encontramos um caso de implementação na ISCTE-IUL, implementou o referencial ITIL ao o projecto-piloto académico de gestão de activos das TI [REM2010].

Por outro lado, nos Estados Unidos, a aplicação do COBIT em instituições de ensino, não tem sido tão implementada quanto o ITL, encontramos como referencia a *University of Lowa*. Contudo este referencial tem sido largamente

aplicado a organizações em todo o mundo com um diferenciado objectivo social, tais como: multinacionais na Austrália [WC2009]; Organizações de Bancos Comerciais no Sul de África [TS2008]; Organizações prestadoras do serviço *VoIP* (*Voice over Internet Protocol*) [MRR2009]; entre muitas outras que demonstraram que este referencial é benéfico para o aumento da qualidade dos serviços nos SI/TI.

No contexto português, existe um projecto [RB2008] recente de mestrado no âmbito contabilístico que aplica o COBIT à organização EDP (Electricidade de Portugal). No âmbito de uma instituição de ensino unicamente encontramos o Instituto Politécnico de Viana do Castelo que implementou este referencial [RG2009]. Tendo sido apresentados relevantes na melhoria do desempenho dos serviços prestados.

2.7 COMPARAÇÃO ENTRE O ITIL E O COBIT

A utilização do modelo ITIL auxilia na definição dos processos ligados aos serviços das TI complementando a iniciativa de processos de negócios, onde procura, por meio de boas práticas, garantir a entrega e suporte dos serviços de TI. Já os controlos e as métricas necessárias para gestão das TI, devem ser definidos na gestão dos processos e projectos.

Como comparação entre essas referências, temos COBIT para gestão das TI inovando através da Governância Tecnológica e o ITIL detêm uma de uma série de processos operacionais e de gestão também associados às TI.

Conforme *Larsen, Pedersen* e *Andersen* [LPA2006], nas últimas décadas várias metodologias, padrões e ferramentas têm surgido para auxiliar na obtenção da Governância das TI, entre elas, as mais comuns são o *Information Technology Infrastructure Library* - ITIL e o *Control Objectives for Information and Related* Technology - COBIT. Comparado ao referencial COBIT, o referencial ITIL descreve de forma detalhada os processos relativos ao suporte e entrega de serviços, mas não cobre todos os requisitos de controlo relacionados gestão das TIC descritos pelo COBIT para este domínio. Alguns

objectivos de controlo do modelo COBIT no domínio planeamento e organização são tratados superficialmente através dos processos do modelo ITIL. Por outro lado, o modelo ITIL não aborda o domínio de Monitorização do modelo COBIT.

O ITGI [COM2008] que foi fundada pela ISACA em 1998, criou o COBIT (3ª edição) em 2000, COBIT (4ª edição) em 2005 e COBIT 4.1 em 2007, criou também uma série de trabalhos de mapeamento COBIT com outros referencias que o poderiam complementar, um desses mapeamentos foi realizado com o referencial ITIL, por complementar o COBIT na Governância das TI.

Conforme Larsen, Pedersen e Andersen [LPA2006], é reforçada a ideia que, o referencial COBIT é aceite como um padrão para a segurança da tecnologia da informação e as práticas de controlo. Este referencial inclui: elementos de medição de desempenho, directrizes para os processos de TI, metas e métricas, melhores práticas para os processos de TI e modelos de maturidade.

Segundo *HP* [HP2005], é possível verificar que enquanto a gestão de Serviços das TI orientam-se na efectividade do fornecimento dos serviços das TI e na gestão das suas operações, a Governância das TI contribui para que a área das TI se integre nos diversos departamentos da organização mediante a apresentação do desempenho das operações subsidiando as tomadas de decisão.

Por outro lado, o modelo ITIL não está orientado para descrever o que deve ser abordado na gestão das TI. Os seus processos estão estruturados e detalhados para indicar como implementar e determinar quem são os responsáveis por cada módulo. O COBIT parte da premissa que processos, informações e recursos devem estar alinhados para permitir a entrega eficaz da informação para a organização, orientada pelos critérios e indicadores de objectivos. Na visão do COBIT, a entrega eficaz da informação é sustentada por um sistema de melhores práticas em processos e controlos, apropriados para o negócio, e que direccionam e monitorizam o valor entregue pelas TI. Ressalta-se, que a Governância das TI existem nas organizações onde o nível de maturidade apropriado da gestão de serviços já foi atingido. Desta forma,

quando a área das TI deixa de existir apenas como provedora de serviços para actuar como uma função estratégica organizacional [HP2005].

O modelo de gestão ITIL como foi verificado evidencia os seus objectivos e estratégias em processos das TI, e está mais limitado em segurança e desenvolvimento de sistemas. Já o modelo COBIT é consistente em controlos e métricas das TI.

Comparando os modelos, eles possuem muitas qualidades em comum, onde procuram uma melhor gestão da área das TI da organização, porém cada modelo evidencia as suas qualidades em objectivos específicos.

O modelo de gestão ITIL tem uma melhor aplicabilidade em organizações que procuram uma estruturação e uma organização na área das TI, baseado na modularização dos processos de TI.

Em termos gerais, o modelo COBIT tem uma maior aplicabilidade em empresas que já possuem uma estruturação na área das TI, e procuram uma gestão mais eficiente e eficaz nas TI norteadas em auditorias, controlos e métricas.

2.8 Conclusões

As organizações tipicamente enfrentam determinados desafios na área das TI que acabam por demandar a necessidade da Governância das TI. Podemos considerar alguns desses desafios, tais como, manter as TI em funcionamento; entregar valor aos clientes; gerir os custos das TI; dominar as complexidades, alinhar as TI com os negócios, garantir conformidades de regulamentos; gestão e segurança.

A Governância de uma organização é caracterizada por uma estrutura de relacionamentos e processos que ajudam a direccionar e controlar as metas a serem atingidas pela organização. Em termos gerais as áreas para onde está orientada a Governância das TI são: alinhamento estratégico; agregação de valor; gestão de risco; gestão de recursos e medição de *perfomance*. Face à

dependência dos SI por parte das organizações cada vez mais os referenciais de Governância e controlo fazem parte das melhores práticas de gestão das TI e são facilitadores para estabelecer uma Governância das TI, e que, em simultâneo, esteja de acordo aos requisitos regulamentares que estão em continua evolução.

A gestão da infra-estrutura das TI e a utilização de referenciais em gestão das TI, podem ser vistos como uma condição obrigatória para se obter uma melhoria nos processos, na qualidade necessária e no cumprimento dos prazos, tão importantes nos ambientes competitivos de hoje.

Conforme visto no decorrer deste trabalho as melhores práticas de Governância com o COBIT e a gestão de serviços das TI têm sido factores importantes para as organizações atingirem todos os seus objectivos, assim como, a biblioteca de processos ITIL está entre as mais aceitas e reconhecidas mundialmente como as melhores práticas para gestão de serviços e infra-estrutura das TI. O ITIL hoje é reconhecido como um padrão na gestão de serviços das TI, e as organizações que o implementaram estão satisfeitas com os resultados, onde o modelo leva a uma maior qualidade e produtividade à organização.

O COBIT é o referencial que possui mais actividades directamente relacionadas e específicas para Auditoria de SI. Assim como a norma ISO 17799 (Família 27000) está mais vocacionada para actividades de Auditoria dos SI relacionados com a conformidade da segurança da informação.

Numa das secções deste trabalho verificou-se a relação entre o referencial COBIT e ITIL, o qual constatou-se que, cada modelo possui as suas particularidades, e oferecem serviços diferenciados, mas ambos são extremamente importantes para atender e resolver os problemas e objectivos das organizações. Podem ser implementados, por uma determinada organização, em conjunto ou separados. Essa flexibilidade é propiciada pelo facto de que os modelos podem ser segmentados, como o ITIL nas suas disciplinas, e o COBIT nos seus 34 objectivos dentro dos 4 domínios. O intuito da união dos modelos é obter o melhor de cada um, suprindo os pontos fracos

de um determinado modelo com a utilização do outro. O COBIT tem como ponto forte as diferentes métricas distribuídas entre os domínios, entretanto não detalha os processos de segurança e serviços de TI que podem ser suportados pelo modelo ITIL.

O COBIT pode ser utilizado num nível mais alto da Governância nas TI, fornecendo uma estrutura de controlo global, baseado nos modelos de processos das TI definido pelo ITGI, sendo destinado genericamente para qualquer organização. Práticas e padrões específicos, tais como o ITIL, que cobrem áreas específicas e podem ser mapeadas pelo guia COBIT, fornecendo assim uma hierarquia mais completa para o material utilizado como guia de melhores práticas .

Capítulo 3

GOVERNÂNCIA DAS TI NUMA INSTITUIÇÃO DE ENSINO PRIVADO

3.1 MOTIVAÇÃO

Actualmente, as organizações estão continuamente orientadas para a estratégias e operacionalização, procurando o sucesso em face ao ambiente de mudança no crescimento do negócio competitivo [MS2005]. Essas mudanças são iminentes e para que a área das TI possam atender a essas demandas, muitas vezes torna-se necessário investimentos de grandes dimensões que devem ser bem sucedidos. A Governância nas TI auxilia na melhor condução desses investimentos.

A motivação na parte da aplicabilidade dos referências da Governância das TI numa Instituição do Ensino Privado, está no facto, de diminuir o espaço existente entre o negócio e as actividades das TI, a fim de utilizar correctamente os recursos das TI e eliminar e ou diminuir as deficiências encontradas na área de tecnologia, reduzindo os custos, aumentando a qualidade dos serviços de TI fornecidos, bem como a possibilidade de melhorar a gestão através da obtenção de métricas de qualidade de serviço.

Os factores impulsionadores mais referidos como determinantes para a escolha do ITIL foram os seguintes: A utilização de um quadro de referência para a

qualidade já reconhecido, não sendo necessário "reinventar a roda"; a possibilidade de fomentar uma cultura de serviço focada no cliente e aumentar a consciência dos colaboradores da área das TI para a gestão de serviços; a implementação das melhores práticas de gestão de serviços para melhorar a qualidade dos serviços fornecidos aos clientes; a necessidade de se tornarem organizações baseadas em processos; a possibilidade de usar uma linguagem comum à área de TI, tanto internamente às unidades organizacionais responsáveis pelas TI, como externamente, na comunidade universitária.

3.2 Diagnóstico

O "objecto social" da Instituição (SEC – Sociedade de Ensino de Campos, cita em Vila Nova de Cerveira, freguesia de Campos) alvo deste estudo centra-se unicamente o ensino básico e secundário. As suas receitas para o ensino regular são exclusivamente provenientes do Ministério da Educação através do contrato (Contrato de Associação) sendo renovado anualmente, enquanto que para o ensino do programa governamental de novas oportunidades é proveniente dos quadros comunitários (neste momento do QREN) . Neste sentido, o ensino é totalmente gratuito para os alunos, de igual forma como o ensino publico.

Os recursos humanos regem-se especificamente pelo Contracto Colectivo de Trabalho das escolas particulares e cooperativas, e genericamente pelo Código Administração Pública. O quadro de pessoal da instituição é composto por 43 docentes, 19 funcionários não docentes e com sensivelmente 400 alunos. Para uma melhor percepção da forma como é a estrutura departamental da escola é apresentado em anexo o seu organograma (Anexo 1).

Relativamente aos equipamentos físicos (Figura 6), detêm 78 computadores, dos quais 17 desses são exclusivos dos serviços administrativos, sendo os restantes utilizados por toda o comunidade educativa.

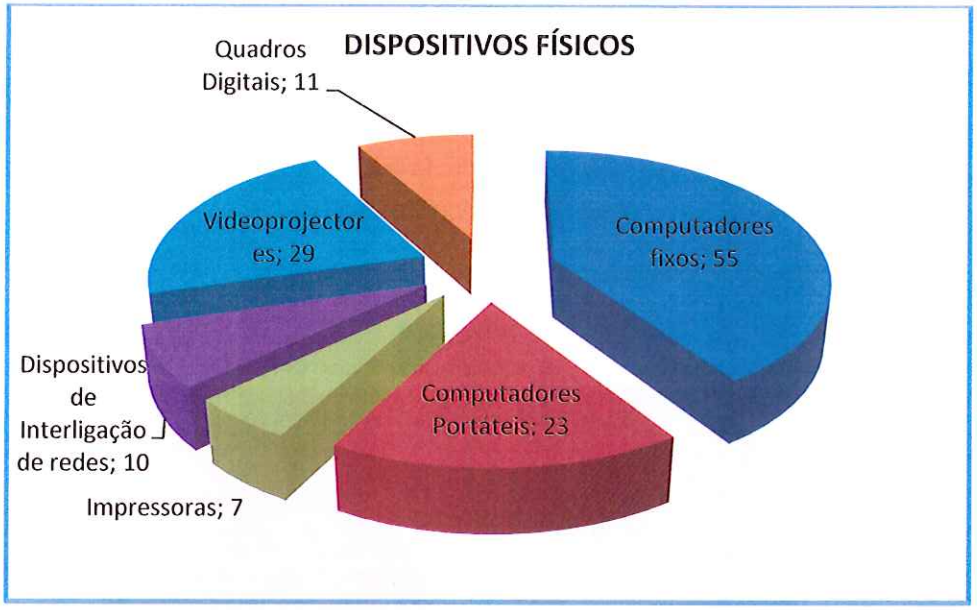


Figura 6 – Dispositivos físicos na SEC em 2010.

A escola utiliza um conjunto de Sistemas de Informação controlados e geridos pelo Departamento de Informática (DI). Em 2009 obteve o certificado da norma ISO 9001, tendo sido implementado o sistema de gestão de qualidade tendo como referência a Norma NP EN ISO 9001:2008. Apesar das vantagens associadas à sua aplicação, esta norma não prevê uma forma especifica para a gestão dos sistemas de informação. Ao longo dos últimos meses, foi efectuado um levantamento das Tecnologias de Informação, as quais são seguidamente apresentadas em forma de gráficos, no sentido de sintetizar a informação mais relevante para este diagnóstico.

No gráfico apresentado na figura 6, constata-se que existem no total 135 dispositivos de relevância para o diagnóstico em causa, dos quais os computadores fixos são os dispositivos que estão em maior número.

Relativamente à infra-estrutura de rede, a escola possui uma rede local LAN (*Local Área Network*), por cabo e *wireless*, que interliga todos os seus computadores. Os equipamentos são interligados por *switch* e *acess point*, sendo os periféricos compartilhados na rede para acesso dos computadores, impressoras, etc. Detém um único servidor onde se encontram todos os aplicativos administrativos partilhados assim como todos os serviços de acesso

à LAN e WAN (*Wide Area Network*). Por outro lado, em termos de infra-estrutura de ligação ao exterior, a instituição possui uma única ligação ADSL (*Asymmetric Digital Subscriber Line*).

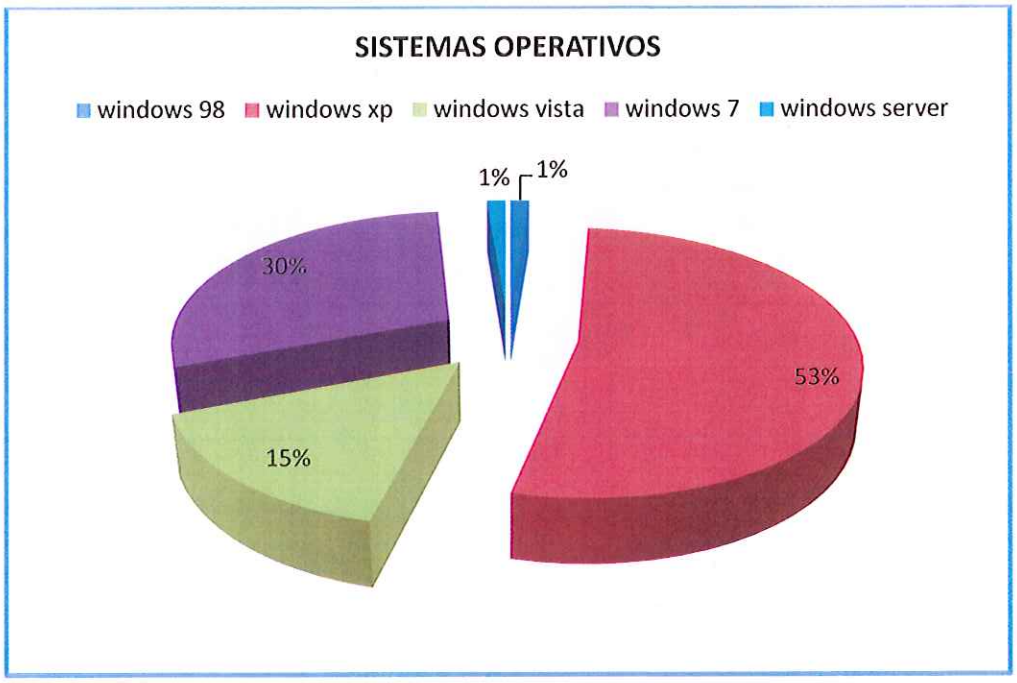


Figura 7 – Sistemas Operativos na SEC em 2010.

A Figura 7 ilustra a relação entre o número (em percentagem) de computadores por cada sistema operativo, o que, permite verificar a existência de 8 tipos de sistemas operativos, sendo o mais presente o Windows XP. Verificamos também, que existe unicamente um servidor em todo o parque informático. É de salientar que 36 desses computadores utilizam aplicativos administrativos como posto cliente.

A Figura 8 revela-nos a existência das 8 aplicações com utilização exclusiva para os serviços administrativos. Para além disso verificamos que a aplicação instalada em maior número (em percentagem) de computadores é o *GestFaltas* seguido de imediato pelo *WingaProfissional* e *Winga*, o qual são todas aplicações para a gestão dos recursos humanos (alunos e docentes) e pedagógicos.

Para este diagnóstico foi elaborado um inquérito, ao departamento de informática, o qual contém questões de extrema relevância para se determinar o estado em que estão as TI/SI.

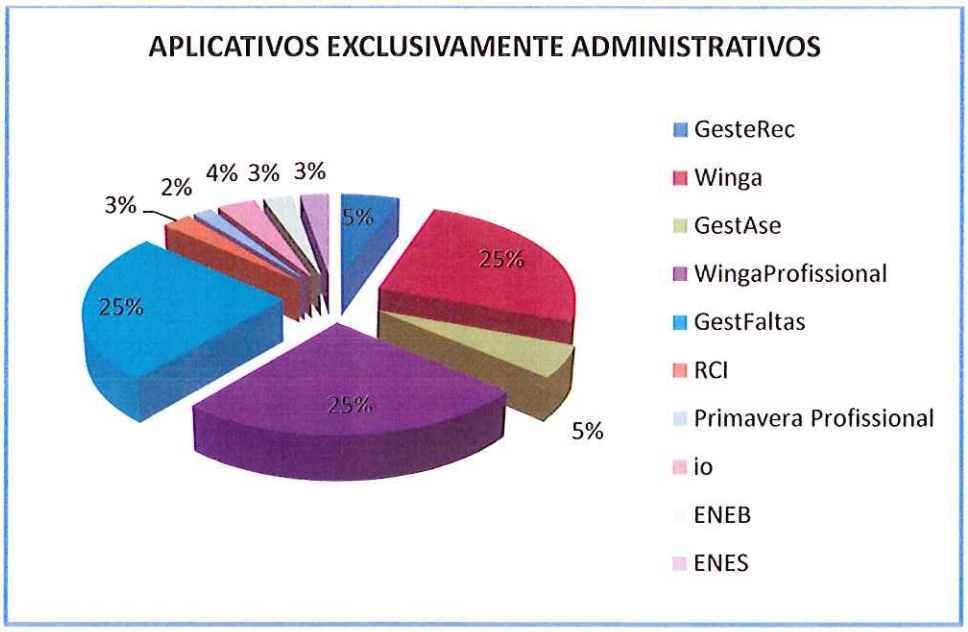


Figura 8 – Aplicações exclusivamente administrativos na SEC em 2010.

Após a análise desse inquérito e do levantamento de todas as TI/SI da SEC, constatou-se que, a gestão dos SI era realizada de forma *ad hoc* (não eficiente) apresentando diversas lacunas em termos de organização, especialmente na: infra-estrutura de rede, gestão de acessos aos sistemas, dificuldade no acompanhamento dos serviços prestados, dificuldade em controlar os *backups*, etc.

Dada a diversidade das TI e dos diferentes serviços de apoio administrativo, verificaram-se várias limitações e dificuldades, nomeadamente:

- Vários SI sem registo ou monitorização do seu desempenho: não existe um registo eficiente das informações relacionadas com os problemas que ocorrem nos componentes tecnológicos;
- Prestação de serviços aos utilizadores: embora o serviço seja executado não havia uma metodologia definida para o processamento de pedidos e o DI seguiram caminhos diferentes para executar a mesma tarefa.
- Registo eficaz das tarefas: as tarefas foram realizadas em vários documentos digitais (e papel) mas não estão centralizados;
- Dificuldade em realizar pesquisas e consultas dos componentes (hardware e software) de toda a infra-estrutura tecnológica;

- Dificuldade de centralizar, controlar e receber os pedidos de apoio do DI e a dificuldade de agilizar o processamento dos pedidos;
- Monitorização dos indicadores de desempenho: estes indicadores praticamente eram ausentes e quando existiam a forma como eles eram registados na monitorização não permitiam que fossem baseados em dados reais;
- Não havia planos de contingência, desempenho e recuperação de desastres;
- Agendamento de tarefas para a implementação de sistemas de monitorização: não existia um plano para fazer o agendamento de *backups* e monitorização associadas às TI e SI;
- Monitorização dos componentes da infra-estrutura de tecnologia: apesar de alguns SI serem monitorizados de forma *ad-hoc*, não houve registo de monitorização eficaz;
- Configuração da infra-estrutura tecnológica: As configurações da infra-estrutura tecnológica (acesso a dados, arquitectura de rede, etc) foram baseadas em documentos digitais (ou em formato papel) dispersos sem estarem centralizados para melhor controlo e gestão dos componentes da infra-estrutura tecnológica;
- O backup de dados e configurações dos sistemas era realizada *ad-hoc*, sem qualquer registo ou metodologia de rotina;
- Os serviços de suporte ao utilizador, componentes de aquisição, instalação e reconfiguração de componentes era realizado de uma forma *ad-hoc*, sem ser baseado em um procedimentos comuns, assim como não existia nenhum procedimento para o registo dos alunos nos SI;
- Dificuldades em prosseguir com o processo de mudança por parte dos colaboradores da escola devido a questões culturais.

Neste contexto, todas essas dificuldades não permitiam uma gestão e controlo eficiente sobre os componentes da infra-estrutura tecnológica e os serviços dos vários SI. Isso provocava dificuldades no desempenho dos serviços, em controlar as TI e dificuldade em aplicar as melhores práticas para resolver problemas e melhorar a qualidade dos serviços. Portanto, este diagnóstico demonstrou a necessidade implementar os referenciais COBIT e ITIL nesta

Instituição de Ensino Particular, para tentar suprir ou diminuir todas as falhas e ausências encontradas.

3.3 APLICAÇÃO DO ITIL

A aplicação do referencial ITIL foi considerada como parte da solução para atingir os objectivos propostos. Em consonância com o contexto apresentado no diagnóstico da SEC, alinhados aos seus objectivos estratégicos, a aplicação deste referencial teve como objectivo a adopção e adaptação das boas práticas de ITIL para a gestão de infra-estruturas das TI. Essa boas práticas foram traduzidas na escolha dos processos que melhor satisfazem os requisitos anteriormente mencionados.

Seguidamente são descritos todos processos [SCC2004], subdivididos em, gestão de Aplicações; Gestão da Infra-estrutura da Tecnologia de Comunicações e Informação e Gestão de Serviços, tidos em consideração para a aplicação do referencial ITIL na organização SEC.

- Gestão da Infra-estrutura da Tecnologia de Comunicações e Informação: Estes processos englobam todos os aspectos de gestão da infra-estrutura da Tecnologia de Comunicações e Informação desde a identificação dos requisitos do negócio, passando pelo projecto e implantação até o suporte e manutenção dos componentes da infra-estrutura e serviços das TI. Os processos escolhidos foram:
    1. *Projecto e Planeamento:* relacionados com a criação e melhoria da solução de TCI.
    2. *Operação:* refere-se à operação e à manutenção diária da infra-estrutura de TCI.
    3. *Suporte Técnico:* refere-se à estruturação e sustentação de outros processos para garantir os serviços implantados.

- Gestão de Serviços: O principal objectivo da gestão de serviços é certificar-se que os serviços das TI estão alinhados com as necessidades do negócio da empresa. Os processos de gestão de

serviços estão subdivididos em dois grupos: entrega de serviços e suporte de serviços. Os processos de entrega de serviços estão relacionados com o fornecimento de entrega de serviços ao utilizador e. Estes processos não foram escolhidos por não se enquadrarem com os objectivos propostos. Os processos de suporte de serviços estão relacionados com o fornecimento de suporte aos serviços que sustentam o negócio da empresa. Os processos que se adequam à organização em estudo são:

Gestão de Incidentes – Têm por objectivo restaurar a operação normal do serviço o mais rápido possível e garantir, desta forma, os melhores níveis de qualidade e disponibilidade do serviço.

Gestão de Problemas – Identifica e remove erros do ambiente das TI, através da análise dos incidentes registados no gestão de incidentes, de forma a garantir uma o máximo de estabilidade possível dos serviços de TI.

Gestão de Configuração – Auxilia na gestão do ambiente de TI através do registo de todos os seus itens numa base de dados efectuando um controlo dos componentes da infra-estrutura das TI utilizados na realização dos serviços de TI.

Gestão de Mudanças – Trata da realização de mudanças na infra-estrutura das TI de forma segura e organizada através da implementação de procedimentos que passam pela avaliação do impacto da mudança, autorização e planeamento da sua implementação.

Gestão de Versões – Assegura que apenas versões testadas e correctas do software autorizado sejam disponibilizadas para a operação controlando, armazenando, distribuindo e implementando software efectivamente e eficientemente.

Este referencial permitiu identificar quais os processos que se adequam com os objectivos estratégicos definidos pela SEC, os quais foram mapeados para o

referencial COBIT e convertidos em procedimentos para serem operacionalizados. Estes processos e procedimentos vão ser descritos e apresentados no seguinte Subcapítulo (3.4 Aplicação do COBIT). Contudo, este referencial foi considerado como uma solução parcial porque não detêm todos os processos necessários, como os de auditoria e controlo dos processos, entre outros, os quais vão ser proporcionados pelo referencial COBIT.

3.4 APLICAÇÃO DO COBIT

O diagnóstico efectuado à instituição SEC indicou, em parte, que a aplicação do COBIT seria uma solução para o objectivo pretendido. De acordo com o contexto apresentado no diagnóstico devem ser seleccionados um subconjunto de objectivos, actividades e indicadores de execução para implementar o referencial COBIT. Relativamente à documentação ISO 9001 (matriz de processos, procedimentos, formas, etc.) a identificação dos processos e pedidos tem a seguinte representação específica: GSI- Número dos procedimentos e GSI/Número para os formulários. Esta representação é mencionada e apresentada, nas figuras, ao lado dos procedimentos, a fim de esclarecer a utilização da documentação do SGQ (Sistema de Gestão de Qualidade). O COBIT cobre todas as áreas das TI e no que refere à sua aplicação à realidade da SEC foram seleccionadas algumas actividades. Como menciona o referencial COBIT, encontra-se dividido em quatro domínios e cada um é caracterizado por um conjunto de processos. Para fazer o mapeamento do COBIT, e considerando que o SGQ da SEC continha muitos tipos de casos, optou-se por considerar os sub-processos da Gestão de Sistema de Informação (GSI), que correspondem aos quatro domínios do COBIT, e para cada sub-processo consideraram-se as actividades a partir do subconjunto de objectivos de controlo do COBIT. Além disso, cada actividade dos objectivos de controlo COBIT foi mapeado no âmbito dos procedimentos de cada actividade do sub-processo.

geral do processo), uma coluna com os documentos e registos utilizados em cada etapa do processo e, finalmente, uma coluna com os responsáveis de cada etapa do fluxo de itens. Como um exemplo simples de um procedimento, a figura 10 e 11 apresentam dois procedimentos para a elaboração de um plano Estratégico e Táctico dos SI.

2) Aquisição e Manutenção dos Sistemas de Informação:

Este sub-processo está centrado na definição de procedimentos para realizar a estratégia das TI definidos no plano estratégico das TI do sub-processo " Planeamento e Organização dos Sistemas de Informação". Ele define os procedimentos para proceder à aquisição, instalação e manutenção dos componentes da infra-estrutura tecnológica da SEC. Como entrada deste domínio foi definida a necessidade de estabelecer procedimentos para adquirir, instalar e manter os componentes da infra-estrutura tecnológica, o plano estratégico e os documentos de origem externa. A saída são os procedimentos para realizar a compra instalação, e manutenção dos componentes das infra-estrutura tecnológicas. Como actividades deste domínio, temos: aquisição de componentes para a infra-estrutura tecnológica, instalar, reinstalar e configurar os componentes dessa infra-estrutura tecnológica e manutenção dos componentes da infra-estrutura tecnológica. O objectivo dos procedimentos apresentados nas figura 12, 13 e 14 é para definir os passos a fim de adquirir componentes para a infra-estrutura tecnológica, instalar, reinstalar e configurar os componentes da infra-estrutura tecnológica e manutenção dos componentes da infra-estrutura tecnológica.

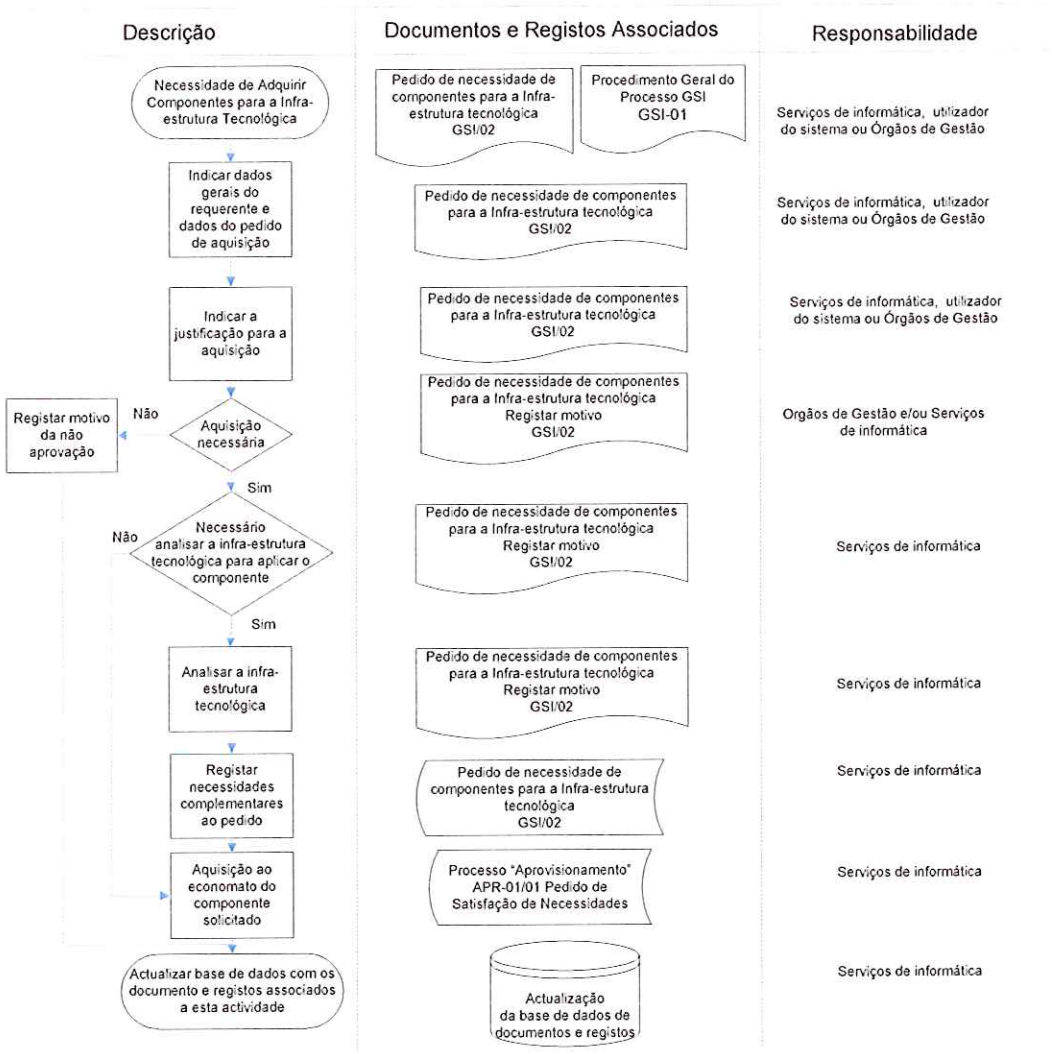


Figura 12 – Procedimento para adquirir componentes para a infra-estrutura tecnológica.

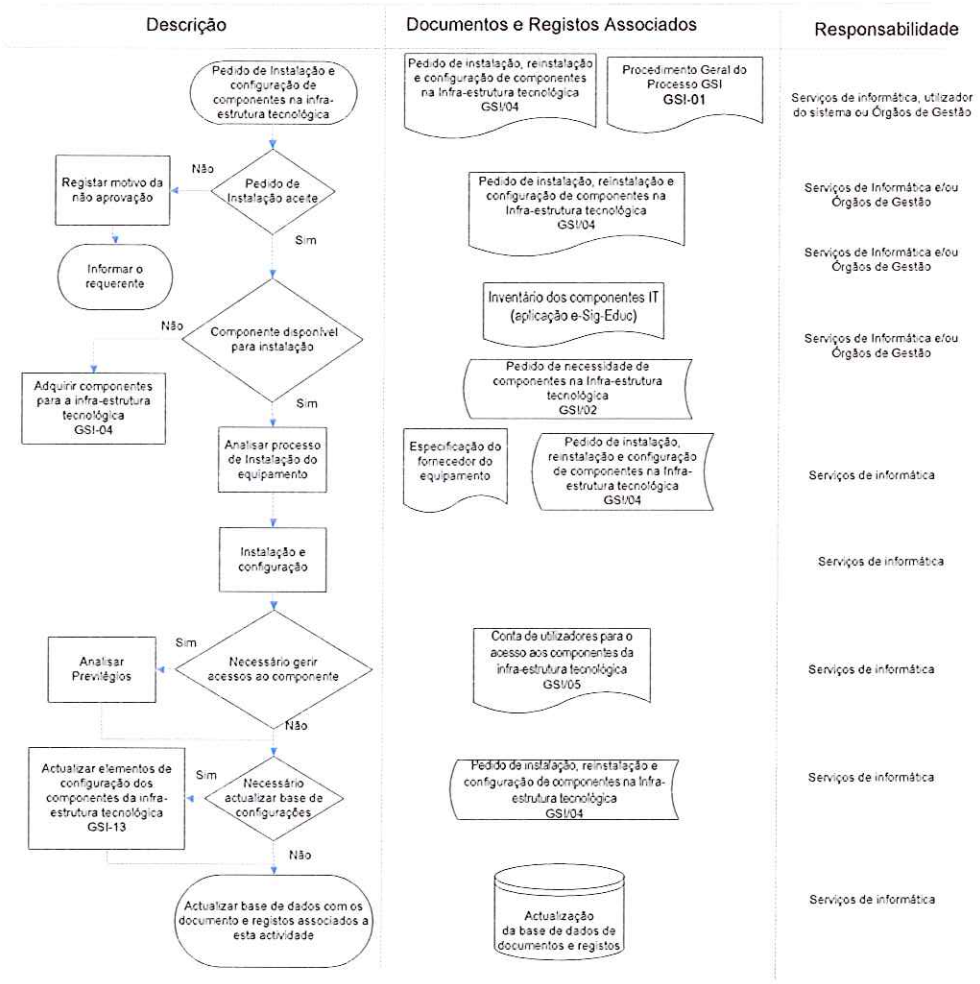


Figura 13 – Procedimento para instalar, reinstalar e configurar os componentes da infra-estrutura tecnológica.

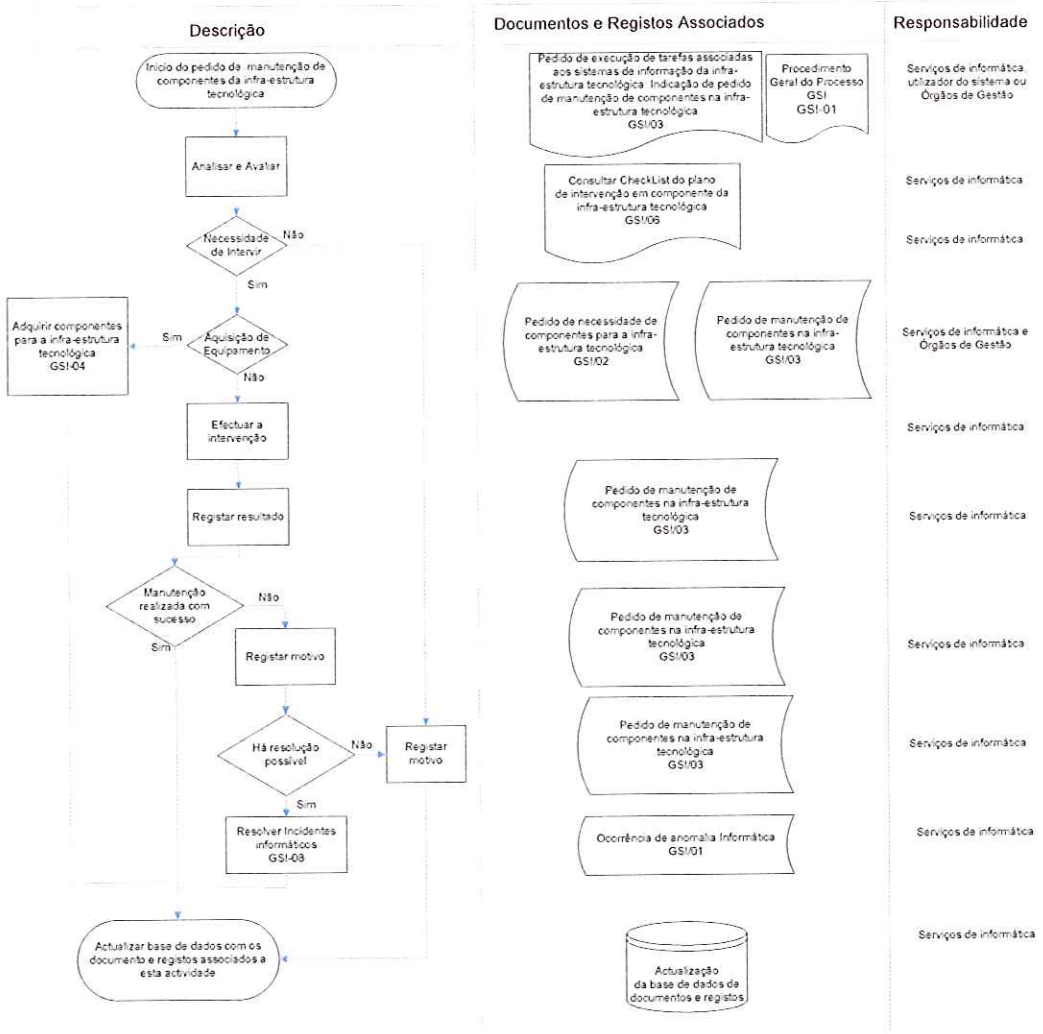


Figura 14 – Procedimento para manter os componentes da infra-estrutura tecnológica.

3) Disponibilização e Suporte dos Sistemas de Informação:

Este sub-processo define os procedimentos para disponibilizar aos utilizadores os SI e as TI. Como entrada deste domínio foi definida a necessidade de estabelecer procedimentos para assegurar a disponibilidade e suporte das TI, planeamento estratégico e os documentos de origem externa. Os resultados de saída são os procedimentos para assegurar o suporte e a disponibilidade das TI. Neste sub-processo existem procedimentos definidos para caracterizar as seguintes actividades definidas pelo referencial COBIT:

3.1) Gestão de Incidentes Informáticos na infra-estrutura tecnológica: o objectivo desta actividade é fazer com que os procedimentos disponíveis possam dar uma resposta efectiva e rápida às questões e problemas das TI apresentados pelos diferentes utilizadores.

3.2) Gestão dos dados da infra-estrutura tecnológica: esta actividade está centrada na gestão dos dados e inclui procedimentos para a gestão da biblioteca digital, *backups* e recuperação, a fim de garantir a qualidade, a resposta em tempo útil e disponibilidade dos dados necessários para as actividades da Instituição.

3.3) Gestão das configuração dos componentes da infra-estrutura tecnológica: um sistema eficaz de gestão da configuração contribui para fiabilidade do sistema, minimizando o número de ocorrências e contribuindo para uma maior velocidade nas soluções. Neste contexto, esta actividade inclui a recolha de informação das configurações de componentes da infra-estrutura tecnológica.

3.4) Garantir a segurança dos componentes da infra-estrutura tecnológica: o objectivo desta actividade é centrada na necessidade de manter a integridade das informações e proteger os processos de gestão das TI solicitando processos de gestão de segurança. Esses processos incluem procedimentos para estabelecer e manter regras e responsabilidades de segurança, política, normas e procedimentos para actuar na área das TI.

3.5) Gestão do desempenho e da capacidade dos componentes da infra-estrutura tecnológica: a fim de garantir a qualidade dos serviços disponibilizados pelas TI, existe a necessidade de gerir a qualidade e a capacidade dos recursos dos componentes da infra-estrutura tecnológica. Essa actividade define um plano de acção e a possibilita os componentes da infra-estrutura tecnológica sejam testados, monitorizados e avaliados (no sub-processo "monitorizar e avaliar os Sistemas de Informação", a fim de garantir a qualidade dos serviços disponibilizados pelas TI).

3.6) Assegurar a continuidade de serviço dos componentes da infra-estrutura tecnológica: a necessidade de disponibilizar a continuidade dos serviços das TI exige o desenvolvimento, manutenção e testes aos planos de continuidade, suportado pelos procedimentos de armazenamento de dados e testes periódicos para o plano de continuidade. Essa actividade define um plano para garantir a continuidade dos serviços, para minimizar a probabilidade e o impacto da interrupção dos serviços nos processos e funções-chave na utilização das TI.

3.7) Gerir as operações dos componentes da infra-estrutura tecnológica: esta actividade inclui a definição de procedimentos para definir os procedimentos das operações associadas aos componentes da infra-estrutura tecnológica, como por exemplo, definir os procedimentos para realizar *backups*, restaurar backup, testar e avaliar a segurança, a continuidade e o desempenho dos componentes das TI. O resto das actividades deste sub-processo são: *service desk* do utilizador, desenvolver e manter a política e os requisitos para executar os *backups*, fazer *backups* e restaurar *backups*, actualizar as versões dos documentos dos SI, desenvolver e manter um repositório de definições para o componentes de infra-estrutura tecnológica, actualização de elementos de configuração dos componentes de infra-estrutura tecnológica, definir e manter o plano de segurança dos componentes da infra-estrutura tecnológica, definir e manter os privilégios dos utilizadores nos componentes de infra-estrutura tecnológica, gerir as contas dos utilizadores da infra-estrutura tecnológica, definir, planear e manter o desempenho e capacidade dos componentes da infra-estrutura tecnológica, definir e manter o plano de contingência para garantir a continuidade dos serviços, definir e manter o plano de recuperação de desastres da infra-estrutura tecnológica, definir e manter o plano de acção para ser executado no período de recuperação de desastres, definir e manter o plano de intervenção nos componentes de infra-estrutura tecnológica, bem como definir e manter o plano da agenda de

tarefas para controlar e monitorizar os componentes de infra-estrutura tecnológica.

As figuras seguintes (Figura 15, 16 17 e 18) apresentam os procedimentos derivados deste sub-processo.

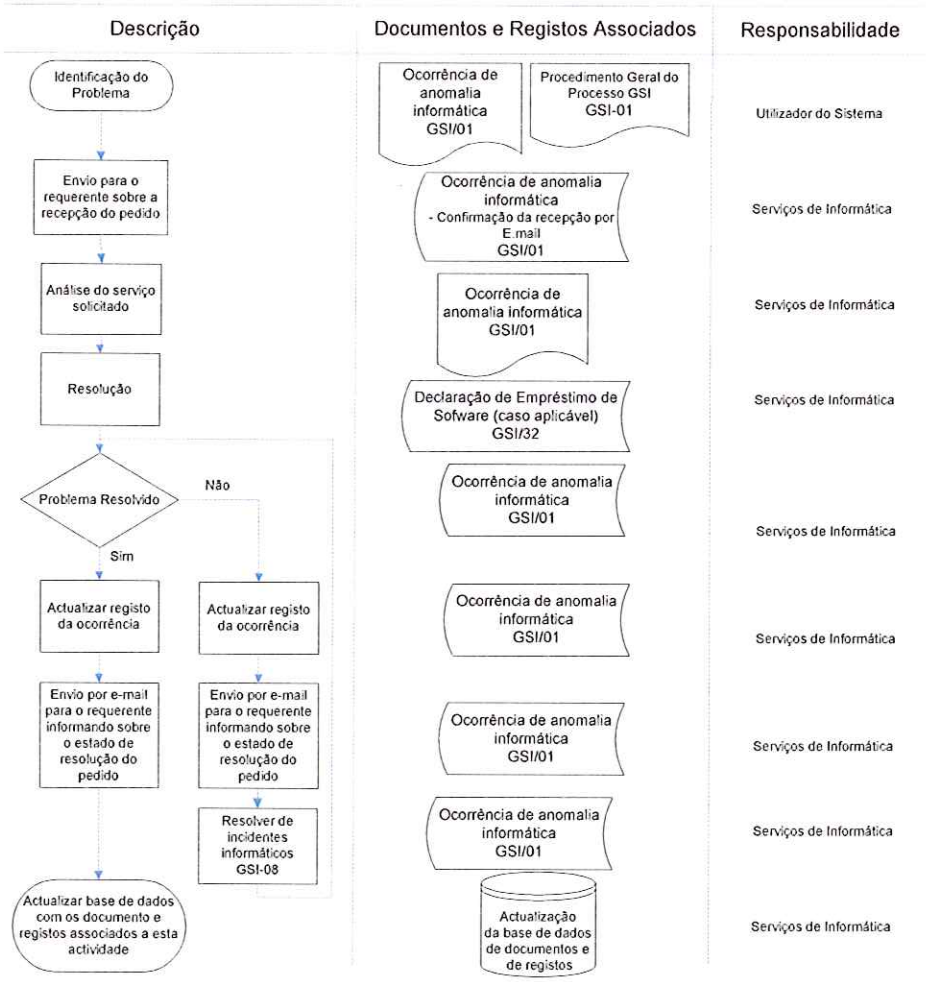


Figura 15 – Procedimento para o serviço de utilizadores.

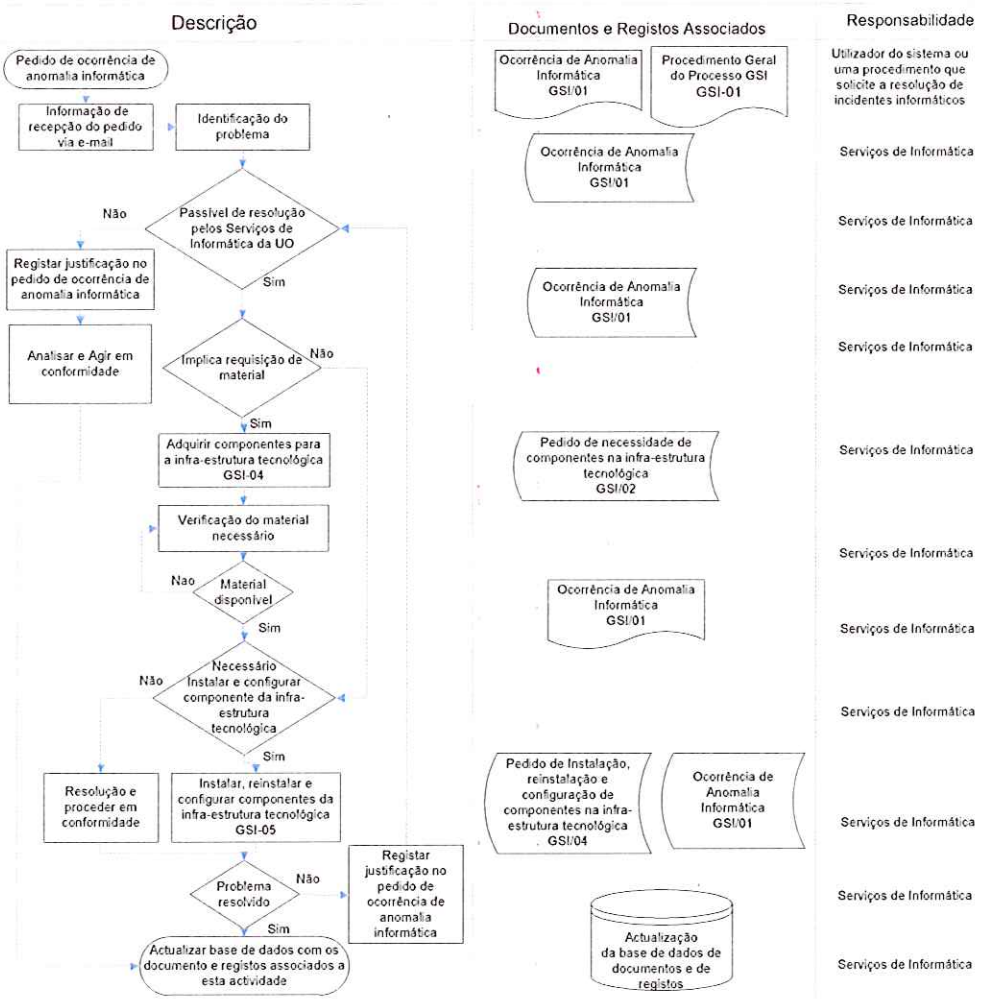


Figura 16 – Procedimento para resolver incidentes informáticos.

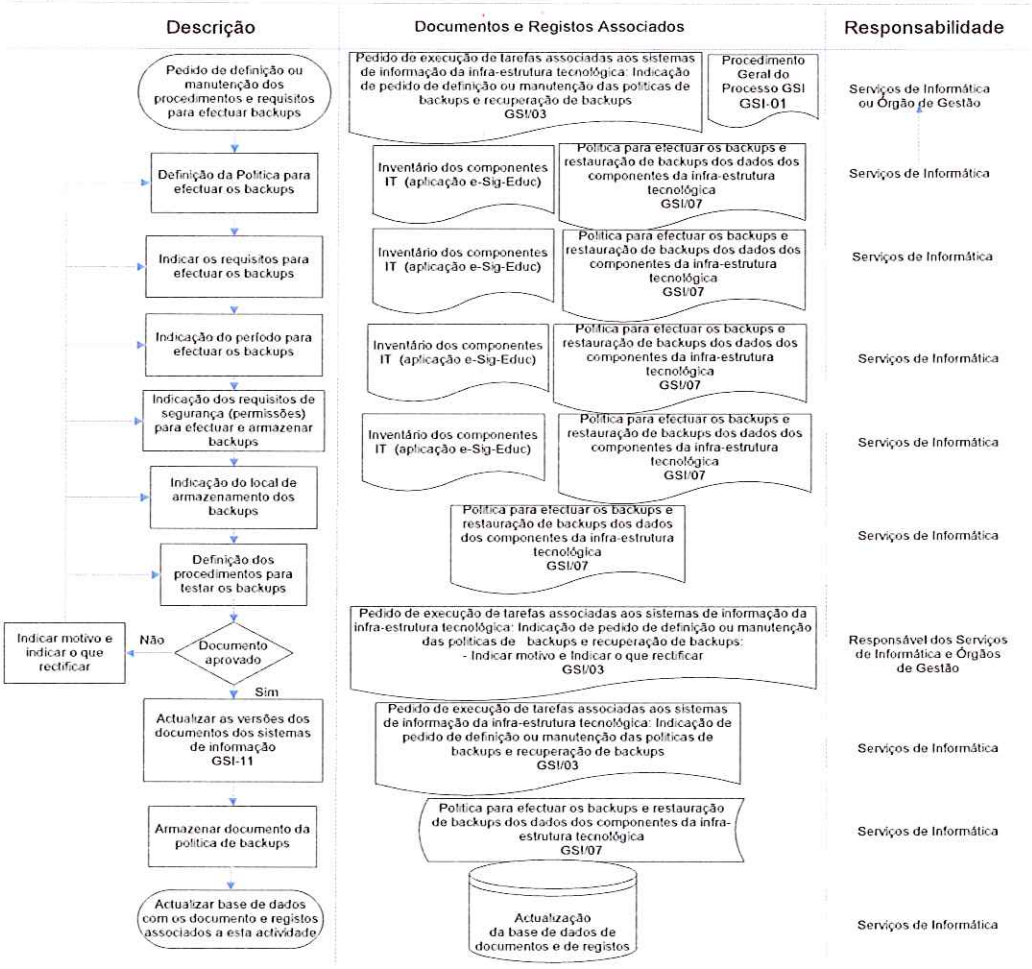


Figura 17 – Procedimento para definir e manter a política e requisitos para efectuar os *backups*.

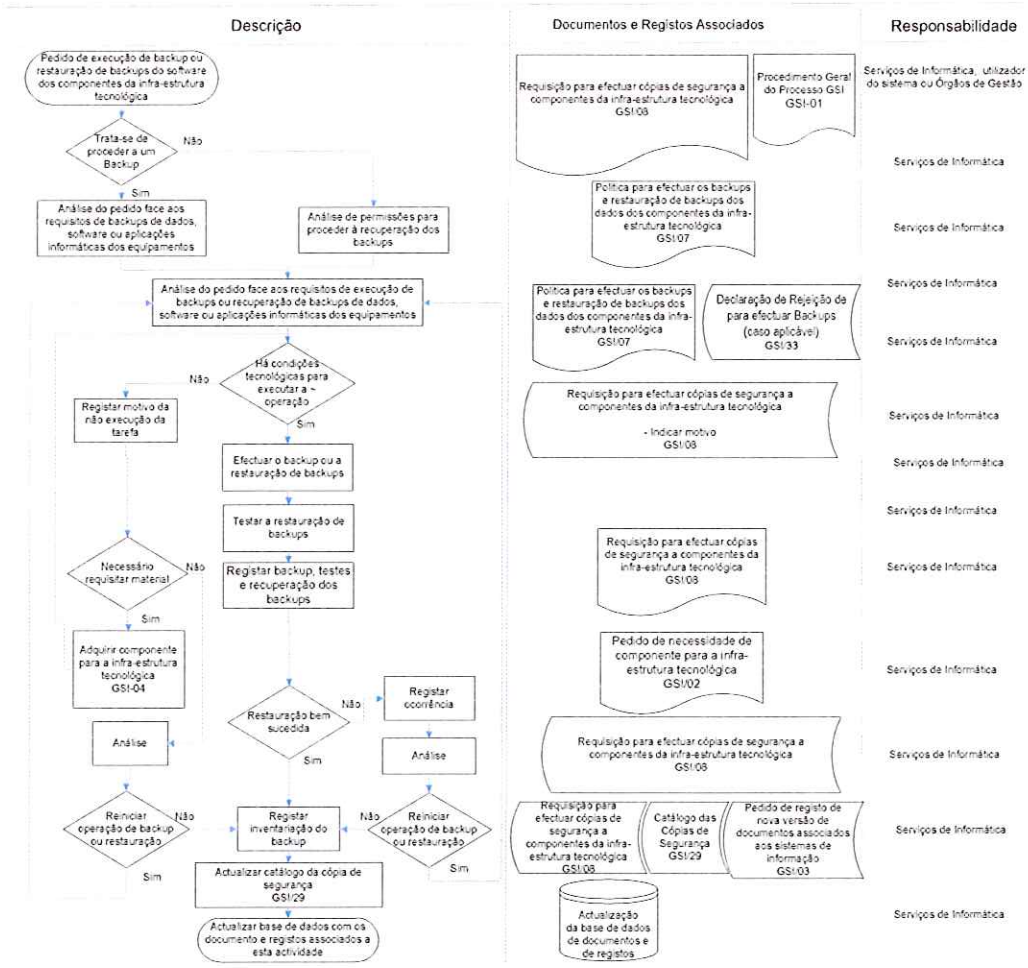


Figura 18 – Procedimento para efectuar *backups* e restauração de *backups*.

4) Monitorização e Avaliação dos Sistemas de Informação:

Todos os processos das TI têm de ser disponibilizados em tempo oportuno de modo a garantir a qualidade e para garantir o plano estratégico das TI na organização. Neste contexto, este sub-processo é centrado na definição de procedimentos para testar, monitorizar e avaliar o desempenho, a segurança e a disponibilidade das TI. Como entrada deste domínio foi definida a necessidade de estabelecer procedimentos para testar, monitorizar e avaliar a qualidade dos serviços prestados pelas TI. Como saída, temos procedimentos e relatórios para a monitorização dos componentes da infra-estrutura tecnológica a fim de garantir a qualidade do Serviço da Informação da SEC.

As seguintes figuras (Figura 19 e 20) apresentam os procedimentos efectuados para este sub-processo.

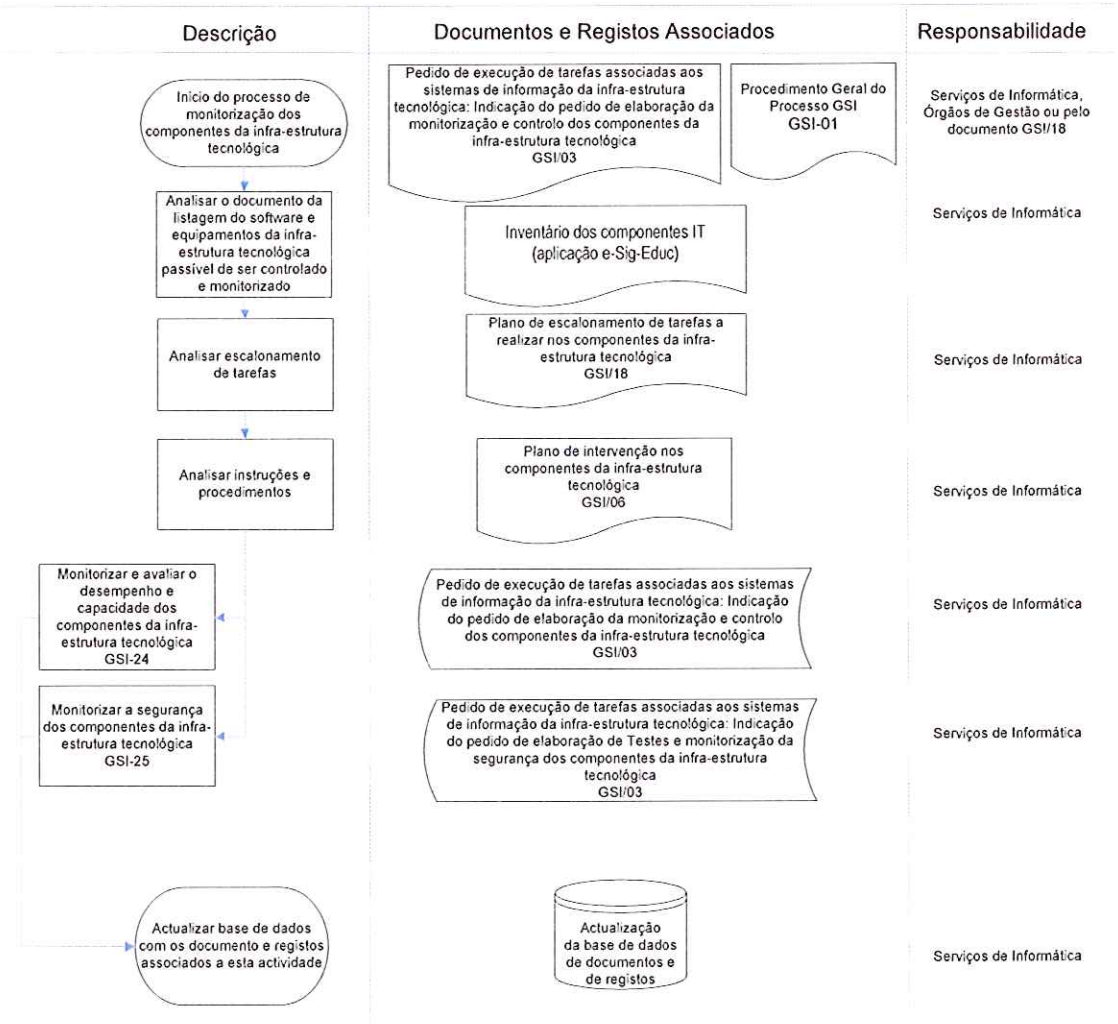


Figura 19 – Procedimento para monitorizar e controlar os componentes da infra-estrutura tecnológica.

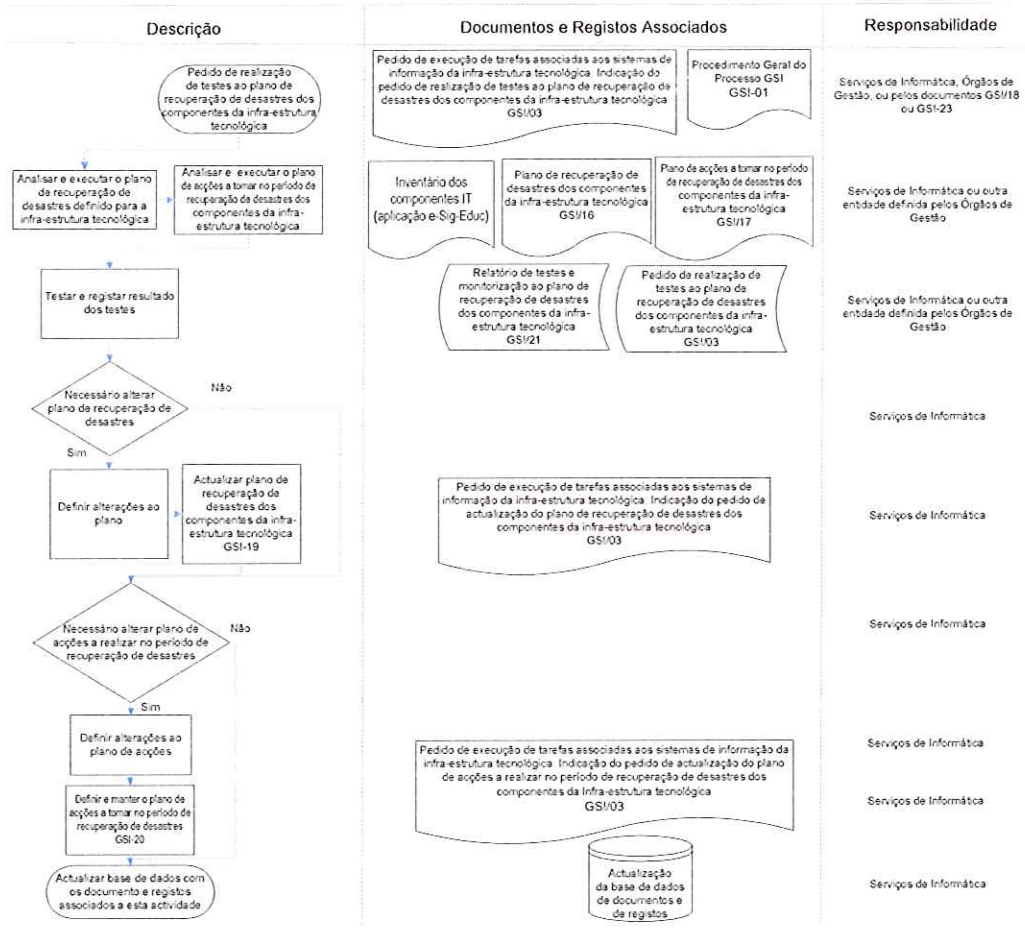


Figura 20 – Procedimento para testar o plano de recuperação de desastres dos componentes da infra-estrutura tecnológica.

No sentido de utilizar os procedimentos torna-se necessário em qualquer estrutura documental de um referencial, a criação de impressos especialmente orientados para a requisição ou registo da situação associada aos componentes de infra-estrutura tecnológica. Neste contexto e no seguimento dos procedimentos ilustrados nas figuras anteriores, foram criados vários impressos necessários descritos na seguinte tabela:

Impresso	Descrição	Objectivo
GSI/01	Ocorrência de anomalia informática	Efectuar o registo de anomalias informáticas
GSI/02	Pedido de necessidades de componentes para a Infra-estrutura tecnológica	Efectuar o registo dos pedidos das necessidades de componentes da Infra-estrutura tecnológica
GSI/03	Pedido de execução de tarefas	Efectuar o registo da execução de

Impresso	Descrição	Objectivo
	associadas aos sistemas de informação da infra-estrutura tecnológica	tarefas associadas aos sistemas de informação da infra-estrutura tecnológica
GSI/04	Pedido de instalação, reinstalação de componentes para a Infra-estrutura tecnológica	Efectuar o registo dos pedidos de instalação, reinstalação de componentes para a Infra-estrutura tecnológica
GSI/05	Conta de utilizadores para o acesso aos componentes da infra-estrutura tecnológica	Efectuar o registo das contas dos utilizadores para o acesso aos componentes da infra-estrutura tecnológica
GSI/06	Plano de intervenção em componentes na Infra-estrutura tecnológica	Efectuar o registo dos planos de intervenção em componentes na Infra-estrutura tecnológica
GSI/07	Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica	Descrever a politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica
GSI/08	Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica	Efectuar o registo das Requisições para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica
GSI/09	Versões dos documentos associados aos Sistemas de Informação	Efectuar o registo das versões dos documentos associados aos Sistemas de Informação
GSI/10	Esquema do modelo da base de dados de configurações	Efectuar o registo dos esquemas de modelos de base de dados de configurações
GSI/11	Configurações dos componentes da infra-estrutura tecnológica	Efectuar o registo dos esquemas das Configurações dos componentes da infra-estrutura tecnológica

Tabela 2 – Impressos inerentes ao Processos.

Temos de referir que a estrutura dos impressos está enquadrada com as orientações da nomenclatura associada à estrutura documental da implementação da norma ISO 9001.

3.5 OPERACIONALIZAÇÃO

No sentido de proceder à operacionalização da Gestão dos Sistemas de Informação (GSI) proposto como solução aos objectivos propostos na aplicação dos referenciais COBIT e ITIL, consideramos ser necessário realizar quatro actividades, que são:

- Afectação de Recursos Humanos;
- Realizar campanhas de divulgação;
- Desenvolver um sistema de informação para o GSI, em ambiente Web (Portal);
- Disponibilizar formação sobre os Processos e sobre o Portal Web.

No sentido de orientar a aplicabilidade deste estudo e em gerir os recursos e a mudança por parte da comunidade, torna-se necessário a alocação de recursos num espírito de equipa heterogénea que vai ser responsável por operacionalizar todo este processo: desde a formação dos colaboradores, dos professores, dos alunos e do pessoal técnico; a criação do sistema de informação e a gestão do sistema de informação.

Tipo	Designação	Quantidade
Computador	Servidor Web	1
Computador	Servidor *Backups*	1
Computador	PC Fixo	4
Quadro interactivo	Quadro interactivo digital	1
Firewall	Firewall Física	1

Tabela 3 – Requisitos de Hardware

A campanha de divulgação deve ser efectuada em diferentes momentos da implementação deste processo, de forma a podermos mostrar o que estava a

ser desenvolvido assim como mostrar quais o benefícios que isso acarreta a todos os colaboradores. Podem ser utilizados diferentes meios de comunicação, desde email, o portal da escola, boletins informativos e os meios formais de comunicado interna.

Tipo	Designação	Quantidade
Sistema Operativo	Windows 7	3
Sistema Operativo	Windows XP	1
Sistema Operativo	Windows Server 2003	1
Aplicativo	OCS Inventory NG Reports	1
Desenvolvimento	Software livre diversificado	-

Tabela 4 – Requisitos de Software

Desenvolver um sistema de informação para o GSI, em ambiente Web (Portal), permite criar um sistema com custos reduzidos, acessibilidades extraordinárias para todos os utilizadores do sistema de informação e por ser uma estrutura em continua expansão.

3.6 AVALIAÇÃO

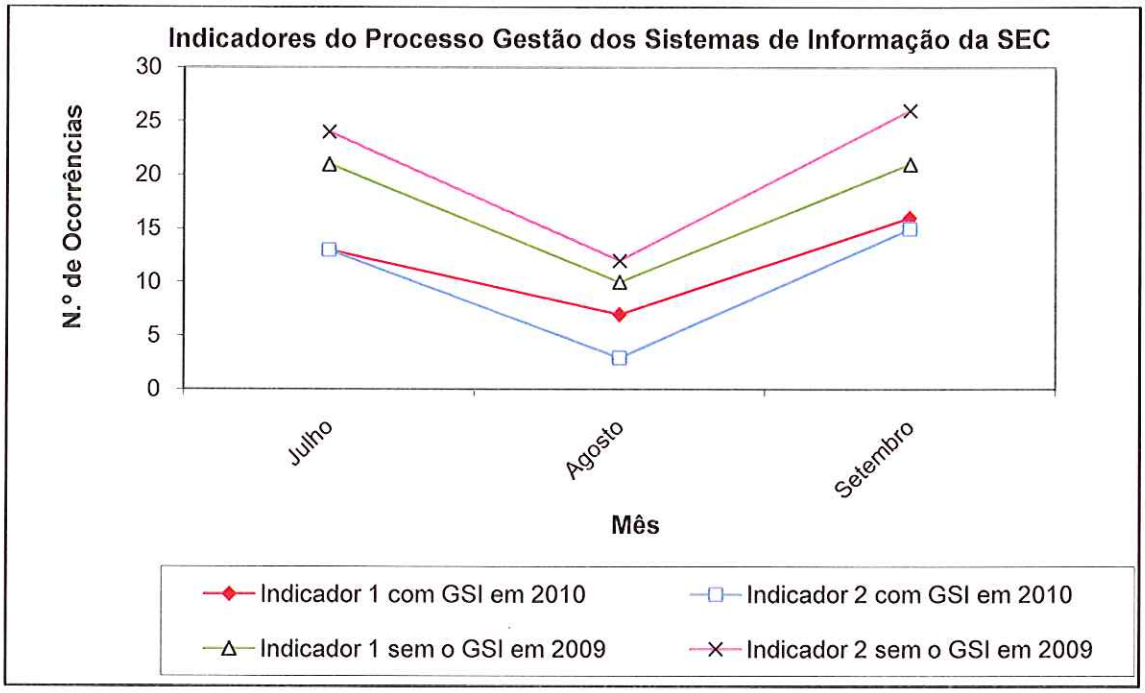
Para avaliar a utilização e implementação do processo GSI foram definidos dois conjuntos de indicadores. O primeiro (tabela 5) tem o objectivo de analisar o começo da utilização do GSI e o segundo conjunto, será adicionado aos poucos ao longo do tempo Esses indicadores serão: tempo médio para configurar os componentes de infra-estrutura, número de componentes de infra-estruturas que não são mais suportáveis, número de horas perdidas por utilizador por mês devido à insuficiente capacidade de planeamento, percentagem de reuniões de ser que satisfazem os níveis de serviço, percentagem dos erros encontrados durante a revisão de garantia de qualidade da instalação e funções de acreditação e aplicação do tempo ou correcções de dados causado por testes inadequados). Temos também o acompanhamento dos níveis de satisfação e de formação associados com os clientes/utilizadores deste processo.

Temos no entanto de salientar que estes indicadores apenas são possíveis de obter se houver respostas. Por este facto a informação associada a estes indicadores é obtida a partir das respostas efectuadas através dos impressos apresentados na secção anterior.

Indicadores/ Metricas	Designação	Objectivo	Acompanhamento
1	Número de pedidos de apoio por parte dos utilizadores originada pela sua inadequada formação	< 50	Annual
2	Número de ocorrências anual por aplicação de software dos servidores que provocaram quebras de funcionamento	< 75	Annual
3	Média do tempo (dias) de resposta até à recuperação do componente da infra-estrutura tecnológica sem aquisição de componentes	< 4 dias	Annual
4	Taxa de incidentes que requerem suporte no local (fora dos Serviços de Informática) da ocorrência	< 50%	Annual
5	Taxa de ocorrências resolvidas e finalizadas da responsabilidade dos Serviços de Informática	> 60%	Annual
6	Taxa de incidentes reabertos	< 20%	Annual
7	Taxa de *backups* dos dados críticos (definido pela política de *backups*)	> 90 %	Mensal
8	Taxa de testes de sucesso a *backups* dos dados dos Sistemas de Informação	> 90 %	Mensal

Tabela 5 -Lista de indicadores disponíveis na implementação do GSI.

Para este estudo, o acompanhamento dos indicadores foi realizado entre Julho e Setembro de 2010. Os três meses de análise dos indicadores apresentados neste estudo foram comparados com o mesmo período registado em 2009 (sem o uso do GSI) e sem a aplicação de um sistema de monitorização para os indicadores de desempenho. Realçamos que este trabalho de operacionalização decorreu durante seis meses do ano 2010. No sentido de proceder a uma comparação com o ano anterior, os valores para 2009 foram estimados com base em registos mantidos manualmente e registado em papel Departamento de Informática. Para mostrar os resultados de uma forma mais perceptível, dividimos os indicadores e cada um vai ser comparado com os mesmos períodos do ano de 2009, conforme apresentam os gráficos ilustrados nas figuras seguintes.

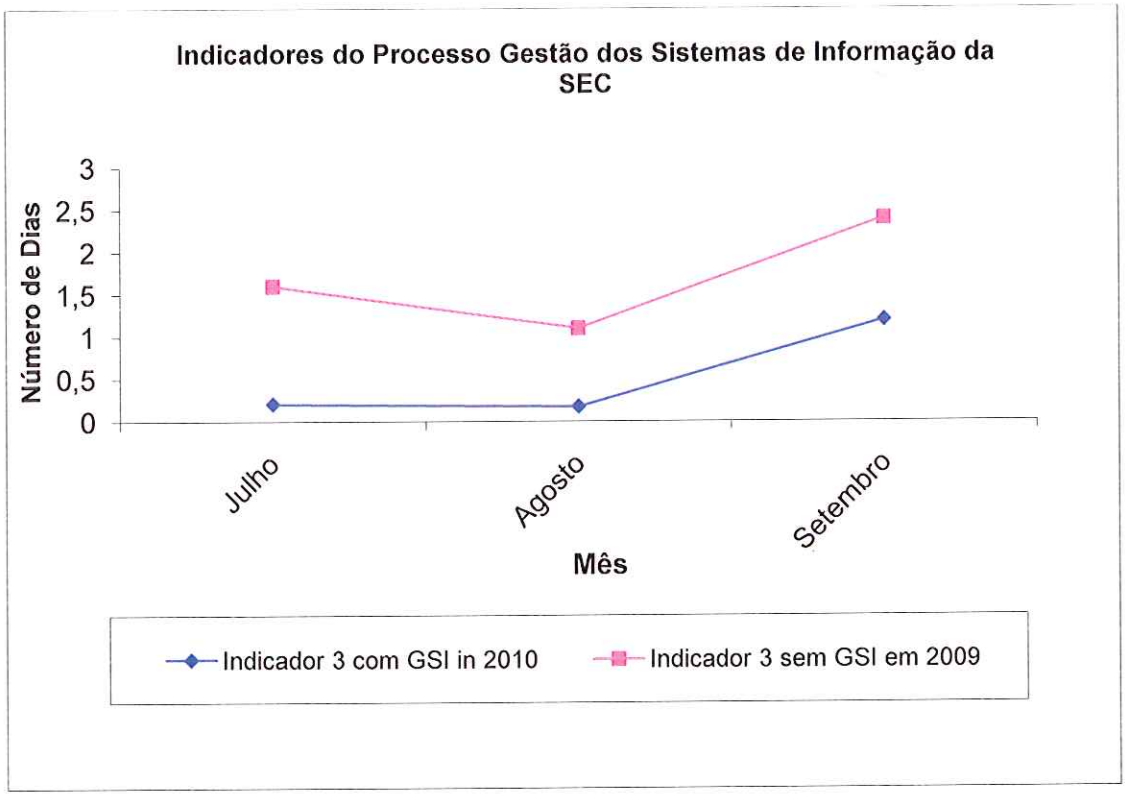


Indicadores/Metricas	Designação	Objectivo	Acompanhamento
1	Número de pedidos de apoio por parte dos utilizadores originada pela sua inadequada formação	< 50	**Annual**
2	Número de ocorrências anual por aplicação de software dos servidores que provocaram quebras de funcionamento	< 75	**Annual**

Figura 21 – Comparação dos indicadores 1 e 2 em 2009 e 2010.

Na Figura 21 estão representados os resultados dos indicadores comparativos 1 e 2 em 2009 sem utilizar o GSI e em 2010 utilizando o GSI. Como podemos verificar o número de pedidos de apoio dos utilizadores causado pela formação inadequada (indicador 1) e o número de ocorrências anual por aplicação de software dos servidores que provocaram quebras de funcionamento (indicador 2) são mais elevados em 2009 do que em 2010. O facto é que com a implementação do GSI e de vários mecanismos estratégicos determinou que, por um dos lados garantiu um melhor nível de formação dos utilizadores, e por outro permitiu definir mecanismos de controlo mais eficientes para monitorizar e controlar os componentes da infra-estrutura tecnológica. Constata-se que há uma melhoria nos indicadores de cerca de 15% para 2010 (com a utilização do GSI) relativamente a 2009 (sem a utilização do GSI).

Para o indicador "Média do tempo (dias) de resposta até à recuperação do componente da infra-estrutura tecnológica sem aquisição de componentes", podemos encontar os dados na Figura 22.

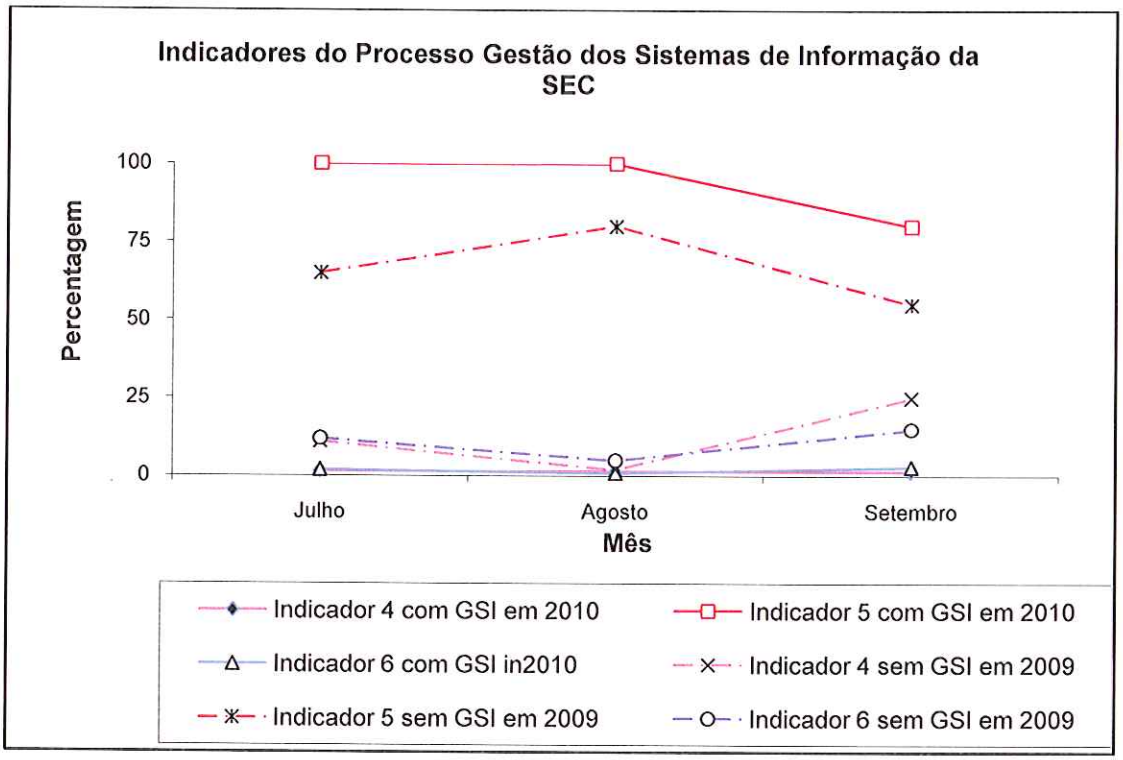


Indicadores/Metricas	Designação	Objectivo	Acompanhamento
3	Média do tempo (dias) de resposta até à recuperação do componente da infra-estrutura tecnológica sem aquisição de componentes	< 4 dias	Annual

Figura 22 – Comparação do indicador 3 em 2009 e 2010.

O número de dias para responder em 2010, comparativamente a 2009 caiu cerca de 25%, com uma redução efectiva de mais de um dia e meio. Isto deveu-se a estrutura interna dos serviços do Departamento de Informática, a várias orientação estratégica e à execução do processamento dos pedidos com base nos procedimentos do GSI. Na Figura 23 mostramos os resultados dos indicadores 4, 5 e 6. A taxa de incidentes que necessitam de apoio no local (fora dos serviços de identificação) da ocorrência (indicador 4), em 2010, relativamente a 2009 diminuiu cerca de 7,4%. A razão para essa melhora deve-

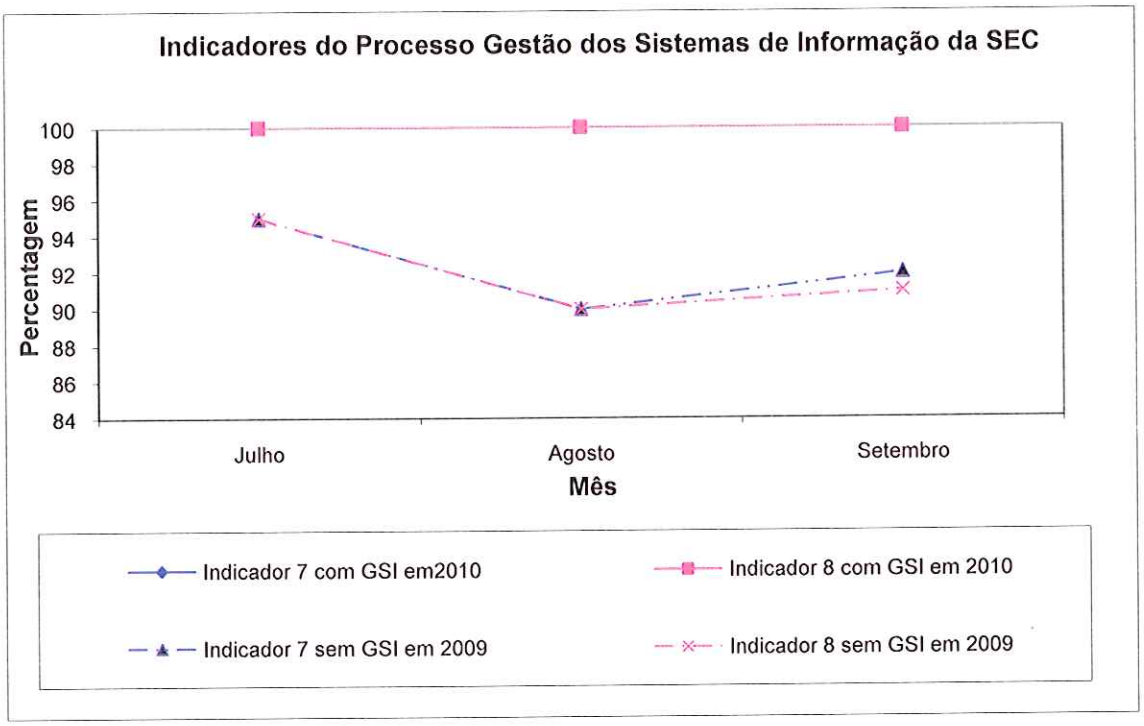
se a uma maior eficiência no tipo de instalação, configuração, e manutenção dos componentes na sua primeira utilização e manutenção regular.



Indicadores/Metricas	Designação	Objectivo	Acompanhamento
4	Taxa de incidentes que requerem suporte no local (fora dos Serviços de Informática) da ocorrência	< 50%	Annual
5	Taxa de ocorrências resolvidas e finalizadas da responsabilidade dos Serviços de Informática	> 60%	Annual
6	Taxa de incidentes reabertos	< 20%	Annual

Figura 23 – Comparação dos indicadores 4, 5 e 6 em 2009 e 2010.

A Taxa de ocorrências resolvidas e finalizadas da responsabilidade dos Serviços de Informática (indicador 5 da Figura 23) melhorou, em 2009 foi cerca de 70% e em 2010 92%. Isto deveu-se a definição de prioridades e de uma definição mais eficiente do planeamento e da manutenção em comparação com 2009, a taxa de incidentes reabertos (indicador 6 da Figura 23) diminuiu cerca de 10% onde em 2009 teve 10,7% e 1,3% em 2010. Isso é justificado pelo aumento de eficiência do DI no processamento de solicitações de utilizadores, assim como na manutenção de equipamentos.



Indicadores/Metricas	Designação	Objectivo	Acompanhamento
7	Taxa de *backups* dos dados críticos (definido pela política de *backups*)	> 90 %	**Mensal**
8	Taxa de testes de sucesso a *backups* dos dados dos Sistemas de Informação	**> 90 %**	**Mensal**

Figura 24 – Comparação dos indicadores 7 e 8 em 2009 e 2010.

Com a implementação do COBIT vários planos foram elaborados (segurança, contingência, escala, intervenção), bem como a política para fazer *backups*. Com a implementação dos *backups*, a taxa de *backups* de dados críticos (definida pela política de *backups*) - Indicador 7 (mencionado na Figura 24) e Taxa de testes de sucesso a *backups* dos dados dos Sistemas de Informação – Indicador 8 (mencionado na Figura 24) é de 100%. Isto é devido à implementação de mecanismos robustos para fazer os *backups*, bem como o número de cópias de segurança de várias gerações da SEC. Em 2009, os mecanismos para fazer *backups* eram bastante mais limitados em comparação com 2010 (com a implementação do GSI) onde conseguiram uma melhoria de cerca de 10% sobre o ano anterior, principalmente porque as condições dos equipamentos voltados para este fim melhoraram.

3.6.1 Vantagens da Operacionalização

A implementação do processo GSI permitiu identificar algumas vantagens, nomeadamente:

(i) Redução de custos por parte dos utilizadores para aceder ao sistema de informação (SI): como o SI é acessível em qualquer lugar e a qualquer momento, os custos de transporte para a entrega dos documentos é evitada, bem como a comunicação online com os serviços estão directamente permitindo esclarecimentos nenhum custo adicional. Além disso, a informação digital pode salvar o custo gasto em papel;

(ii) Redução dos custos operacionais: a utilização do SI permite que os funcionários se comuniquem com os vários serviços administrativos, simplificar as tarefas para reduzir o tempo de execução da tarefa, reduzindo o custo das comunicações entre os serviços, reduzir os custos com o espaço de armazenamento;

(iii) Melhoria na qualidade do serviço: com a implementação do GSI e possibilitou agilizar, e os pedidos de suporte dos utilizadores;

(iv) Aumento do número de utilizadores (alunos, funcionários e professores) e houve um aumento na utilização dos serviços;

(v) Redução: do número de pedidos de apoio por parte dos utilizadores originada pela sua inadequada formação; do número de ocorrências anual por aplicação de software dos servidores que provocaram quebras de funcionamento; a média do tempo (dias) de resposta até à recuperação do componente da infra-estrutura tecnológica sem aquisição de componentes; a taxa de incidentes que requerem suporte no local (fora dos Serviços de Informática) da ocorrência; a taxa de ocorrências resolvidas e finalizadas da responsabilidade dos Serviços de Informática; a taxa de incidentes reabertos.

(vi) Aumento da taxa: de *backups* dos dados críticos (definido pela política de *backups*); taxa de testes de sucesso a *backups* dos dados dos Sistemas de Informação.

Este trabalho permitiu preparar ou abrir caminho para outras certificações, porque com a sua realização foi possível:

- Obter um diagnóstico da realidade;
- Definir procedimentos de gestão e controlo;
- Definir indicadores e permitir a sua monitorização;
- Criar uma base documental estruturante, especialmente orientada para a gestão e controlo das TI.
- Identificar pontos de convergência na infra-estrutura tecnológica, no sentido de focar uma possível centralização (ex.: segurança informática), assente em referenciais mundialmente reconhecidos.

Depois de uma análise aos requisitos de certificação na área da segurança dos SI e TI (em particular a norma ISO 27001), este trabalho identificou algumas necessidades técnicas e de investimento necessárias para assegurar as orientações desta norma, em particular, gestão de riscos, infra-estruturas de suporte ao plano de recuperação de desastres, melhorar a qualidade e quantidade de equipamentos activos da infra-estrutura tecnológica para assegurar um bom nível de segurança. Por outro lado, em termos de requisitos documentais que a norma 27001 necessita, a sua grande maioria já foi desenvolvida com este trabalho, sendo que grande parte da sua estrutura já está realizada.

3.6.2 Proposta de Melhorias

No decorrer deste Consideramos que podemos propor melhorais em duas áreas, no tratamento dos indicadores e no aumento dos indicadores de avaliação. Com a proposta, efectuada no ponto 3.6 Avaliação, de um aumento gradual de indicadores, será possível obter mais informação efectiva e com qualidade para controlar e avaliar todo este processo, de forma a conseguirmos verificar onde resultados são menos bons. A partir dessa informação deve-se agir para reestruturar as lacunas ou limitações identificadas, no sentido de inverter essa avaliação.

Nesta dissertação foram apresentadas algumas melhorias em âmbitos diversos, como na segurança, nos diferentes serviços dos SI e na utilização desses serviços. Contudo, seguidamente apresentamos a seguinte tabela, que resume as melhorias propostas.

Âmbito	Necessidades		Quantidade
Segurança	Hardware	Firewall Física	1
		Servidor de aplicações e dados	1
		Servidor de Backup com Raid	1
		Servidor Proxy	1
		Linha dedicada de acesso á WAN	1
		Router dedicado aos serviços	1
		"UPS"	8
	Software	Sistema Operativo de rede	3
		Aplicação de Backup	3
		Anti-Malware	12
		Aplicação de encriptação de dados	12
		Aplicação de Gestão de credenciais	1
		Aplicação de Gestão de Certificados Digitais	1
		Aplicação de Inventariação dos SI/TI	Todas as unidades existentes
	Instalações	Ar condicionado	-
		Sistema de Videovigilância	-
		Controlo de acessos por dispositivo de acesso (Ex. Cartão)	-
Utilização dos Serviços	Utilizadores Finais	Formação no âmbito da Governância	6h
		Formação em segurança de Sistemas de Informação	25h
		Formação específica nas aplicações finais	60h
Serviços		Pessoal Qualificado	-
		Serviço *Help Desk*	-
		Departamento de I&D	-

Tabela 6 – Plano de Melhorias.

3.6.3 Gestão da Mudança

Actualmente existem múltiplas abordagens à gestão da mudança, contudo, de acordo com *Soraia Figueiredo* e *Miguel Mira da Silva* [SS2009], algumas destas metodologias, podem ser integradas de forma a se complementarem. As metodologias propostas pelos autores são: *People Capability Maturity Model* (*People* CMM), Metodologia de *Steinberg* e ABC of ICT. A solução preconizada é um plano eficaz de comunicação, presente em todas as etapas da Implementação do GSI, ajustável à organização e, consequentemente, à cultura organizacional. Este plano terá um impacto positivo no tempo de Gestão da Mudança despendido actualmente na sua Implementação e consequentemente no seu custo. Baseado na metodologia de *Steinberg* [RS2005], o plano é baseado nas 4 etapas:

- Desenvolver uma estratégia de mudança organizacional: Nesta fase são identificados os benefícios da visão, assim como os *stakeholders*.
- Fazer análise de *stakeholders*: Torna-se fundamental que se compreenda e se consiga gerir os *stakeholders* durante todo o ciclo de implementação; falhar neste campo pode causar resistência à mudança, atrasos no programa ou mesmo anular todos os esforços feitos anteriormente.
- Gerir a resistência: Em relação a esta gestão, surgem três questões a ter sempre em conta na implementação, pois provocam boas reacções nas pessoas: participação na elaboração ou recomendação da solução; introdução progressiva dos novos conceitos; experimentação das novas actividades em forma de jogo.
- Definir o Plano de Comunicação: O plano de comunicação é a estratégia documentada que serve para guiar o programa de comunicações.

Aliado a este plano de comunicação serão abordados alguns temas essenciais na gestão da mudança como, os quais são pontos-chave referidos no *People* CMM: incentivos, recompensas, sinergias nas equipas, ganhos a curto prazo, e liderança. Por este motivo, a metodologia de *Steinberg* será complementada com o *People CMM*.

O plano de comunicação definirá diferentes campanhas ao longo da Implementação do GSI, e para cada campanha serão especificados os respectivos meios de comunicação, a audiência alvo, e o calendário. Cada campanha será definida consoante um conjunto de objectivos a atingir. Este Plano vai permitir lidar com as seguintes barreiras [RS2005] reduzindo o impacto da gestão da mudança, nomeadamente: formar os funcionários e órgãos de gestão sobre as novas práticas e comportamentos; proporcionar eventos frequentes para envolver os *stakeholders* na solução GSI; recolher preocupações e necessidades dos *stakeholders*; produzir cuidadosamente mensagens para as equipas, *stakeholders*, órgãos de gestão e clientes envolvidos na implementação do GSI; lidar com a resistência à mudança; comunicar com as pessoas sobre as actividades e planos do GSI, com as mensagens correctas e na altura correcta.

De acordo com a metodologia apresentada para gerir a mudança foram apresentadas diferentes soluções para lhe dar suporte, tais como: criar uma calendário de reuniões regulares para exemplificar e explicar o uso dos documentos em termos de resistência colaboradores. Desenvolver um sistema de informação para apoiar todas as informações ,com as normas e principais funcionalidades: a centralização de todas as informações num ambiente Web que fornece acesso online a todas as informações do SGQ; fornecer itens de indexação para aceder rapidamente ao documento correcto para realizar uma tarefa/solicitação, fornecer formulários na web para os utilizadores introduzirem apenas os campos necessários nos formulários e, em seguida, gerar automaticamente o formulário correcto de acordo com a especificação do SGQ; permitir o envio dos formulários automaticamente para o serviço certo(com uma resposta de confirmação para o utilizador); disponibilizar uma tarefa para calendarizar os serviços, de forma a poder analisar centralmente as solicitações e disponibilizar acções internas para solucionar com mais eficiência os recursos materiais e humanos e economizar tempo, providenciar automaticamente os indicadores de desempenho chave (KPI) das informações analisadas; disponibilizar estatísticas de desempenho KPI de acordo com os objectivos definidos pelo GSI considerando as diferentes características dos utilizadores a interface do SI deve me simples e fácil de utilizar.

Capítulo 4

CONCLUSÃO E TRABALHO FUTURO

Este trabalho apresenta um estudo de caso da implementação do COBIT - *Control Objectives for Information and Technology* e do ITIL - *Information Technology Infrastructure Library* numa Instituição de Ensino Particular do Ensino Básico e Secundário em Portugal. Foi seguido um método de pesquisa qualitativa, mais concretamente um estudo de caso aplicado a uma instituição de ensino com a firma SEC, Sociedade de Ensino de Campos.

A Governância de uma organização é uma estrutura de relacionamentos e processos que ajudam a direccionar e controlar as metas a serem atingidas pela organização. Cada vez mais os referenciais de Governância das TI fazem parte das melhores práticas de gestão e controlo das organizações e são facilitadores para estabelecer uma Governância das TI, e em simultâneo, devem estar de acordo aos requisitos regulamentares. A gestão da infra-estrutura das TI e a utilização de referenciais em gestão das TI, podem ser vistos como uma condição obrigatória para se obter uma melhoria nos processos, na qualidade necessária. Verificou-se que as melhores práticas na Governância das TI utilizam como preferencialmente os referenciais COBIT e ITL, tendo sido factores importantes para as organizações atingirem todos os seus objectivos, assim como, a biblioteca de processos ITIL está entre as mais aceitas e reconhecidas mundialmente como as melhores práticas para gestão de serviços e infra-estrutura das TI. O ITIL hoje é reconhecido como um padrão

na gestão de serviços das TI, e as organizações que o implementaram estão satisfeitas com os resultados, onde o modelo leva a uma maior qualidade e produtividade à organização.

Na realidade, existem vários referenciais especialmente orientados para a sua aplicabilidade em áreas específicas das TI. Contudo, após prévio estudo e abordagem as esses referenciais decidiu-se aplicar o COBIT e o ITIL pois representam-se como amplamente reconhecidas na área de gestão e controlo das TI, onde nos centramos, contudo, com a experiencia deste trabalho, futuramente tencionamos aplicar outros referenciais em particular modelos de maturidade dos SI, assim como a evolução da aplicabilidade do COBIT e do ITIL.

O COBIT é o referencial que possui mais actividades directamente relacionadas e específicas para Auditoria de SI. Assim como a norma ISO 17799 (Família 27000) está mais vocacionada para actividades de Auditoria dos SI relacionados com a conformidade da segurança da informação.

A relação entre o referencial COBIT e ITIL, determinou, que ,cada modelo possui as suas particularidades, e oferecem serviços diferenciados, mas ambos são extremamente importantes para atender e resolver os problemas e objectivos das organizações. Podem ser implementados, por uma determinada organização, em conjunto ou separados. Essa flexibilidade é propiciada pelo facto de que os modelos podem ser segmentados, como o ITIL nas suas disciplinas, e o COBIT nos seus 34 objectivos dentro dos 4 domínios.

O COBIT é utilizado num nível mais alto na Governância nas TI, fornecendo uma estrutura de controlo global, baseado nos modelos de processos das TI definido pelo ITGI. Ele permite um mapeamento com outras práticas e padrões específicos, tais como o ITIL, que cobrem áreas específicas.

Foram detectadas diversas dificuldades que propiciavam uma gestão e controlo não eficiente sobre os componentes da infra-estrutura tecnológica e os serviços dos vários SI. Isso provocava dificuldades no desempenho dos serviços, em

controlar as TI e dificuldade em aplicar as melhores práticas para resolver problemas e melhorar a qualidade dos serviços.

Concluímos que os referenciais aplicados são uma estrutura adequada para a de Governância das TI/SI numa Instituição de Ensino Privado. Com esta implementação a instituição tem melhorado significativamente a qualidade dos serviços, reduziu o número de anomalias e mecanismos mais eficientes de para gerir e controlar os diversos Sistemas de Informação. Melhorar a qualidade do atendimento, redução do tempo de execução das tarefas em cerca de 25%, mais eficiência na monitorização e controlo dos componentes da infra-estrutura tecnológica, redução em cerca de 30% no número de incidentes resolvidos e concluídos pelos diversos serviços de TI e reduziu mais de 10% o número de incidentes reabertos. Para resolver as dificuldades no uso do GSI, foi necessário realizar reuniões regulares para desenvolver em primeiro lugar um Sistema de Informação para apoiar os colaboradores, para disponibilizar os documentos do SGQ e um conjunto de funcionalidades para melhorar o desempenho do colaboradores, e para o acesso eficiente aos procedimentos e formas de executar uma tarefa.

Para este diagnóstico foi elaborado um inquérito, ao departamento de informática, o qual contém questões de extrema relevância para se determinar o estado em que estão as TI/SI.

Verificamos também que a metodologia adoptada para a gestão da mudança foi imprescindível para o sucesso da implementação do GSI. A maior dificuldade nessa implementação foi a resistência à mudança dos recursos humanos.

No decorrer do desenvolvimento deste trabalho, foram identificadas possíveis propostas para serem desenvolvidas que estão correlacionadas com este estudo de caso. No entanto, existem dois pontos que não foram explorados no modelo conceitual desenvolvido para possibilitar a Governância das TI. Um deles seria implementar procedimentos que avaliassem a segurança da área das TI, e outro em relação à gestão de riscos. Ambos agregariam valor na consolidação da área da tecnologia.

REFERÊNCIAS BIBLIOGRÁFICAS

[BSIWEB] British Standards Institution - http://www.bsi-global.com/.

[CA2004] Carneiro, Alberto, Auditoria de Sistemas de Informação, 2ª Edição Aumentada, Lisboa, FCA, 2004.

[CB2006] Calder, A., Bon, J. "Information Security Based on ISO 27001/ISO 17799: A Management Guide", Van Haren Publishing, 2006.

[CMMWEB] SW-CMM - http://www.sei.cmu.edu/appraisal-program/profile/sw-cmm.html, 2009.

[COB2007] COBIT, "Information Systems Audit and Control Association, Control Objectives for Information and Related Technology, 4.1:th Edition, IT Governance Institute, 2007.

[COM2008] IT Governance Institute - Cobit Mapping - Mapping of ITIL v3 With COBIT® 4.1, USA, 2008.

[COSOWEB] Official Site of COSO- Committee of Sponsoring Organizations: http://www.coso.org/.

[DC2007] Davis, Chris et al, IT Auditing – Using Controls to Protect Information Assets, McGraw-Hill Osborne, 2007.

[DRS2006] Debraceny, R.S., "Re-engineering IT Internal Controls - Applying capability Maturity Models to the Evaluation of IT Controls", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

[GJC2004] G. Ridley, J. Young and P. Carroll, "COBIT and its utilization - A framework from the literature", Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii, 2004.

[GR2009] Gomes, R., Ribeiro J., "the main benefits of Cobit in a High Public Educational Institution – A case study, in Proceedings of the Pacific Asia Conference on Information Systems- Association for Information Systems (AIS), Hyderabad, India, 2009.

[HP2005] HP, Hewlett-Packard Development Company. Fundamentos ITIL para gerenciamento de serviços de TI, 2005.

[HTB2005] Hochstein, A., Tamm, G., Brenner, W., *Service-oriented IT Management: Benefit, Cost and Success Factors.* European Conference on Information Systems, 2005.

[IBG2004] Instituto Brasileiro de Gorvernança Corporativa, www.ibgc.org.br/, 2004.

[IOS2005] International Organization for Standardization, ISO/IEC 20000-1 & ISO/IEC 20000-2, 2005- http:// www.iso.org/.

[ISACWEB] Information Systems Audit and Control Association: http://www.isaca.org.

[ISOWEB] ISO 17799 - http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm Accessed in 12-01-2009.

[ITGWEB] Official site of the IT Governance Institute: http:// www.itgi.org/.

[ITIWEB] Official Site of ITIL - Information Technology Infrastructure Library: http://www.itil-officialsite.com.

[JP2008] Simonsson, Johnson, P. "The IT organization modeling and assessment tool: Correlating IT governance maturity with the effect of IT". In Proceedings of the 41st Hawaii International Conference on System Sciences, 2008.

[JV2009] Van Bon, J., *IT Service Management Based on ITIL® V3 – A Pocket Guide*, VanHaren Publishing, 2009.

[KK2001] N. Korac-Kakabadse and A. Kakabadse, "IS/IT Governance: Need For an Integrated Model". Corporate Governance Journal, volume 1, pages:9-11, 2001.

[KN2004] Kaplan R., and Norton D., Balanced Scorecard: Translating Strategy Into Action (Hardcover), Boston: Harvard Business School Press, 2004.

[LPA2006] Larsen, M. Holm, Pedersen, M. Kühn and Andersen, K. Viborg, "IT Governance – Reviewing 17 IT Governance Tools and Analyzing the Case of Novozymes A/S", Proceedings of the 39th Hawaii International Conference on System Sciences, 2006.

[MC2008] Sílvia, Miguel Vieira e Martins, José Cerqueira, IT Governance – A gestão Informática, FCA, 2008.

[MCB1995] Paulk, M., Weber, C., Curtis, B., Chrissis, M. "The Capability Maturity Model: Guidelines for Improving the Software Process (SEI Series in Software Engineering), Addison-Wesley Professional, 1995.

[MM2010] Myers, M. D. "Qualitative Research in Information Systems," *MIS Quarterly* (21:2), June 1997, pp. 241-242. *MISQ Discovery*, archival version, June 1997, http://www.misq.org/discovery/MISQD_isworld/. *MISQ Discovery*, updated version, 2010.

[MRR2009] Martini, Rafael Rodrigo, "Frameworks de governança de TIC aplicados em SLA de VoIP sobre WLAN", Dissertação de Mestrado, Campinas, 2009.

[MS2005] Sallé M.; Rosenthal S. Formulating and Implementing an HP IT Program Strategy using COBIT and HP ITSM. In: Annual Hawaii International Conference on System Sciences, Hawaii, 2005.

[OCA2007] OGC, *ITIL* – Glossário de Termos, Definições e Acrónimos, Versão v3.1.24, 2007.

[OCB2007] OGC, *The Official Introduction to the ITIL Service Lifecycle*, The Stationary Office, Reino Unido,2007.

[OCG2007] OGC, "Official Introduction to the Itil Service Lifecycle", Stationery Office, Office of Government Commerce, 2007.

[PL2001] Pande, P., Holpp, L., "What Is Six Sigma?", McGraw-Hill, 2001.

[PMBWEB] Official Site of Project Management Institute that define the PMBok Guide: http://www.pmi.org

[PMI2008] PMI, "A Guide to the Project Management Body of Knowledge", Project Management Institute, 2008.

[RB2008] Rocha, Luís Filipe Bronze, "Sistema de controlo interno de reporte financeiro (scirf) no grupo edp – energias de portugal", projecto de Mestrado em Contabilidade, ISCTE, Lisboa, 2008.

[RBS2003] Jackie Rees, Shubho Bandyopadhyay, and Eugene H.Spafford; *A Policy Framework for Information Security*; in *Communcations of the ACM*; July 2003.

[REM2010] Martins, Ricardo, Cardoso, Elsa, Sequeira, Manuel Menezes de Henrique Borges, ITIL nas universidades: projecto-piloto em gestão de activos de TI no ISCTE-IUL, ISCTE – Instituto Universitário de Lisboa, Portugal, 2010.

[RG2009] Ribeiro, Jorge e Gomes, Rui, IT Governance using COBIT implemented in a High Public Educational Institution – A Case

Study, School of Technology and Management Polytechnic Institute of Viana do Castelo, Portugal, 2009.

[RM2007] [MR2007] Moeller, R., "COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework", John Wiley and Son, 2007.

[RS2005] Steinberg, R, *Implementing ITIL*. Trafford, 2005.

[SCC2004] Sortica, Eduardo Almansa, Clementi, Sérgio, Carvalho, Tereza Cristina M. B.,Governança de TI: uma empresa virtual analisada sob a ótica do COBIT e do ITIL,2004.

[SEIWEB] SEI (Software Engineering Institute) – http:// www.sei.cmu.edu/Accessed in 12-01, 2009.

[SG2003] Spafford, G., "The Benefits of Standard IT Governance Frameworks", IT Process Institute, in www.itpi.org, 2003.

[SJ2007] M. Simonsson and P. Johnson, "Model-based IT governance maturity assessments with COBIT", In proceedings of the European Conference on Information Systems, St. Gallen, Switzerland, 2007.

[SOXWEB] A Guide To The Sarbanes-Oxley Act; http://www.soxlaw.com.

[SP2007] Silva, Pedro Manuel Gomes. A Função Auditoria de Sistemas de Informação: Modelo Funcional e de Competências. Dissertação de Mestrado. Universidade do Minho, 2007.

[SS2005] Santos, Luciana de Almeida Araújo e Lemes, Sirlei , A Lei Sarbanes-Oxley: uma tentativa de recuperar a credibilidade do mercado de capitais norte-americano, faculdade de ciências contáveis - universidade federal de Uberlândia, 2005.

[SS2009] Silva, Miguel Mira da, Figueiredo, Soraia, Gestão da Mudança na Implementação do ITIL, IST, 2009.

[SSC2004] Almansa Sortica, Eduardo e Clementi, Sérgio e Cristina M. B. Carvalho, Tereza, Governância de TI: uma empresa virtual analisada sob a ótica do COBIT e do ITIL, EPUSP-LARC / SENAC SP, 2004.

[TH2006] Dahlberg, T.; Kivijarvi H. An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument. In: Annual Hawaii International Conference on System Sciences, Hawaii, 2006.

[TI2007] Sharon Taylor, M.Iqbal, M.Nieves, "ITIL:Service Strategy", TSO publications.Norwith,UK,2007.

[TS2008] Tshinu, Simon Mukenge and Botha, Gerrit, "An Integrated ICT Management Framework forCommercial Banking Organisations in South Africa", Tshwane University of Technology, South Africa, 2008

[TWW2000] C., Tsiakals, J., West, J., West, J. "Iso 9001: 2000 Explained". ASQC/Quality Press, 2000.

[WC2009] Willson, Phyl and Pollard, Carol) "Exploring IT Governance in Theory and Practice in a Large Multi-National Organisation in Australia", Information Systems Management, 2009.

[WHG2004] Van Grembergen, W., S. De Haes and E. Guldentops "Structures, Processes and Relational Mechanisms for IT Governance", In: Van Grembergen, W. (ed.): Strategies for Information Technology Governance. Idea Group Publishing, 2004.

[WR2004] Weill, P. and J.W. Ross, IT governance – How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press, 2004.

ANEXOS

ANEXO A1– LISTA DE SIGLAS

SI	Sistemas de Informação
TI	Tecnologias de Informação
COBIT	*Control Objectives for Information and related Technology*
COSO	*Committee of Sponsoring Organizations*
ITIL	*Information Technology Infrastructure Library*
PMBooK	*Project Management Body of Knowledge*
CMM	*Capability Maturity Model*
ISO	*International Organization for Standardization*
QREN	Quadro Regional Estratégico Nacional
GSI	Gestão de Sistemas de Informação
SEC	Sociedade de Ensino de Campos
TCP	*Transmission Control Protocol*
IP	*Internet Protocol*
LAN	*Local area network*
WAN	*Wide Area Network*
TCI	Tecnologias da Informação e Comunicação
KPI	*Key Performance Indicator*
ITGI	*Information Technology Governance Institute*

SGQ	Sistema de Gestão de Qualidade
CEO	*The Chief Executive Officer*
CIO	Chief Information Officer
SEI	*Software Engeneering Institute*
SW-CMM	*Capability Maturity Model for Software*
IEC	*International Electrotechnical Commission*
SOX	Sarbanes–Oxley
ADSL	Asymmetric Digital Subscriber Line
ISACA	Information Systems Audit and Control Association
BSC	Balanced scorecard
OGC	Office of Government Commerce
FCCN	Fundação para a Computação Científica Nacional

ANEXO A2 - ORGANOGRAMA DO COLÉGIO DE CAMPOS

O organograma da instituição é composto por um conjunto de departamentos funcionais, sendo as suas competências enquadradas com a gestão e operacionalização de uma instituição do ensino particular. O seu organograma é ilustrado na seguinte figura.

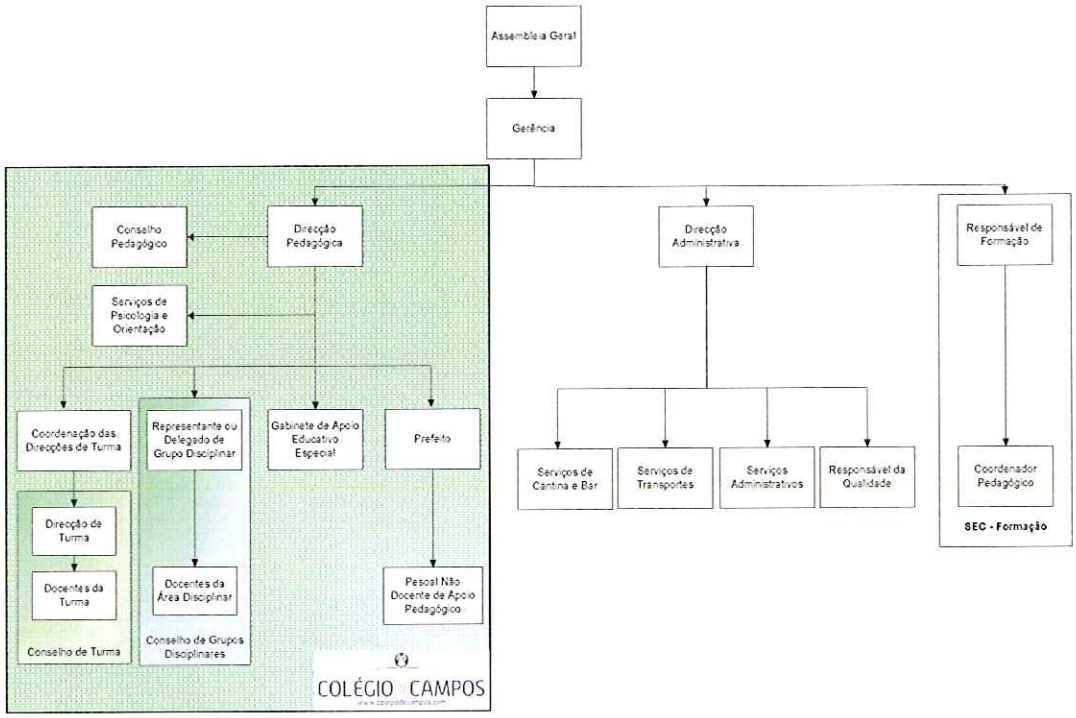


Figura 25 – Organograma do Colégio de Campos.

ANEXO A3 – IMPRESSOS UTILIZADOS NA OPRACIONALIZAÇÃO DO COBIT PARA A GESTÃO DO SISTEMA DE INFORMAÇÃO

COLÉGIO CAMPOS

Ocorrência de Anomalia Informática

1. DADOS GERAIS

- **NÚMERO DA OCORRÊNCIA:**
- **TIPO DE OCORRÊNCIA:**
  - ☐ NOVA OCORRÊNCIA
  - ☐ REABERTURA DE OCORRÊNCIA Nº
- **DATA DA OCORRÊNCIA:**
- **IDENTIFICAÇÃO**
  - NOME:
  - E-MAIL:
  - CONTACTO TELEFÓNICO:
- **CARGO**
  - ☐ **DOCENTE – DEPARTAMENTO:**
  - ☐ **FUNCIONÁRIO – SERVIÇO:**
  - ☐ **ALUNO – NÚMERO:**
  - ☐ **OUTRO:**

2. DESCRIÇÃO DO PROBLEMA

- PROBLEMA NOS ACESSOS:
  - ☐ À INTERNET
  - ☐ AO E-MAIL
  - ☐ A APLICAÇÃO DE SOFTWARE
  - ☐ AOS CONTEÚDOS DOS PORTAIS
  - ☐ OUTRO: _____
- PROBLEMA NOS COMPONENTES DA INFRA-ESTRUTURA TECNOLÓGICA
  - ☐ PROBLEMAS TÉCNICOS NO COMPONENTE
    - Nº DE INVENTÁRIO: _____
    - Nº DE SÉRIE: _____
    - OUTRO IDENTIFICADOR: _____
    - LOCALIZAÇÃO: _____
  - ☐ Incidente reportado por ferramentas automáticas de monitorização

- OBSERVAÇÕES

O requerente

___:___ __/__/____

☐ Foi enviado um e-mail de confirmação da recepção do pedido de ocorrência

3. RESOLUÇÃO DO PROBLEMA

- **RESULTADO DA RESOLUÇÃO**
  - ☐ Problema Solucionável: □ Ocorrências resolvida e finalizada da responsabilidade dos Serviços de Informática
    □ Está pendente por terceiros
  - ☐ Sem resolução (indicar motivo em Outras observações)
- **ACTIVIDADES DESENVOLVIDAS DURANTE A RESOLUÇÃO DO PROBLEMA**
  - ☐ Necessidade de actualizar o repositório de configurações – Preencher documento GSI/03 e indicar "Definição ou manutenção do repositório de configurações". Nº do pedido: _____ Seguir o procedimento GSI/12 – Gerir o Repositório de Configurações
  - ☐ Requer suporte local fora dos Serviços de Informática (indicar local em Outras observações)
  - ☐ Requer requisição de componentes - Nº da requisição (GSI/02): _____
- **OBSERVAÇÕES DETECTADAS DURANTE A RESOLUÇÃO DO PROBLEMA**
  - ☐ Material obsoleto para o pedido efectuado (indicar motivo em Outras observações)
  - ☐ Alteração de emergência dos componentes da infra-estrutura tecnológica
  - ☐ Inadequada utilização do sistema
  - ☐ A anomalia informática provocou quebra de serviço
  - ☐ Anomalia em Servidores (E-mail, Web, Firewall, Bases de Dados, ou outro)
  - ☐ Anomalias nas configurações do equipamento
- **OUTRAS OBSERVAÇÕES:**

Serviço de Informática

I___:___ - __/__/____

Total de Horas _____ F___:___ - __/__/____

☐ Foi enviado um e-mail de confirmação do fim da resolução do problema informático

GSI/01 Rev. 1/ 2010.07.22 Página 1 de 1

COLÉGIO CAMPOS

Pedido de necessidades de componentes para a Infra-estrutura tecnológica

1. DADOS GERAIS DO REQUISITANTE

- **IDENTIFICAÇÃO**
  - NOME: _____
  - E-MAIL: _____
  - CONTACTO TELEFÓNICO: _____
- **CARGO**
  - ☐ DOCENTE – DEPARTAMENTO: _____
  - ☐ FUNCIONÁRIO – SERVIÇO: _____
  - ☐ ALUNO – NÚMERO: _____
  - ☐ OUTRO: _____

2- DADOS DO PEDIDO DE AQUISIÇÃO

3- JUSTIFICAÇÃO PARA A AQUISIÇÃO

4- NECESSIDADES COMPLEMENTARES AO PEDIDO

5- OBSERVAÇÕES

6- RESULTADO DA APROVAÇÃO DO PEDIDO POR PARTE DOS SERVIÇOS DE INFORMÁTICA

☐ Pedido Aceite

☐ Pedido Não Aceite Motivo: _____

7- INFORMAÇÃO SOBRE O PEDIDO AO APROVISIONAMENTO (EM CASO DO PEDIDO TER SIDO ACEITE)

Informação do Pedido ao Aprovisionamento	Informação da Recepção do Pedido do Aprovisionamento
■ DATA DO PEDIDO: ____/____/____	■ NÚMERO DE REQUISIÇÃO AO APROVISIONAMENTO: _____
■ NÚMERO DO PEDIDO: _____	■ DATA DE RECEPÇÃO DOS COMPONENTES: ____/____/____

8- ASSINATURAS:

Requisitante	Responsável do Serviço de Informática
__/__/____ _____	__/__/____ _____

COLÉGIO CAMPOS

Pedido de execução de tarefas associadas aos sistemas de informação da infra-estrutura tecnológica

1. Dados gerais

- Número do pedido: _____ Data do pedido: _____
- Número de requisição ao aprovisionamento _____
- Identificação
  - Nome: _____
  - E-mail: _____
  - Contacto telefónico: _____
- Cargo
  - ☐ Docente – Departamento: _____
  - ☐ Funcionário – Serviço: _____
  - ☐ Aluno – Número: _____
  - ☐ Outro: _____

2. Tipo de pedido

- Pedido gerais
  - ☐ Pedido de Orçamento
  - ☐ Manutenção de Componentes (Computadores, Monitores, Impressoras, etc)
  - ☐ Acesso à Intranet ou à Rede sem fios
  - ☐ Criação de Pastas Partilhadas para Suporte às Disciplinas
  - ☐ Criação de Disciplinas na Plataforma de E-learning
  - ☐ Atribuição de Acessos aos Conteúdos da Plataforma de E-learning
  - ☐ Analise de informação na área das Tecnologias de Informação
  - ☐ Extracção de informação na área das Tecnologias de Informação
- Actualização de versões de documentos
  - ☐ Registo de nova versão de documentos associados aos sistemas de informação
  - ☐ Actualização do portefólio dos documentos dos projectos na área das tecnologias de informação
- Inventariação de componentes ou backups da infra-estrutura tecnológica
  - ☐ Inventariação de componentes
    - ☐ Todos os componentes
    - ☐ Apenas os componentes: _____ _____ _____
  - ☐ Inventariação de backups de armazenamento de dados
    - Versão do documento de inventário _____
- Execução de tarefas ou procedimentos associados aos sistemas de informação
  - ☐ Execução de backups
  - ☐ Restauração de backups
  - ☐ Verificação de integridade das configurações dos equipamentos e aplicações de software
  - ☐ Realização de testes ao plano de contingência dos componentes da infra-estrutura tecnológica
  - ☐ Realização de testes ao plano de recuperação de desastres dos componentes da infra-estrutura tecnológica
- Definição ou Manutenção de planos e procedimentos associados aos siistemas de informação
  - ☐ Definição de novo plano
  - ☐ Manutenção de um plano já existente
  - ☐ Definição ou manutenção das politicas de backups e recuperação de backups
  - ☐ Definição ou manutenção do plano de segurança dos componentes da infra-estrutura tecnológica
  - ☐ Definição ou manutenção da conta de utilizadores dos componentes da infra-estrutura tecnológica

COLÉGIO CAMPOS

Pedido de instalação, reinstalação de componentes para a Infra-estrutura tecnológica

1. DADOS GERAIS DO PEDIDO

- NÚMERO DO PEDIDO: _____ DATA DO PEDIDO: _____
- NÚMERO DE REQUISIÇÃO AO APROVISIONAMENTO: _____
- IDENTIFICAÇÃO
  - NOME: _____
  - E-MAIL: _____
  - CONTACTO TELEFÓNICO: _____
- CARGO
  - ☐ DOCENTE – DEPARTAMENTO: _____
  - ☐ FUNCIONÁRIO – SERVIÇO: _____
  - ☐ ALUNO – NÚMERO: _____
  - ☐ OUTRO: _____
- TIPO DO PEDIDO:
  ☐ INSTALAÇÃO ☐ REINSTALAÇÃO ☐ CONFIGURAÇÃO

2- DADOS DO COMPONENTE DA INFRA-ESTRUTURA TECNOLÓGICA A INSTALAR

3- JUSTIFICAÇÃO PARA A INSTALAÇÃO

4- CENTRO DE CUSTOS ASSOCIADOS:

Há custos associados à instalação do componente?

☐ Sim

Centro de custos: _____

Autorização:

	Responsável pela autorização
	_____ Em: __/__/____

☐ Não

5- OBSERVAÇÕES

6- RESULTADO DA APROVAÇÃO DO PEDIDO DE INSTALAÇÃO

☐ Pedido Aceite

☐ Pedido Não Aceite Motivo: _____

Requisitante	Responsável do Serviço de Informática e/ou Orgão de Gestão
__/__/____ _____	__/__/____ _____

GSI/04 Rev. 1/ 2010.07.22 Página 1 de 1

COLÉGIO CAMPOS

Conta de utilizadores para o acesso aos componentes da infra-estrutura tecnológica

Nova versão do documento:		Data:		Versão anterior:	
Unidade Orgânica/Funcional:					

#	Nome do utilizador	Cargo	Nº mecanográfico	Aplicação de software									
				1	2	3	4	5	6	7	8	9	10
1													
2													
3													
4													
5													
6													
7													
8													

Especificação do perfil aplicação de software:

1	Aplicação:		
	Perfil:	1	
		2	
		3	
		4	
2	Aplicação:		
	Perfil:	1	
		2	
		3	
		4	

GSI05 Rev. 1/ 2010 07 22 Página 1 de 1

COLÉGIO CAMPOS

Plano de intervenção em componentes na infra-estrutura tecnológica

☐ NOVA VERSÃO DATA: _____ VERSÃO ANTERIOR: _____

• TIPO DE COMPONENTES E SERVIÇOS A ANALISAR NA INTERVENÇÃO:

■ Cablagem de rede
- ☐ Integrável: Periodicidade: _____

■ Switches
- ☐ Portas: Periodicidade: _____
- ☐ Sistema de ventilação: Periodicidade: _____
- ☐ Cabos de alimentação: Periodicidade: _____

■ Servidores
- ☐ Cabos de alimentação: Periodicidade: _____
- ☐ Integrável dos discos: Periodicidade: _____
- ☐ Espaço em disco: Periodicidade: _____
- ☐ Sistema de ventilação: Periodicidade: _____

■ Postos de trabalho
- ☐ Cabos de alimentação: Periodicidade: _____
- ☐ Integrável dos discos: Periodicidade: _____
- ☐ Sistema de ventilação: Periodicidade: _____

■ UPS
- ☐ Baterias: Periodicidade: _____
- ☐ Cabos de alimentação: Periodicidade: _____

■ Access Point
- ☐ Equipamento POE: Periodicidade: _____
- ☐ Cabos de alimentação: Periodicidade: _____

GSI06 Rev. 1/ 2010 07 22 Página 1 de 6

COLÉGIO CAMPOS	**Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica**

☐ NOVA VERSÃO DATA: _____ VERSÃO ANTERIOR: _____

Esta política destina-se a delinear regras mínimas e procedimentos para a cópia de segurança (backup) e restauro de dados institucionais da SEC – Sociedade de Ensino de Campos.

Estas regras destinam-se a proteger o interesse das entidades institucionais tais como funcionários, alunos e a própria instituição, na medida em que se fomenta uma arquitectura possibilitadora de continuidade, restauro e recuperação em tempo útil de informação institucional crítica, perdida acidentalmente quer em caso de desastres físicos e/ou lógicos, quer devido à ocorrência de falhas dos sistemas informáticos e/ou suporte de informação ou falha humana.

Toda a informação institucional (adquirida, armazenada, produzida, processada, recebida, transferida) e considerada crítica deve ser abrangida pela presente política uma vez que em caso de perda acidental se pretende reduzir ao mínimo o impacto desta perda no normal funcionamento do negócio, sendo que os processos que dessa informação dependam possam voltar à normalidade no mais curto espaço de tempo e com uma perda mínima de dados.

Esta política não se destina a garantir uma protecção contra erros de utilização, tais como ficheiros apagados ou sobrepostos, nem a garantir um mecanismo de gestão de versões de dados. Esta política também não abrange o processo de armazenamento e retenção dos dados a longo prazo (e.g. registos financeiros e académicos) que são regidos por legislação governamental e por políticas institucionais próprias. Esta política pretende somente garantir a existência de uma cópia (imagem) o mais actual possível da informação institucional em formato "electrónico" e não se aplica à informação existente na forma física tais como em papel ou cassete.

Com esta política pretende-se que as entidades institucionais adquiram sensibilidade para o nível de criticidade da informação institucional da qual são responsáveis e que disponham de um processo bem formalizado para solicitarem aos Serviço de Informática (SI) os seus serviços de cópia de segurança e restauro de forma devidamente regulamentada e informada.

COLÉGIO CAMPOS	**Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica**

Âmbito Esta política destina-se a todas as entidades institucionais que no(s) seu(s) processo(s) façam uso de informação institucional e sejam considerados responsáveis pela mesma.

Aplica-se a todos os sistemas informáticos institucionais conectados ou não às redes de dados que armazenem ou processem informação institucional crítica. Aplica-se também a informação existente em suporte de informação amovível tais como software original em DVD ou dados de aplicações em pen drive.

A mesma destina-se essencialmente a sistemas informáticos propriedade da instituição mas pode aplicar-se excepcionalmente a sistemas informáticos propriedade de terceiros e particulares que contenham informação institucional devidamente comprovada.

Descrição

Esta "política de cópias de segurança e restauro" assegura cinco processos chave na arquitectura de backups da instituição:

1. Notificação: Assegura que os SI informam e sensibilizam convenientemente as entidades institucionais para a importância de se dirigirem aos SI e solicitarem a "abertura de um processo de backup" dos seus dados institucionais críticos;

2. Cópia de Segurança: Assegura que os SI implementam a pedido da entidade institucional um processo para realização de cópias de segurança periódicas da informação institucional crítica e que o mesmo é devidamente documentado e formalizado;

3. Teste ao backup: Assegura que os SI implementam um processo para realização de testes periódicos às cópias de segurança existentes no que se refere à sua integridade e capacidade para assegurarem um restauro efectivo e total da informação institucional crítica em qualquer momento;

4. Restauro do backup: Assegura que os SI implementam um processo para realização de restauro de cópia de segurança efectivo quando solicitados pelo dono do backup e que esse mesmo processo é devidamente documentado e formalizado;

5. Catalogação das cópias de segurança: Assegura que os SI mantêm actualizado um catálogo (inventário) de todas as cópias de segurança efectuadas e existentes On-site e Off-site em qualquer tipo de suporte electrónico.

1 - Notificação

Os SI deverão proceder a notificações e alertas, numa base periódica, às *entidades institucionais* referindo a existência desta política e dos serviços que lhe estão associados.

Deve salientar-se a importância da solicitação e utilização dos referidos serviços como elementos chave de uma boa prática de trabalho e de uma boa gestão da *informação institucional crítica* (dadas as consequências da sua perda). Devem referir-se os documentos e trâmites necessários para a solicitação dos referidos serviços. É responsabilidade do *supervisor de backups* elaborar e efectuar as notificações e alertas às entidades institucionais. Para isso o *supervisor de backups* deve identificar todos os *inputs* ou colecções de dados institucionais críticos e alertar os responsáveis pela informação para o dever de requisitarem os serviços de *cópia de segurança*.

2 – *Cópia de Segurança*

O processo de *cópia de segurança* é solicitado aos SI pela *entidade institucional* responsável pela informação que pretende salvaguardar através do preenchimento do formulário de requisição de *cópia de segurança* (GSI/08) ficando assim designada por *dono do backup*. O *operador do backup* deverá completar o referido formulário e dar início ao respectivo processo.

A frequência da rotina do processo de *backup* é registada no cronograma do documento – "Plano de Intervenção em componentes da infra-estrutura tecnológica" na secção do Mapa de backups, recuperação e testes aos backups (GSI/06).

A frequência, tipo e extensão de cada *cópia de segurança* são parâmetros determinados em conjunto pelos SI pelo *operador de backups* e pelo *dono do backup*, e ficam claramente registados no formulário de requisição de *cópia de segurança* (GSI/08). A definição dos mesmos baseia-se no nível de criticidade da informação institucional e numa análise mínima de risco efectuada pelos SI.

Finalizada a primeira *cópia de segurança* efectua-se a verificação da mesma. Uma rotina de *backup* só se considera completa depois de se finalizar a referida verificação.

A verificação é o procedimento que testa e reporta se a *cópia de segurança* foi bem efectuada e se a informação pode ser restaurada com sucesso na sua totalidade imediatamente a seguir à sua conclusão. O procedimento de verificação do *backup* deve ficar devidamente registado no formulário de requisição de *cópia de segurança* (GSI/08).

COLÉGIO CAMPOS	**Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica**

Na elaboração da arquitectura de *backups* pretendeu-se contemplar a proximidade da informação (acessibilidade e usabilidade) privilegiando-se sempre que possível uma *filosofia de backup de três gerações*, sendo uma dessas gerações um "*backup Off-site*" por questões de segurança.

3 – Teste ao *backup*

A periodicidade da elaboração dos testes aos *backups* e controlo dos mesmos é registada num cronograma - do documento – "Plano de Intervenção em componentes da infra-estrutura tecnológica" na secção do Mapa de backups, recuperação e testes aos backups (GSI/06) existindo um mapa por cada processo de *backup*. O operador do *backup* deverá fazer uso do referido mapa para controlar a realização dos testes periódicos aos *backups*, segundo o cronograma definido, documentando e formalizando devidamente este processo. O teste ao *backup* destina-se principalmente a detectar falhas no hardware em meios de suporte da informação e nos procedimentos de restauro. Estes testes permitem à equipa técnica paralelamente familiarizar-se com os procedimentos envolvidos, bem como ter uma noção do tempo necessário para efectuar o restauro de determinada *cópia de segurança*. O teste ao *backup* não é mais do que uma simulação de um restauro da informação salvaguardada ou seja, um teste ao restauro do *backup*.

4 – Restauro do *backup*

O processo de restauro do *backup* é solicitado aos SI pelo dono do *backup* através do preenchimento do formulário de requisição de restauro de *cópia de segurança* (GSI/08). O dono do *backup* deverá referir a causa porque solicita o restauro juntamente com um conjunto de dados necessário para documentar e formalizar este processo devidamente. O operador do *backup* deverá completar o referido formulário e efectivar o processo de restauro da informação solicitada.

5 – Catalogação de *cópias de segurança*

Assegura que os SI mantêm actualizado um catálogo (inventário) de todas as *cópias de segurança* efectuadas e existentes. No catalogo de *cópias de segurança* (GSI/29) são documentados e registados itens como identificação do *backup*, tipo de cópia, dono do *backup*, operador do *backup* e localização da informação, entre outros. Este catálogo deverá ser permanentemente actualizado sempre que se instaure um novo

processo de *backup* ou se verifique alguma alteração no que se armazena, onde se armazena e como se armazena. O catálogo de *cópias e segurança* é um elemento chave na construção da *"política de recuperação de desastres"* da instituição e o seu principal objectivo é fornecer dados rápida e concisamente ao processo de restauro do *backup*. A implementação deste catálogo e a sua actualização são responsabilidades do *supervisor de backups*.

Modelos de *Backup* Principais

Na instituição distinguem-se cinco modelos principais para o processo de *cópia de segurança*. Estes devem as suas especificidades a factores tais como a criticidade e o processamento da informação, aos serviços que asseguram, ao tipo de meio de suporte da informação, às propriedade e conectividade do sistema à rede. Cada um destes modelos tem procedimentos específicos e uma arquitectura própria. Descrevem-se seguidamente:

1 – Sistemas Institucionais Críticos Com Conectividade ou Não à Rede

Sistemas que assegurem a produção de serviços de rede e aplicações críticas indispensáveis ao normal funcionamento da instituição, quer sejam, respectivamente, globais, departamentais, de serviços, de gabinetes, de projectos ou laboratoriais, devem, sempre que possível, ser alvo de um *backup total* ou *imagem* que permita a sua recuperação integral no mínimo tempo possível em caso de falha.

Sempre que possível as imagens devem ficar armazenadas no servidor de *backups* dos SI e deve efectuar-se uma cópia *On-site* e outra *Off-site*.

2 – Sistemas Institucionais não Críticos Com Conectividade à Rede

Estações de trabalho, computadores portáteis e servidores conectados à rede de dados da instituição, que criem ou actualizem informação institucional crítica numa base diária, devem ser alvo de *backups* diários para minimizar a exposição à perda de informação crítica. Sempre que possível seguindo uma *filosofia de backup de três gerações* com se descreve:

1.ª Geração

Devem efectuar um primeiro *backup* diários para uma unidade de armazenamento fisicamente diferente da original, que é, geralmente, um dispositivo de armazenamento conectado à rede departamental *Onsite*.

Esse *backup* original, 1.ª *cópia de segurança*, deve efectuar-se no final do expediente no caso dos postos de trabalho e será lançado de forma "manual" pelo utilizador ou de forma automática por ferramenta configurada para o efeito pelos SI. Em caso de servidores os SI deverão implementar mecanismos de *backup* diários que não interfiram com o normal funcionamento da instituição. Sempre que possível os *backups* diários serão *backups* incrementais por questões de desempenho.

2.ª Geração

A cópia do *backup* original, 2.ª *cópia de segurança*, deverá ser efectuada semanalmente para a unidade institucional de armazenamento em rede (unidade principal de armazenamento total de *backups On-site* da instituição). A 2.ª *cópia de segurança* será um *backup total* e armazenado *On-site*, devendo realizar-se de forma automática com ferramentas e horários que não interfiram com o normal funcionamento dos serviços da instituição.

3.ª Geração

A cópia do *backup* de segunda geração, 3.ª *cópia de segurança*, deverá ser efectuada mensalmente para o servidor de *backups Off-site*. A 3.ª *cópia de segurança* será total e deverá realizar-se de forma automática com ferramentas e horários que não interfiram com o normal funcionamento dos serviços da instituição.

Esta política básica aplicar-se-á a sistemas informáticos tais como postos de trabalho de funcionários (de serviços e gabinetes) que armazenem informação crítica com uma base diária de actualização.

Aplicar-se-á igualmente à informação crítica (actualizada numa base diária ou regular) dos servidores de frente e de outros servidores da instituição tais como, "Active Directory", configurações de Firewall, logs, estado do sistema e dados de aplicações tais como bases de dados e reports.

3 – Sistemas Institucionais Não Críticos Não Conectados à Rede

Estações de trabalho, computadores portáteis e servidores não conectados numa base permanente à rede de dados, que vejam a sua informação actualizada numa base periódica, devem ser alvo de *backup* sempre que possível privilegiando uma filosofia de *backup* de três gerações sendo que uma das gerações é um "*backup Off-site*" por questões de segurança. A periodicidade do *backup* será definida em função da importância e periodicidade da actualização da informação nos referidos sistemas. O

processo será idêntico ao descrito no modelo anterior com excepção do procedimento de cópia da 1.ª Geração.

1.ª Geração

Idêntico ao descrito anteriormente com a diferença de recorrer a um mecanismo de transporte da informação de *backup* para a unidade de armazenamento em rede departamental uma vez que não existe rede de dados. Pode diferir igualmente no facto de não ter que se efectuar diariamente.

2.ª Geração

A cópia do *backup* original, 2.ª *cópia de segurança*, deverá ser efectuada semanalmente para a unidade institucional de armazenamento em rede (unidade principal de armazenamento total de *backups On-site* da instituição). A 2.ª *cópia de segurança* será um *backup total* e armazenado *On-site*, devendo realizar-se de forma automática com ferramentas e em horários que não interfiram com o normal funcionamento dos serviços da instituição.

3.ª Geração

A cópia do *backup* de segunda geração, 3.ª *cópia de segurança*, deverá ser efectuada mensalmente para o servidor de *backups Off-site*. A 3.ª *cópia de segurança* será total e deverá realizar-se de forma automática com ferramentas e em horários que não interfiram com o normal funcionamento dos serviços da instituição.

4 – Software em Suporte de Informação Amovível

Todo o software adquirido ou desenvolvido e existente em formato "electrónico" em suporte de armazenamento amovível, como por exemplo em DVD, deve ser protegido com pelo menos uma *cópia de segurança*. De preferência devem efectuar-se duas *cópias de segurança*, uma destinada a ser utilizada em substituição do original e a segunda a ser armazenada juntamente com o original em cofre próprio para o efeito (à prova de fogo etc.). Uma das cópias pode ser efectuada para um dispositivo de armazenamento de rede caso se verifiquem vantagens operacionais na utilização da mesma. O original ou uma cópia pode e devem ser transportadas para um cofre *Off-site* por questões de segurança.

5 – Sistemas ou Software Específicos

Sistemas informáticos e software em suporte amovível que não se encontrem englobados em nenhum dos modelos anteriores tais como sistemas informáticos não

institucionais como os que são propriedade de particulares ou de terceiros, conectados ou não à rede, devem ser alvo de um procedimento de *backup* específico sempre que tal seja solicitado. A documentação e formalização desses procedimentos devem, sempre que possível, seguir a presente política nas suas orientações e regras. É da responsabilidade do *supervisor de backups* a definição de novas regras, procedimentos, documentos complementares e acertos caso tal seja necessário. O procedimento de *cópia de segurança* de sistemas ou software específicos devem ficar devidamente documentados e formalizados. Na definição do processo de *backup* específico ter-se-ão em conta um alargado número de factores tais como o *hardware* do sistema, sistema operativo, detalhes da aplicação, volume de dados, frequência da modificação (actualização) da informação e requisitos de disponibilidade da mesma, bem como a propriedade do sistema e o nível de criticidade da informação para a instituição.

Formalização

Os cinco processos chave descritos serão devidamente formalizados e documentados concretamente no que se refere aos seguintes itens:

· Data dos *backups*, testes e restauros
· Frequência dos *backups* e testes
· Tipos dos *backups* (total, incremental)
· Número de Gerações
· Dono do *backup*
· Operador do *backup*
· Tempos requeridos para o restauro da informação
· Tipo de informação copiada (e.g. software, dados do sistema)
· Especificação da informação copiada (ficheiros, directorias)
· Localização dos *backups*
· Tipo de suporte informação
· Ferramentas usadas no *backup*/restauro (versões, comandos, argumentos)

Privacidade e Direitos de Acesso

A autorização referente ao acesso à informação e aos sistemas informáticos que a suportam por parte dos administradores de sistemas, supervisor de *backups*, operadores de *backups*, donos de *backups* ou gestão de topo, são definidas no

documento *"política de acesso a recursos informáticos"* englobada na *"política de segurança dos sistemas de informação"* institucional, sendo que só entidades institucionais autorizadas terão acesso à informação contida nas *cópias de segurança*. É garantida sempre a confidencialidade e segurança da informação. A regulamentação da privacidade, direitos de acesso, integridade e disponibilidade da informação no que se refere a informação armazenada *Off-site*, é devidamente fornecida à gestão e ao responsável do Sistema. A mesma é previamente acordada no âmbito de uma prestação de serviço e formalizada no documento *"política de acesso a recursos informáticos"*, englobada na *"política de segurança dos sistemas de informação"* da instituição.

Quando uma entidade institucional cessa funções, o(s) processo(s) de backup dos quais a entidade era proprietária são suspensos e é seguida a "política de eliminação de informação institucional" caso a mesmo se aplique.

Os SI só efectuarão cópias de segurança sobre a informação expressamente solicitada no formulário de requisição de cópia de segurança (GSI/08) pelo requisitante, tais como "home directory", arquivo de e-mails e favoritos. Essa informação deverá obrigatoriamente ser comprovadamente institucional. Os SI não se responsabilizarão por cópias de segurança de informação comprovadamente não institucional tais como ficheiros multimédia. Os utilizadores deverão por em prática uma filosofia de organização da sua informação pessoal, institucional e não institucional de forma a facilitar a implementação do processo de backup (sobre a informação institucional crítica).

Os SI encorajarão a organização e a não dispersão da informação institucional pelos discos duros dos postos de trabalho.

Definições Backup ou Cópia de Segurança: Processo devidamente formalizado e documentado de cópia de informação, residente em sistemas informático ou em suporte amovível e em formato electrónico, para um meio que é fisicamente diferente (remoto) do sistema original de forma regular e consistentemente.

Visa garantir a possibilidade de restauro da informação original em caso de algum tipo de indisponibilização não planeada da mesma.

COLÉGIO CAMPOS	**Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica**

Backup Total: É o ponto de partida para todos os outros tipos de cópias de segurança. O backup total copia todos os dados de directorias e ficheiros que foram seleccionados para a cópia.

Backup Incremental: É uma cópia que contém somente ficheiros que foram alterados desde o último backup. Existem dois tipos de backup incremental (o que se efectua desde o último backup total, e o que se efectua desde o último backup incremental). Estes variam em tamanho e afectam o tempo de recuperação.

Backup tipo Imagem: É um tipo de backup total (integral) que inclui todo o sistema operativo (e.g. estado, configurações), programas especiais, pacotes e módulos instalados, scripts, dados de licenciamento, e ficheiros de dados. Pode incluir informação de partições e volumes dos discos duros.

As imagens permitem copiar integramente instalações, todos os dados do sistema, bases de dados, ou ficheiros, indiferentemente ao que se copiou no último backup (backup mais recente). Utilizam-se frequentemente em sistemas de produção críticos com instalação e configurações demoradas e trabalhosas e mesmo impossíveis de efectuar em determinado período de tempo. Tecnicamente são conhecidos com *ghosts* ou *snapshots*.

Filosofia de *backup* de três gerações: Arquitectura de *cópias de segurança* que garante o armazenamento de três cópias "autónomas" da informação. A primeira cópia ou cópia mais recente (e.g. diária) é geralmente designada por "Filho". A segunda cópia (e.g. Semanal 2.ª Geração) é geralmente designada por "Pai". E a terceira cópia a cópia mais antiga (e.g. mensal 3.ª Geração) é designada por "Avô". Cada uma das três cópias deve por questões de segurança (redundância) ser armazenada em locais distintos sendo que uma, preferencialmente, deve ser armazenada *Off-site*.

Informação Institucional: refere-se colectivamente a todos os *dados* adquiridos, mantidos, produzidos, tratados, recebidos e transferidos tais como documentos, e-mail, registos de bases de dados bem como todo o *software*, aplicações, serviços instalados e configurados, em desenvolvimento ou produção tais como sistemas operativos, motores de bases de dados, serviços de rede, aplicações de produtividade e aplicações específicas, que processem, armazenem ou transmitam informação institucional. Na tabela de identificação e agregação de elementos de informação

COLÉGIO CAMPOS	**Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica**

(tabela 1) exemplificam-se alguns grupos de informação crítica sobre os quais se considerou uma análise mínima de risco e nível de criticidade.

Elementos de Informação	Níveis de Criticidade			
	Confidencialidade	Integridade	Disponibilidade	Tempo de Vida
Informação académica de docentes Informação geral de bibliografia	L	M	H	H
Informação dos cursos da instituição	L	H	H	M
Informação pessoal de alunos Informação geral de fornecedores/outras instituições	M	M	M	M
Informação pessoal de funcionários/docentes Informação administrativa de funcionários/ docentes	M	M	M	H
Fichas de requisição de bibliografia Informação de identificação de bens móveis e veículos	M	H	H	M
Estatísticas bibliográficas	M	H	M	M
Informação curricular e histórica (académica) do aluno Ficha de registo de expediente Informação de identificação de bens imóveis	M	H	H	H
Informação financeira de fornecedores/outras instituições	H	H	M	M
Informação Financeira de alunos	H	H	H	M
Informação financeira de funcionários/docentes Informação financeira da instituição Informação administ. de saúde de funcionários/docentes	H	H	H	H

Tabela 1 - Identificação e Agregação dos Elementos de Informação Institucional Crítica (utilizadores) *(subconjuntos e conjuntos)*

Entidade institucional: refere-se colectivamente aos indivíduos a que esta política se destina e que são, nomeadamente, as várias unidades de negócio existentes na

instituição (e.q. Gabinetes, Departamentos, Serviços, Projectos) e os vários utilizadores (e.q. funcionários docentes, funcionários não docentes e alunos).

Sistemas informáticos: referem-se colectivamente aos equipamentos informáticos (*software* e *hardware*) que armazenem ou processem informação institucional crítica tais como, estações de trabalho pessoais ou não pessoais, servidores e computadores portáteis.

Sistemas informáticos institucionais: referem-se a sistemas informáticos que são propriedade da Instituição.

Suporte de informação amovível: refere-se colectivamente aos suportes electrónicos de informação tais como, CD-ROM, DVD, pen drive, Zip drive e disquete e não engloba suportes de informação fixos e integrantes de sistemas informáticos tais como discos duros e RAMs.

Supervisor de Backup: refere-se ao técnico dos SI, responsável máximo pela política de *backups* e pelo universo de procedimentos que lhe estão associados, bem como por todas as decisões de fundo associadas aos mesmos, tais como definição de procedimentos de *backup* específicos. É igualmente o responsável pela elaboração e manutenção do catálogo de *cópias de segurança*, e pelas "campanhas" de sensibilização às entidades institucionais. Em caso de falta ou indisponibilidade do *operador do backups* deverá, também, ficar responsável pelas suas tarefas e atribuições. É o responsável por comunicar não conformidades ao órgão de gestão máximo e por promover revisões periódicas desta política.

Operador do Backup: refere-se ao técnico dos SI responsável pelos três processos chave; *cópia de segurança*, teste à *cópia de segurança* e restauro da *cópia de segurança*. É responsabilidade do operador de *backup* apoiar os donos de *backup* a preencherem devidamente os formulários de requisição de serviço e completá-los o mais correctamente possível de forma a documentarem extensivamente e inequivocamente os processo de *backup*, teste e restauro. É responsabilidade do operador de *backup* comunicar ao supervisor de *backups* não conformidades alterações e anomalias nos processos que opera.

Dono do Backup: refere-se à entidade institucional que solicitou o *backup* e é responsável pela informação institucional crítica original copiada, pode ser; funcionário docente, funcionário não docente ou aluno.

COLÉGIO CAMPOS	**Politica para efectuar os backups e restauração de backups dos dados dos componentes da infra-estrutura tecnológica**

Armazenamento On-site: refere-se ao facto de a informação estar armazenada no mesmo edifício em que se encontra armazenada a informação original.

Armazenamento Off-site é baseado no nível de criticidade da informação institucional e cumpre o requisito da dispersão geográfica de redundâncias (requisito de segurança de sistemas de informação). O armazenamento da informação *Off-site* deve ser feito numa localização geográfica diferente da do campus da instituição para que desastres que ocorram na instituição não afectem a informação armazenada que se pretende "protegida".

Informação existente em formato electrónico: refere-se colectivamente a toda a informação institucional que está armazenada temporária ou permanentemente em dispositivos ou meios *electrónicos* tais como Discos Duros, RAMs, CD's, DVD's, *pen drives*, *floppy disks*, e *tape backups*.

Consequências de não Conformidade

Não conformidades resultantes da não aplicação desta política podem ter impactos severos na instituição expondo a perdas permanentes de informação institucional crítica, (e.g. registos financeiros, registos académicos, material de investigação, serviços e projectos) e expor a instituição a acções legais. Pode igualmente ter impacto no bom e normal funcionamento da instituição. Qualquer acção em não conformidade com esta política por parte de qualquer entidade institucional será comunicada por escrito ao órgão de gestão máximo.

Revisão

As condições da infra-estrutura das TIC da instituição são alteradas diariamente bem como os níveis de criticidade da informação institucional variam, tal pode colocar em causa a eficácia dos procedimentos, ferramentas e indicadores adoptados nos processos de cópia, teste e restauro da informação crítica. Assim, caso se verifique que a presente política (regras e procedimentos) se encontra desadequada, desactualizada ou desenquadrada do actual panorama tecnológico institucional, este documento deverá ser revisto e actualizado.

3- ASSINATURAS:

Responsável pela execução do plano
__/__/_____ _____

COLÉGIO CAMPOS	**Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica**

☐ EFECTUAR BACKUP ☐ EFECTUAR RESTAURO DE BACKUP

1- IDENTIFICAÇÃO

DADOS GERAIS:	CARGO:
NOME _____	☐ DOCENTE DEPT: _____
E-MAIL _____	☐ FUNCIONÁRIO: SERVIÇO: _____
CONTACTO TELEFÓNICO _____	☐ OUTRO A INDICAR: _____

2. REQUISITANTE

Identificação do Dono do Backup (ou cópia de segurança)

Nome: _____
N.º Mecanográfico: _____
E-Mail: _____
Telefone: _____

☐ Departamento ☐ Serviço ☐ Gabinete
☐ Projecto ☐ Aluno ☐ Outro

Identificação do Suporte de Informação Original

☐ Estação de Trabalho ☐ Computador Portátil ☐ Servidor ☐ Outro Sistema: _____
Localização do Computador / Sistema:

☐ Departamento ☐ Serviço ☐ Gabinete
☐ Projecto ☐ Aluno ☐ Outro

Nome do Computador / Sistema: _____
Endereço IP do Sistema: _____ ☐ Não Conectado à Rede
Observações: _____

☐ Software Adquirido ☐ Software Desenvolvido ☐ Outro Software: _____
Nome: _____
Versão: _____
Fabricante: _____
Tipo de Suporte:
☐ DVD ☐ CD ☐ Pen Drive ☐ Outro Suporte: _____
Observações: _____

COLÉGIO CAMPOS	**Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica**

Identificação da Informação Original

☐ Dados de Trabalho ☐ Correio Electrónico ☐ Contactos ☐ Favoritos

☐ Aplicação ☐ Dados de Aplicação ☐ Sistema Operativo ☐ Home Directory

Outros: _____

Observações: _____

_____

_____ _____

O Dono do Backup *Data da Requisição*

COLÉGIO CAMPOS	**Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica**

2. EXECUÇÃO DO BACKUP

Operador do Backup: _____

Identificação do Backup: Referência: _____

Caracterização do Backup

☐ Sistema Institucional Crítico

☐ Sistema Institucional não Crítico Conectado à Rede

☐ Sistema Institucional não Crítico não Conectado à Rede

☐ Software em Suporte de Informação Amovível

☐ Sistema ou Software Específico

Observações: _____

Sistema Operativo

Windows 2000 Prof.	☐ Windows XP	☐ Windows Vista	☐ Windows 2003 Server
☐ Linux	☐ MacOS X	☐ Sun Solaris	☐ Windows 2008
☐ Outro			

Observações: _____

Sistema de Ficheiros

☐ FAT16	☐ FAT32	☐ NTFS	☐ ISSO 9660
☐ ext2	☐ ext3	☐ ZFS	☐ UDF
☐ Outro			

Tipo e Localização do Backup

Geração	Tipo	Frequência	Suporte de Inf.	Localização	1.ª Verificação
1.ª	☐ Total ☐ Incremental ☐ Imagem ☐ Outro_____	☐ Diário ☐ Semanal ☐ Mensal ☐ Outro_____	☐ HDD ☐ DVD / CD ☐ HDD Amovível ☐ Outro_____	☐ On-site ☐ Off-site ☐ NAS:_____ ☐ NFS:_____ ☐ Cofre:_____ ☐ Outro:_____	_____ *Data* _____ *Operador Backup*

COLÉGIO CAMPOS

Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica

2.ª	☐ Total ☐ Incremental ☐ Imagem ☐ Outro_____	☐ Diário ☐ Semanal ☐ Mensal ☐ Outro_____	☐ HDD ☐ DVD / CD ☐ HDD Amovível ☐ Outro_____	☐ On-site ☐ Off-site ☐ NAS:_____ ☐ NFS:_____ ☐ Cofre:_____ ☐ Outro:_____	_____ *Data* _____ *Operador Backup*
3.ª	☐ Total ☐ Incremental ☐ Imagem ☐ Outro_____	☐ Diário ☐ Semanal ☐ Mensal ☐ Outro_____	☐ HDD ☐ DVD / CD ☐ HDD Amovível ☐ Outro_____	☐ On-site ☐ Off-site ☐ NAS:_____ ☐ NFS:_____ ☐ Cofre:_____ ☐ Outro:_____	_____ *Data* _____ *Operador Backup*

Responsável Armazenamento Offsite:_____E-Mail:_____

Observações:_____

Método / Ferramenta do Backup

Geração	Método	Ferramenta	Tamanho/Tempo	Observações
1.ª	☐ Manual ☐ Automático ☐ Outro	Nome:_____ Versão:_____ Comando:_____	1.ª Cópia Tamanho Aproximado Cópia Tempo Aproximado Recuperação	_____ _____ _____
2.ª	☐ Manual ☐ Automático ☐ Outro	Nome:_____ Versão:_____ Comando:_____	1.ª Cópia Tamanho Aproximado Cópia Tempo Aproximado Recuperação	_____ _____ _____
3.ª	☐ Manual ☐ Automático ☐ Outro	Nome:_____ Versão:_____ Comando:_____	1.ª Cópia Tamanho Aproximado Cópia Tempo Aproximado Recuperação	_____ _____ _____

Observações:_____

COLÉGIO CAMPOS	**Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica**

2. EXECUÇÃO DO RESTAURO DO BACKUP

A preencher pelo requisitante após processo de restauro da informação concluído.

Avaliação do Processo de Recuperação

- ☐ Informação e/ou Sistema recuperado com sucesso dentro do tempo planeado
- ☐ Informação e/ou Sistema não recuperado com sucesso:
  - ☐ Informação Incompleta
  - ☐ Tempo excessivo
  - ☐ Outro: _____

_____ _____

O Dono do Backup *Data da Avaliação*

Operador do Backup: _____ E-Mail: _____

Referência da Requisição: _____

Identificação do Backup:

Referência do Backup: _____

Caracterização do Restauro

☐ Sistema Institucional Crítico

☐ Sistema Institucional não Crítico Conectado à Rede

☐ Sistema Institucional não Crítico não Conectado à Rede

☐ Software em Suporte de Informação Amovível

☐ Sistema ou Software Específico

Causa da Perda de Informação

Perda de informação motivada por: _____

Origem do Backup Restaurado

Geração: _____

Localização: _____

Data da Ultima Actualização: _____

Indicadores do Restauro

Tempo total para conclusão do restauro: _____

Tamanho total para conclusão do restauro: _____

Anomalias e Observações

Apreciação: _____

COLÉGIO CAMPOS	**Requisição para efectuar cópias de segurança ou restauro de backups a componentes da infra-estrutura tecnológica**

Avaliação do Restauro

- ☐ Informação e/ou Sistema recuperado com sucesso dentro do tempo planeado
- ☐ Informação e/ou Sistema não recuperado com sucesso:
  - ☐ Informação Incompleta
  - ☐ Tempo excessivo
  - ☐ Outro: _____

Causas para insucessos da recuperação:

_____
_____
_____
_____

Observações: _____
_____
_____
_____
_____

Foi gerado e anexado Relatório de Recuperação do Sistema e/ou da Informação

- ☐ Sim
- ☐ Não

Recebido Por: _____ *em:* _____

Implementado pelo Operador do Backup: _____ *em:* _____

Notificação ao Dono e ao Supervisor de Backups: _____ *em:* _____

COLÉGIO CAMPOS	**Versões dos documentos associados aos Sistemas de Informação**

1- VERSÕES DOS DOCUMENTOS

LISTA DE VERSÕES CATEGORIZADAS POR TIPO DE DOCUMENTO (RELATÓRIOS, TESTES, PLANOS, ETC):

TIPO DE DOCUMENTO:_____

Versão anterior	VERSÃO	DATA DA ACTUALIZAÇÃO	REQUERENTE

TIPO DE DOCUMENTO:_____

Versão anterior	VERSÃO	DATA DA ACTUALIZAÇÃO	REQUERENTE

TIPO DE DOCUMENTO:_____

Versão anterior	VERSÃO	DATA DA ACTUALIZAÇÃO	REQUERENTE

2- OBSERVAÇÕES

COLÉGIO CAMPOS	**Esquema do modelo da base de dados de configurações**

2- ESQUEMA DA BASE DE DADOS

☐ NOVA VERSÃO DATA: _____ VERSÃO ANTERIOR: _____

3- OBSERVAÇÕES

4- ASSINATURAS:

Responsável pela execução
__/__/____ _____

COLÉGIO CAMPOS	**Configurações dos componentes da infra-estrutura tecnológica**

1- IDENTIFICAÇÃO

☐ NOVA VERSÃO DATA: _____ VERSÃO ANTERIOR: _____

2- ESQUEMA DAS CONFIGURAÇÕES POR COMPONENTE

NOTA: PODERÁ ANEXAR DOCUMENTOS OU INDICAR ONDE SE ENCONTRAM OS FICHEIROS DAS CONFIGURAÇÕES

3- OBSERVAÇÕES

4- ASSINATURAS:

Responsável pela execução
__/__/____ _____

Responsável pela aprovação
__/__/____ _____