INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Avaliação de Riscos para a Segurança da Informação no ISEP Aplicação ao Processo de Notas

TIAGO NUNO DE OLIVEIRA FERREIRA
Outubro de 2014

POLITÉCNICO
DO PORTO

Avaliação de Riscos para a Segurança da Informação no ISEP

Aplicação ao Processo de Notas

Tiago Nuno Oliveira Ferreira

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Arquiteturas, Sistemas e Redes

Orientador: António Cardoso Costa

Co-orientador: [Nome do Co-orientador (caso exista)]

Júri:

Presidente:

[Nome do Presidente, Categoria, Escola]

Vogais:

[Nome do Vogal1, Categoria, Escola]

[Nome do Vogal2, Categoria, Escola] (até 4 vogais)

Porto, [Mês] [Ano]

“O segredo da sabedoria, do poder e do conhecimento é a humildade.”

Ernest Hemingway [1899-1961]

Resumo

Desde que existe informação, há necessidade de criar um sistema que permita gerir e garantir que a informação está segura e que cumpre os requisitos básicos de segurança. Como tal, é necessário desenvolver técnicas e mecanismos para que os requisitos sejam testados e melhorados continuamente.

Com esta necessidade em vista, apareceram padrões que dão resposta a um conjunto vasto de problemas, em diferentes sistemas e aplicações diversas. Estes tornaram-se guias de reflexão para quem os analisava, de arquitetura para quem os implementava e modelos para quem os geria.

O padrão ISO 27001 dá resposta aos cuidados a ter para se conseguir um sistema de gestão da segurança da informação eficaz e eficiente. Esta norma preocupa-se com os detalhes de aplicação até à forma como é implementado e arquitetado o sistema. Os processos, atividades, fluxos de trabalho são essenciais para que esta norma seja cumprida. É necessário um bom escrutínio dos processos e suas atividades, assim como um fluxo de trabalho bem definido com papéis e responsabilidades de cada ator. É necessário também assegurar a forma como é gerido, a sua verificação e melhoria contínua.

Foi aplicado no ISEP um exercício com o qual se pretendeu verificar se os processos e outros aspetos seguiam estes cuidados e se estavam de acordo com a norma. Durante o exercício foram verificados processos dentro de um certo âmbito, todas as suas atividades, papéis e responsabilidades, verificação de recursos, aplicação de controlos e aplicação de uma análise de risco. Esta análise tem como objetivo verificar o nível de segurança dos recursos, algo que a norma ISO 27001 propõe mas não especifica em que moldes.

No final deste exercício pretendeu-se melhorar o sistema de gestão de informação do ISEP em vertentes tais como a documentação, a qual especifica quais os passos realizados no decorrer do mesmo.

Palavras-chave: Sistema de gestão da informação, norma ISO 27001, processos, análise de risco, fluxo de trabalho, aplicação de controlos

Abstract

Since there is information, a need exists to create a system that allows managing and ensuring the information is safe and meets the basic security requirements. As such, there was a need to develop techniques and mechanisms for requirements to be tested and continuously improved.

With this need in mind, patterns appeared that gave answer to a wide range of problems, different systems and applications. These became guides to those who analyzed the problem, the architecture and who was implementing the models.

The ISO 27001 standard addresses the precautions to ensure that a security management system deals with effective and efficient information. This standard is concerned with every detail of how it is implemented and how a system is architected. Processes, activities, workflows become essential for the application of this standard. A good scrutiny of processes and activities, as well as a workflow with well-defined roles and responsibilities for each actor, are required. It is also necessary to ensure the way it is managed, as well as its verification and continuous improvement.

In ISEP a process aiming to verify if these and other procedures were followed was run, and if security was in accordance with the standard. During this process it was observed the framework, activities, roles and responsibilities, actions, implementation controls, and a risk analysis was undertaken. Risk analysis intends to verify the security level of resources, as ISO 27001 describes, but without specifying the way to do it.

This exercise intended to improve the management system of ISEP, producing documentation describing what steps were performed during the exercise and results obtained.

Keywords: Management information system, ISO 27001, processes, risk analysis, workflow, application controls

Agradecimentos

A elaboração deste trabalho não teria sido possível sem as importantes contribuições que gostaria de destacar:

Agradeço ao Professor João Rocha, Presidente do ISEP, por ter permitido usar o assunto no âmbito de uma tese de mestrado no ISEP.

Agradeço ao Professor José Oliveira, Vice-Presidente do ISEP, pelas contribuições dadas durante a realização da tese e pela grande disponibilidade institucional e pessoal evidenciada.

Agradeço também ao Engenheiro Paulo Borges, pela contribuição inestimável na sua qualidade de auditor/consultor na área da segurança da informação, da qual muito beneficiaram esta tese e os seus intervenientes.

Agradeço igualmente ao Professor António Costa por todo o apoio, acompanhamento, tempo despendido e todas as sugestões na elaboração do trabalho e do relatório.

Por fim, agradeço aos meus pais, familiares e amigos por toda a paciência, carinho e disponibilidade ao longo da realização deste trabalho.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos

Lista de Acrónimos

ISEP	Instituto Superior de Engenharia do ISEP
AENOR	*Asociación Española de Normalización y Certificacion*
NP	Indicação de Norma Portuguesa
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
ISMS	Sistema de gestão da segurança da informação

1 Introdução

1.1 Enquadramento

Relativamente à informação, há necessidade de avaliar frequentemente ou até permanentemente pelo menos três requisitos: confidencialidade, integridade e disponibilidade. Com a evolução tecnológica e tudo o que dela resulta, a gestão da informação transformou-se numa necessidade, quer para os indivíduos como para as organizações.

Com a possibilidade de utilização de suportes tecnologicamente sofisticados que ajudam a respeitar minimamente os requisitos, tornou-se possível a gestão integrada da informação e de todos os seus requisitos e necessidades. Esta transformação permitiu que os requisitos básicos de segurança da informação fossem cumpridos, o que potenciou os resultados do trabalho sobre a informação, tornando-o mais rápido, seguro e eficaz.

Contudo, por diferentes razões e motivos, as necessidades atuais de ritmos elevados de trabalho por vezes podem fragilizar a gestão dos sistemas de informação, perdendo-se a noção de que é um sistema e para o que serve. Em consequência, delega-se para segundo plano a forma como é estruturado e de que formas está a dar respostas, bem como o respeito pelos seus requisitos de segurança (e outros).

Tipicamente um sistema de informação tem obrigatoriamente de respeitar pelo menos três requisitos, podendo ser acrescentados mais, o que irá aumentar a complexidade do sistema e afetar a sua implementação, operação e manutenção. Torna-se então essencial por à prova o sistema de informação, com vista a determinar objetivamente se respeita os seus requisitos de segurança de informação. As normas ou padrões internacionais servem, entre outras funções, para por à prova os mecanismos, as pessoas, os documentos, entre outros, que são "processados" por um sistema de informação. As normas permitem que as organizações se estruturem através da documentação, da definição de papéis e responsabilidades, entre outros, e com isto respeitem a orgânica da segurança da informação, ao invés de transferir a responsabilidade para o próprio sistema de informação, incluindo a necessidade de assegurar os requisitos mínimos de segurança. A universalização destes padrões permite que os sistemas sejam reconhecidos internacionalmente e que possam ser objeto de estudo em termos de implementação. A acreditação internacional dos sistemas de informação gera reputação, respeito e melhoria para uma organização acreditada. O reconhecimento de que

um sistema de informação é seguro, através da acreditação internacional baseada em normas fiáveis, potencia a respetiva organização e todos os seus elementos.

Em suma, os sistemas de informação de uma organização devem respeitar três requisitos básicos de segurança: confidencialidade, integridade e disponibilidade. Ao respeitar estes requisitos, a organização melhora a sua continuidade de negócio, minimiza a possibilidade de perdas, ganha competitividade e poderá mais facilmente a respeitar os normativos aplicáveis. Permite igualmente obter melhor organização interna, bem como uma gestão e planificação mais eficazes. Para isso é necessária uma atitude de melhoria contínua, o que implica a monitorização e verificação do sistema de informação.

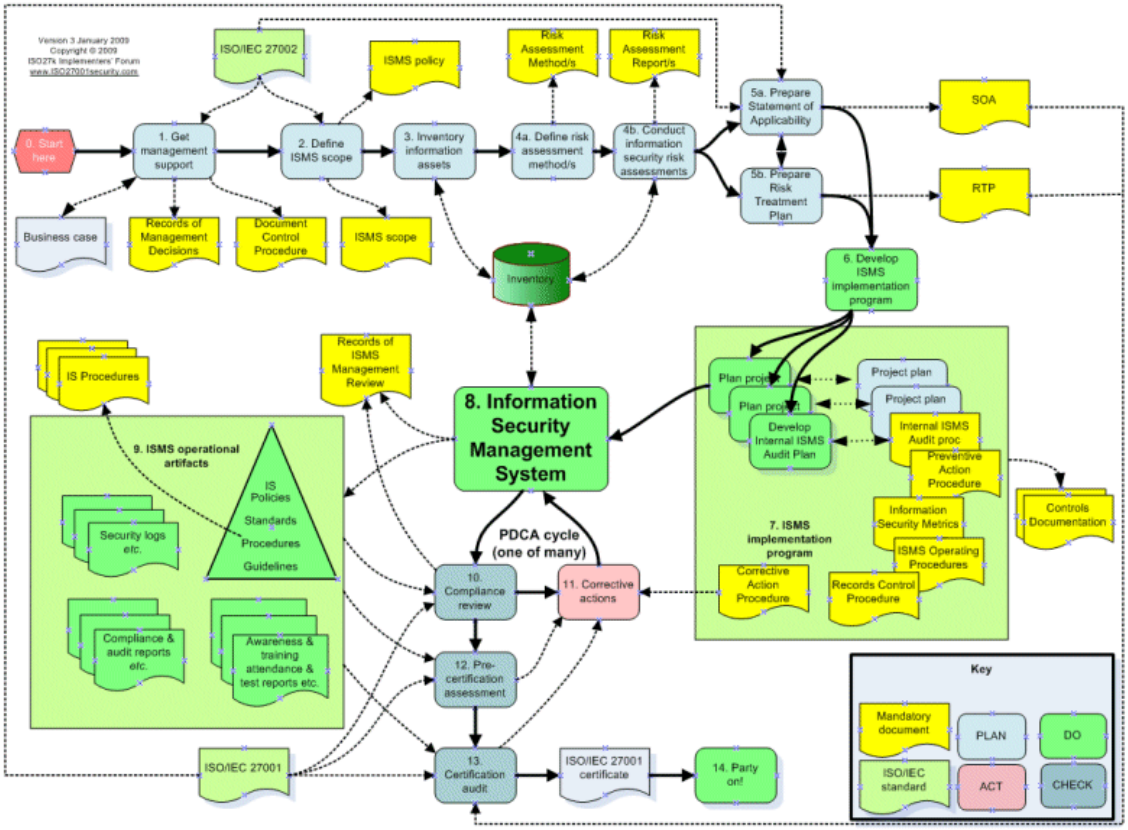
1.2 Apresentação da tese

Esta tese tem como intuito a realização de um exercício estruturado no qual é aplicada a norma ISO 27001 no ISEP. É pretendido, utilizando esta norma, uma obtenção do estado da segurança da informação, processos, recursos e estrutura organizacional, tal como, um ponto de partida para uma eventual acreditação do sistema de gestão da informação do ISEP. Pretende-se verificar toda a documentação disponível e comparar com o pedido pela norma ISO. Em caso de falhas ou não existência dos mesmos é criado um novo documento e que completará essa lacuna. A Figura 1 descreve os passos necessários para a implantação da acreditação num sistema de gestão da informação.

No âmbito da auditoria de 2º acompanhamento anual (AS2, 2013), na sequência da concessão do certificado AENOR conforme a norma NP EN ISO 9001:2008, realizada ao sistema de gestão da qualidade (SGQ) do ISEP, foi identificada por uma equipa auditora da LUSAENOR uma oportunidade de melhoria: ser realizado um exercício estruturado e completo de avaliação de riscos para a segurança da informação (utilizando as recomendações do Anexo A da ISO/IEC 27001:2005). Esta tese consiste no estudo, preparação, realização e avaliação do referido "exercício estruturado e completo", sendo que o resultado obtido terá não só valor técnico-científico, mas também organizacional para o ISEP.

Na Figura 1 descrevem-se os passos da acreditação de um sistema de gestão da informação. As atividades relacionadas com esta tese correspondem às atividades representadas na parte superior esquerda (1, 2, 3, 4a, 4b, 5a e 5b). Espera-se que os resultados desta tese ajudem a organização (ISEP) a avançar para os passos 6 e seguintes.

Figura 1 - ISO 27001 (New, 2014)



Esta tese tem igualmente o propósito de contribuir para uma melhor organização interna dos processos, recursos, entre outros, do ISEP, mas também para uma acreditação futura do sistema de gestão da informação e todos os processos associados. Os resultados obtidos nesta tese são um ponto de partida para trabalhos futuros, podendo a abordagem adotada ser diretamente aplicada noutras organizações.

1.3 Apresentação da organização

1.3.1 História da organização

O ISEP foi fundado em 1852, no período de ascensão do liberalismo português, pela força de uma ideia de progresso: Portugal, país com uma estrutura predominantemente rural e de serviços, precisava de dar um passo em frente. Foi Fontes Pereira de Melo, ministro das Obras Públicas, do Comércio e da Indústria, quem lançou o primeiro sistema público de ensino industrial, assente na ideia de educação para o desenvolvimento, onde a matriz, a Escola

Industrial do Porto, foi uma das duas primeiras, em confronto com a Academia Politécnica, cuja referência era o modelo elitista, academista e retórico da Universidade de Coimbra que, incapaz de responder às necessidades emergentes, vinha sendo contestado pelos intelectuais mais esclarecidos.

Em 1864, sob a égide do Ministro Conselheiro João Chrysostomo de Abreu e Sousa, efetua-se uma ampla reforma e expansão do ensino industrial. O ensino "superior" industrial é, então, dividido em duas partes: a primeira incluía formação geral comum a todas as artes, ofícios e profissões industriais, integrando duas componentes: o ensino teórico, ministrado na Escola, e o ensino prático, ministrado nas oficinas do Estado ou, sob acordo, em fábricas particulares; a segunda incluía o ensino especializado de certas artes e ofícios e também de diversos serviços públicos tais como obras públicas, minas e telégrafos. No âmbito desta reforma a Escola Industrial passa a Instituto Industrial do Porto, formando "mestres", "condutores" e "diretores de fábrica".

Em 1881, durante a visita ao Porto do Rei D. Luís, o então Ministro do Reino Tomás Ribeiro e o Ministro das Obras Públicas Rodrigues de Freitas propuseram a fusão das duas escolas de topo do ensino industrial - a Academia Polytéchnica do Porto e o Instituto Industrial do Porto - numa só, denominado Instituto Polytéchnico do Porto. O Conselho Escolar, considerando que tal projeto era contrário ao seu percurso histórico, recusa o projeto de fusão com a Academia Polytéchnica, assim dando corpo a uma cultura institucional que perdura até hoje: ensinar não só o saber conhecer, mas também o saber fazer.

Durante todo o período da I República discutiu-se se Portugal deveria ser, essencialmente, um país de indústrias ou um país agrícola, diluindo-se nesta indecisão a definição de uma política industrial que se ia afirmando no exterior. E o advento do Estado Novo não altera significativamente o status quo. Mantém-se assim uma situação de grande indefinição, que há-de perdurar até quase aos nossos tempos.

A estrutura do ensino industrial refletirá isso mesmo: só entre 1947 e 1950 se redefine o papel dos Institutos Industriais no âmbito de uma reformulação do ensino industrial, colocando-os no vértice da estrutura de ensino industrial, classificando o seu ensino de "técnico médio no ramo industrial", tendo como objetivo a formação de agentes técnicos de engenharia em todas as especialidades clássicas, dotados de um perfil que lhes possibilita a

entrada direta no sistema produtivo, no desempenho das funções operacionais de topo necessárias ao nascente desenvolvimento industrial.

Em 1974, através do decreto-lei 830/74 de 31 de Dezembro, converteram-se os Institutos Industriais em Institutos Superiores de Engenharia. No preâmbulo deste decreto-lei reconhece-se que "os Institutos Industriais são escolas com um longo passado que formaram gerações de profissionais que, indiscutivelmente, deram um fundamental contributo para o desenvolvimento da indústria portuguesa". É pois no âmbito deste reconhecimento que os Institutos são inseridos na estrutura do ensino superior, como Escolas independentes dotadas de personalidade jurídica e autonomia administrativa, convertendo-se o Instituto Industrial do Porto no atual Instituto Superior de Engenharia do Porto, habilitado à concessão, entre outros, dos graus de bacharel e de licenciado em engenharia, a que correspondem os títulos profissionais de engenheiro técnico e engenheiro.

Em 1989 o Instituto Superior de Engenharia do Porto é integrado no subsistema de Ensino Superior Politécnico, passando o seu modelo de formação a integrar dois cursos distintos: o bacharelato, com a duração de três anos, e os Cursos de Estudos Superiores Especializados, com a duração de dois anos e acesso por concurso documental, que, em conjunto com um bacharelato com ele coerente, conferia o diploma de licenciatura.

Em 1998, no âmbito de uma nova reforma do ensino superior politécnico, o ISEP passa a ministrar as licenciaturas bietápicas, caracterizadas pela sua estruturação em dois ciclos - o bacharelato com a duração de três anos - o que possibilita a inserção no mercado de trabalho, seguido de um segundo ciclo de dois anos - frequentado essencialmente em regime pós-laboral - para a obtenção da licenciatura.

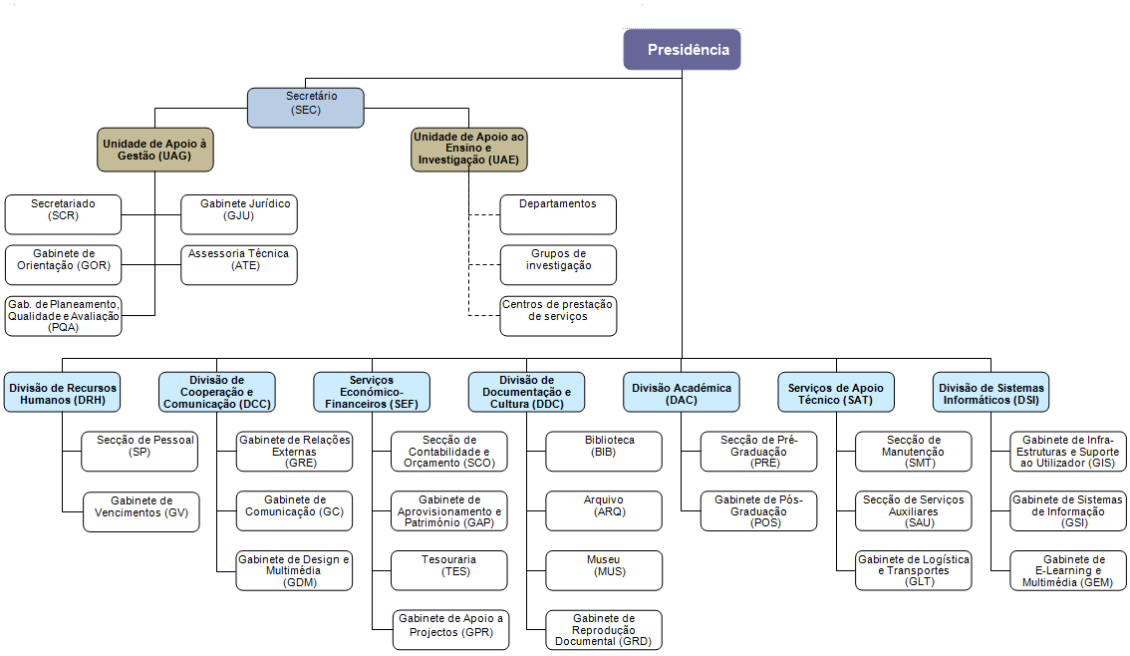
Em 2006, por força da adesão de Portugal à Declaração de Bolonha, o ISEP disponibilizará um novo Plano de Estudos, constituído por licenciaturas e mestrados nas diversas áreas da Engenharia, assim iniciando um novo ciclo da sua já longa história.

Em 2008, Aníbal Cavaco Silva, Presidente da República Portuguesa, enaltece a qualidade do trabalho desenvolvido no ISEP durante o Roteiro para a Ciência. A passagem pelo ISEP constitui a primeira visita oficial de um chefe de Estado português a um instituto politécnico (ISEP, 2014).

1.3.2 Organização do ISEP

A organização atual do ISEP orienta-se para a prestação de serviços, sobretudo relacionados com o ensino superior, incluindo a investigação, os serviços de apoio e outros. A Figura 2 descreve a organização atual dos serviços no ISEP.

Figura 2 - Organização do ISEP (ISEP, 2014)



No topo da Organização existe a Presidência, órgão que inclui o Presidente e os Vice-Presidentes. Num nível abaixo está o Secretário, do qual dependem duas grandes unidades. Na dependência da Presidência estão os serviços e as divisões, nas quais se desenvolve a maior parte da atividade do ISEP. Por exemplo, é na divisão académica (DAC) que se trata grande parte dos problemas relacionados com os estudantes, incluindo a prestação de serviços aos mesmos tais como emissão de certidões, etc.

1.3.3 Contextualização do problema na organização

O exercício estruturado subjacente a esta tese engloba apenas uma parte da organização, dado que foi estabelecido pela Presidência do ISEP que seria apenas tratado o processo de ensino. Trata-se de um processo do ISEP que, na sua qualidade de instituição do ensino superior, é muito importante pelos aspetos legais que comporta e que é, em grande parte,

implementado e operado no âmbito do sistema de informação do ISEP, através de uma interface web designada por “Portal do ISEP”.

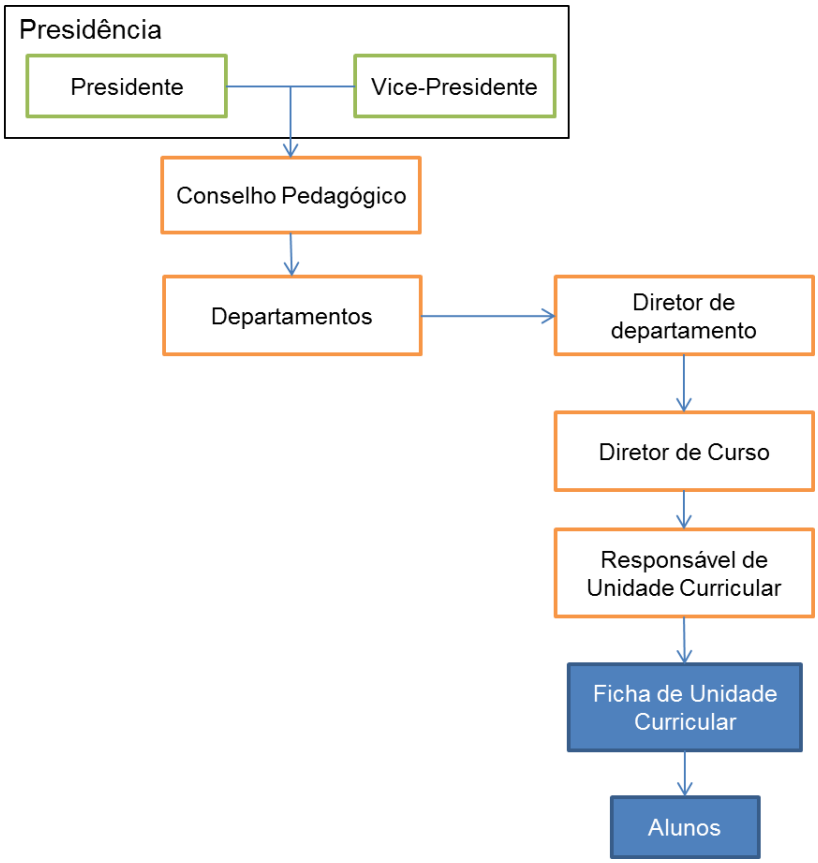
Os objetos organizacionais envolvidos nesta tese foram:

- A Presidência (ator);
- Os Responsáveis de Unidade Curricular (atores);
- Os Diretores de Curso (atores);
- Os Diretores de Departamento (atores);
- Os Alunos (atores);
- O Conselho Pedagógico (ator);
- A Ficha de Unidade Curricular (peça).

A peça processual que armazenará os resultados do processo alvo de estudo nesta tese é a Pauta de Unidade Curricular, a qual contém classificações com notas por aluno. Trata-se de uma peça que é gerida pelo sistema de informação do ISEP e sobre a qual impendem requisitos elevados de segurança da informação.

A Figura 3 apresenta os atores e peças envolvidos neste processo.

Figura 3 - Partes afetadas no processo



O Presidente e um Vice-Presidente (como gestor operacional) têm a responsabilidade máxima no processo. São eles que definem os objetivos a atingir, verificam se existem erros no processo, deliberam, respondem a requerimentos efetuados e agem em casos de incumprimento. São os responsáveis máximos pelos processos implementados no ISEP, pelo seu funcionamento e pelos resultados decorrentes.

Mais abaixo surge o Conselho Pedagógico, que delibera sobre pedidos de alteração de fichas da unidade curricular, sendo necessária a aprovação final do Presidente.

O ator seguinte representa os departamentos do ISEP através dos respetivos diretores, que têm a responsabilidade de propor nomes de docentes para serem responsáveis de unidades curriculares.

Os diretores de cursos, que são nomeados pelo Presidente do ISEP, são responsáveis por aprovar ou recusar a proposta de responsáveis de unidades curriculares. Em caso de recusa

deverão interagir com diretores de departamentos até se obter a aprovação de todos os responsáveis de unidade curricular para o curso em causa.

O responsável de unidade curricular tem como funções o preenchimento da ficha de unidade curricular, na qual se inclui a definição dos momentos de avaliação, a fórmula de cálculo da nota final à unidade curricular, o lançamento de notas de alunos nas pautas de unidade curricular, etc. A ficha da unidade curricular é um recurso indispensável para o funcionamento da unidade curricular. Para tal é necessário que o responsável de unidade curricular a preencha, de modo a ser aprovada pelo diretor de curso e pelo conselho pedagógico. Em caso de recusa de aprovação, o responsável de unidade curricular deverá fazer as alterações adequadas com vista à aprovação definitiva da ficha. Só depois dessa aprovação é que a ficha entra em vigor e os alunos podem tomar oficialmente conhecimento do funcionamento da unidade curricular.

Por fim, os alunos constituem um ator relevante, representando o cliente final na prestação do serviço. Os alunos podem reclamar em caso de incumprimento da ficha de unidade curricular, lapsos na atribuição de notas, etc., o que poderá despoletar outros processos de âmbito corretivo.

1.4 Contributos deste trabalho

Com a realização desta tese, o processo descrito e os resultados obtidos possibilitaram a melhoria de alguns processos do ISEP suportados pelo seu sistema de informação. Como principais contributos devem ser destacados:

1. A alteração proposta e aprovada ao "processo de notas" do ISEP, que se tornou menos dependente de incumprimentos por parte dos seus atores e passou a ter mais e melhores mecanismos de resposta a falhas.
2. A realização de um processo de preparação de análise de risco numa atividade crítica do ISEP (que inclui o "processo de notas"), a qual implicou a definição objetiva de atores, atividades, entradas e saídas das atividades, recursos usados nas atividades, donos de recursos, fontes de risco para os recursos, impactos nos recursos, probabilidades de ocorrência de falhas, riscos para o processo, controlos aplicáveis aos riscos, etc.
3. Poder ser estendido ao ISEP na generalidade e a todos os seus processos, melhorando a organização a nível interno e com repercussões positivas a nível externo.

1.5 Estrutura do relatório

No capítulo 1 abordam-se aspetos organizacionais da informação, a necessidade de um sistema seguro de gestão da informação e apresenta-se a instituição e as entidades envolvidas.

No capítulo 2 apresenta-se o problema, as áreas de negócio afetadas, assim como uma visão da solução e um estudo do estado da arte e da concorrência.

No capítulo 3 explica-se a metodologia de trabalho e o que foi necessário por em prática para cumprir os objetivos com sucesso, detalhando o planeamento e as tecnologias usadas.

O capítulo 4 contém a descrição técnica, os passos para a realização do trabalho, a solução obtida, uma reflexão crítica sobre os resultados e o que deverá ser feito seguidamente.

No capítulo 5 apresentam-se as conclusões desta tese, limitações encontradas e recomendações para trabalho futuro.

Os Anexos contêm documentos elaborados durante a realização do trabalho e elaboração da tese, cuja consulta se recomenda dado serem evidências do exercício e da solução.

2 Contexto

A segurança da informação é um assunto cada vez mais relevante. Trata-se de um tema não meramente tecnológico que não pode ser descurado. Definir o que é "informação" é uma das tarefas mais difíceis numa organização. Definir o que é "importante", quem deve aceder à informação, quem pode alterar a informação, etc., são aspetos críticos de segurança no funcionamento de uma organização.

Numa sociedade virada para as tecnologias e com o aparecimento de aplicações de *software* cada vez mais úteis mas simultaneamente mais complexas, espera-se que estas tenham cuidados especiais e mecanismos de segurança adequados nas funcionalidades disponibilizadas. Por exemplo, são necessárias garantias de segurança porque nem toda a informação deverá ser acessível a todas as pessoas, o que corresponde a dar garantias adequadas de confidencialidade.

Além disso, a segurança da informação é dinâmica, sendo apropriada num certo momento e insuficiente segundos depois, o que complica muito a sua gestão. Por esta e outras razões a segurança da informação deixou de ser um produto e passou a ser um processo, cada vez mais abrangente e importante nas organizações.

A evolução desta problemática gerou a necessidade de a perceber e tratar. Devido a não haver soluções únicas, os estudiosos e especialistas da segurança identificaram a necessidade de especificar soluções genéricas e configuráveis, mais conhecidas por padrões, do que resultou a criação de normas/boas práticas tais como ISO ou *Common Criteria*, entre outras. (Criteria, 2014)

2.1 Problema

Esta tese decorre de uma sugestão feita pela AENOR ao ISEP e tem como objetivo principal a realização de um exercício estruturado, no ISEP, para verificar se a instituição respeita os requisitos da norma ISO 27001 (texto da sugestão da AENOR abaixo, também em anexo).

«*Oportunidades de Melhoria: OM2 – Poderia ser realizado um exercício estruturado e completo de avaliação de riscos para a segurança da informação (ex. utilizando as recomendações do Anexo A da ISO 27001);*»

Para cumprir o objetivo proposto deverá fazer-se, numa fase inicial, um levantamento dos processos, atividades, responsabilidades, normativos aplicáveis, partes interessadas, expectativas de segurança de informação, etc. Na fase seguinte o trabalho deverá ser realizado de acordo com a norma ISO 27001, a qual permite alguma margem de manobra na realização do trabalho. A aplicação desta norma é apropriada dado que se foca em "áreas de negócio" do ISEP sobre as quais incidem requisitos complexos de segurança de informação.

2.2 Áreas de negócio

As normas ISO, como qualquer outra norma de segurança, aplicam-se a qualquer área de negócio, pois são meramente indicativas e de uso não obrigatório. Como tal, estas normas valorizam as organizações que as aplicam porque permitem satisfazer requisitos de segurança que a maior parte das organizações ignorantes destas boas práticas não conseguem atingir. No caso da área de segurança da informação, na qual a família ISO 27000 é a norma mais conhecida e se aplica em quase todos os tipos de negócio. Como cada vez mais as organizações usam pelo menos um sistema de informação, é importante saber se a gestão da informação respeita requisitos apropriados de confidencialidade, integridade e disponibilidade (e eventualmente outros).

A informação é considerada confidencial apenas quando pode ser consultada por entidades previamente autorizadas para o fazer. A informação é considerada íntegra apenas quando pode ser alterada por entidades previamente autorizadas para o fazer. A informação é considerada disponível apenas quando são dadas garantias adequadas que pode ser usada sempre que for necessário.

Quando uma organização dá garantias, em função da sua missão e objetivos, de que estas três vertentes da segurança da informação estão devidamente apropriadas, pode-se afirmar que está "segura". Caso contrário, existe uma oportunidade para se iniciar a implementação da norma 27001 nessa organização.

É importante definir quem é o responsável pela informação e como a informação é transmitida, inclusive em formato não digital. Embora a norma ISO 27001 não se preocupe com as tecnologias que o sistema de informação usa, preocupa-se com o processo de gestão da informação. No âmbito do uso desta norma tem de estar definido quem é o dono da informação, quais os problemas que a podem afetar, como podem falhar os processos e como se responsabilizam os intervenientes. Estas e outras preocupações afetam obviamente uma

organização, podendo até as eventuais mudanças serem incomportáveis. Como referido anteriormente, a aplicação da norma é uma mais-valia para quem a põe em prática, eventualmente melhorando o seu posicionamento perante os competidores diretos devido ao reforço das garantias de segurança e de coesão organizacional.

2.3 Estado da arte

Nesta secção serão analisadas normas relacionadas com a gestão da segurança da informação, incluindo algumas mais centradas na gestão das tecnologias de informação.

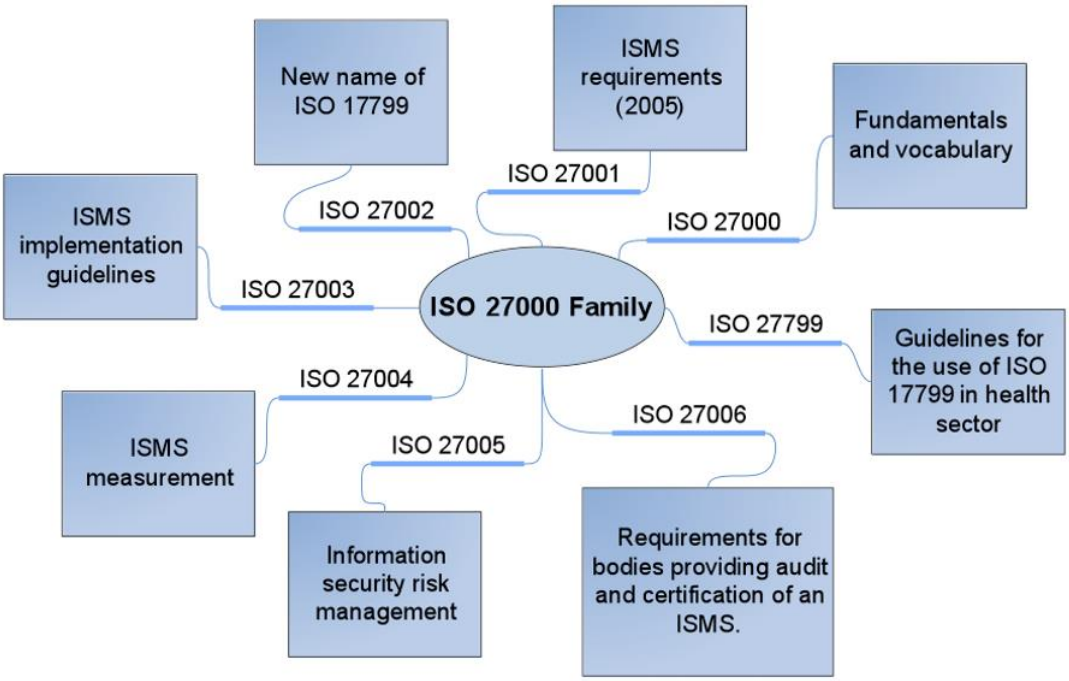
2.3.1 ISO 27001 - Information Security Management System

2.3.1.1 Família ISO 27000

A publicação da BS 7799 pela *British Standard Institution* em 1995 foi o começo do que posteriormente originou a norma ISO 27000. Em 2000 surgiram as primeiras ferramentas informáticas de suporte da BS 7799, sendo adotada pela ISO em dezembro desse ano. Em julho de 2005 a BS 7799 foi convertida em norma ISO (ISO 27001). Passados 5 anos foi lançada a família de normas ISO 27000.

A norma 27000 tem ligação/integração com outras normas, como por exemplo, as normas 9001 e 14001. A versão 2013 da ISO 27001 foi lançada em 25 de setembro desse ano, mais tarde atualizada em 25 de setembro de 2014. A Figura 4 apresenta a família ISO 27000.

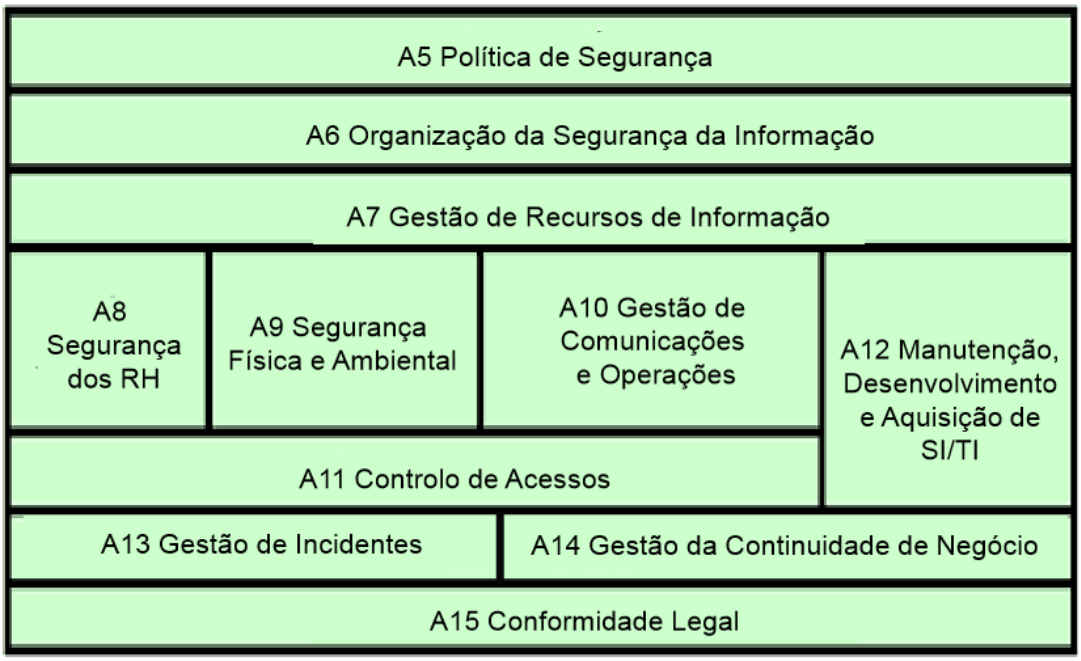
Figura 4 - Família ISO 27000 (Perera, 2014)



2.3.1.2 ISO 27001

Esta norma especifica uma ferramenta de trabalho para gerir a segurança de informação em organizações e, se necessário, evidenciar a terceiros (parceiros de negócio, auditores, clientes ou fornecedores) a sua adequação ao fim previsto. A ISO 27001:2013 é um padrão de segurança da informação e foi publicada em 25 de setembro de 2013, a qual substitui a norma anterior ISO 27001:2005, tendo sido publicada pela ISO e pela IEC. Esta norma descreve a gestão da segurança da informação com base no conceito de risco, verificando se a organização respeita a proporcionalidade e a operabilidade dos controlos de segurança e as proteções da informação definidas. A norma 27001:2013 usa o PDCA (*plan-do-check-act*) como base de gestão do sistema, sendo aplicável a todos os setores da economia. O objetivo principal é fornecer um padrão de gestão da segurança da informação, para o que propõem 114 pontos de controlo distribuídos por 14 grupos (Figura 5).

Figura 5 - Alguns controlos da norma ISO 27001 (Borges, 2014)



Estes 14 grupos de controlos, por sua vez, possuem objetivos de controlo no qual se inserem outros pontos de controlo. A norma ISO 27001 possui grupos de controlos onde são descritas medidas tematicamente relacionadas e diretamente associadas às cláusulas da norma ISO 27002. Por sua vez, os objetivos de controlo delimitam a ação e a aplicabilidade de um ou mais pontos de controlo. Os pontos de controlo correspondem a medidas de implementação, que não são obrigatórias mas tão-somente recomendações.

Na Tabela 1 apresentam-se alguns exemplos de grupos e controlos:

Tabela 1 - Exemplos de grupos e controlos da norma ISO 27001

Controlo	Descrição	Número de Controlos
A.5	Informação das políticas de segurança	2 Controlos
A.6	Organização da segurança da informação	7 Controlos
A.7	Segurança dos recursos humanos	6 Controlos que são aplicáveis antes, durante e depois da sessão de trabalho

2.3.1.3 Principais mudanças da ISO 27001:2005 para a ISO 27001:2013

As principais mudanças entre as duas versões foram:

- Ênfase nos "*Objectives, monitoring and measurement*" do ISMS.
- Alinhamento com a ISO 22301 – Continuidade de Negócio.
- Nova cláusula para tratamento de "*Third Parties*" (partes interessadas externas).
- Nova cláusula acerca da comunicação com "*Third Parties*".
- Nova cláusula sobre criptografia.
- "*Documented Information*" = "*documents*" + "*records*".
- Não há lista de documentos requeridos.
- Alinhamento com a ISO 27005 na Gestão do Risco.
- Distinção entre medidas preventivas e medidas corretivas.
- Total de 14 cláusulas de segurança (eram 11).
- Número de controlos reduzido para 113 (eram 133).

Contudo, para uma melhor adaptação e harmonização com outras normas de gestão, tais como ISO 9000 e ISO 20000, novos controlos foram adicionados:

- A.12.6.2 *Restrictions on software installation*.
- A.14.2.1 *Secure development policy*.
- A.14.2.5 *Secure system engineering principles*.
- A.14.2.6 *Secure development environment*.
- A.14.2.8 *System security testing*.
- A.15.1.1 *Information security policy for supplier relationships*.
- A.15.1.3 *Information and communication technology supply chain*.
- A.16.1.4 *Assessment of and decision on information security events*.
- A.16.1.5 *Response to information security incidents*.
- A.17.2.1 *Availability of information processing facilities*.
- A.6.1.5 *Information security in project management*.

2.3.2 Information Technology Infrastructure Library

O ITIL (biblioteca estruturada de tecnologia de informação) é um conjunto de boas práticas para a gestão de serviços de tecnologia de informação, orientado para as necessidades de negócio. A versão atual do ITIL foi publicada em vários volumes e cada um retrata o ciclo de vida de um gestor de serviços de tecnologia de informação. O ITIL baseia-se na ISO/IEC 20000,

que é o padrão internacional para a gestão de serviços de tecnologia de informação, apesar das diferenças existentes entre os dois instrumentos.

O ITIL descreve processos, procedimentos e tarefas que não são específicos de uma organização, sendo usado para definir uma estratégia organizacional. A sua aplicação permite estabelecer uma linha de base para a organização, a qual pode ser planeada, implementada e medida, permitindo assim demonstrar que os objetivos foram alcançados e que as medidas implementadas geraram melhorias. (David Clifford, 2008)

A versão ITIL de 2011 divide-se em cinco publicações principais – Estratégia de serviços, Desenho de Serviços, Transição de Serviços, Operação de Serviços e Melhoramento Contínuo do Serviço. Existem 26 processos abordados na edição ITIL 2011.

2.3.3 Standard of Good Practice

A norma *Standard of Good Practice* (SGP) para a segurança de informação, publicada pelo *Information Security Forum*, centra-se sobretudo nos aspetos de negócio, sendo um guia prático e de fácil compreensão que permite analisar os problemas, facilitando a identificação e a gestão dos riscos da segurança da informação numa organização.

A última versão data de 2013 e tem o título "*The 2013 Standard of Good Practice for Information Security*", atualizando a forma de lidar com os padrões da segurança da informação, num contexto mais abrangente do que o das normas ISO. Inclui medidas de segurança da informação que têm de ser aplicadas para manter os riscos de negócio num nível aceitável. Apresenta igualmente ferramentas de segurança da informação usadas em casos reais e discutidas no *Information Security Forum* (ISF). Este fórum é uma organização não-governamental que se dedica à investigação, clarificação e resolução de problemas essenciais para a gestão da segurança da informação, propondo metodologias práticas, processos e soluções que resolvam as necessidades de cada negócio. (Forum, Information Security, 2014)

O "*The 2013 Standard of Good Practice for Information Security*" centra-se nos requisitos estabelecidos para um sistema de gestão de segurança da informação que estão especificados na norma ISO/IEC 27000. Comparando a norma ISO 27002 com o SGP 2013, esta é mais ampla e assume maior profundidade na compreensão dos tópicos de *cloud computing*, fuga de

informação, dispositivos e segurança governamental. Tendo como objetivo obter uma certificação da norma ISO 27001, o padrão SGP de 2013 sugere uma ferramenta de validação dos requisitos (Cobit, que é uma outra norma, a descrever adiante).

Estes padrões são relevantes para chefes de segurança da informação (CISO), gestores da segurança da informação, gestores de tecnologias, auditores (internos e externos) e fornecedores de serviços de tecnologia, pois são aqueles que atuam sobre o ambiente da informação e podem fazer com que a organização respeite os requisitos.

2.3.3.1 Benefícios de utilizar o *Standard of Good Practice*

A versatilidade e simplicidade deste padrão permite que seja utilizada de modos muito diversificados. Estes aplicam-se independentemente da forma como a organização definiu a sua política de segurança da informação, normas internas de funcionamento e procedimentos associados. Seja usado de forma independente ou em conjunto com outra ferramenta disponível no *Information Security Forum* (ISF) ou outra norma internacional, o SGP é uma fonte e uma referência para segurança da informação. O SGP visa:

1. Melhorar as políticas de segurança da informação, normas e procedimentos.
2. Ganhar sensibilidade para a segurança da informação na organização.
3. Medir a eficácia da segurança da informação em toda a organização.
4. Desenvolver e melhorar os controlos de segurança da informação.
5. Obedecer aos requisitos internos e externos da segurança da informação.
6. Realizar análises de risco da informação nas aplicações e nos sistemas importantes.

2.3.4 Common Criteria

Os Critérios Comuns para Avaliação da Segurança Informática, conhecido pela abreviatura de *Common Criteria*, é um padrão internacional (ISO/IEC 15408) para certificação de segurança de computadores. A versão atual é a 3.1 revisão 4. (Criteria, 2014)

O *Common Criteria* é uma *framework* que permite especificar as seguranças funcionais e os requisitos necessários para a proteção dos seus recursos. Os utilizadores podem implementar e gerir os atributos de segurança dos produtos. Estes podem ser testados, permitindo avaliar e determinar se os requisitos de segurança correspondem ao pretendido. O *Common Criteria* assegura que o processo de especificação, implementação e operação de um produto de

segurança informática foi realizado de forma rigorosa, aplicando os padrões de modo mensurável em termos do ambiente no qual vai ser usado.

O *Common Criteria* é usado para a esquematização da certificação e para avaliações tipificadas, que são conduzidas por organismos governamentais e de infraestruturas críticas.

2.3.4.1 Requisitos

O *Common Criteria* é muito genérico, não fornecendo diretamente uma lista de requisitos de segurança para aplicações ou recursos específicos. Segue a abordagem proposta pelo ITSEC, sendo debatidas outras abordagens para padrões mais antigos tais como o TCSEC e FIPS 140-2.

2.3.4.2 Valor da certificação

Uma certificação baseada no *Common Criteria* não garante a segurança das soluções, mas assegura os atributos de segurança aplicados e testados nos produtos, pois são verificados independentemente. Os produtos testados de forma rigorosa e de acordo com o padrão *Common Criteria* fornecem evidências relevantes na especificação, implementação e avaliação dos processos. Adicionalmente, o *Common Criteria* reconhece que a limitação do âmbito na avaliação dos processos é um benefício para a redução de custos e uma vantagem para a certificação da segurança.

Baseado em suposições supostamente realistas do uso de um produto, todas as funções de segurança têm de ser avaliadas. Os produtos de *software* só podem ser considerados seguros depois de uma rigorosa avaliação dos pressupostos assumidos nas circunstâncias e configuração definidas.

O valor da certificação *Common Criteria* é reconhecido internacionalmente, contudo a sua avaliação restringe-se frequentemente às funcionalidades de um produto que o "fabricante" quer ver reconhecidas, daí serem importantes as atualizações, correções e outros mecanismos de segurança para colmatar as falhas não analisadas. Assim sendo, outras certificações adicionais tornam-se relevantes.

2.3.5 Sarbanes–Oxley Act

A lei Sarbanes-Oxley de 2002, também conhecida como lei da contabilidade da função pública e proteção de investidores, é uma lei norte-americana sobre a responsabilidade e auditoria da contabilidade em organizações, vulgarmente conhecida como Sarbanes–Oxley, Sarbox or SOX,

que estabelece um novo padrão nos Estados Unidos das América. Com a aplicação da SOX, a gestão de topo tem de certificar o rigor da informação financeira. Além disso, as penalizações pela atividade financeira fraudulenta são muito severas. A SOX reforçou também o papel da supervisão da gestão de topo e tornou-a mais independente dos auditores que escrutinam a situação financeira da organização. (Kimmel, et al., 2011)

Esta lei contém onze seções que descrevem as responsabilidades criminais caso a lei não seja cumprida, para além de definir uma comissão (*Securities and Exchange Commission*, SEC) cuja função é implementar regras e requisitos na aplicação e cumprimento da lei.

2.3.6 COBIT

O *Control Objectives for Information and Related Technology* (Cobit) é um guia de boas práticas apresentado como ferramenta para a gestão de tecnologias de informação, tendo sido criada pela ISACA (*Information Systems Audit and Control Association*).

Neste guia de boas práticas é descreve-se a abordagem de diversos temas tais como *frameworks*, objetivos de controlo, mapas de auditoria, ferramentas para a sua implementação e, principalmente, um guia com técnicas de gestão. (Isaca, 2014)

O Cobit é uma plataforma passível de ser adotada numa organização, tendo em conta o tipo de negócio e o impacto da tecnologia da informação no funcionamento da mesma. A ISACA tem como objetivos a pesquisa, desenvolvimento, publicação e promoção oficial e atualizada de um conjunto de controlos/objetivos de tecnologias de informação para uso diário por gestores e profissionais de tecnologias. Este guia/ferramenta permite aos gestores diminuir os riscos de negócio, o impacto dos requisitos de controlo e as dificuldades técnicas.

A versão atualmente disponível é a versão Cobit 5. Esta define os processos de entrada e saída, processos/atividades essenciais, objetivos dos processos, execução de medidas e maturidade do modelo. As alterações face ao COBIT 4.1 passam pela associação com outros conjuntos de boas práticas e metodologias existentes, tais como os padrões ISSO e ITIL, entre outros (ITGI, 2014).

2.3.6.1 Contexto do Cobit: Necessidade nas empresas

A tecnologia da informação é um fator importante para obter sucesso na economia da informação e na gestão operacional/financeira de uma organização. Os aspetos tecnológicos e as políticas associadas a uma gestão eficaz da informação não devem mais ser considerados

irrelevantes. A gestão empresarial visa tipicamente obter os melhores resultados possíveis, para isso sendo essencial um instrumento de medição de desempenho que ofereça garantias de seriedade na avaliação e resolução de problemas críticos. As tecnologias de informação devem obedecer a normas e procedimentos decorrentes das leis aplicáveis e das adaptações aplicadas pela organização.

2.3.6.2 O Cobit como *framework*

É inegável a necessidade de uma referência para o desenvolvimento, gestão de controlos internos e níveis adequados de segurança que possa ser aplicado às tecnologias de informação. A boa aplicação destas tecnologias tornou-se vital para a estratégia e os processos de negócio das organizações. Assim sendo, as organizações que buscam o sucesso precisam de identificar e compreender os riscos e as limitações.

O foco do Cobit 5 é consolidar e integrar o Cobit 4.1, que é descrito por um modelo de processos que se subdivide em quatro domínios (Planear e Organizar, Adquirir e Implementar, Entregar e Suportar, Monitorizar e Avaliar) e 34 processos integrados nesses quatro domínios de responsabilidade. O Cobit foi alinhado e harmonizado com outros padrões ou normas tais como ITIL e ISO 27000, entre outras. O Cobit pode atuar como integrador desses instrumentos, resumindo os objetivos fundamentais no âmbito dos modelos de boas práticas de gestão e requisitos de negócios.

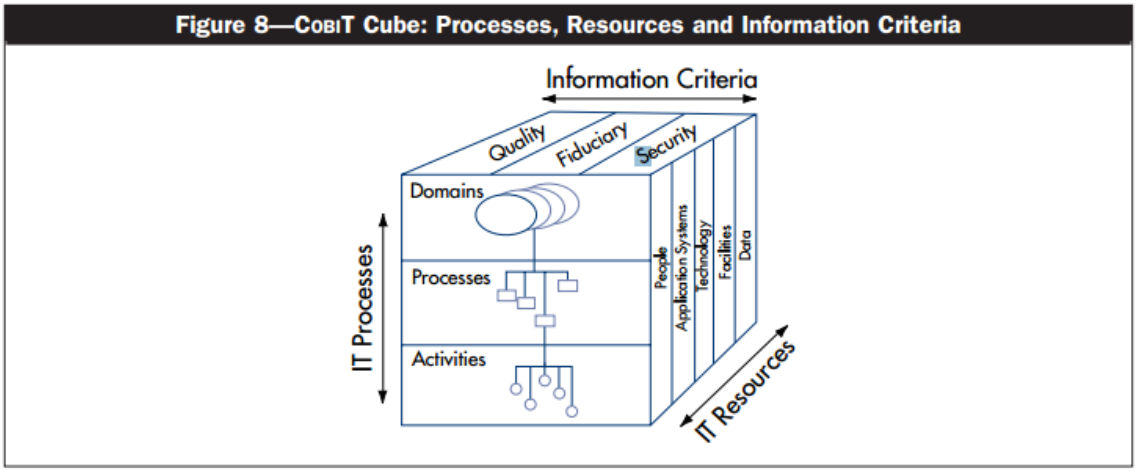
A *framework* Cobit define objetivos de controlo de alto nível e uma estrutura global para a sua classificação. A teoria subjacente para a classificação é que há, essencialmente, três níveis de esforços de tecnologia de informação em termos de gestão dos recursos. Na parte inferior há as atividades e tarefas para alcançar um resultado mensurável. As atividades implicam o conceito de ciclo de vida, ao passo que as tarefas são mais simples, não tendo obrigatoriamente um ciclo de vida. O conceito de ciclo de vida é diferente de um controlo de requisitos para uma atividade. No nível intermédio, os processos são uma camada bem definida com atividades ou tarefas ligadas com pausas, denominados controlos. No nível superior, os processos são agrupados em domínios. O seu agrupamento é muitas vezes descrito como domínios de responsabilidade numa estrutura organizacional e está em linha com o ciclo de gestão/vida aplicável. O modelo conceptual pode ser abordado a partir de três pontos de vista (Figura 6):

• Critérios de informação.

• Recursos das tecnologias de informação.

• Processos das tecnologias de informação.

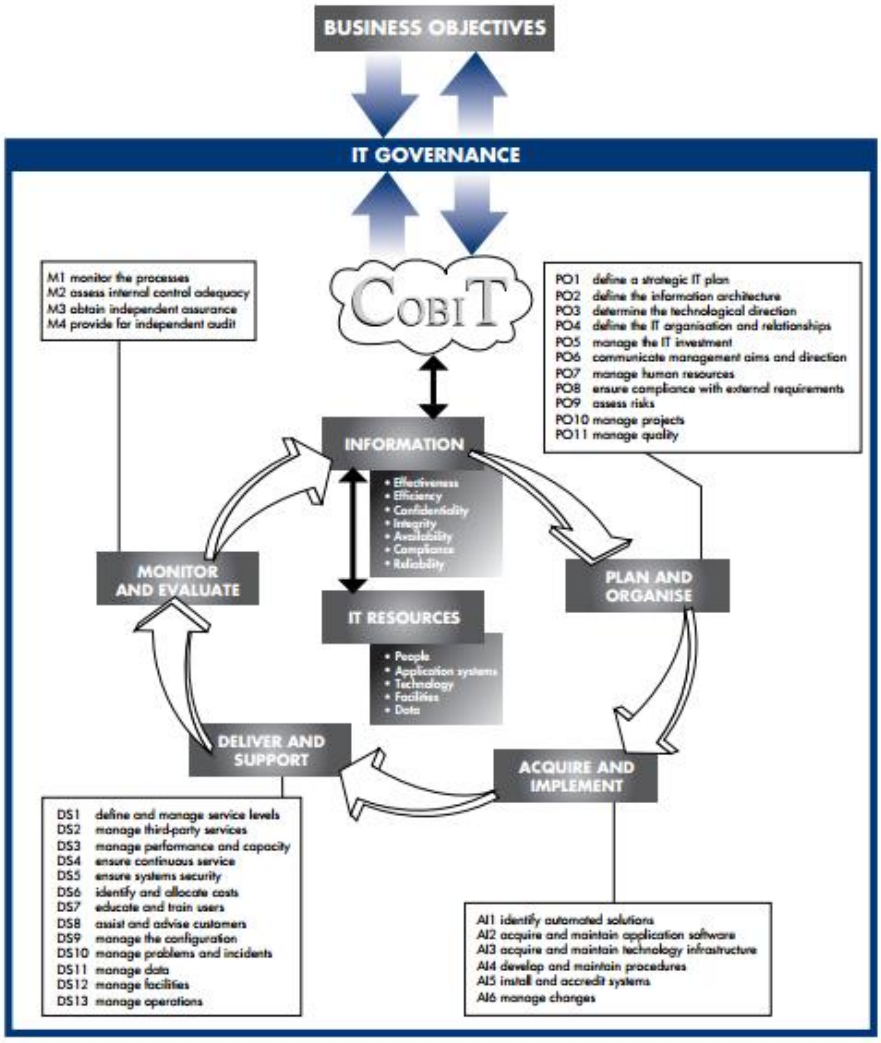
Figura 6 - O cubo do Cobit (Isaca, 2014)



Na figura anterior os domínios são identificados através de uma descrição compreensível no dia-a-dia da organização. Os quatro domínios principais identificados são: planear e organizar, adquirir e implementar, entregar e suportar, monitorizar e avaliar.

A Figura 7 ilustra o funcionamento da *framework* do Cobit.

Figura 7 - Framework do Cobit (ISACA, 2014)



2.3.6.3 Benefícios de usar o Cobit

O Cobit permite a redução da complexidade e o aumento da relação custo-eficácia devido à integração das normas de segurança da informação. Para além disto, o Cobit visa:

- Maximizar a confiança e valor da informação organizacional e tecnologia.
- Lidar com as necessidades das partes interessadas de toda a organização.
- Esclarecer objetivos para a tomada de decisão mais eficaz.
- Fornecer uma abordagem sistemática e vocabulário comum para abordar aspetos mais desafiadores no cumprimento de metas de desempenho organizacional.
- Fornecer uma estrutura completa que integra outras abordagens/normas e simplifica abordagens complexas.

- Suportar informação de qualidade no suporte das decisões de negócio.
- Alcançar objetivos estratégicos e obter benefícios através do uso eficaz das tecnologias de informação.
- Atingir a excelência operacional através da aplicação confiável e eficiente da tecnologia.
- Manter os riscos relacionados com as tecnologias de informação num nível aceitável.
- Otimizar o custo de serviços de tecnologias de informação e tecnologia.
- Respeitar o cumprimento de leis, regulamentos, acordos contratuais e políticas.

2.3.7 ISO 31000 - RISK MANAGEMENT

2.3.7.1 ISO 31000

A norma ISO 31000 foi publicada como padrão em 13 de novembro de 2009 e descreve um padrão na implementação da gestão de risco. O propósito da ISO 31000:2009 é ser aplicável e adaptável a qualquer público-alvo, isto é, ser aplicável e adaptável a todos os tipos de organização, incluindo o caso pessoal.

A ISO 31000 é uma família de padrões para gestão de risco, sendo codificada pela ISO. O propósito da norma ISO 31000:2009 é fornecer princípios e linhas de orientação para a gestão do risco. Esta norma visa fornecer um paradigma universal para as organizações que estejam interessadas em adotar a gestão do risco nos seus processos. Esta norma tem também como intuito substituir outros padrões, metodologias e paradigmas, muitas vezes específicos para os diversos setores de atividade, países, etc.

Na atualidade a família ISO 31000 inclui:

- ISO 31000:2009 - *Principles and Guidelines on Implementation*.
- ISO/IEC 31010:2009 - *Risk Management - Risk Assessment Techniques*.
- ISO Guide 73:2009 - *Risk Management – Vocabulary*.

2.3.7.2 Âmbito

A ISO 31000:2009 fornece guias de orientação genéricas para o desenho, implementação e manutenção da gestão de risco dos processos numa organização. Esta abordagem de formalizar as práticas de gestão de risco facilitou uma grande adoção pelas organizações, que

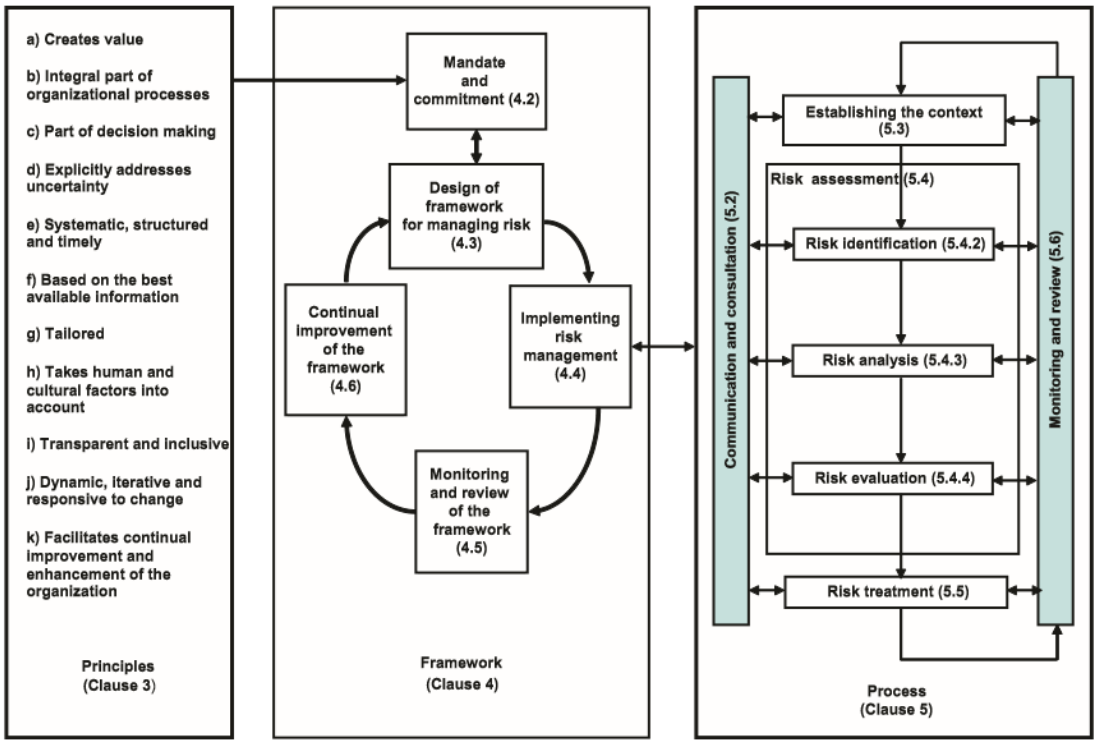
necessitavam de adotar um padrão de gestão para monitorizar os múltiplos sistemas de gestão e de informação.

O âmbito desta abordagem de gestão de risco permite que todas as tarefas de estratégia, gestão e operação de uma organização, que se baseiem em projetos, funções e processos, possam ser alinhadas em objetivos comuns para a gestão de risco (Figura 8).

A ISO 31000:2009 destina-se a um conjunto de partes interessadas tais como:

- Parte executiva da organização.
- Titulares nomeados para a gestão de risco na organização.
- Analistas de risco e agentes de gestão.
- Todo o tipo de gestores.
- Auditores internos e externos.
- Profissionais independentes.

Figura 8 - Funcionamento da norma ISO 31000 (31000, 2009)



2.3.7.3 Implementação da ISO 31000

A ISO 31000 deve ser aplicada no âmbito dos sistemas de gestão existentes para formalizar e melhorar os processos de gestão de risco, em oposição à substituição completa das práticas

de gestão. Por consequência, quando implementada, é relevante a atenção na integração de processos de gestão de risco existentes e a forma como se enquadram no paradigma do padrão.

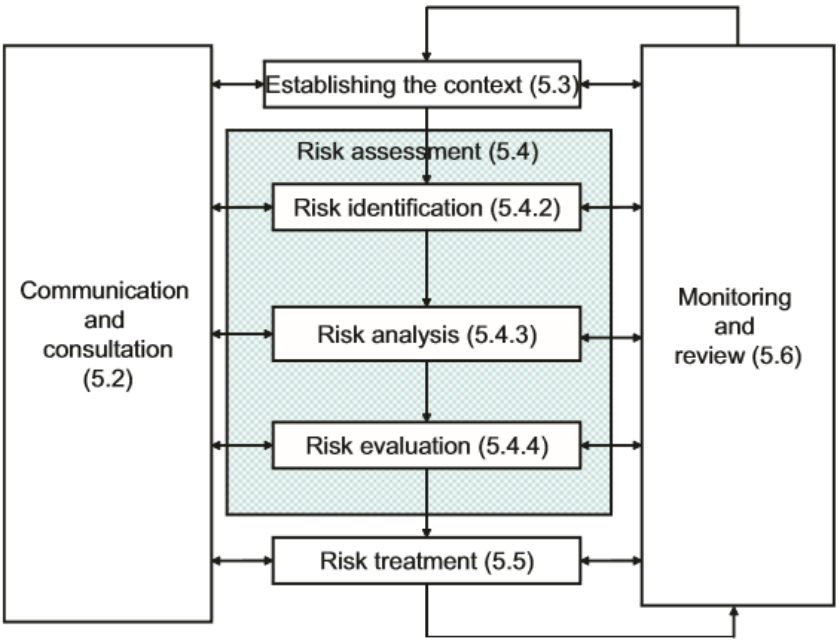
Os aspetos descritos na ISO 3100 focam-se essencialmente em:

- Transferência de falta de responsabilização na gestão de riscos da organização.
- Alinhamento dos objetivos da gestão com a norma ISO 31000.
- Incorporação de mecanismos de comunicação do sistema de gestão.
- Criação de critérios de risco uniformes e métricas de avaliação.

2.3.7.4 Implicações da norma ISO 31000

A maior parte das implicações decorrentes da adoção deste padrão têm a ver com a reengenharia das práticas de gestão existentes, por forma a obedecer à documentação, comunicação e socialização proposta por este paradigma de gestão do risco. Assim sendo, os gestores de topo e os responsáveis da gestão de risco devem consistentemente adotar, aplicar e melhorar as suas estratégias, de modo a torná-las mais eficientes e eficazes, com vista a que a implementação resulte em termos operacionais. Aspetos da responsabilidade da gestão de topo, a implementação de políticas e de ferramentas de trabalho eficazes poderão exigir maior consideração pela organização do que a anteriormente existente. Visando uma gestão de risco apropriada à organização, poderá ser necessário formalizar processos, especificar os donos dos processos, controlar os recursos manipulados, estruturar uma ferramenta de trabalho para os processos e adotar uma atitude de melhoria contínua (Figura 9).

Figura 9 - Gestão do risco (31000, 2009)



2.3.8 Análise de Risco

Os profissionais de segurança da informação têm frequentemente de avaliar riscos. A análise de risco ajuda a decidir, perante uma situação, qual é a melhor escolha. Antes de a decisão ser tomada será necessário identificar e conhecer a organização/sistema em causa, quais os seus ativos valiosos (recursos críticos, etc.), as ameaças pendentes, as probabilidades de ocorrência das ameaças, os danos causados pela ocorrência de cada ameaça, o risco gerado por cada ameaça, os critérios de risco definidos pela organização, as medidas de redução de risco e o orçamento de cada medida. Só após um exercício estruturado e sério de análise de risco, que exige uma preparação estruturada e objetiva, é se torna possível tomar decisões sobre gestão de risco.

Os ativos são recursos que se devem proteger, podendo ser informação, sistemas, pessoas, edifícios, etc. O valor ou criticidade de um ativo vai influenciar as medidas a implementar. Tipicamente as pessoas são consideradas ativos muito valiosos.

As ameaças são ocorrências prejudiciais tais como um terramoto, uma falha de energia, uma sabotagem interna, a exploração de uma falha de *software*, etc. Qualquer ameaça implica, no imediato e no futuro, um incidente com efeito negativo na organização.

Uma vulnerabilidade é uma fraqueza organizacional que permite a uma ameaça causar dano (ou seja, uma ameaça com probabilidade de ocorrência não desprezável pela organização), sendo que a maior parte das ameaças não geram vulnerabilidades.

Os termos ameaça, vulnerabilidade e risco podem ser relacionados entre si. Uma forma de quantificar o risco pode ser através da fórmula $Risco = Ameaça * Vulnerabilidade$. Na fórmula anterior "Ameaça" representa o potencial dano gerado pela ameaça e "Vulnerabilidade" tem a ver com o nível da deficiência que permite que a ameaça ocorra. Por exemplo, podem-se atribuir valores numa escala entre 1 e 5 às variáveis "Ameaça" e "Vulnerabilidade", obtendo-se um valor para o "Risco" entre 1 e 25.

2.3.8.1 Análise de Risco qualitativa

A análise de risco qualitativa consiste em classificar as componentes do risco através de escalas qualitativas do tipo "baixa, média, alta e elevada". Por vezes é difícil atribuir valores numéricos verosímeis às componentes do risco, pelo que a análise qualitativa é uma abordagem adequada para essas situações. Quando uma classificação varia numa escala qualitativa não é possível perceber exatamente de que forma é que a organização é afetada.

Criar uma escala na qual o nível mais alto representa um valor máximo e o nível mais baixo valores mínimos, juntamente com subdivisões entre esses limites, permite gerar escalas qualitativas com aplicação prática relevante.

Numa situação em que o risco é baixo esta poderá ser gerida como um processo normal. No caso de risco moderado, tal poderá obrigar a uma notificação ao responsável da segurança. Um risco elevado deverá implicar uma notificação à gestão de topo, mas no caso de risco extremo deverá ser tomada rapidamente uma medida de redução de risco, a qual deverá incluir um plano detalhado da mitigação realizada.

A Tabela 2 descreve, como mero exemplo de abordagem qualitativa, a probabilidade de algo acontecer versus a consequência que advém para o sistema (risco).

Tabela 2 - Matriz de análise de risco qualitativo

RISCO		Consequências resultantes				
		1 Insignificante	2 Menor	3 Moderado	4 Maior	5 Catastrófico
Probabilidade de ocorrer	5 Quase certo	Alta	Alta	Extrema	Extrema	Extrema
	4 Provável	Média	Alta	Alta	Extrema	Extrema
	3 Possível	Baixa	Média	Alta	Extrema	Extrema
	2 Pouco Provável	Baixa	Baixa	Média	Alta	Extrema
	1 Raro	Baixa	Baixa	Média	Alta	Alta

2.3.8.2 Análise de Risco quantitativa

Como foi referido anteriormente, o cálculo do "risco" é feito através da multiplicação do valor da "ameaça" pelo valor da "vulnerabilidade", mas tal não contempla o "impacto", que decorre da gravidade do dano causado expresso em valor monetário ou relativo. Na abordagem quantitativa podem-se atribuir valores relativos usando gamas de valores ou até valores monetários, reais ou estimados.

A Figura 10 mostra um exemplo de análise quantitativa do risco.

Figura 10 - Matriz de análise de risco quantitativo (Vortal, 2008)

Análise de riscos

Processo de Parametrização									
Activo	Valor do Activo	Ameaça	Vulnerabilidade	Probabilidade	Impacto			Risco	Ref.
					C	I	D		
Área de Desenvolvimento									
Activo 1	2	Falha no processo de parametrização causando prejuízo ao uso dos sistemas	Atraso na realização da parametrização, causando insatisfação ao cliente	2	1	1	3	3,666667	PA001
	2		Parametrização incorrecta, gerando apresentação incorrecta de informações	3	1	1	3	4,666667	PA002
	2		Comprometimento da confidencialidade de informações, através da inclusão de informações no site, devido a ausência da identificação de sua classificação de	2	3	1	1	3,666667	PA003
Activo 2	3	Mau funcionamento dos serviços por parametrização errada	Ausência de processo de identificação dos controlos de segurança na fase de planeamento das mudanças nos sistemas	3	3	3	3	9	PA004
	3		Falha na aplicação de segurança, devido a falta de conhecimento dos parametrizadores	1	3	3	3	6	PA005
	3		Processo de gestão de mudança inadequado para considerar segurança	3	3	3	3	9	PA006
	3		Ausência de aprovação formal sobre as mudanças realizadas	1	2	2	2	4,5	PA007
	3		Ausência de processo de auditoria sobre mudanças implementadas	3	2	2	2	7,5	PA008
	3		Parametrização manual de dados em	3	3	3	3	9	PA009

Na figura acima, a parte do "impacto" está subdividida em 3 campos, C-I-D, que representam a confidencialidade, a integridade e a disponibilidade. No cálculo do risco, a fórmula adotada foi $R = ((C + I + D)/3 + P)/2 * V$, sendo R o "risco", C a confidencialidade, I a integridade, D a disponibilidade, P a probabilidade de ocorrer e V o valor do ativo. Esta fórmula corresponde a um caso prático de um ativo real.

2.4 Visão da solução

Com a realização desta tese pretende-se que os processos da instituição evoluam e que se reforcem as boas práticas de gestão da segurança da informação.

No final espera-se que os processos do sistema de informação indicados pela Presidência do ISEP sejam melhorados através da aplicação de uma metodologia baseada em normas e boas práticas internacionais, o que poderá implicar a revisão dos processos existentes, levando à

criação de documentos de trabalho ainda inexistentes ou à adaptação dos existentes. Exemplos de documentos e atividades relevantes para a gestão da segurança da informação são: folhas de inventário de processo, lista de recursos de processo, critérios de risco por processo, exercício de análise de risco por processo, definição de papéis e responsabilidades dos atores dos processos, etc., culminando em documentos organizacionais de topo tais como política de segurança da instituição, declaração de aplicabilidade, entre outros.

3 Ambiente de trabalho

3.1 Metodologia de trabalho

No decorrer de uma auditoria realizada pela AENOR em 2013, foi recomendada como melhoria a realização, no ISEP, de um exercício estruturado de análise de risco baseado na norma ISO 27001. Esta proposta de melhoria tinha como objetivo geral a verificação e melhoria dos processos e atividades no ISEP. Após a Presidência do ISEP ter autorizado que o referido exercício fosse realizado no âmbito de uma tese de mestrado no ISEP e indicado o Vice-Presidente José Oliveira como contacto oficial do ISEP, foi iniciado o trabalho que se descreve nesta tese.

No início pesquisou-se e recolheu-se material relacionado com a análise de risco, segurança da informação e problemas afins, com vista definir-se um planeamento para estruturar a realização das diversas tarefas. Tratando-se de uma área abrangente e com vários caminhos para a solução, foi considerado como relevante o recurso a um auditor/consultor com provas dadas em segurança de informação, tendo a escolha recaído no Eng.º Paulo Borges, da empresa SECURTI, que gentilmente aceitou o convite para ser consultor no âmbito desta tese.

Assumindo-se o uso da norma ISO 27001, na primeira reunião com o consultor foi criado um guião de trabalho, dividido em seis fases, que especificou, para cada uma das fases, o que deveria ser feito e qual o resultado de cada fase.

As fases definidas no documento guião de trabalho são obrigatórias e sequenciais, dado que cada fase depende da anterior. Uma alteração significativa numa das fases tem impactos nas fases seguintes, mas também poderá ter impactos em fase anteriores.

Todos os passos deste guião implicam a produção de pelo menos um documento por fase, documentos esses suportados por ferramentas digitais do tipo “escritório” (processadores de texto, folhas de cálculo, etc.). Em cada documento descreve-se o que foi realizado, em alguns casos reaproveitando documentos anteriores como ponto de partida, essencialmente acrescentando-se nova informação ou detalhe.

3.2 Planeamento de trabalho

Após a definição do documento guião de trabalho, o planeamento das atividades ficou estabelecido. Apesar da inexperiência das pessoas envolvidas, com exceção do consultor

Paulo Borges, seguidamente estabeleceram-se objetivos e requisitos por fase, de modo a serem tratados nas sucessivas reuniões.

A primeira fase consistiu em fazer o levantamento de documentos oficiais e públicos da instituição, seguida da análise desses documentos.

A segunda fase centrou-se em obter e analisar processos do ISEP relacionados com o ensino. Depois de uma reunião com o Vice-Presidente José Oliveira, ficou decidido que a análise de risco seria apenas aplicada ao "processo de notas", recolhendo-se em seguida a documentação relativa a esse processo. As fases 1 e 2 ocuparam cerca de 3 meses.

A terceira fase consistiu em elaborar a tabela do processo de notas previamente aprovado, o que obrigou várias iterações entre os intervenientes, incluído o consultor e representante do ISEP. Na sequência analisou-se o fluxograma do processo de notas, da qual resultou uma proposta de alteração desse processo, decorrente da aplicação das boas práticas da ISO 27001 e da identificação de aspetos críticos no processo. A proposta de alteração do fluxograma do processo de notas foi seguidamente aprovada pelo Vice-Presidente José Oliveira, sendo dada indicação de implementação para aplicação futura.

Na quarta fase, obtido o consenso sobre a tabela do processo de notas (e documentos associados), passou-se à inventariação dos recursos de informação implicados no processo de notas. As fases 3 e 4 demoraram 4 meses.

Por fim, na quinta fase foi realizada uma análise de risco por recurso identificado, incluindo a definição dos critérios de risco na perspetiva do ISEP, e foi elaborada uma declaração de aplicabilidade para o ISEP. Esta fase durou 2 meses.

A tabela seguinte resume as fases descritas.

Tabela 3 - Planeamento do trabalho

Descrição	Fase	Duração
Levantamento e análise de documentos oficiais e documentação de ensino	1	15 Dias
Análise do fluxograma e respetiva documentação associada	2	15 Dias
Criação do novo fluxograma e análise da documentação, com criação da tabela de processos	2	2 Meses
Alterações ao fluxograma e aprovação pela Presidência do ISEP, revisão da tabela de recursos	3	1 Mês
Ajustes finais ao fluxograma do processo de notas e alterações à tabela de processos	3	2 Meses
Inventariação de recursos	4	1 Mês
Análise de risco por recurso, definição de causas de falhas, identificação de controlos aplicáveis e criação da matriz de critérios de riscos (aprovada pela Presidência do ISEP)	5	2 Meses

3.3 Tecnologias usadas

As tecnologias usadas na realização deste trabalho foram essencialmente ferramentas convencionais de escritório. Sendo o trabalho essencialmente não tecnológico mas sobretudo organizacional, as ferramentas usadas não assumem importância nesta tese.

Foram identificados alguns documentos tipo modelo (acessíveis *online*), previamente formatados e preparados para serem usados imediatamente, que foram considerados durante as fases iniciais, mas posteriormente foram descartados e usados apenas documentos criados pelo autor desta tese.

A @sec disponibiliza um documento de acesso livre que descreve como implementar um sistema de gestão de segurança da informação, o qual serviu de guia nas diversas etapas deste trabalho. (atsec, s.d.)

Para introdução ao tema da segurança da informação foi consultada *online* uma publicação do CISSP. (Conrad, et al., 2010)

Toda a informação referente aos documentos do ISEP foi retirada do *website* oficial, área de documentos públicos. (ISEP, 2014)

4 Descrição técnica

4.1 Análise do problema

Nesta tese foram definidas à partida requisitos de segurança da informação para os seus intervenientes, com ênfase para a confidencialidade da informação a ser usada durante a fase de projeto. A todos foi solicitado, de modo informal e no âmbito de reunião, que respeitassem os aspetos de confidencialidade relacionados com a expetativa de segredo sobre processos, recursos, tecnologias, etc., usados no ISEP. Estes compromissos implicaram, para as pessoas envolvidas, que o tema desta tese e assuntos relacionados não devessem ser discutidos com terceiros.

A primeira fase do projeto, após a aprovação formal da gestão de topo, consistiu em fazer o levantamento da informação disponível, traçar objetivos de segurança, definir papéis de segurança com funções documentadas e disponibilizar recursos para este trabalho.

A divulgação, comunicação e sensibilização para uma política de segurança é essencial para a adesão de todos os intervenientes na organização. No âmbito do projeto considerou-se mais adequado adotar uma postura positiva, ou seja, explicar porque é que a informação deve ser tratada de uma certa forma e o porquê de medidas de segurança para acesso à informação, ao invés de impor uma "ditadura" de segurança da informação. O ISEP pretende que todos os constituintes da organização saibam tratar da segurança da informação, no contexto de uma abordagem positiva à segurança da informação. Um aspeto importante relacionado com a segurança da informação tem a ver com a disponibilização de recursos tecnológicos, devendo ser assegurado que existem os recursos necessários e a disponibilidade de acesso aos mesmos para que o trabalho seja realizado. Sem acesso adequado e atempado à informação, a segurança da informação é posta em causa. Outro aspeto a ter em conta passa pela documentação apropriada dos processos de trabalho que envolvem recursos com requisitos de segurança da informação. Sem uma boa documentação podem surgir práticas incorretas capazes de afetar a segurança da informação, eventualmente prejudicando o funcionamento do sistema de informação.

Numa segunda fase especificou-se o âmbito do sistema de gestão da segurança da informação (ISMS). Durante a definição dos processos a analisar será estabelecido o âmbito e contexto do ISMS. Com os processos definidos torna-se possível perceber cada fluxo de trabalho, que é

específico para cada processo e essencialmente constituído por atividades com responsáveis associados. Caso não existam responsáveis em algumas atividades, isso pode constituir um problema de segurança de informação.

Para definir o âmbito do ISMS é igualmente necessário uma lista de espaços, localizações de recursos e tecnologias, assim como os próprios recursos e tecnologias.

Após a produção desta documentação, inicia-se o estudo dos processos, com base em matrizes de informação que captam as interações entre os conceitos, define-se o contexto organizacional e a estratégia a seguir e, por fim, um compromisso de implementação. Os documentos com processos e atividades serão o alvo e mais-valia desta análise. Os documentos referidos (matrizes, tabelas, etc.) serão construídos e alterados à medida que se avance para as fases seguintes do projeto. Esta abordagem iterativa e incremental é muito importante na análise dos processos. Como resultados deverão ser produzidos um documento de âmbito do ISMS e um guião de atividades a desenvolver para implementar o ISMS.

Terminada a segunda fase, passa-se para a definição da orgânica. Nesta fase têm-se em conta a estrutura e as responsabilidades dos agentes da organização. É essencial analisar todos os cargos e responsabilidades para os processos em causa, desde o gestor de topo até ao operacional que lida diariamente com o ISMS. É nesta fase que se atribuem responsáveis e responsabilidades aos processos. É importante que os donos dos processos sejam definidos tendo em conta os requisitos dos seus processos e atividades, bem como as suas funções e responsabilidades globais na organização.

Na terceira fase define-se o responsável pelo ISMS, apelidado de CISO (*Chief Information Security Officer*). A definição da orgânica deverá permitir uma visão clara dos papéis e responsabilidades com vista a evitar acumulações de funções, mas é aceitável que um gestor de topo possa exercer o cargo de CISO. Estando o CISO definido, deverá ser criado um fórum de segurança, órgão coletivo que inclui as entidades que gerem recursos com impactos relevantes na segurança da informação (essencialmente donos de processos), visando ajudar o CISO na tomada de decisões, das quais ele será o único responsável. Espera-se que o CISO seja capaz de promover discussões construtivas e consensos, mas a decisão final será sempre pessoal. O CISO é responsável por controlar, verificar e melhorar o ISMS ao longo do tempo.

O fórum de segurança deverá funcionar de modo a promover a discussão, devendo ser apresentados problemas a resolver, nos quais os intervenientes opinam e trabalham com

vista à melhoria da organização. Apesar do CISO decidir em nome do fórum de segurança, a organização delega neste fórum, através dos seus representantes, o objetivo de manter e melhorar constantemente o ISMS.

No fim desta fase não podem existir processos e atividades sem dono. Caso existam, é necessário reformular todo o trabalho efetuado com vista a preencherem-se os donos em falta nos processos. Com todos os donos de processos em funções, deverão ser finalizadas todas as tabelas, fluxogramas e demais documentos, de modo passar-se à fase seguinte.

Na quarta fase são inventariados todos os recursos de informação. Deverá ser aproveitado o material produzido na fase dois, durante a qual foram levantadas as atividades e os processos definidos, e adicionarem-se outros aspetos de segurança tais como as vulnerabilidades, por exemplo. Toda a informação produzida na fase dois deverá ser escrutinada, reanalisada e adaptada ao novo contexto. O resultado obtido deverá será mais condizente com a realidade operacional dos processos. Tendo então por base este resultado, será necessário designar os requisitos de segurança, para isso atribuindo a cada um identificador único, de modo a ter em conta os recursos usados por processo, atividade e na aplicação de controlos de segurança.

É com a aplicação de um ou mais controlos que entra a norma ISO 27001, a qual tem, no seu anexo A, descrições de controlos de segurança para vários tipos de aplicações organizacionais. Os controlos são genéricos, podendo ser adaptados a diversos casos. Para cada situação descrita na norma existe um controlo associado, no qual se descreve como tratar o problema e quais as medidas aplicáveis. Estas medidas de segurança servem para “controlar” uma situação, assim evitando um risco não controlado.

Por vezes poderá acontecer a gestão de topo não dispor de recursos operacionais ou humanos para controlar uma situação detetada num processo, ou inclusive ser gerida por terceiros. Nestes casos não se aplica um controlo, assim gerando um risco residual, o qual tipicamente é tratado como risco não controlável. Ao contrário do risco ao qual se aplica um controlo e, desse modo, está em verificação constante, o risco residual fica num estado adormecido, podendo manifestar-se ou não a qualquer momento. Caso não se apliquem medidas de segurança para proteger um recurso de informação, corre-se o risco de ele ser comprometido, embora isso possa nunca acontecer. Em alguns casos o controlo pode estar associado a medidas de segurança geridas por terceiros (por exemplo, uma empresa de

segurança). Nestas situações é necessário à gestão de topo assegurar previamente requisitos de segurança na empresa e verificar que ela os cumpre.

Depois de efetuada esta análise aos controlos, é necessária uma declaração de aplicabilidade na qual se explicita, para cada recurso, se são ou não aplicados controlos e sua justificação em caso negativo. Neste momento deverá haver uma reunião com a gestão de topo para discutir os controlos e elaborar o documento. É a gestão de topo que decide quais os controlos que serão implementados ou não. Cabe ao CISO verificar e analisar possíveis problemas com a aplicação ou não dos controlos, contudo é a gestão de topo que toma a decisão final. Com isto termina a quinta fase do projeto.

Na fase seis do projeto decorre a análise de riscos propriamente dita. É nesta fase que são avaliados os riscos, quantificado os impactos e analisados possíveis ataques, mitigações e medidas a tomar para cada atividade. Com base nas tabelas anteriormente referidas, para cada recurso é necessário avaliar o risco e quantificá-lo, tendo em conta os ataques possíveis. Esta análise pode ser quantitativa ou qualitativa, dependendo do tipo de recurso ou da facilidade da avaliação. Nesta fase a análise deve ser coerente e consistente, optando-se por um dos tipos de análise de risco. Na análise quantitativa de risco estas atividades não deverão ser descuidadas ou usarem-se valores inverosímeis, senão os resultados serão incorretos, podendo criar uma falsa perceção de segurança. No caso da análise qualitativa, a análise tenderá a ser mais simples e com menos probabilidade de erro, dado que se lida com valores categóricos.

Finalizando, o projeto foi dividido em seis grandes fases de atuação, que podem designadas como “suporte da gestão”, “definição do âmbito”, “definição da orgânica”, “inventário de recursos de informação”, “definição de controlos” e “declaração de aplicabilidade e gestão”. Cada uma destas categorias contribui para a solução, que é obtida de modo iterativo e incremental, em que grande parte do trabalho realizado é revisto, completado ou modificado até à fase final. Durante todas as fases é importante manter contacto com a gestão de topo, a qual deverá organizar, clarificar e explicar como se realizam os processos e se os fluxos de trabalho elaborados estão corretos. Ter apenas uma noção do como se faz insuficiente, é necessário compromissos de todas as partes, trabalho de campo e evidências documentais fortes.

4.2 Desenvolvimento da solução

Como foi referido no capítulo anterior, a realização deste exercício estrutura-se em seis grandes fases. Cada uma tem impacto organizacional nos processos da instituição.

Para o desenvolvimento da solução é necessário estudar o funcionamento da organização, como se organiza (responsáveis e responsabilidades), processos, atividades, políticas de segurança, entre outros. Numa primeira fase e depois de reunir conhecimento sobre a organização, inicia-se o primeiro grande tema de trabalho, denominado suporte de gestão. Para que este exercício se iniciasse necessitou-se da autorização da gestão de topo, neste caso a Presidência do ISEP, que deu autorização e assegurou os recursos necessários.

No suporte de gestão é feito o levantamento dos papéis e responsabilidades dos atores mais importantes na organização. É no documento denominado "Estatutos do ISEP" que se podem encontrar informações referentes às responsabilidades dos atores do ISEP. Após esta análise, passa-se para a documentação de funcionamento dos processos. É através destes documentos que será feita a comparação entre a realidade e o desejado, podendo haver diferenças significativas. Após a análise, faz-se um levantamento da existência ou não da política de segurança. No caso do ISEP foi criada uma versão inicial da política de segurança, na qual a instituição assegura que os pontos descritos são cumpridos.

Saber se a instituição possui um mecanismo de divulgação e sensibilização sobre segurança é importante, pois sensibilizando os colaboradores e outros consegue-se que o sistema de gestão da segurança da informação possa melhorar. Os documentos que foram analisados encontram-se no *website* oficial do ISEP (ISEP, 2014). Somente os documentos criados ou melhorados neste projeto constam dos anexos desta tese.

Deste modo conclui-se a fase de análise organizacional do ISEP, da qual resultou uma política de segurança, papéis e responsabilidades dos atores mais importantes e uma breve análise dos processos da instituição.

Avança-se então para a segunda fase, designada definição do âmbito do ISMS. Nesta fase serão tratadas as questões da definição do âmbito dos processos, responsabilidades dos atores, impacto na organização, caracterização dos processos e suas atividades, e o contexto organizacional.

Em termos de definição do âmbito, inicialmente o exercício focou-se no processo de ensino, tendo em vista quatro processos internos: processo de inscrição, processo de avaliação, processo de anulação da inscrição no ano curricular e processo de aprovação da ficha de unidade curricular.

Para cada um destes processos foi elaborado um documento no qual foram descritas as suas atividades, requisitos de segurança, responsabilidade da atividade e possíveis erros. Dado que o ISEP não forneceu fluxos de trabalho para os processos descritos, estes foram elaborados neste trabalho. A descrição de atividades e fluxos de trabalhos foi retirada da análise dos normativos referentes à atividade de ensino.

No âmbito de uma reunião para avaliação e aprovação do trabalho realizado, a Presidência do ISEP solicitou que o trabalho se focasse apenas no que decorre desde a abertura de um ano letivo até ao lançamento de notas no final desse ano letivo, que será em diante designado por "processo de notas". Uma vez que parte da análise e requisitos já tinha sido feita, optou-se por refazer tudo no contexto do "processo de notas". Os documentos desta fase podem ser vistos em anexo. Outro resultado importante da reunião foi a decisão da Presidência do ISEP de designar como CISO o Vice-Presidente José Oliveira.

Na fase seguinte trata-se da definição da orgânica, na qual é definido um responsável (o CISO), quem são os donos dos processos e atividades, os seus papéis e responsabilidades. Quanto ao CISO o assunto já estava resolvido. Relativamente aos papéis e responsabilidades de cada processo e atividade, a informação relevante foi guardada num documento tipo folha de cálculo para cada um dos processos analisados.

Em mais uma reunião é debatida a análise efetuada, o fluxo de trabalho e aspetos relevantes para o futuro. Após a aprovação dos documentos passa-se então para a quarta fase, na qual se trata do inventário de recursos de informação. Com a documentação existente sobre o fluxograma do "processo de notas" e as atividades, requisitos de segurança e outros, passa-se para a análise ao nível dos recursos usados em cada atividade. Para cada atividade é imperativo identificar os recursos associados, assim os fluxos de entrada e saída. Os fluxos de entrada e saída podem ser recursos de uma atividade ou então mensagens informativas, alertas, etc. Os fluxos de entrada podem vir de outros processos ou de diferentes atividades. Tendo sido identificados todos os fluxos e respetivos recursos no contexto do fluxograma, segue-se então para os controlos aplicáveis ou risco residual. Trata-se dos controlos da norma

ISO 27001 (controlos de segurança da informação) e a sua aplicação aos recursos identificados. Em ISO 27001 são implementados controlos em função dos recursos, os quais podem ser pessoas, entidades externas, cargos da organização, aplicações de *software*, sistemas, etc.

A norma ISO 27001 define categorias de controlos e a sua aplicação pode depender da sensibilidade de quem faz a análise. É importante que o controlo seja devidamente aplicado ao recurso, o que implica que o recurso seja gerido, esteja em constante revisão e melhoria, bem como monitorizado regularmente. Para que isto funcione devidamente é necessário que a organiza disponha de fundos. Em algumas situações a organização poderá subcontratar empresas externas para gerir os controlos, mas no caso deste exercício o ISEP descartou essa solução.

Em seguida passa-se para a sexta fase, na qual se trata da gestão de risco. Nesta fase deverá ser escolhida a abordagem de avaliação de risco: qualitativa ou quantitativa. No caso deste exercício optou-se pela análise qualitativa devido a motivos de tipo organizacional, dificuldade na avaliação dos recursos e simplicidade de aplicação dos métodos. Em anexo encontra-se uma tabela de critérios de risco, na qual se atribuem cores para cada nível de risco. Na avaliação qualitativa o valor do "risco" obtêm-se a partir do $valor\ do\ impacto * probabilidade\ de\ acontecer$. Estes valores são obtidos através de pelo menos duas análises: da pessoa que avalia o ISMS e da gestão de topo. No entanto, a análise pode ser alargada a entidades idóneas e que usem o sistema, esperando-se com isso obter um valor mais fiável do "risco".

Após terem sido executadas as várias etapas, é necessário reunir com a gestão de topo de modo a apresentar os resultados e a verificar a possibilidade de aplicação dos controlos. Nesta fase é produzido um documento que explica a implementação dos controlos, devendo justificar-se todos os casos de não aplicação de controlos (risco residual) Todas as decisões deverão ser passadas a escrito, de modo a ficarem devidamente documentadas.

4.3 Interação com a organização

Conforme explicado no capítulo anterior, a realização deste trabalho necessita de conhecimento sobre o funcionamento e a organização do ISEP. Para tal é necessário algum trabalho de campo, não bastando apenas analisar os documentos disponíveis.

Durante a realização deste exercício foi necessário trocar informações de modo formal e informal. À medida que se analisaram os fluxos de trabalho, processos, recursos e demais informação necessária para a produção de documentos, foi necessário dialogar com várias entidades.

No entanto, a necessidade de aprovação, deliberação e modificação do trabalho implica a reunião formal. As várias reuniões serviram essencialmente para apresentação do trabalho realizado, até ao momento, à gestão de topo do ISEP. Nestas reuniões foi discutido e criticado todo o material de trabalho. Em algumas reuniões o trabalho foi orientado para o rumo que a gestão de topo achou mais apropriado. Todos os documentos sob a forma de diagramas, folhas de cálculo e textos foram analisados pela gestão de topo (via CISO) e sujeitos a aprovação. Só houve autorização para avançar quando os documentos estavam alinhados com a situação da organização, caso contrário, era necessário alterar e sujeitá-los a nova aprovação.

5 Conclusões

5.1 Resumo do relatório

A aplicação de uma norma do tipo ISO 27001 traz melhorias para a organização na qual é implementada, neste caso a um sistema de gestão da segurança de informação. Para que seja realmente efetiva, quatro pontos são essenciais na sua aplicação. Planeamento, ação, verificação e revisão. Um ISMS dinâmico está em constante evolução, análise e melhoria, e para que isso seja uma realidade, todas as entidades da organização são chamadas a intervir ativamente.

Neste trabalho foi analisada uma parte do processo de ensino do ISEP e do qual depende o seu bom funcionamento através do "processo de notas". Com o desenvolvimento efetuado é possível afirmar que houve melhorias, quer na forma de um fluxo de trabalho, quer na componente estrutural e organizacional do mesmo. Com esta análise foi possível estruturar de forma consistente um dos processos importantes do ISEP. Focalizando no trabalho realizado, a análise e produção de documentos (em anexos) permitiu perceber como funciona o "processo de notas", uma vez que à data de início do trabalho não existia documentação atualizada. Haver documentos que expliquem os diferentes processos, recursos, responsáveis, papéis e as suas funções é imprescindível para o correto funcionamento de uma organização.

A norma ISO 27001 aplicada ao ISEP vai gerar diversas valências. A nível interno, todos os seus colaboradores poderão ser mais bem-sucedidos, uma vez que os seus papéis e responsabilidades estarão bem definidos, assim como os recursos associados e a sua gestão de risco. Em termos externos também trará mais-valias, sobretudo em termos de reputação devido à aplicação da norma.

Todo o trabalho realizado permitiu que o ISEP fosse testado em termos de segurança de informação num processo, o qual foi analisado e melhorado. Pode-se dizer que com este trabalho houve melhorias e alterações positivas em termos de ISMS. Os principais documentos produzidos deverão servir de ponto de partida e exemplo para trabalho futuro.

5.2 Objetivos realizados

Os objetivos realizados neste trabalho foram:

1. Análise dos papéis e responsabilidades dos diferentes atores.

2. Análise do fluxo de trabalho do processo de ensino disponibilizado pelo ISEP.
3. Elaboração da política de segurança.
4. Definição de processos e atividades (caraterização e requisitos de segurança).
5. Definição da orgânica.
6. Inventário de recursos.
7. Análise e gestão do risco.
8. Declaração de aplicabilidade.

5.3 Outros trabalhos realizados

Neste projeto foi o inicialmente proposto foi realizar o exercício estruturado aplicando a norma ISO 27001, contudo isso não fazia sentido e ficaria muito incompleto sem uma análise de risco associada a cada recurso. Para tal estudou-se a norma ISO 31000 e de que modo pode ser aplicada à gestão de risco dos recursos.

5.4 Limitações e trabalho futuro

As limitações deste trabalho prendem-se com o nível de detalhe apresentado. Poderia haver maior detalhe na análise, contudo não seria adequado para o exercício em questão, tornando-o muito pesado e com pouco interesse prático.

O trabalho futuro prende-se com a implementação e divulgação das práticas de segurança associadas a este exercício, assim como a extensão a outros processos, culminando eventualmente, a médio prazo, na acreditação do sistema de informação do ISEP pela norma ISO 27001.

6 Bibliografia

(UK), O. o. G. C., 2005. [Online]
Available at: http://www.ogc.gov.uk/index.asp?id=1878
[Acedido em 3 6 2014].

31000, I., 2009. s.l.: s.n.

Anon., 2007. Five years of Sarbanes–Oxley. *The Economist,* Issue Five years of Sarbanes–Oxley.

Anon., 2010. *FEI 2007 Survey of SOX 404 Costs.* [Online]
Available at: Fei.mediaroom.com

Anon., 2010. *NPR-Supreme Court Considers Sarbanes-Oxley Board.* [Online]
Available at: Npr.org

Anon., 2010. *The Effect of Corporate Governance Regulation on Transparency: Evidence from the Sarbanes-Oxley Act of 2002.* [Online]
Available at: Papers.ssrn.com

Anon., 2011. *Common Criteria Reforms: Better Security Products Through Increased Cooperation with Industry.* [Online]
Available at: http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf
[Acedido em 25 3 2014].

Anon., 2014. *Infosec Assurance and Certification Services (IACS).* [Online]
Available at: http://www.cesg.gov.uk/

Anon., 2014. *CAPS: CESG Assisted Products Scheme.* [Online]
Available at: http://www.cesg.gov.uk
[Acedido em 16 4 2014].

Anon., 2014. *Common Criteira.* [Online]
Available at: http://www.commoncriteriaportal.org/cc/
[Acedido em 24 3 2014].

Anon., 2014. *PCI Security Standards Council.* [Online]
Available at: https://www.pcisecuritystandards.org/security_standards/

Anon., 2014. *Sarbanes–Oxley Act.* [Online]
Available at: http://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

@sec, s.d. *ISMS.* [Online]
Available at: http://www.atsec.com/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf

Butler, H. N., 2010. *The Sarbanes–Oxley Debacle.* [Online]
Available at: Aei.org

Cannon, F. D., 2011. *ITIL Service Strategy 2011 Edition.* s.l.:The Stationery Office.

Conrad, E., Misenar, S. & Feldman, J., 2010. *CISSP Study Guide.* s.l.:Library of Congress Cataloging-in-Publication Data, British Library Cataloguing-in-Publication Data.

David Clifford, J. v. B., 2008. *Implementing ISO/IEC 20000 Certification: The Roadmap. ITSM Library.* s.l.:Van Haren Publishing.

Farrell, G., 2005. America Robbed Blind. *Wizard Academy Press,* Issue America Robbed Blind.

Forum, Information Security, 2014. *Information Security Forum.* [Online]
Available at: https://www.securityforum.org/membership/

Hollis Ashbaugh-Skaife, D. W. C. R. K. J. ,. L., 28. *The Effect of Internal Control Deficiencies on Firm Risk and Cost of Capital.* [Online]
Available at:
http://web.archive.org/web/20070809115641/http://www.wbur.org/news/local/icd/icd.pdf
[Acedido em 4 3 2014].

Hunnebeck, L., 2011. *ITIL Service Design.* s.l.:The Stationery Office.

Isaca, 2014. *Isaca.* [Online]
Available at: http://www.isaca.org/cobit/Documents/COBIT-5-Introduction.pdf

ISEP, 2014. *Isep.* [Online]
Available at: www.isep.ipp.pt

ITGI, 2014. *COBIT 4.1 Executive Summary.* [Online]
Available at: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Kimmel, P. C. P. D., Weygandt, P. C. J. J. & Kieso, P. C. D. E., 2011. *Financial Accounting, 6th Edition.* Wiley ed. s.l.:s.n.

Lloyd, V., 2011. *ITIL Continual Service Improvement.* s.l.:The Stationery Office.

PCAOB, 2008. *PCAOB.* [Online]
Available at: http://pcaobus.org/News/Releases/Pages/08222008_PCAOBStatement.aspx

Post, W., 2010. Post Store. *Washington Post.*

Rance, S., 2011. *ITIL Service Transition.* s.l.:The Stationery Office.

Rapp, G., 2014. *Opinion analysis: Coverage of SOX whistleblower protection is no longer Up in the Air.* [Online]
Available at: http://www.scotusblog.com/2014/03/opinion-analysis-coverage-of-sox-whistleblower-protection-is-no-longer-up-in-the-aira/

Shakespeare, C., 2008. Sarbanes–Oxley Act of 2002 Five Years On: What Have We Learned?. *Journal of Business & Technology Law: 333,* Issue Sarbanes–Oxley Act of 2002 Five Years On: What Have We Learned?.

Standard of Good Practice, s.d. [Online]
Available at: https://www.securityforum.org/userfiles/public/SOGP.pdf
[Acedido em 26 3 2014].

Steinberg, R. A., 2011. *ITIL Service Operation.* s.l.:The Stationery Office.

Study, F. &. L. 2., 2010. *Foley.com.* [Online]
Available at: Foley.com

ANEXOS

7 ANEXO A. Diagramas e tabelas associadas ao trabalho realizado

Figura 11 - Processo de inscrição versão 1

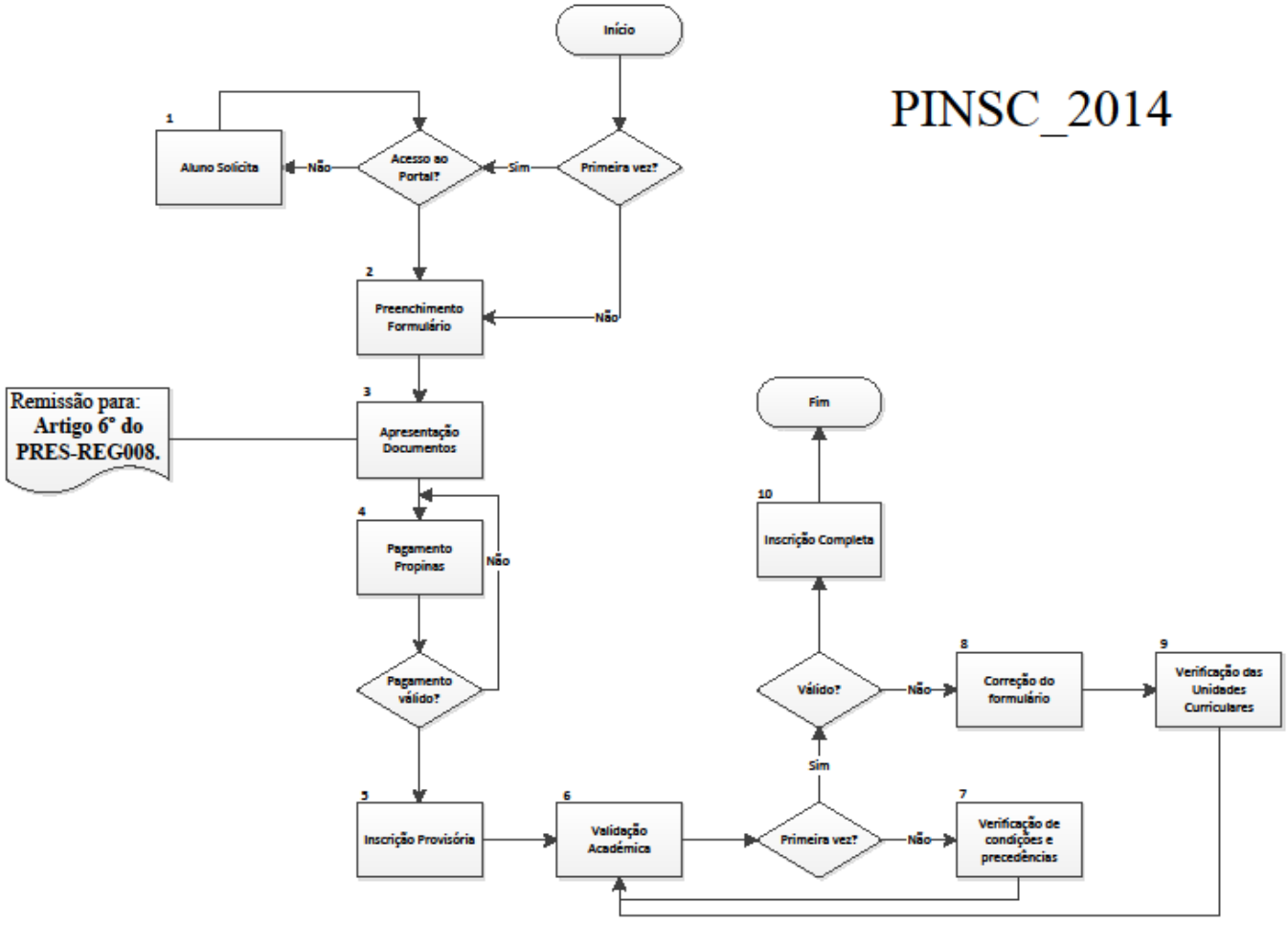


Figura 12 - Processo de inscrição versão 2

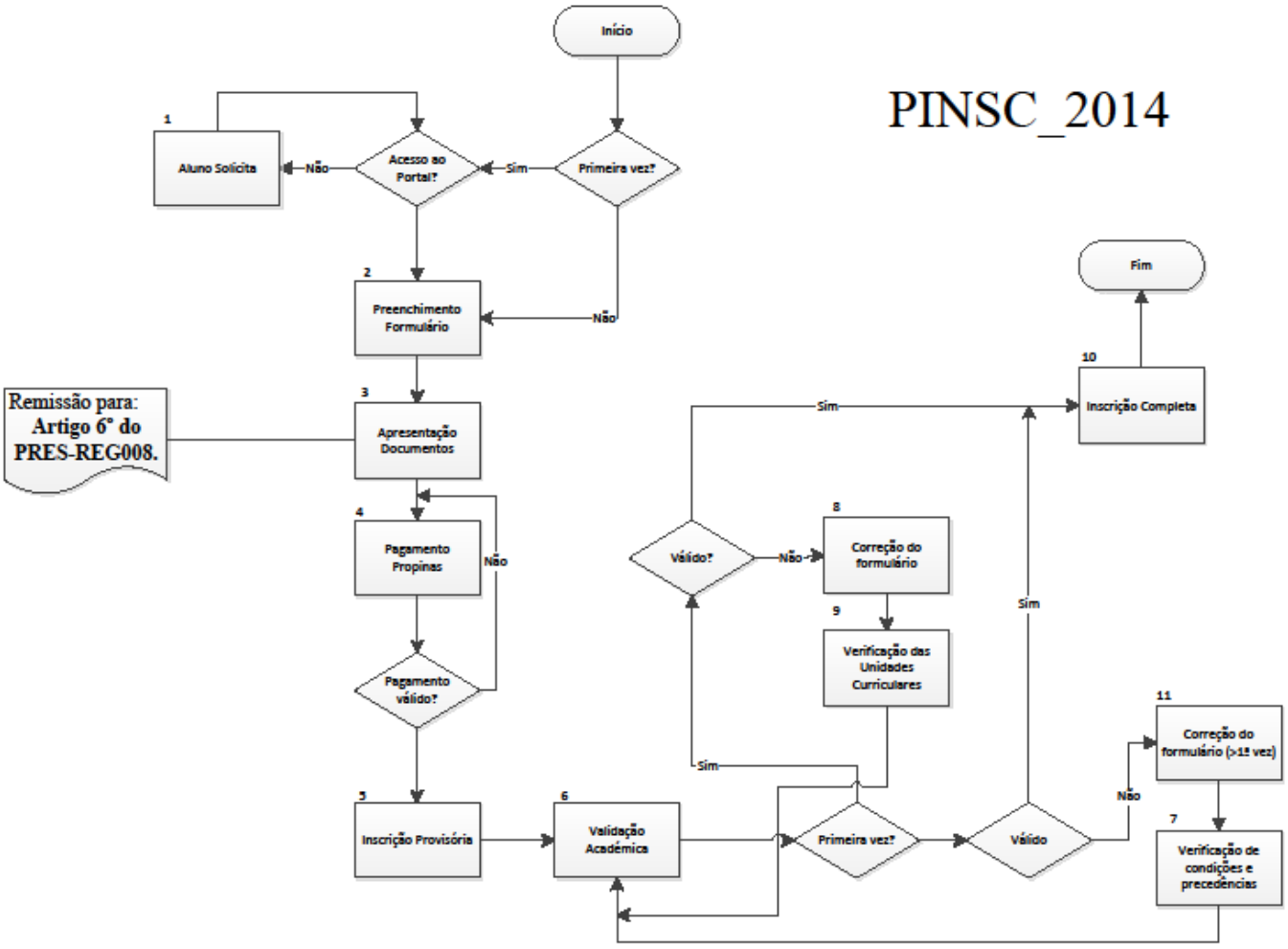


Figura 13 - Processo de avaliação

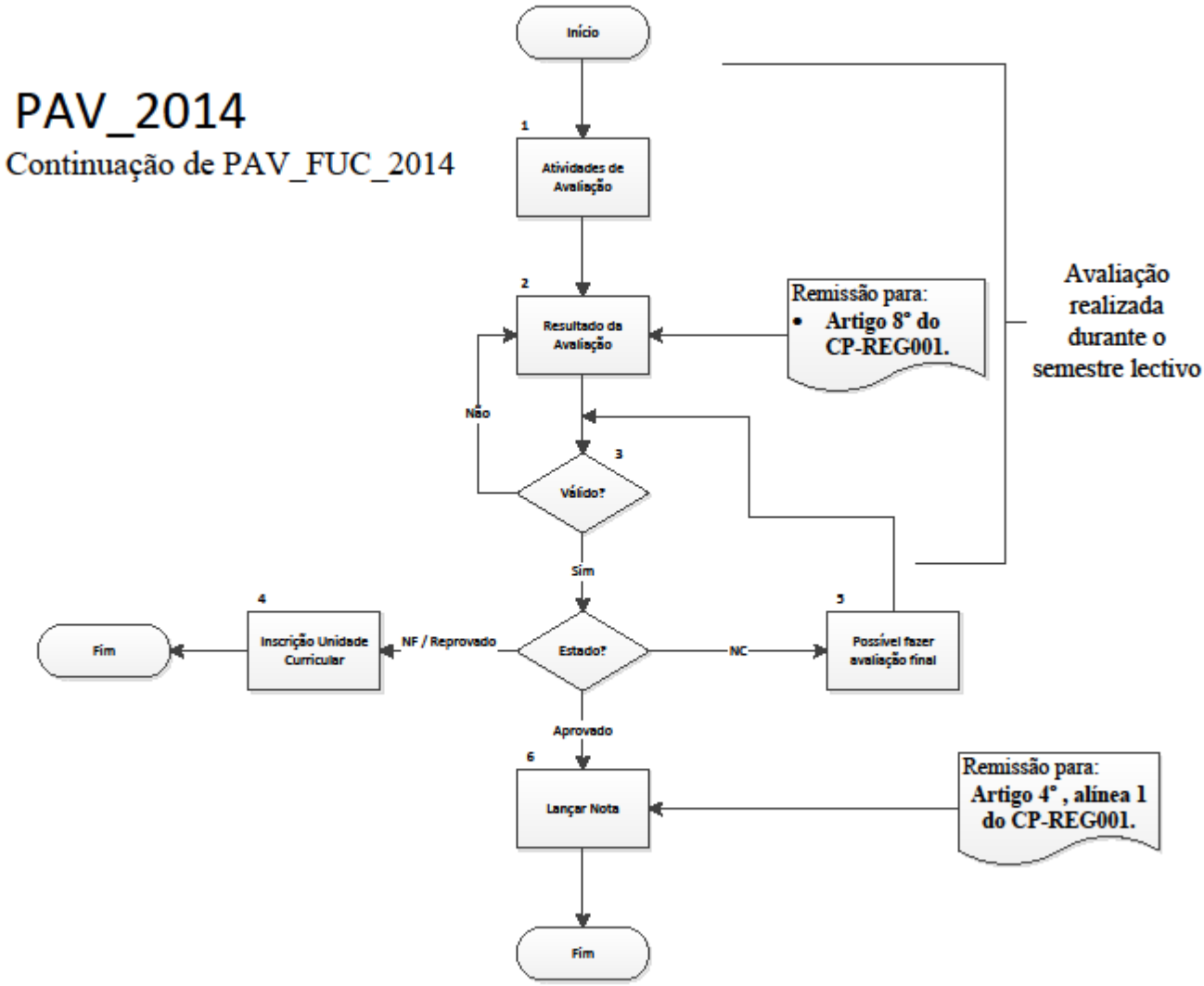


Figura 14 - Processo de aprovação da FUC

PAP_FUC_2014

Continua em PAV_2014

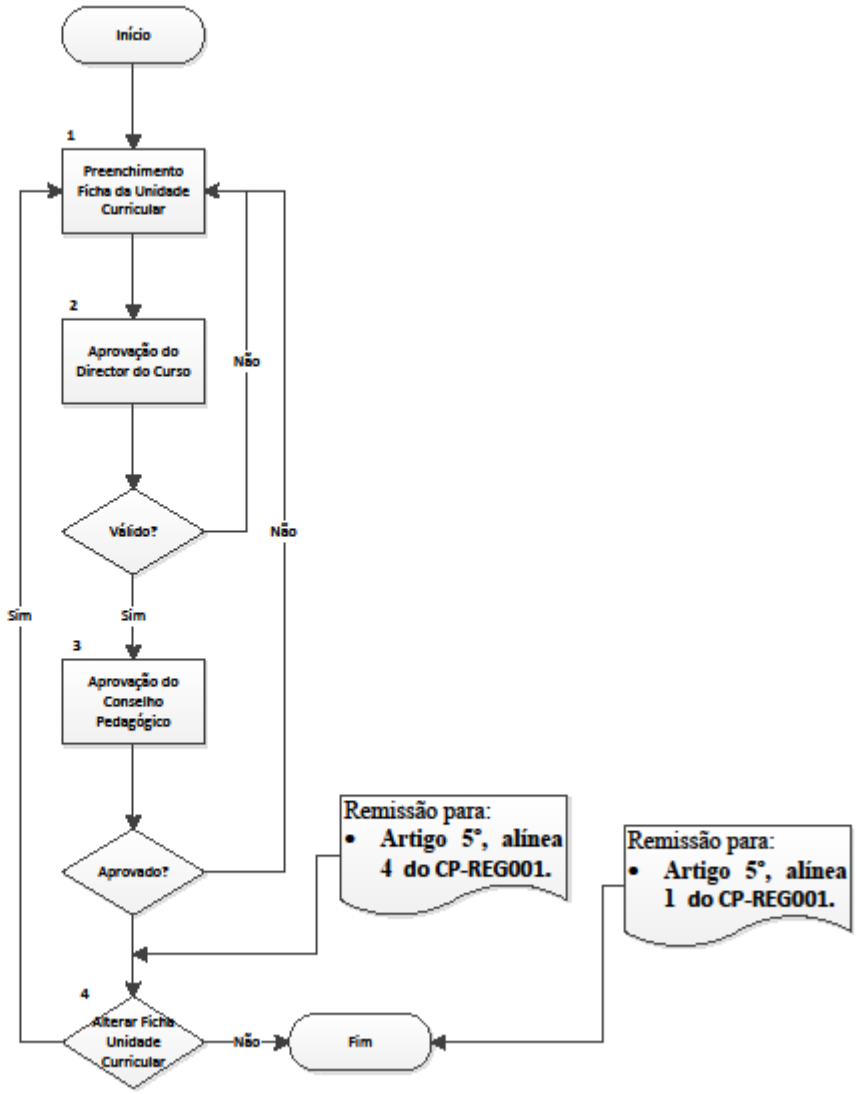


Figura 15 - Processo de anulação de matrícula

PAN_2014

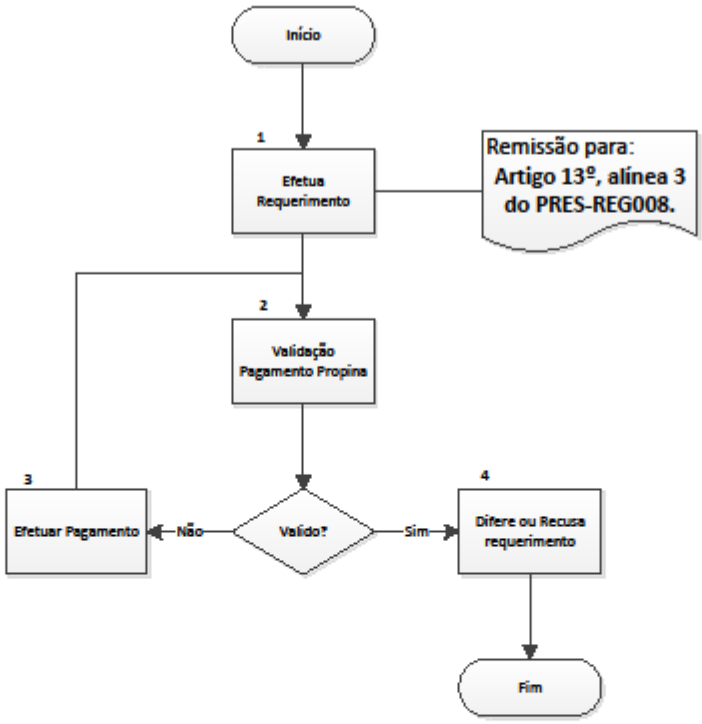


Figura 16 - Processo de notas

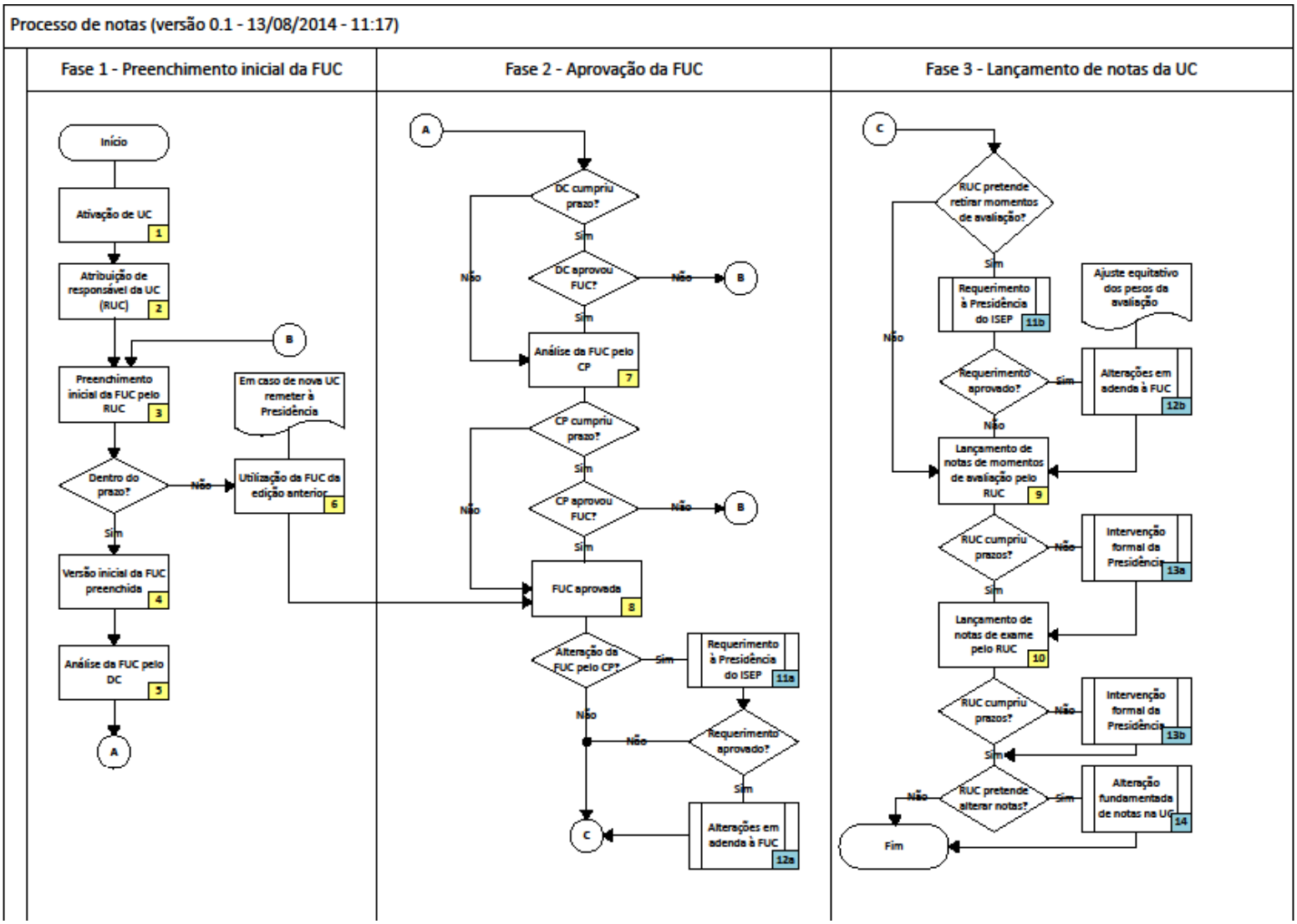


Figura 17 - Processo fornecido pelo ISEP

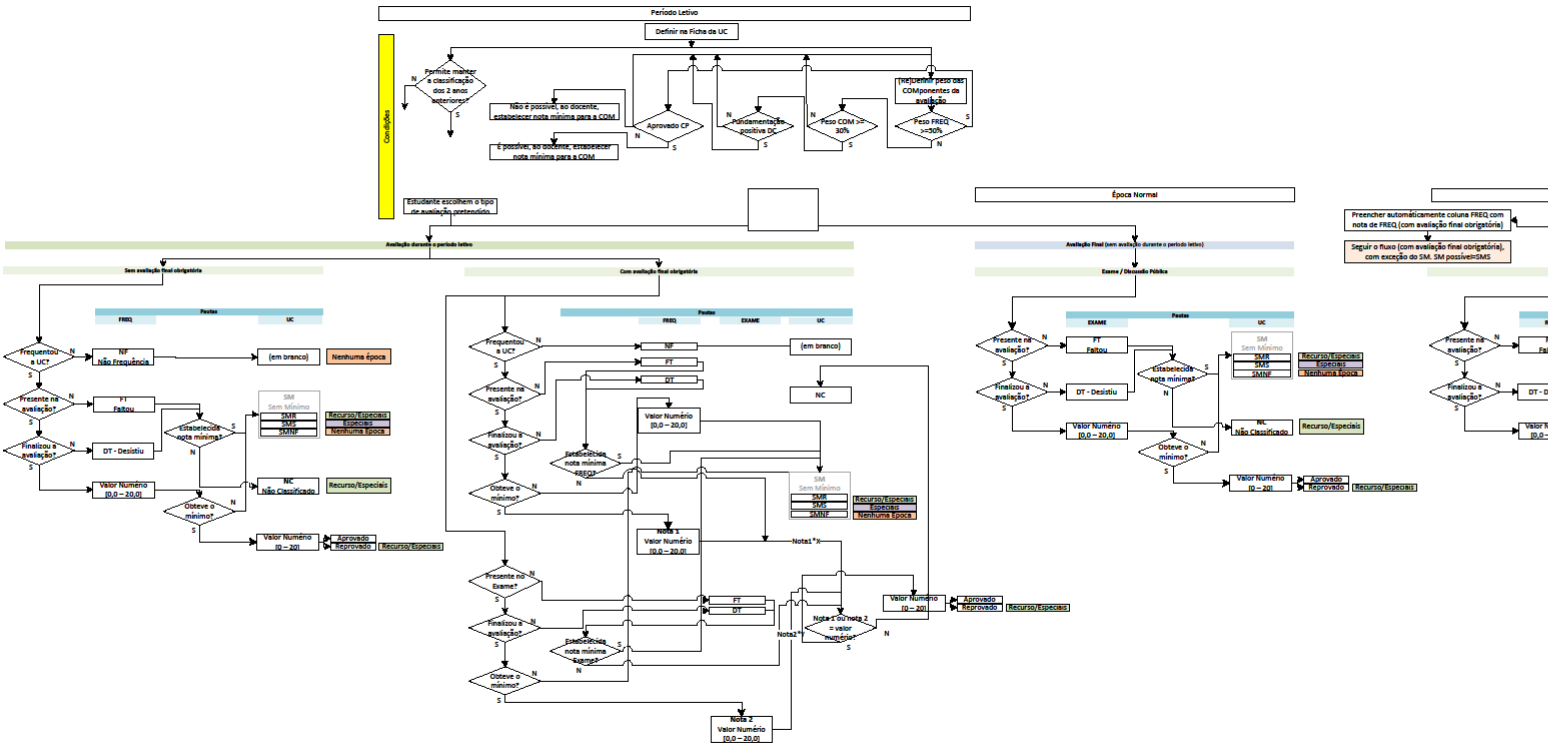


Tabela 4 - Tabela de requisitos do processo de inscrição

Processo de inscrição			PINSC_2014			
Id	Nome do processo	Descrição	Confidencialidade	Integridade	Disponibilidade	Responsabilidade do pro
1	Aluno Solicita	Aluno que não tem acesso ao portal solicita acesso a terceiros	5	5	5	Divisão académica/ Alu
2	Preenchimento Formulário	Preenchimento online do formulário de inscrição atraves do portal.	5	5	3	Divisão académica/ Alu
3	Apresentação de documentos	Envio de Bilhete de Identidade ou documento legal equivalente. Cartão de Contribuinte ou documento legal equivalente. 1 Fotografia. Boletim de Saúde actualizado.	5	5	3	Divisão académica/ Alu
4	Pagamento de propinas	Pagamento correspondente à 1ª propina.	5	5	5	Divisão académica/ Alu
5	Inscrição Provisória	Processo de identificação de erros e triagem de documentos.	5	5	5	?
6	Validação Académica	Processo de identificação de erros e triagem de documentos da inscrição, bem como a inscrição.	5	5	5	Divisão académica
7	Verificação de condições e precedências	Aplicável a alunos que se inscrevem pela 2 ou terceira vez na instituição e tem como intenção verificar se é possivel a inscrição tal como foi preenchida pelo aluno.	5	5	?	Divisão académica
8	Correcção do formulário	Rectificação do preenchimento do formulário	5	5	5	Divisão académica/ Alu
9	Verificação de condições e precedências	Aplicável a alunos que se inscrevem pela 2 ou terceira vez na instituição e tem como intenção verificar se é possivel a inscrição tal como foi preenchida pelo aluno.	5	5	?	Divisão académica

Tabela 5 - Tabela de requisitos do processo de avaliação

Processo de Avaliação			PAV_2014			
Id	Nome do processo	Descrição	Confidencialidade	Integridade	Disponibilidade	Responsabilidade d
1	Atividades de avaliação	Processo que decorre durante o semestre e que difere de Unidade Curricular.	?	5	3	Responsável da Curricular/Cor Pedagógico/Direct
2	Resultado da avaliação	Processo de lançamento do resultado da avaliação decorrente do semestre.	5	5	5	Responsável da Curricular/Do
3	Validação do resultado	Processo de verificação da validade da avaliação de acordo com a FUC.	5	5	5	Divisão Acad
4	Inscrição unidade curricular	Processo de inscrição na unidade Curricular.	5	5	5	Aluno/Divisão Ac
5	Possível fazer avaliação final	Após validação do resultado da avaliação o aluno faz exame ou não, de acordo com a FUC.	5	5	5	Divisão Acad
6	Lançar nota	Processo de lançamento definitivo da nota obtida na Unidade curricular	5	5	5	Responsável da Curricular/Do

Tabela 6 - Tabela de requisitos do processo de anulação da inscrição

Anulação da Inscrição			PAN_2014			
Id	Nome do processo	Descrição	Confidencialidade	Integridade	Disponibilidade	Responsabilidade do pro
1	Efetua Requerimento	Processo de efectuar requerimento fundamentado para anulação da inscrição no site www.ipp.pt	5	5	5	IPP/Aluno
2	Validação Pagamento Propina	Processo de validação do pagamento da propina efectuado pelo aluno.	5	5	5	Aluno/Divisão Acadén
3	Efetuar Pagamento	Processo de efectuar pagamento da propina.	5	5	5	Aluno
4	Difere ou Recusa requerimento	Processo de verificação do requerimento e parecer sobre o mesmo.	5	5	5	IPP

Tabela 7 - Tabela de requisitos do processo da aprovação da FUC

Aprovação da FUC			PAP_FUC_2014			
Id	Nome do processo	Descrição	Confidencialidade	Integridade	Disponibilidade	Responsa
1	Preenchimento Ficha da Unidade Curricular	Processo de preenchimento da ficha da unidade curricular que acontece anualmente.	5	5	?	Respo
2	Aprovação do Director do Curso	Processo de verificação e aprovação da ficha da unidade curricular por parte do director de curso.	5	5	?	Di
3	Aprovação do Conselho Pedagógico	Processo de verificação e aprovação da ficha da unidade curricular por parte do conselho pedagógico.	5	5	3	Cons
4	Alterar Ficha Unidade Curricular	Processo de alteração do preenchimento da ficha da unidade curricular.	5	5	?	Respo

Tabela 8 - Tabela de requisitos do processo de avaliação

Processo de Avaliação				PAV_2014			
Id	Nome do processo	Descrição	Confidencialidade	Integridade	Disponibilidade	Responsabilidade do processo	
1	Definir Ficha da UC	Processo que decorre antes do inicio do periodo de aulas.	5	5	3	Responsável da unidade Curricular/Conselho Pedagógico/Director de Curso	Má
2	Definir peso das Componentes da avaliação	Processo que decorre da formulação da componente de avaliação.	5	5	5	Responsável da unidade Curricular/Conselho Pedagógico/Director de Curso	
3	Fundamentação positiva DC	Fundamentação positiva para aprovação da FUC.	5	5	5	Director de Curso	Der i
4	Aprovado CP	Processo de aprovação da Fuc por parte do conselho pedagógico	5	5	5	Conselho Pedagógico	
5	Estudante escolhem o tipo de avaliação pretendido	Estudante escolhem o tipo de avaliação pretendido	5	5	5	Aluno	Poss d er
6	Frequentou a UC?	Processo de verificação em que o aluno frequentou ou não a Unidade Curricular	5	5	5	Divisão Académica	Dif
7	Finalizou a avaliação?	Processo de verificação no qual o aluno efectou avaliação durante o semestre	5	5	5	Divisão Académica	Dif inf infe
8	Estabelecida nota Mínima?	Processo de verificação no qual verifica se o aluno obteve nota mínima de frequência ou final para a Unidade Curricular em questão.	5	5	5	Divisão Académica/Professor	lar
9	Obteve mínimo?	Processo de verificação no qual verifica se o aluno obteve nota mínima para ir a exame ou passar a UC.	5	5	5	Divisão Académica/Professor	lar

Tabela 9 - Tabela de requisito do processo de notas

Processo de Notas								
Id	**Nome da atividade**	**Descrição**	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Responsabilidade da atividade**	**Vulnerabilidades/Ataques**	**Mitigaç**
1	Ativação de UC	Atividade de ativação de uma UC.	1	5	3	DA	Demora na activação da UC.	
2	Atribuição de responsável da UC (RUC)	Atividade de atribuição de um responsável à UC.	1	5	3	DC	Demora na atribuição do RUC.	
3	Preenchimento inicial da FUC pelo RUC	Atividade de preenchimento da FUC pelo RUC.	2	5	4	RUC	Formulação da ficha com erros e possíveis omissões. Não se encontrar de acordo com o regulamento CP-REG001.	
4	Versão inicial da FUC preenchida	Atividade de conclusão da FUC inicial.	1	5	4	RUC	Demora na submissão.	Salvagua ediçã
5	Análise da FUC pelo DC	Atividade na qual é analisada a FUC inicial pelo DC.	1	5	4	DC	Demora na decisão.	Em incumprim FUC é aut ap
6	Utilização da FUC da edição anterior	Atividade na qual é resgatada a FUC da edição anterior.	3	1	1	Presidência	Ser uma nova UC.	
7	Análise da FUC pelo CP	Atividade na qual é analisada a FUC inicial pelo CP.	1	5	4	CP	Demora na decisão.	Em incumprim FUC é aut ap
8	FUC aprovada	Atividade na qual a FUC é aprovada.	1	5	5	CP e Presidência	Detecção de lapsos à posteriori.	Requ Pre
9	Lançamento de notas de momentos de avaliação pelo RUC	Atividade do lançamento de notas pelo RUC no período letivo.	5	5	5	RUC	Demora no lançamento e lapsos nas notas.	Rectifica po
10	Lançamento de notas de exame pelo RUC	Atividade do lançamento de notas pelo RUC em períodos de exames.	5	5	5	RUC	Demora no lançamento e lapsos nas notas.	Rectifica po

Tabela 10 - Tabela de requisitos de subprocessos do processo de notas

Subprocessos auxiliares							
Id	**Nome da atividade**	**Descrição**	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Responsabilidade da atividade**	**Vulnerabilidades/Ataques**
11	Requerimento à Presidência do ISEP	Atividade externa desencadeada por um requerimento formal e fundamentado à Presidência.	5	5	3	CP ou RUC	Demora na resposta.
12	Alterações em adenda à FUC	Atividade externa na qual se faz uma adenda à FUC aprovada.	1	5	3	Presidência	Demora na resposta.
13	Intervenção formal da Presidência	Atividade externa despoletada pela Presidência	5	5	3	Presidência	
14	Alteração fundamentada de notas na UC	Atividade externa para alteração de notas da UC	5	5	5	RUC	Demora na atividade.

Tabela 11 - Lista de inventário do processo de notas

Atividade	Entrada	Saída	Conf	Int	Disp
P1.A1	Início do ano por DA (externo)	Ativação das UC	N	S	S
	UCs não ativas	Registo			
		Alerta para DC			
P1.A2	UCs ativas	UC com RUC	N	S	S
	Alerta para DC	Registo			
		FUC inicial em branco			
		Alerta para RUC			
P1.A3	RUC	FUC inicial em curso	N	S	N
	FUC inicial em branco	Registo			
	Alerta para RUC				
P1.D1	Data Limite	Decisão do Portal	N	N	S
		Registo			
P1.A4	FUC inicial em curso	FUC inicial preenchida	N	S	S
	Decisão do Portal	Registo			
		Alerta para DC			
P1.A5	FUC inicial preenchida	FUC inicial preenchida	N	S	S
	Alerta para DC	Registo			
		Decisão do DC			
P1.A6	Alerta para DC e Presidência	FUC aprovada	N	S	S
	Decisão do Portal				

Atividade	Entrada	Saída	Conf	Int	Disp
P1.D2	FUC inicial preenchida	Decisão do Portal	N	S	S
	Data Limite	Registo			
P1.D3	FUC inicial preenchida	FUC inicial preenchida (sim) / decisão do DC	N	S	S
	Decisão do Portal	Registo			
		Alerta para CP			
P1.A7	FUC inicial preenchida (sim) / decisão do Portal	Registo	N	S	S
	Alerta para CP	Decisão do CP			
P1.D4	FUC inicial preenchida	Decisão do Portal	N	S	S
	Data Limite	Registo			
P1.D5	FUC inicial preenchida	FUC inicial preenchida (sim) / decisão do CP	N	S	S
	Decisão do Portal	Registo			
P1.A8	FUC inicial aprovada (sim) / FUC de ano anterior	FUC aprovada	N	S	S
		Registo			
		Alerta para CP, DC e RUC			
P1.D6	FUC aprovada	Requerimento de alteração da FUC pelo CP	N	S	S
		FUC aprovada			
		Registo			
P1.A11a	Requerimento de alteração da FUC pelo CP	Alerta para CP	S	S	S
	FUC aprovada	Registo			
P1.D7	FUC aprovada	Decisão sobre Requerimento do CP pela PR	S	S	S
		Registo			
P1.D12a	Decisão sobre Requerimento do CP pela PR	FUC aprovada com adenda	N	N	S
	FUC aprovada	Registo			
		Alerta para CP, DC e RUC			

Atividade	Entrada	Saída	Conf	Int	Disp
P1.D8	FUC aprovada	Decisão do RUC	N	S	N
		Registo			
P1.A9	FUC aprovada	FUC aprovada	S	S	S
	Decisão do RUC / Decisão sobre Requerimento do	Registo			
		Lançamento de notas dos momentos de			
		Alerta para alunos			
P1.D9	FUC aprovada	Decisão sobre Requerimento do RUC pela PR	S	S	S
		Registo			
P1.A11b	Requerimento de alteração da FUC pelo RUC	Requerimento de alteração da FUC pelo RUC	S	S	S
	FUC aprovada	Registo			
P1.A12b	Decisão sobre Requerimento do RUC pela PR	FUC aprovada com adenda	N	N	S
	FUC aprovada	Registo			
		Alerta para CP, DC, RUC e alunos			
P1.D10	FUC aprovada	Decisão do Portal	N	S	N
	Data Limite	Registo			
P1.A10	FUC aprovada	Lançamento de notas de exame	S	S	S
	Decisão do Portal / Intervenção formal da	Registo			
		Alerta para alunos			
P1.A13a	FUC aprovada	Intervenção formal da Presidência	S	S	S
	Decisão do Portal	Registo			

Tabela 12 - Tabela de recursos com avaliação de risco da Presidência

Id	Nome do recurso	Descrição	Atividade	Dono(s)	Valor da Substituição (Impacto, 1-5)	Probabilidad de Acontece (1-5)
R1	Prepraração do ano letivo pela DA (externo)	Processo externo despoletado para preparar o novo letivo.	P1.A1	DA	1	1
R2	UCs não ativas	Unidades Curriculares inativas antes do início do ano letivo.	P1.A1	Portal	1	1
R3	Ativação das UCs	Processo no qual são tornadas ativas as Unidades Curriculares apropriadas e arranca o ano letivo.	P1.A1	DA	5	5
R4	Alerta para DC	Comunicação despoletada para aviso do Diretor de Curso de uma ação ocorrida.	P1.A1, P1.A2, P1.A4, P1.A5, P1.A6, P1.A8, P1.A12b, P1.D12a	Portal	5	2
R5	UCs ativas	Unidades Curriculares ativas durante o ano letivo em questão.	P1.A2	Portal	2	2
R6	UC com RUC	Atribuição da responsabilidade de uma Unidade Curricular a um docente.	P1.A2	DC + Portal	3	4
R7	FUC inicial em branco	Criação de Ficha de Unidade curricular em branco associada a uma UC.	P1.A2, P1.A3	Portal	1	1
R8	Alerta para RUC	Comunicação despoletada para aviso do Responsável da Unidade Curricular de uma ação ocorrida.	P1.A2, P1.A3, P1.A8, P1.D12a, P1.D12b	Portal	2	2
R9	RUC	Responsável da Unidade Curricular.	P1.A3	RUC	5	5
R10	FUC inicial em curso	Ficha de Unidade Curricular criada e em fase de preenchimento.	P1.A3, P1.A4	RUC + Portal	2	2
R11	Data Limite	Data limite pré-definida e usada para verificação de um prazo.	P1.D1, P1.D2, P1.D4, P1.D10, P1.D11	Portal	4	3
R12	Decisão do Portal	Processo automático na qual o Portal toma decisão sobre um estado ou ação.	P1.A4, P1.A6, P1.A7, P1.A10, P1.A13a, P1.A13b, P1.D1, P1.D2, P1.D3, P1.D4, P1.D5, P1.D10, P1.D11, P1.D12b	Portal	5	5
R13	FUC inicial preenchida	Ficha de Unidade Curricular preenchida.	P1.A4, P1.A5, P1.A7, P1.D2, P1.D3, P1.D4, P1,D5	RUC + Portal	1	1
R14	Alerta para Presidência	Comunicação despoletada para aviso da Presidência de uma ação ocorrida.	P1.A6	Portal	3	3

Id	Nome do recurso	Descrição	Atividade	Dono(s)	Val Subst (Impa
R15	FUC aprovada	Ficha de Unidade Curricular aprovada e em vigor para o ano em questão.	P1.A6, P1.A8, P1.A9, P1.A10, P1.A11a, P1.A11b, P1.A12b, P1.A13a, P1.D6, P1,D7, P1.D8, P1.D10, P1.D12a	CP + RUC + DC	
R16	Alerta para CP	Comunicação despoletada para aviso do Conselho Pedagógico de uma ação ocorrida sobre a FUC.	P1.D3, P1.A7, P1.A8, P1.A11a, P1.D12a, P1.D12b	Portal	
R17	Decisão do CP	Decisão tomada pelo Conselho Pedagógico sobre a FUC inicial preenchida.	P1.A7, P1.D5	CP	
R18	Decisão do DC	Decisão tomada pelo Diretor de Curso sobre a FUC inicial preenchida.	P1.D3, P1.A5	DC	
R19	FUC de ano anterior	Ficha de Unidade Curricular do ano anterior e que foi aprovada.	P1.A8	Portal + PR	
R20	Requerimento de alteração da FUC pelo CP	Requerimento feito pelo CP para alteração da FUC.	P1.D6, P1.A11a	CP	
R21	Decisão sobre Requerimento do CP pela Presidência	Decisão tomada pela Presidência e que responde ao requerimento efetuado pelo CP.	P1.D7, P1.D12a	PR	
R22	Decisão do RUC	Decisão do Responsável da Unidade Curricular relativamente a uma ação.	P1.D8, P1.A9, P1.D12, P1.A14	RUC	
R23	Decisão sobre Requerimento do RUC pela Presidência	Decisão tomada pela Presidência e que responde ao requerimento efetuado pelo RUC.	P1.A9, P1.D9, P1,A12b	PR	
R24	Lançamento de notas dos momentos de avaliação	Ato de lançamento das notas dos momentos de avaliação pelo RUC no Portal	P1.A9	RUC + Portal	
R25	Alerta para alunos	Comunicação despoletada para aviso dos alunos.	P1.A9 P1.A10, P1.A14	Portal	
R26	Lançamento de notas de exame	Ato de lançamento das notas de exame.	P1.A10, P1.D11	RUC + Portal	
R27	Intervenção formal da Presidência	Intervenção da Presidência quando o RUC não cumpre prazos.	P1.A10, P1.A13a, P1.A13b, P1.D12b	PR	
R28	Notas lançadas	Notas correspondentes à avaliação final (notas de momentos de avaliação + notas de exame).	P1.A14	RUC + Portal + PR	
R29	Fundamentação da alteração de notas	Formalismo ativado pelo RUC em caso de necessidade de mudança de nota.	P1.A14	RUC + Portal	
R30	Registo	Registo de evento(s) efetuado nos diferentes momentos para fins de histórico e evidência futura.	P1.A1, P1.A2, P1.A3, P1.A4, P1.A5 P1.A7, P1.A8 P1.A9, P1.A10, P1.A11a, P1.A11b, P1.A12b, P1.A13a, P1.A13b, P1.A14, P1.D1, P1.D2, P1.D3, P1.D4, P1.D5, P1.D6, P1.D7, P1.D8, P1.D9, P1.D10, P1.D11, P1.D12a, P1.D12b	Portal	

Tabela 13 - Tabela de recurso com a avaliação inicial do risco

Id	Nome do recurso	Descrição	Atividade	Dono(s)	Valor da Substituição (Impacto)	Probabilidade de Acontecer (Risco)	?	Con Apli
R1	Início do ano por DA (externo)	Processo externo despoletado para dar início ao novo letivo.	P1.A1	DA	5	1	5	
R2	UCs não ativas	Unidades Curriculares inativas no início do ano letivo.	P1.A1	Portal	5	1	5	
R3	Ativação das UCs	Processo no qual são tornadas ativas as Unidades Curriculares apropriadas.	P1.A1	DA + Portal	5	1	5	
R4	Alerta para DC	Comunicação despoletada para aviso do Diretor de Curso de uma ação ocorrida.	P1.A1, P1.A2, P1.A4, P1.A5, P1.A6, P1.A8, P1.A12b, P1.D12a	Portal	2	1	2	
R5	UCs ativas	Unidades Curriculares ativas durante o ano letivo em questão.	P1.A2	Portal	5	1	5	
R6	UC com RUC	Atribuição da responsabilidade de uma Unidade Curricular a um docente.	P1.A2	DC + Portal	3	3	9	
R7	FUC inicial em branco	Criação de Ficha de Unidade curricular em branco associada a uma UC.	P1.A2, P1.A3	Portal	1	1	1	
R8	Alerta para RUC	Comunicação despoletada para aviso do Responsável da Unidade Curricular de uma ação ocorrida.	P1.A2, P1.A3, P1.A8, P1.D12a, P1.D12b	Portal	2	1	2	
R9	RUC	Responsável da Unidade Curricular.	P1.A3	RUC	3	2	6	
R10	FUC inicial em curso	Ficha de Unidade Curricular criada e em fase de preenchimento.	P1.A3, P1.A4	RUC + Portal	1	1	1	
R11	Data Limite	Data limite pré-definida e usada para verificação de um prazo.	P1.D1, P1.D2, P1.D4, P1.D10, P1.D11	Portal	5	1	5	
R12	Decisão do Portal	Processo automático na qual o Portal toma decisão sobre um estado ou ação.	P1.A4, P1.A6, P1.A7, P1.A10, P1.A13a, P1.A13b, P1.D1, P1.D2, P1.D3, P1.D4, P1.D5, P1.D10, P1.D11, P1.D12b	Portal	5	1	5	
R13	FUC inicial preenchida	Ficha de Unidade Curricular preenchida.	P1.A4, P1.A5, P1.A7, P1.D2, P1.D3, P1.D4, P1,D5	RUC + Portal	4	3	12	
R14	Alerta para Presidência	Comunicação despoletada para aviso da Presidência de uma ação ocorrida.	P1.A6	Portal	1	1	1	

Id	Nome do recurso	Descrição	Atividade	Dono(s)	Valor da Substituição (Impacto)	P A
R15	FUC aprovada	Ficha de Unidade Curricular aprovada e em vigor para o ano em questão.	P1.A6, P1.A8, P1.A9, P1.A10, P1.A11a, P1.A11b, P1.A12b, P1.A13a, P1.D6, P1,D7, P1.D8, P1.D10, P1.D12a	CP + RUC + DC	5	
R16	Alerta para CP	Comunicação despoletada para aviso do Conselho Pedagógico de uma ação ocorrida sobre a FUC.	P1.D3, P1.A7, P1.A8, P1.A11a, P1.D12a, P1.D12b	Portal	2	
R17	Decisão do CP	Decisão tomada pelo Conselho Pedagógico sobre a FUC inicial preenchida.	P1.A7, P1.D5	CP	5	
R18	Decisão do DC	Decisão tomada pelo Diretor de Curso sobre a FUC inicial preenchida.	P1.D3, P1.A5	DC	5	
R19	FUC de ano anterior	Ficha de Unidade Curricular do ano anterior e que foi aprovada.	P1.A8	Portal + PR	1	
R20	Requerimento de alteração da FUC pelo CP	Requerimento feito pelo CP para alteração da FUC.	P1.D6, P1.A11a	CP	5	
R21	Decisão sobre Requerimento do CP pela Presidência	Decisão tomada pela Presidência e que responde ao requerimento efetuado pelo CP.	P1.D7, P1.D12a	PR	5	
R22	Decisão do RUC	Decisão do Responsável da Unidade Curricular relativamente a uma ação.	P1.D8, P1.A9, P1.D12, P1.A14	RUC	5	
R23	Decisão sobre Requerimento do RUC pela Presidência	Decisão tomada pela Presidência e que responde ao requerimento efetuado pelo RUC.	P1.A9, P1.D9, P1,A12b	PR	5	
R24	Lançamento de notas dos momentos de avaliação	Ato de lançamento das notas dos momentos de avaliação pelo RUC no Portal	P1.A9	RUC + Portal	5	
R25	Alerta para alunos	Comunicação despoletada para aviso dos alunos.	P1.A9 P1.A10, P1.A14	Portal	1	
R26	Lançamento de notas de exame	Ato de lançamento das notas de exame.	P1.A10, P1.D11	RUC + Portal	5	
R27	Intervenção formal da Presidência	Intervenção da Presidência quando o RUC não cumpre prazos.	P1.A10, P1.A13a, P1.A13b, P1.D12b	PR	5	
R28	Notas lançadas	Notas correspondentes à avaliação final (notas de momentos de avaliação + notas de exame).	P1.A14	RUC + Portal + PR	5	
R29	Fundamentação da alteração de notas	Formalismo ativado pelo RUC em caso de necessidade de mudança de nota.	P1.A14	RUC + Portal	5	
R30	Registo	Registo de evento(s) efetuado nos diferentes momentos para fins de histórico e evidência futura.	P1.A1, P1.A2, P1.A3, P1.A4, P1.A5 P1.A7, P1.A8 P1.A9, P1.A10, P1.A11a, P1.A11b, P1.A12b, P1.A13a, P1.A13b, P1.A14, P1.D1, P1.D2, P1.D3, P1.D4, P1.D5, P1.D6, P1.D7, P1.D8, P1.D9, P1.D10, P1.D11, P1.D12a, P1.D12b	Portal	3	

Tabela 14 - Critérios de risco definidos pela Presidência do ISEP

	Probabilidade de acontecer (1-5)				
Impacto (1-5)	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

(faz a tua versão)

Critérios de Risco	
Nível	Cor
Muito Baixo	
Baixo	
Médio	
Alto	
Muito alto	

Colorir as células numeradas de acordo com a percepção de risco
Risco = Probabilidade de acontecer * Impacto
Impacto = consequência de ter acontecido (dano)

Tabela 15 - Avaliação de risco (exemplo)

	Probabilidade de acontecer (1-5)				
Impacto (1-5)	1	2	3	4	5
	2	4	6	8	10
	3	6	9	12	15
	4	8	12	16	20
	5	10	15	20	25

Critérios de Risco	
Nível	Cor
Muito Baixo	
Baixo	
Médio	
Alto	
Muito alto	

Colorir as células numeradas de acordo com a percepção de risco
Risco = Probabilidade de acontecer * Impacto
Impacto = consequência de ter acontecido (dano)

8 ANEXO B. Documentos produzidos ou usados na elaboração da tese

Security Policy of ISEP

Protection of information is vital to the success of our organization. To achieve this, an information security management system is required to manage all the relevant processes in order to identify the information to protect and how it must be protected in terms of security.

Because we need improve our system and need to apply new frameworks and new features, the management system must be continually monitored and improved to meet its goals. To achieve it, the system must be continuously improved and the processes regularly reviewed.

It is the policy of ISEP to ensure that:

- *Information is only accessible to authorized entities from within or outside ISEP.*
- *Confidentiality of information is maintained.*
- *Integrity of information is maintained throughout the processes.*
- *Business continuity plans are established, maintained and regularly tested.*
- *All personnel is trained on information security and is informed that compliance with policy is mandatory.*
- *All breaches of information security and suspected weaknesses are reported and investigated.*
- *Procedures exist to support the policy, verification of the data and correction of malfunctions in the processes.*
- *Processes have self-assessment and quality improvement procedures.*
- *The Chief Information Security Manager is responsible for maintaining the policy and providing support and advice during its implementation and furthermore.*
- *All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments or units.*

Papéis e responsabilidades

Presidente

- O presidente é o órgão superior de governo e de representação externa do ISEP;
- O presidente é o órgão de condução da política da instituição;
- Representar o ISEP, em juízo e fora dele;
- Presidir ao Conselho Técnico-científico;
- Dirigir os serviços do ISEP e aprovar os necessários regulamentos;
- Gerir os recursos humanos, físicos e materiais afetos ao ISEP;
- Conduzir a gestão patrimonial e financeira;
- Decidir, no âmbito do ISEP, a abertura de concursos, a designação de júris e a nomeação e contratação de pessoal, a qualquer título, com exceção da composição de júris de concursos de provas académicas, quando legalmente atribuídas ao Presidente do IPP;
- Homologar a distribuição do serviço docente;
- Homologar os regimes de transição entre planos de estudo;
- Pronunciar-se sobre o regime de prescrições;
- Aprovar o calendário e horário das atividades letivas, ouvido o Conselho Pedagógico;
- Executar as deliberações dos Conselhos Técnico-científico e Pedagógico, quando vinculativas;
- Elaborar o plano de atividades e o orçamento, bem como o relatório de atividades e as contas;
- Nomear e exonerar o Presidente do Conselho Técnico-Científico;
- Nomear e exonerar os vice-presidentes;
- Nomear e exonerar o Administrador ou Secretário e os dirigentes dos serviços do ISEP;
- Exercer as funções que lhe sejam delegadas pelo Presidente do IPP; q) Propor ao Presidente do IPP os valores máximos de novas admissões e de inscrições de estudantes;
- Criar, participar ou incorporar, no âmbito do ISEP, entidades subsidiárias de direito privado;
- Garantir a existência de um meio de divulgação de informação institucional onde são publicadas as decisões dos órgãos do ISEP;
- Instituir prémios escolares no âmbito do ISEP;
- Exercer as demais competências previstas na lei, nos Estatutos do IPP ou nos Estatutos, bem como as que não sejam atribuídas a outros órgãos.

Vice-Presidentes

- O Presidente pode nomear livremente entre um e três vice-presidentes;
- Os vice-presidentes iniciam funções na data do despacho de nomeação;
- O Administrador ou Secretário tem as competências delegadas pelo Presidente do ISEP;
- Os vice-presidentes podem ser exonerados a todo o tempo pelo Presidente e seu mandato cessa com a cessação do mandato do Presidente.

Divisão Académica

Diretor nomeado pelo Presidente do ISEP.

- Secção de Pré-Graduação (PRE)
    - Realizar os procedimentos académicos inerentes à inscrição e frequência dos cursos de Licenciatura ou Cursos de Especialização Tecnológica pelos estudantes ordinários, extraordinários e ainda pelos estudantes com estatutos especiais;
    - Emitir certidões, diplomas, suplementos ao diploma e demais documentos certificativos das atividades realizadas pelos estudantes durante o seu percurso académico;
    - Prestar informações e esclarecimentos aos estudantes sobre os procedimentos académicos;
    - O atendimento ao público em geral;
    - Realizar os procedimentos académicos inerentes à inscrição e frequência dos demais cursos não conducentes a grau e demais atividades definidas pela gestão;
    - A gestão do arquivo dos estudantes.

- Secção de Pós-graduação (POS)
    - Apoiar os processos de candidatura dos cursos de Mestrado e Pós-Graduação do ISEP;
    - Realizar os procedimentos académicos inerentes à inscrição e frequência dos cursos de Mestrado e Pós-Graduação pelos estudantes ordinários, extraordinários e ainda pelos estudantes com estatutos especiais;
    - Emitir certidões, diplomas, suplementos ao diploma e demais documentos certificativos das atividades realizadas pelos estudantes durante o seu percurso académico;
    - Prestar informações e esclarecimentos aos estudantes sobre os procedimentos académicos;
    - O atendimento ao público em geral.

Divisão de Sistemas Informáticos

- Gabinete de Infraestruturas e Suporte ao Utilizador (GIS)
    - O desenho, definição e implementação de soluções tecnológicas ao nível da infraestrutura de rede;
    - A definição, implementação e monitorização de políticas de segurança;
    - O suporte ao utilizador ao nível da microinformática e infraestrutura telefónica;
    - A gestão e manutenção das comunicações de voz em suporte tradicional e VoIP;
    - A definição de soluções tecnológicas ao nível dos sistemas de informação, incluindo o *hardware* de suporte, sistemas operativos, aplicações e armazenamento, assegurando o seu bom funcionamento e elevados índices de disponibilidade.

- Gabinete de Sistemas de Informação (GSI)
    - A conceção, desenvolvimento, implementação e administração do sistema de informação;
    - A administração dos sistemas de suporte à Divisão de Recursos Humanos e à Direção de Serviços Económico-Financeiros;
    - O fornecimento dos dados necessários à elaboração do relatório de gestão e de estatísticas a que o ISEP esteja legalmente obrigado.

- Gabinete de E-learning e Multimédia (GEM)
    - A manutenção e administração das plataformas Moodle e Dspace;
    - O desenvolvimento, manutenção e administração do sítio internet institucional;
    - O desenvolvimento de mecanismos e ferramentas de interoperabilidade entre as aplicações de suporte aos serviços, o sistema de informação e o sítio internet institucional.

ISMS do ISEP – Guia de trabalho da tese

Ter suporte da gestão

Tem de haver compromisso formal da gestão de topo nas várias fases do ISMS.

Resultados:

- Política de segurança ou parte de um plano de segurança
- Plano e objetivos da segurança, idem
- Papéis e responsabilidades da segurança através de funções documentadas
- Divulgação e comunicação na organização da política de segurança e adesão
- Disponibilizar os recursos necessários e suficientes
- Idioma do ISMS
- Exemplo

Definição do âmbito do ISMS

Necessário:

- Lista de espaços, localizações, recursos, tecnologias, etc.

Questões:

- Áreas da organização (caraterísticas)
- Impactos nos fornecedores
- Dependências de terceiros
- Normativos aplicáveis

Objetivos:

- Definir os processos que vão estabelecer o âmbito e o contexto do ISMS
- Com base na matriz de processos, analisar os processos e as suas atividades
- Caraterizar os processos e as atividades críticas em termos de C/I/D
- Definir o contexto organizacional e a estratégia
- Compromissos de implementação

Resultados:

- Documento do âmbito do ISMS
- Guião das atividades a desenvolver para implementar o ISMS
- Exemplo

Definição da orgânica

Resultado:

Documento que define:

- Responsável (CISO)
- Donos dos processos, funções e responsabilidades
- Fórum de segurança (como funciona – CISO, donos dos processos, outros)

Inventário de recursos de informação

Tabela de inventário baseada em recursos de informação:

- Identificador
- Requisitos de segurança C/I/D
- Processos de gestão
- Política de inventário
- Política de uso
- Identificação de requisitos de segurança (recursos versus processos/atividades)
- Controlos aplicáveis ou risco residual

Declaração de aplicabilidade

Matriz de controlos com cláusulas sobre uso ou não (neste caso implica justificação)

Os controlos são os da ISO 27001 (lista)

Exemplo

Gestão de riscos

Exercício de análise de riscos:

- Identificação de riscos

Avaliação de riscos com definição de:

- Valor dos recursos
- Frequência de ocorrência
- Dano causado

Fases seguintes... (implementação)

Declaração de aplicabilidade

Pretende-se com este documento obter uma vista geral dos controlos aplicáveis ou aplicados. Com isto em mente, o sistema de gestão da segurança da informação torna-se mais seguro e robusto.

A lista seguinte mostra os controlos e os recursos associados:

Id do Recurso	Nome do recurso	Atividade	Controlos aplicáveis	Estado	Justificação	Controlos identificados	Fonte de Risco
R1	Início do ano por DA (externo)	P1.A1	A.8.1.3, A.12.4.1				Falhas da DA ou do Portal
R2	UCs não ativas	P1.A1	A.8.1.2				Falhas do Portal
R3	Ativação das UCs	P1.A1	A.8.1.3, A.12.4.1				Falhas da DA ou do Portal
R4	Alerta para DC	P1.A1, P1.A2, P1.A4, P1.A5, P1.A6, P1.A8, P1.A12b, P1.D12a	A.12.4.1				Falhas do Portal
R5	UCs ativas	P1.A2	A.8.1.2				Falhas do Portal
R6	UC com RUC	P1.A2	A.8.1.3, A.12.4.1, A.8.2.3				Falhas do DC ou do Portal
R7	FUC inicial em branco	P1.A2, P1.A3	A.8.1.2				Falhas do Portal
R8	Alerta para RUC	P1.A2, P1.A3, P1.A8, P1.D12a, P1.D12b	A.12.4.1				Falhas do Portal
R9	RUC	P1.A3	A.8.1.2				Falhas do RUC
R10	FUC inicial em curso	P1.A3, P1.A4	A.8.1.3, A.12.4.1, A.8.2.3				Falhas do RUC ou do Portal

Id do Recurso	Nome do recurso	Atividade	Controlos aplicáveis	Estado	Justificação	Controlos identificados	Fonte de Risco
R11	Data Limite	P1.D1, P1.D2, P1.D4, P1.D10, P1.D11	A.8.1.2				Falhas do Portal
R12	Decisão do Portal	P1.A4, P1.A6, P1.A7, P1.A10, P1.A13a, P1.A13b, P1.D1, P1.D2, P1.D3, P1.D4, P1.D5, P1.D10, P1.D11, P1.D12b	A.12.1.1, A.12.4.1				Falhas do Portal
R13	FUC inicial preenchida	P1.A4, P1.A5, P1.A7, P1.D2, P1.D3, P1.D4, P1,D5	A.8.1.3, A.12.4.1, A.8.2.3				Falhas do RUC ou do Portal
R14	Alerta para Presidência	P1.A6	A.12.4.1				Falhas do Portal
R15	FUC aprovada	P1.A6, P1.A8, P1.A9, P1.A10, P1.A11a, P1.A11b, P1.A12b, P1.A13a, P1.D6, P1,D7, P1.D8, P1.D10, P1.D12a	A.8.1.2				Falhas do CP, do RUC do DC
R16	Alerta para CP	P1.D3, P1.A7, P1.A8, P1.A11a, P1.D12a, P1.D12b	A.12.4.1				Falhas do Portal
R17	Decisão do CP	P1.A7, P1.D5	A.12.1.1, A.12.4.1				Falhas do CP
R18	Decisão do DC	P1.D3, P1.A5	A.12.1.1, A.12.4.1				Falhas do DC
R19	FUC de ano anterior	P1.A8	A.8.1.2				Falhas da PR ou do Portal
R20	Requerimento de alteração da FUC pelo CP	P1.D6, P1.A11a	A.12.1.1, A.12.4.1				Falhas do CP
R21	Decisão sobre Requerimento do CP pela Presidência	P1.D7, P1.D12a	A.12.1.1, A.12.4.1				Falhas da PR

Id do Recurso	Nome do recurso	Atividade	Controlos aplicáveis	Estado	Justificação	Controlos identificados	Fonte de Risco
R22	Decisão do RUC	P1.D8, P1.A9, P1.D12, P1.A14	A.12.1.1, A.12.4.1				Falhas do RUC
R23	Decisão sobre Requerimento do RUC pela Presidência	P1.A9, P1.D9, P1,A12b	A.12.1.1, A.12.4.1				Falhas da PR
R24	Lançamento de notas dos momentos de avaliação	P1.A9	A.8.1.3, A.12.4.1, A.8.2.3, A.12.1.1				Falhas do RUC ou do Portal
R25	Alerta para alunos	P1.A9 P1.A10, P1.A14	A.12.1.1, A.12.4.1				Falhas do Portal
R26	Lançamento de notas de exame	P1.A10, P1.D11	A.8.1.3, A.12.4.1, A.8.2.3, A.12.1.1				Falhas do RUC ou do Portal
R27	Intervenção formal da Presidência	P1.A10, P1.A13a, P1.A13b, P1.D12b	A.12.1.1, A.12.4.1				Falhas da PR
R28	Notas lançadas	P1.A14	A.8.1.2, A.12.3.1				Falhas da PR, do RUC ou do Portal
R29	Fundamentação da alteração de notas	P1.A14	A.8.1.3, A.12.4.1, A.8.2.3, A.12.1.1				Falhas do RUC ou do Portal
R30	Registo	P1.A1, P1.A2, P1.A3, P1.A4, P1.A5 P1.A7, P1.A8 P1.A9, P1.A10, P1.A11a, P1.A11b, P1.A12b, P1.A13a, P1.A13b, P1.A14, P1.D1, P1.D2, P1.D3, P1.D4, P1.D5, P1.D6, P1.D7, P1.D8, P1.D9, P1.D10, P1.D11, P1.D12a, P1.D12b	A.12.4.2, A.12.4.3				Falhas do Portal

Página de documento da AENOR sobre análise de risco (OM2)

pela sistematização da aplicação de metodologias e ferramentas adequadas e definidas no âmbito da qualidade.

Assim, em razão das evidências apresentadas e suportada nos resultados globais da auditoria, o auditor recomenda que seja mantida a certificação para o sistema de gestão da qualidade do ISEP.

Pontos Fortes

Como pontos fortes da organização e sistema de gestão a equipa auditora reforça e destaca os seguintes aspectos, à parte dos formalizados em anteriores relatórios de auditoria:

- Ênfase da Presidência nos resultados;
- O envolvimento dos gestores de processo no exercício de revisão pela gestão;
- As iniciativas de envolvimento dos colaboradores (ex. pequenos almoços temáticos);
- Os esforços evidenciados ao nível da desmaterialização do serviço ao estudante (e processos internos) via o Portal;
- A consolidação de práticas e actividades dos processos do SGQ;
- Plano e relatório de actividades do ISEP;
- Dinâmica de melhoria (ex. ao nível das funcionalidades do Portal, projecto de implementação de sondagens como complemento aos inquéritos de avaliação, "incursões" do Gabinete de Orientação no apoio aos colaboradores, etc)

Oportunidades de Melhoria:

Como complemento às constatações de observação, identificadas nos pontos seguintes deste relatório, a equipa auditora da LUSAENOR identificou as seguintes oportunidades de melhoria:

OM1 – Os indicadores e metas incluídas no plano de medição e monitorização dos processos poderiam distinguir as situações que reflectem padrões ou níveis de serviço (necessários para se ir de encontro aos requisitos do serviço), mais adequadas à monitorização do desempenho dos processos que à promoção de melhoria;

OM2 – Poderia ser realizado um exercício estruturado e completo de avaliação de riscos para a segurança da informação (ex. utilizando as recomendações do Anexo A da ISO 27001);

OM3 – Ponderar a inclusão, no processo de gestão de sistemas e infraestruturas informáticas, da gestão das páginas Web do ISEP e de serviços incluídos no âmbito da certificação (ex. actualização e aprovação de conteúdos, permissões, etc), a qual foi evidenciada mas não é visível no âmbito do SGQ;

OM4 – O plano de actividades poderia incluir, na ausência de outro suporte documental, as metodologias e critérios associados ao seu acompanhamento, monitorização, avaliação e fecho;

Observações:

São constatadas diversas observações, a merecer a análise da Escola de forma a avaliar o risco associado e o custo/benefício de desencadear acções correctivas:

OBS1 – Ainda que evidenciada a efectiva implementação da generalidade das acções associadas à NC1 do anterior relatório de auditoria da LUSAENOR, constataram-se acções ainda em curso (ex. formalização de contrato para manutenção de extintores);

OBS2 – Os resultados da revisão pela gestão deveriam ser inequívocos quanto às conclusões da gestão de topo sobre o grau de definição, implementação e adequação dos processos e do SGQ;

OBS3 – O procedimento de suporte à actividade de formação deveria incluir a possibilidade de se estabelecer métodos e/ou momentos não standard para a avaliação da eficácia das acções de formação, caso se constate apropriado face à natureza ou objectivos específicos das mesmas;