Definição de Política de Segurança Informática no IPCB

Joaquim Manuel Pires dos Santos

Orientador

Prof. Doutor Osvaldo Arede dos Santos

Dissertação apresentada à Escola Superior de Tecnologia do Instituto Politécnico de Castelo Branco para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Desenvolvimento de Software e Sistemas Interativos, realizada sob a orientação científica Professor Doutor Osvaldo Arede dos Santos, do Instituto Politécnico de Castelo Branco.

março de 2016

Composição do júri

Presidente do júri

Prof. Doutor, Fernando Reinaldo Silva Garcia Ribeiro

Vogais

Prof. Doutor, Pedro Ricardo Morais Inácio

Professor Auxiliar, Universidade da Beira Interior

Prof. Doutor, Vasco Nuno da Gama de Jesus Soares

Professor Adjunto, Escola Superior de Tecnologia de Castelo Branco

Dedicatória

À minha esposa Ana Martinho e filha Inês Santos

Agradecimentos

A todos os familiares e amigos que me acompanharam, motivaram e encorajaram na realização deste trabalho, especialmente a minha esposa e filha pela paciência e apoio dado.

Um agradecimento especial ao meu orientador, pelo seu trabalho, incentivo e apoio.

Resumo

Nos dias de hoje, os sistemas de informação são essenciais ao bom funcionamento das instituições, existindo uma dependência crescente entre o bom funcionamento das instituições e o normal funcionamento dos sistemas de informação e infraestruturas de comunicações. As ameaças contra a disponibilidade, integridade e confidencialidade destes sistemas informáticos podem resultar em situações altamente prejudiciais para o normal funcionamento das instituições.

A utilização de políticas de segurança ajuda na identificação das áreas de responsabilidade dos utilizadores, administradores de sistemas e da gestão da instituição. As políticas de segurança devem fornecer um enquadramento para a implementação de mecanismos de segurança, definir procedimentos de segurança adequados, processos de auditoria à segurança e estabelecer uma base para procedimentos legais na sequência de eventos relevantes.

Para a elaboração da política de segurança da informação do IPCB, foram analisadas algumas metodologias utilizadas na área da gestão de segurança da informação, nomeadamente a ISO 27000, COBIT e ITIL. Em seguida, foi efetuada uma comparação entre as diversas metodologias de forma a identificar aquela que mais se adequava à realização deste trabalho, concluindo-se que as orientações da norma ISO 27002 eram as que mais se ajustavam.

Após a análise do funcionamento dos sistemas de informação do IPCB, foram identificadas as áreas que deveriam ser incluídas na elaboração de uma política de segurança.

Finalmente, foi redigida a política de segurança da informação, de acordo com as indicações da norma ISO 27002, ajustada aos requisitos do IPCB.

Palavras chave

Segurança Informática, Política de Segurança, Sistema de Gestão de Segurança da Informação.

Abstract

Information systems are nowadays essential for the proper functioning of the institutions. There is a growing dependence on the normal operation of the information systems and communications infrastructure. The threats to the availability, integrity and confidentiality of these information systems can result in highly harmful situations for the normal functioning of those institutions.

The use of security policies helps identifying the areas of responsibility of users, system administrators and the institution's management. Security policies should provide a framework for the implementation of security mechanisms, define appropriate security procedures, audit security processes and establish a basis for legal proceedings in the sequence of relevant events.

In order to create an information security policy for the IPCB, some methodologies usually used in the area of information security management have been studied, including ISO 27000, COBIT and ITIL. A comparison between these methodologies has been made, in order to identify the best for this work. The guidelines of the ISO 27002 standard were considered the most suitable.

After an analysis of the IPCB information system's functioning, the areas that should be included in the development of a security policy were identified.

Finally, the information security policy has been written, according to the indications of the ISO 27002 standard, adjusted to the IPCB's requirements.

Keywords

Security Computing, Security Policy, Information Security Management Systems.

Índice geral

Índice de figuras

Lista de tabelas

Lista de abreviaturas, siglas e acrónimos

COBIT – Control Objectives for Information and related Technology

IEC - International Electrotechnical Commission

IPCB – Instituto Politécnico de Castelo Branco

ISACA – Information Systems Audit and Control Associations

ISO - International Organization for Standardization

ITIL – Information Technology Infrastructure Library

OGC – Office of Government Commerce

SGSI – Sistema de Gestão de Segurança da Informação

SI – Serviços de Informática

1. Introdução

Neste capítulo é apresentado o contexto do trabalho, a motivação que originou a escolha deste tema e explicados os objetivos concretos do trabalho. É também apresentada a planificação do trabalho e explicada a estrutura da dissertação.

1.1. Contexto e Motivação

Os sistemas de informação são, nos dias de hoje, uma das partes mais importantes e essenciais ao bom funcionamento das instituições (Imboden et al., 2013). Existe, progressivamente, uma dependência entre a atividade das instituições e o normal funcionamento dos sistemas de informação e infraestruturas de comunicações. As ameaças contra a disponibilidade, integridade e confidencialidade dos sistemas podem resultar em situações prejudiciais para o normal funcionamento das mesmas (Solomon & Kim, 2013).

Neste sentido, torna-se fundamental a definição de um Sistema de Gestão de Segurança da Informação (SGSI), através do qual se consigam minimizar danos que possam ser causados pela má utilização dos sistemas, ou pela interpretação errada dos procedimentos a adotar. Assim, o SGSI deve ter definidas políticas de segurança (Disterer, 2013).

As políticas de segurança devem identificar claramente as áreas de responsabilidade dos utilizadores, administradores de sistemas e direção, devendo adaptar-se às alterações que possam existir na organização. As políticas de segurança devem fornecer um enquadramento para a implementação de mecanismos de segurança, definir procedimentos de segurança adequados, processos de auditoria à segurança e estabelecer uma base para procedimentos legais na sequência de ataques (Astani, 2012).

As políticas de segurança devem incluir as intenções e prioridades no que diz respeito à proteção dos sistemas de informação, "*An IS security policy includes the intentions and priorities with regard to the protection of the IS, usually referred to as security objectives, together with a general description of the means and methods to achieve these objectives*", (Karyda et al. 2005, p. 247).

De acordo com o *Request for Comments* (RFC) 2196 (B. Fraser, 1997) uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores.

O ensino superior contém uma grande concentração de pessoas com conhecimentos informáticos, que têm a liberdade e incentivo para explorar tecnologias de ponta. O acesso à Internet, correio eletrónico, e os dispositivos pessoais tornaram-se "críticos" para os administradores de sistemas informáticos. Ao mesmo tempo, existem preocupações crescentes sobre compromissos, internos e externos, de informações sensíveis e confidenciais. Estas preocupações levam à seguinte questão:

Quais as questões políticas que as universidades enfrentam na melhoria da segurança e da privacidade no campus (Manson, 2008)?

O Instituto Politécnico de Castelo Branco (IPCB) é uma instituição de ensino superior com sensivelmente 5000 utilizadores, com diferentes perfis de acesso. Nos últimos anos a infraestrutura de rede e dados do IPCB sofreu um rápido crescimento, tanto no número de dispositivos que se ligam à rede como no número de aplicações utilizadas, sem que tenham sido definidas políticas na área da segurança da informação.

Sendo a segurança também uma questão cultural, cabe às instituições de ensino a responsabilidade de promover uma cultura de utilização responsável das tecnologias de informação. "A academia tem um papel fundamental a desempenhar na liderança do esforço para manter o ciberespaço" (Davidson, 2005).

Uma vez que existe uma grande dependência dos sistemas informáticos no funcionamento do IPCB, torna-se necessário implementar políticas de segurança informáticas de modo a aumentar a confiança no sistema e a resistência da infraestrutura informática do IPCB às ameaças de segurança.

1.2. Objetivos do Trabalho

Os sistemas de informação são, nos dias de hoje, um dos pilares de qualquer empresa ou instituição, desta forma torna-se necessária a utilização de mecanismos que garantam os três princípios básicos no que se refere à segurança da informação: confidencialidade, integridade e disponibilidade.

Neste projeto foi realizado, inicialmente, um estudo sobre normas e boas práticas na área da gestão de segurança da informação. Com este estudo pretende-se identificar áreas que devam ser incluídas na implementação de um modelo de gestão da segurança de informação.

Após essa análise, foi efetuada uma avaliação do atual funcionamento dos sistemas de informação no IPCB, de modo a ser possível definir e implementar políticas de segurança onde constem regras e orientações, que garantam um bom funcionamento desses sistemas de informação.

Pretende-se com este projeto definir e implementar políticas, padrões e orientações nas seguintes áreas:

- Segurança da informação;
- Utilização dos meios tecnológicos existentes;
- Controlos de acesso à informação;
- Identificação e atribuição de responsabilidades.

Estas políticas e orientações devem estar de acordo com o definido nos procedimentos do sistema de gestão da qualidade em funcionamento no IPCB, uma vez que a instituição tem certificação ISO 9001.

Com a implementação das políticas definidas antevê-se uma melhoria nos serviços prestados, em termos de confidencialidade, integridade e disponibilidade dos dados.

1.3. Cronograma

A realização deste projeto envolveu as tarefas apresentadas no diagrama de Gantt, representado nas Figuras 1 e 2.

	Task Name	Duratio	Start	Finish	Predecessors
1	Efetuar uma revisão de literária	90 days	Wed 04-02-15	Tue 09-06-15	
2	Realizar uma análise à Instituição	30 days	Wed 10-06-15	Tue 21-07-15	1
3	Definir os Objectivos da Politica	7 days	Wed 22-07-15	Thu 30-07-15	2
4	Definir metodologia da avaliação de riscos	30 days	Fri 31-07-15	Thu 10-09-15	3
5	Elaborar o Plano de tratamento de riscos	15 days	Fri 11-09-15	Thu 01-10-15	4
6	Definir como medir a eficiência dos controlos	7 days	Fri 02-10-15	Mon 12-10-15	5
7	Escrever a Política	30 days	Tue 13-10-15	Mon 23-11-15	6
8	Implementar os controlos e procedimentos	70 days	Tue 24-11-15	Mon 29-02-16	7
9	Implementar ações corretivas e preventivas	70 days	Tue 24-11-15	Mon 29-02-16	7
10	Escrever a dissertação	239 days	Wed 01-04-15	Mon 29-02-16	

Figura 1 — Tarefas a realizadas

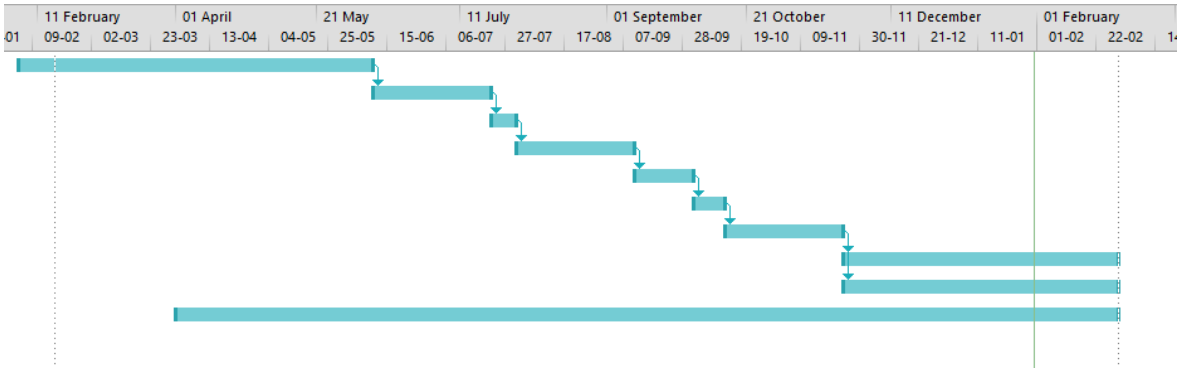

Figura 2 — Diagrama de Gantt

As tarefas definidas foram desenvolvidas de acordo com os seguintes aspetos:

Tarefa 1: Consiste numa pesquisa e estudo de normas, boas práticas e recomendações na área de segurança da informação. Para além de identificar que normas e boas práticas existem, foi necessário compreender o seu funcionamento, tendo sido estabelecido um período mínimo 90 dias.

Tarefa 2: Análise e estudo da instituição, de modo a conhecer a estrutura e sistemas em funcionamento. Esta tarefa teria, no mínimo, a duração de 30 dias.

Tarefa 3: Tendo em consideração o tipo de instituição, identificada na tarefa anterior, definir os objetivos esperados da política. Esta tarefa teria a duração de 7 dias.

Tarefa 4: Nesta tarefa devem ser definidas as regras para a identificação de ativos, vulnerabilidades, ameaças, impactos e probabilidade, e definir o nível de risco aceitável. Dada a importância desta tarefa a mesma deveria ter uma duração mínima de 30 dias.

Tarefa 5: O objetivo desta tarefa é definir como os controles da política devem ser implementados – quem irá fazer o trabalho, quando, com que orçamento etc. A realização desta tarefa deveria ser de 15 dias.

Tarefa 6: Esta tarefa irá servir para definir a forma como medir o cumprimento dos objetivos definidos. A duração esperada para esta tarefa será de 7 dias.

Tarefa 7: Com base nas tarefas anteriores, nesta tarefa irá ser escrita a política de segurança, definindo o que se deseja alcançar e como o controlar. A execução desta tarefa deveria ter a duração de 30 dias.

Tarefa 8: Esta tarefa envolve a aplicação das políticas anteriormente definidas, podendo implicar a implementação de novos comportamentos na instituição. Esta tarefa deveria passar a ser aplicada continuamente, caso a gestão da instituição assim o entenda.

Tarefa 9: Esta tarefa serve para assegurar que tudo o que está errado (inconformidades) seja corrigido ou, de preferência, prevenido. Esta tarefa deveria passar a ser aplicada continuamente, caso a gestão da instituição assim o entenda.

Tarefa 10: Com base em todas as tarefas anteriores, a dissertação será redigida. Esta tarefa começaria a ser realizada durante a execução da primeira tarefa e até ao final das restantes.

1.4. Estrutura da Dissertação

No primeiro capítulo, correspondente à introdução, são apresentados o contexto, motivação, objetivos e cronograma do projeto.

No segundo capítulo, será apresentado o estudo que procurou reunir informações sobre as principais metodologias na área dos sistemas de gestão e segurança de informação.

No terceiro capítulo, é feita uma análise de requisitos baseando-se na estrutura e funcionamento do IPCB.

No quarto capítulo, é elaborada uma proposta de política de segurança.

No quinto capítulo é apresentada a conclusão deste trabalho.

2. Gestão e Segurança da Informação

Quando se aborda o tema de gestão e segurança da informação, existem algumas metodologias que nos podem guiar/ orientar na sua implementação.

Neste capítulo é realizado um estudo sobre as principais metodologias na área dos sistemas de gestão e segurança de informação.

2.1. Conceitos Essenciais de Segurança da Informação

O mundo atual encontra-se interligado (interconectado), nele as ações individuais e coletivas podem resultar em boas ações ou causar danos. O objetivo da segurança da informação é proteger a economia, a infraestrutura crítica e o país de atos que podem ser resultado do uso indevido, acidental ou intencional, e que possam comprometer ou destruir a informação ou os sistemas de informação (Greene, 2014).

As organizações devem possuir sistemas de gestão que assegurem a segurança da informação, dada a sua importância (Karyda et al., 2005). Na implementação de um SGSI, deve ser definido um sistema de políticas de segurança da informação, existindo vários fatores (leis e regulamentos, o tipo da informação, os processos) que influenciam a escolha das políticas a adotar. No entanto, após criadas as políticas, existem desafios a enfrentar na aplicação das mesmas, podendo estes ser de cariz técnico ou humano. É essencial que na fase de implementação das políticas exista um bom sistema de gestão, mas também aceitação das mesmas pelos colaboradores da instituição. Uma boa política vale pouco se ninguém a seguir. Neste sentido é essencial o apoio da gestão de topo, de modo a garantir a implementação e cumprimento das políticas de segurança a serem adotadas (Ghormley, 2006).

Robert Johnson (Johnson 2014, p. 2) refere que "*A good definition of information system security (ISS) is the act of protecting information and systems that store and process it.*". Uma boa definição de um sistema de segurança da informação é o ato de proteger informação e os sistemas que a armazenam e processam, referindo que esta proteção é contra os riscos que levariam ao acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição de informações.

Ao elaborar um sistema de segurança é necessário ter em consideração o que são políticas, padrões e orientações (p*olicy, standard or guideline*) (SANS, 2013).

A **política** é um documento que descreve os requisitos ou regras específicas que devem ser cumpridas. No domínio das redes de computadores e segurança da informação, as políticas são geralmente específicas de uma determinada área.

O **padrão** é um conjunto de requisitos específicos que devem ser cumpridos. Por exemplo, pode ter-se um padrão que descreve como proceder de modo a associar um servidor a uma rede de uma zona exclusiva (DMZ).

A **orientação** é um conjunto de sugestões específicas para as melhores práticas. Não é obrigatório que as orientações sejam cumpridas, mas são fortemente recomendadas.

As políticas de segurança eficazes fazem frequentemente referências às normas e orientações definidas.

David Kim e Michael G. Solomon (Solomon & Kim 2013, p. 6) referem que para se compreender como aumentar a segurança dos sistemas é necessário perceber os riscos, ameaças e vulnerabilidades.

A **ameaça** é qualquer ação que possa prejudicar um ativo, podendo ser ameaças naturais ou induzidas pelo homem. Ameaças naturais tais como inundação, sismo, ou tempestades severas, exigem que as organizações tenham planos que assegurem a continuidade do negócio enquanto a organização recupera. Um plano de continuidade de negócios (*business continuity plan*) dá prioridade às funções que a organização precisa para continuar as operações se um local de negócios for afetado por diferentes níveis de desastre (Omar et al., 2011). Um plano de recuperação de desastres (*disaster recovery plan*) define o processo ou conjunto de procedimentos para recuperar e proteger a infraestrutura de Tecnologia de Informação (TI) em caso de um desastre (Omar et al., 2011). As ameaças causadas por humanos podem ser vírus (código malicioso) e acesso não autorizado.

A **vulnerabilidade** é uma fraqueza que permite que uma ameaça seja materializada ou que tenha efeito sobre um ativo. Uma ameaça por si só nem sempre causa danos, no entanto, tem de existir uma vulnerabilidade para que a ameaça seja materializada.

O **risco** é a probabilidade de que algo prejudicial vai acontecer com um ativo. É a exposição a um evento que venha a ter um efeito sobre um ativo. No contexto de segurança de TI, um ativo pode ser um computador, uma base de dados ou uma parte da informação. Exemplos de risco: perda de dados; perda de negócio por causa de um desastre que destrua o edifício da empresa; não cumprimento das leis e regulamentos. O risco é o resultado da combinação da ameaça com a vulnerabilidade.

Num estudo publicado no "*International Journal of Information Security and Privacy*" (Yadav, 2010), Surya B. Yadav elaborou uma tabela (Tabela 1), com base na publicação de vários autores, onde apresenta um resumo de cinco métodos utilizados em sistemas de segurança. Nessa tabela, para além das etapas, existentes em cada método, são ainda apresentadas as coberturas e as orientações que cada método dá para a determinação dos requisitos de segurança.

Tabela 1 — Métodos, coberturas e orientações utilizados em sistemas de segurança

Métodos e Fases	Cobertura e requisitos	Orientações
Security Systems Development Life Cycle (SecSDLC): 1. Investigação 2. Análise 3. Projeto lógico 4. Projeto físico 5. Implementação e mudança	As duas primeiras fases lidam com requisitos de segurança. Incluem as Sub-etapas: 1. Documentação e análise das políticas de segurança existentes 2. Analisar as ameaças e controlos atuais 3. Examinar as questões jurídicas 4. Realizar a análise de risco	São especificadas as diferentes categorias de ameaças, tais como: atos de erro humano, propriedades intelectuais e falhas técnicas. São discutidos diferentes tipos de, questões éticas e profissionais do direito. São ainda analisados os vários tipos de ativos, tais como: empregados/ não empregados, procedimentos de informação e *software*.
Systematic Approach to Developing Security Architectures: 1. Desenvolver o modelo do processo de negócio 2. Estabelecer os objetivos do projeto de segurança 3. Selecionar e enumerar subsistemas de segurança 4. Documentar a arquitetura de segurança e integra-la na arquitetura da solução geral	As duas primeiras fases lidam com a planificação de objetivos de segurança.	São especificados os perigos para os fluxos de processos de TI. *Few guidelines are provided to identify information assets and security requirements. Guidelines are not comprehensive.*
Plan-Do-Check-Act (PDCA): 1. Estabelecer o sistema de gestão de segurança da informação (SGSI) 2. Implementar e operar o SGSI 3. Acompanhar e analisar o SGSI 4. Manter e melhorar o SGSI	Os riscos e políticas de segurança são identificados e avaliados durante a fase de plano. Após determinados os requisitos de segurança, é utilizada como especificação a ISO/IEC 17799: 2005 [1].	O processo PDCA assume que os requisitos de segurança já são conhecidos. *No guidelines for security requirements determination are provided.*
Structured Security Analysis and Design: 1. Criar um modelo físico do sistema existente 2. Produzir um modelo lógico do sistema existente 3. Introduzir mecanismos de fiscalização no modelo lógico 4. Criar novo modelo lógico do novo sistema 5. Adicionar uma referência cruzada para controlar cada entrada do dicionário de dados	As atividades de segurança, tais como identificar entidades, identificar riscos e identificar os controlos são explicitamente integrados nos sistemas de análise e criação do método estruturado.	Três classes de risco - a divulgação, modificação e destruição. As ideias de controlos de dados e processos são usadas para ajudar a identificar os requisitos de segurança. *Identification of entities is left to the Structured Analysis method which does not provide any guideline for identifying security-related entities. Guidelines are incomplete. Focus is mainly on data and process controls.*

[1] Atualizada para numeração ISO/IEC 27002 em julho de 2007

Data Control Life Cycle Methodology: 1. Identificar exposição 2. Avaliar o risco 3. Seleção de controlos 4. Analisar custo/eficácia	A primeira fase lida com as necessidades de segurança. A abordagem define seis grupos de exposição de dados: divulgação acidental, divulgação intencional, modificação acidental, modificação intencional, destruição acidental e destruição intencional.	Estão definidos onze pontos de controlo de dados (CPS) para ajudar a identificar os requisitos de segurança. Cada dado é verificado por seis tipos de exposição em cada ponto de controlo de dados. *The identification process using data exposure and control point is quite extensive. However, it is physically oriented [Baskerville 1988]. The guidelines are limited to only data exposure. They are technical in nature. The guidelines are not comprehensive.*

2.2. Família de Normas ISO 27000

A ISO 27000 é a norma internacional que define os conceitos de tecnologias de informação (*Information technology*) – técnicas de segurança (*Security techniques*) – sistemas de gestão e segurança da informação (*Information security management systems*) e descrições e vocabulário (*Overview and vocabulary*) (ISO/IEC, 2014).

Esta norma ISO fornece uma visão geral do sistema de gestão de segurança da informação (SGSI), e dos termos e definições normalmente utilizados em normas da família do SGSI. A norma é aplicável a qualquer tipo de organização, independentemente da sua tipologia e dimensão (por exemplo, empresas comerciais, agências governamentais, organizações não-lucrativas).

As normas da família ISO 27000 definem políticas de segurança, linhas de orientação e gestão do risco, que se aplicam na implementação de um SGSI e são compostas por várias normas internacionais, sob o título geral de tecnologia da informação, das quais se destacam:

ISO 27000: Vocabulário e definições a serem utilizadas pelas restantes normas;

ISO 27001: Define os requisitos para a implementação de um SGSI;

ISO 27002: Define as boas práticas para a gestão da segurança da informação;

ISO 27003: Guia para a implementação de um SGSI;

ISO 27004: Define as métricas e meios de medição para avaliar a eficácia de um SGSI;

ISO 27005: Define linhas de orientação para a gestão do risco da segurança da informação.

Através do uso desta família de normas, pode desenvolver-se e implementar uma estrutura para gerir a segurança dos ativos de informação, incluindo informações

financeiras, a propriedade intelectual e detalhes do funcionário, ou a informação que lhe é permitida.

A Figura 3 mostra as inter-relações das normas na família 27000, separadas em requisitos e orientações.

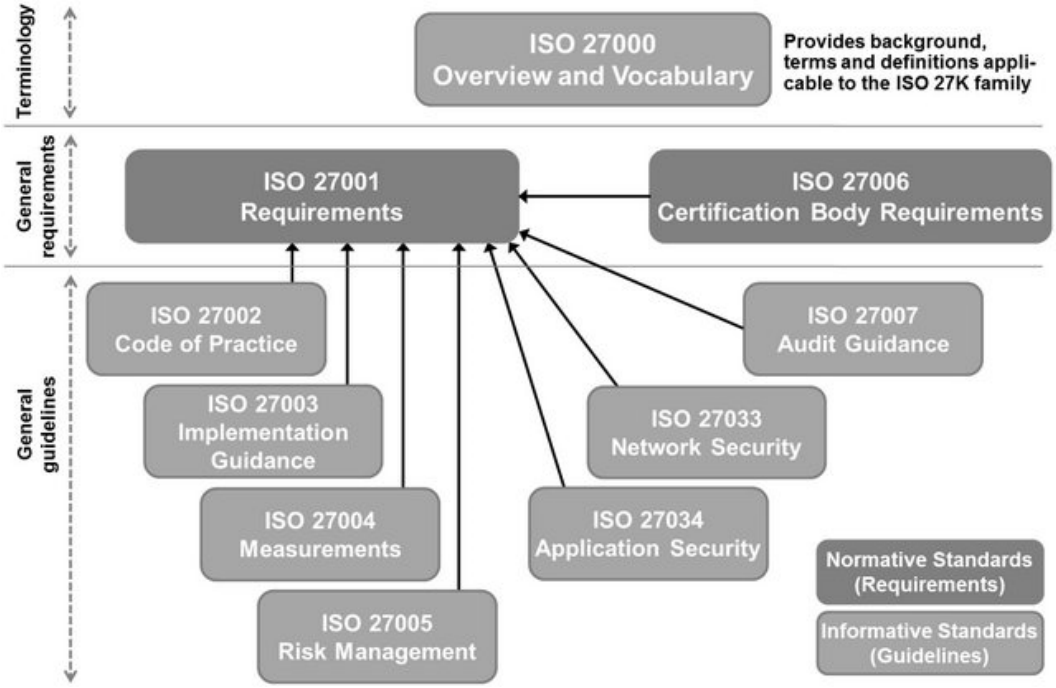

Figura 3 — Relações entre as normas da família da ISO 27000 (Disterer, 2013)

2.2.1. ISO 27000

De forma a evitar diferentes interpretações é necessária a definição clara de um vocabulário, que neste caso é definido na ISO 27000. De seguida são apresentados alguns dos termos definidos por esta norma (ISO/IEC 27000, 2014).

2.1 Controlo de acesso: meios para assegurar que o acesso aos bens é autorizado e limitado com base em requisitos de negócios e de segurança.

2.3 Ataque: tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado ou a utilização não autorizada de um ativo.

2.4 Atributo: propriedade ou característica de um objeto que pode ser distinguido quantitativa ou qualitativamente por meios humanos ou automatizados.

2.5 Auditoria: processo sistemático, independente e documentado para a obtenção de evidência de auditoria e avaliá-la objetivamente para determinar a extensão do cumprimento dos critérios de auditoria.

2.7 Autenticação: prestação de garantia de que uma característica reivindicada por uma entidade é correta.

2.8 Autenticidade: propriedade que comprova que uma entidade é o que diz ser.

2.9 Disponibilidade: propriedade de ser acessível e utilizável por uma entidade autorizada.

2.12 Confidencialidade: propriedade que a informação não é disponibilizada ou divulgada a pessoas não autorizadas, entidades ou processos.

2.13 Conformidade: cumprimento de um requisito.

2.16 Controlo: meio de gestão de risco.

2.20 Dados: Conjunto de valores atribuídos a medidas de base, medidas derivadas e/ou indicadores.

2.24 Eficácia: medida em que as atividades planeadas são realizadas e os resultados planeados são alcançados.

2.40 Integridade: propriedade de plenitude de exatidão.

2.60 Políticas: intenções e estratégia de uma organização, expressas pela administração.

2.61 Processo: conjunto de atividades inter-relacionadas que transforma entradas (*inputs*) em saídas (*outputs*).

2.62 Confiabilidade: propriedade de comportamento e resultados consistentes.

2.63 Requisito: expectativa ou necessidade expressa, geralmente implícita ou obrigatória.

2.68 Risco: efeito da incerteza sobre os objetivos.

2.83 Ameaça: causa potencial de um incidente indesejado, que pode resultar em danos para um sistema ou organização.

2.89 Vulnerabilidade: fraqueza de um ativo ou controlo que pode ser explorado por uma ou mais ameaças.

2.2.2. ISO 27001

A norma ISO 27001 é o padrão e a referência internacional para a gestão da segurança da informação. A mesma tem vindo, de forma continuada, a ser melhorada ao longo dos anos, sendo que a versão mais recente desta norma foi publicada em 2013, tendo sido desenvolvida com base na Norma Britânica BS7799-2 (Disterer, 2013).

Esta norma foi preparada para fornecer os requisitos que permitem estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação. A adoção de um SGSI é uma decisão estratégica da organização.

A criação e implementação de um SGSI é influenciada por necessidades, objetivos e requisitos de segurança da organização, assim como, os processos organizacionais utilizados e a dimensão e estrutura da organização. É expectável que todos estes fatores que influenciem o SGSI sofram alterações ao longo do tempo. Uma vez que esta

norma define o sistema de gestão da segurança da informação (SGSI) é possível obter certificação para a ISO 27001.

O SGSI preserva a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão de risco e transmite confiança às partes interessadas de que os riscos são adequadamente geridos. Isto é realizado através da identificação dos potenciais problemas que podem ocorrer (avaliação de risco), e definindo o que deve ser feito para prevenir que esses problemas aconteçam (tratamento de risco).

Esta norma tem como princípio geral a adoção, pela organização, de um conjunto de requisitos, processos e controlos com o objetivo de reduzir/ gerir adequadamente o risco da organização. Desta forma, a gestão da segurança da informação não se refere apenas à segurança em TI (*fierwalls*, antivírus, etc.) mas também à gestão de processos, proteção legal, recursos humanos, proteção física, etc. A ISO 27001 não descreve detalhadamente como deve ser feita a segurança da informação, por exemplo com que frequências devem ser feitas cópias de segurança, que tipo de tecnologias devem ser usadas para a proteção da rede ou como os equipamentos devem estar configurados. O objetivo desta norma é fornecer uma estrutura de modo a que possa ser realizada uma proteção adequada às necessidades da empresa. O modo como se atinge essa adequação é realizado através de uma análise e tratamento de riscos.

A norma ISO 27001 está dividida em 11 seções e num Anexo A. As primeiras secções, de 0 a 3, são secções introdutórias, não sendo obrigatórias para a implementação. Os requisitos das restantes seções, de 4 a 10, são obrigatórios e devem ser implementados. As secções de 4 a 7 fazem parte da etapa de planeamento (*Plan*) do ciclo PDCA, a secção 8 faz parte da etapa de execução (*Do*), a secção 9 da etapa de verificação (*Check*) e a secção 10 da etapa de atuação (*Act*). Os controlos do Anexo A devem ser implementados apenas se declarados como aplicáveis na declaração de aplicabilidade.

De seguida são apresentadas as secções da ISO 27001:

Seção 0: Introdução – explica o propósito da ISO 27001 e sua compatibilidade com outras normas de gestão.

Seção 1: Objetivo (*Scope*) – explica os objetivos que esta norma pretende alcançar.

Seção 2: Referência normativa – refere-se à ISO 27000 como a norma de referência.

Seção 3: Termos e definições – referindo-se à ISO 27000 como a norma onde termos e definições são dados.

Seção 4: Contexto da organização – define requisitos para o entendimento de assuntos externos e internos, partes interessadas e os seus requisitos, além da definição do objetivo do SGSI.

Seção 5: Liderança – define as responsabilidades da "alta direção", estabelecendo papéis e responsabilidades, assim como o conteúdo da política de segurança da informação de alto nível.

Seção 6: Planeamento – define requisitos para a avaliação de risco, tratamento de risco, declaração de aplicabilidade, plano de tratamento de risco, além de definir os objetivos de segurança da informação.

Seção 7: Apoio – define requisitos de disponibilidade de recursos, competências, conscientização, comunicação e controlo de documentos e registos.

Seção 8: Operação – define a implementação da avaliação e tratamento de risco, assim como controlos e outros processos necessários para atingir os objetivos de segurança da informação.

Seção 9: Avaliação do desempenho – define requisitos para a monitorização, medição, análise, avaliação, auditoria interna e análise crítica pela direção.

Seção 10: Melhoria – define requisitos para não conformidades, ações corretivas e melhoria contínua.

Anexo A – este anexo disponibiliza um catálogo de 114 controles (salvaguardas) distribuídos em 14 seções (seções de A.5 até A.18).

Esta norma é implementada tendo como referência as restantes normas da família da ISO 27000 como, por exemplo, a ISO 27005 (gestão do risco) e a ISO 27002 (segurança da informação), sendo que o nível de detalhe é muito menor do que utilizando a norma separadamente. Por exemplo, aquando da aplicação desta norma, na criação do SGSI são definidas orientações para a segurança da informação, também definidas através da aplicação da ISO 27002, no entanto, enquanto na aplicação da ISO 27001 é feita uma breve descrição, na aplicação da ISO 27002 o nível de detalhe dedicado a cada controlo (definidos no Anexo A da ISO 27001) é muito maior.

2.2.3. ISO 27002

Esta norma fornece orientações para a segurança da informação da organização e práticas de gestão de segurança da informação, incluindo a seleção, implementação e gestão de controlo levando em consideração ambiente de riscos de segurança da informação (ISO/IEC 27002, 2013). A ISO 27002 era anteriormente referenciada como ISO/ IEC 17799, tendo surgido a partir da norma Britânica BS 7799-1.

Esta norma é desenhada para ser utilizada para organizações que pretendem:

- Controlos de seleção dentro do processo de implementação de um SGSI, com base na ISO 27001;
- Implementar controlos de segurança da informação geralmente aceites;
- Desenvolver as suas próprias orientações de gestão de segurança da informação.

A segurança da informação é conseguida através da implementação de um conjunto de controlos adequados, incluindo as políticas, processos, procedimentos, estruturas organizacionais, *software* e funções de *hardware*. Esses controlos precisam ser estabelecidos, implementados, monitorizados, revistos e melhorados, de forma a garantir que os objetivos de segurança e de negócios específicos da organização sejam alcançados.

Os três princípios base da segurança da informação são a preservação da **Confidencialidade**, **Integridade** e **Disponibilidade** da informação. Esta norma recomenda controlos de segurança da informação de acordo com os objetivos para segurança da informação resultantes da análise de riscos para a confidencialidade, integridade e disponibilidade da informação.

A norma está estruturada de modo lógico em torno de grupos de controlo de segurança relacionados. A ISO 27002 está dividida em 19 secções (figura 4) e possui 114 controlos.

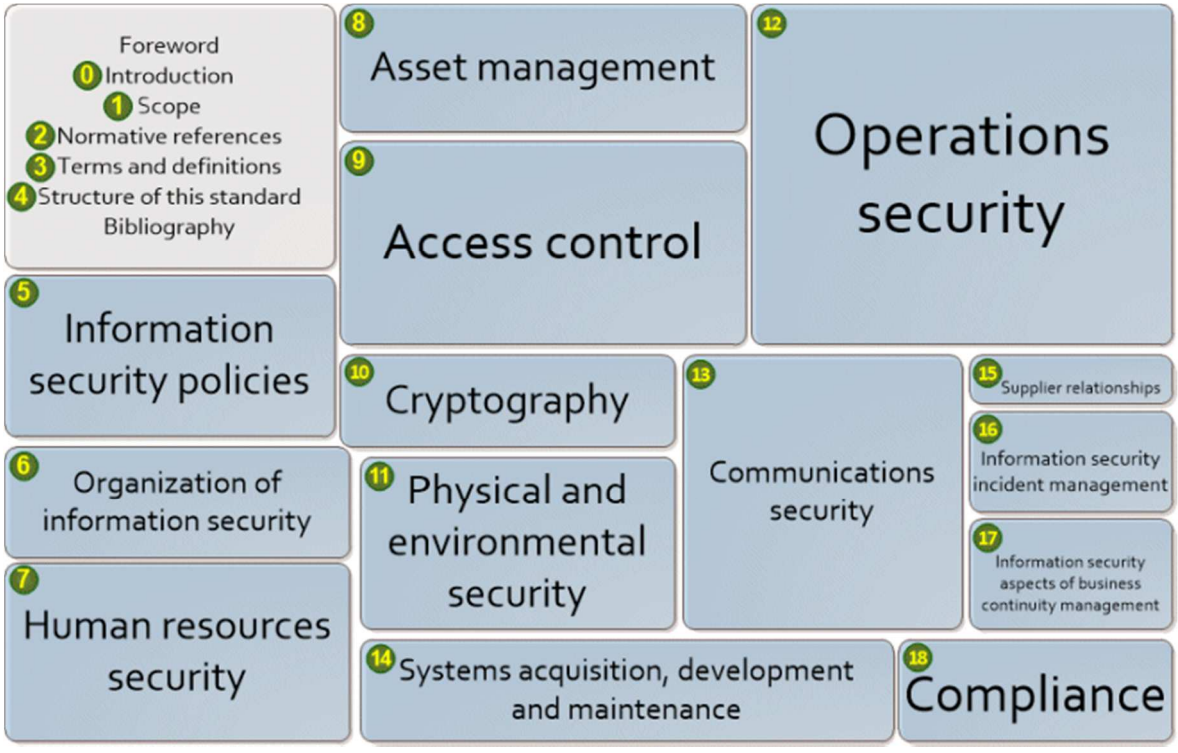

Figura 4 — Secções da ISO 27002 (IsecT, n.d.)

Seção 0: Introdução – explica o propósito da ISO 27002 e a sua compatibilidade com outras normas de gestão.

Seção 1: Objetivo (Scope) – explica os objetivos que esta norma pretende alcançar.

Seção 2: Referência normativa – refere-se à ISO 27000 como a norma de referência.

Seção 3: Termos e definições – referindo-se à ISO 27000 como a norma onde termos e definições são dados.

Seção 4: Contexto da organização – define requisitos para o entendimento de assuntos externos e internos, partes interessadas e os seus requisitos, assim como a definição do objetivo do SGSI.

Seção 5: Políticas de segurança da Informação – orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Seção 6: Organização da segurança da Informação – Estabelecer uma estrutura de gestão, para iniciar e controlar a implementação da segurança da informação dentro da organização.

Seção 7: Segurança em recursos humanos – Assegurar que funcionários e partes externas entendam as suas responsabilidades e estejam em conformidade com os papéis para os quais foram selecionados.

Seção 8: Gestão de ativos – Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos.

Seção 9: Controlo de acessos – Limitar o acesso à informação e aos recursos de processamento da informação e assegurar o acesso a utilizadores autorizados, prevenindo o acesso não autorizado a sistemas e serviços.

Seção 10: Criptografia – Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

Seção 11: Segurança física e do ambiente – Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e as informações da organização.

Seção 12: Segurança nas operações – Garantir a operação segura e correta dos recursos de processamento da informação. Assegurar que as informações e os recursos de processamento da informação estão protegidos contra códigos maliciosos. Proteger contra a perda de dados. Assegurar a integridade dos sistemas operacionais.

Seção 13: Segurança nas comunicações – Garantir a proteção das informações em redes e dos recursos de processamento da informação que os apoiam. Manter a segurança da informação transferida dentro da organização e com quaisquer entidades externas.

Seção 14: Aquisição, desenvolvimento e manutenção de sistemas – Garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação. Garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. Assegurar a proteção dos dados utilizados para teste.

Seção 15: Relacionamento com fornecedores – Garantir a proteção dos ativos da organização que são acessíveis pelos fornecedores. Manter um nível acordado de

segurança da informação e de entrega de serviços em consonância com os acordos com fornecedores.

Seção 16: Gestão de incidentes de segurança da informação – Assegurar um enfoque consistente e efetivo para gerir os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Seção 17: Aspetos da segurança da informação na gestão da continuidade do negócio – É recomendado que a continuidade da segurança da informação seja considerada nos sistemas de gestão da continuidade do negócio da organização. Assegurar a disponibilidade dos recursos de processamento da informação.

Seção 18: Conformidade – Evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas com a segurança da informação e de quaisquer requisitos de segurança.

2.2.4. Conciliação da Norma

Podem ainda ser referidas mais duas normas da família 27000.

A ISO 27033, cujo objetivo é fornecer orientação detalhada sobre os aspetos da gestão e utilização das redes de sistemas de informação, assim como as suas interconexões de segurança. Esta norma deve satisfazer as necessidades dos responsáveis pela segurança da informação em geral e da segurança de rede, em particular (ISO/IEC 27033, 2010).

A ISO 27034, cujo objetivo é auxiliar as organizações na integração do sistema de segurança durante o ciclo de vida das suas aplicações, nomeadamente:

- Fornecendo conceitos, princípios, estruturas, componentes e processos;
- Fornecendo mecanismos orientados para o processo de estabelecimento de requisitos de segurança, avaliar os riscos de segurança, a atribuição de um nível desejado de confiança e selecionando controlos de segurança e medidas de verificação;
- Fornecendo diretrizes para se estabelecerem critérios de aceitação para as organizações de terceirização do desenvolvimento ou operação de aplicativos, e para organizações de compras a partir de aplicativos de terceiros;
- Fornecer mecanismos orientados para o processo de determinação, gerando as provas necessárias para demonstrar que as suas aplicações podem ser usadas de forma segura em um ambiente definido;
- Apoiar os conceitos gerais especificados na norma ISO 27001 e ajudar com a execução satisfatória da segurança da informação com base numa abordagem de gestão de riscos;
- Fornecendo uma estrutura que ajuda a implementar os controlos de segurança especificados na norma ISO 27002 e outras normas.

Tal como acontece noutras metodologias, a família de normas ISO 27000 utiliza como base o modelo "*Plan-Do-Check-Act*", ciclo PDCA (Figura 5), que enfatiza a necessidade de orientação do processo, bem como a integração do planeamento das operações e a verificação constante da execução (Disterer, 2013).

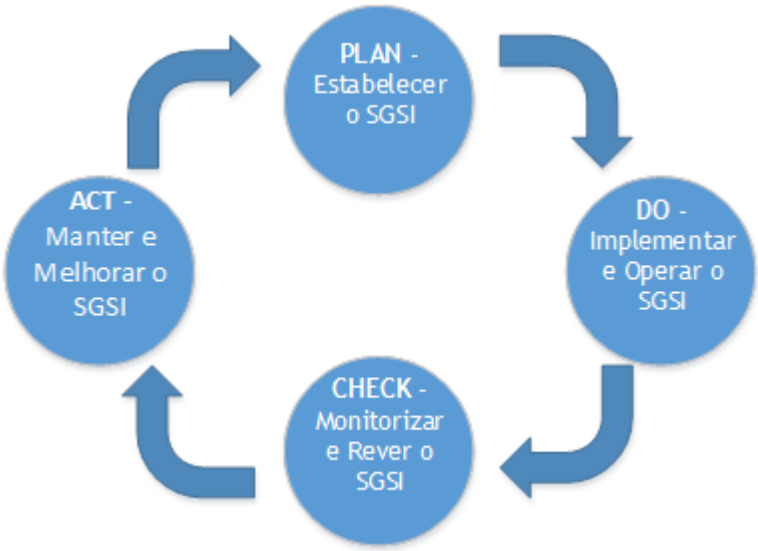

Figura 5 — Modelo PDCA

O SGSI é baseado numa aproximação sistemática dos riscos inerentes aos negócios, com o objetivo de estabelecer, implementar e operar, monitorizar e rever, manter e melhorar a segurança da informação, tratando-se de uma abordagem à segurança da informação numa perspetiva organizacional.

2.3. Metodologia COBIT

A Associação de Controlo e Auditoria aos Sistemas de Informação (*Information Systems Audit and Control Associations – ISACA*) desenvolveu uma *framework* de boas práticas que foi aceite internacionalmente. Esta *framework* é chamada de COBIT – *Control Objectives for Information and Related Technology* (Objetivos de Controlo para Informação Relacionada com Tecnologia), sendo que a primeira versão foi lançada em 1996 e, a última versão, (versão 5.0) em abril de 2012 (Orakzai, 2014).

O COBIT foi lançado em 1996, como uma *framework* para auditoria e controle das TI, com foco nos objetivos de controlo. Quatro anos mais tarde, foi lançada a terceira versão com a inclusão de orientações para a gestão das TI. Em 2005, com o COBIT 4.0, tornou-se numa *framework* de *governance*, com a inclusão de processos de conformidade. Na sua última versão, COBIT 5, evoluiu para uma *framework* integradora de processos de governança e gestão das TI. Na Figura 6 podemos observar a evolução desta *framework*.

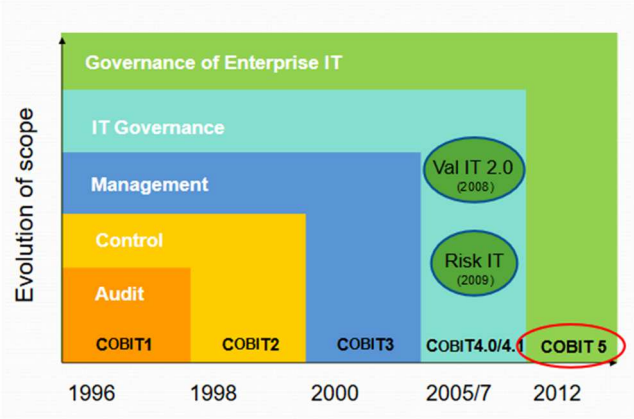

Figura 6 — Evolução do COBIT (Darveau, 2013)

O COBIT é um guia de boas práticas que possui uma série de recursos que podem servir como um modelo de referência para gestão da TI, incluindo um sumário executivo, uma *framework*, objetivos de controlo, mapas de auditoria, ferramentas para a sua implementação e, principalmente, um guia com técnicas de gestão. O COBIT fornece princípios globalmente aceites, práticas, ferramentas e modelos analíticos que ajudam a aumentar a confiança e valor dos sistemas de informação.

As principais caraterísticas do COBIT são:

- Focado no negócio;
- Orientado para o processo;
- Baseado em controlos;
- Direcionado para a medição;
- Inclui inúmeros recursos para implementar a gestão de tecnologias da informação;
- Independente das plataformas de tecnologias da informação adotadas nas empresas.

O COBIT 5 foi desenvolvido tendo em conta uma série de outras normas e padrões, a Figura 7 retrata as áreas e domínios abrangidos pelo COBIT 5, assim como outros padrões e normas.

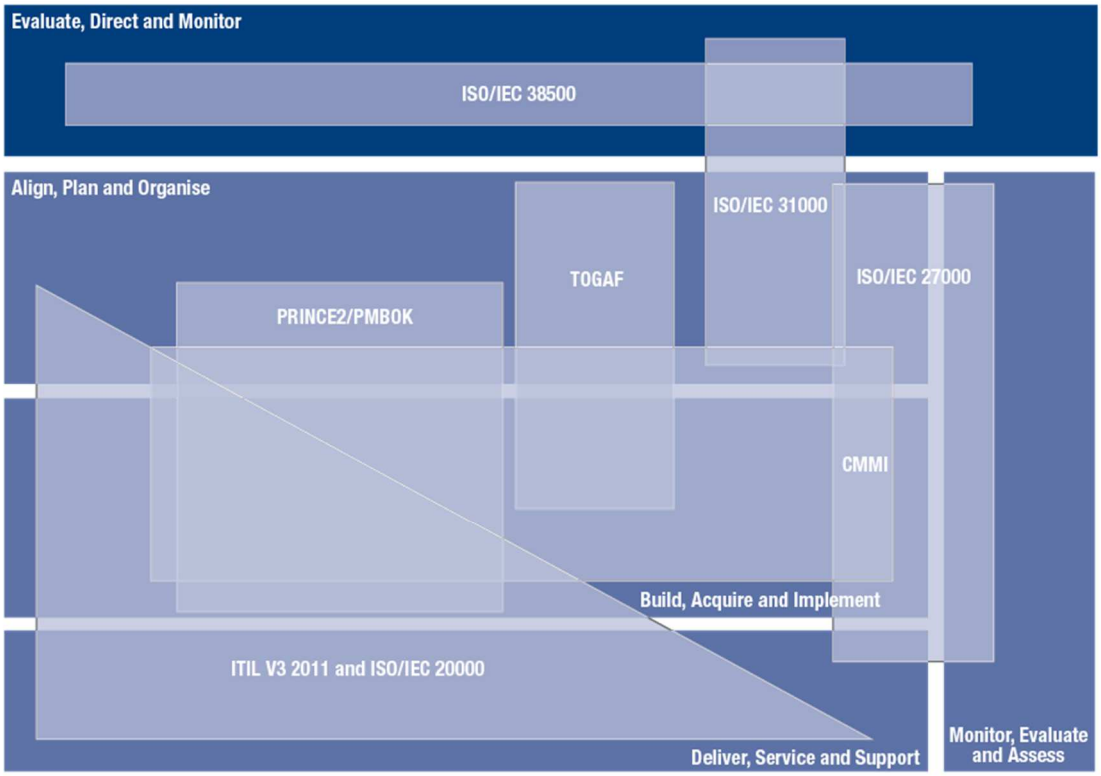

Figura 7 — COBIT 5 cobertura de outras normas e padrões (ISACA, n.d.)

O COBIT define controlo interno como ''... as políticas, procedimentos, práticas e estruturas organizacionais destinadas a fornecer uma garantia razoável de que os objetivos de negócio serão alcançados, e eventos indesejáveis serão evitados ou detetados, e corrigidos.'' (Kerr & Murthy 2013, p. 590). São identificados um conjunto de 34 objetivos de controlo de alto nível agrupados em quatro domínios: Planear e Organizar; Adquirir e Implementar; Entregar e Suporte; Monitorizar e Avaliar.

O novo modelo de referência de processos do COBIT 5 subdivide os processos de TI em duas principais áreas de atividade: processos de governança (*governance*,) e processos de gestão.

O COBIT 5 é baseado em cinco princípios fundamentais (Figura 8) para a gestão estratégica e funcional de TI da empresa.

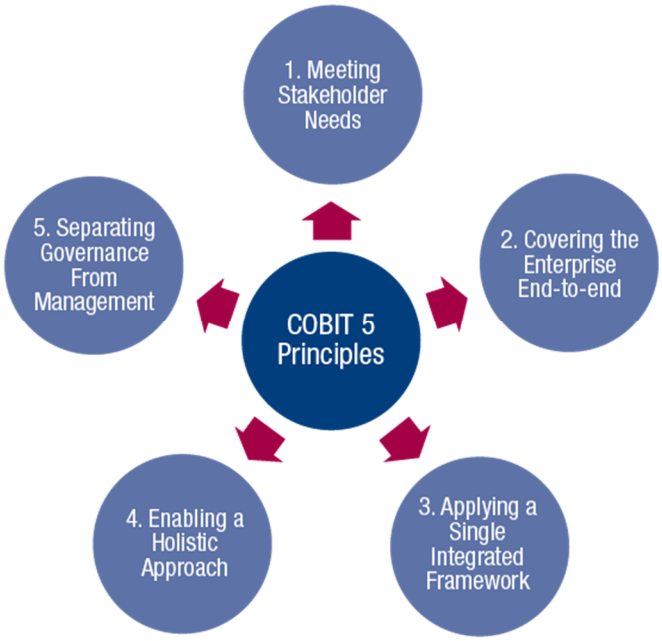

Figura 8 — Princípios do COBIT 5 (ISACA, n.d.)

Princípio 1: Ir de encontro às necessidades dos *Stakeholders*. Como cada empresa tem objetivos diferentes, uma empresa pode personalizar o COBIT para se adequar ao seu próprio contexto, alinhando deste modo os objetivos estratégicos da empresa aos objetivos definidos no COBIT. Com este princípio, e tendo o conhecimento das necessidades das partes interessadas, mais facilmente se consegue a realização de benefícios, a otimização dos riscos e a otimização dos recursos.

Princípio 2: Cobrir a empresa de extremo a extremo (*end-to-end*): abrange todas as funções e processos dentro da empresa; considera todas as informações de gestão relacionadas com TI.

Princípio 3: Aplicar uma única *framework* integrada. O COBIT 5 alinha com outros padrões e estruturas relevantes a um nível elevado e, portanto, pode servir como o quadro de referência para a gestão de TI corporativa.

Princípio 4: Permitir uma abordagem global. O COBIT 5 define um conjunto de facilitadores para apoiar a implementação de um sistema de gestão global de TI. Estão definidas sete categorias de facilitadores: princípios e políticas; processos; estruturas organizacionais; cultura, ética e comportamento; informações; serviços, infraestrutura e aplicações; pessoas e competências.

Princípio 5: Separar a gestão estratégica da funcional. O COBIT 5 faz uma clara distinção entre gestão estratégica e gestão funcional.

O COBIT 5 ajuda as empresas a criar valor para as TI, mantendo o equilíbrio entre os investimentos em recursos e os riscos organizacionais. O COBIT considera os negócios, as áreas funcionais de TI da empresa e as partes interessadas, tanto internas como externas.

A utilização do COBIT 5 proporciona os seguintes benefícios (ISACA, n.d.):

- Informação de qualidade para apoio nas decisões;
- Definição de objetivos estratégicos e benefícios através da eficácia na sua utilização;
- Manutenção dos riscos relacionados com TI num nível aceitável;
- Otimização de custos com serviços de TI;
- Conformidade com leis, regulamentos, acordos contratuais e políticas.

Os facilitadores são fatores que, individual e coletivamente, influenciam o funcionamento do sistema, neste caso, a governação e gestão ao longo de TI da empresa. São movidos por objetivos em cascata, ou seja, as metas de alto nível relacionadas com TI definem o que os diferentes facilitadores devem alcançar.

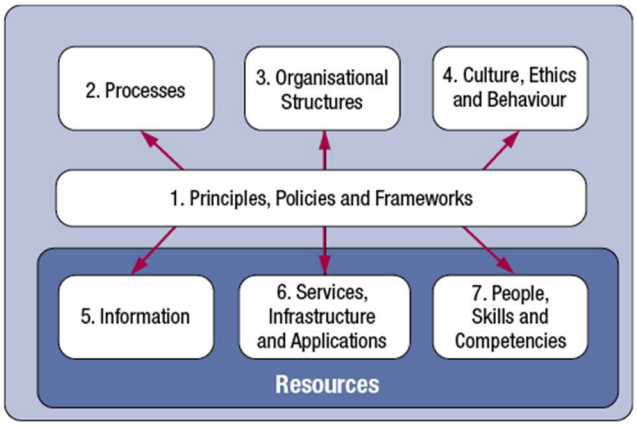

Figura 9 — COBIT 5: Facilitadores (ISACA, n.d.)

O COBIT descreve sete categorias de facilitadores (Figura 9):

- **Princípios, políticas e quadros**: são o veículo para traduzir o comportamento desejado em orientações práticas para a gestão do dia-a-dia.
- **Processos**: descrevem um conjunto organizado de práticas e atividades para atingir determinados objetivos e produzir um conjunto de *outputs* em apoio ao alcance de metas globais relacionadas com as TI.
- **Estruturas organizacionais:** são as entidades de tomada de decisão numa empresa.
- **Cultura, ética e comportamento** dos indivíduos e das empresas, são muitas vezes subestimadas como fator de sucesso em atividades de governança e de gestão.
- **Informações:** necessárias para manter a organização a funcionar com um bom nível de gestão; no nível operacional, a informação é muitas vezes o produto chave da própria empresa.

- **Serviços, infraestrutura e aplicações** (incluindo a infraestrutura, tecnologia e aplicativos): fornecem à empresa os recursos necessários para o processamento e serviços de tecnologia da informação.
- **Pessoas, habilidades e competências**: são necessários para a conclusão bem-sucedida de todas as atividades e para a tomada de decisões corretas e tomada de ações corretivas.

Com a evolução para a versão 5, o COBIT passou a ter 5 domínios e 37 processos (Figura 10).

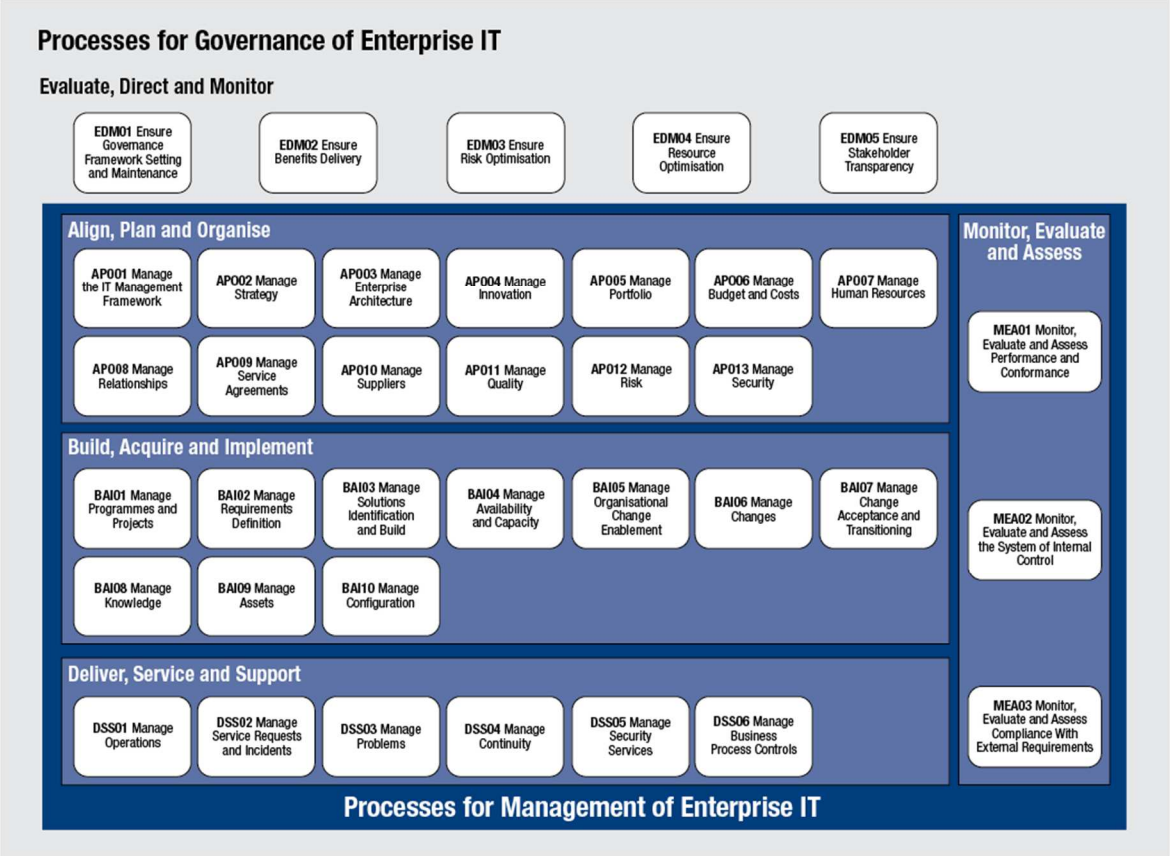

Figura 10 — COBIT 5: Domínios e processos (ISACA, n.d.)

Os processos são:

- Alinhar, Planear e Organizar (*Align, Plan and Organize*) que contém 13 processos;
- Construir, Adquirir e Implementar (*Construct, Acquire and Implement*), que contém 10 processos;
- Entregar, Serviço e Suporte (*Deliver, Service and Support*), que contém 6 processos;
- Monitorizar, Avaliar e Analisar (*Monitor, Evaluate and Assess*), que contém 3 processos;
- Avaliar, Direcionar e Monitorizar (*Evaluate, Direct and Monitor*), que contém 5 processos.

2.4. Metodologia ITIL

O ITIL (*Information Technology Infrastructure Library*) é um conjunto estruturado de boas práticas em que os vários processos comunicam uns com os outros. Cada um tem o seu próprio papel por forma a que, no final, possam dar resposta a duas questões: a melhoria contínua e a satisfação do cliente (Orakzai, 2014).

O conceito ITIL surgiu na década de 1980, quando o governo Britânico determinou que o nível de qualidade de serviço de TI que lhes era fornecido não era suficiente. A Agência Central de Computação e Telecomunicações (CCTA), agora designado por *Office of Government Commerce* (OGC), foi encarregue de elaborar uma estrutura para a utilização eficiente e financeiramente responsável dos recursos de TI dentro do governo britânico e do setor privado.

O ITIL não é um padrão, porque não fornece critérios ou define requisitos que estejam definidos internacionalmente. No entanto, de modo a aproveitar as boas práticas propostas pelo ITIL, e na sequência do reconhecimento mundial da robustez dos seus processos, em 2006 foi criada uma norma, ISO 20000, com base nessas boas práticas (Bahsani et al., 2011).

O ITIL não é uma metodologia ou método. Ele fornece e utiliza métodos para melhor explorar as boas práticas. É comum o ITIL ser implementado conjuntamente (ou como complemento) com outras plataformas e modelos de boas práticas para a gestão das tecnologias de informação.

O ITIL é baseado na definição das melhores práticas para os processos de gestão de serviços de TI e suporte, em vez de, na definição de uma *framework* de controlo de base ampla. Centra-se sobre o método e define um conjunto mais abrangente de processos. Além disso, o ITIL fornece um negócio e contexto estratégico para a tomada de decisão de TI e pela primeira vez, descreve Melhoria de Serviço Continuada como a atividade principal que impulsiona a manutenção da entrega de valor aos clientes (Nãstase et al., 2009).

O ITIL é baseado em cinco pilares: foco no cliente; o ciclo de vida de serviço; o conceito de processo; melhoria contínua; comunicação.

Tal como representado na Figura 11, a perspetiva de ciclo de vida sugere uma evolução circular e repetida dos serviços, permitindo que estes se adaptem melhor ao ambiente de negócio da organização, que está em permanente modificação.

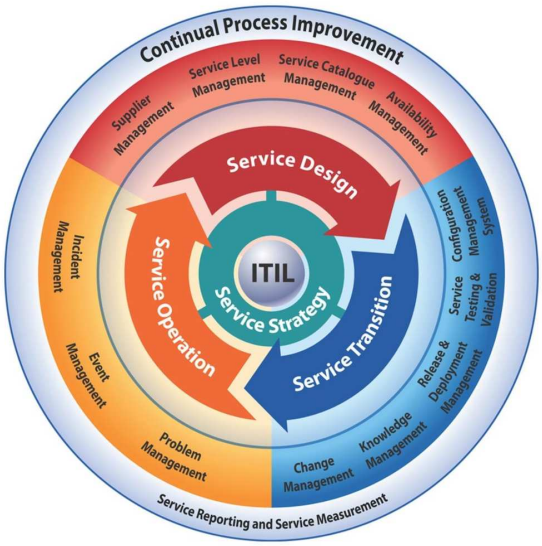

Figura 11 — Modelo do ciclo de vida do ITIL V3 (Martins et al., 2010)

O ITIL V3 divide-se em cinco fases: *Service Strategy* (estratégia de serviço), *Service Design* (desenho de serviço), *Service Transition* (transição de serviço), *Service Operation* (operação de serviço) e *Continual Service Improvement* (melhoria contínua de serviço). Cada parte do ciclo de vida de serviço influencia os restantes e comportam as entradas (*inputs*) e realimentações entre si. Desta forma, através do ciclo de vida de serviço assegura-se que quando os requisitos do negócio mudam, os serviços podem ser adaptados, respondendo de forma eficiente.

O ***Service Strategy*** fornece orientações sobre como projetar, desenvolver e implementar a gestão de serviço, não só como uma capacidade de organização, mas também como um ativo estratégico.

O ***Service Design*** fornece orientação para a conceção, desenvolvimento e processos de gestão de serviços, orientações para transformar a estratégia de serviço para a produção e desenvolvimento de serviços TI.

O ***Service Transition*** fornece orientações para o desenvolvimento e melhoria das capacidades para a transição de novos serviços operacionais. Fornece orientação sobre como os requisitos são efetivamente realizados no *Service Operation*, controlando os riscos de fracasso e rutura.

O ***Service Operation*** inclui orientações sobre como alcançar a eficácia e eficiência na entrega e suporte de serviços, de modo a garantir valor acrescentado para o cliente e o prestador de serviços, incorporando práticas na gestão de operações de serviço.

O ***Continual Service Improvement*** fornece uma orientação instrumental na criação e manutenção de valor para os clientes através de um melhor desenho, introdução e operação de serviços. Combina os princípios, práticas e métodos de gestão da qualidade, gestão da mudança e aumento da capacidade.

Cada uma das fases é composta por uma série de processos específicos associados a cada fase do ciclo de vida (Tabela 2). Os processos são conjuntos estruturados de

atividades destinadas a alcançar um objetivo específico. Estes têm quatro características básicas: transformam as entradas (*inputs*) em saídas (*outputs*); devolvem resultados para um cliente ou parte interessada específica; são mensuráveis; são acionados por eventos específicos.

Tabela 2 —ITIL: processos do ciclo de vida

Ciclo de vida	Processos
Estratégia de serviço (*Service Strategy*)	• Estratégia de serviço • Gestão de portfólio • Gestão do pedido • Gestão financeira
Desenho de serviço (*Service Design*)	• Gestão de catálogo de serviço • Gestão de nível de serviço • Gestão de disponibilidade • Gestão de capacidade • Gestão de continuidade • Gestão de segurança da informação • Gestão de fornecedores
Transição de serviço (*Service Transition*)	• Gestão de mudança • Gestão de configuração de ativos e serviços • Gestão de implantação e lançamento • Plano de transição e suporte • Validação e teste de serviço • Avaliação de serviço • Gestão do conhecimento
Operação de serviço (*Service Operation*)	• Gestão de incidentes • Gestão de problemas • Gestão de eventos • Serviço de execução de requisição • Gestão de acesso
Melhoria contínua de serviço (*Continual Service Improvement*)	• Melhoria de processos

2.5. Comparação das Metodologias

As metodologias anteriormente apresentadas (ISO 27000, COBIT e ITIL) podem ser utilizadas na implementação de boas práticas e na criação de uma estrutura de controlo na área das Tecnologias da Informação.

A tabela seguinte (Tabela 3) permite uma visão geral das três metodologias, permitindo observar as semelhanças e diferenças entre elas:

Tabela 3 — COBIT, ITIL, ISO 27002: visão geral

	COBIT	ITIL	ISO 27002
Emissora	ISACA	OGC	ISO
Função	Framework de Governança e Gestão	Associar a gestão de TI ao nível do serviço	Framework de Segurança da Informação
Implementação	Auditoria do Sistema de Informação	Gestão ao nível do serviço	Cumprimento das normas de segurança

Para além das três metodologias serem emitidas por diferentes organizações, com diferentes áreas de atividade e objetivos, a função principal de cada uma também é diferente. Enquanto o COBIT fornece uma *framework* de governança e gestão de processos, o foco do ITIL é a gestão de TI ao nível do serviço, sendo que a norma ISO 27002 fornece orientações para a implementação de uma estrutura de segurança.

O modo de atuação das diferentes metodologias pode ser verificado na Figura 12. O COBIT fornece orientação para a estratégia global de TI, enquanto que o ITIL fornece detalhes do processo, alinhando o objetivo de negócio com as TI, otimizando os recursos e criando valor para os clientes. No nível mais baixo, encontra-se a disponibilidade da informação, tratada pela implementação da norma ISO 27002, minimizando riscos e garantindo a segurança e integridade da mesma (Orakzai, 2014).

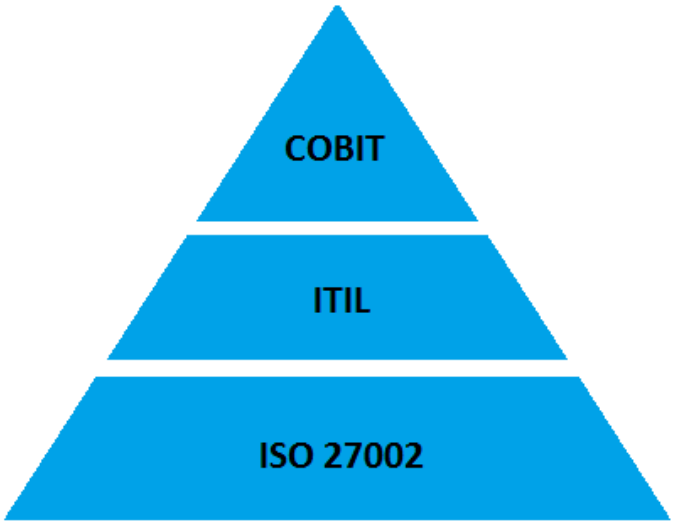

Figura 12 — COBIT, ITIL, ISO27002: visão geral

Procurando sintetizar: a metodologia COBIT está mais vocacionada para avaliação crítica, fatores de sucesso, métricas, indicadores e auditorias (governança e gestão de TI); a metodologia ITIL está mais orientada para ser utilizada para definir as estratégias e processos de operação relacionados com a gestão de TI; a norma ISO 27002 fornece orientações relacionadas com questões de segurança.

Uma vez que o propósito deste trabalho é a definição de uma política de segurança, optou-se por seguir as indicações da norma ISO 27002 durante a elaboração da mesma.

A utilização da norma ISO 27002 para a elaboração da política de segurança poderá, no futuro, ser aproveitada pelo IPCB para a obtenção da certificação ISO 27001.

3. Caracterização da Instituição

Neste capítulo é apresentada uma caracterização da instituição para a qual vai ser proposta a política de segurança da informação, assim como do sistema de informação e infraestrutura que se encontra neste momento em utilização.

3.1. Introdução

O Instituto Politécnico de Castelo Branco (IPCB) é uma instituição de ensino superior criado pelo Decreto-Lei nº 513 T/79 de 26 de dezembro, que tem como missão a qualificação de alto nível dos cidadãos, a produção e difusão do conhecimento, bem como a formação cultural, artística, tecnológica e científica dos seus estudantes, num quadro de referência internacional.

O IPCB é constituído por sete unidades orgânicas de ensino e investigação, designadas por Escolas Superiores, Agrária (ESACB), de Artes Aplicadas (ESART), de Educação (ESECB), de Gestão (ESGIN), de Saúde Dr. Lopes Dias (ESALD) e de Tecnologia (ESTCB), e o Centro de Estudos e Desenvolvimento Regional (CEDER), existindo ainda o edifício da Presidência e Serviços Centrais (PSC), que coordenam toda a atividade.

Em termos de estrutura física, as escolas do IPCB encontram-se dispersas, possuindo cada uma instalações próprias, localizadas em espaços diferentes na cidade de Castelo Branco e com a Escola Superior de Gestão localizada na vila de Idanha-a-Nova, a cerca de 35 Km de Castelo Branco.

Para além das escolas e do edifício da Presidência e Serviços Centrais, fazem parte do campus do IPCB três residências de estudantes, duas delas localizadas em Castelo Branco e a outra em Idanha-a-Nova.

O Instituto Politécnico de Castelo Branco é frequentado por cerca de 4000 alunos, tendo ainda cerca de 370 docentes e 270 não docentes.

3.2. Serviços de Informática

Os Serviços de Informática (SI) constituem um serviço de apoio à presidência do IPCB e desenvolvem a sua ação nos domínios da informática, dos sistemas e tecnologias da informação, e das comunicações, incluindo o apoio às atividades de ensino, investigação e extensão, à informatização geral do IPCB, bem como à promoção e divulgação das novas tecnologias de informação.

A estrutura dos SI tem subjacentes os princípios de segregação de funções, sendo composta por uma equipa de Infraestruturas Informáticas e outra de Desenvolvimento de Sistemas, e por duas unidades de apoio transversal, denominadas respetivamente,

Unidade de Arquitetura e Planeamento de Tecnologias e Sistemas de Informação e Unidade de Apoio ao Utilizador (*Service Desk*).

Das principais atividades dos SI destacam-se as seguintes:

- Contribuir para o desenvolvimento da visão, objetivos e estratégias dos SI, em articulação com a estratégia do IPCB;
- Definir estratégias e objetivos de atuação que permitam antecipar as necessidades de adaptação dos SI às realidades interna e externa;
- Produzir normas internas e procedimentos a adotar;
- Garantir o desenvolvimento informático que permita facilitar os processos, controlar a qualidade e fiabilidade dos dados e informação e facilitar a sua apresentação e utilização;
- Garantir a segurança dos sistemas de informação;
- Definir normas de funcionamento e utilização estabelecidas para os recursos e sistemas disponibilizados, bem como assegurar a sua divulgação e sensibilização dos utilizadores para o seu cumprimento.

A nível de infraestruturas informáticas o IPCB deixou de possuir em cada uma das escolas uma "sala de servidores", centralizando esta valência numa única sala (centro de dados) localizada no edifício da Presidência e Serviços Centrais, onde se encontram alojadas as aplicações e serviços disponibilizados à comunidade do IPCB. Neste centro de dados encontram-se, para além dos servidores aplicacionais, o ponto de acesso à internet, tornando-se este um local crítico para o bom funcionamento da instituição.

3.3. Rede do Instituto Politécnico de Castelo Branco

Tal como referido anteriormente, em termos de estrutura física, as escolas do IPCB encontram-se dispersas, em diferentes espaços na cidade de Castelo Branco e na vila de Idanha-a-Nova.

Uma vez que o centro de dados está localizado no edifício da Presidência e Serviços Centrais, as escolas estão ligadas ao centro de dados por um sistema de comunicação de dados, utilizando uma infraestrutura em fibra ótica e radio frequência.

As comunicações são efetuadas em fibra ótica com os polos mais próximos, com redundância em rádio frequência e apenas em rádio frequência com os polos mais distantes, existindo uma ligação do edifício da Presidência e Serviços Centrais a uma antena colocada no castelo (366 Mb/s Full Duplex), que depois liga à ESACB (300 Mb/s, Half Duplex) e à ESGIN (40 Mb/s Full Duplex). A ligação à residência de estudantes em Idanha-a-Nova é efetuada utilizando tecnologia de rede sem fios, com uma ligação entre a ESGIN e a residência de estudantes (36 Mb/s Half Duplex). Na Figura 13 encontra-se o esquema das ligações.

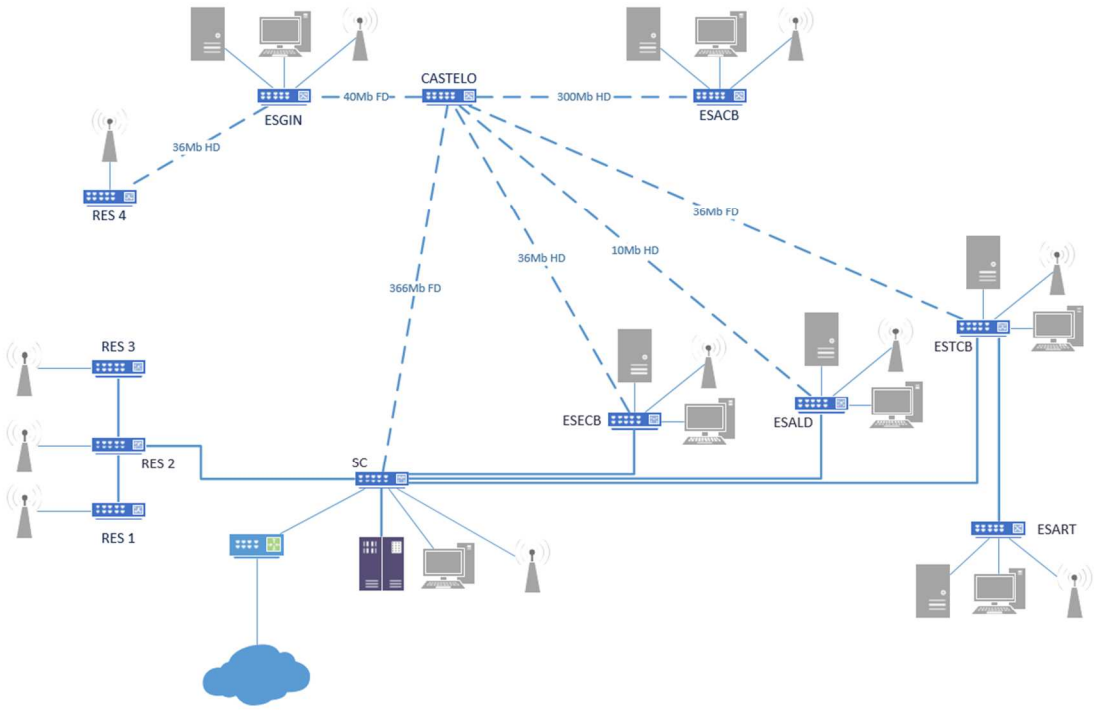

Figura 13 — Esquema de rede de interligação do IPCB

A estrutura de rede nas escolas do IPCB é similar em todas elas, existindo um equipamento de rede (*switch core*) utilizado para interligar a escola ao edifício da Presidência e Serviços Centrais. Esta interligação é feita através de uma rede privada, com endereçamento diferente para cada escola.

Cada escola tem instalada uma *firewall*, servidores com Linux instalado e utilizando *IPTABLES*, cuja função é fazer o *routing* e filtrar o tráfego da escola.

De forma a separar e controlar o tráfego, existem várias redes privadas dentro de cada escola, para além da rede local (LAN), onde se encontram ligados a maioria dos computadores da escola, existem outras redes virtuais (VLAN) para conexão de outros equipamentos. Deste modo, em cada escola existem as seguintes redes privadas:

- LAN: zona de rede cablada utilizada por alunos e docentes e funcionários, vlanid é 1 com endereçamento privado 10.x.0.0/16;
- EWC: zona de rede para a gestão dos pontos de acesso (AP's) da rede sem fios, vlanid é 1x82 com endereçamento privado.
- WIFI: zona de rede sem fios (eduroam), utilizado por alunos, docentes, funcionários e convidados, vlanid é 1x50 com endereçamento público;
- VoIP: zona de rede de comunicação de voz, vlanid é 1x05 com endereçamento privado 10.8x.0.0/24;
- NETTIME: zona de rede para equipamentos de controlo de acessos e câmaras de videovigilância, vlanid é 1x90 com endereçamento privado 10.10x.0.0/24;

- MGMT: zona de rede de gestão de equipamentos de rede, vlanid é 1x99 com endereçamento privado 10.24x.0.0/24.

3.4. Centro de dados do Instituto Politécnico de Castelo Branco

O centro de dados do IPCB está instalado numa sala térrea situada no edifício da Presidência e Serviços Centrais. Este local está equipado com porta corta-fogo, chão técnico e um sistema de refrigeração redundante. No centro de dados estão instalados o ponto de acesso à internet, os *switches de core* que interligam as várias escolas e residências de estudantes (localizadas na cidade de Castelo Branco) e onde se encontram alojados os servidores aplicacionais da instituição.

O IPCB dispõe de um sistema de virtualização de servidores utilizando o VMware vSphere. Esta infraestrutura suporta atualmente os servidores aplicacionais, servidores de base de dados e servidores web de todo o IPCB.

A utilização do VMware facilita a gestão do ambiente aplicacional e permite, entre outras funcionalidades, adicionar memória, disco ou aumentar a capacidade de processamento (CPU) nas máquinas virtuais sem perda de serviço, fazer movimentação de servidores virtuais entre servidores físicos (*vMotion*), sem *downtime*. Esta infraestrutura conta atualmente com 92 servidores virtuais.

Como base de suporte ao sistema de virtualização existem três servidores físicos, da marca Cisco (UCS C200 M2), cada um dos quais compostos com 2 processadores Intel Xeon (X5650 a 2.67GHz de 6 cores) e com 131 GB de memória instalada.

A nível de armazenamento, o IPCB tem instalado um sistema de armazenamento de dados (*storage*) da marca Netapp (modelo NA2552) composto por três gavetas, disponibilizando a nível de armazenamento um total de 18.44 TB (9.61TB numa gaveta e 8.83TB na outra) em tecnologia SAS e 32.68TB em SATA; numa das gavetas estão instalados 8 discos ssd de 200 GB utilizados em cache de forma a aumentar o desempenho do sistema.

O sistema de virtualização está instalado de modo totalmente redundante, configurado com um *cluster*, composto pelos três servidores, partilhando os recursos e permitindo que o sistema esteja configurado com alta disponibilidade (*High Availability – HA*), o que significa que caso exista uma falha num dos servidores, as máquinas (servidores) virtuais associadas ao mesmo passam a ser executadas utilizando os recursos disponíveis fornecidos pelos outros servidores do *cluster*.

Os servidores e sistema de virtualização estão interligados utilizando FCoE (*Fiber Channel over Ethernet*), ligados a dois equipamentos da marca Cisco, modelo Nexus 5672UP, de modo redundante. Na Figura 14 pode-se verificar como os equipamentos que servem de suporte ao sistema de virtualização estão interligados.

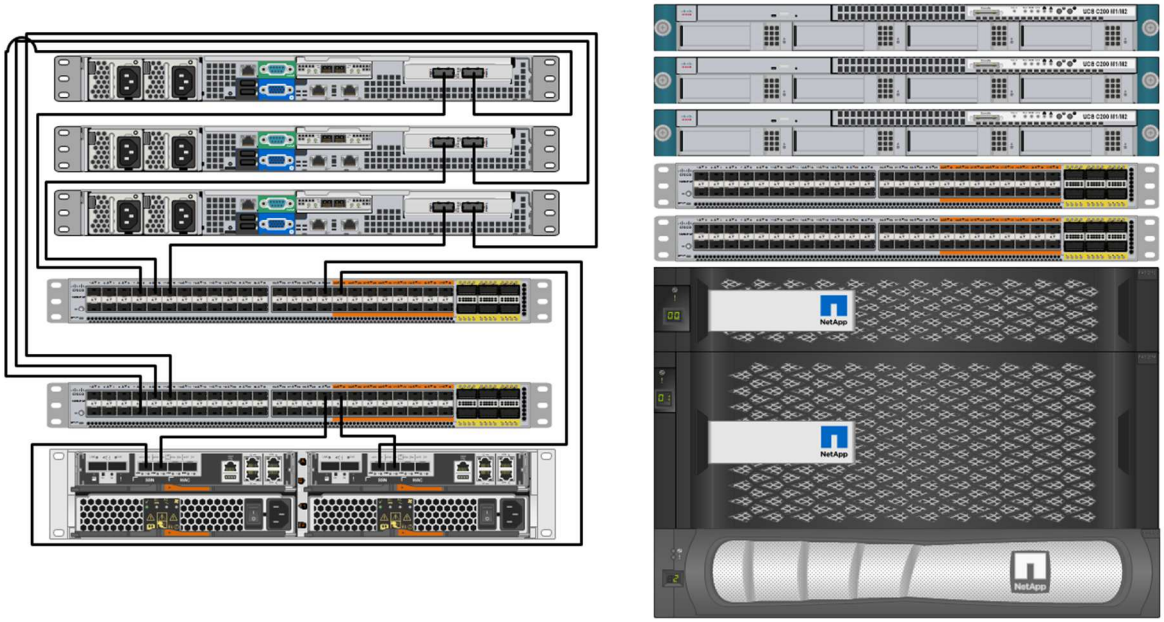

Figura 14 — Interligação dos servidores ao sistema de armazenamento

Para além do armazenamento que é disponibilizado ao sistema de virtualização, esta *storage* disponibiliza também servidores de armazenamento virtual, que permitem que os utilizadores (atualmente funcionários, mas futuramente toda a comunidade do IPCB) e serviços possam guardar informação.

Os servidores de armazenamento virtual (SVMs, também conhecidos como *vServers*) contêm volumes de dados e um ou mais LIFs através dos quais fornecem dados para os clientes. Cada um dos SVMs conter um ou mais volumes FlexVol, ou um único volume infinito.

O uso de SVMs permite isolar de modo seguro a rede e armazenamento de dados virtualizada e partilhado, uma vez que cada SVM aparece como um único servidor dedicado para os clientes.

3.5. Ambientes Aplicacionais

O IPCB dispõe de várias aplicações que servem de apoio à gestão. No entanto existem duas destas aplicações que são fundamentais ao bom funcionamento da instituição, a aplicação de gestão académica e a aplicação de gestão financeira e de recursos humanos.

O "SIGES", atual sistema de gestão académica em utilização no IPCB, é um sistema de gestão informática integrado, colaborativo, que é composto por vários módulos administrativos e de gestão do conhecimento. Esta aplicação é composta por três áreas de atuação:

- Módulos para ambiente de trabalho Windows, que servem para a gestão académica por parte da secretaria e tesouraria, também designado de *BackOffice*;
- Módulos para a Internet, destinados maioritariamente para a comunidade docente e alunos, também designado por portal académico ou Netp@.
- Módulos integradores de serviço (IS), utilizados para integrarem informação da base de dados do SIGES com aplicações de terceiros.

A nível financeiro e de recursos humanos, gestão administrativa e financeira, é utilizado o *software* "Primavera Public Sector", cuja solução solidifica a gestão através de um centro financeiro, a partir do qual se obtém um controlo global sobre a atividade do IPCB. Os mecanismos desta solução promovem um controlo financeiro global – desde a fase da orçamentação e respetivas alterações, execução e controlo; passando pelos pagamentos e recebimentos, controlo de duodécimos, cabimentos, compromissos e gestão de fontes de financiamento, até à consolidação e prestação de contas.

Esta solução permite ainda a gestão de vínculos, carreiras e remunerações, contribuições, abono de família, formação, balanço social, relatório único, entre outros procedimentos próprios da administração pública.

A solução instalada no IPCB é composta pelos seguintes módulos:

- Plataforma e Administrador;
- Contabilidade;
- Declarações Fiscais;
- Add-In Financeiro;
- Património;
- Recursos Humanos;
- Tesouraria.

O IPCB utiliza, como repositório central de dados de utilizadores, um diretório LDAP (*Lightweight Directory Access Protocol*), que é usado por quase todas as aplicações de Internet para autenticar e atribuir os diferentes perfis de utilizador.

3.6. Perfil de Utilizadores

O perfil de utilizador é o conjunto de definições mediante as quais o utilizador tem diferentes tipos de acessos e privilégios. Cada colaborador do IPCB tem, pelo menos, um perfil de utilizador associado. Entende-se por colaborador alguém que está ligado à instituição. No IPCB estão identificados cinco tipos de utilizadores: docentes, não docentes, alunos, estagiários e convidados. Um colaborador pode ter mais do que um perfil associado: por exemplo um colaborador pode ter perfil de não docente e aluno

ao mesmo tempo. Mediante o perfil de utilizador existem diferentes privilégios de acesso, privilégios esses que dependem do serviço, unidade científica ou curso a que estão afetos (Tabela 4). Por exemplo um colaborador não docente, que esteja afeto aos Serviços de Informática tem acesso à área de partilha de ficheiros desse serviço.

Tabela 4 — IPCB: Perfil de utilizadores

Perfil de utilizador	Privilégios
Docente	• Acesso à rede interna; • Acesso à rede sem fios; • Conta de correio eletrónico institucional; • Área de partilha de ficheiros comum; • Área pessoal para armazenamento de ficheiros; • Acesso ao portal académico; • Acesso à aplicação de *e-learning*;
Não Docente	• Acesso à rede interna; • Acesso à rede sem fios; • Conta de correio eletrónico institucional; • Área de partilha de ficheiros comum; • Área de partilha de ficheiros de serviço; • Área pessoal para armazenamento de ficheiros; • Acesso a aplicações de *backoffice*;
Aluno	• Acesso à rede interna; • Acesso à rede sem fios; • Conta de correio eletrónico institucional; • Área de partilha de ficheiros comum; • Acesso ao portal académico; • Acesso à aplicação de *e-learning*;
Estagiário	• Acesso à rede interna; • Acesso à rede sem fios; • Área de partilha de ficheiros comum; * Dependendo do tipo de estagiário pode ter acesso à área de partilha de ficheiros de serviço.
Convidados	• Acesso à rede interna; • Acesso à rede sem fios;

Dentro de cada perfil definido de utilizador existem depois sub-perfis: por exemplo, o perfil não docente possuí como sub-perfil o serviço a que o utilizador está associado (ex. Informática, Académicos, etc.).

4. Política de Segurança

Neste capítulo é realçada a importância da aplicação de uma política de segurança da informação, sendo apresentadas de seguida as definições da norma ISO 27002. Finalmente, são apresentados os resultados da análise do funcionamento dos sistemas de informação e infraestrutura do IPCB, que foram tidos em consideração na elaboração da política de segurança.

4.1. Conceitos

Uma política de segurança é uma ferramenta importante para proteger uma organização contra ameaças à segurança da informação a que ela pertence. A política de segurança, segundo a RFC 2196 (B. Fraser, 1997), consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

A política de segurança não deve definir procedimentos específicos de proteção da informação, mas deve atribuir direitos e responsabilidades às pessoas que lidam com a informação. A política de segurança deve deixar de fora aspetos técnicos de implementação, uma vez que esse aspeto pode variar ao longo do tempo. A política deve ainda ser flexível de modo a que seja possível adaptar-se a alterações que venham a existir na organização (Karyda et al., 2005).

Uma política de segurança deve ter as seguintes características:

- Ser acessível a todos os membros da organização;
- Não deve ser um documento muito extenso, devendo ser de fácil leitura e compreensão;
- Definir os objetivos, o que se espera alcançar com a aplicação da mesma;
- Definir os papéis dos principais agentes da organização;
- Definir o nível de privacidade garantido aos utilizadores;
- Definir as circunstâncias em que é aplicada cada regra;
- Definir o tratamento de situações omissas;
- Identificar contatos para esclarecimentos adicionais.

Apesar de as políticas por si só não resolverem problemas, podem definir o caminho ideal para onde todos os esforços organizacionais devem apontar. Por definição, a política de segurança refere-se a planos abrangentes e bem definidos, regras e práticas que regulam o acesso aos sistemas de uma organização e à informação neles contidos. Uma boa política não protege apenas a informação e os sistemas, mas também os funcionários e a organização como um todo. Pode também funcionar como uma afirmação para o exterior sobre o compromisso da organização com a segurança (Szuba, 1998).

4.2. Gestão de Risco

O primeiro passo para garantir de forma eficaz a proteção da informação e equipamentos é dado com um processo de avaliação de risco. Neste processo devem ser identificados os ativos que a instituição possui, possíveis ameaças a que esses ativos estão sujeitos, pontos em que podem existir vulnerabilidades sobre as ameaças e estimativas de prejuízos caso uma das ameaças se venha a concretizar.

Uma vez que a realização de uma avaliação de risco fornece um retrato exato das necessidades específicas, a definição da política de segurança deve basear-se nos resultados da mesma.

Para efeitos de segurança da informação, um risco é qualquer perigo a que a informação ou equipamentos estão sujeitos.

A segurança da informação e a gestão de risco são duas áreas distintas. Enquanto a segurança da informação diz respeito à implementação de um conjunto de controlos que têm como finalidade proteger os ativos, a gestão de risco preocupa-se com a identificação de potenciais riscos e implementar as soluções necessárias para mitigar esses riscos (Casaca, 2014).

4.3. Definições da Norma ISO 27002

A norma ISO 27002 foi planeada para ser utilizada como referência na seleção de controlos dentro do processo de implementação de um sistema de gestão da segurança da informação (SGSI), baseado na norma ISO/IEC 27001, ou como um documento de orientação para implementar controlos de segurança da informação vulgarmente aceites. Esta norma pode ainda ser utilizada na gestão da segurança da informação, tendo em consideração ambientes de risco de segurança da informação específicos.

Para a definição de uma política de segurança da informação é essencial que sejam identificados os seus requisitos, que podem ser obtidos da seguinte forma:

- A partir da avaliação de riscos, tendo em conta os objetivos e as estratégias globais de negócio. Através da avaliação de riscos são identificadas as ameaças aos ativos, e as suas vulnerabilidades, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial no negócio;
- Através da legislação vigente, estatutos, regulamentação e cláusulas contratuais que a organização e parceiros comerciais têm que obedecer;
- Através de conjuntos particulares de princípios, objetivos e requisitos de negócio para a gestão, processamento, armazenamento, comunicação e arquivo da informação de uma organização.

A definição dos controlos a implementar deve ter em consideração a probabilidade de danos que possam causar, e quais os problemas de segurança que podem resultar

devido à ausência desses controlos. Efetuar uma avaliação de riscos ajuda na orientação e determinação de ações de gestão apropriadas e prioridades para a gestão de riscos de segurança da informação.

A norma ISO 27002 refere a norma ISO 27005 como referência para obter diretrizes sobre gestão de riscos de segurança da informação, incluindo orientações sobre avaliação de riscos, tratamento e aceitação de riscos, comunicação, monitorização e análise crítica dos riscos.

A seleção dos controlos de segurança da informação fornecidos por esta norma depende das decisões da organização e devem ser baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização. Para além disso, convém que esteja sujeito a toda a legislação e regulamentações nacionais e internacionais, relevantes.

Alguns dos controlos referidos por esta norma podem ser considerados como princípios básicos para a gestão da segurança da informação e podem ser aplicados na maioria das organizações.

A norma ISO 27002 pode ser considerada como um ponto de partida para o desenvolvimento de diretrizes específicas. No entanto, podem não ser aplicados todos os controlos e diretrizes contidos nesta norma. Para além disso, pode ser necessário adicionar novos controlos e recomendações que não estejam incluídas nesta norma.

Esta norma prevê que a informação tem um ciclo de vida natural, iniciando-se com a sua criação e origem, passando pelo armazenamento, processamento, uso e transmissão, tendo depois um final que pode eventualmente levar à sua destruição. O valor e os riscos associados aos ativos podem variar durante o seu tempo de vida; porém, a segurança da informação deve ser sempre assegurada.

Os sistemas de informação têm ciclos de vida nos quais são concebidos, especificados, projetados, desenvolvidos, testados, implementados, usados, mantidos e, eventualmente, retirados do serviço e descartados. Convém que a segurança da informação seja considerada em cada uma destas etapas.

O desenvolvimento de novos sistemas e alterações nos sistemas existentes são oportunidades para serem atualizados e melhorados os controlos de segurança, devendo ser considerados os incidentes reais e os riscos de segurança da informação, projetados e atuais.

4.4. Definição da Política de Segurança

Em conjunto com os colaboradores dos Serviços de Informática e o Vice-Presidente do IPCB foram identificadas as seguintes áreas que deviam ser incluídas na política de segurança:

- Definição de ciclo de vida dos utilizadores: clarificar as responsabilidades e ações a tomar quando um colaborador termina a sua ligação com o IPCB;
- Definição de direitos de acesso: clarificar as responsabilidades sobre quem autoriza e atribui os direitos de acesso à informação;
- Gestão de palavra-passe de administrador: definir como e onde são registadas as palavras-passe de administração dos sistemas;
- Gestão de redes: elaborar e manter atualizados os esquemas de rede interna de cada escola e de interligação de edifícios;
- Inventário de ativos: elaborar e manter atualizado o inventário de ativos;
- Acesso à informação: alinhar a política com o procedimento de trabalho existente no Sistema de Gestão de Qualidade (SGQ), sobre o acesso à informação;
- Cópias de segurança: alinhar a política com o procedimento de trabalho existente no SGQ, sobre as cópias de segurança.

Para definir a política de segurança da informação foi realizada uma análise ao funcionamento dos sistemas e infraestrutura do IPCB. Da análise resultaram as seguintes situações, que devem ser refletidas na política de segurança:

- A gestão de ativos possibilita a identificação dos ativos e definição de responsabilidades apropriadas para a sua proteção. Esta gestão é facilitada com a utilização de um inventário de ativos. No IPCB existe uma aplicação web para gerir o inventário de alguns equipamentos, que contém computadores, impressoras, projetores, UPS e equipamentos VoIP. Esta aplicação é também utilizada para gerir o *software* adquirido.
- O acesso aos sistemas de informação e serviços é realizado através de autenticação, composta por um nome de utilizador e uma palavra-passe. Deve ser implementada uma política de palavra-passe, definindo requisitos mínimos para a sua composição.
- A aplicação de gestão de alunos (SIGES) é uma aplicação crítica para o funcionamento do IPCB. Esta aplicação contém todo o histórico académico dos alunos. Para além desta informação, a aplicação contém dados pessoais de alunos e docentes. De forma a garantir a confidencialidade, o acesso a esta informação deve ser restrito a alguns utilizadores.
- A aplicação de gestão financeira, patrimonial e de recursos humanos (Primavera) é uma das aplicações mais críticas em utilização no IPCB, uma vez que contém dados financeiros e de fornecedores, e dados pessoais dos colaboradores docentes e não docentes do IPCB. É necessário garantir a integridade e confidencialidade destes dados. O acesso a esta informação deve ser restrito apenas a utilizadores autorizados.
- As aplicações de *BackOffice* (Primavera e SIGES) não devem ser acessíveis a todos os utilizadores. Assim, é necessário garantir que o acesso a essas aplicações é efetuado apenas pelas pessoas devidamente autorizadas. No entanto, para além da implementação de políticas de restrição de acesso à

informação, devem também ser implementadas políticas de segregação de redes, de modo a controlar o acesso a essas aplicações, por exemplo através da utilização de uma *firewall*, garantido acesso apenas ao endereço IP do computador atribuído ao utilizador autorizado.

- A rede cablada (com fios) não necessita de autenticação. Significa isto que qualquer pessoa, mesmo alguém externo ao IPCB, ao ligar um computador a uma tomada de rede em qualquer dos edifícios fica ligado na rede interna, com acesso à internet e outros serviços. Uma forma de proteger o acesso a estas redes pode ser através da implementação de autenticação 802.1x, à semelhança dos requisitos de acesso à rede sem fios. Em alternativa, deve ser realizado um inventário de todas as tomadas de rede existentes e desativadas as que não estejam em utilização.
- Atualmente o IPCB tem instalado um servidor de registo de eventos que recolhe informações de todos os servidores e equipamentos de rede instalados na infraestrutura. No entanto, esta solução não tem capacidade para gerar alertas.
- Como já foi referido, o centro de dados é o local onde se encontram alojados os servidores aplicacionais do IPCB, o ponto de acesso à internet e os *switches* de *core* que interligam as várias escolas, tornando-se um local crítico para o bom funcionamento da instituição. De modo a proteger tanto as áreas que contenham as instalações de processamento da informação, como as informações críticas ou sensíveis, prevenindo também o acesso físico não autorizado, a política deve incluir a definição de áreas seguras.
- Dada a importância do centro de dados, estão associadas várias utilidades a este local:
    - O controlo de temperatura. Neste momento, o centro de dados tem instalado dois equipamentos de ar condicionado, sendo que é apenas necessário um para garantir a temperatura da sala (redundante);
    - Sistema de autonomia no caso de falta de energia (UPS). No centro de dados estão instaladas duas UPS capazes de garantir, por trinta minutos, o funcionamento dos equipamentos instalados no centro de dados. Os Serviços de Informática não consideram prioritário que os bastidores instalados fora do centro de dados possuam UPS, uma vez que, não existindo UPS de edifício, os equipamentos dos clientes irão ficar inoperacionais;
    - Detetor de incêndios e existência de extintor de CO2 dentro do centro de dados e um extintor de CO2 do lado de fora;
    - Porta corta-fogo.
- O sistema de gestão da qualidade em uso no IPCB define, através do procedimento de trabalho PT.IPCB.SI.02.01, a metodologia para a realização de cópias de segurança de dados informatizados, classificando os dados em três níveis (Nível 1, Nível 2 e Nível 3), de acordo com o grau de importância dos mesmos, devendo ser guardados num local diferente do centro de dados.

Atualmente as cópias de segurança são guardadas num sistema de armazenamento instalado no edifício de uma das escolas do IPCB.

Durante a elaboração da política de segurança foram identificados dois temas que devem ser incluídos na política de segurança:

- Política sobre a utilização do endereço de correio eletrónico institucional: do endereço de correio eletrónico atribuído a um colaborador, que por vezes é chamado pessoal (ex. joaojoao@ipcb.pt); e do endereço de correio eletrónico com o nome de um serviço, partilhado por um ou mais colaboradores (ex. informatica@ipcb.pt).
- Política sobre a utilização do acesso à internet: abordando temas como a permissão de acesso a toda internet, se devem existir endereços barrados (ex. redes sociais, sites com conteúdo para adultos, etc.), se devem ser barradas aplicações e acesso a aplicações de partilha de ficheiros (*torrents*).

No entanto, uma vez que estas políticas comprometem a garantia de privacidade dos utilizadores, estas devem ser definidas em momento oportuno pela presidência do IPCB e não pelo autor deste trabalho.

As situações anteriormente descritas foram tidas em consideração na elaboração da política de segurança, que se apresenta em anexo (Anexo A). A definição da política de segurança foi elaborada tendo em consideração a norma ISO 27002, adaptada à realidade do IPCB.

5. Conclusão

Este capítulo apresenta as conclusões gerais deste trabalho, bem como o trabalho futuro que foi desde já identificado mas que só será possível realizar em próximas fases da implementação da política de segurança.

5.1. Conclusões Gerais

Após a realização deste trabalho conclui-se que a segurança da informação já não deve ser vista apenas como a gestão desenquadrada de *firewalls* e antivírus. Atualmente, a segurança da informação exige uma abordagem de gestão de risco global. A segurança não passa apenas por proteger os sistemas, mas também pela consciencialização dos utilizadores para a sua necessidade, tornando-se necessária a definição de políticas adequadas.

Pode ainda concluir-se que a segurança da informação não deve ser apenas preocupação dos departamentos de TI, ou Serviços de Informática, sendo necessário que os responsáveis das organizações envolvam todos os colaboradores. As políticas de segurança devem ser alinhadas com os objetivos estratégicos da organização, de forma a manter ou melhorar o seu valor.

Verificou-se ainda, que existem várias metodologias que podem ser utilizadas na implementação de sistemas de segurança da informação. Para a elaboração deste trabalho foram analisadas três: a família de normas da ISO 27000, a metodologia COBIT e a metodologia ITIL. Após esta análise, optou-se por elaborar a política de segurança do IPCB seguindo as indicações da norma ISO 27002, uma vez que esta norma fornece orientações para a elaboração de políticas de segurança.

Analisado o caso específico do IPCB, verificou-se que o normal funcionamento da instituição está cada vez mais dependente dos seus sistemas de informação, o que intensifica a necessidade de maximizar a segurança dos mesmos. Com a implementação desta política de segurança prevê-se que o IPCB obtenha:

- Um aumento da consciencialização interna relativo à segurança da informação;
- Uma otimização de planos e processos de gestão da informação, através da padronização de processos;
- Definição das responsabilidades pelos ativos;
- O comprometimento com a aplicação da política;

Esta política de segurança pode também ser utilizada como um auxílio na antecipação do risco e na garantia de continuidade do serviço.

Os objetivos inicialmente propostos foram cumpridos. Foi escrita uma política de segurança de acordo com uma norma internacional de referência, ajustada à realidade

do IPCB, que garante melhorias no funcionamento do sistema de informação da instituição.

Pessoalmente, a realização deste trabalho permitiu-me aprofundar conhecimentos e capacidades na área de segurança da informação.

5.2. Trabalho Futuro

A política de segurança foi escrita tendo em conta as necessidades do IPCB, pelo que após a sua aprovação pelo Presidente deverá ser divulgada a todos os colaboradores e implementada de forma a proteger os sistemas de informação em funcionamento.

Adequando este trabalho ao modelo PDCA, a elaboração da política situa-se na parte do ciclo de planeamento (*Plan*). Seguem-se as fases de implementação (*Do*), a verificação (*Check*) e a manutenção/ atualização (*Act*). Uma boa política de segurança da informação nunca está completa, devendo ser mantida, revista e ajustada, de acordo com as necessidades da organização.

Esta política pode futuramente ser complementada com algumas questões que foram levantadas no capítulo 4, que deverão ser definidas em conjunto com a presidência do IPCB, uma vez que comprometem de alguma forma a garantia de privacidade dos utilizadores.

Esta política pode ainda ser utilizada num projeto futuro de definição de um Sistema de Gestão de Segurança da Informação (SGSI), utilizando as orientações da norma ISO 27001.

Com a implementação da política o IPCB poderá, futuramente, criar uma equipa de resposta a incidentes de segurança de forma a melhorar a eficácia geral da reação a incidentes de segurança, articulando as suas ações e a partilha de informação relevante com o centro de coordenação da resposta a incidentes (CERT.PT, 2015) a operar no Centro Nacional de Cibersegurança (CNCS, 2015).

Referências Bibliográficas

Astani, M., 2012. Information security polices' changes in organizations. *Issues in Information Systems*, 13(1), pp.177–184.

B. Fraser, 1997. Site Security Handbook. Available at: https://www.ietf.org/rfc/rfc2196.txt [Accessed March 20, 2015].

Bahsani, S. et al., 2011. Towards a pooling of ITIL V3 and COBIT. *International Journal of Computer Science*, 8(6), pp.185–191.

Casaca, J., 2014. *Gestão do Risco na Segurança da Informação - Conceitos e Metodologias*,

CERT.PT, 2015. Coordenação da resposta a incidentes. Available at: http://www.cncs.gov.pt/cert-pt/coordenacao-da-resposta-a-incidentes/index.html [Accessed October 8, 2015].

CNCS, 2015. Centro Nacional de Cibersegurança. Available at: http://www.cncs.gov.pt/pagina-inicial/index.html [Accessed October 7, 2015].

Darveau, D., 2013. Comparing Cobit 4.1 and Cobit 5. Available at: http://www.isaca.org/chapters3/Las-Vegas/NewsAndAnnouncements/Documents/DENIS - COBIT5-Compare-With-41.pdf.

Davidson, M.A., 2005. Leading by example: The case of IT security in academia. *EDUCAUSE Review*, 40(February), pp.14–22.

Disterer, G., 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 4(April), pp.92–100. Available at: 10.4236/jis.2013.42011\nhttp://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=89254050&site=ehost-live.

Ghormley, Y., 2006. Security Policies and Procedures. *IGI Global*, Chapter XX, pp.320–324.

Greene, S.S., 2014. *Security Program and Policies: Principles and Practices* Second Edi., Pearson.

Imboden, T.R. et al., 2013. How Are Nonprofit Organizations Influenced To Create and Adopt Information Security Policies ? *Issues in Information Systems*, 14(2), pp.166–173.

ISACA, Cobit 5. Available at: https://cobitonline.isaca.org/.

IsecT, Contents of ISO/IEC 27002:2013. Available at: http://www.iso27001security.com/html/27002.html [Accessed April 30, 2015].

ISO/IEC, 2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63411 [Accessed March 30, 2015].

ISO/IEC 27000, 2014. ISO/IEC 27000:2014 Overview and vocabulary. , 1. Available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56891 [Accessed May 13, 2015].

ISO/IEC 27002, 2013. ISO/IEC 27002:2013 Information technology — Security

techniques — Code of practice for information security controls. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533 [Accessed March 30, 2015].

ISO/IEC 27033, 2010. ISO/IEC 27033-3:2010 Threats, design techniques and control issues. Available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51582 [Accessed May 30, 2015].

Johnson, R., 2014. *Security Policies And Implementation Issues* Second Edi. I. JONES AND BARTLETT PUBLISHERS, ed.,

Karyda, M., Kiountouzis, E. & Kokolakis, S., 2005. Information systems security policies: a contextual perspective. *Computers & Security*, 24(3), pp.246–260. Available at: http://www.sciencedirect.com/science/article/pii/S0167404804002378 [Accessed February 13, 2015].

Kerr, D.S. & Murthy, U.S., 2013. The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey. *Information and Management*, 50(7), pp.590–597. Available at: http://dx.doi.org/10.1016/j.im.2013.07.012.

Manson, D., 2008. Security, Privacy, and Politics in Higher Education. *IRM PRESS*, Chapter XI, pp.324–333. Available at: http://www.igi-global.com/gateway/chapter/full-text-pdf/6871.

Martins, R. et al., 2010. ITIL nas universidades : projecto-piloto em gestão de activos de TI no. In *10ª Conferência da Associação Portuguesa de Sistemas de Informação CAPSI 2010*. pp. 1–15. Available at: http://hdl.handle.net/10071/2174.

Nãstase, P., Nãstase, F. & Ionescu, C., 2009. Challenges generated by the implementation of the it standards cobit 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Economic Computation and Economic Cybernetics Studies and Research*, 3.

Omar, A., Alijani, D. & Mason, R., 2011. Information technology disaster recovery plan: Case study. *Academy of Strategic Management Journal*, 10(2), pp.127–142. Available at: http://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=19396104&AN=64876635&h=e+ZuXW1kGSQEgnSXrGsFwszpZ3M5/QzEhps/87wrx8QpJ0OH+igjvSRDN82BXc1C2kMei+cbS5ZgL/QbpMEWuA==&crl=c.

Orakzai, T., 2014. COBIT, ITIL and ISO 27002 Alignment for Information Security Governance in Modern Organisations. *SSRN Electronic Journal*, p.7. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2385845.

SANS, 2013. SANS: Information Security Resources. Available at: http://www.sans.org/security-resources/policies/ [Accessed April 30, 2015].

Solomon, M.G. & Kim, D., 2013. *Fundamentals Of Information Systems Security* Second Edi. I. JONES AND BARTLETT PUBLISHERS, ed.,

Szuba, T., 1998. *Safeguarding your technology Pratical Guidelines for Electronic Education Information Security*, Available at: http://nces.ed.gov/pubs98/safetech/chapter1.asp\nhttp://nces.ed.gov/pubs98/98297.pdf.

Yadav, S.B., 2010. A Six-View Perspective Framework for System Security. *International Journal of Information Security and Privacy*, 4(March), pp.61–92.

Anexo A

Instituto Politécnico de Castelo Branco

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO

Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
01/02/2016	1	Joaquim Santos	Elaboração do documento

Índice

1. FINALIDADE E CONTEXTO

Este documento foi elaborado como meio de orientação para a implementação de controlos de segurança da informação no Instituto Politécnico de Castelo Branco, tendo em consideração os ambientes de risco de segurança da informação específicos da instituição.

No mundo atual, a informação, os sistemas e processos com ela relacionados, as redes e as pessoas envolvidas no seu manuseamento, são muito importantes para o negócio das organizações e, tal como outros ativos, requerem proteção contra vários riscos a que possam estar sujeitos. Verifica-se que no IPCB existe cada vez mais uma dependência do normal funcionamento dos sistemas de informação e infraestruturas de comunicações, pelo que as ameaças informáticas são também uma ameaça regular ao funcionamento da instituição.

Ameaças contra a disponibilidade, integridade e confidencialidade dos sistemas podem resultar em situações prejudiciais para o normal funcionamento do IPCB. Os ativos do IPCB são suscetíveis a ameaças, que podem ser acidentais ou deliberadas. Possuem também algumas vulnerabilidades das quais as ameaças se podem aproveitar para causar danos. Assim, os riscos de segurança da informação estão sempre presentes. A aplicação de uma política de segurança da informação reduz estes riscos, protegendo o IPCB das ameaças e vulnerabilidades, reduzindo o impacto aos seus ativos.

O objetivo desta Política é definir a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação no IPCB.

Os utilizadores deste documento são colaboradores do Instituto Politécnico de Castelo Branco (IPCB), podendo também ser colaboradores de empresas externas com as quais o IPCB tenha contratos.

2. REFERÊNCIAS NORMATIVAS

Este documento foi escrito seguindo diretrizes da família de normas da ISO/IEC 27000, que definem políticas de segurança e linhas de orientação e gestão do risco, que se aplicam na implementação de um sistema de gestão de segurança da informação (SGSI).

3. TERMINOLOGIA BÁSICA DE SEGURANÇA DA INFORMAÇÃO

Ameaça: causa potencial de um incidente indesejado, o que pode resultar em danos para um sistema ou organização.

Ataque: conjunto de ações que visam destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado ou a utilização não autorizada de um ativo.

Atributo: propriedade ou característica de um objeto que pode ser distinguido quantitativa ou qualitativamente por meios humanos ou automatizados.

Autenticação: prestação de garantia de que uma característica reivindicada por uma entidade é correta.

Autenticidade: propriedade em que uma entidade é o que é diz ser.

Competências: capacidade de aplicar conhecimentos e habilidades para alcançar os resultados pretendidos.

Confiabilidade: propriedade de comportamento e resultados consistentes.

Confidencialidade: propriedade em que a informação não é disponibilizada ou divulgada a pessoas não autorizadas, entidades ou processos.

Conformidade: cumprimento de um requisito.

Controlo: no contexto deste documento, meio de gestão de risco.

Disponibilidade: propriedade de ser acessível e utilizável por uma entidade autorizada.

Eficácia: medida em que as atividades planeadas são realizadas e os resultados planeados são alcançados.

Integridade: propriedade de plenitude de exatidão.

Políticas: intenções e direção de uma organização, expressas pela administração.

Processo: conjunto de atividades inter-relacionadas que transforma entradas (*inputs*) em saídas (*outputs*).

Requisito: expectativa ou necessidade expressa, geralmente implícita ou obrigatória.

Risco: efeito da incerteza sobre os objetivos.

Vulnerabilidade: fraqueza de um ativo ou controlo que pode ser explorado por uma ou mais ameaças.

4. REVISÃO DA POLÍTICA

De modo a manter a política adequada e atualizada, deverá ser efetuada revisão anual da mesma, ou quando ocorram mudanças significativas no funcionamento do IPCB.

A revisão deve ser efetuada pelos serviços de informática (SI). Nesta revisão deve ser efetuada uma análise crítica dos sistemas de informação, podendo ser incluídas oportunidades de melhoria, bem como ter em consideração a evolução tecnológica e condições legais.

Após a sua revisão, a política deve ser submetida ao Presidente do IPCB, para que as alterações sejam aprovadas e comunicadas à comunidade do IPCB.

5. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

5.1. Responsabilidades e Papéis pela Segurança da Informação

Nesta secção são definidos os responsáveis e os respetivos papéis para manter a segurança da informação.

Gestão de equipamento de rede
A equipa de infraestruturas dos serviços de informática é responsável pela configuração, gestão e atualização dos equipamentos de rede.

Gestão de utilizadores:

- Utilizadores do domínio (Active Directory): A equipa de infraestruturas dos SI é responsável pela gestão, atualização e remoção (que deve ser comunicada pelos serviços de recursos humanos) dos utilizadores do domínio.
- Utilizadores de correio eletrónico: A equipa de infraestruturas dos SI é responsável pela gestão, atualização e remoção (que deve ser comunicada pelos serviços de recursos humanos) das contas de correio eletrónico.
- Utilizadores da aplicação SIGES: O responsável dos serviços académicos é responsável pela inserção, gestão, atualização e remoção dos utilizadores da aplicação, assim como atribuição dos respetivos privilégios.
- Utilizadores da aplicação Primavera: O responsável dos serviços financeiros e patrimoniais é responsável pela inserção, gestão, atualização e remoção dos utilizadores da aplicação, assim como atribuição dos respetivos privilégios.

Cópias de segurança
A equipa de infraestruturas dos SI é responsável pela gestão e manutenção das cópias de segurança, que devem ser realizadas de acordo com o definido no sistema de gestão de qualidade.

6. SEGURANÇA EM RECURSOS HUMANOS

O objetivo desta secção é assegurar que os colaboradores do IPCB e colaboradores externos estão consciencializados para cumprir com as suas responsabilidades pela segurança da informação.

6.1. Termos e Condições de Contratação

No ato da contratação de novos funcionários, deve ser transmitida a Política de Segurança do IPCB, que deve ser lida pelo novo funcionário e assinada concordando com a sua aceitação.

Os contratos de fornecedores externos, que incluam acesso à informação e à infraestrutura do IPCB, devem conter cláusulas de segurança informática e privacidade que devem ser cumpridas por todos os seus colaboradores.

6.2. Responsabilidades do Presidente do IPCB

O Presidente do IPCB deve assegurar que todos os colaboradores do IPCB e colaboradores externos cumpram as normas de segurança da informação, de acordo com o estabelecido nas políticas e procedimentos do IPCB.

Deve ser assegurado que os funcionários e colaboradores externos:

- Tenham conhecimento das suas responsabilidades e deveres no âmbito da segurança da informação, antes de obter acesso a informações sensíveis ou aos sistemas de informação;
- Tenham conhecimento da política de segurança;
- Sejam consciencializados das suas responsabilidades e dos danos que podem causar ao não cumprirem com as mesmas.

7. GESTÃO DE ATIVOS

7.1. Responsabilidades pelos Ativos

O objetivo desta secção é identificar os ativos do IPCB e definir as responsabilidades apropriadas para a proteção dos mesmos.

7.1.1. Inventário dos Ativos

Computadores
A equipa de infraestruturas é responsável por gerir e manter atualizados os inventários relativos aos computadores de cada escola, e serviço a que estão afetos, devendo ser identificado:

- Localização do equipamento;
- Sistema operativo instalado;
- Capacidade de armazenamento e memória;
- Pessoa a quem o equipamento está afeto.

Equipamentos de rede
A equipa de infraestruturas dos SI é responsável por manter atualizado o inventário dos equipamentos de rede (*switch*, pontos de acesso à rede sem fios, etc.), bem como a respetiva localização.

Destruição de ativos
A equipa de infraestruturas dos SI é responsável por apagar os dados de sistemas de armazenamento obsoletos ou avariados, e de equipamento que seja abatido. Este processo deve ficar registado num auto de abate, onde deve ficar registado o equipamento e a data do abate. Após este processo, a equipa de infraestruturas deve remover o ativo do inventário respetivo.

7.1.2. Uso Aceitável dos Ativos

Os colaboradores do IPCB e colaboradores externos devem fazer uma utilização responsável e dentro dos limites legais da lei República Portuguesa, dos ativos e da rede do IPCB, nomeadamente:

- Não instalar ou desinstalar *software* nos equipamentos pertencentes ao IPCB, sem a devida autorização;
- Não descarregar ficheiros protegidos por direitos de autor (ilegais);
- Não partilhar ficheiros protegidos por direitos de autor;
- Não aceder ou eliminar dados a que não estão autorizados.

7.1.3. Devolução de Ativos

Os colaboradores do IPCB e colaboradores externos, após o encerramento das suas atividades ou términus de contrato, devem devolver todos os ativos do IPCB que estejam na sua posse.

Deve ser instituído um processo de cessação de atividades e tratamento dos dados que contemple a devolução de todos os equipamentos físicos e eletrónicos, de propriedade do IPCB.

7.2. Classificação da Informação

O objetivo desta secção é assegurar que a informação recebe um nível adequado de proteção, de acordo com a sua importância para o IPCB.

7.2.1. Classificação da Informação

A informação deve ser classificada em termos do seu valor, sensibilidade e criticidade, para evitar modificação ou divulgação não autorizada.

Foram definidos três níveis de classificação de informação:

- Nível 1 – informação muito crítica: a este nível pertencem dados referentes à base de dados de gestão de alunos, dados relativos à base de dados de contabilidade e gestão de recursos humanos; O acesso a estes dados deve estar alinhado com a política de controlo de acesso definido na secção 8.4.1. (Restrição de acesso à informação).
- Nível 2 – informação crítica: a este nível pertencem dados relativos a:
    - Bases de dados afetas a todos os sítios de Internet do domínio ipcb.pt.
    - Informação partilhada entre vários colaboradores, do mesmo serviço ou de serviços diferentes, por exemplo: uma pasta acessível apenas pelos colaboradores afetos ao serviço de aprovisionamento e uma pasta acessível pelos serviços de recursos humanos e pelos serviços de contabilidade.
    - Configurações de servidores.
- Nível 3 – informação pouco crítica: a este nível pertencem os dados pessoais, do ponto de vista das funções do colaborador, por exemplo: enunciados de testes de um

professor. Estes dados encontram-se no sistema de armazenamento do IPCB e é acessível apenas pelo respetivo colaborador.

8. CONTROLO DE ACESSOS

8.1. Acesso às Redes e aos Serviços de Rede

O acesso aos serviços internos e externos de rede deve ser controlado de modo a evitar o comprometimento da segurança e respeito pelos regulamentos. O acesso a serviços críticos e serviços internos do IPCB, através de ligações externas só é permitido quando justificado e através da utilização de VPN.

Acesso à rede sem fios

Todos os colaboradores do IPCB têm acesso à rede sem fios, de nome *eduroam, sendo* necessário que se registem no sistema de gestão de credencias, de acordo com o definido na secção 8.2.1. (Registo e cancelamento de utilizadores).

Para que colaboradores externos tenham acesso à rede sem fios deve ser solicitado aos serviços de informática (equipa de infraestruturas) a criação de um utilizador com perfil de convidado, sendo necessário indicar aos SI o nome do convidado, o âmbito da colaboração com o IPCB e a data final da colaboração, para que o utilizador seja desativado.

8.2. Gestão de Acesso dos Utilizadores

8.2.1. Registo e Cancelamento de Utilizadores

Registo de utilizadores

O registo de utilizadores é efetuado em dois passos:

1. Mediante o perfil de utilizador, os seus dados são inicialmente inseridos na aplicação de gestão de recursos humanos ou gestão académica. Os responsáveis pela introdução dos dados na respetiva aplicação são:
    a. Serviço de recursos humanos no caso dos utilizadores com perfil de docente e não docente;
    b. Serviços académicos no caso de utilizadores com perfil de aluno;
    c. Gabinete de relações internacionais no caso de utilizadores com perfil de alunos Erasmus.
2. O utilizador deve aceder ao sistema de gestão de credenciais e efetuar o seu registo. Neste sistema é solicitado ao utilizador para escolher um endereço de correio eletrónico e palavra-passe. Estas credenciais servem para autenticação em várias aplicações do IPCB, nomeadamente no acesso à rede sem fios e acesso ao portal académico.

Cancelamento de utilizadores

Quando um colaborador termina as suas funções, deixando de colaborar com o IPCB, deve ser comunicado, pelo serviço de recursos humanos, serviços académicos ou pelo Presidente do

IPCB, aos serviços de informática para que o utilizador seja cancelado/ suspenso ou removido do sistema, de modo a não ter acesso à informação.

8.2.2. Gestão de Direitos de Acesso

Os serviços de informática são responsáveis por atribuir os direitos de acesso aos utilizadores, após autorização do Presidente do IPCB, aos sistemas e aplicações existentes, com exceção da aplicação de gestão académica e aplicação de gestão financeira, patrimonial e de recursos humanos.

Aplicação de Gestão Académica (*BackOffice*)
O responsável dos serviços académicos gere os utilizadores da aplicação e atribui os respetivos direitos de acesso aos módulos.

Aplicação de Gestão Financeira, Patrimonial e de Recursos Humanos
O responsável do serviço financeiro e patrimonial gere os utilizadores da aplicação e atribui os respetivos direitos de acesso aos módulos.

8.2.3. Análise dos Direitos de Acesso dos Utilizadores

Anualmente os serviços de informática devem fornecer ao Presidente do IPCB a lista de todos os utilizadores e os respetivos privilégios de acesso à informação que detêm, de modo a serem revistos.

8.2.4. Remoção ou Ajuste de Direitos de Acesso

Sempre que um colaborador é transferido para um novo serviço devem ser ajustados os seus direitos de acesso.

Quando um colaborador termina as suas funções, deixando de colaborar com o IPCB, devem ser-lhe removidos ou suspensos todos os privilégios de acesso.

Qualquer uma das alterações anteriores deve ser comunicada, pelo serviço de recursos humanos ou pelo Presidente do IPCB, aos serviços de informática para que procedam à devida alteração.

8.3. Responsabilidades dos Utilizadores

8.3.1. Utilização da Informação de Autenticação

Os principais sistemas de informação do IPCB estão protegidos por palavra-passe, por forma a assegurar que o acesso à informação é feito apenas por pessoas autorizadas. Os utilizadores não devem fornecer as suas credenciais de acesso a outras pessoas.

Qualquer tentativa de obter acesso não autorizado ou de forçar a entrada em sistemas não autorizados é considerada como comportamento indevido, e será tratada em conformidade com a lei.

A definição da palavra-passe deve ser feita de acordo com os requisitos identificados na secção 8.4.3. (Sistema de gestão de palavra-passe) devendo os utilizadores ter em consideração que:

- Devem definir palavra-passe das quais se conseguem lembrar facilmente (evitando ter de as escrever em papeis);
- A palavra-passe não deve ser baseada em informação pessoal, por exemplo: nomes de familiares próximos, números de telefone, datas de aniversário, etc.

8.4. Controlo de Acessos aos Sistemas e Aplicações

8.4.1. Restrição de Acesso à Informação

Existem no IPCB três tipos de informações (dados) que estão identificados:

- Tipo 1: Dados de colaboradores docentes e não docentes;
- Tipo 2: Dados de alunos;
- Tipo 3: Dados de fornecedores.

Dependendo do tipo de dados, os colaboradores que têm responsabilidades de acesso são, respetivamente:

- Tipo 1: Colaboradores pertencentes ao serviço de recursos humanos;
- Tipo 2: Colaboradores pertencentes aos serviços académicos, gabinete de relações internacionais e serviços de ação social;
- Tipo 3: Colaboradores pertencentes aos serviços financeiros e patrimoniais e serviços de aprovisionamento.

Os computadores dos utilizadores com privilégios de acesso às aplicações B*ackOffice* de gestão académica e de gestão financeira, patrimonial e de recursos humanos devem ser identificados de modo que apenas esses computadores tenham permissões de acesso aos respetivos servidores e aplicações.

8.4.2. Procedimentos Seguros de Entrada no Sistema

O acesso a qualquer uma das aplicações é feito com recurso à introdução de um nome de utilizador (*login*) e palavra-passe de conhecimento exclusivo do colaborador identificado em cada um dos serviços. Os utilizadores não devem divulgar as suas credenciais de acesso.

8.4.3. Sistema de Gestão de Palavra-passe

A palavra-passe de utilizadores operacionais devem ser alteradas periodicamente, de 6 em 6 meses, e não deve ser mostrada no ecrã quando for digitada. De modo a evitar erros, deve existir

um procedimento de confirmação da palavra-passe. A palavra-passe deve cumprir requisitos mínimos de qualidade, nomeadamente:

- Não conter o nome de conta do utilizador;
- Ter comprimento de pelo menos nove caracteres;
- Conter caracteres de três das quatro categorias seguintes:
    - Letras maiúsculas (A a Z);
    - Letras minúsculas (a a z);
    - Números base (0 a 9);
    - Caracteres não alfanuméricos tais como: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

8.4.4. Palavra-passe de Administrador

Todas as palavras-passe de administrador devem obedecer aos requisitos definidos na secção 8.4.3 "Sistema de gestão de palavra-passe".

Deve existir um repositório seguro de palavras-passe de administrador, onde sejam registadas as credenciais de acesso (nome de utilizador e palavra-passe), localização, nome e endereço do servidor ou equipamento a que as credenciais digam respeito. O repositório deve estar protegido por uma palavra-passe, do conhecimento dos membros da equipa de infraestruturas. Esta palavra-passe deve ser entregue ao Presidente do IPCB em envelope fechado para utilização em casos excecionais, em que seja necessário acesso de administrador a um sistema e não esteja presente nenhum dos membros da equipa de Infraestruturas.

9. SEGURANÇA FÍSICA E DO AMBIENTE

9.1. Áreas Seguras

Centro de dados

O acesso ao centro de dados é restrito aos funcionários dos serviços de informática (SI) do IPCB. Qualquer outro colaborador que pretenda aceder a esta sala tem de ser acompanhado por um funcionário dos SI. Nesta sala encontram-se os servidores de dados e aplicações que servem o IPCB. A entrada nesta sala é controlada por fechadura mecânica instalada na porta, estando a chave guardada nos SI.

Bastidores

O acesso aos bastidores que contêm equipamento de rede, existentes nos edifícios do IPCB (escolas, residências de estudante, etc.), é restrito aos funcionários dos serviços de informática. Os bastidores devem estar fechados à chave e a chave deve estar guardada nos respetivos serviços de informática.

9.2. Equipamentos

9.2.1. Utilidades

Centro de dados

A temperatura deve ser controlada de modo a manter a sala com uma temperatura ambiente inferior 22ºC, por forma a proteger os equipamentos instalados. Esta sala deve possuir um sistema que assegure a autonomia da mesma no caso de falta de energia. Caso a energia não seja restabelecida após 20 minutos, toda a infraestrutura instalada na sala deve ser desligada. O centro de dados deve estar equipado com porta corta-fogo, detetor de incêndios e extintores de CO2, que devem ser utilizados em caso de incêndio.

9.2.2. Segurança da Cablagem

Deve ser mantido e atualizado o esquema da rede de dados cablada. Neste esquema devem constar todas as ligações, a localização dos bastidores, os locais de passagem dos cabos e o tipo de cablagem. A instalação elétrica deverá ser feita de modo a estar em conformidade com as especificações do fabricante, prevenir danos aos equipamentos e garantir um fornecimento seguro de energia.

9.2.3. Manutenção

Mensalmente deve ser efetuada uma vistoria, por parte da equipa de infraestruturas, a todos os bastidores de modo a verificar possíveis anomalias nos equipamentos. Deve ser efetuado o registo das mesmas, indicando a data da realização, o nome do colaborador e registando informação sobre o estado do equipamento.

10. SEGURANÇA NAS OPERAÇÕES

10.1. Responsabilidades e Procedimentos Operacionais

A documentação de procedimentos operacionais deve ser mantida em local seguro, acessível apenas a pessoas autorizadas. Os sistemas aplicacionais devem ser adequadamente protegidos, garantindo que a sua utilização é feita exclusivamente por utilizadores autorizados.

Os serviços de informática devem, mensalmente ou sempre que se justifique, proceder à instalação de atualizações de sistema operativo e de outros programas instalados, e analisar possíveis anomalias nos computadores instalados no IPCB.

10.2. Proteção Contra Códigos Maliciosos

Devem ser implementados controlos para a deteção e prevenção de programas maliciosos, assim como procedimentos para a consciencialização dos utilizadores. A proteção contra

programas maliciosos deve ser baseada na consciencialização de segurança, no controlo de acessos adequado e nos mecanismos de gestão de alterações.

10.3. Cópias de Segurança

De acordo com a sua classificação, secção 7.2.1 (Classificação da informação), os dados devem ser guardados durante diferentes períodos de tempo:

- Nível 1 – deste tipo de dados devem existir cópias de segurança diárias dos últimos 7 dias, uma cópia mensal (último dia do mês) dos últimos 12 meses, anual (último dia do ano) dos últimos 10 anos;
- Nível 2 – deste tipo de dados devem existir cópias de segurança diárias dos últimos 7 dias, uma cópia mensal (último dia do mês) e dos últimos 12 meses;
- Nível 3 – deste tipo de dados devem existir cópias de segurança diárias dos últimos 7 dias.

As cópias de segurança não devem estar guardadas na mesma localização onde se encontra o centro de dados do IPCB.

Apenas são efetuadas cópias de segurança dos dados que se encontram nas pastas, partilhadas ou pessoais, disponibilizadas pelos SI. Por este motivo, não deve ser permitido guardar informação nos discos rígidos instalados nos computadores.

Anualmente deve ser verificada, através de um restauro aleatório de cada um dos níveis, o correto funcionamento das cópias de segurança.

10.4. Registos e Monitorização

Deve ser implementado um sistema centralizado de recolha e análise de registos de eventos (*logs*) de todos os servidores e equipamento de rede, capaz de gerar alertas (por exemplo: mensagens de correio eletrónico) enviando-os para a equipa de infraestruturas. Diariamente devem ser verificados e analisados, pela equipa de infraestruturas, os eventos recolhidos.

10.5. Controle de *Software* Operacional

Todos os programas instalados nos computadores pertencentes ao IPCB devem estar licenciados. Apenas os utilizadores afetos aos serviços de informática (SI) estão autorizados a instalar programas nos computadores do IPCB.

11. SEGURANÇA NAS COMUNICAÇÕES

11.1. Gestão da Segurança em Redes

11.1.1. Controlo das Redes

Os serviços de informática devem manter atualizados os esquemas de rede, contendo a identificação dos equipamentos, e as ligações entre os mesmos.

Os serviços de informática devem realizar um inventário de todas as tomadas de rede. As mesmas devem ser identificadas com a sua numeração, localização, informação do equipamento ligado, bastidor e número da porta do equipamento de rede a que está ligada. As portas dos equipamentos de rede que não estejam identificadas no inventário devem ser configuradas como inativas (*shutdown*/ *disable*).

11.1.2. Segregação de Redes

As redes do IPCB devem estar divididas em diferentes domínios de rede. Devem existir domínios diferentes por escola, existindo ainda domínios diferentes no edifício da Presidência e Serviços Centrais. O acesso entre os diferentes domínios de rede deve ser controlado pelo uso de uma *firewall* ou *router*.

Devem ser identificados, de acordo com o definido no controlo de acessos, os computadores com acesso a servidores aplicacionais de forma a serem adicionados à respetiva *firewall*.

11.2. Transferência de Informação

11.2.1. Acordos de Confidencialidade e não Divulgação

A informação considerada confidencial deve ser protegida através de sistemas de criptografia. Quando se encontra em forma escrita deverá ser protegida através de proteções físicas adequadas. A troca de informação em suporte físico ou lógico com fornecedores externos só deve ser feita após a definição de uma política sobre os termos da comunicação e sobre as restrições à utilização dessa informação.

12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

12.1. Requisitos de Segurança de Sistemas de Informação

Antes de se iniciar o desenvolvimento de qualquer sistema é necessário identificar os requisitos de segurança. Os requisitos de segurança devem ponderar o valor dos ativos de informação que estão envolvidos e os danos causados por possíveis perdas ou violação desses ativos, seja de forma voluntária ou involuntária. A segurança deve ser arquitetada em simultâneo com os sistemas.

12.2. Dados para Teste

12.2.1. Proteção dos Dados para Teste

Na execução de testes, não devem ser utilizados dados reais que sejam confidenciais ou privados. Caso seja indispensável a utilização desse tipo de dados, deve ser pedida autorização ao respetivo proprietário e devem ser implementadas medidas rigorosas de segurança.

13. RELACIONAMENTO COM FORNECEDORES

13.1. Segurança da Informação no Relacionamento com os Fornecedores

Os contratos com fornecedores de serviços que colaborem com o IPCB, que incluam acesso a informação, devem cumprir com os requisitos de segurança definidos pelo IPCB, com o objetivo de garantir a privacidade e confidencialidade da informação.

Aos contratos, devem ser adicionadas políticas que identifiquem e exijam os controlos de segurança da informação para disponibilizar o acesso às informações do IPCB ao fornecedor.

Os requisitos de segurança da informação relevantes devem estar estabelecidos e acordados com cada fornecedor antes que possa o mesmo aceda, processe ou armazene qualquer tipo de informação do IPCB.

13.2. Gestão da Entrega do Serviço do Fornecedor

13.2.1. Monitorização e Análise Crítica de Serviços com Fornecedores

Deve ser efetuada regularmente uma monitorização e análise crítica dos serviços fornecidos, de modo a garantir que os termos e condições dos acordos de segurança estão a ser cumpridos. Devem ser fornecidas informações sobre eventuais incidentes de segurança e analisados de forma a resolver e gerir quaisquer problemas identificados.

14. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

14.1. Gestão de Incidentes de Segurança da Informação e Melhorias

14.1.1. Responsabilidades e Procedimentos

Devem ser implementadas responsabilidades e procedimentos de gestão que assegurem respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.

As responsabilidades pela gestão devem ser estabelecidas para assegurar que os seguintes procedimentos são desenvolvidos e comunicados, de forma adequada:

- Preparação e planeamento de respostas a incidentes;
- Monitorização, deteção, análise e notificação de incidentes e eventos de segurança da informação;
- Registos das atividades de gestão de incidentes;
- Avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da informação;

Qualquer deteção de incidentes de segurança deve ser comunicada aos serviços de informática, para que se proceda à sua resolução.

14.1.2. Notificação de Eventos de Segurança da Informação

Todos os incidentes e vulnerabilidades são objeto de registo, por forma a permitir uma resposta célere aos problemas. Todos os colaboradores do IPCB e colaboradores externos são responsáveis por notificar qualquer evento de segurança da informação o mais rapidamente possível aos serviços de informática. Entendendo-se por evento de segurança da informação os seguintes pontos:

- Mau funcionamento de *software* ou *hardware*;
- Violação de acesso;
- Violação da disponibilidade, confidencialidade e integridade da informação;
- Erros humanos;
- Violações de procedimentos de segurança física;
- Controlo de segurança ineficaz;

15. ASPETOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

15.1. Continuidade da Segurança da Informação

15.1.1. Plano de Continuidade da Segurança da Informação

Devem ser elaborados planos de contingência, para que, em caso de falha ou interrupção de serviço dos sistemas de suporte à informação considerada muito crítica, nomeadamente gestão académica e gestão financeira, patrimonial e de recursos humanos, os processos não fiquem parados. Assim, quando ocorram este tipo de situações, os serviços respetivos devem guardar as informações em papel para posteriormente serem inseridas nas aplicações.

15.1.2. Verificação, Análise Crítica e Avaliação da Continuidade da Segurança da Informação

Os controlos de continuidade da segurança da informação, estabelecidos e implementados, devem ser verificados em intervalos regulares, garantindo que são válidos e eficazes em situações adversas. Assim, o plano de continuidade de negócio deve ser testado com frequência

mínima de uma vez ao ano, simulando várias condições de desastre. As falhas detetadas no decorrer das simulações devem ser avaliadas pelo responsável da segurança e corrigidas no plano.

15.2. Redundâncias

15.2.1. Disponibilidade dos Recursos de Processamento da Informação

Devem ser identificados os requisitos quanto à disponibilidade dos sistemas de informação, devendo ser considerados componentes e arquiteturas redundantes assegurando a disponibilidade dos mesmos.

Os sistemas de informação redundantes devem ser testados, de 6 em 6 meses, para assegurar que na transferência de um componente para outro, quando existe falha do primeiro, o funcionamento seja assegurado conforme esperado.

16. CONFORMIDADE

16.1. Conformidade com Requisitos Legais e Contratuais

16.1.1. Identificação da Legislação Aplicável e de Requisitos Contratuais

Todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes devem estar explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização, de acordo com a legislação aplicável:

- Constituição da República – artigo 35º, Utilização da informática.
- Decreto-Lei n.º 256/2003, de 21 de outubro – Transpõe para a ordem jurídica nacional a Diretiva n.º 2001/115/CE, do Conselho, de 20 de Dezembro, que altera a Diretiva n.º 77/388/CEE, tendo em vista simplificar, modernizar e harmonizar as condições aplicáveis à faturação em matéria de imposto sobre o valor acrescentado.
- Decreto-Lei n.º 290-D/99, de 2 de agosto – Regula a validade, eficácia e valor probatório dos documentos eletrónicos e a assinatura digital.
- Decreto-Lei n.º 62/2003, de 3 de abril – Transpõe a diretiva 1999/93/CE – relativa a um quadro legal sobre assinaturas eletrónicas, tendo alterado algumas disposições do DL 290-D/99.
- Decreto-Lei n.º 88/2009, de 9 de abril – Estabelece o regime jurídico dos documentos eletrónicos e da assinatura digital, e à primeira alteração ao Decreto-Lei n.º 116-A/2006, de 16 de Junho, que cria o Sistema de Certificação Eletrónica do Estado.
- Decreto-lei n.º 7/2004, de 7 de janeiro - Transpõe para a ordem jurídica interna a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre Comércio Eletrónico) bem como o artigo 13º da Diretiva n.º 2002/58/CE, de 12 de Julho de 2002, relativa ao

tratamento de dados pessoais e a proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à Privacidade e às Comunicações Eletrónicas).

- Lei n.º 109/2009, de 15 de setembro – Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.
- Decreto-lei n.º 252/94, de 20 de outubro – Transpõe para a ordem jurídica interna a Diretiva n.º 91/250/CEE, do Conselho, de 14 de Maio, relativa ao regime de proteção jurídica dos programas de computador.

16.1.2. Direitos de Propriedade Intelectual

Os procedimentos devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de *software* proprietários. Aplicando-se a seguinte legislação:

- Decreto-lei n.º 63/85, de 14 de março – Aprova o Código do Direito de Autor e dos Direitos Conexos.
- Decreto-lei n.º 252/94, de 20 de outubro – Transpõe para a ordem jurídica interna a Diretiva n.º 91/250/CEE, do Conselho, de 14 de Maio, relativa ao regime de proteção jurídica dos programas de computador.

16.1.3. Proteção e Privacidade de Informações de Identificação Pessoal

A privacidade e a proteção das informações de identificação pessoal devem ser asseguradas conforme requerido por legislação e regulamentação:

- Lei n.º 67/98, de 26 de outubro - Lei da Proteção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Dir. n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados)
- Lei n.º 41/2004, de 18 de agosto – Transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.