ISCTE Business School
Instituto Universitário de Lisboa

GESTÃO DE CIBERSEGURANÇA EM ORGANIZAÇÕES FINANCEIRAS

Pedro Miguel Lopes Martins da Silva

Projeto submetido como requisito parcial para obtenção do grau de Mestre em Gestão de Empresas

Orientador:
Carlos José Corredoura Serrão, *PhD*
Escola de Tecnologia e Arquitetura ISCTE-IUL/ISTAR-IUL

Coorientador:
Luís Carlos Barruncho dos Santos Gonçalves, *MsC*
Escola de Tecnologia e Arquitetura ISCTE-IUL/ISTA
Banco de Portugal

outubro 2018

If ignorant both of your enemy and yourself,
you are certain to be in peril.

- The Art of War, Sun Tzu

RESUMO

Pode-se dizer que a informação é o ouro da época moderna. As organizações estão cada vez mais dependentes da informação para os seus processos de negócio e cada vez mais sentem a necessidade de proteger esse ativo tão precioso. Contudo, são muitas e muito relevantes as ameaças que se colocam no contexto em que as organizações desenvolvem a sua atividade e pode-se afirmar que nunca foi tão difícil como agora proteger a informação interna das organizações.

Neste contexto, ganha relevância o conceito de cibersegurança, em que a segurança não deve mais ser entendida como uma preocupação quase exclusiva das TI, mas tem que ser compreendida e encarada de uma forma global, por toda a organização. Para ser eficaz, a gestão da cibersegurança tem que ser implementada de forma transversal na organização e tem que ser assumida e patrocinada pela gestão de topo.

Neste sentido, é importante que os gestores olhem cada vez mais e de forma mais séria para a gestão da cibersegurança e apliquem modelos reconhecidamente adequados de gestão e governança da cibersegurança, que deem garantias de controlo de risco e que contemplem todas as vertentes da organização, ao nível de processos, pessoas e tecnologias.

Este trabalho pretende dar um contributo nesse sentido. Partindo da identificação e integração de vários modelos e guias ligados à gestão da cibersegurança, foca-se nos aspetos particulares e específicos do setor financeiro, criando assim uma ferramenta passível de ser utilizada em ambiente organizacional no âmbito da implementação de projetos nesta área.

Palavras-chave: Segurança, Informação, Cibersegurança, Governança

Classificação JEL:
L86 - Information and Internet Services; Computer Software
D83 - Search; Learning; Information and Knowledge; Communication; Belief; Unawareness

ABSTRACT

One can say that information is the gold of modern age. Organizations are getting increasingly more dependent on information for their business processes and consequently feel the need to protect that precious asset even more. However, the threats that are placed in the context in which organizations carry out their activities are many and very relevant and it has never been as difficult as it is now to protect their internal information.

In this context, the concept of cybersecurity becomes highly relevant. Security should no longer be understood as a quasi-exclusive concern of IT, and instead, it has to be understood and addressed as a global concern throughout the organization. In order for it to be effective, cybersecurity management has to be implemented across the organization and it has to be assumed and sponsored by top management.

In this regard, it is important that managers start taking cybersecurity management more and more seriously and applying well-recognized cybersecurity management and governance frameworks, in order to provide guarantees in terms of risk control and to address all aspects of the organization, at the processes, people and technologies levels.

It is this work's intent to make a contribution in this sense. Based on the identification and integration of several frameworks and guides related to cybersecurity management, it focuses on the particularities and specific aspects of the financial sector, thus creating a tool that can be used in an organizational environment for the implementation of projects in this area.

Keywords: Security, Information, Cybersecurity, Governance

JEL Classification:
L86 - Information and Internet Services; Computer Software
D83 - Search; Learning; Information and Knowledge; Communication; Belief; Unawareness

AGRADECIMENTOS

Os meus agradecimentos vão, em primeiro lugar, para toda a minha família, que me apoiou nesta demanda. E um agradecimento especial à minha esposa Raquel e às minhas filhas Inês e Madalena, pelo apoio e pelo suporte que são na minha vida.

Deixo aqui também um grande agradecimento aos meus orientador e coorientador Carlos Serrão e Luís Gonçalves, pela disponibilidade, paciência, flexibilidade e pela resposta pronta e assertiva que sempre me deram às dúvidas e exigências do trabalho.

Agradeço igualmente a todos os meus professores e colegas do *Executive MBA* e sobretudo àqueles que fizeram parte do meu grupo de trabalho – Dina Santos, José Santos, Jorge Penedo, Carlos Morais e Clara Costa. O *MBA* foi uma experiência única e marcante e tal deve-se sobretudo aos momentos desafiantes que passei com eles. Ainda uma referência especial à Dina, pela grande ajuda que me deu na revisão deste trabalho.

Por fim, um agradecimento ao Banco de Portugal, e a quem o representa, pelo apoio logístico e financeiro que me proporcionaram e pela oportunidade que me deram de poder realizar este trabalho.

página intencionalmente deixada em branco

ÍNDICE

ÍNDICE DE QUADROS

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AIM – *Asset Inventory Management*
APO – *Align, Plan and Organise*
BAI – *Build, Acquire and Implement*
BCE – Banco Central Europeu
BdP – Banco de Portugal
BIS – *Bank of International Settlements*
CE – Comissão Europeia
CEO – *Chief Executive Officer*
CFO – *Chief Financial Officer*
CISO – *Chief Information Security Officer*
CNSS – *Committee on National Security Systems*
COBIT – *Control Objectives for Information and Related Technology*
CROE – *Cyber Resilience Oversight Expectations*
CSIRT – *Computer Security Incident Response Team*
CTI – *Cyber Threat Intelligence*
DSS – *Deliver, Service and Support*
EDM – *Evaluate, Direct and Monitor*
EMBA – *Executive Master in Business Administration*
ENISA – *European Union Agency for Network and Information Security*
ERMC – *Enterprise Risk Management Committee*
EUA – Estados Unidos da América
GRC – *Governance, Risk and Compliance*
GTI – Governança de Tecnologias de Informação
IAM – *Identity and Access Management*
IP – *Internet Protocol*
IPS – *Intrusion Prevention System*
ISACA – *Information Systems Audit and Control Association*
ISM – *Information Security Manager*
ISMS - *Information Security Management System*
ISSC – *Information Security Steering Committee*
KPI – *Key Performance Indicators*
KRI – *Key Risk Indicators*
MEA – *Monitor, Evaluate and Assess*
NIST – *National Institute of Standards and Technology*
PPF – Política de Prontidão Forense
PWC - *Price Waterhouse Coopers*
RGPD – Regulamento Geral de Proteção de Dados
SDLC - *System Development Life Cycle*
SI – Sistemas de Informação
SIEM – *Security Information and Event Management System*
SOC – *Security Operations Center*
SW – *Software*
TI – Tecnologias de Informação
UE – União Europeia
WEF – *World Economic Forum*

página intencionalmente deixada em branco

1. Sumário Executivo

1.1. Tema

O tema escolhido para o trabalho – **gestão da cibersegurança em organizações financeiras**, justifica-se, em primeiro lugar, pela constatação que o autor faz da existência de várias dificuldades e dúvidas relativas ao que deve constituir uma adequada gestão de cibersegurança nas organizações, importando dar respostas que ajudem ao esclarecimento das questões existentes. Em segundo lugar, o trabalho tem um enfoque no setor financeiro, por opção do autor. Concretamente, embora o trabalho tenha um caráter abrangente de aplicação, foi desenvolvido para aplicação concreta num banco central do eurosistema, designado no âmbito deste trabalho por "Banco Central".

O primeiro fator a relevar neste tema é o de que a informação é, cada vez mais, um ativo precioso e de importância fulcral para as organizações. Cada vez mais, as organizações dependem da informação para a sua missão. Cada vez mais, a informação está intrincada nos processos de negócio. Os estudos e investigações disponíveis e que se encontram referidos na revisão de literatura podem divergir na definição do grau e alcance dessa importância, mas são convergentes no sentido da crescente dependência que os processos de negócio das organizações têm relativamente à informação.

Acresce que existem ameaças muito significativas à segurança de informação e que as mesmas têm uma tendência crescente quer em número, quer em sofisticação. Neste contexto, é natural um enfoque crescente sobre a necessidade da boa gestão das Tecnologias de Informação (TI).

Adicionalmente, a análise focou-se não apenas em segurança de informação, mas alargou-se o campo de análise para o mundo da cibersegurança, enquanto conceito mais abrangente e incontornável na envolvente atual. A estratégia de defesa atual deve passar por um conjunto de medidas organizacionais, envolvendo pessoas, processos e tecnologia, e com estes três vetores atuando de forma coordenada e concertada. E aqui tem que entrar de forma clara a gestão e a governança de cibersegurança, com um papel chave na definição e promoção desses fios condutores que interligam todas as peças e que colocam a cibersegurança a funcionar de forma coordenada, dentro da organização.

Assim, neste quadro de envolvência, este trabalho partiu da seguinte questão de investigação: "**Face ao problema das ameaças que pendem sobre os ativos de informação, qual o modelo**

de gestão de cibersegurança, a aplicar no Banco Central, que melhor responde aos desafios que se colocam no contexto atual?".

1.2. Abordagem

O formato seguido para o trabalho foi o de um Projeto-Empresa.

Para a definição do projeto em perspetiva, com base na revisão da literatura, identificou-se o *COBIT 5* (ISACA, 2012a) como o modelo de gestão e governança de TI mais amplamente utilizado nas organizações e que é reconhecido como permitindo integrar outros modelos, de forma eficaz, tendo sido por isso utilizado como base do trabalho.

Contudo, a utilização do *COBIT* não é suficiente para os objetivos preconizados, dado que se trata de um modelo genérico, de alto nível, com flexibilidade e adaptabilidade, mas que não permite *de per si* o enfoque que se pretende dar a este trabalho no campo da cibersegurança e no setor financeiro, o que requer a utilização de outras ferramentas. Assim, concretamente, para a metodologia de implementação do projeto, aproveitou-se o desenvolvimento específico – *COBIT 5 implementation*, o qual constitui um guia de implementação baseado numa abordagem de ciclo de vida de melhoria contínua (ISACA, 2012c). Com base nesse guia, foram identificadas as etapas a considerar para o projeto. Contudo, tendo este guia um caráter genérico de aplicação, como identificado pela revisão de literatura, houve que identificar e tratar os aspetos particulares associados ao contexto concreto, os quais estão apresentados no capítulo 7 deste trabalho.

De forma complementar, no âmbito da referida metodologia do ciclo de vida de implementação, uma das principais etapas, e aquela que se considera mais relevante para este trabalho, consiste na análise e avaliação do estado de maturidade da organização, que permita perceber onde se está e perspetivar onde se pretende chegar. Ou seja, para uma implementação com sucesso, é fundamental que se identifique de forma clara qual o estado atual da cibersegurança na organização, que se estabeleçam metas e, consequentemente, que se identifiquem as lacunas sobre as quais haverá que identificar e implementar medidas concretas (ISACA, 2012c). Para isso, no âmbito deste trabalho, buscou-se a resposta à questão de como identificar o estado de maturidade da cibersegurança numa organização, através do cruzamento de vários modelos identificados na revisão de literatura e os quais se focam em contextos particulares. Assim, concretamente, utilizaram-se: i) o *COBIT 5 for Information Security* (ISACA, 2012b), para identificação de processos organizacionais relevantes; ii) o *Cyber*

resilience oversight expections (CROE) for financial market infrastructures (BCE, 2018), como modelo adaptado à cibersegurança e ao setor financeiro; iii) a *framework for improving critical infrastructure cybersecurity* (NIST, 2017), como modelo associado à cibersegurança e iv) as Diretiva 2016/1148 (União Europeia, 2016a), Diretiva 2016/680 (União Europeia, 2016b) e respetivo Regulamento Geral de Proteção de Dados (RGPD) (União Europeia, 2016c), como forma de integrar os aspetos normativos e legais mais relevantes associados aos processos identificados.

Do cruzamento destes vários guias, normas e modelos, resultou um conjunto de critérios de análise e avaliação do estado de maturidade de gestão e governança de cibersegurança em instituições financeiras, os quais são apresentados em detalhe no capítulo 6.

1.3. Conclusão

Deste modo, com a realização deste trabalho, disponibiliza-se a definição de um projeto de implementação, aplicado aos processos de cibersegurança do Banco Central, a qual contempla também uma lista objetiva e exaustiva dos critérios a considerar no âmbito duma avaliação do nível de maturidade de cibersegurança da organização.

Embora todas as etapas de implementação sejam aqui identificadas e apresentadas, a sua implementação prática, nomeadamente a avaliação do grau de sucesso de implementação, são remetidas para um tempo posterior, dado não serem ajustáveis aos condicionalismos temporais de realização deste trabalho.

De qualquer modo, com este trabalho, disponibiliza-se um modelo para a definição e implementação duma estratégia de cibersegurança no Banco Central, o qual, existindo disponibilidade temporal e de recursos humanos e materiais para a sua efetiva implementação, poderá constituir uma mais valia importante para a organização.

2. Definição do contexto

2.1. Problemática

O problema que está na base deste trabalho, e para o qual se pretende ajudar a dar resposta, foi identificado pelo autor com base na sua experiência profissional e formação académica.

As organizações sentem hoje uma necessidade crescente de se munirem de capacidades e competências em matéria de cibersegurança, com vista à proteção contra todas as ameaças que pendem sob a informação e os Sistemas de Informação (SI). Particularmente, no setor financeiro, esta situação tem uma especial importância, pois, como se retira da revisão de literatura, este é o setor mais visado pelos ataques à segurança da informação.

Efetivamente, muitos gestores de TI sentem que nunca como agora foi tão difícil proteger a informação interna das organizações. São muitas e muito relevantes as ameaças que se colocam no contexto em que as organizações desenvolvem a sua atividade, que incluem:

- Com a adoção crescente de ambiente *cloud*, a informação circula e é colocada em repositórios que estão mais fora da esfera de controlo das organizações, os quais, muitas vezes privilegiam a eficiência em detrimento da segurança;
- A utilização massiva de recursos humanos em regime de *outsourcing*, propicia taxas elevadas de rotação e controlo reduzido sobre o perfil de caráter de quem entra na organização e a quem é dado acesso à informação;
- As organizações têm vindo a adotar regimes de teletrabalho aplicados a cada vez mais colaboradores, possibilitando o acesso e tratamento da informação muito para além das fronteiras físicas da organização, onde é mais difícil o controlo da mesma;
- A portabilidade dos dados é uma evidência hoje em dia; qualquer pessoa consegue transportar vários *Gigabytes* de informação num bolso, num pequeno suporte magnético;
- As novas gerações têm enraizada uma cultura de partilha de informação; é algo natural colocar dados nas redes sociais, por exemplo; e o número de ferramentas de colaboração é vasto e é habitual a confusão entre sistemas de uso pessoal e de trabalho;
- Os atacantes estão munidos de ferramentas cada vez mais poderosas e atuam de modo cada vez mais profissional, com o patrocínio de empresas ou até estados.

Neste cenário complexo, os gestores veem-se confrontados com inúmeras questões sobre os melhores caminhos a seguir e decisões a tomar nas vertentes de processos, pessoas e tecnologias internas da organização, tendo em vista a proteção dos seus ativos de informação.

A problemática descrita é transversal a todas as organizações, de todos os setores. De qualquer modo, no âmbito deste trabalho, será focada a situação concreta e particular de um banco central da zona euro, aqui designado por "Banco Central", embora se pretenda desenvolver uma solução que seja mais genérica, válida e aplicável a qualquer organização financeira.

Assim, a questão chave a que este trabalho pretende ajudar a dar resposta é a seguinte: "**Face ao problema das ameaças que pendem sobre os ativos de informação, qual o modelo de gestão de cibersegurança, a aplicar no Banco Central, que melhor responde aos desafios que se colocam no contexto atual?**".

2.2. Motivação do autor

O tema escolhido para a tese de mestrado é, em primeiro lugar, motivado pelo interesse do autor no mesmo. Este enquadra-se na experiência pessoal de vários anos do autor em segurança de redes informáticas e cibersegurança em geral.

Por outro lado, a revisão de literatura mostra que este é um tema extremamente atual, numa sociedade cada vez mais digital, globalizada, e onde as preocupações de segurança e privacidade da informação ganham relevo, decorrente nomeadamente de inúmeras situações de ciberataques que têm ocorrido.

É ainda um tema que permite cruzar questões tecnológicas com conceitos de gestão, que encaixam de forma natural no percurso académico do autor, na sequência da realização do *EMBA* no *INDEG-IUL*.

É também um tema particularmente pertinente e sensível no setor bancário, em que o autor desenvolve a sua atividade profissional há vários anos e para o qual gostaria de dar o seu contributo.

3. Revisão da literatura

A revisão de literatura decorreu em torno do tema da informação e dos modelos e metodologias de segurança associados. Concretamente, desenvolveram-se os seguintes tópicos (apresentados nas secções seguintes):

- A importância da informação para as organizações;
- Definições de segurança de informação e cibersegurança;
- Ameaças à segurança da informação;
- Gestão de segurança;
- Modelos de gestão e governança de segurança.

3.1. Importância da Informação

Vários estudos e investigações mostram que o desempenho e vantagens competitivas das organizações estão cada vez mais ligadas a elementos intangíveis, como a riqueza da informação e o desenvolvimento e partilha de conhecimento (Porter e Millar, 1985; Davis e Botkin, 1994; Davenport e Harris, 2007). Fenz *et al.* (2016) defendem que, atualmente, a informação é um dos bens mais preciosos para as organizações, o que vai ao encontro de um estudo da Symantec (2012), que estima que a informação corresponda em média a 49% do valor duma organização.

Assim, em múltiplos domínios, o funcionamento da sociedade tornou-se crescentemente dependente de tecnologias de informação e comunicação, assim como da gestão de dados massivos, passando por ambientes físicos e virtuais (Adams, 2017). A geração deste conjunto extensivo de dados, estruturados ou não, levou à designação de '*big data*', referindo-se não apenas ao seu enorme tamanho, mas também à velocidade com que o volume de informação é gerado e a complexidade de o organizar e analisar (Berman, 2013; Chen *et al*., 2014).

Woolf (2010) reforçou que a informação é um ativo de negócio crucial e, como qualquer ativo de negócio, tem que ser gerido. Quando é mal gerido, pode custar caro e potencialmente danificar a reputação da organização. Assim, como referido por Karlsson *et al*. (2015), com as organizações a depender cada vez mais da informação e dos sistemas de informação, não é de estranhar que a segurança da informação esteja no topo da agenda dos gestores.

3.2. Segurança de Informação e Cibersegurança

Com o foco crescente sobre a importância da informação para as organizações, termos como "segurança de informação" e "cibersegurança" surgem cada vez mais no discurso dos gestores, sendo algumas vezes utilizados de forma indistinta. Importa aqui também analisar o que a literatura especializada entende por cada um.

Relativamente a "segurança de informação", a *European Union Agency for Network and Information Security* (ENISA) (2017) refere que o modelo clássico de segurança de informação define três objetivos: confidencialidade, integridade e disponibilidade. A segurança de informação e de redes, como definido pelo regulamento 526/2013 da ENISA, significa a capacidade de uma rede ou sistema de informação resistir, com um determinado nível de confiança, a eventos acidentais ou ações ilícitas ou maliciosas, que comprometam a disponibilidade, autenticidade, integridade ou confidencialidade de dados em repouso ou em trânsito e dos serviços associados disponibilizados por ou através dessas redes ou sistemas. Para o *Committee on National Security Systems* (CNSS) (2015), "segurança de informação" significa a proteção da informação ou sistemas de informação de acessos não autorizados, utilização, divulgação, disrupção, modificação ou destruição, por forma a garantir confidencialidade, integridade e disponibilidade. Por seu lado, o *Information Systems Audit and Control Association* (ISACA) (2016) refere que a "segurança de informação" garante que, dentro da organização, a informação é protegida contra a divulgação a utilizadores não autorizados (confidencialidade), modificações indevidas (integridade) e inacesso quando requerido (indisponibilidade).

Relativamente ao termo "cibersegurança", a ENISA (2017) refere que tal cobre todos os aspetos de prevenção, previsão, tolerância, deteção, mitigação, remoção, análise e investigação de ciberincidentes. Acrescenta ainda que, considerando os diferentes tipos de componentes do ciberespaço, a cibersegurança deveria cobrir os seguintes atributos: disponibilidade, fiabilidade, proteção, confidencialidade, integridade, manutenção (para sistemas tangíveis, informação e redes), robustez, sobrevivência, resiliência (para suportar a dinâmica do ciberespaço), responsabilização, autenticidade e não-repúdio (para suportar a segurança de informação). Quanto ao CNSS (2015), define "cibersegurança" como a prevenção, proteção e recuperação de computadores, sistemas de comunicações eletrónicos, serviços de comunicação eletrónicos, comunicações por fio e comunicações eletrónicas, incluindo a informação aí contida, por forma a garantir a sua disponibilidade, integridade, autenticidade,

confidencialidade e não repúdio. O ISACA (2016) define ”cibersegurança” simplesmente como a proteção dos ativos de informação através da identificação de ameaças à informação processada, armazenada e transportada por sistemas de informação interconectados.

3.3. Ameaças e mitigação de riscos

Fenz *et al*. (2016) referem que se assiste a um crescimento de ameaças e vulnerabilidades de segurança, como resultado de mais interligações e processamentos eletrónicos e que a melhoria nos processos de segurança também requer conhecimentos ao nível das estratégias e tecnologias utilizadas pelos atacantes, as quais estão em permanente evolução. Assim, considerando os múltiplos cenários de ataque, é necessário um esforço significativo para definir e implementar controlos de segurança e estratégias de mitigação para proteger os ativos mais valiosos da organização.

No contexto das ameaças à segurança de informação, é incontornável a crescente ameaça que o cibercrime representa para a segurança de informação. Como referido por Sabillon *et al*. (2017), atualmente, o cibercrime continua a crescer a ritmos acelerados devido à conetividade global e aos avanços nas redes de comunicação, troca de informações e tecnologias móveis. Acresce que os cibercrimes também aumentam ao nível da sofisticação. A McAffee (2014) estima que, em 2014, o cibercrime tenha tido um impacto global anual na economia de cerca de 400 biliões de dólares, e com tendência claramente crescente. Destes, cerca de 160 biliões referem-se ao roubo de informações pessoais. Acrescente-se ainda que os estudos indicam que o setor financeiro é o mais visado pelas ameaças à segurança (Accenture, 2017). Têm, aliás, sido lançados vários alertas, por parte de responsáveis de algumas das principais organizações mundiais, em que se inclui a Comissão Europeia (CE) (2017) ou o Banco Central Europeu (BCE) (2016), sobre a necessidade de as empresas se adaptarem ao presente cenário de ameaças.

Segundo Mugavero e Sabato (2014), o ciberespaço, um ponto de vulnerabilidade potencial das sociedades modernas, não é ainda percecionado por todos com o mesmo nível de seriedade.

Por outro lado, como referido por Wang *et al*. (2015), as ameaças internas à segurança da informação são um problema crítico das organizações. Essas ameaças podem vir de colaboradores atuais, antigos empregados, contratados e outras pessoas a quem sejam dadas credenciais de acesso a ativos de informação da organização (Warkentin e Willison, 2009). Uma vez que, habitualmente, estes possuem privilégios elevados e têm capacidades,

conhecimentos, recursos, acessos e motivações (Siponen e Willison, 2009), relativamente a sistemas e dados internos da organização, os colaboradores podem facilmente contornar os controlos de segurança da organização, roubar dados importantes e causar prejuízo. Os controlos de perímetro e de proteção de terminais, como *firewalls*, sistemas de deteção de intrusão e *software* tipo antivírus são ineficazes para proteger destas ameaças. Efetivamente, as violações às políticas de segurança organizacionais por parte de empregados, são frequentemente identificadas como a maior ameaça à segurança da informação (Boss *et al*., 2009; Warkentin e Willison, 2009), com os colaboradores a serem tipicamente identificados como o elo mais fraco da cadeia de segurança, na medida em que incorrerão frequentemente em comportamentos de segurança incorretos seja devido a uma insuficiente sensibilização para a necessidade de cumprimento de políticas, seja devido a incompetência ou descuido (Culnan e Williams, 2009; Hsu *et al.*, 2015). Estima-se que pelo menos metade das falhas de segurança dos sistemas de informação sejam devidas a pessoas internas à organização, sobretudo devido à atribuição de acessos não autorizados aos sistemas (Gordon *et al*., 2005).

As causas que originam comportamentos de segurança incorretos por parte de colaboradores de determinada organização, têm sido objeto de vários estudos, que analisam fatores culturais e geracionais (Miltgen e Guillard, 2014), questões de formação desadequada ou inexistente (Tsohou *et al*., 2015) e até relações de género (Foth, 2016).

Quando se aborda a questão das ameaças internas para a segurança de informação, tem que se ter em conta também aspetos ligados à crescente adoção de contratos em regime de *outsourcing* por parte das organizações, dado que o controlo e o conhecimento que as mesmas têm sobre os indivíduos com acesso à informação é menor. Como referido por Gupta e Zhdanov (2012), com o advento de novas tecnologias, como a computação em nuvem, muitas organizações entendem não poderem gerir a segurança dos seus ativos, optando pelo *outsourcing* de serviços de segurança. Tal, pode-se traduzir em ganhos financeiros, maior especialização, disponibilidade e instalações dedicadas (Allen *et al*., 2003), mas traduz-se por outro lado em maiores preocupações de segurança, pela dependência de uma entidade externa para o suporte de funções críticas.

Uma outra vertente de ameaça à segurança de informação das organizações, relaciona-se com o crescente alargamento e até, em muitos casos, rutura do denominado perímetro de segurança. Ou seja, até há alguns anos atrás, era comum o estabelecimento de um perímetro de segurança rígido para a infraestrutura de comunicação e guarda das informações nas organizações. Este perímetro era delimitado por equipamentos de segurança que implementavam regras de

controlo de entrada e saída da informação. Atualmente, com a crescente adoção de ambientes *cloud*, este perímetro deixa de fazer sentido, pois as informações circulam e residem naturalmente fora do limite geográfico da organização. Como referem Aleem e Antwi-Boasiako (2011), o advento de *cloud computing* é um resultado direto de avanços tecnológicos que permitiram novas oportunidades para diferentes negócios. Aleem e Sprott (2013) referem que, em especial no setor corporativo financeiro, são inegáveis os benefícios que a adoção do modelo *cloud* veio trazer, ao nível da flexibilidade e elasticidade que permite. Contudo, como referem os mesmos autores, existem repercussões ao nível da segurança, que importa ter em devida conta.

Existem ainda ameaças que decorrem do maior inter-relacionamento organizacional. O atual ambiente de negócio está a tornar-se cada vez mais competitivo. Tanto organizações nacionais como internacionais estão a afastar-se da operação como negócios individuais para se tornarem alianças estratégicas (Tomkins, 2001; Gomes *et al.*, 2016). A colaboração através de processos de negócio mais integrados é muitas vezes potenciada através do uso de TI. A Price Waterhouse Coopers (PWC) (2010) mostrou que a troca de informações entre organizações cresceu nos anos mais recentes. Kunz *et al*. (2011) também concluíram que com este intensificar das trocas de informação, a segurança de informação torna-se uma questão chave. A colaboração inter-organizacional introduz novas formas de risco, abrindo oportunidades para intrusão, não conformidades e exposição indesejada (Goodman e Ramer, 2007; Karlsson *et al*., 2016).

Um outro cenário a considerar, como salientado por Aleem *et al*. (2013) é o de ameaças combinadas. Ou seja, por exemplo, um ataque baseado em TI que provoca a paragem de infraestruturas críticas ou um ataque físico a um sistema que permite instalar dispositivos de espionagem em computadores. A defesa contra estas ameaças requer uma abordagem de convergência na gestão da segurança da organização, com o reconhecimento de que certos riscos vão para lá do âmbito de uma única direção e requerem uma abordagem colaborativa. A cibersegurança, com o seu caráter abrangente, terá aqui um papel chave a desempenhar.

Neste cenário global de ameaças, Randazzo *et al*. (2005) referem que as instituições financeiras são especialmente suscetíveis, dada a sua dependência de TI e a natureza altamente sensível dos dados armazenados. Esta ideia é reforçada por Ifinedo (2014), que aponta como razões para as entidades do setor financeiro sofrerem com mais ameaças:

- Maior dependência dos sistemas de informação nas suas operações;
- Maior potencial de perdas devido a falhas nas suas operações;
- A necessidade de manter uma boa imagem pública.

3.4. Gestão de segurança

Dzazali e Zolait (2012) referem que, dado que a segurança da informação é uma disciplina complexa, dinâmica e multifacetada, em que nenhum componente pode ser ignorado, é fundamental uma gestão efetiva para qualquer organização que pretenda sobreviver na era da informação. Também Haufe *et al*. (2016), reforçam que a segurança da informação sensível é atualmente uma tarefa vital para qualquer organização.

Rubino e Vitolla (2014) indicam que a utilização abrangente das TI como um meio de desenvolvimento dos processos de negócio tornou críticos os processos de gestão dos sistemas de informação e de medição de desempenho das organizações. Os sistemas de informação das organizações devem garantir um fluxo adequado de informação para suportar as atividades relacionadas com a gestão e controlo da organização, assim como suportar os processos de governança corporativa. Neste contexto, existem múltiplas motivações para a aplicação de metodologias de gestão às TI. Por um lado, em face dos custos crescentes que se anteveem, a organização sente a necessidade de avaliar com cuidado os investimentos em TI. Por outro lado, há a necessidade também crescente de medir a contribuição que os sistemas de TI dão para o alcançar das estratégias e metas da organização.

Segundo Kwon e Johnson (2014), alguns investigadores defendem que os investimentos em segurança, ao contrário de outros investimentos em TI, dependem de decisões políticas e regulatórias, para além de decisões económicas (Ryan e Ryan, 2005; Bodin *et al*., 2005; Rowe e Gallaher, 2006). Também nesse sentido, Anderson (2001) defende que os problemas de segurança têm que ser resolvidos com uma abordagem holística que combine fatores tecnológicos e económicos com fatores legais e políticos. Vários outros autores referem que a informação de segurança inclui aspetos organizacionais, aspetos legais, definição e aplicação das melhores práticas, como adição às tecnologias de segurança (Von Solms, 2000, 2006; Siponen e Oinas-Kukkonen, 2007).

Um fator a ter em conta é que é difícil dispor de indicadores precisos para uma análise económica, dado que o sucesso em segurança é não acontecer nada e os benefícios são a maior parte das vezes intangíveis. Consequentemente, muitas organizações apenas reagem a falhas e gastam o que for necessário para resolver um problema existente ou ir ao encontro de determinado regulamento, ao invés de atuarem antes de acontecer a falha (Liberti, 2008).

Como referido por Stewart (2012), as decisões sobre gastos em segurança de informação são de grande importância para a organização. As mesmas ou criam ou destroem valor. Como tal

devem ser devidamente analisadas e avaliadas. Há questões a colocar permanentemente, como se se deve comprar, quanto se deve gastar e o que comprar.

Também deve ser tido em atenção que várias pressões para melhorar a segurança de informação, sem permitir uma devida análise, podem empurrar a organização para ineficiências nos gastos que realiza. Hasan (2010) refere que apesar da importância fundamental da segurança de informação, as organizações nem sempre fazem os melhores investimentos. Uma vez que não são desejáveis nem sub-investimentos, nem sobre-investimentos, as organizações devem entender os fatores que, de forma adversa, afetam os seus processos de decisão (Angst *et al*., 2017).

Os resultados indicam que, para que as medidas de segurança de informação sejam eficazes, a segurança deve ser construída como uma escada de medidas combinadas. Para produzirem efeito, as medidas de segurança são mutuamente dependentes umas das outras (Berghel, 2005; Sundt, 2006). Os fundamentos de segurança tecnológica têm que estar implementados. Sem as soluções tecnológicas de segurança, não haveria necessidade de medidas administrativas, dado que são as soluções tecnológicas que previnem, detetam e reagem a incidentes de segurança. E os mesmos argumentos podem ser utilizados em sentido contrário: são os colaboradores que implementam diariamente as rotinas de segurança.

Karlsson *et al*. (2015) referem que, atualmente, as organizações têm um desafio enorme de tentar encontrar procedimentos para identificar e mitigar qualquer situação possível de risco. Nesse sentido, é necessário considerar a atitude dos colaboradores para com a segurança de informação. A cultura das organizações relativamente à segurança de informação tem estado na agenda de investigação desde o início do século (Von Solms, 2000; Schlienger e Teufel, 2002; Vroom e Von Solms, 2004; Furnell, 2007; Da Veiga e Eloff, 2010; Kolkowska, 2011). Ainda que existam diferentes definições de "cultura de segurança de informação" (Schlienger e Teufel, 2002; Da Veiga e Eloff, 2010; Ilvonen, 2011), existe uma base comum de entendimento de que tal consiste numa plataforma partilhada de valores, modelos mentais e atividades que são trocadas entre os colaboradores da organização ao longo do tempo, afetando a segurança de informação.

Um outro aspeto a ter em atenção é o de que, dadas as exigências da função, os gestores de topo da organização têm um tempo limitado disponível para qualquer área de responsabilidade, razão pela qual podem ser tentados a delegar as responsabilidades de gestão de TI (Davenport e Beck 2001). Tal é ainda mais potenciado pela natureza tecnologicamente sofisticada da gestão de TI (Bensaou e Earl 1998; Feld e Stoddard 2004). Esta delegação, contudo, não libera

a gestão de topo das responsabilidades pela gestão de TI. A investigação demonstra, aliás, que os *Chief Executive Officers* (CEO) e os *Chief Financial Officers* (CFO) são normalmente responsabilizados por deficiências sérias no TI, como apontado por Masli *et al*. (2016).

3.5. Modelos de Gestão e Governança de Segurança

A Governança de TI (GTI) é entendida como um conjunto de processos de gestão, planeamento, acompanhamento e revisão, com a definição de responsabilidades associadas, que estabelecem o controlo e métricas de desempenho sobre investimentos chave em TI, serviços entregues e conformidade com regulamentos, leis e políticas organizacionais. Desse modo, a GTI formaliza e clarifica a supervisão, responsabilização e tomada de decisão (Weill, 2004; Bainbridge, 2008). A GTI é a componente do processo de governança corporativa que diz respeito aos ativos de TI e consiste em estruturas organizacionais, processos, políticas, normativos e princípios de TI destinados ao alinhamento com a estratégia de TI. A relação bidirecional entre GTI e governança corporativa torna-se clara quando se atenta que a governança corporativa guia e define a GTI, mas, ao mesmo tempo, as TI disponibilizam indicadores que são críticos para os planos estratégicos, constituindo assim uma componente importante dos mesmos (Dittmeier, 2011). Como referido por Selig (2016), a GTI deve ser uma parte integral da governança da organização. Marrone *et al*. (2010) referiram que organizações que implementaram GTI alcançaram lucros 20% superiores às que não o fizeram.

Assim, os requisitos, oportunidades e desafios de governança e gestão das necessidades, investimentos e recursos associados às TI tornaram-se uma preocupação chave das administrações e gestão executiva das organizações, à escala global.

Mishra (2015) refere que o desenvolvimento organizacional de governança de segurança coloca desafios significativos às organizações, dadas as vulnerabilidades sempre crescentes, pela falta ou desadequação dos controlos de segurança apropriados. Este autor acrescenta que ocorreram em anos recentes vários casos de falhas colossais em empresas devido a medidas inadequadas de governança de segurança. Em muitos casos, as organizações inclusive ignoram quais sejam os seus objetivos de governança de segurança de informação.

Os modelos de GTI são entendidos como modelos de alto nível que têm o objetivo de desenvolver as funções de TI de forma profissional (Haes e Van Grembergen, 2008). Há vários modelos alternativos e guias para ajudar as organizações a planear, desenvolver e gerir as iniciativas de GTI, as quais se focam no alcançar de níveis mais elevados de maturidade e

eficiência de TI. Por forma a garantir que as funções de TI estão alinhadas com e suportam as estratégias e metas da organização pode ser necessária a utilização integrada de vários modelos de GTI (Wessels e Loggerenberg, 2006). Efetivamente, muitas organizações implementam múltiplos modelos de processos e conformidade (Cater-Steel, Tan, e Toleman, 2006).

Dentro dos modelos de GTI, o *COBIT* (ISACA, 2012a) é o mais utilizado. O *COBIT* é considerado como bastante abrangente (Hardy, 2006; Ahmed, 2011) e é muitas vezes referido como um integrador, na medida em que permite conjugar vários modelos de GTI. É ainda referido que o *COBIT* não pode funcionar de forma isolada, dado que não é muito detalhado, e que apresenta o que fazer, mas não como o fazer (Mataracioglu e Ozkan, 2011). Foi ainda referido (Pereira e Mira da Silva, 2012) que a sua implementação é complexa, por ser demasiado genérico e, como tal, requerer conhecimentos especializados. Desse modo, necessita de modelos complementares para facilitar a sua implementação.

Segundo Bernard (2012), o *COBIT* é um conjunto de guias e ferramentas de apoio às TI, usado como suporte de governança corporativa, aceite à escala mundial. Este autor acrescenta que auditores e gestores utilizam-no como um mecanismo para integrar tecnologia na implementação de controlos e ir ao encontro de objetivos específicos de negócio. É assim um modelo bem adequado para empresas focadas na gestão e mitigação de risco.

O *COBIT* (ISACA, 2012a) baseia-se em 5 princípios chave:

- Ir ao encontro das necessidades de todas as partes interessadas;
- Cobrir toda a organização, de forma transversal;
- Aplicação de um modelo único, integrado;
- Possibilitar uma abordagem holística;
- Separação entre Governança e Gestão.

De forma complementar, o ISACA desenvolveu também o *COBIT 5 for Information Security* (ISACA, 2012b) o qual se foca em disponibilizar guias mais práticos e detalhados de segurança de informação, assim como o *COBIT 5 implementation* (ISACA, 2012c), que constitui um modelo de implementação de projetos, para além de outros desenvolvimentos específicos.

Um outro modelo globalmente reconhecido e utilizado no âmbito da segurança de informação, focando particularmente na cibersegurança é a *framework for improving critical infrastructure cybersecurity* (NIST, 2017), geralmente designada simplesmente por "*framework NIST*". Segundo Shen (2014), esta, embora desenvolvida com o intuito de melhorar a gestão do ciber-risco em infraestruturas críticas, é flexível e pode ser utilizada por organizações de qualquer setor, possibilitando a aplicação de princípios de boas práticas de gestão de risco e melhoria da

segurança e resiliência. Alguns autores baseiam-se na *framework NIST* para o desenvolvimento de modelos de maturidade de cibersegurança, que auxiliem a governança organizacional (Teodoro, Gonçalves e Serrão, 2015). Refira-se ainda que a *framework NIST* se baseia em parte no *COBIT*.

No setor bancário e financeiro, o Conselho de Governadores do Banco Central Europeu adotou o *CROE* (BCE, 2018) como um modelo de cibersegurança, a ser aplicado em entidades do setor financeiro. O *CROE* contempla 5 categorias de gestão de risco (governança, identificação, proteção, deteção e resposta e recuperação) e 3 categorias adicionais (testes, análise situacional e aprendizagem e evolução). Refira-se que o *CROE* tem por base um outro documento, o *Guidance on Cyber resilience for financial market infrastructures* (BIS, 2016), o qual se baseia parcialmente na *framework NIST* (NIST, 2017).

A nível da União Europeia, as preocupações com a segurança de informação e a cibersegurança, traduziram-se, nomeadamente, na diretiva (UE) 2016/1148 do parlamento europeu e do conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva *NIS*) (União Europeia, 2016a), e na diretiva (UE) 2016/680, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados (União Europeia, 2016b), com o associado Regulamento (EU) 2016/679 do parlamento europeu e do conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD) (União Europeia, 2016c).

4. Quadro conceptual

4.1. Contexto da Informação

Resulta, como ponto central da revisão de literatura, o enorme valor que a informação constitui atualmente para as organizações e a tendência crescente dessa importância. Paradoxalmente, a informação é também um dos ativos mais difíceis de proteger e controlar. Daí, decorrem preocupações também cada vez maiores com a segurança dessa informação, com os gestores a serem chamados para a linha da frente dessa batalha pela proteção dum ativo tão valioso.

É também patente que a informação é hoje em dia um conceito omnipresente. Qualquer indivíduo ativo da sociedade atual produz, consome, utiliza, tem, vê, ouve e é informação.

Também é apontado que, se no século passado a informação existia nas organizações sobretudo em suporte físico de papel, hoje em dia o papel é utilizado de forma acessória, tendo dado lugar a suportes digitais. Está-se, portanto, na era da informação digital. E é naturalmente também a era da internet. A informação existe nas organizações em suportes digitais, mas é transmitida e partilhada através da internet, onde se tem acesso a toda essa informação, de forma mais ou menos controlada.

Com tudo isto, ao longo da última década, o mundo tornou-se global. Com a massificação do uso da internet, não há fronteiras ou barreiras físicas que garantam a segurança da informação. Esta, circula à velocidade da luz e é acessível ou enviada de e para qualquer lugar com um simples clique de rato. E o volume de dados continua a subir de forma exponencial.

No campo da segurança, o tradicional conceito de segurança de informação, dá cada vez mais o espaço ao conceito de cibersegurança. Como resulta da revisão de literatura, pode-se dizer que a segurança de informação se preocupa com a proteção de toda a informação da organização, nos três vetores: confidencialidade, integridade e disponibilidade, assim como com os sistemas que suportam e onde a informação reside. Atendendo à revisão de literatura efetuada, o conceito de cibersegurança é mais abrangente. A cibersegurança preocupa-se com a informação[1], com todos os sistemas que permitem guardar e transmitir informação e mesmo com outros sistemas de suporte, como os sistemas eletrónicos de segurança física ou de controlo e manutenção de instalações. A ENISA (2017) afirma de forma clara que a segurança

[1] Pode-se excluir a informação em suporte não digital, como a informação em papel, do conceito de cibersegurança, mas é vastamente referido na literatura que tal representa um sub-universo da informação cada vez mais residual

de informação é um subconjunto da cibersegurança e atribui a esta última um papel de visão holística da organização, posicionando-a desde os processos de antecipação de ameaças, até à proteção, deteção e reação aos incidentes que ameacem a informação.

Assim, no âmbito deste trabalho, será privilegiada a utilização do termo e conceito de cibersegurança, entendendo-se que, desse modo, se está a incluir também os determinantes da segurança de informação. De qualquer forma, serão utilizadas, no desenvolvimento do trabalho, ferramentas associadas a segurança de informação, entendendo-se que a sua utilização será integralmente válida também num âmbito de cibersegurança, podendo, quando muito, pecar por alguma falta de abrangência, mas o que não vicia o resultado final.

4.2. O problema da segurança

Como fica patente pela revisão de literatura, são cada vez mais e mais complexas as ameaças que pendem sobre a proteção da informação, a que a cibersegurança pretende dar resposta. E existem cada vez mais vozes a alertar para o problema.

O presidente da Comissão Europeia, Jean-Claude Juncker, no *Discurso do Estado da União* (Comissão Europeia, 2017), referiu que os ciberataques podem ser mais perigosos para a estabilidade das democracias e economias, do que armas ou tanques e que no ano transato ocorreram mais de 4000 ataques de *ransomware* por dia e 80% das companhias europeias experienciaram pelo menos um incidente de ciberataque.

Na 13ª edição do *The Global Risks Report* (WEF, 2018) são identificados os ciberataques como o 4º maior risco à economia global, apenas atrás dos eventos climáticos extremos, desastres naturais e falhas na mitigação e adaptação às alterações climáticas. Ainda no mesmo relatório, é identificada uma tendência forte no sentido do aumento da dependência de cibersegurança para o negócio, relacionando-se esse aspeto com o incremento dos riscos de ciberataques e de quebras nas infraestruturas críticas de informação.

Pode-se igualmente citar um estudo da Accenture (2017) que alerta que os ataques estão a crescer, quer em número, quer em potencial disruptivo. Ainda um outro aspeto importante e relevante no contexto do trabalho, e que é focado num estudo da IBM (2017), é que o setor financeiro foi o mais visado pelos ataques em 2016. Isto é algo a ter em conta também.

Neste contexto, são colocados grandes desafios à cibersegurança. A gestão da cibersegurança nas organizações é um tema complexo e muitas vezes incompreendido. É uma disciplina muito

específica que tem que cruzar conceitos transversais de gestão com conhecimentos de tecnologia e não descurando os aspetos legais e regulamentares.

As empresas deparam-se com múltiplas dificuldades no momento de definir quais as medidas de proteção mais eficazes e mais prementes e em que faz mais sentido investir. Acontece com frequência tomarem-se medidas avulso, desagregadas duma estratégia global, e sem compreensão efetiva do nível de segurança que estas consubstanciam.

A literatura focada no tema é consensual no sentido de afirmar que, para ser eficaz, a cibersegurança tem inequivocamente que ser implementada de forma transversal e tem que ser assumida e patrocinada pela gestão de topo. E cada indivíduo que tenha acesso a informação sensível tem que ser um agente informado e ciente do papel que lhe cabe nessa missão.

4.3. Gestão de cibersegurança

Coloca-se, portanto, a questão de o que deve constituir uma boa gestão de cibersegurança? Não será fácil responder e nem haverá uma única resposta. Por um lado, não é uma matéria ainda suficientemente estudada e não é um campo de conhecimento sedimentado. Por outro lado, não existirá uma resposta única, também por força das variadas envolventes organizativas, porque aquilo que faz sentido para uma empresa que vende calçado *on-line*, não é o mesmo que faz sentido para uma empresa que presta serviços de manutenção automóvel, por exemplo. E não existem soluções perfeitas. Trata-se, em primeiro lugar, de gerir o risco, ou seja, encontrar um ponto de equilíbrio entre a necessidade de investir em segurança e o imponderável de nunca existir uma segurança total. Trata-se, ainda, de apostar numa lógica de resiliência, tanto quanto de prevenção. Como apontado pelo BCE (2016), é consensual que os ciberataques vão acontecer e que, em determinada altura, os mesmos vão ter sucesso, i.e., vão conseguir penetrar os controlos de segurança da organização. Nessa altura, será o nível de resiliência existente que fará a diferença. Essa terá que ser também uma aposta da gestão de segurança atual.

Há, portanto, várias vertentes a considerar quando se pensa na gestão da cibersegurança. Na metodologia identificada para este trabalho, a abordagem é efetuada a partir dos processos da organização, interligando a partir daí com os outros componentes (Figura 1). É também complementada e cruzada a informação com os guias focados no ecossistema financeiro.

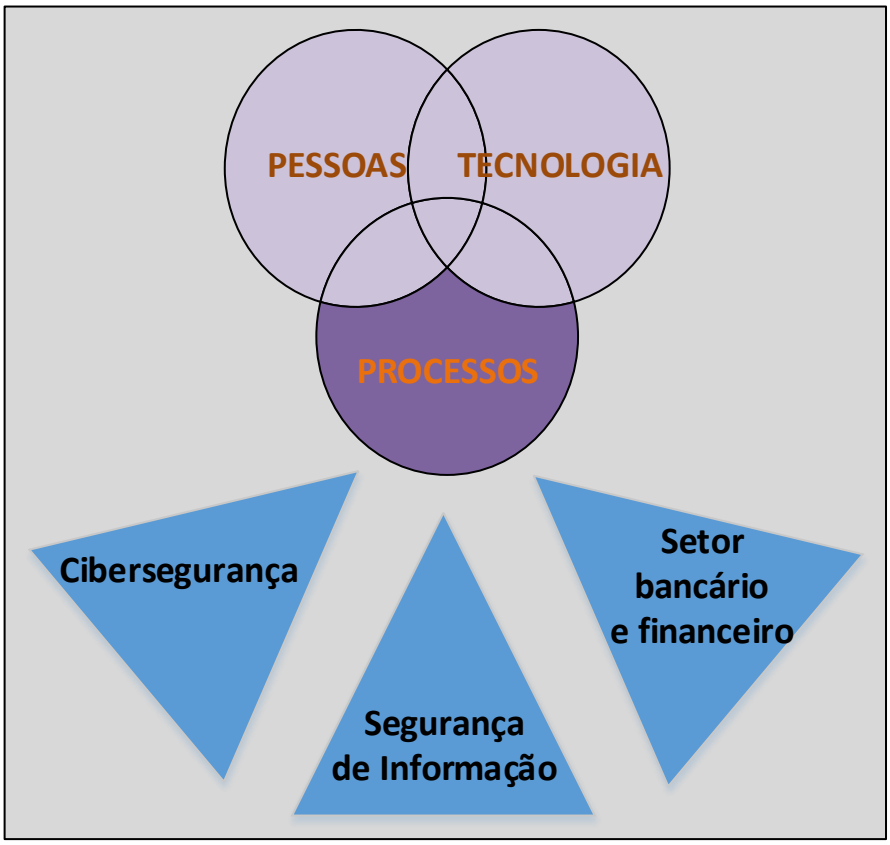

Figura 1 – Abordagem centrada em Processos

5. Metodologia

A metodologia a seguir é a de um Projeto-Empresa, com aplicação no Banco Central.

Este projeto incide sobre a reformulação e adaptação dos processos internos da organização, associados à gestão e governança da cibersegurança, tendo em conta aquilo que foi identificado na revisão de literatura e que é entendido pelos principais atores internacionais como os melhores modelos a seguir neste domínio. Prevê-se, de qualquer modo, que o plano tenha um caráter suficientemente abrangente, que permita a sua fácil adaptação e implementação noutras entidades, sobretudo do setor financeiro, uma vez que existe a intenção de foco nas particularidades desse setor.

Como base de organização de todo o projeto, vai-se recorrer ao modelo e fundamentos do *COBIT 5* (ISACA, 2012a), enquanto modelo de gestão e governança, pelo reconhecimento apontado pela revisão de literatura relativamente à qualidade, relevância e caráter abrangente que o mesmo possui. Ao contrário de outros modelos, com o *COBIT* consegue-se ter uma visão holística da organização e este permite cobrir todos os aspetos relevantes para este projeto.

O modelo do *COBIT 5* é utilizado em duas vertentes:

i) Como modelo de implementação

   Por um lado, o *COBIT 5* é usado como modelo de implementação, numa lógica de projeto de ciclo de vida de melhoria contínua, o qual tem por base o *COBIT 5 implementation* (ISACA, 2012c).

   Nesta medida, é efetuada a definição e explicitação da metodologia de implementação prática do projeto de reestruturação dos processos internos da organização. Tal, é especificado e explicado em detalhe no capítulo 7.

   Refira-se de qualquer modo que, embora todas as etapas de implementação sejam aqui identificadas e apresentadas no âmbito deste trabalho, a sua implementação prática e as fases posteriores, nomeadamente a avaliação do grau de sucesso de implementação, são remetidas para um tempo posterior, dado não serem ajustáveis aos condicionalismos temporais de realização deste trabalho.

ii) Como modelo base de processos, para identificação de critérios de avaliação associados

   Por outro lado, a implementação do processo de melhoria contínua pressupõe, como uma das etapas principais, a avaliação do estado de maturidade da organização, atual e pretendido. Para isso, é fundamental definir os parâmetros sobre os quais será focada essa

análise, ou seja, quais os critérios de avaliação, da forma mais objetiva possível. Essa identificação e definição, implica um trabalho de integração de diferentes modelos e guias de boas práticas, focados em diferentes aspetos que se pretende avaliar.

Nessa medida, o COBIT 5 também será utilizado, partindo da sua componente de processos, os quais serão cruzados com requisitos provenientes de outros modelos, mais focados em cibersegurança e no setor financeiro, assim como com requisitos normativos e legais. Concretamente, identificam-se aqui os seguintes modelos e regulamentos a cruzar com o *COBIT 5* ao nível dos processos:

- *CROE* (BCE, 2018);
- *Framework NIST* (NIST, 2017);
- Diretiva *NIS* (União Europeia, 2016a);
- Diretiva RGPD (União Europeia, 2016b).

Esse cruzamento foi realizado e é explicitado em maior detalhe no capítulo 6.

A figura 2 representa o resumo da abordagem descrita para o desenvolvimento do trabalho.

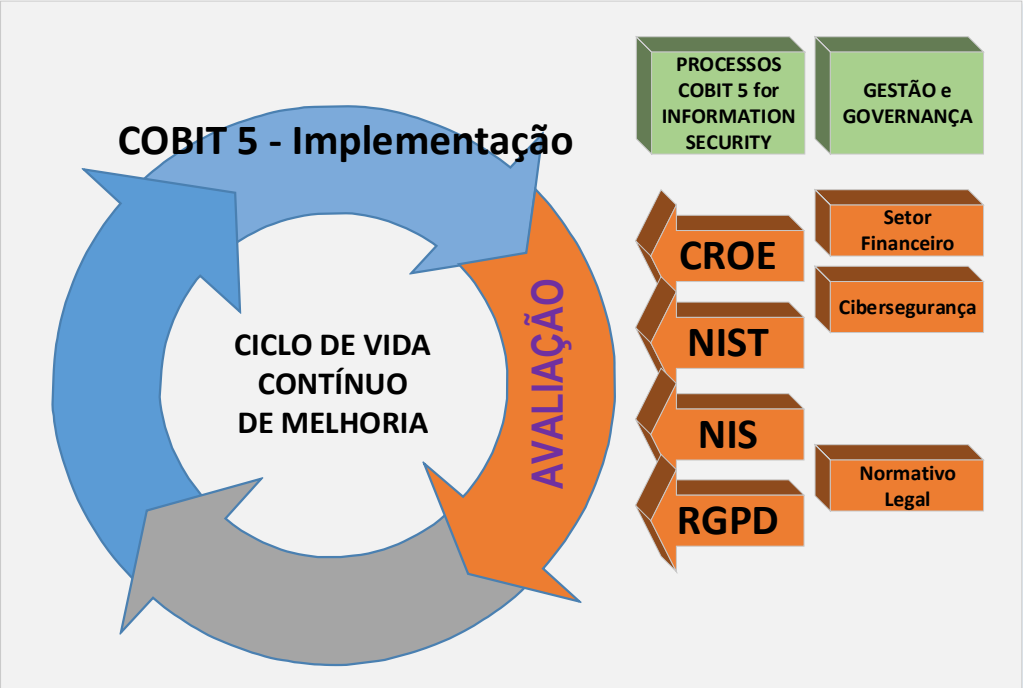

Figura 2 – Integração de modelos, usando o COBIT 5

6. Análise de informação e conclusões

6.1. Modelos a considerar

O tema da gestão de cibersegurança é de difícil tratamento, na medida em que é um tema recente, em permanente evolução e sobre o qual não existe ainda um conhecimento muito consolidado na maior parte das organizações.

Quando se abordam as questões relativas à segurança da informação e cibersegurança, a liderança do conhecimento encontra-se em organizações internacionais de referência, onde os principais especialistas confluem e se organizam no sentido de encontrarem as melhores práticas a seguir. Importa, assim, em primeiro lugar identificar essas organizações, definir quais os principais atores, quais os modelos que devem ser tidos em conta e porque é que os mesmos são relevantes para este trabalho.

Nos parágrafos seguintes são identificados e sumariamente descritos os principais modelos que, no contexto em causa e com base na revisão de literatura, se identificou melhor poderem contribuir para a definição dos processos de organização a considerar e como os avaliar. Os mesmos são apresentados pela ordem com que foram considerados, em termos de importância, no âmbito do presente trabalho. Assim, com base na revisão de literatura, foram identificados:

- *COBIT 5 for Information Security* (ISACA, 2012b);
- *CROE* (BCE, 2018);
- *Framework NIST* (NIST, 2017);
- Diretiva *NIS* (União Europeia, 2016a);
- RGPD (União Europeia, 2016b e União Europeia, 2016c).

Deste modo, a recolha de informação que se pretende efetuar, como forma de identificar quais as melhores práticas de cibersegurança a aplicar nas instituições financeiras, irá percorrer estas várias organizações, de várias naturezas, as quais, a nível mundial, mais se destacam e preocupam com o tema, desenvolvendo e sistematizando modelos adequados.

6.2. ISACA – *COBIT 5 for Information Security*

O ISACA é uma associação global, independente e não-lucrativa, que promove o desenvolvimento, adoção e utilização dos melhores conhecimentos e práticas na área dos

sistemas de informação. Tem-se destacado, no campo das organizações não governamentais, pela qualidade e especialidade dos documentos produzidos.

O ISACA foi criado em 1967. Atualmente, é constituído por mais de 140.000 membros a nível mundial, de mais de 180 países, que refletem a sua diversidade e que permitem que haja uma aprendizagem mútua e a troca frequente de pontos de vista divergentes numa variedade de tópicos profissionais. Tal, é considerado um dos seus principais pontos fortes.

No âmbito da sua ação, o ISACA disponibiliza guias práticos e ferramentas de análise para todas as empresas que utilizam sistemas de informação. Desse modo, visa auxiliar os líderes no sentido duma governança efetiva dos atuais sistemas digitais e das futuras tecnologias emergentes. Relativamente às publicações produzidas, destaca-se o desenvolvimento do *COBIT*, considerado como o principal modelo de referência para a governança e gestão das TI nas organizações, há mais de 20 anos.

O *COBIT 5* tem um desenvolvimento específico dentro da segurança de informação, designado como "*COBIT 5 for Information Security*" e que é a principal base em que assenta este trabalho.

O Modelo "*COBIT 5 for Information Security*" assenta em 5 princípios base (os mesmos que o modelo *COBIT 5*), representados na Figura 3. São eles:

1. Ir ao encontro das necessidades de todas as partes interessadas;
2. Cobrir toda a organização, *end-to-end*;
3. Aplicação de um único modelo, integrado;
4. Permitir uma abordagem holística;
5. Separação entre Governança e Gestão.

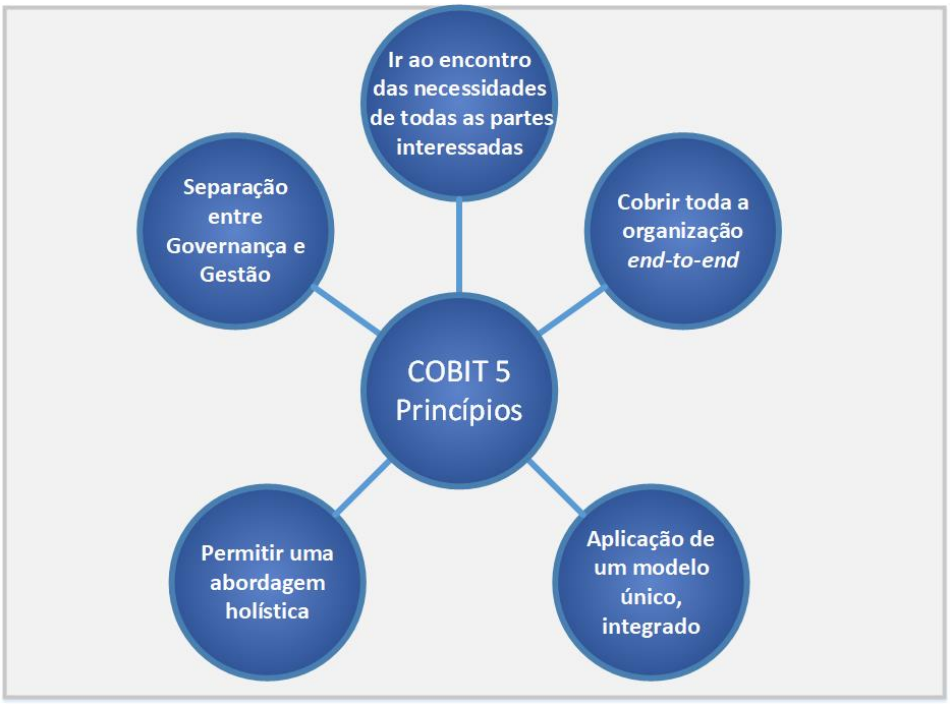

Figura 3 - Princípios do *COBIT 5* (adaptado de ISACA, 2012a)

Para alcançar os objetivos, o "*COBIT 5 for Information Security*" define o conceito de "*enabler*", que é aqui traduzido por "facilitador". Os facilitadores são as peças chave da organização que, no seu conjunto, contribuem para o alcançar dos objetivos de segurança da informação. Estes facilitadores não são peças isoladas, mas precisam de operar em conjunto e interagir uns com os outros.

Na prática, os facilitadores podem ser entendidos como os suportes sob os quais assenta a segurança de informação da organização, em que todos contribuem para os objetivos e nenhum pode falhar.

Figura 4 - Facilitadores *COBIT 5* (adaptado de ISACA, 2012a)

Os facilitadores identificados no "COBIT 5 *for Information Security"* estão representados na Figura 4 e são sumariamente descritos de seguida:

1) **Princípios, Políticas e Modelos**

Refere-se aos mecanismos de comunicação desenvolvidos com o objetivo de transmitir da forma mais adequada as diretivas e instruções dos órgãos de governança e gestão. Estes veículos traduzem em guias formais, mas práticos, o comportamento desejado por parte dos colaboradores no que respeita à segurança de informação, na gestão do dia-a-dia. É neste contexto colocado enfoque na necessidade de existirem mecanismos de comunicação que transmitam de forma adequada as diretrizes e instruções emanadas dos órgãos de governança e gestão.

2) Processos

Os processos descrevem um conjunto organizado de práticas e atividades tendo em vista atingir certos objetivos e produzir um determinado conjunto de resultados. O *COBIT 5* identifica 37 processos gerais, divididos em processos de governança e processos de gestão e organizados depois por áreas. Os processos e os objetivos associados são apresentados no Anexo A.

Refira-se que este é o facilitador base utilizado neste trabalho. É partindo dos processos que se vai procurar identificar todos os fatores chave para a boa governança e gestão da cibersegurança em instituições financeiras. Como foi referido no capítulo 5, quando se entra no campo da cibersegurança, existe uma rede interligada de fatores que contribuem para os resultados e que importa ter em devida conta. Existindo aí ligações de todos com todos, seria teoricamente possível começar a desenrolar o fio a partir de qualquer um desses determinantes. A escolha dos processos como ponto de partida deve-se ao entendimento de que este é o facilitador mais estudado e sistematizado e aquele que de forma mais completa estabelece laços diretos com os outros facilitadores. Efetivamente, é fácil compreender que, no desenvolvimento dum processo, é natural estabelecer relações com pessoas, tecnologia e toda a organização, identificando assim também esses pilares, no desenrolar desse mesmo processo. Na prática, ao contemplar e incluir na análise todos os processos, está-se, ao mesmo tempo, de forma natural, a incluir na análise todos os outros facilitadores. Por outro lado, e não menos importante, uma análise partindo dos

processos permite de forma mais fácil estabelecer paralelos e comparações com outros modelos, os quais terão também uma estrutura organizada em processos

3) **Estruturas organizacionais**

As estruturas organizacionais são entidades chave de tomada de decisão numa organização. No âmbito da Segurança de Informação, identificam-se papéis chave, como:

- CISO (*Chief Information Security Officer*);
- ISSC (*Information Security Steering Committee*);
- ISM (*Information Security Manager*);
- ERMC (*Enterprise Risk Management Committee*);
- *Information Custodians/Business Owners*.

Este facilitador não é, no âmbito deste trabalho, diretamente analisado. De qualquer modo, o mesmo é contemplado na análise, na medida em que, ao abordar os processos, os mesmos remetem para a necessidade de existirem estes papéis na organização e a sua intervenção é explicitada.

4) **Cultura, Ética e Comportamento**

O comportamento dos indivíduos e das organizações é muitas vezes subestimado como fator de sucesso no âmbito da governança e gestão da segurança de informação, embora ele assuma um papel fulcral e insubstituível para uma cibersegurança eficaz. Neste aspeto, a liderança assume um papel preponderante, enquanto influenciador de comportamentos.

5) **Informação**

A informação é aqui identificada não no sentido de informação de negócio, mas no sentido de meta informação, ou seja, na produção de guias e recolha de indicadores, essenciais para manter a organização a funcionar e com boa GTI.

6) **Serviços, Infraestruturas e Aplicações**

Os serviços, infraestruturas e aplicações capacitam a organização com informação, processamento de informação e serviços. As capacidades de serviços são fundamentais para garantir a segurança de informação e as funções associadas numa organização. Para além de infraestrutura e aplicações adequadas, os serviços são garantidos através duma combinação de outros facilitadores, como processos, informação e estruturas organizacionais.

7) **Pessoas, Capacidades e Competências**

Como já referido, e decorre da revisão de literatura, as pessoas são um elemento fulcral na boa gestão e governança da cibersegurança. Por um lado, é importante que todos os

colaboradores tenham conhecimento e consciência do papel que lhes cabe na proteção dos ativos de informação da organização. Por outro lado, aqueles colaboradores que têm um papel mais ativo nos processos de cibersegurança, seja por exemplo na deteção de incidentes, seja por exemplo na gestão dos acessos à informação, deverão ter as capacidades e competências adequadas por forma a garantir que todas as atividades são completadas com sucesso e que são tomadas as decisões mais corretas.

6.3. BCE - *CROE*

Estando o trabalho em causa direcionado para o setor bancário e financeiro, e tendo em conta as suas especificidades próprias, importa analisar de que forma as entidades com as principais responsabilidades neste setor encaram a problemática da segurança da informação e que documentação sobre o tema estão a produzir para as organizações do setor.

A nível da união europeia e monetária, é o BCE que é responsável pela política monetária e que exerce o papel de topo de supervisão sobre as entidades financeiras. O BCE atua como banco central para os 19 países que adotaram o euro. A sua principal função é a manutenção da estabilidade de preços na zona euro e apoiar o crescimento económico e a criação de emprego.

A um nível geográfico mais alargado, identifica-se o *Bank for International Settlements* (BIS). Criado em 1930, o BIS é a organização financeira internacional mais antiga a nível mundial. É controlado por 60 bancos centrais de países de todo o mundo que, no seu conjunto, representam 95% do Produto Interno Bruto mundial. A missão do BIS é a de servir os bancos centrais no objetivo da estabilidade financeira e monetária, de promover a cooperação internacional nessas áreas e atuar como um banco para os bancos centrais.

No âmbito da sua missão, o BIS promove a discussão e a colaboração entre bancos centrais, estabelecendo também o diálogo com outras autoridades responsáveis pela promoção da estabilidade financeira e desenvolvendo pesquisas e análises de políticas em assuntos de relevância para a estabilidade monetária e financeira. No âmbito das suas atividades, há uma crescente preocupação com os assuntos relacionados com a segurança de informação e a cibersegurança.

Nesse sentido, o BIS tem vindo a produzir documentação, direcionada para o setor, focada nos aspetos de cibersegurança e nos passos que devem ser dados para uma correta gestão e governança. Concretamente, o BIS (2016) produziu o *Guidance on cyber resilience for*

financial market infrastructures, com o objetivo de definir um modelo para todas as entidades do setor financeiro se capacitarem em termos de cibersegurança.

Posteriormente, baseado no trabalho que o BIS produziu, o BCE elaborou e difundiu aquele que é um documento chave na organização das infraestruturas do mercado financeiro – *CROE* (BCE, 2018), e que constitui o segundo pilar principal deste trabalho. Ou seja, cruzando os processos do *COBIT 5 for Information Security* com os determinantes do *CROE*, espera-se obter um modelo que tem em linha de conta vários vetores chave importantes e necessários para o trabalho: processos, cibersegurança e setor bancário e financeiro.

6.4. EUA/*NIST – Framework for Improving Critical Infrastructure Cybersecurity*

De base governamental, sediada no outro lado do Atlântico, o *National Institute of Standards and Technology* (NIST) foi fundado em 1901 e faz parte do *Department of Commerce*, dos Estados Unidos da América. É um dos mais antigos laboratórios de ciências físicas do mundo. O *NIST* tem produzido documentação muito relevante na área da cibersegurança e da segurança da informação e é visto à escala mundial como uma referência nesta matéria, tendo sido desenvolvidos muitos estudos tendo como base os modelos do *NIST*.

Neste contexto, merece destaque especial a designada *framework NIST* (2017), que foi um dos primeiros e mais completos modelos elaborado sobre o tema da governança e gestão da cibersegurança. Este, serviu e serve ainda de base a muitos dos modelos posteriores de cibersegurança.

A *framework NIST* constitui uma ferramenta preciosa para a compreensão, gestão e determinação de riscos de cibersegurança, quer internos à organização, quer externos. Nesse sentido, pode ser utilizada para a identificação e priorização de ações com vista à redução dos ciber-riscos, como é intuito deste documento. É também uma ferramenta que visa criar uma linguagem comum, a ser utilizada e aplicada em diferentes organizações, de diferentes naturezas, mas que seguem uma visão e uma abordagem semelhante em termos de cibersegurança.

A *framework NIST* prevê a existência de 5 funções, que contribuem para esse alinhamento, para a criação de uma cultura operacional comum e adequada às necessidades atuais. Essas funções centrais são as seguintes:

- Identificação - Compreensão do que é a organização, ao nível dos seus sistemas, ativos, dados e capacidades, com vista a uma gestão adequada do risco de cibersegurança;
- Proteção – Desenho e implementação dos controlos de segurança adequados para garantir a entrega dos serviços infraestruturais críticos;
- Deteção - Criação das condições para identificação correta e atempada de eventos de cibersegurança;
- Resposta – Desenvolvimento das atividades adequadas à tomada de ações de contenção e mitigação de riscos de cibersegurança, perante a ocorrência de um incidente de cibersegurança;
- Recuperação – Atividades com vista à promoção de mecanismos de ciber-resiliência na organização e a restaurar quaisquer capacidades ou serviços afetados por um evento de cibersegurança.

Refira-se que o trabalho de cruzamento da *framework NIST* com o *COBIT 5*, ao nível dos processos, foi já realizado pelo ISACA. Esse cruzamento foi aproveitado no âmbito deste trabalho, para verificar, validar e complementar a lista de critérios identificados.

6.5. UE – Diretivas *NIS* e RGPD

Após a incorporação dos requisitos ligados ao setor bancário e financeiro e na área da cibersegurança, o vetor seguinte a considerar relaciona-se com os aspetos legais e de conformidade. Nesse sentido, no quadro atual em que Portugal se insere, as principais diretrizes vêm da União Europeia (UE), pelo que importa analisar e integrar os requisitos daí oriundos.

A UE é uma união económica e política de 28 estados-membros independentes. A sua política externa e de segurança tem como objetivo permitir que os 28 estados-membros tenham mais peso na esfera mundial do que se agissem individualmente. Além de preservar a paz e reforçar a segurança internacional, visa promover a democracia, o estado de direito e o respeito pelos direitos e pelas liberdades do ser humano a nível mundial.

A UE intervém em diversos domínios, sendo a segurança uma das áreas que tem vindo a merecer uma atenção crescente, associada sobretudo às questões ligadas à cibersegurança, nas quais se inclui também o tema de segurança da informação.

As preocupações relativas à segurança da informação, levaram a UE a criar, em 2004, a ENISA, com o objetivo de contribuir de forma ativa para um nível elevado de segurança da informação e das redes e para o desenvolvimento de uma cultura de segurança da informação na sociedade.

Assim, a ENISA é um centro de especialização em cibersegurança na europa. A sua missão é a de contribuir para a segurança da sociedade da informação no espaço europeu, através do incremento da sensibilidade para a segurança das redes e informação e para a promoção de uma cultura de segurança para benefício dos cidadãos, consumidores, empresas e organizações do setor público na UE. A ENISA trabalha de forma próxima com os estados-membros e o setor privado no sentido de disponibilizar conselhos e soluções. Tal, inclui exercícios de cibersegurança à escala europeia, o desenvolvimento de estratégias nacionais de cibersegurança, cooperação ao nível de *Computer Security Incident Response Teams* (*CSIRT*) e desenvolvimento de capacidades, assim como estudos de segurança de serviços de computação em nuvem, proteção de dados, entre outros. A ENISA também dá suporte à UE ao nível do desenvolvimento e implementação de políticas e leis em matérias relacionadas com a segurança de informação.

O maior contributo documental para a segurança da informação, proveniente da UE, traduz-se nas diretivas e regulamentos emitidos que visam estabelecer os princípios de atuação em várias áreas onde a segurança é chave. Concretamente, identificam-se os seguintes principais regulamentos e diretivas, que importa ter em atenção:

6.5.1. Diretiva *NIS*

A aqui designada Diretiva *NIS* (União Europeia, 2016a), corresponde à Diretiva (UE) 2016/1148 do parlamento e do conselho, de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.
No seu Anexo I, a mesma define "Obrigações e atribuições das equipas de resposta a incidentes de segurança informática (*CSIRT*)", onde se inclui um conjunto de aspetos relevantes a ter em devida conta, no contexto deste trabalho.

6.5.2. RGPD

O RGPD está definido por dois documentos da União Europeia:

- Diretiva (UE) 2016/680 do parlamento europeu e do conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados (União Europeia, 2016b);
- Regulamento (UE) 2016/679 do parlamento europeu e do conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (União Europeia, 2016c).

Para o contexto deste documento, destaca-se a Secção 2 "Segurança dos dados pessoais" da Diretiva indicada.

6.6. Conclusões – Critérios de análise e avaliação

Identificados os principais atores à escala global, relevantes para o trabalho em causa, e os modelos de gestão de segurança de informação e de cibersegurança produzidos por cada um deles e que relevam para a análise pretendida, importa efetuar o cruzamento desses modelos, com o objetivo de identificar e sistematizar um conjunto de processos, que constituam, *de per si*, um modelo de funcionamento base, reconhecidamente entendidos como um modelo de boas práticas, para aplicação em instituições financeiras do eurosistema.
Associado a cada processo, identifica-se um conjunto de critérios que funcionarão como validadores e avaliadores do nível de cumprimento da organização face a esse processo e que

servirá, em última análise, para a aferição do estado de maturidade em termos de cibersegurança. Esta avaliação é uma etapa crucial no processo de implementação do projeto. Essa metodologia de cruzamento de modelos, foi realizada do seguinte modo:

i) Partiu-se, em primeiro lugar, de um desenvolvimento específico que o ISACA efetuou, com a elaboração do guia *COBIT 5 for Information Security* (ISACA, 2012b), em que o modelo do *COBIT 5* foi particularizado para o campo da segurança de informação.

ii) O modelo *COBIT* identifica 6 facilitadores, que são, no fundo, as componentes que suportam a gestão de TI nas organizações e que devem ser tidos em conta na implementação do projeto. A abordagem que se teve neste trabalho ao modelo *COBIT* partiu da componente de Processos, por se entender ser aquela com campo de aplicação mais direto e facilitado na organização e que de forma mais natural interliga com os restantes facilitadores do *COBIT 5*, permitindo também aproveitar os aspetos relevantes associados a cada uma das outras componentes. Os processos do *COBIT 5* estão elencados no Anexo A.

iii) Como já referido, o *COBIT 5* constitui um modelo muito genérico, com campo amplo de aplicação. Este caráter genérico permite, nomeadamente, o cruzamento do modelo com outros mais específicos, incorporando com isso contextos específicos de análise. Neste sentido, identificou-se um modelo reconhecido de aplicação no setor financeiro, o *CROE*, promovido pelo BCE, e efetuou-se o cruzamento dos dois modelos ao nível dos processos preconizados. O *CROE* também tem um enfoque específico na cibersegurança, pelo que, com este cruzamento, consegue-se trazer à análise contextos específicos da cibersegurança no setor financeiro. Com esta etapa, são também identificados os processos do *COBIT 5* que têm pouca ou nenhuma relevância no âmbito do *CROE* e que serão, por isso, omitidos do quadro final. A Figura 5 representa este processo de mapeamento dos requisitos *CROE* em critérios associados à avaliação do cumprimento dos processos COBIT 5.

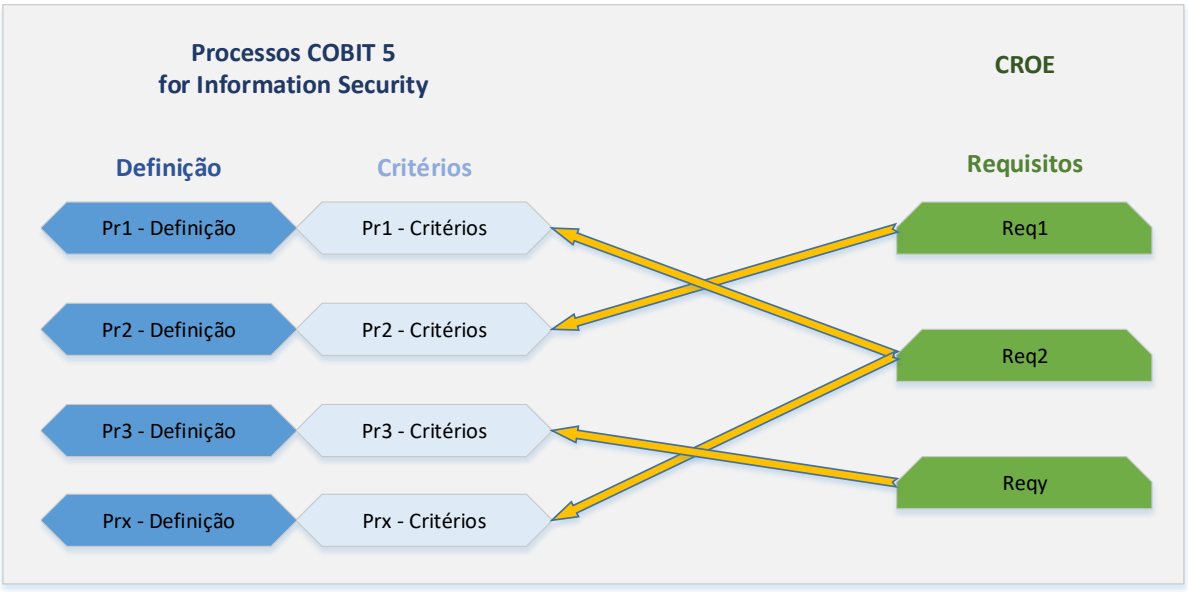

Figura 5 – Cruzamento do *CROE* com o *COBIT 5*, ao nível dos processos

iv) Como complemento, integrou-se ainda na análise o modelo de cibersegurança desenvolvido pelo *NIST*, a designada *framework NIST*, aproveitando-se um trabalho que já tinha sido realizado pelo ISACA (2012a) de cruzamento da *framework NIST* com o *COBIT 5*.

v) Por fim, teve-se ainda em atenção alguns aspetos legais mais relevantes para a análise em causa. Para isso, consideraram-se as Diretivas da UE - Diretiva *NIS* e diretiva RGPD, as quais foram integradas na identificação de critérios de avaliação de processos.

O cruzamento que foi efetuado é apresentado no Anexo B, onde se identifica, para cada processo *COBIT 5*, o conjunto de critérios, no âmbito dos outros modelos considerados, que têm relevância para o produto final.

Nas tabelas seguintes é apresentado o resultado do trabalho descrito nos pontos anteriores. Concretamente, para cada um dos processos *COBIT 5* considerados como relevantes, é apresentada uma tabela com os critérios de validação da efetiva implementação desse processo, os quais estão organizados em 3 níveis de maturidade: Base, Intermédio e Avançado.

EDM01 - Garantir a Definição e Manutenção do Modelo de Governança
Critérios BASE – Questões de avaliação:
▪ Existe um documento de estratégia de ciber-resiliência, a mesma está alinhada com a estratégia corporativa e com a estratégia de TI, e esse documento é regularmente revisto e atualizado? ▪ Existe um documento de modelo de ciber-resiliência que defina objetivos de cibersegurança e tolerância ao risco, assim como a forma como são implementadas as fases de identificação, mitigação e gestão de ciber-riscos na organização, assim como os papéis e responsabilidades pela tomada de decisão? ▪ O modelo de ciber-resiliência incorpora de forma sistemática os requisitos (políticas, procedimentos e controlos) relacionados com governança, identificação, proteção, deteção, resposta e recuperação, testes, análise situacional e formação? ▪ São utilizados os mais reconhecidos normativos, guias e recomendações internacionais, nacionais e setoriais na gestão da cibersegurança? ▪ O modelo de ciber-resiliência é consistente com o modelo de gestão de risco da organização? ▪ O modelo de ciber-resiliência está alinhado com a estratégia de ciber-resiliência e é revisto e atualizado, pelo menos, anualmente? ▪ O Conselho de Administração aprovou a estratégia e modelo de ciber-resiliência, assim como o nível de tolerância de risco e acompanha de perto a implementação do modelo e das políticas, procedimentos e controlos que o suportam? ▪ O Conselho de Administração tem as capacidades, conhecimentos e experiência apropriados para a compreensão dos ciber-riscos? ▪ Está formalmente designado um CISO (*Chief Information Security Officer*) na organização, independente dos departamentos de TI e auditoria, e responsável pela implementação da estratégia e modelo de ciber-resiliência? ▪ Os colaboradores com funções focadas em atividades de cibersegurança têm capacidades, conhecimentos e experiência adequados e estão suficientemente informados e mandatados para a tomada de decisões?

▪ As questões relacionadas com ciber-risco, implementação do modelo de ciber-resiliência e temas associados, estão regularmente na agenda do Conselho de Administração?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ São usadas métricas e modelos de maturidade para avaliar e medir a adequabilidade e eficácia de adesão ao modelo de ciber-resiliência, sendo a avaliação realizada através de auditorias e programas de conformidade independentes?
Critérios AVANÇADOS – Questões de avaliação:
▪ A estratégia de ciber-resiliência define metas de curto prazo e de longo prazo? ▪ A estratégia e modelo de ciber-resiliência definem a forma como devem ser efetuadas revisões e proactivamente identificar, mitigar e gerir os ciber-riscos para todo o setor? ▪ Estão estabelecidas as estruturas adequadas, assim como os processos e relações com as entidades do setor para continuamente melhorar a ciber-resiliência de todo o setor? ▪ Existe um especialista em cibersegurança dedicado a apoiar o Conselho de Administração nestas matérias?

Tabela 1 – Critérios EDM01

APO03 - Gerir Arquitetura da Organização
Critérios BASE – Questões de avaliação:
▪ Estão identificadas e documentadas todas as funções críticas, papéis chave, processos e ativos de informação que suportam essas funções e o inventário é mantido numa base regular? ▪ Esse inventário também inclui os prestadores de serviços e interligações que suportam funções críticas? ▪ O inventário está integrado com os processos de aquisição e de gestão de mudança? ▪ Existe um mapa simplificado da rede, com inclusão dos recursos de rede, endereçamento IP associado e ligações com o exterior?

▪ Estão identificados e documentados e são regularmente revistos os sistemas e processos de suporte a funções ou operações críticas, que são dependentes de conectividade externa?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ Existem ferramentas automatizadas e centralizadas de AIM (*Asset Inventory Management*) que permitam e suportem a identificação e classificação de funções críticas, processos, ativos de informação e interligações? ▪ Esse inventário é atualizado de forma efetiva e atempada, numa base regular e sempre que ocorrem mudanças? ▪ São enviados alertas em caso de alterações ao inventário? ▪ Existem mapas atuais e completos dos recursos de rede, das interligações e dependências e fluxos de dados com outros sistemas, incluindo ligações com parceiros, prestadores de serviços *cloud* e outros prestadores de serviços? ▪ Esses mapas são utilizados para a análise de risco, identificação de dependências chave e aplicação de controlos de segurança?
Critérios AVANÇADOS – Questões de avaliação:
Não identificados

Tabela 2 - Critérios APO03

APO07 - Gerir Recursos Humanos
Critérios BASE – Questões de avaliação:
▪ Existe um programa contínuo de formação em cibersegurança para todos os colaboradores da organização? ▪ Esse programa é conduzido pelo menos numa base anual e inclui os membros da administração e gestão de topo? ▪ Esse programa da formação inclui temas como identificação e reporte de eventos e atividades anómalas, bem como resposta a incidentes, ciberameaças atuais e tendências futuras?

- No programa de formação, existem módulos específicos focados na segurança de dados pessoais e procedimentos a ter em caso de deteção de fuga de informação relacionada?
- Nos programas e materiais de formação e sensibilização a prestar aos colaboradores são incorporadas lições aprendidas, assim como informações decorrentes das análises realizadas de ciberameaças, numa base contínua e dinâmica?
- É transmitido aos colaboradores, de forma clara, os ciber-riscos a que estão sujeitos na execução das suas atividades e no papel e responsabilidades que cada um tem na proteção dos ativos da organização?
- Os colaboradores e elementos contratados com contas de utilizador com acessos privilegiados, ou com acesso a ativos e informação sensíveis, recebem formação adicional em cibersegurança, de acordo com o seu grau de responsabilidade?
- Os colaboradores das unidades de negócio recebem formação focada nos riscos particulares da atividade que desenvolvem?
- Os colaboradores com funções de elevado ciber-risco (gestores, administradores de sistemas, programadores, etc) recebem formação específica, relevante para as suas funções?
- A equipa de resposta a incidentes recebe formação focada nas suas responsabilidades e atribuições?
- Os colaboradores com funções operacionais recebem formação e treino focado nos procedimentos operacionais, previamente à entrada em produção de um novo sistema?
- Na situação de ocorrer um ciberincidente de grande visibilidade ou um alerta por parte de entidades regulatórias, são disponibilizados materiais de sensibilização em cibersegurança explicativos da situação a todos os colaboradores?
- É preocupação da gestão, garantir que identifica e assegura as competências, capacidades e recursos necessários à implementação da estratégia e modelo de cibersegurança e tal é revisto numa base contínua, à medida que a tecnologia e os riscos evoluem?

Critérios INTERMÉDIOS – Questões de avaliação:

▪ É efetuada uma análise da eficácia dos programas de formação em cibersegurança e são efetuados ajustes aos mesmos com base nos resultados dessa análise? ▪ Existe um código formal de conduta de cibersegurança, aplicável a todos os colaboradores? ▪ A avaliação de desempenho dos colaboradores contempla como variável de indexação o cumprimento do colaborador com as normas de cibersegurança da organização? ▪ Estão previstos incentivos aos trabalhadores que promovam comportamentos e uma cultura adequados de ciber-riscos? ▪ Existe um programa de recursos humanos focado especificamente no recrutamento, retenção e sucessão dos colaboradores com funções em cibersegurança? ▪ Todos os colaboradores envolvidos na gestão de incidentes de cibersegurança têm capacidades adequadas para a eficaz gestão do incidente, por forma a garantir que as evidências recolhidas são juridicamente válidas?
Critérios AVANÇADOS – Questões de avaliação:
▪ Os programas de formação em cibersegurança são permanentemente atualizados tendo em conta a evolução do cenário de ameaças do setor? ▪ Há ações concretas desenvolvidas pela gestão de topo com o objetivo de melhorar a cultura de cibersegurança da organização?

Tabela 3 – Critérios APO07

APO08 - Gerir Relacionamentos
Critérios BASE – Questões de avaliação:
▪ Estão identificados e documentados todos os processos de negócio dependentes de serviços de terceiros? ▪ Estão identificadas as interligações com terceiros e a lista é mantida numa base regular? ▪ É efetuada regularmente uma análise de risco aos prestadores de serviços e tido em conta a evolução do cenário de ameaças, nessa análise? ▪ É garantido que os prestadores de serviços em *outsourcing* têm um nível adequado de ciber-resiliência?

Critérios INTERMÉDIOS – Questões de avaliação:
▪ Existe uma ferramenta de GRC (*Governance, Risk and Compliance*) que garanta automatismos na inventariação de parceiros, prestadores de serviços e interligações externas? ▪ São efetuadas auditorias independentes que validem a efetiva gestão de segurança por parte dos prestadores de serviços e *outsourcing*? ▪ São recebidas, da parte dos prestadores de serviços, evidências relativas às suas capacidades de ciber-resiliência, como certificações, auditorias externas e relatórios de testes efetuados?
Critérios AVANÇADOS – Questões de avaliação:
▪ Estão identificados os ciber-riscos colocados por e colocados a outras entidades do setor financeiro? ▪ É mantida uma colaboração estreita com os prestadores de serviços e outras entidades do setor financeiro no sentido de melhorar a segurança dos terminais e interligações, nomeadamente através da realização conjunta de testes de resposta e recuperação a incidentes? ▪ Há uma cooperação estreita com outras entidades do setor financeiro, ao nível da gestão de topo, no sentido da promoção duma cultura de ciber-resiliência em todo o setor?

Tabela 4 - Critérios APO08

APO10 - Gerir Fornecedores
Critérios BASE – Questões de avaliação:
▪ É mantido e atualizado regularmente um inventário das interligações com outras entidades e fornecedores? ▪ O modelo de ciber-resiliência aborda essas interligações, numa perspetiva de risco? ▪ É efetuada uma avaliação das capacidades de segurança dos fornecedores (pelo menos através de *self-assessment*)?
Critérios INTERMÉDIOS – Questões de avaliação:

Não identificado
Critérios AVANÇADOS – Questões de avaliação:
Não identificado

Tabela 5 - Critérios APO10

APO12 - Gerir Riscos
Critérios BASE – Questões de avaliação:
▪ Existe um modelo de gestão de riscos, com vista à identificação de riscos e à definição da condução de análises de risco, numa base regular? ▪ São realizadas análises de risco antes da introdução de novas tecnologias, produtos, serviços e conexões, para a identificação de potenciais ameaças e vulnerabilidades? ▪ O processo de análise de risco é atualizado no caso de surgirem novas informações que afetem os riscos de segurança de informação? ▪ O resultado das análises de risco é utilizado para alimentar a estratégia e modelo de ciber-resiliência?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ É feito uso de CTI (*Cyber Threat Intelligence*) para antecipar as capacidades, intenções e *modus operandi* de atacantes e, desse modo, antecipar possíveis futuros ataques? ▪ Nesse sentido, existem análises e relatórios de risco de ciberameaças que usem essas informações de CTI? ▪ Essas análises são continuamente revistas e atualizadas à luz de novas ameaças e vulnerabilidades? ▪ São consideradas mesmo as ameaças pouco prováveis, mas que podem ter impactos significativos? ▪ Essas análises e relatórios são analisados e discutidos ao nível do Conselho de Administração e gestão de topo?
Critérios AVANÇADOS – Questões de avaliação:

▪ As informações recolhidas no âmbito dos processos de CTI, incluem a capacidade de análise sob informações provenientes de outras instituições financeiras? ▪ A análise de informação é efetuada de forma a permitir a implementação de controlos de segurança focados nas ameaças concretas identificadas? ▪ Os processos de CTI são tendencialmente automáticos?

Tabela 6 - Critérios APO12

APO13 - Gerir Segurança
Critérios BASE – Questões de avaliação:
▪ Existe, e é mantido numa base regular de atualização, um inventário exaustivo de todas as contas pessoais e de sistema (especialmente incluindo contas privilegiadas e de acesso remoto), que permita conhecer as autorizações de acesso a ativos de informação e sistemas de suporte? ▪ Existe, e é mantido numa base regular de atualização, um inventário exaustivo de todos os repositórios da organização onde residem dados pessoais, no âmbito da categorização efetuada no âmbito do RGPD?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ Existem ferramentas automáticas de IAM (*Identity and Access Management*) que suportem a identificação e classificação de perfis de contas e garantam que essa gestão é efetuada de forma correta? ▪ Essas ferramentas permitem o envio de alertas automáticos em caso de alterações? ▪ Nessas ferramentas de AIM (*Asset Inventory Management*) e IAM estão definidos e implementados critérios e regras para identificar alterações inesperadas que precisem de investigação? ▪ É efetuada uma monitorização contínua das ligações via IP (*Internet Protocol*) realizadas entre máquinas e dos níveis de ciber-risco associados a essas ligações e são mantidos e analisados os dados dessas ligações?
Critérios AVANÇADOS – Questões de avaliação:

▪ São identificados riscos emergentes, em tempo real, e utilizadas ferramentas automáticas (AIM e IAM), de modo a atualizar permanentemente a análise de risco e tomar as medidas de mitigação necessárias, de forma rápida e em linha com o nível de tolerância de risco da organização?

Tabela 7 - Critérios APO13

BAI01 - Gerir Programas e Projetos
Critérios BASE – Questões de avaliação:
Não identificado
Critérios INTERMÉDIOS – Questões de avaliação:
▪ Está desenvolvido e implementado um ISMS (*Information Security Management System*) baseado em reconhecidos normativos internacionais (p.e. ISO 27001) de modo a desenvolver, implementar, operar, monitorar de forma contínua, manter e melhorar um modelo de controlo de segurança de informação? ▪ A ciber-resiliência está integrada no SDLC (*System Development Life Cycle*), nas etapas de desenho, implementação, aquisição ou modificação dos sistemas, processos e produtos?
Critérios AVANÇADOS – Questões de avaliação:
▪ O ISMS está certificado? ▪ Estão desenvolvidos processos e procedimentos para, de forma permanente e automática, ajustar e melhorar os controlos de segurança, por forma a garantir proteção contra ameaças existentes e emergentes? ▪ Estes controlos são tendencialmente preditivos (ao invés de reativos), usando informação em tempo real sobre ameaças, vulnerabilidades e alterações operacionais?

Tabela 8 - Critérios BAI01

BAI02 - Gerir Definição de Requisitos
Critérios BASE – Questões de avaliação:

▪ No desenho e desenvolvimento dos sistemas e processos, os requisitos de segurança são identificados ao mesmo tempo que os requisitos de sistema e processos de modo a identificar os controlos de segurança nas etapas iniciais? ▪ Todas as aplicações usadas foram desenvolvidas tendo em conta as práticas de desenvolvimento seguro e com requisitos de controlos de segurança, quer as mesmas tenham sido adquiridas ou desenvolvidas internamente?
Critérios INTERMÉDIOS – Questões de avaliação:
Não identificado
Critérios AVANÇADOS – Questões de avaliação:
Não identificado

Tabela 9 - Critérios BAI02

BAI06 - Gerir Mudanças
Critérios BASE – Questões de avaliação:
▪ Estão em vigor políticas, procedimentos e controlos para a gestão da mudança, incluindo critérios de priorização e classificação das mudanças? ▪ Anteriormente a qualquer mudança, a mesma é revista à luz das necessidades de negócio, categorizada e aprovada ao nível adequado de gestão? ▪ Existem políticas e processos de gestão de *patching*, que incluam a manutenção do conhecimento dos *patches* disponíveis, a identificação dos *patches* aplicáveis a cada sistema interno, a análise de impactos e testes antes e após a instalação? ▪ A equipa responsável pela cibersegurança está envolvida em todo o ciclo do processo de gestão de mudança? ▪ Estão implementados procedimentos (p.e. revisão de código, testes modulares), baseados nas melhores práticas, por forma a garantir a implementação correta e eficiente das mudanças? ▪ São testadas, validadas e documentadas as mudanças dos sistemas de informação antes da sua implementação em produção?

▪ Existem processos que permitam identificar, analisar e aprovar mudanças que sejam efetivamente urgentes e é feita uma revisão da mesma pós implementação? ▪ São privilegiadas configurações padrão nos equipamentos, para facilitar o processo de gestão de *patching*? ▪ A instalação de novos *patches* requer a aprovação prévia do nível adequado de gestão? ▪ Existem procedimentos para a rápida recuperação em caso de problema na aplicação da mudança ou *patches*? ▪ Qualquer alteração no ambiente de produção tem um plano de retorno associado? ▪ Existem políticas e procedimentos que proíbam a instalação de alterações e *patches* que não tenham sido pré aprovados?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ O processo de gestão da mudança está assente em normativos e boas práticas bem estabelecidos e reconhecidos? ▪ O processo de gestão da mudança está, tanto quanto possível, automatizado? ▪ Existe um ambiente replicado e separado do ambiente de produção, que permite o teste e implementação rápidos das mudanças ou *patches* e uma rápida reposição, quando necessário?
Critérios AVANÇADOS – Questões de avaliação:
▪ Existe um processo automático que impeça a instalação de alterações e *patches* em sistemas de informação, que não tenham sido previamente aprovados?

Tabela 10 - Critérios BAI06

BAI08 - Gerir Conhecimento
Critérios BASE – Questões de avaliação:
▪ Existem políticas e procedimentos que permitam a divulgação, de forma responsável, de informações relativas a potenciais vulnerabilidades, especialmente informações que permitam uma resposta pronta e mitigação de riscos por parte de outras entidades, contribuindo assim para a segurança de todo o setor?

- Existem e são regularmente revistos as regras, os acordos e as formas de partilha de informação, como forma de controlar a publicação e distribuição dessas informações e prevenir a disseminação de informação sensível que pode ter consequências adversas se feita de forma desadequada?
- Há processos estabelecidos de identificação de ciberameaças, que coloquem em risco a continuidade de serviço da organização ou que possam ter um impacto significativo no setor?
- Existe a capacidade de recolha de informações de ciberameaças a partir de fontes internas (p.e. aplicações*, logs* de sistema e de rede, *firewalls, IPS*) e fontes externas (fornecedores credíveis de ciberinformações, informações públicas)?
- A organização pertence a ou subscreve informações de algum centro de partilha, que produza informações sobre ciberameaças e vulnerabilidades?
- Existe a capacidade de análise de informações de ciber-ameaças recolhidas de diferentes fontes, enquadrando-as na realidade técnica e de negócio da organização?
- Estão definidos os objetivos da partilha de informação, em linha com os objetivos de negócio e o modelo de ciber-resiliência adotado?
- Está definido o âmbito das atividades de partilha de informação, estando identificados os tipos de informação a partilhar, as circunstâncias em que tal deve ser feito, com quem pode ser partilhada e o tratamento que deve ser dado a essas informações?
- Estão definidos e são revistos regularmente as regras e acordos de partilha de informação e implementados procedimentos que permitam a rápida partilha de informação, assegurando ao mesmo tempo as obrigações de proteção de informações sensíveis?
- Estão estabelecidos canais seguros de comunicação com outras entidades do setor para a partilha de informação?

Critérios INTERMÉDIOS – Questões de avaliação:

- São trocadas informações com entidades relevantes do setor, incluindo instituições financeiras e fornecedores de serviços, para permitir melhorar os planos de resposta e recuperação a incidentes?

- É feita uma análise contínua às soluções e desenvolvimentos tecnológicos disponíveis no mercado, que possam melhorar as capacidades de resposta e recuperação a incidentes da organização?
- Estão desenvolvidas capacidades para procurar, analisar e usar informações de ciberameaças para com isso atualizar os programas de testes?
- Há uma participação ativa em grupos de partilha de informações, incluindo grupos setoriais, governamentais e internacionais?
- Estão estabelecidos protocolos de partilha de informações de ciberameaças, vulnerabilidades e incidentes com os colaboradores da organização, com base nas suas funções e responsabilidades?
- São partilhadas informações com entidades relevantes do setor?
- São incorporadas lições aprendidas a partir de ciberevents ocorridos, ou a partir de testes realizados, nos processos de resposta e recuperação a incidentes?

Critérios AVANÇADOS – Questões de avaliação:

- Existe uma colaboração ativa com outras entidades do setor bancário e financeiro, no sentido de haver uma partilha de conhecimento e boas práticas, para identificação e implementação de controlos de segurança para o setor bancário e financeiro, no seu todo?
- São utilizadas múltiplas fontes de informação externas para previsão de potenciais ataques futuros e tendências de ataques e para proactivamente serem tomadas medidas para melhorar as capacidades de cibersegurança?
- Existe uma colaboração e cooperação ativas com as entidades relevantes dentro do setor bancário e financeiro, no sentido de desenvolver planos de resposta e recuperação conjuntos, para incidentes que possam impactar todo o setor?
- E são realizados regularmente exercícios envolvendo as várias entidades?
- Há uma atitude de abertura e colaboração para com o setor, no sentido de melhorar as investigações forenses e as metodologias e ferramentas de gestão de incidentes?
- São partilhados os resultados dos cibertestes com as entidades relevantes do setor, como forma de melhorar a ciber-resiliência global e enquadrado em acordos específicos de partilha de informação?

▪ Existem capacidades internas de CTI (incluindo pessoas, tecnologia e treino), que permitam desenvolver e guardar informações de ameaças e vulnerabilidades internas e externas, analisar as informações e disseminá-las às entidades relevantes do setor? ▪ Há iniciativas desenvolvidas para identificar falhas nos mecanismos atuais de partilha de informação e resolvê-las, para facilitar uma resposta global do setor a incidentes de larga escala?

Tabela 11 - Critérios BAI08

DSS01 - Gerir Operações
Critérios BASE – Questões de avaliação:
▪ Estão definidos parâmetros normais de funcionamento dos sistemas, para permitir a deteção de anomalias com base em desvios a esse padrão? ▪ Estão desenvolvidas capacidades, ao nível de pessoas, processos e tecnologia, que permitem a monitorização e deteção de atividades e eventos anómalos? ▪ Existem capacidades de monitorização de eventos de segurança de informação relacionados com atividades de utilizadores? ▪ Existem capacidades de monitorização de ligações, fornecedores de serviço, equipamentos e *software*? ▪ A informação recolhida no âmbito das operações é utilizada para melhorar as capacidades de deteção e monitorização e os processos de resposta a incidentes? ▪ Estão definidos parâmetros e patamares de alerta para a deteção de incidentes de cibersegurança? ▪ Os perfis base de utilização dos sistemas, que servem de referência à deteção de anomalias, são periodicamente revistos, testados e atualizados? ▪ Estão definidos patamares para os sistemas de monitorização e deteção, para a geração de alertas automáticos que facilitem o processo de resposta a incidentes? ▪ As capacidades de monitorização e deteção contemplam a recolha e guarda de dados de investigação forense e esses dados são replicados numa localização segura?

▪ Os processos de recolha e análise de informação de ciberameaças e produção de CTI são regularmente revistos e atualizados? ▪ As informações de CTI são disponibilizadas aos colaboradores com responsabilidades de mitigação de ciber-riscos, aos níveis estratégico, tático e operacional?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ Está implementado um SIEM (*Security Information and Event Management System*), que permita correlacionar de forma automática todos os alertas de rede e de sistemas? ▪ Está implementado um SOC (*Security Operations Centre*), que possibilite a recolha, centralização e correlação de informações de eventos provenientes de múltiplas fontes? ▪ Existem processos de monitorização de atividades que não estejam em linha com a política de segurança da organização? ▪ Existem mecanismos de envio de alertas automáticos aos colaboradores apropriados, em caso de incidente? ▪ É continuamente monitorizado e inspecionado o tráfego de rede, incluindo ligações remotas e dos terminais e comparado com o padrão expectável?
Critérios AVANÇADOS – Questões de avaliação:
▪ Estão implementados mecanismos de deteção de intrusões, com capacidade de automaticamente detetar e bloquear ataques, em tempo real, incluindo ataques *0day*? ▪ Estão implementados mecanismos tipo *honeypot*, que chamem a atenção de potenciais atacantes e permitam o lançar de alertas e detetar ataques, sem comprometer os sistemas reais? ▪ Estão implementados mecanismos de monitorização em tempo real das ligações externas, associados a diagramas que apresentem mudanças em tempo real da infraestrutura de ligações de rede, flutuações de volume de tráfego e lancem alertas quando o ciber-risco suba? ▪ Os processos de CTI estão integrados e alinhados com a informação produzida e utilizada pelo SOC?

Tabela 12 - Critérios DSS01

DSS02 - Gerir Solicitações e Incidentes de Serviços
Critérios BASE – Questões de avaliação:
▪ Existem planos claros de resposta e recuperação face à ocorrência de incidentes? ▪ Esses planos são testados regularmente? ▪ Esses planos são aprovados ao nível do Conselho de Administração? ▪ Existe uma equipa CSIRT responsável pela resposta aos incidentes de segurança e intrusões e pela coordenação de atividades dentro da organização e com outras entidades do setor? ▪ É feita recolha e cruzamento de informação proveniente dos ciberincidentes ocorridos e dos testes realizados, com vista à melhoria contínua dos planos de resposta e recuperação? ▪ Estão identificados os colaboradores que são essenciais para a mitigação de risco de ciberincidentes e eles estão cientes do seu papel no escalamento do incidente? ▪ Estão identificadas as unidades internas e entidades externas a notificar em caso de incidente, assim como que informações transmitir e quando? ▪ Estão definidos critérios objetivos para o escalamento de ciberincidentes e vulnerabilidades para a Administração e gestão de topo, baseados no impacto potencial e criticidade de risco? ▪ Existe um plano de comunicação e procedimentos definidos para a notificação de todas as entidades relevantes (incluindo reguladores, media, clientes) de forma atempada, em caso de ciberincidente? ▪ Estão identificados quais os cenários de incidentes que podem ter impacto potencial no negócio e para os quais deverão ser recolhidas evidências digitais para investigação futura mais aprofundada? ▪ Existe um processo de gestão das evidências digitais disponíveis nos sistemas, que preveja o seu tratamento no âmbito do seu ciclo de vida? ▪ Estão mapeados os tipos e localização de evidências digitais para os vários cenários de ameaça identificados? ▪ Existe uma PPF (Política de Prontidão Forense) aprovada pelo Conselho de Administração, que defina os tipos de log a manter e os períodos de retenção?

- Existem procedimentos para recolher evidências digitais de forma correta e em concordância com requisitos definidos no PPF?
- Existem políticas para o tratamento e guarda seguros das evidências digitais recolhidas?

Critérios INTERMÉDIOS – Questões de avaliação:

- Existe capacidade para detetar ciberincidentes (como tentativas de intrusão, exploração de vulnerabilidades, acessos indevidos, fugas de informação) e rapidamente adaptar os controlos de segurança para a sua mitigação?
- A gestão de ciberincidentes inclui fases de preparação, deteção, análise, contenção, erradicação e recuperação?
- Existem mapas com identificação das dependências funcionais e de segurança dos vários ativos de informação dos sistemas?
- São tiradas lições dos ciberataques reais que ocorrem na organização e as mesmas são introduzidas nos planos de resposta e recuperação?
- Os processos e sistemas estão desenhados no sentido de permitirem o retomar de operações críticas em duas horas após uma ciber-disrupção e para retomar a normalidade até ao fim do dia, mesmo em cenários extremos?
- Estão identificados um conjunto de cenários plausíveis de ciberincidentes e desenvolvidos planos específicos de resposta e de comunicação para cada um desses cenários, tendo em consideração também os aspetos legais e regulatórios aplicáveis?
- Há planos de prontidão forense integrados com os planos de gestão de incidentes e outras atividades de negócio relacionadas?
- Existem procedimentos definidos sobre a forma como recolher e guardar evidências digitais por forma a que as mesmas sejam válidas judicialmente?

Critérios AVANÇADOS – Questões de avaliação:

- Existem processos implementados para a melhoria contínua dos planos de resposta e recuperação, que tenham em conta as informações provenientes de CTI, as informações partilhadas com as outras entidades do setor e as lições aprendidas de eventos anteriores?
- Estão estabelecidos KPI (*Key Performance Indicators*) que meçam os objetivos de tempo de recuperação?

▪ A equipa CSIRT tem autoridade dentro da organização para definir as mudanças necessárias realizar para a recuperação ao incidente? ▪ Estão definidos processos de resposta automática a incidentes, desencadeados por critérios, parâmetros e patamares pré definidos? ▪ A infraestrutura de ligações de rede está definida de um modo que permita a segmentação ou isolamento imediato de determinadas ligações, em caso de incidente? ▪ Na ocorrência de ciberincidentes, existem mecanismos de notificação instantânea da gestão de topo, colaboradores relevantes e entidades externas relevantes através de múltiplos canais de comunicação, com possibilidade de validação da entrega? ▪ Existe um processo de gestão de revisão dos PPF, que tenha em conta a experiência e novos conhecimentos?

Tabela 13 - Critérios DSS02

DSS04 - Gerir Continuidade
Critérios BASE – Questões de avaliação:
▪ Estão definidos RPO (*Recovery Point Objectives*) e RTO (*Recovery Time Objectives*) face à ocorrência de um ciberincidente, que sejam coerentes com as necessidades de negócio e o evitar de risco de sistémico no setor? ▪ Estão identificados cenários de ciberincidentes, incluindo cenários extremos mas plausíveis, e foram realizadas análises de impacto desses incidentes? ▪ Estão definidos planos de contingência, face a diferentes cenários de ciberincidentes, que permitam definir objetivos de recuperação, prioridades de restauro e identifiquem as capacidades necessárias garantir, nomeadamente papéis e responsabilidades? ▪ Está definida uma política formal de *backups*, que especifique a frequência mínima e o âmbito, com base na criticidade e frequência de atualização de dados? ▪ Estão definidas estratégias e métodos para a realização de *backups* e *restores* com um tempo mínimo de indisponibilidade e disrupção limitada?

▪ Estão definidas políticas e procedimentos sobre como trabalhar em conjunto com as entidades relevantes interligadas para o retomar de operações, assim que seja seguro e prático fazê-lo?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ Os processos de resposta e recuperação a ciberincidentes estão integrados com os planos de gestão de crises, continuidade de negócio e recuperação de desastres?
Critérios AVANÇADOS – Questões de avaliação:
▪ As estratégias e métodos de realização de *backups* e *restores* de informação são integrados na infraestrutura dos sistemas, na fase de desenvolvimento ou de aquisição?

Tabela 14 - Critérios DSS04

DSS05 - Gerir Serviços de Segurança
Critérios BASE – Questões de avaliação:
▪ Está implementada uma estratégia de defesa em profundidade, com múltiplos controlos de segurança independentes, para garantir redundância? ▪ Existe proteção de perímetro na infraestrutura de rede, com recurso a ferramentas de defesa como *Firewall, IPS/IDS e Proxies*? ▪ Existe uma rede dedicada para acessos de administração de sistemas? ▪ Estão definidas configurações de segurança base para os sistemas e componentes, com vista a facilitar a aplicação consistente de segurança? ▪ As configurações aplicadas na infraestrutura de rede e nos sistemas de informação seguem normativos de segurança reconhecidos e alterações a isso são controladas e monitoradas? ▪ São utilizados protocolos seguros de rede para o acesso aos sistemas, como SSH? ▪ Existem mecanismos para limitar, impedir e terminar sessões após um determinado período de inatividade? ▪ Existem configurações efetuadas ao nível dos *firewalls* locais das máquinas que bloqueiem, por omissão, portos IP de administração? ▪ Estão implementados sistemas de IPS/IDS e soluções de segurança de *endpoint*?

- Estão implementados controlos que evitem que dispositivos não autorizados se liguem à rede (p.e. telemóveis pessoais) e às máquinas (p.e. *pen usb*)?
- Existem políticas e controlos que impeçam utilizadores de instalar aplicações não autorizadas?
- Existem controlos implementados para proteção de dados em repouso, em uso e em trânsito?
- Existem controlos específicos para prevenir o acesso indevido a chaves criptográficas?
- Existem procedimentos e políticas específicos para a gestão e acesso às chaves criptográficas?
- Estão implementados controlos de deteção multi-camada, abrangendo pessoas, processos e tecnologia, que permitam uma rápida deteção de ataque e isolamento de pontos infetados?
- Existem controlos de monitorização cobrindo todas as ligações externas?

Critérios INTERMÉDIOS – Questões de avaliação:

- Está implementada uma arquitetura de segurança de defesa em profundidade, baseada em diagramas de rede e de fluxos de informação, com identificação de componentes de *hardware*, *software* e de rede, ligações internas e externas e tipos de informação trocados entre sistemas?
- A infraestrutura de rede está segmentada, com políticas de segurança adequadas, que definem os acessos aos sistemas e aplicações?
- Os ambientes de TI e as funções de TI estão bem definidas, com diferentes níveis de segurança e de controlos implementados?
- Existem medidas implementadas para evitar a execução de código não autorizado nos equipamentos da instituição, na infraestrutura de rede e nos componentes dos sistemas?
- Existem mecanismos automáticos que ajudem a manter a informação sobre as configurações de segurança e dos sistemas atual, precisa e prontamente disponível?
- Estão implementados controlos técnicos que gerem notificações automáticas para quem apropriado, quando há alteração de permissões de acesso de utilizadores?

▪ Estão implementados mecanismos automáticos de suporte à gestão das contas de acesso aos sistemas de informação (p.e. desativação da conta após um determinado período de inatividade)? ▪ Estão implementados controlos de segurança que detetam e previnem intrusões oriundas de ligações a terceiros? ▪ Estão implementados procedimentos para isolar ou bloquear rapidamente ligações a terceiros, em caso de ciberataque?
Critérios AVANÇADOS – Questões de avaliação:
▪ A infraestrutura de rede está desenhada por forma a bloquear, ou pelo menos limitar, os efeitos de um ciberataque em ambiente produtivo, nomeadamente com a utilização de controlos automáticos e a possibilidade de automaticamente desligar ou isolar componentes afetadas? ▪ Estão implementadas técnicas de despiste de atacante, tipo '*honeypot*', que levem o atacante a concentrar-se nessas componentes, onde as suas atividades podem ser contidas e analisadas?

Tabela 15 - Critérios DSS05

DSS06 - Gerir Controles do Processo de Negócio
Critérios BASE – Questões de avaliação:
▪ Está implementado um conjunto de controlos de segurança apropriado aos objetivos de segurança necessários às funções de negócio, incluindo garantir a disponibilidade, integridade e confidencialidade dos sistemas de informação e dados, assim como a conformidade legal? ▪ Há controlos de segurança focados na segurança física e de pessoas? ▪ O acesso físico e lógico aos sistemas é restringido de acordo com o princípio de mínimo privilégio? ▪ Estão definidas políticas, procedimentos e controlos que definam os privilégios de acesso aos sistemas e como devem ser administrados?

- As contas de utilizador são definidas e geridas com base em esquemas de RBAC (*Role Based Access Control*), que relacionam os perfis de acesso com as funções?
- Existem processos definidos para a criação, modificação e eliminação de direitos de acessos de utilizadores?
- Existem procedimentos específicos para a alocação de privilégios de acesso numa base permanente ou evento a evento?
- Os administradores têm dois tipos de conta: uma para acessos gerais e outra para acessos de administração?
- A utilização de contas privilegiadas é monitorado e controlado?
- A utilização de contas genéricas, não nominais, é muito limitada e monitorada?
- Existe uma política de definição de *passwords* que especifique características como complexidade, período de renovação, limite de tentativas erradas de acesso?
- Existem ações de segurança definidas para as fases do ciclo de vida do emprego: seleção, desenvolvimento e saída de colaboradores?
- No processo de seleção de novos colaboradores, são realizadas verificações de perfil de segurança, tendo em conta as responsabilidades futuras na organização?
- Quando um colaborador muda de funções, há um processo prévio de atualização atempada de direitos de acesso aos sistemas?
- Quando um colaborador cessa funções, há um processo de revogar de imediato os acessos desse utilizador aos sistemas?
- Existem políticas, procedimentos e controlos para dar ou revogar acessos lógicos e físicos aos sistemas, baseados nas responsabilidades, princípios de privilégio mínimo e segregação de funções?
- Existem capacidades, incluindo pessoas, processos e tecnologia, para monitorizar a atividade de utilizadores com acessos privilegiados e acessos a sistemas críticos?
- Os *backups* são protegidos para garantir a confidencialidade, integridade e disponibilidade dos dados?
- Os *backups* são testados regularmente para verificar a sua disponibilidade e integridade?
- Os *backups* de informação são testados periodicamente?

Critérios INTERMÉDIOS – Questões de avaliação:
▪ É efetuada encriptação dos dados, com base em classificação dos dados e análise de risco? ▪ Há mecanismos automáticos de notificação de alteração do estado de empregabilidade de determinado colaborador, para que quem de direito atualize os acessos desse colaborador aos sistemas? ▪ Existem mecanismos automáticos de atribuição ou retirada de privilégios de acesso, perante alterações de funções de determinado colaborador? ▪ São realizadas cópias de *backups* para localização alternativa, afastada do sistema operacional? ▪ Estão implementados mecanismos de recuperação de transações (para sistemas baseados em transações), que incluam *rollback* e *logging* de transações?
Critérios AVANÇADOS – Questões de avaliação:
▪ São utilizadas ferramentas de IAM (*Identity and Access Management*) e GRC, de forma integrada, garantindo que todos os sistemas atualizam de forma consistente? ▪ É usado um paradigma ABAC (*Access Based Access Control*) para contextualmente e de forma dinâmica, gerir os acessos aos ambientes dos Sistemas de Informação? ▪ São utilizados mecanismos automáticos para continuamente auditar e monitorar a criação, modificação, ativação, desativação e remoção de contas? ▪ Existem sistemas de monitorização e análise comportamental de colaboradores (equipamentos utilizados, localização, horários), que permitam alertar para alterações de padrão? ▪ Existe um sistema secundário redundante, em localização distinta do primário, e que pode ser ativado sem perca de informações e sem disrupção de operações? ▪ Está considerada a possibilidade de acordos de partilha de dados com terceiras partes, para apoio aos processos de recuperação?

Tabela 16 - Critérios DSS06

MEA01 - Monitorar, Avaliar e Analisar Desempenho e Conformidade

Critérios BASE – Questões de avaliação:
▪ É feita uma análise periódica à eficácia dos controlos de segurança implementados, por forma a adaptá-los ao atual ambiente de ameaças? ▪ Existe um programa de testes como parte integral do modelo de ciber-resiliência? ▪ Estão desenvolvidas as capacidades necessárias à realização de testes e são envolvidas linhas de negócio e unidades operacionais na implementação dos mesmos? ▪ Há testes realizados por entidades independentes, internas ou externas? ▪ São testados, pelo menos anualmente, planos de recuperação de sistemas críticos, aplicações e dados? ▪ São realizados testes de vulnerabilidades para os sistemas expostos externamente e para os sistemas internos e redes numa base regular? ▪ São realizadas análises de vulnerabilidades antes da entrada em produção de serviços novos/alterados que suportem funções críticas? ▪ São periodicamente realizadas análises de vulnerabilidades sobre os serviços em produção, aplicações e componentes de infraestrutura? ▪ São realizados, pelo menos anualmente, testes de penetração sobre os serviços expostos externamente e os sistemas internos e as redes? ▪ Nos testes de penetração são, de algum modo, envolvidos os *system owners*, equipas de continuidade de negócio e equipas de resposta a crises e incidentes? ▪ São produzidos indicadores e informação de gestão para medir e monitorizar a eficácia da implementação da estratégia e modelo de ciber-resiliência numa base regular e a sua evolução ao longo do tempo?
Critérios INTERMÉDIOS – Questões de avaliação:
▪ O Conselho de Administração revê e aprova as decisões de alocação de recursos e de priorização, com base nas análises de cibersegurança, cruzando com os KPI e a sua evolução face ao pretendido? ▪ Estão definidos, pela gestão de topo, KPI e KRI e outros parâmetros de análise, para monitorização, medição, e reporte das ciberatividades? ▪ No âmbito da gestão de risco da organização, está prevista a realização de testes práticos?

▪ Estão adotadas as melhores práticas e ferramentas automatizadas para suportar os processos e procedimentos em vigor, no sentido de corrigir falhas técnicas e organizacionais identificadas durante a realização de testes? ▪ São realizados testes em todas as fases do SDLC e aos níveis de negócio, aplicação e tecnologia? ▪ São realizados testes de vulnerabilidades de forma contínua e rodando entre ambientes? ▪ Estão desenvolvidos e são realizados testes de penetração que simulem técnicas realísticas de ataque a sistemas, redes, aplicações e procedimentos? ▪ São ativamente monitorados desenvolvimentos tecnológicos e mantida atenção sobre novos processos de gestão de ciber-riscos que possam combater novas e existentes formas de ciberataques?
Critérios AVANÇADOS – Questões de avaliação:
▪ Estão desenvolvidas, monitorizadas e analisadas métricas para avaliar a performance e eficiência dos programas de testes?

Tabela 17 - Critérios MEA01

MEA02 - Monitorar, Avaliar e Analisar o Sistema de Controlo Interno
Critérios BASE – Questões de avaliação:
▪ São realizados regularmente relatórios escritos para o Conselho de Administração sobre o estado geral do programa de ciber-resiliência e os riscos e eventos chave? ▪ São apresentados ao Conselho de Administração os planos de orçamento e de atividades de cibersegurança em curso e para as necessidades futuras? ▪ É adotada uma abordagem baseada em risco no desenvolvimento dos programas de teste? ▪ Estão desenvolvidas políticas e procedimentos de priorização e remediação de situações identificadas pelos testes? ▪ São testados os planos de resposta e recuperação, pelo menos anualmente, incluindo a governança e coordenação e comunicações de crise?

- Está desenvolvido e documentado e atualizado regularmente um processo de gestão de vulnerabilidades que permita classificar, priorizar e remediar potenciais falhas identificadas?
- O processo de gestão de vulnerabilidades suporta a identificação de qualquer tipo de fraqueza explorável (técnica, processual, organizacional e emergente) nas funções críticas, nos processos de suporte e nos ativos lógicos e físicos onde residem?
- São realizados testes baseados em diferentes cenários, incluindo cenários extremos mas plausíveis, para avaliar e melhorar as capacidades de deteção de incidentes, assim como resposta e recuperação?
- O Conselho de Administração e a gestão de topo são envolvidos nos testes baseados em cenários?
- Os testes incluem situações simuladas de engenharia social e *phishing*?
- É testada a adequabilidade das capacidades internas e dos processos e procedimentos para responder a cenários não convencionais?
- Existem capacidades de recolha e análise de informações sobre vulnerabilidades, ciberameaças e cibereventos, quer de origem interna, quer externa?
- É feita uma identificação e classificação (estratégicas, táticas e operacionais) das lições aprendidas e as mesmas são incorporadas nos processos da organização e são partilhadas com as entidades externas relevantes?

Critérios INTERMÉDIOS – Questões de avaliação:

- É aferido, de forma regular, a compreensão e conhecimentos que os membros do Conselho de Administração e a gestão de topo têm dos seus papéis e responsabilidades, no que concerne à ciber-resiliência, incluindo o seu conhecimento dos ciber-riscos?
- É assegurado pelo Conselho de Administração que são regularmente realizadas análises de ciber-resiliencia, que permitam avaliar o nível de maturidade de cibersegurança da organização?
- São realizadas avaliações à eficácia das formações, no sentido de aferir se as mesmas influenciam comportamentos, melhoram a conformidade com as políticas de segurança e os processos de reporte de incidentes?

▪ Os testes de planos de resposta e recuperação incluem cenários de ataque contemplando destruição de dados, corrupção de dados, perca de dados e falhas de disponibilidade dos sistemas e informação? ▪ São conduzidos exercícios de *red teaming*, usando informações úteis e fiáveis de CTI, baseados em cenários de ameaças específicos e plausíveis? ▪ É validada a eficácia de incorporar lições aprendidas nos programas de formação e sensibilização, numa base regular? ▪ São analisadas e correlacionadas as informações provenientes de auditorias, incidentes, quase falhas, testes, exercícios e CTI interna e externa? ▪ É acompanhado e avaliado continuamente o progresso no desenvolvimento das capacidades de ciber-resiliência, utilizando um modelo de maturidade?
Critérios AVANÇADOS – Questões de avaliação:
▪ A gestão de topo realiza regularmente análises comparativas com outras entidades equivalentes do setor, no sentido de identificar falhas ao nível da governança, capacidades, recursos e ferramentas? ▪ Está considerada a implementação de um programa *Bug Bounty*, como parte do processo de gestão de vulnerabilidades? ▪ São elaborados cenários de incidentes de cibersegurança, em conjunto com outras entidades do setor, no sentido de testar o risco de contágio? ▪ Está desenvolvida internamente a capacidade de *red team*, com as metodologias, ferramentas sofisticadas e pessoas com capacidades apropriadas? ▪ São utilizadas e correlacionadas várias fontes de informação, como análise de logs, alertas, fluxos de tráfego, cibereventos ocorridos neste e noutros setores e eventos geopolíticos, para prever tendências e futuros ciberincidentes e tomar medidas proactivas de proteção?

Tabela 18 - Critérios MEA02

MEA03 - Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos
Critérios BASE – Questões de avaliação:

Não identificado
Critérios INTERMÉDIOS – Questões de avaliação:
Não identificado
Critérios AVANÇADOS – Questões de avaliação:
▪ Nas reuniões regulares do Conselho de Administração, são apresentadas análises de cibereventos e ciberincidentes, para além de tendências de CTI para o setor? ▪ A gestão tem criadas parcerias com associações do setor e empresas de cibersegurança para o desenvolvimento de soluções úteis para o setor? ▪ São regularmente realizados testes de cibersegurança em colaboração com outras entidades do setor? ▪ São realizados testes setoriais que permitam avaliar os planos de comunicação e protocolos de cooperação e coordenação no setor? ▪ São promovidos e a organização participa em exercícios de cibertestes cross setoriais? ▪ São testados, pelo menos anualmente, os acordos de cooperação em vigor com entidades externas relevantes?

Tabela 19 - Critérios MEA03

7. Forma de Implementação

Perspetivou-se também a utilização do *COBIT 5*, como base de implementação do projeto. Nesse sentido, utiliza-se como modelo o desenvolvimento do ISACA (2012c), *COBIT 5 for implementation*.

O objetivo é estabelecer uma abordagem sustentável à governança e gestão da cibersegurança. O projeto é dado como concluído quando se percecionem benefícios mensuráveis e os processos de cibersegurança estejam embebidos de forma natural na atividade em curso.

O modelo de implementação do *COBIT 5* baseia-se num princípio de ciclo de vida de projeto, de melhoria contínua, adaptado à organização em concreto. Significa isto, portanto, que as iniciativas a desenvolver para a implementação de cibersegurança, diferirão de organização para organização e o contexto próprio tem que ser entendido e devidamente considerado. O ciclo de vida de implementação permite às organizações lidarem com a complexidade e os desafios que tipicamente se encontram durante a implementação, ajustando permanentemente o rumo.

Enquadrado na implementação do *COBIT 5*, estão previstas 7 fases do ciclo de vida. São elas:

1) Reconhecimento da necessidade do projeto;
2) Avaliar o estado atual;
3) Definir o objetivo a alcançar;
4) Definir as atividades de melhoria a aplicar;
5) Implementar as melhorias;
6) Operar e retirar indicadores;
7) Monitorar e avaliar.

A Figura 6 representa esse modelo de implementação.

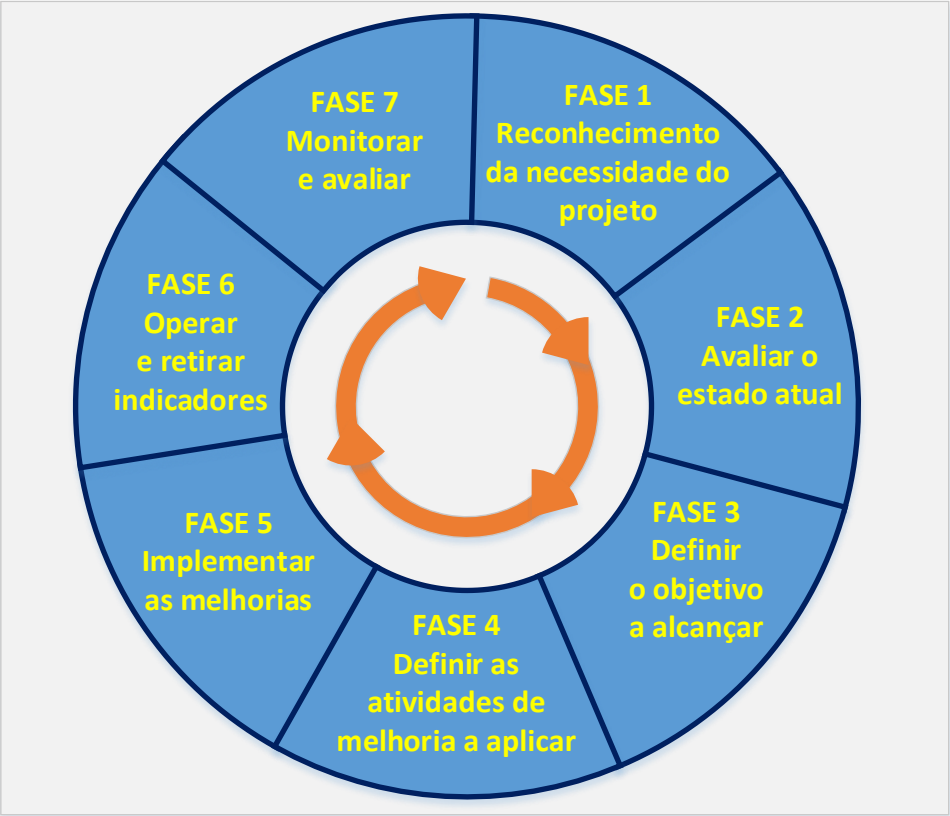

Figura 6 – As 7 fases do ciclo de vida de implementação (adaptado de ISACA, 2012c)

No âmbito do trabalho, o objetivo passa por apresentar e delinear todo o processo, chamando a atenção para os aspetos mais críticos de implementação, em cada etapa do ciclo. De qualquer modo, tratando-se de uma abordagem de melhoria contínua, a implementação segue uma lógica de ajustes permanentes, pelo que haverá sempre condicionalismos e situações não antecipáveis. No entanto, dadas as limitações temporais que este trabalho tem, não é viável, no decurso da realização do mesmo, a concretização prática de todo o ciclo de implementação. Assim, o foco será colocado nas 3 primeiras etapas. Relativamente às restantes fases, as mesmas serão aqui abordadas, mas de uma forma mais superficial e condicionada e a sua realização será deixada para altura posterior, a definir.

Nas secções seguintes são descritas estas fases de implementação.

7.1. Preparação do ambiente organizacional

Numa primeira fase, importa entender o contexto particular em que a organização se situa para, com isso, criar um ambiente propício ao acolhimento e desenvolvimento das atividades preconizadas. Dentro dessa análise deverão ser identificadas questões como:

- A ética e cultura da própria organização, no que se refere à segurança de informação;
- Políticas e práticas existentes; modelos e guias de boas práticas adotados;
- Práticas do setor;
- Nível de maturidade em vetores relacionados com segurança de informação;
- Capacidades e recursos disponíveis;
- Contratos aplicáveis;
- Leis, regulamentos e políticas aplicáveis.

Deverão igualmente estar identificados requisitos próprios da organização no que se refere a opções de governança e gestão, que incluem:

- As intenções associadas ao plano de negócio e estratégia da organização;
- O estilo de gestão;
- O perfil de risco associado à informação;
- O apetite para o risco.

Para o sucesso da implementação, é fundamental que as iniciativas tenham um suporte adequado quer ao nível da governança, quer ao nível da gestão. É fundamental existir um suporte visível por parte da gestão de topo, que promova um compromisso com o programa de cibersegurança, a todos os níveis. O compromisso para com a cibersegurança por parte dos decisores mais relevantes deve existir desde o primeiro momento. Para se conseguir isso, os objetivos e benefícios precisam de estar claramente expressos em termos de negócio e sumarizados num plano de negócio ou equivalente. Uma vez criado o compromisso, é fundamental que sejam alocados os recursos adequados e que sejam definidos e assignados os papéis e responsabilidades chave para o projeto. Devem ser criadas e mantidas estruturas e processos que suportem o alinhamento contínuo com a estratégia de segurança.

Por outro lado, a identificação de situações concretas, vividas ou conhecidas, poderá servir de impulsionador à evidência de necessidade de investimento em cibersegurança. Neste aspeto, podem-se apontar algumas situações exemplificativas, como sejam:

- Incidentes de segurança ocorridos na organização ou no setor, tais como: fuga de dados causada por acessos indevidos à informação; ciberataques de negação de serviço; modificação não autorizada de informação crítica;
- Falhas legais, regulatórias ou contratuais relativamente a regras de privacidade;
- Recomendações de auditoria relacionadas com fracas capacidades de cibersegurança.

Adicionalmente, outros eventos ocorridos na envolvente, podem assinalar ou desencadear um foco sobre a gestão e governança de cibersegurança. Tem-se como exemplo:

- Novos quadros regulatórios, de conformidade ou contratuais;
- Alterações significativas da tecnologia ou mudanças de paradigma;
- Avaliações externas de consultores ou de auditoria;
- Fusões, aquisições ou outras alterações profundas da organização.

Estando criadas as condições propícias à mudança, o sucesso dependerá da gestão da mudança ser efetuada de forma efetiva. Para se promover uma gestão de mudança adequada, devem ser tidos em atenção quer os aspetos tecnológicos, quer os aspetos humanos, de comportamento e culturais, assim como os motivacionais. Influenciar o comportamento através de uma comunicação eficaz, identificando claramente os incentivos e recompensas relevantes e promover a adesão à mudança são fatores chave a ter em consideração. Isto é, de qualquer modo, algo que requer tempo e paciência.

Na prática, no caso concreto das instituições financeiras, pode-se afirmar que o alcançar desta fase estará facilitado. Há hoje em dia um sentimento crescente da importância da cibersegurança nas organizações do setor, e uma sensibilização da gestão de topo para a necessidade de estruturar a organização da melhor forma para lidar com os riscos que as ciber-ameaças emergentes representam.

7.2. Avaliação do estado atual

Para o arranque dum programa contínuo de implementação de segurança de informação na organização, há duas questões chave a que importa dar resposta:

- Qual o estado atual?
- Qual o estado pretendido?

A resposta a ambas implica identificar claramente quais os parâmetros em que fazer essa análise. Ou seja, quais são os aspetos relevantes que importa identificar?

Nessa medida, é necessário construir um modelo de referência, que represente aquilo que será o ideal de organização relativamente a cibersegurança. Foi o que foi feito e apresentado no Capítulo 7. Com isso, dispõe-se agora do conjunto de questões a formular, que servem de base à análise e avaliação pretendida, do estado atual de maturidade da organização.

Procurou-se que as questões fossem eminentemente colocadas de uma forma objetiva, como meio de garantir que a análise reflete a realidade existente, independentemente do interlocutor que responda às questões colocadas. No entanto, é impossível retirar por completo o caráter de subjetividade que as respostas sempre terão, quanto mais não seja, devido a diferentes interpretações que sejam feitas do que está a ser questionado.

Assim, no sentido de se obter o máximo de alinhamento com a realidade, perspetiva-se que o questionário seja procedido de entrevistas com interlocutores da organização, com responsabilidades a vários níveis de gestão, com quem seja possível esclarecer as respostas dadas e assim aferir do correto entendimento tido quanto ao que estava a ser questionado.

7.3. Identificação de lacunas

A resposta à questão de onde a organização quer estar em termos de maturidade de cibersegurança, não é evidente. Diferentes intervenientes estabelecerão naturalmente diferentes objetivos, em função dos critérios e abordagem que utilizem, assim como das responsabilidades que desempenhem na cibersegurança da organização. É fácil obviamente dizer-se que se pretende estar no topo da segurança, mas tal tem que ser analisado numa perspetiva de risco e de disponibilização de recursos.

De qualquer modo, estando este trabalho a ser iniciado, não existindo ainda uma referência de maturidade para a organização e estando o processo ainda na sua primeira iteração dum ciclo de melhoria contínua, entende-se como adequado que, na primeira iteração do modelo, se estabeleça como meta o cumprimento dos critérios Base identificados e, nessa medida, a identificação de lacunas se estabeleça pela diferença do que existe e se identifica para aquilo que se considera uma maturidade base.

À medida que o processo de melhoria contínua segue as suas interações, haverá um momento em que a organização se identificará como capaz de subir um patamar de maturidade e assim adaptar-se aos novos critérios, mais exigentes. Essa decisão terá sempre que ser assumida pela gestão de topo e suportada pelo Conselho de Administração.

7.4. Plano de ação

A definição do plano de ação decorrerá naturalmente da identificação das lacunas realizada na fase anterior. Haverá, nessa medida, que estabelecer uma priorização de atividades, uma identificação dos recursos humanos e materiais necessários à sua concretização e uma aprovação superior quanto à utilização desses recursos.

7.5. Execução do plano

No âmbito da execução, há que optar e balancear entre o desenvolvimento à medida com a aquisição de soluções mais normalizadas.
Há igualmente que deixar espaço para testes e afinação das soluções.
O planeamento meticuloso de atividades é nesta fase de importância capital, por forma a não comprometer o funcionamento correto das soluções.

7.6. Operação e recolha de indicadores

Nesta fase, é importante deixar os processos decorrerem naturalmente, mas sob uma apertada vigilância que permita a recolha de um máximo de indicadores com vista a uma aferição o mais correta possível do nível de eficiência atingido.
A comunicação de todos os resultados, quer positivos, quer negativos, é fundamental num processo de melhoria contínua, como o preconizado.

7.7. Análise de indicadores e avaliação do nível de sucesso

Nesta fase, são analisados os resultados obtidos e confrontados com a expetativa e objetivos preconizados. São também identificadas as lições aprendidas.
Em função dos resultados, pode-se decidir pela conclusão formal do processo, ou pela continuidade, com a identificação de novos objetivos, decorrentes de um desejo de mudança, que leva novamente à etapa 1 do processo de implementação.

8. Conclusões

8.1. Trabalho realizado

Considera-se que o principal produto resultante deste trabalho é o modelo de avaliação do estado de maturidade de cibersegurança, aplicável ao contexto particular do Banco Central e, dum modo genérico, a qualquer entidade do setor financeiro da área do eurosistema. Concretamente, conseguiu-se efetuar uma integração dos principais determinantes associados à gestão da cibersegurança no setor financeiro, identificados por modelos, guias e recomendações elaborados pelos principais autores mundiais nesta área.

Neste aspeto, refira-se que se identificou que já havia sido realizado um cruzamento dos processos do *COBIT 5* com a *framework NIST*, efetuado pelo *ISACA*, mas não se identificou, pela revisão de literatura efetuada, a existência de um cruzamento especificamente focado no setor financeiro, integrando requisitos específicos desse setor, como foi realizado neste trabalho, nomeadamente com a inclusão do *CROE* e dos aspetos normativos e legais associados às Diretivas *NIS* e RGPD, da União Europeia.

Tal resultou num conjunto de questões que estão associadas aos vários processos da organização (apresentadas no capítulo 6) e as quais, uma vez que sejam corretamente respondidas, permitirão avaliar do estado de maturidade do Banco Central.

Por outro lado, identificou-se também neste trabalho um modelo de implementação do projeto, que integra de forma natural o modelo de avaliação de maturidade atrás referido e que permitirá ao Banco Central progredir iterativamente no sentido duma gestão de cibersegurança cada vez mais eficaz e eficiente.

Como principal limitação do trabalho, aponta-se a impossibilidade de concretização prática de um ciclo completo de implementação do modelo a que se chegou, até à conclusão deste documento. A implementação prática de um projeto dessa envergadura demorará consideravelmente mais que um ano, e não era viável realizá-lo nos prazos determinados para a elaboração deste documento.

De qualquer modo, com o trabalho realizado, designadamente i) a definição do processo de implementação de ciclo de vida de melhoria contínua, como preconizado no capítulo 7; e ii) sobretudo, a definição do modelo de avaliação do estado de maturidade de cibersegurança em organizações financeiras, apresentado no capítulo 6; entende-se ter contribuído de forma muito relevante para a resposta à questão chave que deu origem a este trabalho: *Face ao problema*

das ameaças que pendem sobre os ativos de informação, qual o modelo de gestão de cibersegurança, a aplicar no Banco Central, que melhor responde aos desafios que se colocam no contexto atual?.

8.2. Trabalho futuro

Como etapas futuras decorrentes deste trabalho identifica-se:

- Em primeiro lugar, quando exista disponibilidade temporal e de recursos humanos e materiais, se passe à concretização prática de todas as etapas previstas para o processo de implementação, que incluem a execução do plano de ação, a recolha de indicadores e a avaliação do nível de sucesso da implementação. Efetivamente, só com a conclusão dessas etapas se poderá de forma mais clara avaliar da qualidade e relevância deste trabalho.
- Uma atividade de mapeamento dos requisitos de avaliação do nível de maturidade de cibersegurança com um modelo de avaliação de risco, que permita valorizar o risco associado ao não cumprimento de cada um dos critérios identificados.
- Seria interessante poder comparar este modelo de gestão de cibersegurança, focado no setor financeiro, com outros modelos que também estejam centrados nas particularidades desse setor e, a partir daí, avaliar as vantagens que cada modelo pode aportar e, eventualmente, integrar as mais valias de cada um num modelo posterior.

9. Referências bibliográficas

Accenture; Cost of cyber crime study 2017, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf, publicado em 26 de setembro de 2017

Adams, M. 2017. Big data and individual privacy in the age of the internet of things. ***Technology Innovation Management Review***, 7 (4): 12-24.

Ahmed, A.; Using COBIT to manage the benefits, risks and security of outsourcing cloud computing (2011). http://www.isaca.org/Knowledge-Center/Documents/Using-COBIT-to-Manage-the-Benefits-Risks-and-Security-of-Outsourcing-Cloud-Computing.pdf, consultado em 31 de outubro de 2017

Aleem, A., & Antwi-Boasiako, A. 2011. Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat. ***International Journal of Law, Crime and Justice***, 39(3): 140-160.

Aleem, A., & Sprott, C. 2013. Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. ***Journal of Financial Crime***, 20(1): 6-24.

Aleem, A., Wakefield, A., & Button, M. 2013. Addressing the weakest link: Implementing converged security. ***Security Journal***, 26(3): 236–248.

Allen, J., Gabbard, D., & May, C. 2003. ***Outsourcing managed security services***. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Anderson, R. 2001. Why information security is hard: An economic perspective. In ***Proceedings of the 17th Annual Computer Security Applications Conference:*** 358-365. Washington, DC: IEEE Computer Society.

Angst, C., Block, E., D'Arcy, J., & Kelley, K. 2017. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. ***MIS Quarterly***, 41(3): 893-916.

Bainbridge, S. 2008. ***The new corporate governance in theory and practice***. Oxford: Oxford University Press.

BCE. 2018. ***Cyber resilience oversight expectations (CROE) for financial market infrastructures***. Frankfurt: BCE.

BCE; Cybersecurity for the financial sector, https://www.ecb.europa.eu/paym/pol/shared/pdf/qa_cybersecurity.pdf, publicado em outubro de 2016

Bensaou, M., & Earl, M. 1998. The right mind-set for managing information technology. ***Harvard Business Review***, 76(5): 118-128.

Berghel, H. 2005. The two sides of ROI: return on investment vs. risk of incarceration. ***Communications of the ACM***, 48(4): 15-20.

Berman, J. 2013. ***Principles of big data: Preparing, sharing, and analyzing complex information***. Waltham, MA: Morgan Kaufmann, Elsevier.

Bernard, P. 2012. ***COBIT 5 - A Management Guide***. Reading: Van Haren Publishing.

BIS. 2016. ***Guidance on cyber resilience for financial market infrastructures***. Basileia: BIS.

Bodin, D., Gordon, A., & Loeb, P. 2005. Evaluating information security investments using the hierarchy. ***Communications of the ACM***, 48(2): 79-83.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., & Boss, R. 2009. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. ***European Journal of Information Systems***, 18(2): 151–164.

Cater-Steel, A., Tan, W.G., & Toleman, M. 2006. Challenge of adopting multiple process improvement frameworks. In J. Ljungberg & M. Andersson (Eds.), ***Proceedings of the 14th European conference on information systems***. Gothenburg: Association for Information Systems.

Chen, M., Mao, S., Zhang, Y., & Leung, V.C. 2014. ***Big Data: Related Technologies, Challenges and Future Prospects***. London: Springer.

CNSS. 2015. ***Committee on National Security Systems Glossary***. Ft Meade, MD: CNSS.

Comissão Europeia; Resilience, deterrence and defence: Building strong cybersecurity in europe, http://ec.europa.eu/newsroom/document.cfm?doc_id=46998, publicado em 19 de setembro de 2017

Culnan, M., & Williams, C. 2009. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. ***MIS Quarterly***, 33(4): 673-687.

Da Veiga, A., & Eloff, J. 2010. A framework and assessment instrument for information security culture. ***Computers & Security***, 29(2): 196-207.

Davenport, T. H., & Beck, J. C. 2001. ***The attention economy: Understanding the new currency of business***. Boston, MA: Harvard Business School Press.

Davenport, T. & Harris, J. 2007. ***Competing on analytics; The new science of winning.*** Boston, MA: Harvard Business School Press.

Davis, S. & Botkin J. 1994. The coming of knowledge-based business. ***Harvard Business Review***, 72 (5): 165-170.

Dittmeier, C. 2011. ***Internal auditing - Chiave per la corporate governance***. Milan: EGEA.

Dzazali, S., Zolait, A. 2012. Assessment of information security maturity: An exploration study of Malaysian public service organizations. ***Journal of Systems and Information Technology***, 14 (1): 23-57.

ENISA. 2017. ***Overview of cybersecurity and related terminology***. Heraklion: ENISA.

Feld, C. S., & Stoddard, D. B. 2004. Fixing the Corporation-IT disconnect. ***Harvard Business Review***, 82(2).

Fenz, S., Plieschnegger, S., & Hobel, H. 2016. Mapping information security standard ISO 27002 to an ontological structure. ***Information & Computer Security***, 24(5): 452-473.

Foth, M. 2016. Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. ***European Journal of Information Systems***, 25(2): 91–109.

Furnell, S. 2007. An assessment of website password practices. ***Computers & Security***, 26(7.8): 445-451.

Gomes, E., Barnes, B., & Mahmood, T. 2016. A 22 year review of strategic alliance research in the leading management journals. ***International Business Review***, 25(1): 15-27.

Goodman, S. & Ramer, R. 2007. Global sourcing of IT services and information security: Prudence before playing. ***Communications of the Association for Information Systems***: 20(50): 812-823.

Gordon, A., Loeb, P., Lucyshyn, W., & Richardson, R. 2005 CSI/FBI computer crime and security survey. http://safbd.ru/sites/default/files/2005csi.doc, consultado em 31 de outubro de 2017

Gupta, A., & Zhdanov, D. 2012. Growth and sustainability of managed security services networks: an economic perspective. ***MIS Quarterly***, 36(4): 1109-1130.

Haes, S. D., & Grembergen, W. V. 2008. Analysing the relationship between IT governance and business/IT alignment maturity. ***Proceedings of the 41st Annual Hawaii International Conference on System Sciences***: 428-428. Washington, DC: IEEE Computer Society.

Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. ***Information Security technical report***, 11(1): 55-61.

Hasan, C. 2010. Making sound security investment decisions. ***Journal of Information Privacy & Security***, 6(1): 53-71.

Haufe, K., Colomo, R., Dzombeta, S., Brandis, K., & Stantchev V. 2016. A process framework for information security management. ***International Journal of information Systems and Project Management***, 4(4): 27-47.

Hsu, J., Shih, S., Hung, Y., & Lowry P. 2015. The role of extra-role behaviors and social controls in information security policy effectiveness. ***Information Systems Research***, 26(2): 282-300.

IBM; IBM X-Force Threat Intelligence Index 2017, https://www.leadersinsecurity.org/component/phocadownload/category/11-2017-cybersecurity-publications.html?download=185:2017-cybersecurity-publications, publicado em março de 2017.

Ifinedo, P. 2014. The effects of national culture on the assessment of information security threats and controls in financial services industry. ***International Journal of Electronic Business Management***, 12 (2): 75-89.

Ilvonen, I. 2011. Information security culture or information safety culture - What do words convey?. ***Proceedings of the 10th European Conference on Information Warfare and Security:*** 148-154. Reading: Academic Conferences International Limited.

ISACA. 2012a. ***COBIT 5 – A business framework for the governance and management of enterprise IT***. Rolling Meadows, IL: ISACA.

ISACA. 2012b. ***COBIT 5 for information security***. Rolling Meadows, IL: ISACA.

ISACA. 2012c. ***COBIT 5 implementation***. Rolling Meadows, IL: ISACA.

ISACA. 2016. ***Cybersecurity Fundamentals Glossary***. Rolling Meadows, IL: ISACA.

Karlsson, F., Astrom, J., & Karlsson, M. 2015. Information security culture –state-of-the-art review between 2000 and 2013. ***Information & Computer Security***, 23(3): 246-285.

Karlsson, F., Kolkowska, E., & Prenkert, F. 2016. Inter-organisational information security: a systematic literature review. ***Information & Computer Security***, 24(5): 418-451.

Kolkowska, E. 2011. Security subcultures in an organization – Exploring value conflicts. ***Proceedings of the 19th European conference on information systems***: 237. Helsinki: Association for Information Systems.

Kunz, R., Lavenex, S., & Panizzon, M. 2011. ***Multilayered migration governance. The promise of partnership***. London: Routledge.

Kwon, J., Johnson, M. 2014. Proactive versus reactive security investments in the healthcare sector. ***MIS Quarterly***, 38(2): 451-471.

Liberti, L. 2008. Survey results: Reduce the cost of compliance while strengthening security. ***Security Management Newsletter***. Alexandria, VA: ASIS International.

Marrone, M., Hoffmann, L. & Kolbe, L. 2010. IT executives' perception of COBIT: Satisfaction, business-IT alignment and benefits. ***Proceedings of the 16th Americas conference on information systems***: 216. Lima: Association for Information Systems.

Masli, A., Richardson, V., Watson, M., & Zmud R. 2016. Senior executives' IT management responsibilities: Serious IT-related deficiencies and CEO/CFO turnover. ***MIS Quarterly***, 40(3): 687-708.

Mataracioglu, T. & Ozkan, S. 2011. Governing information security in conjuction with COBIT and ISO 27001. ***International Journal of Network Security & Its Applications***, 3(4): 1-5.

McAfee. 2014. Net losses – estimating the global cost of cybercrime. https://www.mcafee.com/us/about/news/2014/q2/20140609-01.aspx, acedido em 11 de dezembro de 2017.

Miltgen, C., & Guillard, D. 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. ***European Journal of Information Systems***, 23(2): 103–125.

Mishra, S. 2015. Organizational objectives for information security governance: a value focused assessment. ***Information & Computer Security***, 23(2): 122-144.

Mugavero, R., & Sabato, V. 2014. Analysis and estimation of expected cyber-attack scenarios and consequences. ***Journal of Information Privacy and Security***, 10(3): 138-152.

NIST. 2017. ***Framework for improving critical infrastructure cybersecurity***. Gaithersburg, MD: NIST.

Pereira, R., & Mira da Silva, M. 2012. Designing a new integrated IT governance and IT management framework based on both scientific and practitioner viewpoint. ***International Journal of Enterprise Information Systems***, 8(4): 1-43.

Porter, M., & Millar V. 1985. How information gives you competitive advantage. ***Harvard Business Review***, 85: 149-160.

PWC; Building relationships. Creating value. Global annual review 2010, https://www.pwc.ec/es/publicaciones/assets/pdf/global-annual-review-2010.pdf, publicado em julho de 2010

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. 2005. ***Insider threat study: Illicit cyber activity in the banking and finance sector***. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute.

Rowe, R., & Gallaher, P. 2006. Private sector cyber security investment strategies: An empirical analysis. ***Proceedings of the 5th Workshop on the Economics of Information Security.*** Cambridge: University of Cambridge.

Rubino, M., & Vitolla, F. 2014. Corporate governance and the information system: how a framework for IT governance supports ERM. ***Corporate Governance***, 14(3): 320-338.

Ryan, J., & Ryan, J. 2005. Proportional Hazards in Information Security. ***Risk Analysis***, 25(1): 141-149.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano J. 2017. Digital forensic analysis of cybercrimes: Best practices and methodologies**.** ***International Journal of Information Security and Privacy (IJISP)***, 11(2): 25-37.

Schlienger, T., & Teufel, S. 2002. Information security culture: The socio-cultural dimension in information security management. In Ghonaimy M.A., El-Hadidi M.T. & Aslan H.K. (Eds.), ***Security in the Information Society. IFIP Advances in Information and Communication Technology***, vol 86. Boston, MA: Springer.

Selig, G. 2016. IT governance - An integrated framework and roadmap: How to plan, deploy and sustain for improved effectiveness. ***Journal of International Technology and Information Management***, 25(1): 55-76.

Shen, L. 2014. The NIST cybersecurity framework: overview and potential impacts. ***Scitech Lawyer***, 10(4): 16-19.

Siponen, M., & Oinas-Kukkonen, H. 2007. A review of information security issues and respective research contributions. ***Data Base***, 38(1): 60-80.

Siponen, M., & Willison, R. 2009. Information security management standards: Problems and solutions. ***Information & Management***, 46(5): 267-270.

Stewart, A. 2012. Can spending on information security be justified? Evaluating the security spending decision from the perspective of a rational actor**.** ***Information Management & Computer Security***, 20(4): 312-326.

Sundt, C. 2006. Information security and the law. Information Security Technical Report, ***Computing-Information Security,*** 11(1): 2-9.

Symantec; State of information global results (2012), https://www.symantec.com/content/dam/symantec/docs/reports/2012-state-of-information-global-en.pdf, acedido em 11 de dezembro de 2017.

Teodoro, N., Gonçalves, L., & Serrão, C. 2015. NIST CyberSecurity Framework Compliance. ***IEEE Trustcom/BigDataSE/ISPA***, 402: 418-425.

Tomkins, C. 2001. Interdependencies, trust and information in relationships, alliances and networks. ***Accounting, Organizations and Society***, 26(2), 161-191.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. 2015. Managing the introduction of information security awareness programmes in organisations. ***European Journal of Information Systems***, 24(1): 38–58.

União Europeia; 2016a, Diretiva (UE) 2016/1148 do parlamento europeu e do conselho de 6 de julho de 2016, https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L1148&from=PT, publicado em 19 de julho de 2016.

União Europeia; 2016b, Diretiva (UE) 2016/680 do parlamento europeu e do conselho de 27 de abril de 2016, https://eur-lex.europa.eu/legal-

content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=PT, publicado em 4 de maio de 2016.

União Europeia; 2016c, Regulamento (UE) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016, https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt, publicado em 4 de maio de 2016.

Von Solms, B. 2000. Information Security - The Third Wave?. ***Computers and Security***, 19(7): 615-620.

Von Solms, B. 2006. Information Security - The Fourth Wave?. ***Computers and Security***, 25(3): 165-168.

Vroom, C., & Von Solms, R. 2004. Towards information security behavioural compliance. ***Computers and Security***, 23(3): 191-198.

Wang, J., Gupta, M., & Rao, H. 2015. Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. ***MIS Quarterly***, 39(1): 91-112.

Warkentin, M., Willison, R. 2009. Behavioral and policy issues in information systems security: The insider threat. ***European Journal of Information Systems***, 18(2): 101-105.

WEF; The Global Risks Report 2018, http://www3.weforum.org/docs/WEF_GRR18_Report.pdf, publicado em 17 de janeiro de 2018

Weill, P. 2004. Don't just lead, govern: how top-performing firms govern IT. ***MIS Quarterly Executive***, 3(1): 1-17.

Wessels, E. & Loggerenberg, J. 2006. ***IT governance: theory and practice***. Paper presented at the Conference on Information Technology in Tertiary Education, Pretoria, South Africa.

Woolf, K. 2010. Information matters: Government's strategy to build capability in managing its knowledge and information assets. ***Legal Information Management***, 10(1): 47–50.

10. ANEXOS

10.1. ANEXO A - Processos *COBIT 5*

Avaliar, Dirigir e Monitorar		**Descrição**	**Objetivos**
EDM01	Garantir a Definição e Manutenção do Modelo de Governança	Analisar e articular os requisitos de governança de TI, e implementar e manter estruturas de suporte adequadas, princípios, processos e práticas, com definição clara de responsabilidades e autoridade para alcançar a missão, metas e objetivos da organização.	Disponibilizar uma abordagem consistente, integrada e alinhada com a abordagem de governança da organização. Garantir que as decisões são tomadas em linha com a estratégia e objetivos da organização, que os processos são abordados de forma correta, que são cumpridas as normas legais e regulatórias e que são cumpridos os requisitos de governança relativos aos elementos do Conselho de Administração
EDM02	Garantir a obtenção de Benefícios	Otimizar a contribuição de valor para a organização, proveniente dos processos de negócio, serviços de TI e ativos, resultantes de investimentos efetuados, a custos aceitáveis	Assegurar a otimização de valor proveniente das iniciativas, serviços e ativos de TI; entrega de soluções e serviços eficientes do ponto de vista de custos; uma visão fiável e precisa dos custos e benefícios esperados, para que as necessidades de negócio sejam suportadas de forma eficiente
EDM03	Garantir a Otimização do Risco	Garantir que o apetite de risco e tolerância ao risco da organização são bem entendidos, articulados e comunicados e que o risco para a organização relacionado com a utilização de tecnologia é identificado e gerido	Garantir que o risco organizacional de TI não excede o apetite e a tolerância de risco, que o impacto do risco de TI é identificado e gerido e que as hipóteses de falhas de conformidade são minimizadas
EDM04	Garantir a Otimização de Recursos	Garantir que existem recursos suficientes (pessoas, processos e tecnologia) para suportar de forma eficaz os objetivos da organização, a custos otimizados	Garantir que as necessidades de recursos são satisfeitas de forma otimizada e os custos são otimizados
EDM05	Garantir a Transparência às partes interessadas	Garantir que as medidas e relatórios da organização relativamente a desempenho e reporte são transparentes, com as partes interessadas a aprovar os objetivos e métricas e as necessárias ações de remediação	Garantir que a comunicação às partes interessadas é efetiva e atempada e que a base de reporte é estabelecida por forma a melhorar o desempenho, identificar áreas de melhoria e confirmar o alinhamento com a estratégia empresarial

Tabela 20 – Processos *COBIT 5* – EDM (ISACA, 2012b)

Alinhar, Planear e Organizar		**Descrição**	**Objetivos**
APO01	Gerir a Estrutura de Gestão de TI	Clarificar e manter a missão e visão da governança de TI. Implementar e manter mecanismos e autoridades para a gestão de informação e o uso de TI na organização, suportando os objetivos de governança, em linha com os princípios e políticas orientadores	Disponibilizar uma abordagem de gestão consistente que permita que os requisitos de governança sejam alcançados, cobrindo os processos de gestão, as estruturas organizacionais, os papéis e responsabilidades, atividades fiáveis e repetitivas e as capacidades e competências
APO02	Gerir a Estratégia	Disponibilizar uma visão holística do negócio e do ambiente tecnológico, as direções futuras e as iniciativas necessárias para atingir o objetivo desejado. Gerir os componentes da arquitetura da organização, incluindo os serviços fornecidos externamente, e as respetivas capacidades, por forma a garantir uma resposta eficiente e fiável aos objetivos estratégicos	Alinhar os planos estratégicos de TI com os objetivos de negócio. Comunicar de forma clara os objetivos e métricas de forma a que sejam compreendidos por todos, com as opções estratégicas de TI identificadas, estruturadas e integradas com os planos de negócio.
APO03	Gerir Arquitetura da Organização	Estabelecer uma arquitetura comum, composta por processos de negócio, informação, dados, aplicações e níveis de arquitetura tecnológica, para alcançar de forma efetiva e eficiente as estratégias corporativa e de TI, através da criação de modelos chave e práticas que descrevam as arquiteturas base e pretendida. Definir requisitos de taxonomia, normativos, guias, procedimentos, modelos e ferramentas, e garantir a interligação destes elementos. Melhorar o alinhamento, aumentar a agilidade, melhorar a qualidade de informação e gerar poupanças potenciais através de iniciativas como de reutilização de componentes constitutivas.	Representar os diferentes blocos construtores que compõem a organização e as suas inter-relações, assim como os princípios que guiam o seu desenho e evolução ao longo do tempo, permitindo uma entrega uniforme, responsiva e eficiente dos objetivos estratégicos e operacionais.
APO04	Gerir Inovação	Manter atualização sobre as tendências de TI e serviços relacionados, identificar oportunidades de inovação e planear como beneficiar da inovação relativamente a necessidades de negócio.	Alcançar vantagens competitivas, inovação de negócio e melhorar a eficácia e eficiência operacional através de desenvolvimentos em TI

		Analisar que oportunidades para melhorias ou inovação de negócio podem ser criadas através das tecnologias emergentes, inovação de negócio, assim como através de tecnologia existente e inovação de processos. Influenciar o planeamento estratégico e as decisões de arquitetura estratégicas.	
APO05	Gerir Portfólio	Executar o conjunto de diretivas estratégicas relativas a investimento, em linha com a visão de arquitetura da organização e as características desejáveis de investimento e o portfólio de serviços associado, considerando as diferentes categorias de investimento e os constrangimentos de recursos disponíveis. Avaliar, priorizar e gerir programa e serviços, gerindo a procura com os recursos disponíveis, com base no alinhamento com os objetivos estratégicos, o valor da organização e o risco. Deslocar os programas selecionados para o portfólio de serviços ativos para execução. Monitorar o desempenho do portfólio de programas e serviços, propondo os ajustamentos necessários em resposta ao desempenho dos programas e serviços ou alteração de prioridades da organização.	Otimizar o desempenho do portfólio de programas, em resposta ao desempenho dos programas e serviços e à alteração da procura e prioridades da organização.
APO06	Gerir Orçamento e Custos	Gerir as atividades financeiras relacionadas com TI, quer de negócio, quer de funções TI, cobrindo o orçamento, a gestão de custos e benefícios e a priorização de gastos através da utilização de práticas formais de dispêndios e um sistema justo e equitativo de alocação de custos na organização. Consultar as partes interessadas no sentido de identificar e controlar o total de custos e	Promover acordos entre as partes interessadas da organização e as TI, como forma de possibilitar uma eficaz e eficiente utilização dos recursos de TI e aportar transparência e prestação de contas sobre os custos e valor de negócio das soluções e serviços Permitir que a organização tome decisões informadas sobre a utilização de soluções e serviços de TI.

		benefícios no contexto dos planos táticos e da estratégia de TI, e iniciar ações corretivas onde for necessário.	
APO07	Gerir Recursos Humanos	Disponibilizar uma abordagem estruturada para garantir uma otimização da estrutura, colocação, direitos de decisão e capacidades dos recursos humanos. Tal inclui a comunicação dos papéis e responsabilidades definidos, planos de formação e crescimento, e expetativas de desempenho, suportados com pessoas competentes e motivadas.	Otimização das capacidades dos recursos humanos, indo ao encontro dos objetivos da organização.
APO08	Gerir Relacionamentos	Gerir a relação entre o negócio e o TI numa forma formal e transparente que assegure o foco no alcançar de um objetivo comum e partilhado de sucesso da organização, suportado nos objetivos estratégicos e dentro dos limites orçamentais e de tolerância de risco. Basear a relação em confiança mútua, utilizando termos abertos e compreensíveis e uma linguagem comum e uma vontade de assumir decisões chave.	Criar benefícios adicionais, aumentar a confiança em TI e numa eficaz utilização dos recursos
APO09	Gerir Contratos de Prestação de Serviços	Alinhar os serviços de TI e os níveis de serviço com as necessidades e expetativas da organização, incluindo a identificação, especificação, desenho, publicação, acordos e monitorização dos serviços de TI, níveis de serviço e indicadores de desempenho	Garantir que os serviços e os níveis de serviço vão ao encontro das necessidades atuais e futuras da organização
APO10	Gerir Fornecedores	Gerir os serviços de TI assegurados por todos os tipos de fornecedores, para ir ao encontro das necessidades da organização, incluindo a seleção de fornecedores, gestão de relações, gestão de contratos e revisão e monitorização do desempenho de fornecedores relativamente a eficiência e conformidade	Minimizar o risco associado ao não cumprimento dos fornecedores e garantir preços competitivos

APO11	Gerir Qualidade	Definir e comunicar os requisitos de qualidade em todos os processos, procedimentos e nos respetivos resultados, incluindo controlos, monitorização, e a utilização de práticas e normas estabelecidas numa lógica de melhoria contínua e esforços de eficiência	Garantir uma entrega consistente de soluções e serviços para ir ao encontro dos requisites de qualidade da organização e satisfazer as necessidades de todas as partes interessadas
APO12	Gerir Riscos	De forma continua, identificar, avaliar e reduzir os riscos de TI para níveis de tolerância estabelecidos pela gestão executiva da organização	Integrar a gestão de riscos de TI com a gestão global de riscos da organização e balancear os custos e benefícios da gestão de risco de TI da organização
APO13	Gerir Segurança	Definir, operar e monitorizar um Sistema de gestão de segurança de informação	Manter a ocorrência e o impacto de incidentes de segurança de informação dentro dos limites de apetite de risco da organização

Tabela 21 – Processos *COBIT 5* – APO (ISACA, 2012b)

Construir, Adquirir e Implementar		**Descrição**	**Objetivos**
BAI01	Gerir Programas e Projetos	Gerir todos os programas e projetos do portfólio de investimento em linha com a estratégia da organização e numa forma coordenada. Iniciar, planear, controlar e executar programas e projetos e efetuar uma revisão pós-implementação	Obter benefícios de negócio e reduzir o risco de atrasos inesperados, custos e erosão de valor, através da melhoria de comunicações e envolvimento com utilizadores de negócio, garantindo o valor e qualidade dos entregáveis e maximizando o seu contributo para o portfólio de investimentos e serviços
BAI02	Gerir Definição de Requisitos	Identificar soluções e analisar requisitos antes da aquisição ou desenvolvimento, por forma a garantir que estão em linha com os requisitos estratégicos da organização, cobrindo processos de negócio, aplicações, dados, infraestrutura e serviços. Coordenar com as partes interessadas a revisão de opções viáveis, incluindo custos e benefícios relativos, análise de riscos e aprovação de requisitos e soluções propostas	Criar soluções ótimas viáveis, que vão ao encontro das necessidades da organização, ao mesmo tempo que minimizam o risco
BAI03	Gerir Identificação e implementação de soluções	Estabelecer e manter soluções identificadas, em linha com os requisitos da organização, abrangendo o desenho, desenvolvimento, compras e estabelecimento de parcerias com fornecedores. Gerir a configuração, a preparação de testes, os testes, requisitos de gestão e manutenção dos processos de negócio, aplicações, dados, infraestrutura e serviços	Estabelecer soluções atempadamente e com custos controlados, capazes de suportar a estratégia da organização e os objetivos operacionais
BAI04	Gerir Disponibilidade e capacidade	Balancear as necessidades atuais e futuras de disponibilidade, desempenho e capacidade com fornecimento de serviço a custos controlados. Incluir avaliação das capacidades atuais, previsão de necessidades futuras com base em requisitos de negócio, análise de impacto de negócio e avaliação de risco das ações de planeamento e implementação para ir ao	Manter disponibilidade de serviço, gestão eficiente de recursos e otimização do desempenho dos sistemas através da previsão de requisitos de capacidade e desempenho futuros

		encontro das necessidades identificadas	
BAI05	Gerir Capacidade de Mudança	Maximização da probabilidade de implementar com sucesso mudanças sustentáveis em toda a organização, de forma rápida e com risco reduzido, abrangendo todo o ciclo de vida das mudanças e todas as partes interessadas afetadas no negócio e nas TI	Preparar e envolver as partes interessadas nas mudanças de negócio e redução do risco de falha
BAI06	Gerir Mudanças	Gerir todas as mudanças numa forma controlada, incluindo mudanças correntes e manutenções de emergência relacionadas com os processos de negócio, aplicações e infraestruturas. Tal inclui normativos e procedimentos de mudança, avaliações de impacto, priorização e autorização, mudanças de emergência, controlo, reporte, fecho e documentação de mudanças.	Promover uma entrega rápida e fiável da mudança para o negócio e mitigação do risco de impactos negativos para a estabilidade ou integridade do ambiente em mudança
BAI07	Gerir Aceitação e Transição da Mudança	Formalmente aceitar e executar novas soluções operacionais, incluindo planeamento de implementação, conversão de sistemas e dados, testes de aceitação, comunicação, preparação da entrega, promoção da produção de processos de negócio e serviços de TI novos ou alterados, suporte atempado à produção e revisão à pós-implementação	Implementação de soluções de forma segura e em linha com as expetativas e resultados acordados
BAI08	Gerir Conhecimento	Manter a disponibilidade do conhecimento relevante, atual, validado e fiável para suportar todas as atividades dos processos e facilitar a tomada de decisão. Planear a identificação, recolha, organização, manutenção, utilização e descartar do conhecimento	Disponibilizar o conhecimento necessário ao suporte do trabalho de todos os colaboradores, nas suas atividades e para uma tomada de decisão informada e incremento de produção
BAI09	Gerir Ativos	Gerir os ativos de TI através do seu ciclo de vida de forma a garantir que a sua utilização entrega valor a um custo ótimo, que se mantêm operacionais e estão fisicamente protegidos e que os ativos críticos	Controlo sobre todos os ativos de TI e otimização do valor dado por estes ativos

		para o serviço são fiáveis e disponíveis. Gerir as licenças de software, por forma a garantir que é adquirido, mantido e aplicado um número ótimo em relação à necessidade do negócio e que o software instalado está de acordo com os acordos de licenciamento	
BAI10	Gerir Configuração	Definir e manter registo dos recursos chave, das capacidades necessárias para entregar os serviços TI e das relações entre eles, incluindo informações de configurações, estabelecimento de configurações base, verificação e auditoria de informação de configurações e atualização do repositório de configurações	Fornecer informação suficiente sobre os ativos associados aos serviços para promover uma gestão efetiva dos serviços, avaliar o impacto das mudanças e lidar com incidentes de serviços

Tabela 22 – Processos *COBIT 5* – BAI (ISACA, 2012b)

Entregar, Atender e Apoiar		**Descrição**	**Objetivos**
DSS01	Gerir Operações	Coordenar e executar as atividades e procedimentos operacionais necessários para entregar serviços de TI internos e externos, incluindo a execução de procedimentos operacionais pré-definidos e as atividades de monitorização necessárias	Entregar resultados dos serviços operacionais de TI, em concordância com o planeado
DSS02	Gerir Solicitações e Incidentes de Serviços	Dar uma resposta efetiva e atempada às solicitações dos utilizadores e resolução de todos os tipos de incidentes. Restaurar a normalidade do serviço; guardar e executar os pedidos dos utilizadores e guardar, investigar, diagnosticar, escalar e resolver incidentes	Alcançar uma melhoria da produtividade e minimizar disrupções através da rápida resolução de pedidos e incidentes
DSS03	Gerir Problemas	Identificar e classificar problemas e respetivas causas e assegurar uma resolução atempada para prevenir incidentes recorrentes. Disponibilizar recomendações para melhorias	Melhorar a disponibilidade e os níveis de serviço, reduzir custos e melhorar a satisfação dos utilizadores, através da redução do número de problemas operacionais
DSS04	Gerir Continuidade	Estabelecer e manter um plano para promover que o negócio e o TI responda aos incidentes e disrupções de modo a continuar operações dos processos críticos de negócios e serviços de TI necessários e manter disponibilidade da informação a um nível aceitável para a organização	Continuar operações críticas de negócio e manter a disponibilidade da informação a um nível aceitável para a organização em situação de uma disrupção significativa
DSS05	Gerir Serviços de Segurança	Proteger a informação da organização, mantendo o risco de segurança de informação num nível aceitável para a organização em concordância com a política de segurança. Estabelecer e manter as funções de segurança de informação e os privilégios de acesso e realizar monitorizações de segurança	Minimizar o impacto no negócio proveniente de vulnerabilidades e incidentes operacionais de segurança de informação
DSS06	Gerir Controlos do Processo de Negócio	Definir e manter controlos apropriados de processos de negócio para garantir que a informação associada e processada por processos de	Manter a integridade da informação e a segurança dos ativos de informação tratados no âmbito de processos de negócio na empresa ou em *outsourcing*

		negócio satisfaz todos os requisitos relevantes de controlo de informação. Identificar os requisitos relevantes de controlo da informação e gerir e operar controlos adequados para garantir que a informação e o processamento de informação satisfaz esses requisitos	

Tabela 23 – Processos *COBIT 5* – DSS (ISACA, 2012b)

Monitorar, Avaliar e Analisar		**Descrição**	**Objetivos**
MEA01	Monitorar, Avaliar e Analisar Desempenho e Conformidade	Recolher, validar e avaliar métricas e objetivos de negócio, de TI e de processos. Identificar processos que têm um desempenho, metas ou métricas contrários ao esperado e disponibilizar reportes sistemáticos e atempados	Disponibilizar transparência de desempenho e conformidade e alcance de metas
MEA02	Monitorar, Avaliar e Analisar o Sistema de Controlo Interno	Continuamente monitorar e avaliar o ambiente de controlo, incluindo auto-avaliações e análises independentes. Promoção da gestão para identificar deficiências de controlos e ineficiências e iniciar ações de melhoria. Planear, organizar e manter guias para avaliação do controlo interno e revisões de conformidade	Obter transparência para as partes interessadas mais relevantes sobre a adequabilidade do sistema de controlos internos e assim garantir confiança nas operações, confiança no alcance dos objetivos da organização e uma compreensão adequada do risco residual
MEA03	Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos	Avaliar que os processos de TI e os processos de negócio suportados em TI são conformes com os requisitos legais, regulatórios e contratuais. Obter garantia de que os requisitos foram identificados e cumpridos e há ligação da conformidade de TI com a conformidade da organização	Garantir que a organização cumpre com todos os requisitos externos aplicáveis

Tabela 24 – Processos *COBIT 5* – MEA (ISACA, 2012b)

10.2. ANEXO B – CRITÉRIOS

PROCESSOS COBIT 5		CROE			NIST	NIS	RGPD
		Baseline	Intermediate	Advanced			
EDM01	Garantir a Definição e Manutenção do Modelo de Governança	G1; G2; G3; G4; G5; G6; G7; G8; G9; G10; G11; G12; G18; G19; G20; G21; G22; G25; G26; G27; C1; C2; C3; C4	G13; G14	G15; G16; G17; G42; G44	ID.GV-1		

Tabela 25 – Critérios de análise e avaliação de processos EDM

PROCESSOS COBIT 5		CROE			NIST	NIS	RGPD
		Baseline	**Intermediate**	**Advanced**			
APO03	Gerir Arquitetura da Organização	I1; I3; I5; R30	I8; I11; I13		ID.AM-5; ID.BE-2; ID.BE-3		√
APO07	Gerir Recursos Humanos	G28; G29; G30; G31; P64; P65; P66; P67; D7; R5; A8; L4; L5; L6	G35; G36; G37; G39; G40; G41; P69; R52		PR.AT-1; PR.AT-2; PR.AT-3; PR.AT-4; PR.AT-5; PR.IP-11; DE.CM-6		√
APO08	Gerir Relacionamentos	I2; P71	P73; P76; P77	I15; P78; G45	ID.BE-1	√	
APO10	Gerir Fornecedores	P70; P72			ID.BE-1; PR.AT-3		
APO12	Gerir Riscos	I4; I6	A9; A10; A11; A12	A13; A14	ID.RA-1; ID.RA-3; ID.RA-5; ID.RA-6; ID.RM-1; ID.RM-2; DE.AE-4; DE.AE-5; DE.DP-4		√
APO13	Gerir Segurança	I7	I9; I10; I12	I14	PR.AC-3; PR.DS-4; PR.IP-2; PR.IP-4; PR.PT-2; PR.PT-4; ID.GV-2; ID.RA-6; ID.RM-1; DE.DP-3	√	√

Tabela 26 – Critérios de análise e avaliação de processos APO

PROCESSOS COBIT 5		CROE			NIST	NIS	RGPD
		Baseline	**Intermediate**	**Advanced**			
BAI01	Gerir Programas e Projetos		P6; P7	P8; P9	PR.IP-3; RS.RP-1; RS.IM-1		
BAI02	Gerir Definição de Requisitos	P4; P21			PR.DS-1; ID.RM-1		
BAI05	Gerir Capacidade de Mudança	P44; P49;	P54		PR.AT-1; RC.IM-1		
BAI06	Gerir Mudanças	P45; P46; P47; P48; P50; P51; P52; P53	P55; P56	P57	PR.DS-1; PR.IP-3		
BAI08	Gerir Conhecimento	R40; R41; A1; A2; A3; A4; A16; A17; A18; A19; A20	R13; R15; T22; A21; A22; A23; L11	P10; D18; R17; R54; T38; A24; A25		√	√

Tabela 27 – Critérios de análise e avaliação de processos BAI

PROCESSOS COBIT 5		CROE			NIST	NIS	RGPD
		Baseline	**Intermediate**	**Advanced**			
DSS01	Gerir Operações	D1; D2; D3; D4; D5; D6; D9; D10; D11; R6; A5; A6; A7	D12; D13; D14; D15; D17	D19; D20; R34; A15	PR.AC-2; PR.AC-3; PR.IP-5	√	√
DSS02	Gerir Solicitações e Incidentes de Serviços	R4; R7; R8; R36; R37; R38; R39; R44; R45; R46; R47; R48; R49	D16; R10; R11; R12; R14; R42; R50; R51	R16; R18; R19; R35; R43; R53	RC.RP-1; RS.AN-1	√	√
DSS04	Gerir Continuidade	R1; R2; R3; R20; R21; R22; R32	R9	R27	ID.BE-5; ID.GV-4; ID.RA-4; PR.IP-9; PR.IP-7; DE.DP-5	√	

PROCESSOS COBIT 5		CROE			NIST	NIS	RGPD
		Baseline	Intermediate	Advanced			
DSS05	Gerir Serviços de Segurança	P5; P11; P12; P13; P14; P15; P16; P17; P18; P19; P20; P22; P36; P37; D8; R31	P23; P24; P25; P26; P27; P38; P40; P74; P75	P28; P29	DE.CM-4; DE.DP-1; ID.AM-3; PR.PT-2; PR.PT-3; PR.PT-4; PR.AC-3; PR.AC-1; PR.MA-2; PR.AC-2; PR.IP-5; DE.CM-1	√	√
DSS06	Gerir Controles do Processo de Negócio	P1; P2; P30; P31; P32; P33; P34; P35; P58; P59; P60; R23; T9	P39; P61; P62; R24; R25; R26	P41; P42; P43; P63; R28; R29	ID.AM-6; PR.AC-1; PR.AT-2; PR.DS-1; PR.DS-2	√	√

Tabela 28 – Critérios de análise e avaliação de processos DSS

PROCESSOS COBIT 5		CROE			NIST	NIS	RGPD
		Baseline	**Intermediate**	**Advanced**			
MEA01	Monitorar, Avaliar e Analisar Desempenho e Conformidade	P3; T1; T3; T4; T7; T12; T13; T14; T19; T20; L7	G34; G38; T21; T23; T24; T25; T27; T28; L9	T33			
MEA02	Monitorar, Avaliar e Analisar o Sistema de Controlo Interno	G23; G24; T2; T5; T6; T8; T10; T11; T15; T16; T17; T18; L1; L2; L3	G32; G33; P68; T26; T29; T30; T31; T32; L8; L10; L12	G47; T39; T40; T41; T42; L13		√	
MEA03	Monitorar, Avaliar e Analisar Conformidade com Requisitos Externos			G43; G48; T34; T35; T36; T37	ID.GV-3; RC.CO-2		

Tabela 29 – Critérios de análise e avaliação de processos MEA