Auditoria de Cibersegurança: um caso de estudo

Joana Catarina Pimenta Couto

Trabalho de Projeto

Mestrado em Auditoria

Versão final (Esta versão contém as críticas e sugestões dos elementos do júri)

Porto – 2018

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTITUTO POLITÉCNICO DO PORTO

Auditoria de Cibersegurança: um caso de estudo

Joana Catarina Pimenta Couto

Trabalho de Projeto

apresentado ao Instituto de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Auditoria, sob orientação de Luís Silva Rodrigues

Porto – 2018

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DO PORTO
INSTITUTO POLITÉCNICO DO PORTO

Resumo:

O papel da cibersegurança, nas organizações, tem vindo a mudar ao longo dos anos. A cibersegurança tem-se tornado uma prática imprescindível nas organizações, pois assume um papel cada vez mais importante no que concerne à segurança dos sistemas de informação. O principal objetivo é assegurar a disponibilidade, integridade e confidencialidade dos ativos em relação às ameaças do ciberespaço.

Neste sentido, o presente estudo de caso pretende perceber quais as práticas de cibersegurança que uma determinada organização segue, tendo em conta as práticas recomendadas por uma publicação intitulada de "Transforming cybersecurity using COBIT 5" . O COBIT5 é a versão 5 do *Control Objectives for Information and Related Technology e* é um guia de boas práticas apresentado como ferramenta para a gestão de tecnologias de informação.

Inicialmente elaboramos a revisão da literatura, onde se trataram os principais conceitos inerentes à compreensão do tema em estudo e à realização deste estudo de caso.

Relativamente à escolha da metodologia de investigação, esta recaiu na abordagem qualitativa visto que consideramos a mais adequada para o tratamento dos dados recolhidos durante as entrevistas. Este trabalho consistiu na realização de várias entrevistas ao responsável pela secção de *Auditing & Compliance,* assim como pelo responsável pelo departamento de *security* de uma e-commerce portuguesa. Com base na execução das entrevistas, é feito o tratamento dos dados e respetiva apresentação e análise dos resultados.

O último capítulo apresenta as conclusões do trabalho realizado com possíveis soluções a serem desenvolvidas e implementadas pela organização. Neste capítulo são também descritas as dificuldades e limitações encontradas assim como, são apresentadas, propostas para trabalhos futuros.

Palavras chave: Auditoria; Segurança da informação; Cibersegurança; COBIT

Abstract:

The role of cybersecurity in organizations has been changing over the years. Cybersecurity has become an indispensable practice in organizations, as it assumes an increasingly important role in the security of information systems. The main goal is to ensure the availability, integrity, and confidentiality of assets in relation to cyberspace threats.

In this sense, the present case study intends to realize what cybersecurity practices a certain organization follows, taking into account the practices recommended by a publication entitled "Transforming cybersecurity using COBIT 5". COBIT5 is the version 5 of Control Objectives for Information and Related Technology and is a guide of good practices presented as tool for the management of information technologies.

Initially, we elaborated the literature review, where the main concepts inherent to the understanding of the topic under study and the accomplishment of this case study were discussed.

Regarding the choice of research methodology, this was the qualitative approach since we consider the most appropriate for the treatment of the data collected during the interviews. This work consisted on the realization of several interviews with the person in charge of the Auditing & Compliance section, as well as the person responsible for the security department of a Portuguese e-commerce. Based on the execution of the interviews, the data is processed as well the presentation and analysis of the results.

The last chapter presents the conclusions of the work carried out with possible solutions to be developed and implemented by the organization. This chapter also describes the difficulties and limitations encountered, as well as proposals for future work.

Key words: Audit; Information security; Cybersecurity; COBIT

Dedicatória

Aos meus pais,

Pelo apoio constante e amor incondicional

Agradecimentos

Depois de um longo percurso de trabalho e dedicação, seria bastante ingrato deixar de parte este especial agradecimento a todos os que me deram apoio para alcançar esta conquista.

Em primeiro lugar, e como não poderia deixar de ser, agradeço aos meus pais e irmão, pelo amor e apoio incondicional em todos os momentos, principalmente nos de incerteza, muito comuns para quem tenta percorrer novos caminhos. Sem vocês nenhuma conquista valeria a pena.

À Mafalda, a minha melhor amiga, a irmã que Deus me deu. Por me acompanhar incansavelmente nos últimos anos. Por todos os bons e maus momentos em que nunca deixou de estar presente, por ser o meu porto de abrigo, o meu confessionário diário e o meu maior tesouro. Que se cumpra sempre a tradição, porque "o que Viana uniu, ninguém separa!"

À Filipa que sempre esteve do meu lado desde que me lembro, por todo o apoio que sempre me deu, e por me provar diariamente que quando a amizade é verdadeira nunca nada mudará. A distância pode separar dois olhares, mas nunca dois corações!

À minha Sara, a melhor coisa que o Porto me deu! Por todo o companheirismo durante dois anos de descoberta. Por ter sido o meu maior apoio neste mestrado, e essencialmente por ser a pessoa mais doce, justa e compreensiva que já conheci.

Às minhas teinhas todas, a Daniela, Telma, Joana, Vanessa e Andreia, por todos os programas de Sábado e Domingo à noite. Por acompanharem este trabalho desde o início e por sempre me darem o apoio e motivação para nunca desistir.

Ao orientador desta dissertação o Professor Luís Siva Rodrigues pela orientação prestada, pelo seu incentivo, disponibilidade e apoio que sempre demonstrou. Aqui lhe exprimo a minha gratidão.

À Ecosteel, a empresa onde trabalho. À minha colega e amiga Joana pela motivação e apoio diário que sempre me transmitiu desde que a conheço. E por fim, mas não menos importante, às minhas orientadoras na empresa, Mónica, Luzia e Natália, por sempre me motivarem, apoiarem e permitirem ausentar quando necessitei.

Lista de Abreviaturas

APO - *Align, Plan and Organize*

BAI - *Build, Acquire and Implement*

COBIT - *Control objectives for information and related technology*

COBIT5SI - COBIT 5 para Segurança da Informação

COBIT5TC – *Publicação "Transforming cybersecurity using COBIT5"*

DSS - *Deliver, Service and Support*

EDM - *Evaluate, Direct and Monitor*

ISACA - *Information Systems Audit and Control Association*

ISO – *International Organization for Standardization*

ITIL - *Information Technology Infrastructure Library*

MEA - *Monitor, Evaluate and Asses*

SGSI - Sistema de Gestão de Segurança da Informação

SI – Sistemas de informação

TI – Tecnologias da informação

TSI – Tecnologias de sistemas de informação

Índice Geral

Índice de tabelas

Índice de figuras

Introdução

Na atual era, o poder da informação tomou enormes proporções. Derivado ao que a tecnologia nos permite, assiste-se a uma grande dependência de informação, fomentada pelo aumento da capacidade de armazenamento e tratamento da mesma. A um ritmo elevado, a indústria informática, lança no mercado novas tecnologias, que impulsionam a evolução neste contexto.

Cada vez mais, as tecnologias de informação são essenciais nas organizações, tanto para a sua sustentabilidade e desenvolvimento, no suporte e operação como também para a sua prospeção. Desta forma, todos os processos duma organização tendem a depender de sistemas de informação para executar as suas tarefas, tornando a informação e as tecnologias a ela associada, ativos estrategicamente significativos. Como tal, o recurso a SI – sistemas de informação e TI – tecnologias da informação levantam questões relativamente à sua eficácia, eficiência, integridade e qualidade da função organizacional (Carneiro, 2009).

As TI são consideradas facilitadores de desenvolvimento e têm grande impacto na estratégia das empresas (Gomes & Romão, 2012). O acréscimo associado aos investimentos em TI aumenta a preocupação das organizações em garantir os benefícios esperados (Wilkin, Campbell, Moore, & Grembergen, 2013). O valor deste investimento tanto deve ser encarado como um retorno financeiro, como também deve ser considerado um fator estratégico com impactos positivos na organização. A criação de valor significa obtenção de benefícios com otimização de custos dos recursos enquanto se otimiza os riscos (Moeller, 2013), devendo ser considerado como um objetivo, relativamente às práticas de Gestão do Valor das TI.

Organizações que adotam boas práticas de Gestão do Valor das TI vêm simplificada a identificação e criação de valor dos investimentos realizados em TI (Keyes - Pearce, 2005) (Maes, Bruyn, Oorts, & Huysmans, 2014). Estas práticas implicaram a alteração completa do modo de operar da maioria das organizações, passando elas próprias, como refere Carneiro (2009), *"*de sociedades de indústria para sociedades de informação*"*.

No entanto, estas tecnologias são vulneráveis, criando riscos sociais e materiais. Se por um lado, são inúmeros os benefícios que proporcionam aos seus utilizadores, por outro, é notório o aumento significativo dos riscos resultantes da sua dependência, aumento da

quantidade de informação armazenada e em circulação. É neste novo mundo em que vivemos, com novos modos de atuação, que se destacam o cibercrime e, em particular, o cibercrime organizado. O cibercrime organizado está bastante associado à fraude bancária, intrusão de identidade ou espionagem industrial, com o objetivo do desvio e revelação de informação sensível ou classificada ou sabotagem informática (Resolução da Assembleia da Repúblicanº 63/2015, 2015).

É fundamental a implementação de mecanismos capazes de assegurar a segurança da informação e dos meios que a transmitem ou a armazenam. Como tal, tem-se verificado, nos últimos anos, um desenvolvimento nos normativos que visam apoiar as organizações na implementação de um sistema de gestão de segurança da informação. Três desses normativos de referência, muitas vezes utilizados em conjunto e que podem ser aplicados às diferentes estratégias e focos são a ISO 27001 (Information security management), a ITIL 3 (Information Technology Infrastructure Library) e o COBIT 5 (Control Objectives for Information and Related Technologies). Estes normativos permitem às organizações implementar métodos, princípios e políticas, tendo por base um estudo do universo organizacional ao longo dos últimos anos.

Neste contexto, o principal foco deste trabalho de projeto, centra-se nas práticas de cibersegurança. Transformando o contexto do COBIT 5 para segurança da informação ao contexto da cibersegurança, o objetivo deste trabalho de projeto é realizar uma auditoria às práticas de cibersegurança numa organização, neste caso, uma e-commerce, uma vez que se enquadra melhor no âmbito do tema.

Organização do documento

O presente trabalho de projeto está organizado em 5 capítulos.

O primeiro capítulo é destinado à revisão da literatura. Nesse capítulo é feito o enquadramento dos conceitos inerentes à realização deste estudo de caso. É abordada a temática da segurança dos sistemas de informação, nomeadamente alguns conceitos associados como o conceito de informação e sistemas de informação. No contexto da segurança da informação é discutida a sua importância, alguns agentes, ameaças e invasores e os tipos de segurança existentes.

No capítulo II é feita uma apresentação da importância das normas e boas práticas de segurança de sistemas e tecnologias de informação, identificando os principais normativos contêm uma forte componente de segurança da informação. Uma vez o caso de estudo deste trabalho de projeto se baseou no conjunto de boas práticas de segurança da informação da publicação *Transforming Cybersecurity using COBIT5* (COBIT5TC), apresenta-se uma descrição mais detalhada do COBIT 5 para a Segurança da Informação (COBIT5SI).

No Capítulo III são apresentadas as metodologias e técnicas aplicadas assim como o respetivo planeamento cronológico de todo o projeto, tendo em conta as tarefas e objetivos. Nesse capítulo é também descrito todo o trabalho realizado ao longo de várias fases e apresentada a organização em estudo.

Tendo por base a execução do estudo de caso, é feita uma apresentação e análise dos resultados no capítulo IV. Neste capítulo é feita a estruturação dos dados recolhidos e respetiva análise.

O último capítulo apresenta as conclusões do trabalho realizado com possíveis soluções a serem desenvolvidas e implementadas pela organização. Nesse capítulo são também descritas as dificuldades e limitações obtidas, apresentadas possíveis propostas para trabalhos futuros e as considerações finais do trabalho.

Capítulo I – Enquadramento de conceitos

1.1. Informação

A informação adquiriu um papel fundamental na nossa sociedade, e com o decorrer do tempo, a importância deste recurso acresce cada vez mais, sendo a sociedade atual considerada como a sociedade da informação (Piattini, 2000).

Informação pode ser assim definida como um conjunto de dados que foram interpretados e compreendidos pelo destinatário da mensagem (Lucey, 2005). Trata-se de factos ou conclusões que adquirem significado num determinado contexto. Os dados são manipulados e apresentados, e esse tratamento conduz a uma melhor compreensão da situação (Oz, 2009). É vital que exista um cuidado com a simbologia utilizada e o contexto da mensagem, por forma a reduzir a incerteza e a aumentar a probabilidade da entrega da informação ao destinatário (Lucey, 2005) e potencializar a racionalidade do processo de decisão, isto é, de administração e gestão (Oliveira A. , 1998/9).

A informação deve ser reconhecida como um ativo ou um recurso que gera benefícios às organizações (ISACA, 2013a) e é considerada uma ferramenta que acrescenta valor, cria vantagem competitiva e deve ser usada como suporte na gestão (Marchand, 2000).

São várias as definições atribuídas ao conceito de informação. No entanto, a maioria dos autores refere que a informação tem valor no conhecimento e no processo de decisão e é reconhecida como uma mais valia para a atividade de gestão.

A importância da informação para as organizações é universalmente aceite, constituindo, senão o mais importante, um dos recursos cuja gestão e aproveitamento mais influência o sucesso das organizações (Ward, Griffiths, & Whitmore, 1990). A informação é considerada e utilizada em muitas organizações como um fator estruturante e um instrumento de gestão (Zorrinho, 1991), bem como uma arma estratégica indispensável para a obtenção de vantagens competitivas (Porter, 1985).

Como tal, uma vez considerada como um recurso fundamental para as organizações, é necessário que haja precaução na proteção da mesma, para que se garanta que é fidedigna, protegendo assim a reputação da organização aos olhos dos seus stakeholders (FFIEC, 2016)

1.1.1. Gestão da Informação

A aceitação de que a informação possa ser gerida da mesma forma tal como outros recursos da organização é ainda um assunto bastante discutido. Enquanto recurso, e à semelhança de outros bens económicos, a informação deve ser gerida [(King & Kraemer, 1988), (Oliveira A. , 1994)], sendo aconselhado por alguns autores que esta até seja considerada um bem de inventário (Ronen & Spiegler, 1991). No entanto, as diferenças entre a "informação" e os outros recursos dificultam ou impossibilitam a sua categorização em termos económicos.

Arrastadas pela importância que reconhecem à informação, muitas organizações não se apercebem de alguns excessos na sua procura e manutenção. A informação não contem toda o mesmo valor ou a mesma importância. Como tal há uma necessidade de distinguir/classificar a informação, de modo a que o seu tratamento e manutenção seja feito de forma correta. Segundo Sutter (1993) a informação pode ser classificada como "crítica", "útil", "interessante" e "sem interesse", identificando assim qual o seu grau de relevância em função do papel que pode desempenhar nas atividades da organização.

Os autores Amaral & Varajão (2007), reformulam a classificação acima referida, atribuindo-lhe os termos "informação crítica", "informação mínima", "informação potencial" e "informação lixo", aos quais estão atribuídos os seguintes significados:

- "Informação crítica – essencial à sobrevivência da organização"
- "Informação mínima – essencial para uma boa gestão da organização"
- "Informação potencial – essencial para a obtenção de vantagens competitivas pela utilização do SI"
- "Informação lixo – essencial para nada"

Em função desta classificação, os mesmos autores acrescentam ainda que deverá haver uma evolução do esforço por parte da organização na procura e manutenção da "informação crítica", da "informação mínima" e da "informação potencial". Quanto à "informação lixo", o esforço que deverá ser feito é, obviamente, no sentido de se evitar qualquer dispêndio de recursos com ela. A aceitação do princípio subjacente a classificações como esta é comum e utilizado em muitas abordagens de Gestão de Sistemas de Informação.

1.2. Sistema de Informação

O termo Sistemas de Informação (SI) é, nos dias de hoje bastante conhecido e discutido mundialmente. A sua utilidade e impacto em diversas áreas, têm vindo a despertar um crescente interesse, na exploração de formas inovadoras de aplicação de tecnologia (Ray & Acharya, 2004).

Dado este interesse de grande escala, seria de esperar que fosse fácil obter uma definição universal para sistemas de informação, porem são várias as definições propostas por autores e investigadores ao longo dos anos (Alter, 1992).

Uma definição comum para SI é proposta por Buckinham, Hirschheim, Land & Tully (1987): "Sistema de Informação é um sistema que reúne, guarda, processa e faculta informação relevante para a organização (…), de modo que a informação é acessível e útil para aqueles que a querem utilizar, incluindo gestores, funcionários, clientes, (…). Um sistema de informação é um sistema de atividade humana (social) que pode envolver ou não a utilização de computadores."

Ainda que concetualmente seja aceite a existência de SI sem a participação de computadores, a observação da realidade permite concluir que são muito raras as organizações que não integram computadores no seu SI (Bretschneider & Wittmer, 1993). Aceitando a presença das TI como participantes nos SI, podem-se redefinir, como uma perspetiva mais organizacional, segundo Alter (1992): "Sistema de Informação é uma combinação de procedimentos, informação, pessoas e TI, organizadas para o alcance de objetivos de uma organização."

De uma forma muito semelhante, Oliveira (1998/9) define sistema de informação como um conjunto de meios físicos e lógicos, humanos, financeiros, organizacionais e consumíveis diversos, que de uma forma racional interagem entre eles, se integram e se combinam com vista à produção, memorização e distribuição/consulta de informação, para satisfazer determinadas necessidades de gestão.

Todas as organizações têm obrigatoriamente um sistema de informação. A hipótese da sua não existência põe em causa a comunicação e relacionamento entre os seus elementos e, portanto, o próprio conceito de organização (Rivas, 1984). Rivas (1984) defende inclusive que "qualquer organização, seja de que tipo for, pode e deve ser encarada como um sistema de informação", na medida em que pode ser encarada como um sistema que

recolhe, memoriza, processa e utiliza informação nos seus processos de decisão e de operação (Rivas, 1984).

De um modo geral, "O sistema de informação de uma organização deverá possibilitar, aos responsáveis pela decisão, a informação necessária para as decisões programadas, auxiliando na tomada de decisões não programadas, apoiar o desempenho do sistema de operações, e assegurar a comunicação entre os elementos da organização" (Caldeira, 2008).

Como todos os outros sistemas, os SI devem ser compreendidos por todos os colaboradores da organização. A sua compreensão é necessária para que consigam utilizá-los como suporte do seu trabalho e na interação com as outras pessoas da organização (Oz, 2009). No entanto, e apesar dos avanços tecnológicos, ainda se encontram nas organizações problemas de falta de aplicação de normas, metodologias, formação e cultura generalizada (Carneiro, 2009). Apesar de não existirem organizações sem sistema de informação, nem sempre o sistema de informação existente é eficiente.

Quanto à classificação de sistemas de informação, são utilizados diferentes critérios com diversas combinações, o que faz com que existam inúmeras propostas, de diferentes autores, sobre as características fundamentais desses tipos (Amaral & Varajão, 2007). Contudo, são mais frequentes e aceites as classificações que utilizam como critérios: as funções desses SI e os componentes que integram; os níveis de gestão que prioritariamente servem; a era a que pertencem; uma mistura de critérios (Amaral & Varajão, 2007). Como exemplo de uma classificação baseada numa mistura de critérios, tem-se a proposta de Alter (1992) citada por Amaral & Varajão (2007), onde identificados os seis tipos de SI definidos na Tabela 1.

Tipo de sistema	Definição
Sistema de Processamento de Transações	Recolhe e mantem a informação sobre transações e controla pequenas decisões que delas fazem parte
Sistema de Informação de Gestão	Converte informação relativa a transações em informação útil para a gestão da organização
Sistema de Apoio à decisão	Ajuda os utilizadores no processo de tomada de decisão, fornecendo-lhes informação, modelos e ferramentas importantes para análise da mesma
Sistema de Informação para executivos	Fornece aos gestores, de um modo interativo e flexível, acesso a informação geral para usar na gestão da organização
Sistema Pericial	Suporta os profissionais do desenho, diagnóstico e avaliação de situações complexas que requerem conhecimento especializado em áreas específicas
Sistema de Automação de Escritório	Mantem as tarefas de comunicação e processamento de informação associadas ao ambiente e escritório

Tabela 1– Tipos de Sistemas de informação – (Amaral & Varajão, 2007)

Segundo Amaral & Varajão (2007) um dos critérios de classificação mais adotadas, é o dos níveis de gestão de Anthony (Anthony, 1965). Os níveis de gestão resultam da estratificação das atividades de gestão de acordo com a sua natureza estratégica, tática e operacional em três níveis: Planeamento estratégico; Controlo de Gestão; Controlo Operacional

"Os SI são então classificáveis em sistemas de planeamento, sistemas de controlo e sistemas operacionais, de acordo com o nível de gestão que prioritariamente servem" (Ward, Griffiths, & Whitmore, 1990) citado por (Amaral & Varajão, 2007)

A tabela 2 apresenta uma classificação para os tipos de Sistemas de informação, de acordo com esta proposta de Anthony. (Earl, 1988).

Nível de gestão	Tipo de sistema
Planeamento estratégico	Sistema de Informação Estratégico
Controlo de Gestão	Sistema de Apoio à decisão
Controlo Operacional	Sistema de Processamento de transações

Tabela 2- Tipos e sistemas de Informação, adaptado de Earl (1988)

"A utilização das TI como suporte dos SI das organizações tem sofrido uma evolução, de acordo com uma mudança no papel que se atribui às TI/SI ou de acordo com a função principal que lhes é imposta" (Amaral & Varajão, 2007).

1.3. Segurança da informação

Segurança trata-se de garantir a proteção contra adversidades, quer estas aconteçam de forma intencional ou não. Segurança da informação estabelece que o foco dessa proteção se encontra na informação e nos seus elementos mais críticos, tais como os seus sistemas e hardware, que usam, armazenam e processam essa mesma informação (Whitman & Mattord, 2008).

O ISACA- *Information Systems Audit and Control Association* (2012b) define segurança da informação como algo que "garante, dentro da organização, que a informação é protegida da divulgação a utilizadores não autorizados (confidencialidade), das modificações inapropriadas (integridade) e da ausência de acesso quando requerido (disponibilidade)" explicando cada uma das componentes:

- Confidencialidade – Confidencialidade significa preservar as restrições de autorização de acesso e divulgação, incluindo meios para proteção de privacidade e informações confidenciais.
- Integridade – evitar a modificação ou a destruição imprópria da informação, garantindo que estes atos só são efetuados pelas pessoas autorizadas, por forma a garantir a autenticidade da informação.
- Disponibilidade – O acesso e o uso da informação devem ser atempados e de confiança.

Segundo Pimenta & Quaresma (2016) *"*para que os sistemas de informação (SI) estejam sempre disponíveis e garantam a integridade e confidencialidade da informação que recolhem, processam, armazenam e distribuem, há um fator muito importante a ter em consideração, para além da tecnologia propriamente dita e de todos os mecanismos de segurança que venham a adotar, que são os usuários dos SI/TI*".* Ou seja, se estes usuários da informação não tiverem um conjunto de práticas e regras na utilização dos SI/TI, corre-se o risco de gerar informação incoerente, desfasada da realidade o que, consequentemente, levará a tomadas de decisão incorretas (Pimenta & Quaresma, 2016). Os usuários devem ser sensibilizados para as questões de segurança, nomeadamente para os efeitos negativos que uma falha ou quebra de segurança podem provocar (Kruger & Kearney, 2008). Portanto, é necessário que se promova dentro da organização uma cultura de segurança e garantir que as boas práticas são uma componente natural do comportamento dos usuários. (Pimenta & Quaresma, 2016).

Para Knapp, Marshall, Byrd, & Morris (2009), o primeiro passo, e mais importante, para preparar a organização contra eventuais ataques, quer estes tenham origem interna ou externa é, desenvolver um conjunto de políticas de segurança da informação.

Para Kruger & Kearney (2008) a implementação efetiva de controlos de segurança, numa organização, depende da criação e divulgação de um conjunto de boas práticas e comportamentos que sejam percebidos e adotados por todos os elementos da mesma. As organizações, além de definirem os procedimentos de segurança dos SI a adotar, devem também motivar os usuários a aplicá-los, mostrando-lhes através de simulações que as suas ações podem provocar vulnerabilidades na organização e, consequentemente, ataques aos SI (Workman, Bommer, & Straub, 2008) citado por (Pimenta & Quaresma, 2016).

1.3.1. Importância

Uma vez que não é inevitável que aconteçam incidentes, é necessário garantir, em qualquer que seja a circunstância, a continuidade das atividades da empresa, tendo em conta a minimização de prejuízos que possam ocorrer, prevenindo e reduzindo os seus impactos. Portanto, é necessário que se definam padrões que permitam a análise e avaliação do SI (Carneiro, 2009).

Segundo o ISACA (2010) *"*um dos fatores mais importantes na proteção da informação e seus elementos básicos, reside na determinação e constituição de boas bases para uma gestão eficaz da segurança da informação". Essa gestão está focalizada na prática de reunir, monitorizar e analisar dados relacionados com a segurança da informação (Rouse, 2009), com o intuito de medir a eficácia que os controlos implementados e mantidos pelas organizações têm, idealizando estratégias de monitorização contínua ou de avaliações independentes de controlos de segurança (Gantz, 2014). Com o objetivo de automatizar esta gestão, as organizações podem basear-se num Sistema de Gestão de Segurança da Informação (SGSI) (Rouse, 2009).

Um Sistema de Gestão de Segurança da Informação é definido como um conjunto de processos e procedimentos, baseados em normas e legislação, que uma organização implementa para promover a segurança no uso de seus ativos. O sistema deve ser seguido por todos aqueles que se relacionam direta ou indiretamente com a infraestrutura de TI da organização, como é o caso dos: funcionários, prestadores de serviço, parceiros e terceiros. O SGSI deve possuir obrigatoriamente a aprovação da direção e do departamento jurídico da organização para conferir sua legalidade (Mendes, Oliveira, Costa, & Gomes, 2015).

1.3.2. Ameaças à segurança

Associado à questão da segurança da informação, existem ameaças, vulnerabilidades, ataques e riscos que podem afetar a atividade dos SI nas organizações. Como tal, é necessário proceder à sua identificação e caracterização para conseguir dar melhor resposta e proteção aos SI, no caso de se verificar alguma destas ocorrências (Gaivéo, 2008).

Entender o significado de risco, ameaça e vulnerabilidade torna-se muito importante no contexto da segurança da informação, pois estes funcionam como ponto central para todo

o conhecimento das questões da segurança da informação. A segurança da informação existe para o gerir o risco e o risco existe em função das ameaças e vulnerabilidades.

O risco é um conceito usado para expressar incerteza sobre eventos e / ou seus resultados que poderiam ter um efeito material sobre os objetivos da organização (McNamee & Selim, 1998). Expressa a possibilidade de ocorrência de um evento que tenha impacto na consecução dos objetivos. O risco é medido em termos de impacto e probabilidade (IIA, 2004).

A vulnerabilidade neste contexto pode ser definida como uma falha ou debilidade no hardware, software ou processo que pode comprometer um sistema, rede ou aplicação. De acordo com Wadlow (2000) as vulnerabilidades são os pontos fracos existentes nos ativos, que quando explorados por ameaças, afetam a confidencialidade, a disponibilidade e a integridade das informações de uma pessoa ou organização.

Relativamente àquilo que é uma ameaça, define-se como sendo qualquer circunstância ou evento com potencial para impactar negativamente nas operações organizacionais, bens organizacionais ou indivíduos, pelo seu sistema de informação, através do acesso não autorizado, destruição, divulgação, modificação de informações e / ou negação de serviço (NIST, 2017).

1.3.3. Classificação das ameaças

Nos dias de hoje, as organizações têm que lidar com várias ameaças ao seu negócio. Como tal existem vários exemplos de ameaças que podem interferir com uma organização, desde o roubo da informação, a fraude, sabotagem, espionagem industrial, etc.

Ter conhecimento dos tipos de ameaças que podem pôr em causa a segurança das organizações é uma mais-valia no processo de gestão da segurança da informação (Cannon, 2008). Segundo Loch, Carr & Warkentin (1992) podemos definir as ameaças de acordo com quatro dimensões, referidas de seguida e apresentadas na figura 1:

- Fonte - pode ser interna ou externa à organização;
- Perpetrador - representa a origem da ameaça, podendo ser humana ou não humana (i.e. ambiental, tecnológica);
- Intenção - define se o incidente é acidental ou intencional;

- Consequência do incidente - expõe quais os pilares da segurança da informação (integridade, confidencialidade ou disponibilidade) foram violados.

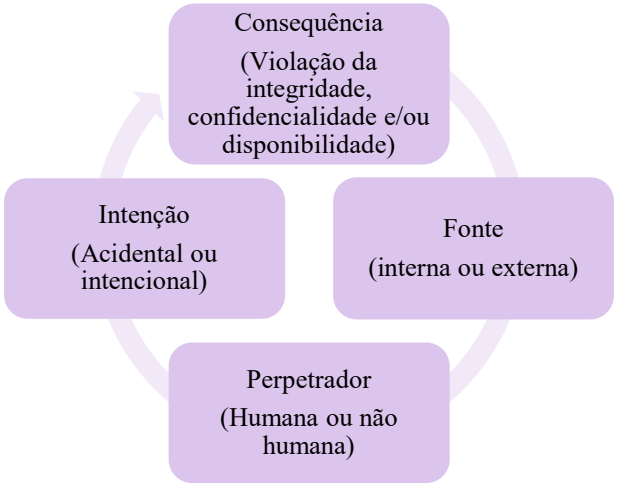

Figura 1- As quatro dimensões da ameaça - adaptado (Loch, Carr, & Warkentin, 1992)

A título de exemplo, segue-se a tabela 3 para complementar a figura 1:

Tipo de ameaça	Exemplos
Naturais	Terramotos, vulcões, fogos, tempestades, acidentes de transporte, cheias
Humanas	Erro humano, sabotagem, vandalismo, roubo, fraude, negligência
Tecnológicas	Bugs de software, defeito técnico
Competição organizacional	Espionagem, roubo de propriedade intelectual, infração de direitos de cópia

Tabela 3– Exemplos de ameaças à segurança da informação- adaptado (Loch, Carr, & Warkentin, 1992)

Apesar de serem acontecimentos imprevisíveis, não deve ser descartada a possibilidade de acontecerem. Deve então usar-se a informação relativamente a estas ameaças na definição do plano de segurança da informação, para que a organização esteja pronta a lidar com elas (Cannon, 2008).

Este fator de imprevisibilidade é, sem dúvida, uma mais-valia para os invasores, e nunca se sabe quais são os motivos que os irão mover para a ação, pois estes podem ser políticos, económicos, com teor vingativo ou simplesmente por pura paixão e divertimento. Mas, seja qual for o motivo, acaba sempre por interferir e causar danos à organização, embora uns sejam mais graves do que outros. Existem muitos invasores com tempo, acesso e habilidades necessárias para perpetuar os diferentes ataques (Cannon, 2008).

Contudo, não de deve descartar a possibilidade destes ataques serem perpetuados por membros da própria organização, uma vez que já têm garantido o acesso aos sistemas da

organização, o que facilita a execução de qualquer atividade ilícita contra a entidade, e podendo, assim, utilizar a informação disponibilizada internamente para ações que ponham em causa o alcance dos objetivos da entidade (ISACA, 2010).

1.4. Auditoria dos sistemas de informação

Segundo Oliveira (2006) a auditoria define-se como "um exame ou verificação de uma dada matéria, tendente a analisar a conformidade da mesma com determinadas regras, normas ou objetivos, conduzindo por uma pessoa idónea, tecnicamente preparada, realizado com observância de certos princípios, métodos e técnicas geralmente aceites, com vista a possibilitar ao auditor formar uma opinião e emitir um parecer sobre a matéria analisada". No seguimento desta mesma definição, o mesmo autor refere que o conceito de auditoria dos sistemas de informação não difere muito daquilo que é o conceito geral de auditoria, sendo que a única diferença se encontra no facto de ser direcionada para os sistemas de informação.

Ron Weber (1999) citado por (Oliveira J. A., 2006) define a auditoria dos sistemas de informação como um "processo de recolha e avaliação de evidencias para determinar se um sistema computadorizado salvaguarda os bens, mantém a integridade dos dados, permite atingir os objetivos da organização de forma eficaz e utiliza os recursos de forma eficiente".

O mesmo autor relaciona ainda a definição dada pela instituição espanhola *Intervencion General de la Administración del Estado (IGAE)*, onde a definição de auditoria de sistemas de informação é descrita como uma "revisão dos sistemas de informação, para verificar se realizam as funções e operações para as quais foram criados, assim como comprovar se os dados e demais informações neles contidos correspondem aos princípios de fiabilidade, integridade, precisão e disponibilidade".

Como tal, e relacionando as definições supracitadas, a auditoria dos sistemas de informação pode ser definida como uma verificação efetuada aos sistemas de informação presentes numa dada organização, com base em regras, normas e objetivos, com o intuito de recolher e avaliar evidencias. A sua finalidade é verificar se as funcionalidades dos sistemas e os dados se encontram salvaguardadas, assim como o cumprimento dos princípios de fiabilidade, integridade, precisão e disponibilidade.

Tanto Oliveira (2006) como Carneiro (2009), enumeram um conjunto de objetivos a cumprir, aquando da realização de uma auditoria de sistemas de informação. Consolidando todo este conjunto de objetivos, enumera-se os seguintes:

- Verificar a existência, assim como a adequação e eficácia das medidas de controlo interno aplicáveis;
- Verificar se as suas atividades se desenvolvem eficientemente e de acordo com os normativos legais aplicáveis;
- Verificar as condições em que ocorre a exploração dos procedimentos de controlo e os processos de segurança inerentes, no que respeita a hardware, software, dados, informações e até o próprio pessoal;
- Rever a eficácia da gestão dos recursos materiais e humanos que pertencem a essa função;
- Verificar se a informação proporcionada pelo sistema de informação é fiável, íntegra e precisa:
- Oferecer uma descrição do SI com base nas suas especificações funcionais e nos resultados que proporciona;
- Determinar se o sistema de informação atinge os objetivos para os quais foi desenhado, de forma eficaz e eficiente;
- Propor recomendações oportunas para que o SI se adapte às diretrizes consideradas como essenciais para o seu bom funcionamento.

1.5. Tipos de segurança

Numa organização é essencial a existência de um programa de segurança que tenha como objetivo assegurar que os diferentes tipos de informação que suportam as atividades do negócio, como é o caso dos sistemas, dados, imagens, textos ou registos de voz, estejam protegidos (Musaji, 2001). Como tal, para que e garanta esta segurança, são utilizados vários instrumentos em diversas áreas de ação (Silva, Carvalho, & Torres, 2003).

Carneiro defende que a informação essencial à existência de uma organização deve ser guardada em instalações que garantam a segurança adequada com acessos condicionados, independentemente do suporte (papel, CD'S). No entanto, salienta que para além da segurança física é importante considerar a segurança lógica dos SI (Carneiro, 2009).

1.5.1. Segurança Física

Este tipo de segurança tem como objetivo assegurar a proteção dos SI respetivamente às suas dimensões físicas e aos seus componentes (Carneiro, 2009). Basicamente, a segurança física consiste em implementar barreiras físicas e procedimentos de controlo, que sejam utilizados como medidas de prevenção e contramedidas perante as possíveis ameaças aos recursos e à informação confidencial da organização (Carneiro, 2009). Em muitas organizações a segurança física encontra-se abaixo dos padrões aceitáveis [(Cascarino, 2007), (Carneiro, 2009)].

No sentido de fazer uma análise à segurança física, Carneiro (2009) propõe a sua subdivisão em dois subgrupos: pessoal e instalações. No que diz respeito à segurança física correspondente ao pessoal, incluem-se as situações em que a componente humana é o principal foco e o risco é associado a situações de erro, roubo, fraudes e/ou má utilização dos recursos existentes (Carneiro, 2009). Nesta perspetiva é importante ter em conta algumas questões fundamentais como (Carneiro, 2009):

- Seleção e recrutamento dos recursos humanos;
- Documentação que serve de apoio à sua atuação (manuais, normativos internos);
- Formação desses recursos humanos, assim como a sua sensibilização e motivação;
- Conhecimento da política de segurança, e o respetivo plano de segurança;
- Ter em atenção os utilizadores (internos ou externos) dos sistemas que utilizam e geram informação. Gestão de acessos e uso da informação;

Quanto à segurança física relativa às instalações, o objetivo é garantir um nível de segurança adequado relativamente à localização e estrutura dos edifícios que são destinados aos centros de informática (Carneiro, 2009). Neste contexto, trata-se por exemplo, do local onde está instalado o centro do sistema que gere e armazena a informação.

1.5.2. Segurança Lógica

A segurança lógica tem como objetivo estabelecer barreiras e procedimentos que controlem o acesso aos dados e à informação (Carneiro, 2009). Consoante o grau de risco associado ao sistema, são então implementados controlos. Quanto maior for o risco

apresentado por um sistema, maior será a dedicação em termos de tempo e recursos (Champlain, 2003).

Tal como na segurança física, Carneiro (2009) também propõe uma divisão a nível da segurança lógica, constituindo então 3 subgrupos: Gestão e controlo de acessos, gestão do SI informatizado e da Rede e segurança dos sistemas aplicacionais.

Quanto à gestão e controlo de acessos, o principal objetivo é que os acessos aos SI sejam condicionados. Assim sendo um dos pré-requisitos para as medidas de segurança é a identificação e autenticação dos utilizadores (Cascarino, 2007), evitando assim o acesso ao sistema de informação de pessoas não autorizadas (ISACA, 2010). Para autenticar a identidade de um utilizador, Carneiro (2009) refere algumas técnicas: palavra-chave, uma chave criptográfica ou um PIN[1]; cartão magnético; impressões digitais ou análise das iris; padrões de escrita.

A nível da gestão do SI informatizados e da rede, o foco é assegurar uma segura e adequada gestão de todos os computadores existentes numa determinada rede (Carneiro, 2009). Um dos problemas mais frequentes nas redes de computadores é o controlo de acesso. Se por um lado o uso do sistema tem que ser de acesso relativamente fácil para os utilizadores, por outro, os responsáveis pelos mesmos esperam que existam controlos mais rígidos para garantir a segurança. Como tal, com o objetivo de melhorar os controlos de acesso à rede, tem-se implementado um sistema de elevada segurança e fácil para o utilizador: o sistema *single sign-on* (ligação única) (Cannon, 2008).

Quando uma organização está conectada à internet isso representa um perigo potencial, uma vez que a tornará vulnerável a ataques. Uma solução para proteger as redes de computadores de ameaças, quer de origem interna ou de origem externa, é a utilização de firewalls, uma vez que reduz o acesso externo à rede (Cannon, 2008).

A redes privadas virtuais (VPN – *Virtual Private Network*), são outro elemento que permite conectar vários utilizadores através de uma rede pública. Este mecanismo permite que se estabeleça uma ligação temporária, caracterizada como rentável e altamente flexível (Cannon, 2008).

[1] PIN - Número de identificação pessoal

No mesmo âmbito das ligações efetuadas na internet é essencial considerar a existência de ameaça de vírus às redes utilizadas pelas organizações. É importante que as organizações implantem mecanismos que se dediquem à deteção de vírus. Neste contexto, são utilizados então os antivírus, que são constituídos por uma base de dados composta por excertos de códigos binários que caracterizam o vírus, permitindo a identificação do mesmo. Como tal é necessária uma atualização constante deste tipo de soluções (Silva, Carvalho, & Torres, 2003).

Outra ferramenta muito semelhante à da deteção do vírus é o IDS (*Intrusion Detection System*) que tem como função a deteção de intrusões. O objetivo é informar o administrador quando houver alguma suspeita de invasão ou de ataque que esteja a ocorrer (Costa, 2010). Para alem do bloqueio do ataque, este mecanismo faculta a possibilidade de saber exatamente o que aconteceu assim como o número de tentativas de intrusão que atingiu a rede da organização (Silva, Carvalho, & Torres, 2003). Para além destas tecnologias, existem inúmeras outras que também são exemplos de segurança lógica que uma organização pode aplicar na sua rede de maneira a garantir a sua segurança.

1.5.3. Cibersegurança

As últimas décadas têm sido marcadas por profundas mudanças de paradigmas na sociedade, no que respeita a tecnologias de informação e comunicação, ligando toda a humanidade numa cultura globalizada. Consequente deste crescimento exponencial da utilização das tecnologias e do ciberespaço, a sociedade tem vindo a ficar cada vez mais vulnerável, tendo aumentado a quantidade de ameaças aos sistemas de informação assim como o impacto dos danos causados por ataques.

Os sistemas de informação, comunicação digital e ambiente digital circundante, representam entre os governos e organizações, o coração do sucesso no que toca aos processos de tomada de decisão sobre assuntos críticos e sensíveis (Raposo, 2016). De forma a conseguir manter as infraestruturas sustentáveis e competitivas, tem sido crescente a procura de mecanismos de processos para garantir recursos digitais seguros. Assim, "a necessidade de edificar mecanismos de proteção e defesa, destinados a garantir a livre circulação da internet e do ciberespaço, tem encaminhado os Estados para o aprofundamento de uma cultura de cibersegurança e à tomada de consciência coletiva,

relativamente à importância do desenvolvimento de políticas e estratégias cooperativas de combate a todas as formas de ataque cibernético" (IDN-CESEDEN, 2013).

Segundo a definição do *International Telecomunications Union* (ITU), a cibersegurança designa-se como um conjunto de ferramentas, políticas, guias, abordagens de gestão de risco, ações de formação, boas práticas e tecnologias que podem ser usadas para proteção dos ativos da organização e de todos os utilizadores no ambiente virtual. Estes ativos e utilizadores referidos incluem dispositivos ligados em rede, aplicações e serviços, sistemas de telecomunicações e de comunicação multimédia e a informação transmitida e/ou armazenada no mundo virtual. Esta referida proteção visa assegurar, a disponibilidade, integridade e confidencialidade dos ativos em relação às ameaças do ciberespaço (ITU, 2009).

A cibersegurança abrange tudo aquilo que visa proteger as organizações e indivíduos face a ataques intencionais, violações e incidentes, bem como as suas respetivas consequências. Esta aborda essencialmente os tipos de ataques, violação ou incidente que são direcionados, sofisticados e difíceis de detetar ou gerir. Atuar contra estes ataques geralmente pode ser tratado usando estratégias e ferramentas simples, mas eficazes. Como resultado, o foco principal da cibersegurança está nas ameaças persistentes avançadas, ciberguerra e seu impacto sobre empresas e indivíduos. A cibersegurança deve estar alinhada com todos os outros aspetos da segurança da informação no contexto da organização, incluindo a governação, gestão e garantia da mesma. Nesse sentido, a noção geral de segurança é sistêmica e não linear, tendo em conta a ideia de que, ser seguro é um estado transitório que requer manutenção e melhoria contínua de forma a atender às necessidades e exigências dos stakeholders (ISACA, 2013b).

Assim, a nível nacional e internacional têm vindo a surgir normativos de cooperação, iniciativas legais e entidades "que definem normas e princípios destinados a garantir uma internet sustentável e um comportamento aceitável no ciberespaço" (IDN-CESEDEN, 2013).

Capítulo II - Normas e Boas Práticas em TSI e segurança da informação

2.1. Normas e práticas de segurança de sistemas e tecnologias de informação

Nos últimos anos, tem-se observado uma crescente dependência das tecnologias de informação, por parte das organizações, quer sejam públicas ou privadas, considerando cada vez mais a essencialidade para a sua sustentabilidade e desenvolvimento, no suporte, operação e prospeção do seu negócio (Pereira & Ferreira, 2015).

A esta dependência das tecnologias de informação, está associado um investimento que as organizações devem fazer em prol da busca de valor. Por outro lado, este investimento em TI aumenta a preocupação das organizações em garantir os benefícios esperados, uma vez que são vários os estudos, que demonstram casos de insucesso com os investimentos realizados em TI (Wilkin, Campbell, Moore, & Grembergen, 2013). Como tal, um dos dilemas mais frequentes para as organizações e os seus responsáveis, é saber como podem garantir a realização de valor dos seus investimentos realizados em TI.

O significado de criação de valor, traduz-se na obtenção de benefícios com otimização de custos dos recursos, mas ao mesmo tempo, otimizando também os riscos (Moeller, 2013), o que por norma, deverá ser o objetivo das práticas de gestão do valor das TI. Como tal, as organizações adotam boas práticas de gestão do valor das TI com o objetivo de facilitar a identificação, criação e obtenção de valor dos investimentos realizados em TI (Keyes - Pearce, 2005) (Maes, Bruyn, Oorts, & Huysmans, 2014).

Em função desta realidade, as organizações têm vindo a procurar soluções, quer seja através da adoção de frameworks de gestão e Governação das TI já desenvolvidos e propostos pela comunidade profissional ou então por modelos próprios adaptados à sua realidade organizacional (Bartens, et al., 2014). No âmbito de segurança da informação, existem diversas opções tais como: normas da série ISO/IEC 27000[2]; lei SOX[3]; COBIT; COSO[4]; ITIL[5]; entre outras (Arora, 2010), que disponibilizam um conjunto de

[2] A série ISO / IEC 27000 inclui normas de segurança da informação publicadas conjuntamente *pela International Organization for Standardization* e pela *International Electrotechnical Commission*

[3] A lei Sarbanes-Oxley, apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas organizações

[4] O COSO(*Committee of Sponsoring Organizations of the Treadway Commission*) é uma organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nos procedimentos e processos internos da empresa.

[5] Information Technology Infrastructure Library - é um conjunto de boas práticas para serem aplicadas na infraestrutura, operação e gerenciamento de serviços de tecnologia da informação.

importantes referências às organizações para uma aplicação apropriada (Kajava, Anttila, Varonen, Savola, & Roning, 2007).

Neste contexto iremos desenvolver as normas do COBIT, ITIL e a série ISO/IEC 27000, pelo motivo de serem consideradas as normas mais evidenciadas para uma boa implementação nas organizações, no contexto da segurança da informação (Susanto, Almunawar, & Tuan, 2011), assim como as suas respetivas as estruturas e adjacentes componentes de segurança da informação (COBIT 5 para segurança da informação, ITIL - *information security management* e ISO/IEC 27001).

A série ISO/IEC 27000 é considerada como conjunto de normas criadas com o objetivo de apoiar as organizações no que toca à segurança da informação. O seu uso ajuda a organização a gerir a segurança dos seus ativos, informação financeira, propriedade intelectual, assim como outros tipos de informação (ISO, 2018). Estas normas concedem às organizações um conjunto de diretrizes para apoiar na introdução, implementação e manutenção do sistema de gestão de segurança da informação, com o propósito de fornecer aos utilizadores uma base que seja comum a todos no que toca ao desenvolvimento de táticas e técnicas de segurança, assim como estabelecer a confiança nos relacionamentos intra e interorganização (NP ISO/IEC 27000, 2014).

A ISO 27001 é a norma mais conhecida na família ISO/IEC 27000 e fornece os requisitos para um sistema de gestão de segurança da informação. A criação desta norma foi baseada no objetivo de poder disponibilizar os "requisitos para estabelecer, implementar, operar, monitorizar, analisar criticamente, manter e melhorar de forma contínua um Sistema de Gestão de Segurança da Informação (SGSI), dentro do contexto da organização" (NP ISO/IEC 27001, 2013). Em paralelo, a ISO 27002 estabelece um conjunto de diretrizes e princípios gerais, tendo por base as boas práticas de gestão de informação, para que o utilizador possa analisar os requisitos de cada um dos controlos definidos na ISO/IEC 27001, tendo em atenção o ambiente dos riscos de segurança da informação da organização (NP ISO/IEC 27002, 2013).

A aplicabilidade destas normas não é obrigatória, como tal, algumas organizações optam por implementar, com objetivo de beneficiar com as práticas que estas normas especificam. "Os responsáveis de sistemas e tecnologias de informação reconhecem, cada vez mais, na adoção de referenciais de boas práticas e de standards universais uma mais-valia para o sucesso dos seus projetos" (itSMF-12ª Conferência Anual, 2015).

O ITIL pode ser designado como um conjunto de boas práticas que descreve como os recursos das tecnologias de informação podem ser organizados para acrescentar valor ao negócio, documentando os processos, funções e papéis dos seus intervenientes (AXELOS, 2017). A versão atual, foi publicada em 2011, sendo constituída por 5 livros, que se que se focam nas cinco seções fundamentais do ciclo de vida de um serviço. Este ciclo de vida é inicialmente composto pela definição do serviço e em seguida por uma análise dos requisitos do negócio nas fases de estratégia e de design do mesmo. Nesta análise dos requisitos é essencialmente valorizado o ambiente da organização na fase da transição do serviço, uma vez que o principal objetivo é o seu funcionamento e a melhoria contínua (Cartlidge, et al., 2007).

A ITIL prevê um processo de gestão da segurança da informação (ISM – *information security management)* cujos objetivos passam por garantir que:

> "As informações estão disponíveis para utilizar quando necessário, e os sistemas que a fornecem possam resistir adequadamente a ataques e recuperar ou evitar falhas (disponibilidade); as informações são observadas ou divulgadas apenas para aqueles que têm o direito de asaber (confidencialidade); as informações são completas, precisas e protegidas contra modificações não autorizadas (integridade); as transações comerciais, bem como as trocas de informações entre empresas ou parceiros, podem ser confiáveis (autenticidade e não-repúdio)" (bmc, 2017).

A gestão da segurança da informação, de acordo com a ITIL, é composta por cinco atividades principais: planeamento, implementação, avaliação, controlo e manutenção (ITGI, 2005). Deste modo, são alinhadas as TI com a segurança organizacional, garantindo que a segurança da informação seja efetivamente gerida em todos os serviços ou atividades de gestão de serviços (bmc, 2017).

Relativamente ao COBIT 5, este será discutido nos pontos 2.2, 2.2.1 e 2.2.2 do presente capítulo de uma forma mais detalhada uma vez que este guia de boas práticas será a base para o estudo de caso deste trabalho de projeto.

2.2. COBIT

O *Control Objectives for Information and Related Technology* (COBIT) é um guia de boas práticas apresentado como ferramenta para a gestão de tecnologias de informação, tendo sido publicado pela ISACA (*Information Systems Audit and Control Association*). A primeira versão deste framework surgiu em 1996, no entanto, têm sido muitas as edições lançadas posterior a essa, como podemos observar na linha do tempo representada na figura 2. A versão que vigora atualmente é a versão 5 do COBIT, publicada em 2012 (ISACA, 2012b).

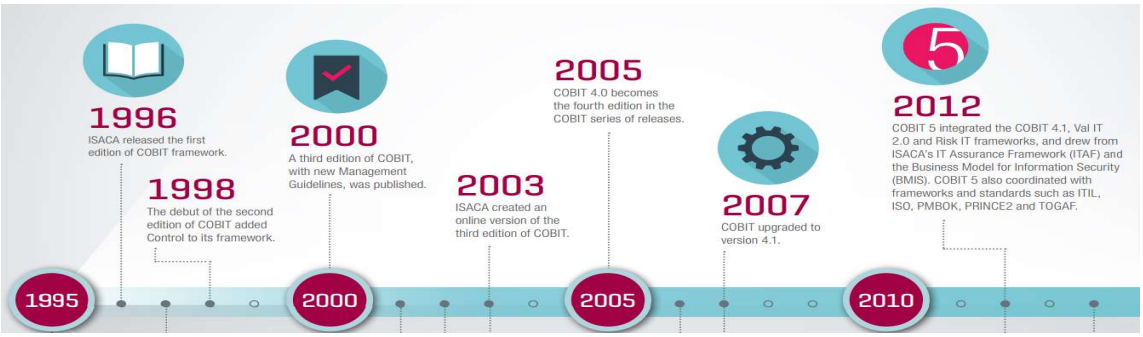

Figura 2– Time-line das edições do COBIT extraída e adaptada da ISACA (2016)

O COBIT 5 reflete o pensamento mais recente em técnicas de governação e de gestão, disponibiliza princípios, práticas, ferramentas analíticas e modelos globais aceites para ajudar a aumentar a confiança e o valor dos sistemas de informação das organizações. O COBIT 5 é uma versão expandida do COBIT 4,1, no entanto integra também outros grandes *frameworks*, padrões e recursos, incluindo o ISACA Val IT[6] e Risk IT[7], assim como ITIL e ISO (ISACA, 2017).

O COBIT é uma plataforma de possível adoção numa organização, tendo em conta o tipo de negócio e o impacto da tecnologia da informação no funcionamento da mesma. Esta ferramenta permite às organizações diminuir os riscos de negócio, o impacto dos requisitos de controlo e as dificuldades técnicas (ITGI, 2014).

O COBIT 5 apresenta cinco princípios básicos ao seu funcionamento. A orientação e especificação destes princípios é feita de uma forma detalhada através de instrumentos chamados de habilitadores de governação e de gestão das tecnologias de sistemas de

[6] Val IT é uma estrutura de governação que pode ser usada para criar valor comercial a partir de investimentos em TI.
[7] Risk IT é uma estrutura que fornece uma visão completa e abrangente de todos os riscos relacionados ao uso da tecnologia da informação.

informação da organização, divididos em sete categorias. Alem dos referidos cinco princípios e dos sete habilitadores, o COBIT5 contém ainda, um conjunto de trinta e sete processos, dos quais cinco deles estão associados á área de governação e os restantes trinta e dois à área da gestão (ISACA, 2012b). Será em seguida explicado em que consiste cada uma destas componentes referidas anteriormente.

O COBIT 5 é suportado por cinco princípios fundamentais, como está representado na figura 3:

Figura 3- 5 princípios fundamentais do COBIT (ISACA, 2017)

Com base no princípio de que a governação e gestão eficiente e eficaz das TI requerem que seja feita uma abordagem holística, tendo em conta os seus diversos componentes, o COBIT 5 estabelece um conjunto de sete categorias de habilitadores (figura 4). Os habilitadores podem ser definidos como fatores que, individualmente ou em conjunto, influenciam o desempenho da governação e gestão corporativa das TI (ISACA, 2012b).

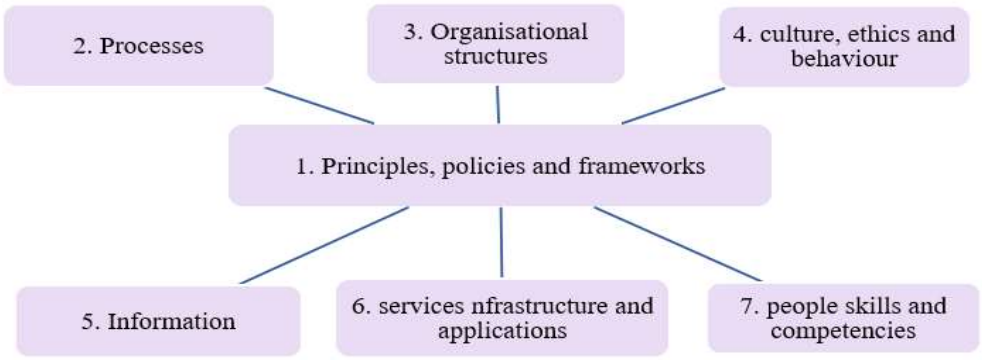

Figura 4– Habilitadores – Adaptado da ISACA (2012b)

Segundo a ISACA (2012b), estes domínios de habilitadores caracterizam-se da seguinte forma:

1. Princípios, Políticas e Modelos - correspondem a meios de explicação do comportamento que é desejado, através de orientações práticas para gestão diária.

2. Processos - correspondem a um conjunto de práticas e atividades para atingir e que produzir resultados para alcançar determinados objetivos.

3. Estruturas Organizacionais - correspondem às entidades responsáveis pela tomada de decisão da organização.

4. Cultura, Ética e Comportamento - domínio onde se enquadram todos os fatores diretamente relacionados com as pessoas.

5. Informação – corresponde às informações produzidas e utilizadas pela organização, considerada muitas vezes como produto, ao nível operacional;

6. Serviços, Infraestruturas e Aplicações – correspondem aos fatores que fornecem à organização a tecnologia e os serviços de TI.

7. Pessoas, Habilidades e Competências – correspondem aos recursos associados às pessoas e são essenciais para que, tanto as atividades como a tomada de decisão, sejam respetivamente bem-sucedidas a adequada.

A últimas três categorias de habilitadores (5, 6 e 7) são consideradas recursos ou capacidades TI da organização que devem ser geridos e governados, em conjunto com os restantes habilitadores. Uma gestão e utilização efetiva destes domínios em conjunto com as restantes práticas leva à criação de valor das TI (ISACA, 2012b).

Tal como é possível observar na figura 5, o modelo de referência de processos do COBIT5 está dividido em duas áreas principais de atividade – governação e gestão, divididas em domínios de processos e subdividido em trinta e sete processos.

Figura 5- Domínios e processos do COBIT entre as áreas de governação e gestão – retirado do ISACA (2012b)

Quanto aos cinco processos da área de governação, estes estão associados ao domínio avaliar, dirigir e monitorizar (*EDM - Evaluate, Direct and Monitor*). Em relação aos trinta e dois da área da gestão, estes dividem-se pelos domínios alinhar, planear e organizar (*APO - Align, Plan and Organize*), construir, adquirir e implementar (*BAI - Build, Acquire and Implement*), entrega, serviço e suporte (DSS - *Deliver, Service and Support)* e monitorizar, avaliar e aferir (*MEA - Monitor, Evaluate and Assess*) (ISACA, 2012b).

De um modo geral, estes quatro domínios da área da gestão, podem designar-se de uma forma mais simplificada, de acordo com as áreas de responsabilidade de planear, criar, executar e monitorar (PBRM), tal como é possível observar na figura 6:

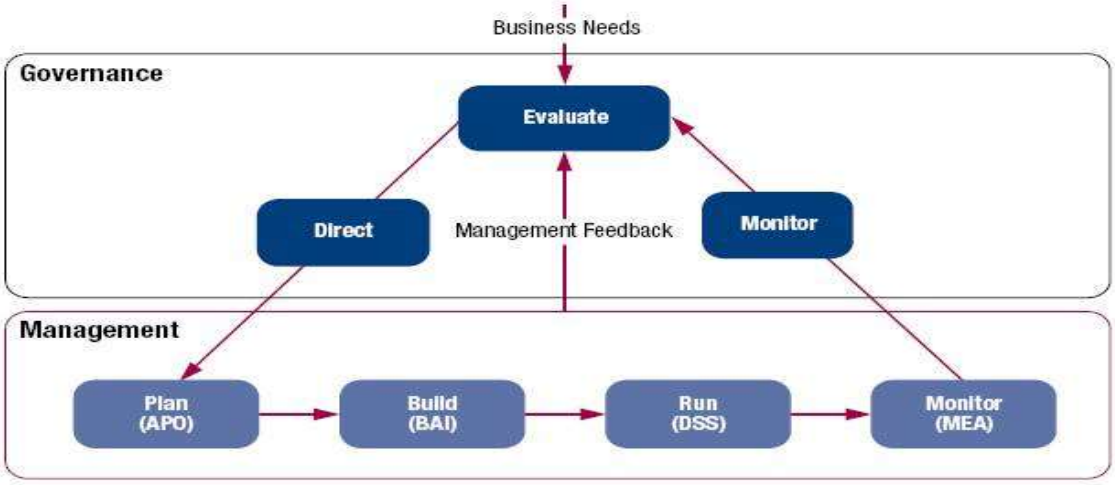

Figura 6– Domínios da área da governação e gestão – retirada da ISACA (2012b).

O COBIT 5 é considerado um framework genérico e útil para organizações de todos os tamanhos, quer sejam de carater comercial, sem fins lucrativos ou setor público. Considera-se que, para além deste, nenhum outro framework focalizado na tecnologia de informação corporativa oferece a sua amplitude ou benefícios. O COBIT 5 proporciona às organizações, os seguintes benefícios (ISACA, 2017):

- Manter informações de alta qualidade para apoiar as decisões empresariais
- Alcançar metas estratégicas através do uso eficaz e inovador da tecnologia da informação
- Alcançar a excelência operacional através de uma aplicação fiável e eficiente da tecnologia
- Manter o risco relacionado com a tecnologia da informação a um nível aceitável
- Otimizar o custo dos serviços de tecnologia da informação e tecnologia
- Apoiar o cumprimento das leis, regulamentos, acordos contratuais e políticas pertinentes

Apesar do COBIT 5 fornecer um conjunto de boas práticas, estas estão mais focadas nos controlos a aplicar do que na sua execução. Nele pode encontrar-se a informação que as organizações necessitam de adotar se eventualmente pretenderem implementar uma estrutura de governação e de controlos de TSI (ITGI, 2007). Uma vez que é um framework que não requer necessidade de ser implementado em conjunto com outros *frameworks*, considera-se que seja uma boa solução integrada por si só para os gestores (Arora, 2010).

2.2.1 COBIT 5 Segurança da Informação

Na versão do COBIT 5, é possível encontrar uma publicação mais focada na segurança da informação: o COBIT5SI (ISACA, 2012a).

O COBIT 5 para Segurança da Informação é o guia mais completo e atualizado que incorpora o COBIT com padrões e práticas globalmente aceites na atualidade, quanto à segurança da informação. Considera-se como um guia útil tanto para profissionais de segurança, como para os negócios ou utilizadores de TI em geral (Thomas, 2015).

Os principais motivos que conduziram para o desenvolvimento do COBIT 5 na segurança da informação incluem (ISACA, 2012a):

1. A necessidade de descrever a segurança da informação num contexto organizacional, tendo em conta a sua responsabilidade em todas as áreas da organização, a sua governação e gestão eficaz, e a sua relação e ligação com os objetivos da organização;
2. Uma necessidade crescente das organizações para:
   2.1. Manter a informação a um nível de risco aceitável e protege-la contra a divulgação não autorizada, modificações não autorizadas ou inadvertidas, e eventuais intrusões;
   2.2. Assegurar que os serviços e sistemas estejam continuamente disponíveis para os stakeholders, quer sejam internos ou externos, garantindo a satisfação do utilizador dos serviços de tecnologia da informação;
   2.3. Cumprir o crescente número de leis e regulamentações, bem como requisitos contratuais e políticas internas, providenciando transparência relativamente ao nível de conformidade;
3. A necessidade de se conectar e, quando pertinente, alinhar com outros grandes *frameworks* e padrões no mercado e entender como podem ser usados em simultâneo e de forma complementar ao abrigo do COBIT 5 para Segurança da informação;
4. A necessidade de vincular todas as principais pesquisas do ISACA, *frameworks* e orientações. A necessidade de vincular as principais ferramentas do ISACA, *frameworks* e orientação, com um foco primário no *Business Model for Information Security* (BMIS) e COBIT, mas também considerando *Val IT, Risk IT*, o *IT Assurance Framework (ITAF)*, a publicação *Board Briefing on IT Governance* e o *Taking Governance Forward (TGF).*

No COBIT 5, os processos *APO13 Manage security e DSS05 Manage security services* fornecem orientação básica sobre como definir, operar e monitorar um sistema de gestão de segurança geral. No entanto, a suposição feita nesta publicação é que a segurança da informação é generalizada em toda a organização, com aspetos de segurança da informação em todas as atividades e processos realizados. Portanto, o COBIT 5 para a segurança da informação fornece uma nova geração de orientação da ISACA sobre a governação corporativa e a gestão da segurança da informação (ISACA, 2012a).

O COBIT 5 SI segue os mesmos princípios do COBIT5 já referidos anteriormente, e descreve como os habilitadores podem ser postos em prática de forma a implementar uma governação e gestão de segurança da informação eficaz e eficiente. Os princípios de segurança comunicam as regras a seguir dentro da organização que servem de apoio ao alcance dos objetivos de governação definidos pelo conselho de administração e pela gestão executiva (ISACA, 2012a).

Em 2010, o ISACA, o ISF[8] e o ISC[9] uniram-se para desenvolver 12 princípios independentes que visam ajudar os profissionais de segurança da informação a adicionar valor às suas organizações (ISACA, 2012a). Esses princípios estão divididos em três módulos, especificadas na tabela 4. A descrição dos princípios, segundo o ISACA (2013b), pode ser encontrada nas tabelas 41 e 42 do Anexo I.

PRINCÍPIOS
Suporte ao Negócio
Foco no Negócio
Fornecer qualidade e valor aos Stakeholders
Cumprir com os requisitos legais e regulamentares relevantes
Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação
Avaliar atuais e futuras ameaças à informação
Promover a melhoria contínua da segurança da informação
Defender o Negócio
Adotar uma abordagem baseada no risco
Proteger informação confidencial
Concentrar-se nas aplicações de negócio críticas
Desenvolver sistemas de forma segura
Promover um comportamento responsável de segurança da informação
Agir de forma ética e profissional
Fomentar uma cultura positiva de segurança da informação

Tabela 4- Princípios recomendados no COBIT5SI adaptada de (ISACA, 2012)

[8] ISF - Information Security Forum
[9] ISC - International Information System Security Certification Consortium

As políticas, por sua vez, fornecem orientações mais detalhadas relativamente à forma como se deve pôr em prática os princípios seguidos pela organização. O COBIT5SI, sugere a existência de políticas no âmbito das funções de segurança da informação e das restantes funções existentes na organização, como constatado na tabela 5. A descrição das políticas, segundo o ISACA (2013b), pode ser encontrada nas tabela 43, 44 e 45 do Anexo I.

POLÍTICAS
Impulsionadas pela função de segurança da informação
Controlo de acesso
Pessoal de segurança da informação
Meio físico e ambiental de segurança da informação
Resposta a incidentes
Impulsionadas por outras funções dentro da organização
Continuidade do negócio e recuperação de desastres
Gestão de ativos
Regras de comportamento
Adquirir sistemas de informação, desenvolvimento e manutenção de software
Gestão de fornecedores
Gestão das operações e da comunicação
Conformidade
Gestão de Risco

Tabela 5- Políticas recomendadas no COBIT5SI adaptada de (ISACA, 2012)

Respetivamente aos processos, estes descrevem um conjunto de práticas e atividades para atingir os objetivos da organização. Esse conjunto, como é verificável na figura 7, é constituído por 37 processos que se encontram divididos inicialmente por duas áreas de atuação, governação e gestão, sendo depois divididos pelos 5 domínios já referidos anteriormente: EDM, APO, BAI, DSS e MEA.

Destes 37 processos, dois deles, no âmbito geral do COBIT, estão associados à segurança da informação: APO13 Gestão da Segurança, e DSS05 Gestão de Serviços de Segurança. No âmbito da publicação COBIT5SI, é apresentada informação específica de segurança relacionada com os diferentes processos de governação e gestão apresentados no COBIT. A descrição dos diferentes processos, segundo o ISACA (2013b), pode ser encontrada nas tabelas 46 à 77 do Anexo I do presente trabalho de projeto.

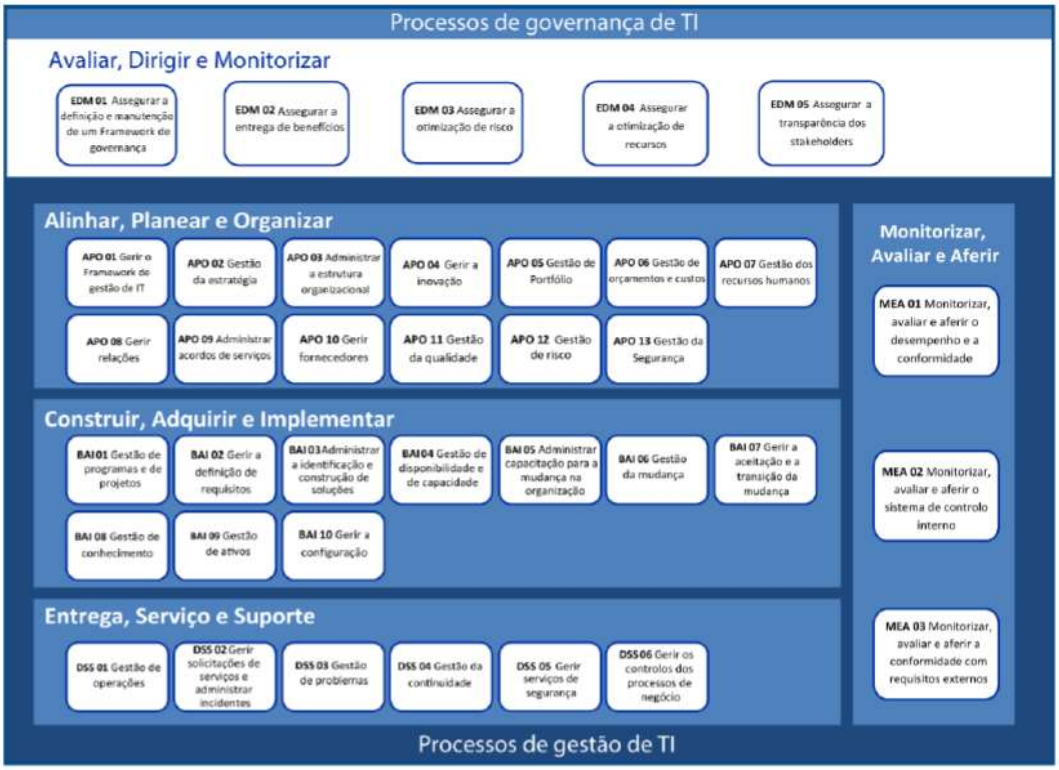

Figura 7- Representação dos 37 processos do COBIT e adjacentes domínios (adaptada de (ISACA 2012)

No que diz respeito às estruturas organizacionais, é de referir que são consideradas as entidades chave para a tomada de decisão dentro da organização. Este habilitador pretende que seja executado um conjunto de práticas associadas às diferentes funções, que ofereçam como resultado à organização a tomada de boas decisões. O COBIT5SI, recomenda a existência de certas funções ou estruturas dentro da organização que estejam diretamente relacionadas com a segurança da informação, especificadas na tabela 6.

FUNÇÕES / ESTRUTURAS ORGANIZACIONAIS
Diretor de Segurança da Informação (CISO)
Comité de Direção de Segurança da informação (ISSC)
Gestor de Segurança da informação (ISM)
Comité de Gestão do Risco do Negócio (ERM – Enterprise Risk Management)
Responsáveis pela informação / Proprietários da organização

Tabela 6 - Funções e/ou estruturas organizacionais recomendadas pelo COBIT5SI (adaptada da ISACA (2012))

Quanto à Cultura, Ética e Comportamento, o ISACA (2012a) prende a sua atenção no ciclo de vida cultural, na liderança, assim como no ambiente desejado. Este habilitador visa que os comportamentos devem ser medidos ao longo do tempo para se conseguir, desta forma, aferir a cultura de segurança na organização. Pode-se também encontrar uma lista de comportamentos sugeridos que influenciam positivamente a cultura de segurança da informação, como é possível observar na tabela 7.

A descrição dos diferentes comportamentos desejados segundo a ISACA (2013b), pode ser encontrada na tabela 79 do Anexo I do presente trabalho de projeto.

COMPORTAMENTOS DESEJADOS
A segurança da Informação é praticada nas operações diárias
As pessoas respeitam as políticas e princípios
É providenciada orientação suficiente e detalhada às pessoas e estas são encorajadas a participar e a desafiar a situação atual
Todos são responsabilizados pela proteção
Os stakeholders identificam e respondem às ameaças da organização
A gestão de topo apoia e antecipa inovações de forma proativa
A gestão do negócio empenha-se na obtenção de uma colaboração interfuncional continua
A gestão executiva reconhece o valor do negócio

Tabela 7 - Comportamento considerados no COBIT5SI como desejados numa organização adaptada da ISACA (2012)

Como já constatado anteriormente, a informação é um recurso valioso para as organizações e trata-se de mais um dos habilitadores apresentados pelo ISACA. No COBIT5SI, são analisados os diferentes tipos de informação de segurança relevantes, que podem ser consultados na tabela 9, assim como a relação com os stakeholders. Mais propriamente, quais são os stakeholders que aprovam, originam, são informados, ou utilizam os diferentes tipos de informação (ISACA, 2012a). A listagem de stakeholders sugerida no COBIT 5 para a Segurança da Informação pode ser consultada na tabela 8.

	Tipo de Informação									
Stakeholders	Estratégia de Segurança da informação	Orçamento da segurança da informação	Plano de segurança da informação	Políticas	Requisitos de segurança da informação	Material de conscienciatização	Relatórios de revisão de segurança da informação	Catálogo de serviços de segurança da informação	Perfil de risco da informação	Painel de segurança da informação
Interno: Organização										
Concelho										
Presidente e diretor executivo - CEO										
Diretor executivo de finanças - CFO										
Diretor das operações - COO										
Diretor de Risco - CRO										
Comité de Direção de Segurança da Informação-ISSC										
Diretor de Segurança da informação – CISO										
Executivos										
Sócios										
Comités de Direção de Projetos e Programas										
Direção da Estrutura										
Comité de Gestão do Risco do Negócio - ERM										
Chefe de Recursos Humanos										
Consultoria										
Auditoria										
Gabinete de gestão de projetos e programas – PMO										
Gabinete de gestão de valor - VMO										
Interno: TI										
Comité de Estratégia de TI										
Diretor da informação – CIO										
Chefe de Estrutura										
Chefe de desenvolvimento										
Chefe das Operações TI										
Chefe da administração de TSI										
Gestor de Serviços										
Gestor da Segurança da informação - ISM										
Gestor da continuidade de Negócio										
Diretor da Privacidade										
Externo										
Investidores										
Seguradoras										
Autoridade Legal										
Reguladoras										
Parceiros de Negócio										
Vendedores/ Fornecedores										
Auditores Externos										

Tabela 8 - Stakeholders que o COBIT5SI prevê existirem numa organização adaptada de ISACA (2012)

O ISACA aponta o tipo de informação relacionada com a segurança: a estratégia de segurança da informação, o seu orçamento, plano, requisitos, políticas e materiais de consciencialização, relatórios de avaliação e perfil de segurança da informação assim

como seu o painel de incidentes. É ainda referido o ciclo de vida da informação, a partir da perspetiva de segurança, que se inicia no planeamento e organização da informação, seguindo-se pelo uso da mesma. Posteriormente dá-se a monitorização dessa mesma informação para garantir que a informação ainda é viável, sendo que a fase final do ciclo de vida da informação se dá com o seu arquivo ou exclusão (ISACA, 2012a).

TIPOS DE INFORMAÇÃO
Estratégia de Segurança da Informação
Orçamento de Segurança da Informação
Plano de Segurança da Informação
Políticas
Requisitos de Segurança da Informação
Material de Consciencialização
Relatórios de Revisão de Segurança da Informação
Perfil de Risco da Informação
Painel de Segurança da Informação

Tabela 9 - Tipos de Informação de segurança da informação que o COBIT5SI recomenda adaptada de ISACA (2012)

Para que seja possível desenvolver serviços, infraestruturas ou aplicações é necessário identificar quais os recursos que são necessários para garantir a segurança da informação e as funções relacionadas à mesma. O COBIT5SI identifica uma lista de serviços relacionados com a segurança, na tabela 10, que têm um grande potencial de aparecer num catálogo de serviços de segurança, e para cada um deles apresenta descrições detalhadas, atributos e objetivos (ISACA, 2012a).

CATÁLOGO DE SERVIÇOS
Arquitetura de segurança
Consciência de segurança
Desenvolvimento seguro
Avaliações de segurança
Sistemas adequadamente configurados e seguros
Acessos dos utilizadores, consoante os direitos estabelecidos
Proteção adequada contra ataques externos e tentativas de intrusão
Resposta adequada a incidentes
Testes de Segurança
Serviços de monitorização e alerta

Tabela 10 - Serviços de segurança recomendados pelo COBIT5SI adaptada de (ISACA, 2012)

No sétimo habilitador, pessoas, skills e competências, o COBIT5SI apresenta sugestões de skills/competências que os colaboradores da organização devem ter. Os colaboradores a exercer funções na área de segurança da informação, devem ter conhecimentos de governação e formulação de estratégia de segurança da informação assim como de gestão

de risco da própria informação. Habilidade em desenvolver a arquitetura e as operações de segurança da informação, assim como a realização da avaliação, testes ou observância da informação é também uma mais-valia referida no framework de boas práticas. Encontram-se na tabela 11 o conjunto de skills acima referidos.

SKILLS/ COMPETÊNCIAS
Governação de segurança da informação
Formulação da estratégia de segurança da informação
Gestão de risco da informação
Desenvolvimento da estrutura de segurança da informação
Operações de segurança da informação
Avaliação, testes e observância da informação

Tabela 11 - Skills e Competências que o COBIT5SI considera importantes serem cobertas pelos colaboradores da organização adaptada de (ISACA, 2012).

2.2.2 COBIT 5 Segurança da Informação aplicado à cibersegurança

A cibersegurança evoluiu de várias fases distintas desde meados da década de 1990 até à atualidade. Cada uma destas fases é definida com um conjunto de características. Nessa época, as soluções encontradas para a gestão da segurança estavam direcionadas a produzir tanto software antivírus como correções direcionadas àquilo que seriam as vulnerabilidades e ameaças conhecidas (ISACA, 2013b).

Mais tarde, no período de 2000 a 2004, ocorreu uma evolução rápida da economia e do comércio eletrônico, no entanto, apesar do crescente número de vulnerabilidades e ameaças, assim como ataques, era dada uma atenção limitada à segurança da informação. Este facto levava a que os orçamentos destinados à segurança da informação sempre permanecessem baixos, acompanhando de longe todos os investimentos em processos de negócios eletrônicos (ISACA, 2013b).

Desde 2004 até ao ano de 2010, tornou-se conhecido o ato de cibercrime, sento que, a consciencialização assim como os gastos em segurança da informação, sofreram um enorme aumento. Neste contexto de orçamentos crescentes, este período caracterizou-se como uma recuperação, em que o foco seria consolidar e proteger a economia que cada vez mais se estaria a tornar dependente da informação e com infraestruturas críticas (ISACA, 2013b).

A partir de 2010, foi exponencial o crescimento do número de ameaças, cenários de risco e vulnerabilidades. A cibersegurança tornou-se um campo de interesse a nível político e

social, sento até mesmo considerada como essencial à sobrevivência e proveito organizacional (ISACA, 2013b).

Atualmente, a cibersegurança é frequentemente subdividida em quatro fases de um ciclo de vida contínuo (1º preparar; 2º investigar; 3º Corrigir e 4º transformar), o que acaba por ilustrar a natureza contínua do conceito de segurança. Manter o nível de segurança desejado dentro e ao redor de uma organização e seus associados é uma jornada de melhoria contínua. Para se defender com sucesso contra APTs e outras ameaças e vulnerabilidades críticas, a cibersegurança deve ser transformada num processo de negócio que esteja alinhado com as disposições de governação, gestão de risco e conformidade da organização (ISACA, 2013b).

Tal como já é sabido, o framework COBIT5 oferece um conjunto de publicações que incluem um conjunto de práticas prontas a serem seguidas por profissionais, no que diz respeito a espetos de segurança da informação. No entanto, a cibersegurança também se vai enquadrando no framework, à medida que evolui no sentido social e técnico.

Segundo a ISACA (2013b) é possível categorizar, priorizar e mapear as fases e medidas associadas à cibersegurança e seguidamente atribui-las aos diferentes processos e domínios do framework COBIT 5. A título de exemplo, as políticas de investimento em cibersegurança que podem ser associados aos processo EDM01, APO13 assim como nos princípios e politicas do framework COBIT 5.

O facto das políticas de cibersegurança se associarem ás do COBIT5, ajuda a que as organizações possam determinar um conjunto de soluções relevantes para as atividades de governação, gestão e garantia de cibersegurança.

No anexo I pode ser encontrada a base desta associação entre a cibersegurança e o framework COBIT 5, retirado da publicação do ISACA *Transforming cybersecurity using COBIT 5*, que servem como base do presente trabalho de projeto. Por questões de simplificação, a publicação do ISACA *Transforming cybersecurity using COBIT 5*, será apelidada nos próximos capítulos como “COBIT5TC”.

Capítulo III – Abordagem de Investigação/Descrição do projeto

3.1. Enquadramento do trabalho

A primeira motivação para iniciar este projeto surgiu no tema "Segurança da Informação" dada a enorme importância que este apresenta no contexto da auditoria interna. No sentido de acompanhar a atualidade e tendo em conta a posição que o ciberespaço tem ocupado nas organizações, verificou-se que, mais adequado do que verificar a segurança física e lógica da informação, seria verificar cibersegurança praticada. O principal objetivo não seria verificar a sua existência ou importância, mas sim a sua aplicabilidade em contexto organizacional.

Deste modo, a dificuldade associada à realização deste trabalho encontrava-se em achar uma forma de verificar a aplicabilidade da cibersegurança em contexto organizacional.

3.2. Metodologias e técnicas aplicáveis ao projeto

Segundo Teixeira (2006) o capítulo associado à metodologia é de extrema importância, uma vez que é através dela que se estuda, descreve e explicam os métodos aplicados ao longo do trabalho. O objetivo é sistematizar os procedimentos adotados durante as várias etapas, garantindo assim a validade e fiabilidade dos resultados obtidos.

Neste contexto, a metodologia de investigação consiste num processo onde de efetua a seleção da estratégia de investigação, seleção esta que condiciona a escolha das técnicas de recolha de dados. Estas escolhas devem ser adequadas aos objetivos que se pretendem atingir (Baptista & Sousa, 2011).

Segundo Fortin (1999) para elaborar um trabalho de investigação é necessário ter sentido crítico e questionar aquilo que já foi feito, pois é nesse sentido que depois se procura dar resposta às dúvidas e questões que possam surgir sobre determinado tema (Fortin, 1999). Face a isso, uma das primeiras questões a surgir foi "**de que forma se verifica a aplicabilidade de cibersegurança numa organização?".**

Existem várias formas de realizar uma investigação, porém, apenas conhecendo todas as alternativas é que se poderá escolher a mais adequada. A figura 8 demonstra as principais alternativas que poderão ser consideradas para definir o método de investigação.

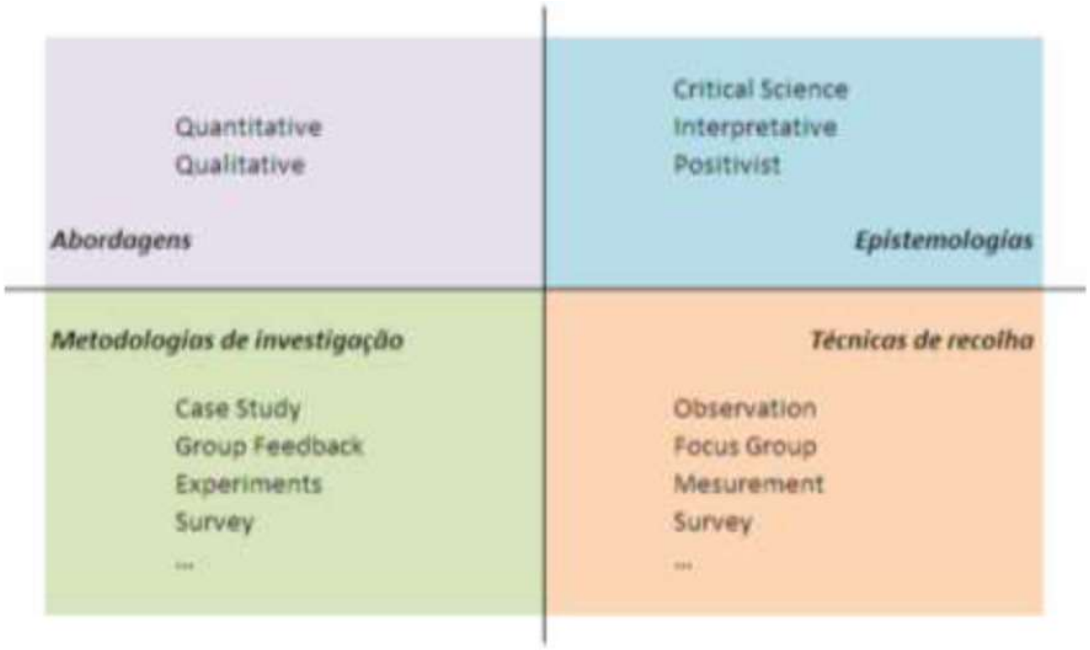

Figura 8 - Elementos de investigação em sistemas de informação - retirado de Grilo (2008)

Tendo em conta tipo de abordagem, esta poderá ser quantitativa ou qualitativa. A abordagem quantitativa tem por base a utilização da quantificação, quer na recolha dos dados como também no tratamento da informação, através da utilização de técnicas estatísticas. Tem como objetivo evitar possíveis distorções de análise e interpretação, possibilitando uma maior margem de segurança (Diehl & Tatim, 2004). A pesquisa qualitativa, por sua vez, descreve a complexidade do problema, através da compreensão e classificação dos processos dinâmicos vividos em grupo, o que possibilita a compreensão das diferentes particularidades dos indivíduos (Diehl & Tatim, 2004). Este método carateriza-se essencialmente pelo estudo de crenças, perceções, opiniões, representações e tem como intuito desenvolver conceitos, ideias, a partir dos dados encontrados (Minayo (Org), 2010).

Segundo Grilo (2008) "métodos de investigação quantitativa foram originalmente desenvolvidos em ciências naturais para o estudo de fenómenos naturais. Exemplos de métodos quantitativos são os *Survey, Experiments, Formal Methods e Numeric Methods*, em que os dados são recolhidos através de inquéritos, medições ou métodos matemáticos conhecidos". Relativamente aos métodos de investigação qualitativa, Grilo (2008) refere que "foram desenvolvidos em ciências sociais, para permitir aos investigadores o estudo de fenómenos sociais e culturais. São exemplos de métodos qualitativos *Action Research,*

Case Study e Ethnography, onde as origens de dados qualitativos incluem a observação, trabalho de campo, entrevistas ou documentos".

O estudo de caso é considerado o método com maior tendência para a análise de eventos contemporâneos, onde os comportamentos não podem ser de forma alguma manipulados. Uma das principais vantagens do estudo de caso encontra-se na capacidade de lidar com um conjunto abrangente de evidências distintas – "documentos, artefactos, entrevistas e observações*"* (Yin, 2009).

Assim sendo, considerou-se o estudo de caso a opção mais adequada para verificar a aplicabilidade de práticas de cibersegurança no contexto organizacional.

Relativamente à epistemologia, existem três interpretações diferentes: *Positivist, Interpretative e Critical Science.* A epistemologia *Interpretative*, assenta na tentativa da compreensão de valores, crenças e conceitos de eventos sociais, através de uma perceção de experiências e atividades humanas de juízo cultural (Grilo, 2008). Assim sendo, considera-se que o presente estudo é interpretativo, uma vez que se terá em consideração questões sociais, comportamentais e culturais, para verificar o desempenho e utilização de práticas de cibersegurança.

Segundo Yin (2009) o estudo de caso abrange algumas etapas:

- Planeamento – Etapa onde se desenvolvem as questões de investigação e a decisão da metodologia a utilizar.
- Desenho – Etapa de seleção da teoria que suportará o estudo, desenvolvimento das questões a abordar, a unidade de análise e o caso a ser estudado.
- Preparação – Etapa de preparação de competências como investigador e desenvolvimento do protocolo a seguir.
- Recolha de dados – Etapa em que se define qual a metodologia adequada para a recolha dos dados.
- Análise – Etapa de análise dos dados recolhidos.
- Partilha – Etapa de partilha das análises e conclusões do estudo de caso.

Tal como eferido anteriormente, na metodologia de estudo de caso são várias formas de recolha de dados: a documentação, registos, entrevistas, observação direta ou participativa e artefactos físicos. Dada a necessidade de verificar a aplicabilidade das práticas de cibersegurança através da recolha de informação empírica e análise de

documentação interna, considerou-se para este estudo de caso, a realização de entrevistas e observação direta.

Haguette (1997) define entrevista como “um processo de interação social entre duas pessoas na qual uma delas, o entrevistador, tem por objetivo a obtenção de informações por parte do outro, o entrevistado”. Haguette (1997) acrescenta ainda que a entrevista, como forma de coleta de dados, é a técnica mais utilizada no estudo de caso.

Segundo Sousa, Moreira & Vieira (2006) a vantagem principal da entrevista é "a possibilidade de se obterem informações detalhadas sobre valores, experiências, sentimentos, motivações, ideias, posições e comportamentos, entre outras características dos entrevistados". Durante a entrevista, o entrevistado desenvolve um processo de co-construção do conhecimento, reformulando os dados e interpretando-os para dar resposta às questões pretendidas. Neste sentido, os dados coletados vão além da objetividade pois vão sendo construídos em função das reflexões do sujeito sobre o que lhe é perguntado (Sousa, Moreira, & Vieria (Org), 2006).

A preparação da entrevista é uma das etapas mais importantes da investigação, destacando-se alguns cuidados fundamentais (Lakatos & Marconi, 1996):

- Planeamento da entrevista - deve ser feito tendo em conta o objetivo a ser alcançado;
- Escolha do entrevistado – ter o cuidado de selecionar alguém familiarizado com o tema em estudo;
- Oportunidade da entrevista - a disponibilidade do entrevistado em fornecer a entrevista para garantir a sua realização;
- Condições de confidencialidade – ajustar com o entrevistado as condições retrativas às confidências prestadas e da sua identidade;
- Preparação específica - organizar o roteiro ou formulário com as questões do estudo;

Segundo Haguette (1997) e Bauer e Gaskell (2017) existem três tipos de entrevistas e cada uma delas deve ser utilizada em diferentes situações para obter melhores resultados:

- Entrevista estruturada- é aquela que é realizada a partir de um roteiro previamente definido e deverá ser seguida pelo entrevistador.
- Entrevista não estruturada/aberta- é aquela em que não há qualquer roteiro pré-definido.
- Entrevista semi estruturada - é aquela em que, o roteiro pré-definido poderá ser acrescido de novas perguntas, a critério do entrevistador, caso o entrevistado apresente dados relevantes que não estavam previstos no roteiro original ou ainda, se o entrevistador achar que deve interromper o roteiro original para acrescentar novas questões.

Para este estudo, considera-se pertinente o uso da entrevista semi estruturada com roteiro previamente definido, onde não é descartada a possibilidade de serem acrescidas novas componentes que não estavam previstas no roteiro original.

3.3. Caracterização do Projeto

Nos pontos seguintes far-se-á uma apresentação do planeamento do projeto, descrição do trabalho realizado em cada uma das etapas e caracterização da organização estudada.

3.3.1. Planeamento do projeto

O presente estudo de caso foi devidamente planeado em quatro etapas distintas. Na figura 9, apresentam-se as etapas de trabalho, em função do prazo de elaboração e objetivo.

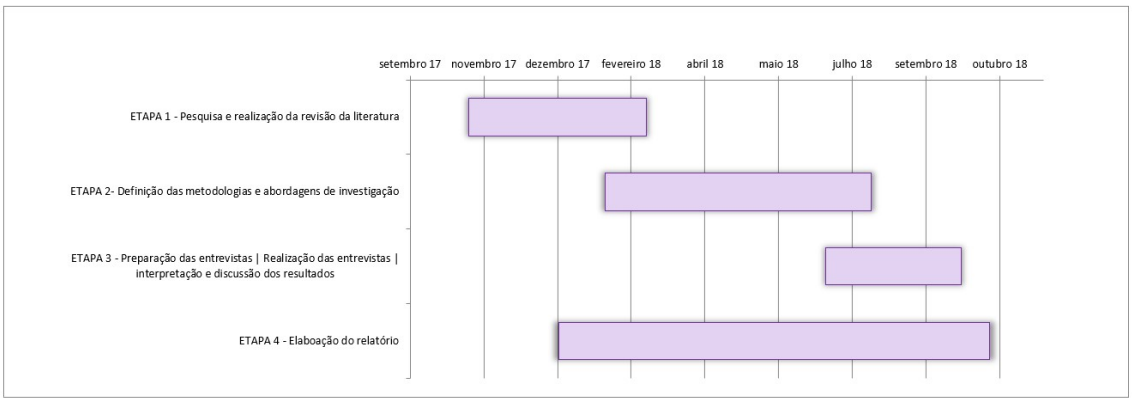

Figura 9- Etapas de planificação do projeto - elaboração própria

Neste contexto, estabeleceu-se que a ETAPA 1 corresponderia à revisão da literatura. Através da clarificação e discussão de ideias e conceitos alusivos ao tema, com o objetivo de entender de que forma seria possível verificar a aplicabilidade de cibersegurança numa organização. Esta etapa é o ponto de partida do trabalho, sem a qual nada será possível elaborar. Previu-se a concretização desta etapa durante os meses de novembro e dezembro de 2017, janeiro e fevereiro de 2018.

A ETAPA 2 destina-se à identificação e escolha das metodologias e abordagens de investigação, prevendo-se a realização entre os meses de fevereiro e julho. Tendo em conta que existem várias formas de realizar uma investigação, é fundamental que nesta etapa se estude todas as alternativas, para que se possa escolher a mais adequada. Uma vez que o método selecionado foi o de investigação qualitativa através de um caso de estudo, estabeleceu-se o cumprimento de algumas tarefas estabelecidas por Yin (2009):

A primeira tarefa engloba o planeamento das questões que se pretendem investigar, tendo em conta o COBIT5TC assim como a decisão da metodologia a utilizar. Dada a necessidade de verificar a aplicabilidade das práticas de cibersegurança através de recolha de informação empírica e análise de documentação interna, considerou-se realização de entrevistas e observação direta.

A tarefa seguinte é a de desenho, onde se desenvolvem as questões a abordar, define-se a unidade de análise e o caso a ser estudado. Nesta tarefa enquadra-se a elaboração de uma check list constituída pelas práticas que se pretendem verificar. É também definida que a unidade de análise será uma organização do tipo e-commerce e selecionam-se um conjunto de organizações possíveis para a realização do estudo.

Realizada a tarefa de desenho, inicia-se a ETAPA 3 com previsão de realização entre os meses de julho e setembro, onde ocorreria a preparação de competências como entrevistador e desenvolvimento do protocolo a seguir. Para a realização desta tarefa consideraram-se os cuidados fundamentais para a preparação de uma entrevista mencionados por Lakatos & Marconi (1996):

Em primeiro lugar é fundamental planear devidamente a entrevista. Neste sentido, e dada a dimensão da check list elaborada, considerou-se a necessidade de realizar seis reuniões com o entrevistado, com duração de pelo menos duas horas cada. Assim sendo, prevê-se que na primeira reunião ocorra, por parte do entrevistado, uma apresentação e descrição

da organização e, por parte do entrevistador sejam apresentados todos os pontos que se pretendem verificar na check list. As quatro reuniões seguintes destinam-se ao preenchimento da check list através da verificação das práticas e por fim, a última reunião destina-se à revisão do trabalho realizado e possíveis acertos a fazer.

Selecionada a organização para o estudo, a fase que se segue é a escolha do entrevistado e oportunidade da entrevista. Nesta fase planeou-se que o entrevistado deveria pertencer ao departamento de segurança de informação e possuir conhecimentos na área de auditoria de cibersegurança. Após a seleção do entrevistado, segue-se o agendamento da primeira reunião debatendo-se todas as condições de confidencialidade e possíveis datas para a realização da entrevista, tendo em conta disponibilidade do entrevistado.

No contexto da recolha de dados, planeia-se levar a check list em suporte papel onde são registados todos os factos que comprovem o cumprimento total, parcial ou não cumprimento das práticas de cibersegurança. A par disto, o mesmo documento será partilhado através da ferramenta "Google Sheets" e atualizado constantemente tanto pelo entrevistador como pelo entrevistado.

Finda a recolha de dados planeia-se a análise dos resultados e sua apresentação ao longo do capítulo IV e respetivas conclusões do estudo no capítulo V.

A ETAPA 4, destina-se à componente de escrita com a elaboração do relatório final. Esta etapa inicia-se durante a ETAPA 1 de pesquisa e revisão da literatura em janeiro e finda com as conclusões do estudo de caso, em outubro.

3.3.2. Descrição do trabalho realizado em cada uma das etapas

Uma vez que o objetivo da ETAPA 1 seria responder à questão "de que forma se verifica a aplicabilidade de cibersegurança numa organização?", procedeu-se então à revisão da literatura. A solução encontrada para responder a esta questão foi que, seria possível verificar a prática de segurança da informação, através adoção de *Frameworks* de gestão e governação das TI tais como: normas da série ISO27000, lei SOX, COBIT, COSO, ITIL, entre outros. No entanto, verificou-se que a adaptabilidade destes frameworks ao contexto da cibersegurança ainda não era muito desenvolvida, à exceção do COBIT 5, uma vez que o ISACA já se teria antecipado em desenvolver uma publicação intitulada de "*Transforming cybersecurity using COBIT5*". Assim sendo, optou-se por usar esta

publicação como base para a elaboração de um conjunto de recomendações de práticas de cibersegurança e verificar a sua aplicabilidade numa organização.

Tendo em conta o contexto de cibersegurança, foi facilmente constatável que aplicar este estudo numa *e-commerce* seria o mais adequado, dada a sua dependência pelas tecnologias da informação.

No final do mês de janeiro de 2018 considerou-se concluída a ETAPA 1 do trabalho. As principais dificuldades encontradas foram: encontrar matérias teóricas referentes à cibersegurança, uma vez que é uma temática bastante recente e ter acesso a documentos originais dos normativos acima referidos.

Posto isto, iniciou-se a ETAPA 2 do trabalho. Após uma análise cuidada ao COBIT5TC, constatou-se que o método mais ajustado para analisar o pretendido, seria através da realização e verificação de uma check list. O objetivo da check list seria verificar o cumprimento, cumprimento parcial ou não cumprimento das práticas de cibersegurança, em função da verificação de documentos e evidências.

Observando todas as práticas sugeridas pelo COBIT5TC, constatou-se que **diferentes processos, princípios ou políticas possuíam práticas semelhantes**. Assim sendo, uma única prática, pode comprovar o cumprimento ou não cumprimento de vários processos, políticas ou princípios distintos. Com isto, foi possível sintetizar todos as práticas recomendadas pelo COBIT5TC numa única check list com apenas 116 práticas, que poderá ser consultada nas tabelas 80 à 85 do anexo II.

Nos exemplos 1, 2 e 3 das tabelas 12, 13 e 14 respetivamente, pode observar-se a forma como se fez o tratamento das práticas do COBIT5TC e se chegou aos pontos encontrados na check list.

Exemplo1

PROCESSOS		CHECK LIST
APO13.02 Definir e gerir um plano de tratamento de riscos de segurança da informação	**- Identificar e categorizar o risco relacionado à cibersegurança e as opções de tratamento.** - Incorporar tratamento de risco de cibersegurança no plano geral de segurança da informação. - Identificar e listar todos os controlos existentes e inclui-los no tratamento e plano de risco de segurança da informação.	**Identificar e categorizar o risco relacionado à cibersegurança e as opções de tratamento**
APO03.03 Selecionar oportunidades e soluções.	**- Verificar todo e qualquer risco arquitetural decorrente de problemas relacionados à cibersegurança**, incluindo visão sistêmica sobre migração.	
APO05.06 Gerir a realização de benefícios.	**- Verificar e atualizar o perfil de risco de cibersegurança,** com base em dados de ataque / violação / incidente e respetiva resposta.	
APO12.02 Analisar o risco	- **Analisar o risco de cibersegurança** - Definir e manter cenários de risco relacionados à cibersegurança	
BAI02.03 Gerir risco de requisitos.	**- Definir e documentar o risco associado às soluções, incluindo o risco residual após a mitigação e possível exposição a ataques e violações.**	

Tabela 12 - Exemplo prático número 1 de compreensão à check list presente no Anexo II. Elaboração própria

Com isto, entendeu-se que, os processos APO13.02, APO03.03, APO12.02, BAI 02.03 e APO05.06 estão relacionados à identificação e categorização e tratamento do risco relacionado à cibersegurança. A análise e tratamento destes cinco processos deram origem ao ponto número 26 da check list (**Identificar e categorizar o risco relacionado à cibersegurança e as opções de tratamento**) presente no anexo II.

Exemplo 2

PROCESSOS		CHECK LIST
APO13.03 Monitorar e rever o SGSI	**- Definir processo de melhoria contínua para cibersegurança** - Incluir melhoria contínua nos conjuntos de controlo corporativo e social	**Definir o processo de melhoria contínua para cibersegurança**
APO01.07 Gerir a melhoria contínua dos processos.	- Fornecer plano e perspetiva para **melhorar a gestão de cibersegurança**, incluindo padrões emergentes e requisitos de conformidade	
DSS02.07 Rastrear status e produzir relatórios	- Consolidar dados e evidências de incidentes; obter lições aprendidas para cibersegurança; **definir melhorias e necessidades de transformação**.	

Tabela 13 - Exemplo prático número 2 de compreensão à check list presente no Anexo II. Elaboração própria

À semelhança do exemplo 1, no exemplo 2, entendeu-se que os processos APO13.03, APO01.07 e DSS02.07 se assemelham uma vez que os três têm por objetivo a definição de um processo de melhoria contínua para a componente de cibersegurança. A análise e tratamento destes três processos deram origem ao ponto número 108 da check list (**Definir o processo de melhoria contínua para cibersegurança)** presente no anexo II.

Exemplo 3

PROCESSOS		**CHECK LIST**
EDM01.02 Dirigir o sistema de Governação	- Atribuir uma **função de cibersegurança apropriada**, incluindo resposta a incidente e ataques.	**Atribuir a organização, função e responsabilidades de cibersegurança apropriada (uso do RACI – matriz das responsabilidades)**
APO01.01 Definir a estrutura organizacional	- Alinhar a organização à cibersegurança **nas funções de segurança** da informação e de risco da informação. **Definir modelo RACI** de alto nível para a função de cibersegurança, incluindo recursos externos. - Destacar qualquer obstáculo ou outra segregação organizacional de deveres / informações. Estabelecer uma plataforma / comitê apropriado para cibersegurança.	
APO01.02 Estabelecer funções e responsabilidades	**- Determinar obrigações, responsabilidades e tarefas de cibersegurança de outras funções organizacionais.** - Definir como se organiza a cibersegurança, alinhando funções e responsabilidades com a segurança geral da informação.	
APO01.06 Definir informações e propriedade do sistema	**- Definir funções e responsabilidades de cibersegurança**	

Tabela 14 - Exemplo prático número 3 de compreensão à check list presente no Anexo II. Elaboração própria

À semelhança dos exemplos anteriores, entendeu-se que os processos EDM01.02, APO01.01 APO01.02 e APO01.06 se assemelham uma vez que os quatro têm por objetivo a atribuição das funções e responsabilidades de cibersegurança. A análise e tratamento destes quatro processos deram origem ao ponto número 33 da check list (**Atribuir a organização, função e responsabilidades de cibersegurança apropriada (uso do RACI – matriz das responsabilidades))** presente no anexo II.

Tendo em conta a complexidade daquilo que é o framework COBIT, optou-se por excluir a análise de alguns habilitadores, dada a dificuldade que implicaria a sua análise. Como tal, deixou-se de parte a análise dos tipos de informação relacionadas à cibersegurança, os stakeholders da mesma, o existente catálogo de serviços e os skills/ competências associadas às estruturas organizacionais.

Na ETAPA 2 de trabalhos, realizada desde o final do mês de Janeiro de 2018 até meados do mês de Julho de 2018, as principais dificuldades encontradas foram: sintetizar todos as práticas recomendadas pelo COBIT5TC numa única check list com apenas 116 práticas.

Neste sentido, definido o roteiro para a entrevista como sendo uma check list e após seleção da organização em estudo, iniciou-se a ETAPA 3 do trabalho.

Tendo em conta o planeamento desta etapa, realizou-se a entrevista nos meses de agosto e setembro. Para a realização desta, foram realizadas seis reuniões, que se descrevem nos pontos seguintes:

- A primeira reunião realizou-se no dia 30 de agosto e teve durabilidade de uma hora. Nesta primeira reunião, o entrevistado fez uma apresentação oral relativamente à caracterização e constituição da organização tendo em conta os assuntos pertinentes ao propósito do estudo. Da parte do entrevistador foi apresentado oralmente o contexto do estudo de caso e qual a adequação deste com a organização, assim como também foi apresentada a check list. Nesta primeira reunião foram também discutidas as necessidades de confidencialidade ficando acordado que o entrevistador assinaria um acordo de não divulgação (NDA).
- A segunda reunião realizou-se no dia 11 de setembro e teve a durabilidade de duas horas e meia. Procedeu-se à assinatura do NDA (acordo de não divulgação) como compromisso de confidencialidade, assumindo-se assim a aceitação oficial do estudo de caso por parte da organização. Nesta reunião iniciou-se a verificação da check list.

No contexto da recolha de dados, foi levada a check list em suporte papel e, à medida que se verificava a existência de documentos que justificassem o cumprimento total, parcial ou não cumprimento das práticas de cibersegurança, a check list era preenchida com os símbolos ✓; + ; ✗ respetivamente, acrescida da referência às evidências documentais associadas. A par disto, o mesmo documento encontrava-se partilhado através da ferramenta "Google Sheets".

- A terceira, quarta e quinta reunião foram realizadas dos dias 19, 25 e 28 de setembro respetivamente, com durabilidade média de duas horas e destinaram-se à continuação do trabalho iniciado anteriormente. A par disto, e fora do horário

das reuniões, tanto o entrevistador como o entrevistado, trabalharam em cooperação, melhorando as respostas à entrevista, atualizando constantemente o documento partilhado digitalmente.

- A sexta e última reunião teve lugar no dia 11 de outubro e, tal como planeado, foram analisadas todas as respostas da check list e retificadas todas as que careciam de alteração.

Findas as entrevistas foi possível responder a todos os pontos da check list, assim como ter o conhecimento acerca da organização e a sua respetiva estrutura organizacional.

Nesta ETAPA 3 de trabalhos, a principal dificuldade foi adequar todos as práticas da check list ao contexto real da organização.

Relativamente ao cumprimento da ETAPA 4, esta foi cumprida numa linha temporal paralela à linha temporal das outras etapas, resultando na elaboração do presente documento. Esta etapa iniciou-se em janeiro de 2018 e findou com a conclusão do presente trabalho de projeto.

3.3.3. Caracterização da organização

A organização em estudo trata-se se uma e-commerce portuguesa que opera em diversos mercados internacionais. É considerada uma grande empresa e conta com o apoio de mais de 1000 colaboradores. A classificação de atividades económicas é a 63110, referente a atividades de processamento de dados, domiciliação de informação e atividades relacionadas. A organização inclui as atividades domiciliação de páginas Web, serviços de "*streaming*" ou domiciliação de aplicações, serviços de fornecimento de aplicações. As atividades de processamento de dados incluem o processamento de dados fornecidos pelo cliente ou provenientes de processamento automático e serviços de introdução de dados.

A principal missão da organização é ser uma plataforma tecnológica global que faça a perfeita conexão entre produtores e clientes. Dentro da organização, a principal prioridade é que todos os envolvidos estejam absolutamente focados nos objetivos e nos valores, que neste caso são três: otimização, sustentabilidade e disrupção.

Tem como visão criar um ecossistema único que possa atender a todas as necessidades dos consumidores e dos vendedores

. A plataforma eletrónica é constituída por um conjunto de tecnologias patenteadas e habilitadas por API (*application programming interface*) que fornece a base para os três principais componentes: aplicativos, serviços e dados.

Relativamente ao organograma, podemos verificar através da figura 10 que o departamento de segurança é constituído por quatro secções*: Security Applications, Security Infrastructures, incidence response* e *Auditing & complience.*

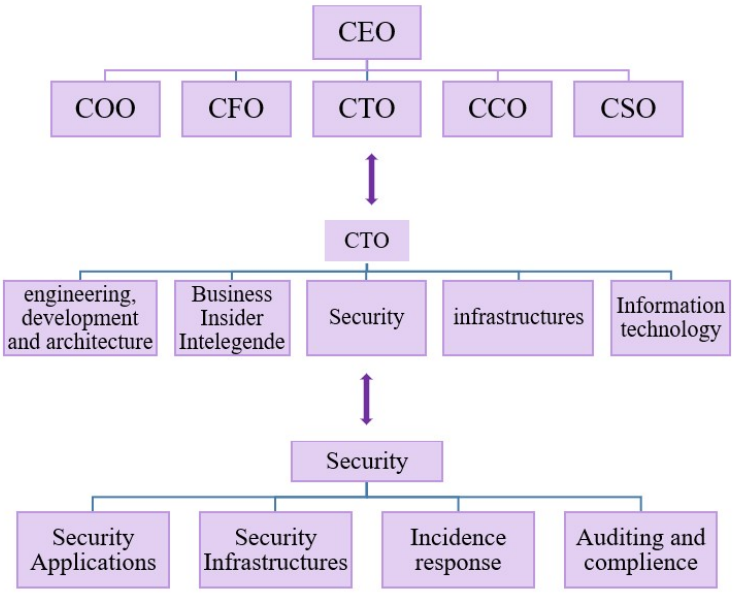

Figura 10- Organigrama da e-commerce estudada

Para a realização deste estudo de caso obteve-se colaboração do responsável pela secção de *Auditing & Complience,* assim como pelo responsável pelo departamento de *security*.

A grande maioria das entrevistas foram realizadas ao responsável pela secção de *Auditing & Complience.* Com mais de um ano de atividade na organização em estudo, é detentor de vários certicados: *Certified Information Systems security Professional (CISSP), Certified Ethical Hacker (CEH, Information Security) e Certification, ISSO 27001 Lead Auditor*.

Relativamente ao responsável pelo departamento de *security,* encontra-se a exercer funções na organização em estudo há quatro anos, totalizando oito anos de experiência na função de *Security Officer*. O seu contributo para o estudo esteve na resposta a algumas questões mais específicas às quais o responsável pela secção de *Auditing & Complience* não tinha conhecimento e fundamento para responder.

Capítulo IV – Apresentação e análise dos resultados

4.1. Resultados obtidos no estudo de caso

Com base no objetivo deste projeto, o principal foco esteve na verificação e avaliação de evidências que pudessem comprovar se as orientações apresentadas no COBIT5TC seriam cumpridas pela organização em estudo.

Dada a definição de cibersegurança, no capítulo 1.5.3, o intuito da realização de uma auditoria à cibersegurança, é verificar que a referida proteção assegura a disponibilidade, integridade e confidencialidade dos ativos em relação às ameaças do ciberespaço. Esta verificação passa pela análise das ferramentas, políticas, guias, abordagens de gestão de risco, ações de formação, boas práticas e tecnologias que podem ser usadas para proteção dos ativos da organização e de todos os utilizadores no ambiente virtual. Como já referido anteriormente, estes ativos e utilizadores incluem: dispositivos ligados em rede, aplicações e serviços, sistemas de telecomunicações e de comunicação multimédia e a informação transmitida e/ou armazenada no mundo virtual.

Dada a extensão e complexidade do framework COBIT5, optou-se por retirar a análise de alguns habilitadores. Como tal, foram analisados:

- Processos (ponto 4.1.1)
- Princípios de cibersegurança (ponto 4.1.2)
- Políticas de cibersegurança (ponto 4.1.3)
- Estruturas organizacionais (ponto 4.1.4)
- Cultura, ética e comportamento (ponto 4.1.5)

Nos pontos seguintes, é feita a discussão dos resultados em função dos pontos mencionados anteriormente.

4.1.1. Processos

Para facilitar o tratamento da informação assim como a verificação das práticas optou-se por subdividir esta análise em 21 categorias:

- 4.1.1.1. Existência de disposições legais e governo do sistema de cibersegurança
- 4.1.1.2. Tratamento de ataques, ameaças e vulnerabilidades - Preocupação com necessidade existenciais, lacunas, deficiências e fragilidades
- 4.1.1.3. Avaliação e tratamento do risco, apetite pelo risco e tolerância ao mesmo
- 4.1.1.4. Interligação entre cibersegurança e segurança da informação
- 4.1.1.5. Métricas e medidas de consciencialização
- 4.1.1.6. Reporte
- 4.1.1.7. Monitorização
- 4.1.1.8. Recursos
- 4.1.1.9. Confidencialidade e sigilo
- 4.1.1.10. Auditorias internas e externas
- 4.1.1.11. Controlos
- 4.1.1.12. Acessos / Identidade
- 4.1.1.13. Classificação e tratamento da informação
- 4.1.1.14. Inovação
- 4.1.1.15. Investimentos de cibersegurança
- 4.1.1.16. Recursos humanos
- 4.1.1.17. Serviços
- 4.1.1.18. Fornecedores
- 4.1.1.19. Programas e projetos de cibersegurança
- 4.1.1.20. Disponibilidade dos serviços
- 4.1.1.21. Mudança/ Melhoria contínua

Posto isto, apresentam-se nos pontos seguintes a discussão dos resultados pelas categorias acima mencionadas. As práticas encontram-se apresentadas sob forma de tabelas onde se discute o seu "cumprimento", "cumprimento parcial" ou "não cumprimento", representados pelos símbolos "✓","+" e "✗" respetivamente.

4.1.1.1. Existência de disposições legais e governo do sistema de cibersegurança

No COBIT5TC é salientada a importância da existência de um modelo de governo do sistema de cibersegurança, criado através da identificação e revisão de disposições legais e regulamentares existentes. O objetivo é obter um conjunto de requisitos a cumprir, relativamente a ocorrências que possam afetar o bom funcionamento das práticas de cibersegurança. O modelo de governo deve ser devidamente aprovado pela gestão da organização, a fim existir um compromisso da parte da gestão sobre o modelo de governo do sistema de cibersegurança existente.

É recomendado que este modelo contenha alguns pontos fulcrais, como por exemplo, o alinhamento entre o risco de cibersegurança e o modelo de governo geral da organização, assim como a aplicabilidade de normas e procedimentos chave de operacionalidade.

Na tabela 15 são identificadas as práticas recomendadas pelo COBIT5TC no contexto da existência de disposições legais e governo do sistema de Cibersegurança e a sua aplicação na empresa em estudo.

Nº	Requisito de Cibersegurança **Disposições legais e governo do sistema de cibersegurança**	Processo COBIT5	
1	Identificar e validar o modelo de governo do sistema de cibersegurança	EDM01.01	+
2	Identificar/Rever disposições legais e regulamentares existentes que possam influenciar no desenvolvimento do governo do sistema de cibersegurança, assim como os requisitos a cumprir, relativos a ocorrências que afetem a cibersegurança.	EDM01.01 MEA03.01	✓
3	Alinhar o risco de cibersegurança de acordo com o modelo de governo geral da organização	EDM03.03	✓
4	Aplicar normas e procedimentos chave de operacionalidade (KOP's)	Princípio 11	+
5	Obter compromisso de gestão para o modelo de governo ou de gestão selecionado	EDM01.02	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 15 - Práticas de existência de disposições Legais e Governo do sistema de Cibersegurança, adaptado da publicação do COBIT5TC

Relativamente à identificação e validação de um modelo de governo do sistema de cibersegurança, a organização não possui um modelo definido. No entanto existe um conjunto de documentos criados na mesma linha de pensamento onde estão definidas as políticas e práticas, estipulando assim um conjunto de procedimentos e outros elementos de orientação. Estes procedimentos vão respondendo a ocorrências que surgem à medida da necessidade existente.

A identificação e revisão das disposições legais e regulamentares existentes é realizada pelo departamento legal da organização. A par disto, a organização dá prioridade ao cumprimento de leis essenciais como: PCI-DSS (*Payment Card Industry – Data Security Standard)*; *General data protection Regulation*, *Lei Sarbanes- Oxley,* entre outras.
O alinhamento entre o risco de cibersegurança e o modelo geral de governo da organização é feito através do uso de OKR's (*objectives and Key Results*). Assim sendo, este alinhamento permite que o sistema de governo dos sistemas de segurança caminhe na mesma direção que o sistema geral de governo da organização, no que diz respeito ao cumprimento de metas e objetivos definidos.

No que diz respeito à prática número 4, referente à aplicação de normas e procedimentos chave de operacionalidade (KOP's), a organização segue um conjunto de "Políticas / Procedimentos / Metodologias", que cobrem o mesmo intuito, como é o caso, por exemplo do programa "Denial of service incidente procedure".

Por fim, dada a exigência de compromisso por parte da gestão da organização, todas as decisões de governo e de gestão tomadas pelo departamento de segurança da informação, carecem de aprovação superior, vendo assim assumido o compromisso anteriormente referido.

4.1.1.2. Tratamento de ataques, ameaças e vulnerabilidades - Preocupação com necessidade existenciais, lacunas, deficiências e fragilidades

É fundamental que uma organização saiba como identificar e caracterizar todas as ameaças, vulnerabilidade, ataques e riscos que possam afetar a atividade dos sistemas de informação

(Gaivéo, 2008).

Assim sendo, é importante que a organização faça a identificação de todas ameaças e vulnerabilidade que possam conduzir à ocorrência de ataques, a fim de poder evitá-los com a introdução de medidas necessárias.

Na tabela 16 é possível observar o conjunto de recomendações previstas no COBIT5TC assim como o cumprimento por parte da organização em estudo.

Nº	Requisito de Cibersegurança Ataques, ameaças e vulnerabilidades	Processo COBIT5	
6	Avaliar as ameaças e vulnerabilidades relevantes para a cibersegurança	EDM01.03	✓
7	Categorizar ataques e ameaças em termos de conformidade e necessidades regulatórias	EDM01.01	✓
8	Estabelecer escala de pontos para ataques, infrações e incidentes	EDM01.02 DSS02.02	✓
9	Identificar adaptabilidade, capacidade de resposta e resiliência em termos de ataques/violações de cibersegurança	EDM01.01	✓
10	Fornecer sugestões baseadas no risco em relação a possíveis ataques ou violações, sugerindo etapas e medidas de cibersegurança necessárias	APO04.05	✓
11	Definir vulnerabilidades relacionadas à cibersegurança e integrá-las nos relatórios de vulnerabilidade	BAI10.02	✓
12	Identificar os incidentes relevantes para a cibersegurança, proteger dados e todas as evidências potenciais	DSS02.04	✓
13	Investigar e diagnosticar ataques, violações e incidentes; incluir quase falhas e tentativas frustradas; estabelecer a causa raiz, se possível, e deduzir características comuns	DSS03.02	✓
14	Comparar acontecimentos atuais com o histórico de conhecimentos de ataques e violações	DSS05.03	✓
15	Identificar quaisquer elementos /frágeis ou lacunas que possam conduzir ao cibercrime ou ciberguerra	EDM01.01 DSS05.04	✓
16	Verificar as necessidades do negócio em relação a ataques e violações	EDM01.01	✓
17	Documentar deficiências sistémicas na cibersegurança	EDM01.01	✓
18	Definir o mecanismo de análise de lacunas para o risco de cibersegurança vs tratamento / controlos existentes	APO13.03	✓
19	Corrigir/ fechar lacunas através do processo formal de gestão de mudanças de cibersegurança.	APO02.04	✓
20	Determinar um modelo de tomada de decisão para a cibersegurança – prever respostas/recuperação ciberataques específicos (preparação, investigação, correção e erradicação de causas raiz)	EDM01.01 EDM01.02 APO12.05 DSS02.07	✓
21	Definir/planear propostas de projetos de cibersegurança (portfólio de ações)	APO12.05 BAI01.08	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 16 - Práticas associadas ao tratamento de ataques, ameaças e vulnerabilidades, adaptado do COBIT5TC

Relativamente à avaliação de ameaças e vulnerabilidades, a organização assume a existência e prática de dois mecanismos distintos: mecanismos automáticos realizados através de softwares próprios à função (ex: software de análise de vulnerabilidades – ASV) e mecanismos manuais. Os mecanismos manuais podem ser de origem interna, cujo objetivo é testar o nível de vulnerabilidade a nível interno (ex: *intern penetration testing* realizado pela equipa de resposta a incidentes) e nível externo (como se estivesse dentro ou fora da organização).

Finda a análise de vulnerabilidades, a categorização destas é feita através do uso de uma matriz de classificação de vulnerabilidades, onde é estipulada a sua a gravidade em função do tempo em que terá de ser eliminada, como pode ser observado na tabela 17.

Tipo de vulnerabilidade	Tempo para tratamento
Crítica	Current sprint
Alta	Next sprint or 2 weeks
Média	Next 3 sprints or 6 weeks
Baixa	Next 4 sprints or 8 weeks

Tabela 17 - Classificação dos tipos de vulnerabilidades associada ao tempo em que devem ser tratadas. Fornecido pela organização em estudo.

Em seguida, são realizados relatórios de vulnerabilidades que permanecem sujeitos à realização de auditorias de frequência semestral, a fim de verificar a conformidade do seu tratamento.

Face às lacunas existentes no processo de cibersegurança, a organização procede á sua correção através dum processo formal de gestão de mudanças, cuja designação é "*Change Management Developmente*", realizado com a frequência anual.

No que diz respeito aos ataques, infrações e incidentes, a organização procede à categorização dos mesmos, através uma escala de pontos, tendo em conta o seu impacto no nível de segurança da informação existente. Esta escala contém as seguintes classificações: *low; medium; high; critical; catastriphic*).

É fundamental assumir a potencial ocorrência de ataques e violações e prever de imediato como agir/responder. Como tal, a organização em estudo desenvolveu um plano para poder dar resposta a estes incidentes. Este plano é constituído por seis etapas de tratamento, como é possível observar na figura 11:

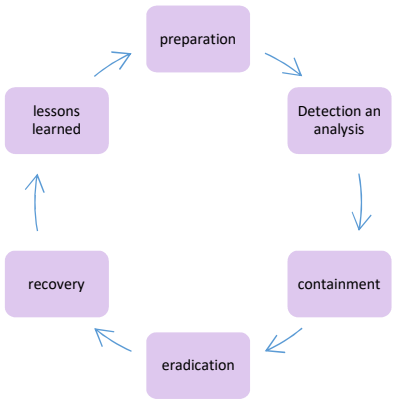

Figura 11- Plano de resposta a incidentes. Fornecido pela organização em estudo

Com base no plano apresentado na figura 11, a organização consegue realizar uma análise a fim de comparar acontecimentos atuais, que contenham o histórico de conhecimentos de ataques e violações passadas. Desta forma é também possível retirar lições de como atuar em acontecimentos futuros, com mesma causa raiz ou características comuns, sugerindo etapas, medidas e controlos de cibersegurança necessários.

Relativamente aos ataques e incidentes, são verificadas, através de um plano chamado *Risk impact level*, as necessidades comportamentais ao nível do negócio.

4.1.1.3. Avaliação e tratamento do risco, apetite pelo risco e tolerância ao mesmo

A cibersegurança existe para que o risco possa ser gerido, surgindo este, em função das ameaças e vulnerabilidades existentes. Através do risco é expressa a probabilidade de ocorrência de algum evento que possa ter impacto nos objetivos gerias da organização.

Assim sendo, é recomendado que toda a organização tenha claramente definido o seu perfil de risco assim como um conjunto de práticas associadas à forma como estes devem ser avaliados e tratados. A tabela 18 mostra o conjunto de práticas associadas à avaliação e tratamento do risco, apetite pelo risco e tolerância ao mesmo.

Nº	Requisito de Cibersegurança Risco, apetite pelo risco e tolerância ao mesmo	Processo COBIT5	
22	Coletar dados sobre riscos, ataques, violações e incidentes relacionados à cibersegurança, incluindo dados externos se apropriado	APO12.01 DSS02.02 DSS02.07	✓
23	Manter e transformar um perfil de risco de cibersegurança	APO12.03	✓
24	Identificar o nível de tolerância da organização em relação a ataques e violações	EDM01.02 EDM03.01	✓
25	Comparar os níveis de tolerância ao risco e comparar inconsistências entre a segurança da informação e a cibersegurança.	EDM03.01	✓
26	Identificar e categorizar o risco relacionado à cibersegurança e as opções de tratamento	APO13.02 APO03.03 APO05.06 APO12.02 BAI02.03	✓
27	Realizar e atualizar BIA (Business impact analysis) e avaliação de risco para vulnerabilidades /ameaças de cibersegurança e risco associado	DSS04.02	✓
28	Incorporar o tratamento de risco de cibersegurança no plano geral de segurança da informação	APO13.02	✓
29	Definir e manter cenários de risco de cibersegurança	APO12.02	✗
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 18 - Práticas associadas à avaliação e tratamento do risco, apetite pelo risco e tolerância ao mesmo, adaptado da publicação do COBIT5TC

A organização tem claramente definido o seu perfil de risco, assim como o seu nível de tolerância em relação à ocorrência de ataques e violações. Consoante o tipo de risco, a organização faz a gestão do mesmo, através de um processo chamado *Proposed treatment approach,* onde são discutidas as formas de tratamento do risco existente, dentro das opções: *accept, reduce, transform, avoid.*

Relativamente à identificação e categorização do risco assim como as opções de tratamento, a organização desenvolveu uma política onde o risco é categorizado em função de uma escala que avalia a sua gravidade. Consoante a classificação do risco, que pode ser classificado como muito baixo, baixo, modelado, alto ou crítico, é atribuída a responsabilidade de tratamento a diferentes estruturas da organização. Esta escala pode ser verificada na tabela 19:

Classificação	Escala	Responsável
Muito baixo	0 – 5	Head or Manager
Baixo	6 – 10	
Moderado	11 – 15	
Alto	16 – 20	VP or Directors
Crítico	21 – 25	CTO

Tabela 19 - Classificação do risco em função da gravidade e respetiva responsabilidade de tratamento. Fornecido pela organização em estudo.

Consoante o nível de risco, e através do *Business impact analysis* é realizada uma análise de impactos a vários níveis, dentro dos quais se destaca a análise dos impactos financeiros e impactos funcionais.

No seguimento desta temática, o COBIT5TC salienta a importância de definir e manter um conjunto de cenários possíveis de risco de cibersegurança por forma a evitar situações futuras indesejáveis. No entanto, a organização em estudo não aplica esta prática nas suas operações de cibersegurança.

4.1.1.4. Interligação entre cibersegurança e segurança da informação

É fundamental a existência de uma alta interligação entre a função de cibersegurança e a função de segurança da informação. Uma vez que na organização em estudo não existe um departamento específico de cibersegurança, a função é assegurada pelo departamento de segurança da informação. Como tal, é garantida a presença de interligação entre estas duas componentes. Neste contexto, encontram-se na tabela 20 as recomendações do COBIT5TC:

Nº	Requisito de Cibersegurança **Interligação entre cibersegurança e segurança da informação**	Processo COBIT5	
30	Estabelecer e assegurar a participação do comité ao nível da cibersegurança (ISSC)	EDM01.02 APO01.01	✗
31	Integrar a direção da cibersegurança na direção geral de segurança da informação	EDM02.01	✓
32	Estabelecer ligação/comunicação entre a função de cibersegurança e outras funções de segurança da informação (Alinhar as duas funções)	EDM01.02 APO01.01	✓
33	Atribuir a organização, função e responsabilidades de cibersegurança apropriada (uso do RACI – matriz das responsabilidades)	EDM01.02 APO01.01 APO01.02 APO01.06	✗
34	Identificar e definir formalmente os direitos de decisão para a organização de cibersegurança, incluindo os que possam ser aplicáveis em situações de tratamento de crises /incidentes	APO01.01	+
35	Definir e comunicar metas e objetivos de cibersegurança ao nível estratégico e inclui-los na estratégia de segurança. Fornecer e incluir marcos e datas de conclusão para metas e objetivos de cibersegurança	APO02.05 APO12.04 BAI05.01	✓
36	Definir requisitos de cibersegurança como um subconjunto de requisitos gerais de segurança da informação	BAI02.01	✓
37	Fornecer política de cibersegurança e padrões subsidiários alinhados e integrados com o conjunto geral de políticas de segurança da informação	APO01.03	✓
38	Interligar as políticas de segurança da informação aos princípios orientadores para a cibersegurança	Política 1	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 20 - - Práticas associadas à interligação entre as funções de cibersegurança e segurança da informação, adaptado da publicação COBIT5TC

Uma vez que não existe um departamento de cibersegurança claramente definido, pode considerar-se que a direção de cibersegurança encontra-se completamente integrada na direção geral de segurança da informação. Assim sendo, é afirmável que os requisitos de cibersegurança encontram-se definidos como um subconjunto de requisitos gerais de segurança da informação, assim como, o facto de as políticas de cibersegurança e padrões subsidiários estarem alinhados e integrados com o conjunto geral de políticas de segurança da informação.

No que diz respeito às funções de cibersegurança, o COBIT5TC defende que a organização deve possuir um *Information security steering committee* (ISSC) que participe ativamente na atividade de cibersegurança. Esta prática não se verifica na organização em estudo, uma vez que não há existência do referido *information security steering committee*. Esta prática será discutida posteriormente no ponto 4.1.4 - Estruturas Organizacionais.

No seguimento da mesma temática é ainda recomendado que a organização atribua aos membros responsáveis pela cibersegurança, funções e responsabilidades de cibersegurança apropriadas. Constatou-se que esta prática não é inteiramente cumprida

pela organização, uma vez que as funções e responsabilidades não se encontram claramente definidas e documentadas. A existência de atribuição de responsabilidades é feita em situações de tratamento de risco que, dependendo do nível deste, a responsabilidade de tomada de decisão varia.

Por fim, e no contexto da prática número 35, verificou-se que é devidamente feita a definição e comunicação das metas e objetivos de cibersegurança ao nível estratégico no contexto da realização do plano anual destinado à cibersegurança. Esta definição e comunicação de metas e objetivos é realizada através de mapas de ações com o respetivo prazo de realização.

4.1.1.5. Métricas e medidas de consciencialização

Desenvolver um programa de consciencialização e instrução sobre cibersegurança, é uma das práticas recomendadas pelo COBIT5TC. Na tabela 21 encontram-se as recomendações de cibersegurança, no contexto da definição de métricas e medidas de consciencialização:

Nº	Requisito de Cibersegurança Métricas e medidas de consciencialização	Processo COBIT5	
39	Definir o cenário para consciencialização de cibercrime e ciberguerra	EDM01.02	✗
40	Desenvolver um programa de consciencialização e instrução sobre cibersegurança, incluindo elementos baseados no risco	APO01.04 APO07.03	✓
41	Integrar medidas e métricas de cibersegurança em mecanismos de verificação e avaliação rotineira da conformidade. Identificar e anotar exceções à conformidade que possam ser necessárias.	EDM01.03 APO01.08	✗
42	Incluir medidas financeiras (impacto, danos) e não financeiras (legal, reputação, operacional, outras) para descrever o valor agregado das iniciativas de cibersegurança	EDM02.02	+
43	Obter aprovações necessárias para soluções, medidas e requisitos de cibersegurança; incluindo aceitações de risco para exposição remanescente a ataques, violações e incidentes (junto de quem financia assim como os stakeholders – estudos de viabilidade ou análises de risco)	BAI02.04	✓
44	Atualizar as soluções de cibersegurança de acordo com as necessidades do negócio e requisitos operacionais (planos de manutenção/ revisões periódicas)	BAI03.10	✓
45	Desenvolver etapas, ações e medidas detalhadas de cibersegurança para abordar o risco e incorporá-las ao sistema de cibersegurança (iniciativas)	BAI03.02 BAI05.05	+
46	Estabelecer testes apropriados, incluindo os ambientes de área restrita, para testar ações relacionadas à cibersegurança	BAI07.04	✓
47	Definir ações corretivas relacionadas a ataques/violações/ incidentes; incorporar quaisquer ações corretivas e planos relacionados com a transformação geral de cibersegurança	MEA01.05	✓
48	Adotar a mentalidade do atacante – maior estrago com menor esforço		✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 21 - Práticas associadas à introdução de métricas e medidas de consciencialização, adaptado da publicação COBIT5TC.

Uma vez que a consciencialização e instrução sobre cibersegurança é considerada uma mais valia, verifica-se na organização em estudo uma preocupação existente neste sentido. Com objetivo de dar orientação aos colaboradores das áreas mais críticas, foi desenvolvida uma plataforma cujo nome é *security awareness*, para fornecer informação sempre atual e útil que possa apoiar as medidas e métricas utilizadas no contexto da cibersegurança. Neste contexto, na apresentação de novas iniciativas de cibersegurança, é dada uma relevância maior ao valor das medidas não financeiras que expressam o impacto legal, ao nível da reputação e operacional do que propriamente às medidas financeiras. No entanto, a organização não adota a prática de definir cenários para consciencialização relativa a cibercrime e ciberguerra, tal como surge na prática número 39.

Apesar da organização conter um conjunto de medidas e métricas de cibersegurança, não se verifica a prática de mecanismos de verificação e avaliação rotineira da conformidade. Desde o momento em que uma medida é inserida no protocolo de cibersegurança, o processo de avaliação/verificação apenas se realiza caso se observe alguma deficiência.

Relativamente ao desenvolvimento de etapas, ações e medidas detalhadas de cibersegurança para abordar o risco, estas vão sendo inseridas à medida que surge a necessidade de as incorporar no processo de cibersegurança. Contudo, no momento em que for necessário cria-las e incorpora-las na cultura da organização, estas são devidamente testadas, aprovadas e inseridas no plano de resposta a incidentes com medidas corretivas e consequente transformação do processo geral da cibersegurança da organização.

4.1.1.6. Reporte

A componente de reporte, em qualquer que seja a organização, é uma componente fundamental, para que os stakeholders, quer a nível interno como externo, possam acompanhar o conjunto de previsões, ações e devidas conclusões. Neste sentido, a publicação COBIT5TC recomenda o conjunto de práticas observáveis na tabela 22, respeitantes ao reporte/elaboração de relatórios.

Nº	Requisito de Cibersegurança Reporte	Processo COBIT5	
49	Identificar os meios e canais para comunicar questões e soluções de cibersegurança	EDM05.01	✓
50	Incorporar o reporte de cibersegurança nos métodos genéricos de segurança da informação	EDM02.02	✓
51	Identificar os requisitos que devem compor um relatório de cibersegurança	EDM05.01	✓
52	Alinhar e priorizar os requisitos de relatórios às necessidades dos stakeholders internos e externos	EDM05.01 EDM05.02	✓
53	Fornecer relatórios sobre projetos de cibersegurança, com referência específica a pontos fracos decorrentes de novas formas de cibercrime e ciberguerra	BAI01.11	✓
54	Preparar relatórios de desempenho de cibersegurança	APO09.05	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 22 - Práticas associadas ao reporte de cibersegurança, adaptado da publicação TCU-COBIT 5

A organização realiza o constante reporte dos acontecimentos atuais, como é o caso relatórios de desempenho de cibersegurança com periodicidade trimestral. Para a elaboração destes, estão definidos um conjunto de componentes obrigatórios ou facultativos, tendo em conta quem lê esses relatórios, quer a nível interno (outras estruturas organizacionais) como externo (caso dos auditores externos).

Todos as alterações ao nível da cibersegurança são devidamente reportadas assim como, aquando da estruturação de novos projetos relacionados à cibersegurança, é feito um relatório descritivo onde são incluídos os objetivos, benefícios, possíveis pontos fracos e vulnerabilidades decorrentes de novas formas ataques, tal como indica na prática número 53

De uma forma geral, é possível ainda concluir que a organização realiza uma boa identificação dos meios e canais para comunicar questões e soluções de cibersegurança.

4.1.1.7. Monitorização

Mais importante do que implementar qualquer medida ou controlo de cibersegurança numa organização é efetuar um posterior acompanhamento, a fim de comprovar a sua eficácia e eficiência. A publicação COBIT5TC define um conjunto de práticas de monitorização a várias vertentes do processo de cibersegurança, como é possível observar na tabela 23.

Nº	Requisito de Cibersegurança Monitorização	Processo COBIT5	
55	Acompanhar os resultados e efeitos da cibersegurança, relativamente às mudanças nos ataques, ameaças e incidentes. Comparar os resultados com as expectativas iniciais (atualidade) e futuro e outros marcos passados	EDM02.03	✓
56	Integrar e medir o nível de integração da avaliação e gestão de risco de cibersegurança com gestão geral de risco de informação.	EDM03.01 EDM03.02 EDM03.03	✓
57	Monitorizar a conformidade das medidas e métricas de cibersegurança que não fazem parte dos mecanismos regulares e rotineiros	EDM01.03	✗
58	Monitorizar o perfil de risco para ataques/ameaças e o apetite de risco correspondente para alcançar um equilíbrio ótimo entre riscos de cibersegurança e as oportunidades de negócio	EDM03.03	✓
59	Estender as regras de monitorização para cobrir todos os requisitos de cibersegurança; Definir métodos analíticos apropriados para coletar dados de desempenho e conformidade e incluir especificamente a monitorização de ataques e violações reais ou potenciais.	DSS01.03 MEA01.03	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 23 - Práticas associadas à monitorização das práticas de cibersegurança, adaptado da publicação TCU-CONBIT5

Observando a tabela 23, verifica-se por parte da organização em estudo, a preocupação em acompanhar os resultados e efeitos da cibersegurança, tendo em conta a mudanças observadas ao nível dos ataques, ameaças e incidentes. Através da componente de *lessons learned* do processo observado na figura 11, a organização projeta medidas futuras tendo em conta os resultados e as expectativas iniciais.

Respeitante às medidas de cibersegurança que não fazem parte de mecanismos regulares do dia a dia, não se verifica o devido acompanhamento destas. A sua alteração é apenas efetuada em função de necessidades momentâneas observadas, caso se verifique que estas já não se encontrem em conformidade com a sua utilidade.

No contexto da prática número 58, já se observa uma maior preocupação em acompanhar constantemente o perfil de risco da organização face a possíveis ataques e ameaças. De um modo geral, verifica-se a nível da componente de monitorização, uma cobertura completa a todos os requisitos de cibersegurança. Embora este processo seja abrangente a toda a organização, a atenção é fundamentalmente dada a situações mais críticas.

Relativamente à definição de métodos analíticos apropriados para coletar dados de desempenho, estas práticas apenas se observam em algumas componentes, como é o caso de análises de risco face a ataques e violações reais ou potenciais.

4.1.1.8. Recursos

Uma vez os recursos são a base para o desempenho de uma organização é necessário que se efetue uma boa gestão destes. Com base na publicação COBIT5TC, é fundamental que aquando da sua aquisição esta seja devidamente validada em função de metas ou objetivos específicos que os justifiquem. Posteriormente, é necessário avaliar constantemente a eficácia destes, tendo em conta as necessidades pelas quais foram adquiridos assim como pelo cumprimento dos objetivos e metas definidas. Apresentam-se na tabela 24 o conjunto de práticas associadas à validação e eficácia dos recursos de cibersegurança:

Nº	Requisito de Cibersegurança Recursos	Processo COBIT5	
60	Avaliar a eficácia dos recursos de cibersegurança, em comparação com as necessidades de segurança da informação e risco da informação (incluindo recursos externos)	EDM04.01 EDM04.02	✓
61	Validar recursos de cibersegurança em termos de metas e objetivos específicos (incluindo recursos externos)	EDM04.02	✓
62	Medir a eficácia dos recursos de cibersegurança (interna e externa) relativamente às necessidades, objetivos e metas definidas pela segurança da informação	EDM04.03	✓
63	Desenvolver uma linha base de recursos para cibersegurança, incluindo critérios e indicadores de desempenho (KPI's)	APO02.02	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 24 - Práticas associadas aos recursos de cibersegurança necessários, adaptado da publicação COBIT5TC5

Aquando da necessidade de qualquer que seja o recurso, como por exemplo um software específico para apoio às práticas de cibersegurança, a organização em estudo valida a sua necessidade em função dos resultados passados e metas futuras.

Relativamente aos recursos já presentes na organização, são periodicamente realizadas análises de desempenho, tendo em conta indicadores e critérios, a fim de avaliar a sua eficácia relativamente às necessidades, objetivos definidos e riscos associados ao seu desempenho.

4.1.1.9. Confidencialidade e sigilo

Impedir a divulgação de informação confidencial deverá ser uma das maiores preocupações ao nível da segurança da informação. Neste sentido, e tendo em conta que nem toda a informação é de acesso restrito, é necessário incorporar no processo de reporte e permissão de acesso à informação, todas as necessidades de confidencialidade e sigilo. Neste sentido, o COBIT5TC recomenda que as organizações definam de antemão todas

as necessidades de confidencialidade e sigilo, aquando a ocorrência do processo de definição dos stakeholders.

Nº	Requisito de Cibersegurança Confidencialidade e sigilo	Processo COBIT5	
64	Incorporar as necessidades de confidencialidade e sigilo no processo de identificação dos stakeholders	EDM05.01	✓
65	Definir e observar formalmente os requisitos de confidencialidade e sigilo para auditores externos	EDM05.02	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 25 - Práticas associadas às práticas de confidencialidade e sigilo, adaptado da publicação COBIT5TC

A organização em estudo tem a preocupação em analisar e incorporar as necessidades de confidencialidade e sigilo no processo de partilha da informação. Estas necessidades são automaticamente definidas no processo de identificação dos stakeholders. Para cada stakeholder existem práticas diferentes. A título de exemplo, no caso da partilha de informação para a elaboração deste projeto, foi utilizada uma NDA (*non-disclosure agreement)*, um acordo de não divulgação/termo de confidencialidade.

4.1.1.10. Auditorias internas e externas

Realizar a revisão dos sistemas de segurança, quer seja através de auditorias internas ou externas, é crucial para comprovar que estes realizam as funções e operações para as quais foram criados, assim como comprovar se os dados e demais informações neles contidos correspondem aos princípios de fiabilidade, integridade, precisão e disponibilidade.

Assim sendo, a publicação COBIT5TC recomenda a realização de auditorias internas e externas para avaliar a eficácia do programa de governo de cibersegurança, assim como uma definição antecipada das instâncias de dependência do trabalho dos auditores externos, como é possível observar na tabela 26.

Nº	Requisito de Cibersegurança Auditorias internas e externas	Processo COBIT5	
66	Realizar auditorias internas e externas para avaliar a eficácia do programa de governo de cibersegurança.	EDM05.02	✓
67	Definir e articular as instâncias de dependência do trabalho de terceiros (para auditores externos)	EDM05.02	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 26 - Práticas associadas à realização de auditorias internas e externas de cibersegurança, adaptado da publicação COBIT5TC.

Com base naquilo que foi discutido na entrevista, a organização está sujeita a auditorias internas e externas regulares a fim de avaliar a eficácia de todos os processos de cibersegurança existentes.

4.1.1.11. Controlos

Implementar controlos de segurança numa organização, depende da criação e divulgação de um conjunto de boas práticas e comportamentos que sejam percebidos e adotados por todos os elementos da mesma. Da mesma forma que é importante implementa-los, também é fundamental motivar os usuários a aplicá-los (Workman, Bommer, & Straub, 2008) citado por (Pimenta & Quaresma, 2016).

A criação de um sistema de Gestão de Segurança da informação também é uma prática recomendada por vários autores assim como pela publicação COBIT5TC uma vez que a sua implementação promove a segurança no uso de seus ativos.

Na tabela 27 encontram-se as principais práticas recomendadas pelo COBIT5TC, relativamente à criação e implementação de controlos de cibersegurança.

Nº	Requisito de Cibersegurança **Controlos**	Processo COBIT5	
68	Definir relação entre os controlos de cibersegurança e os controlos genéricos de segurança da informação e incorporá-los no SGSI geral	APO13.01	✓
69	Identificar e listar todos os controlos existentes e inclui-los no tratamento e plano de risco de segurança da informação	APO13.02	+
70	Recolher potenciais pontos de entrada (conectividade) a todos os níveis e tipologias de rede, categorizá-los e identificar os controlos relacionados existentes	DSS05.02 DSS05.03 DSS05.05 DSS05.06	✓
71	Definir rotinas de verificação/verificações aleatórias, conforme apropriado (controlos – acesso físico aos ativos)	DSS05.05	✓
72	Identificar e categorizar os controlos existentes sobre intrusões, incluindo deteção técnica, reconhecimento de padrões, técnicas de invasão avançadas e não padronizadas	DSS05.07	✓
73	Monitorizar e avaliar continuamente, incluindo autoavaliações de controlo (CSA's) na cibersegurança, incluindo relatórios de ataques/fraquezas/falhas e outras atividades suspeitas, baseadas no risco	MEA02.04	✓
74	Estabelecer controlos de ciclo de vida de software para aplicações autodesenvolvidas e personalizadas	Princípio 10	✗
75	Participar com os fornecedores para alcançar os controlos de cibersegurança a montante	Princípio 10	✗
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 27 - Práticas associadas aos controlos de cibersegurança a implementar, adaptado da publicação COBIT5TC

Através da análise das práticas da tabela 27, pode constatar-se que a organização em estudo contem um conjunto de controlos listados e associados às ameaças e vulnerabilidades que justificam a sua existência, a todos níveis e pontos de entrada. No entanto não se encontram incluídos no plano de risco de segurança da informação. Assim como recomenda na prática 72, a organização também tem o cuidado de identificar e categorizar os controlos existentes sobre intrusões, incluindo deteção técnica, reconhecimento de padrões, técnicas de invasão avançadas e não padronizadas.

Este conjunto de controlos de cibersegurança acabam por se assemelhar aos controlos genéricos de segurança da informação que se encontram no sistema de gestão de segurança da informação (SGSI).

No contexto da prática número 71, a organização tem a preocupação de realizar verificações aos controlos como é o caso, por exemplo, dos controlos no acesso físico dos ativos através da política do utilizador único.

Relativamente à prática de descrita no número 73 onde recomenda a monitorização e avaliação contínua, incluindo autoavaliações de controlo na cibersegurança, baseadas no risco, a organização realiza este processo através da ferramenta "ciclo PDCA[10]".
Quanto ao controlo associado ao ciclo de vida de software, a organização não efetua esta prática, assim como também não existe participação com os fornecedores para alcançar controlos de cibersegurança, tal como recomenda a prática número 75.

[10] O ciclo PDCA é um método iterativo de gestão de quatro passos, utilizado para o controlo e melhoria contínua de processos e produtos.

4.1.1.12. Acessos / Identidade

A confidencialidade é uma das principais componentes de segurança da informação e garante as restrições de autorização de acesso e divulgação, incluindo meios para proteção de privacidade e informações confidenciais. Neste sentido, e dada a sua relevância, o COBIT5TC recomenda um conjunto de práticas, que podem ser observadas na tabela 28:

Nº	Requisito de Cibersegurança **Acesso / Identidade**	Processo COBIT5	
76	Assegurar que todos os usuários tenham direitos de acesso à informação de acordo com os requisitos do negócio, assim como, é feita uma adequada segregação das funções	DSS05.04	✓
77	Alinhar a gestão de identidade ao modelo de governança selecionado	DSS05.04	+
78	Identificar controlos existentes sobre o acesso físico, combinados com a gestão de identidades.	DSS05.05	✓
79	Definir verificações de antecedentes para indivíduos que entram em áreas sensíveis, particularmente para funcionários temporários e visitantes.	DSS05.05	+
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 28 - Práticas associadas aos acessos físicos e gestão de identidades, adaptado da publicação COBIT5TC

A organização em estudo assegura que todos os usuários tenham direitos de acesso à informação de acordo com os requisitos do negócio, assim como é feita uma adequada segregação das funções. Assim sendo o acesso à informação é dado em função do tipo de responsabilidade que o usuário tem na organização.

A gestão da identidade é devidamente efetuada com base em políticas, práticas e regulamentos, no entanto não se pode considerar que este esteja corretamente alinhado com o modelo de governança selecionado, pelo facto de não haver um modelo claramente definido, tal como como referido anteriormente.

No contexto do acesso, a organização tem o cuidado de verificar os antecedentes dos indivíduos que entram em áreas sensíveis como refere no número 79, excetuando-se a realização desta análise aos visitantes.

4.1.1.13. Classificação e tratamento da informação

A informação deve ser reconhecida como um ativo ou um recurso que gera benefícios às organizações (ISACA, 2013a), acrescenta valor, cria vantagem competitiva e deve ser usada como suporte na gestão (Marchand, 2000). No entanto, nem toda a informação

contem o mesmo valor, havendo necessidade de distinguir/classificar a informação, de modo a que o seu tratamento e manutenção seja feito de forma correta.

Segundo a publicação COBIT5TC, a informação é o ativo central com necessidade de proteção e que, para alem do valor intrínseco, também há um grande valor comercial associado. Face a isso, e a título de exemplo, são apresentados dois tipos de informação, assim como o seu valor associado:

• Dados de cartão de crédito – O valor intrínseco associa-se ao facto de ser considerada informação privilegiada confiada pelo cliente. O valor comercial é encontrado nos pagamentos efetuados que, geralmente é a principal atração para a ocorrência de cibercrime.

• Perfis pessoais de login e senha – O valor intrínseco associa-se à existência de informação de identidade pessoal. O valor comercial associa-se ao acesso a dados confidenciais que, uma vez mais, se torna uma atração muito alta para cibercrime e ciberguerra.

Assim sendo, é fundamental o cumprimento de práticas para que a sua segurança não seja comprometida. Na tabela 29 enumeram-se algumas práticas no contexto da identificação, classificação e tratamento da informação, no contexto de cibersegurança.

Nº	Requisito de Cibersegurança Informação	Processo COBIT5	
80	Fornecer diretrizes relacionadas à cibersegurança sobre o significado de informação sensível e pessoal, assim como a respetiva classificação da informação no que toca a ataques e violações	APO01.06	✓
81	Identificar e classificar fontes de informação de cibersegurança, inteligência externa e serviços relacionados e estatísticas de ataques/violações	BAI08.02	✓
82	Avaliar a informação relacionada a ataques e violações, TI em geral, potenciais alvos e retirar informações obsoletas	BAI08.05	✓
83	Fornecer informações sobre serviços, equipamentos e dispositivos para monitorizar e controlar o ambiente	DSS01.04	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 29 - Práticas associadas à classificação e tratamento da informação, adaptado da publicação COBIT5TC

No contexto deste ponto, uma das práticas realizadas pela organização foi a criação de um processo chamado *Data classification scheme*. Através deste, toda a informação é classificada e processada em função da sua necessidade de confidencialidade. Seguidamente a informação é classificada através de uma escala, podendo esta ser

classificada como: informação pública, informação interna, informação restrita e informação confidencial. No que diz respeito à informação específica relacionada com ataques e violações, esta é avaliada e utilizada para solucionar situações futuras, como por exemplo, na deteção de fraudes.

Relativamente á identificação e classificação das fontes de informação de cibersegurança, inteligência externa e serviços relacionados, esta avaliação da informação é feita através da utilização do software SIEM (*security information and event management*) que faz a análise de *cyberfeeds*, as fontes de informação existentes.

4.1.1.14. Inovação

Outra das preocupações existentes na publicação COBIT5TC é a capacidade das organizações em gerar inovação nos processos e procedimentos usuais. Na tabela 30 enumeram-se as recomendações ao nível desta temática:

Nº	Requisito de Cibersegurança Inovação	Processo COBIT5	
84	Incluir inovação na gestão de cibersegurança como parte a inovação geral de segurança da informação	APO04.01	✓
85	Avaliar potenciais vulnerabilidades, ameaças e risco associado de novas iniciativas	APO04.02	+
86	Verificar o impacto potencial de cibersegurança em relação às tecnologias e inovações emergentes e incluir os seus riscos e problemas associados	APO04.04	✓
87	Priorizar as iniciativas de cibersegurança e os recursos necessários	APO06.02	✓
88	Pesquisar e identificar tendências emergentes no cibercrime e ciberguerra e medidas de segurança relacionadas	APO04.03	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 30 - Práticas associadas à introdução de inovação ao sistema de cibersegurança, adaptado da publicação COBIT5TC

A organização tem presente a preocupação de desenvolver e incluir iniciativas de cibersegurança, baseando-se nas tendências emergentes. A priori de serem integradas novas iniciativas de cibersegurança como parte de inovação geral de segurança da informação, estas iniciativas são sujeitas ao processo *secure software development lifecicle*, onde passam por várias fases até se realizar o seu desenvolvimento, tal como é possível verificar na seguinte figura 12:

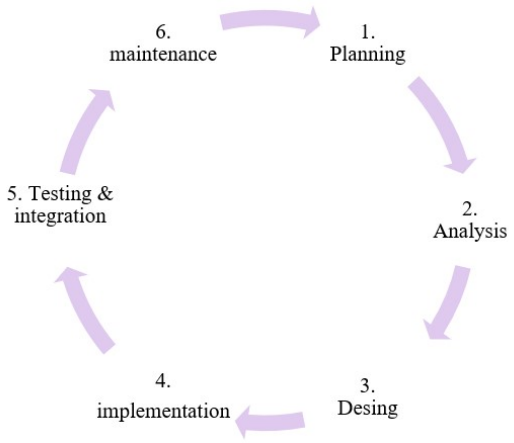

Figura 12- Secure software development lifecicle. Fornecido pela organização.

Depois de implementadas novas iniciativas de cibersegurança, apenas se realizam avaliações às iniciativas no caso de se verificar a necessidade, caso algo não esteja em conformidade com o planeado.

No contexto da formação profissional dos colaboradores verifica-se a preocupação existente na integração de novas iniciativas de cibersegurança. Mensalmente é dada uma formação, o seguimento de um programa chamado *secutity university,* onde é apresentado o OWASP TOP 10[11], descrevendo claramente cada uma das ameaças, a forma como atuam e controlos a usar para se proteger das mesmas.

4.1.1.15. Investimentos de cibersegurança

Por forma a conseguir um bom sistema de cibersegurança, é necessário garantir que o investimento neste seja feito da melhor forma a fim de conseguir manter as infraestruturas sustentáveis e competitivas. Assim sendo, a publicação COBIT5TC recomenda, como é possível observar na tabela 31, as seguintes práticas:

Nº	Requisito de Cibersegurança Investimentos	Processo COBIT5	
89	Determinar uma apropriada gestão dos investimentos de cibersegurança no contexto sistémico	APO05.01	✓
90	Garantir que haja financiamento apropriado para cibersegurança	APO05.02	✓
91	Obter as aceitações de risco quando o financiamento é insuficiente	APO05.02	✓
92	Preparar e manter um orçamento de cibersegurança	APO06.03	✓

[11] O OWASP, ou Projeto Aberto de Segurança em Aplicações Web, é uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web. O OWASP TOP 10 são os dez riscos mais críticos da segurança de aplicativos da Web

✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;

Tabela 31 - Práticas associadas aos investimentos de cibersegurança, adaptado da publicação COBIT5TC

No que diz respeito a esta temática, a organização prepara e mantem anualmente um orçamento destinado à cibersegurança, face às necessidades previstas, sendo feita uma posterior gestão adequada desses mesmos investimentos. Em caso de necessidades posteriores não incluídas no orçamento inicial previsto, a situação é analisada em função dos seus riscos, ocorrendo um alargamento do orçamento. Caso não se justifique o investimento, o risco subjacente à decisão é devidamente aceite por parte do responsável.

4.1.1.16. Recursos Humanos

Um dos prontos principais para o bom funcionamento do sistema de cibersegurança é assegurar que é feita uma boa gestão dos recursos humanos existentes. Estipular adequadamente as obrigações, responsabilidades e tarefas de cibersegurança é fundamental para o bom funcionamento do sistema, assim como é recomendado na publicação COBIT5TC, e apresentado na tabela 32.

Nº	Requisito de Cibersegurança Recursos Humanos	Processo COBIT5	
93	Determinar obrigações, responsabilidades e tarefas de cibersegurança de outras funções organizacionais	APO01.02	+
94	Definir equipa de cibersegurança assim como requisitos necessários para a mesma	APO07.01	✓
95	Definir e implementar procedimentos adequados para o final da contratação		✓
96	Assegurar o reconhecimento do pessoal da cibersegurança através de incentivos e reconhecimento apropriados		✗
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 32 - Práticas de cibersegurança associadas aos recursos humanos, adaptado da publicação COBIT5TC

No departamento de segurança da informação, está definida uma equipa de recursos humanos destinados a diferentes funções, nomeadamente à função de cibersegurança, inseridos nesta por cumprirem um conjunto de requisitos necessários. Através da análise feita na organização em estudo, é possível observar que é realizada uma adequada distribuição das tarefas diárias de trabalho no seguimento normal do plano de trabalho de cada colaborador assim como o compromisso de responsabilidade pelas mesmas. No

entanto, não existe documentação interna onde estipula, a priori, todas as funções e responsabilidades de cada colaborador.

Aquando de se verificar o final de uma contratação, a organização procede automaticamente a práticas de *off – boarding*, a fim de assegurar a continuidade de confidencialidade e proteção da informação, tal como recomenda a prática número 95 da tabela 32. Quanto à prática número 96, não se verifica na organização qualquer tipo de reconhecimento apropriado ou incentivo, pela boa prática das ações de cibersegurança implementadas.

4.1.1.17. Serviços

Dada a variedade de serviços a que uma organização precisa de recorrer para assegurar o bom funcionamento do sistema de cibersegurança e continuidade do negócio, é importante que se faça uma gestão e avaliação destes, quer em relação a critérios e requisitos de cibersegurança como a nível operacional. Assim sento, são recomendadas as práticas descritas na tabela 33:

Nº	Requisito de Cibersegurança Serviços	Processo COBIT5	
97	Definir/Adicionar serviços necessários, relacionados à cibersegurança e catalogá-los conforme apropriado	APO09.02	✓
98	Avaliar os níveis de serviços do fornecedor em relação a critérios e requisitos de cibersegurança e definir os níveis operacionais	APO09.03	✓
99	Analisar as cláusulas/requisitos relacionadas à cibersegurança nos contratos e atualizar os SLA's conforme necessário	APO09.05 DSS01.02	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 33- Práticas de cibersegurança associadas aos serviços, adaptado da publicação COBIT5TC

Face ao acima apresentado, foi possível verificar que a organização faz a correta definição e introdução dos serviços necessários, relacionados à cibersegurança e cataloga-os conforme apropriado.

Todo o novo fornecedor de serviços, independentemente de se classificar como fornecedor de serviços de pagamentos, fornecedor de serviços marketing, corporate, fornecedor de software para análise vulnerabilidades, entre outros, antes da realização do contrato de prestação de serviços, está sujeito a um processo de avaliação, baseado num

programa com o nome *a Iaas*[12]*, Paas*[13] *e Saas*[14] *Rules*. Nesta avaliação são verificados o cumprimento/não cumprimento de requisitos necessários em função do seu impacto e do facto de serem cruciais para garantir a segurança da informação.

4.1.1.18. Fornecedores

No seguimento do ponto anterior, o presente ponto complementa a atenção dada aos fornecedores a partir do momento em que estes já se encontram a colaborar com a organização.

Como é possível observar na tabela 34, a publicação COBIT5TC recomenda a avaliação e revisão constante dos fornecedores para conformidade e desempenho de cibersegurança assim como a avaliação e classificação dos riscos associados a estes:

Nº	Requisito de Cibersegurança Fornecedores	Processo COBIT5	
100	Atualizar a classificação de risco para todos os fornecedores sujeitos a requisitos de cibersegurança. Avaliar a garantia, reunindo informação apropriada para verificações de antecedentes	APO10.04 MEA02.05	✓
101	Avaliar e rever fornecedores para conformidade e desempenho de cibersegurança	APO10.05	+
102	Comunicar com os fornecedores para gerir as vulnerabilidades e pontos de entrada		✗
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 34 - Práticas de cibersegurança associadas aos fornecedores, adaptado da publicação COBIT5TC

Através da análise feita à organização em estudo, verifica-se a preocupação em avaliar e classificar os riscos existentes, verificando a fiabilidade dos serviços prestados por fornecedores. No entanto, a avaliação e revisão dos fornecedores não é feita de forma regular, sendo que, na maioria dos casos, esta revisão só acontece aquando da verificação de uma ocorrência que a justifique.

Relativamente à prática número 102, constatou-se que a comunicação com os fornecedores para gerir vulnerabilidades e pontos de entrada, não se verifica inserida nas tarefas de cibersegurança.

[12] *Infrastructure as a Service*
[13] *Platform as a Service*
[14] *Software as a Service*

4.1.1.19. Programas e projetos de cibersegurança

A implementação de novos casos de negócio carece de uma análise cuidada, para não colocar em causa a cibersegurança existente na organização. Neste sentido, é necessário acompanhar novas práticas de negócio, com um adequado programa de cibersegurança, constituído por medidas obrigatórias e prioridades críticas. Relativamente à definição e desenvolvimento de programas e projetos de cibersegurança, a publicação COBIT5TC recomenda, na tabela 35, as seguintes práticas:

Nº	Requisito de Cibersegurança Programas e projetos de cibersegurança	Processo COBIT5	
103	Definir casos de negócio e respetivo programa de cibersegurança com base em medidas de segurança obrigatórias e prioridades críticas de negócio	BAI01.02	+
104	Priorizar planos e projetos de cibersegurança num cronograma e identificar objetivos e benefícios de curto prazo, ou seja, ações imediatas para reduzir o número de ataques e violações	BAI05.04	✓
105	Desenvolver e documentar projetos com especificações de cibersegurança de alto nível de acordo com o modelo de segurança e a dinâmica do sistema	BAI03.01	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 35 - Práticas associadas aos programas e projetos de cibersegurança, adaptado da publicação COBIT5TC

Relativamente à prática número 103, foi constatável que a tarefa de definição de casos de negócio não se aplica como tarefa destinada ao departamento se segurança de informação. Apesar disso, quando é definida uma nova estratégia de negócio, o departamento de segurança da informação desenvolve de imediato o respetivo programa de cibersegurança com base em medidas de segurança obrigatórias e prioridades críticas de negócio.

No contexto da preocupação em desenvolver novos planos e projetos, observa-se essa iniciativa, sendo que, aquando da sua projeção, são identificados os objetivos e benefícios de curto prazo, tal como sugere na prática número 104.

4.1.1.20. Disponibilidade dos serviços

Um dos interesses fundamentais para a prática de segurança da informação numa organização é seguramente a possibilidade de garantir a disponibilidade total, assim como o desempenho e capacidade dos serviços. Assim sendo, é fundamental que a organização tenha plena noção de todos os problemas/ ameaças que possam pôr isso em causa. Associadas ao contexto da disponibilidade, encontram-se na tabela 36 as seguintes práticas recomendadas pela publicação COBIT5TC:

Nº	Requisito de Cibersegurança Disponibilidade	Processo COBIT5	
106	Definir e incluir quaisquer problemas/ameaças relacionados à cibersegurança, especificamente ataques e violações que ponham em causa a disponibilidade, desempenho e capacidade dos serviços; fazer o levantamento daqueles que incluem fraquezas sistémicas	BAI04.01 DSS03.01 DSS03.03	✓
107	Realizar avaliações de impacto para processos de TI e do negócio potencialmente afetados por ataques e violações	BAI04.02	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 36 - Práticas associadas à disponibilidade dos serviços, adaptado da publicação COBIT5TC

Após a análise da organização, foi constatável que, todo o tipo de ameaças ou ploblemas de cibersegurança que possam pôr em causa a disponibilidade, desempenho e capacidade dos serviços assim como a funcionalidades dos TI e processos de negócio, são devidamente estudadas e tratadas em função do seu nível de impacto.

4.1.1.21. Mudança/ Melhoria contínua

Assim como indica o nome, a melhoria contínua é um esforço contínuo que uma organização tem, com o objetivo de melhorar produtos, processos ou serviços. Apesar de se considerar um esforço contínuo, esta melhoria também gera uma vantagem competitiva para as organizações. Neste sentido, a publicação COBIT5TC recomenda a definição de um processo me melhoria contínua para a cibersegurança. Apresentam-se na tabela 37 um conjunto de práticas relacionadas com a criação de melhoria contínua numa organização:

Nº	Requisito de Cibersegurança Mudança/ Melhoria Contínua	Processo COBIT5	
108	Definir o processo de melhoria contínua para cibersegurança	APO13.03 APO01.07 DSS02.07	✓
109	Implementar um processo de reconhecimento de padrões (a todos os níveis) apontado para ataques e violações	DSS05.01 APO01.07	+
110	Definir estados-alvo/metas como parte da transformação geral, para cibersegurança, em intervalos regulares e em função de ataques e violações reais	APO02.03	✓
111	Avaliar as alterações de cibersegurança do ponto de vista da transformação; incorporar essas mudanças à gestão geral de mudanças	BAI06.01	✓
112	Rever e consolidar quaisquer mudanças de emergência relacionadas à cibersegurança: Incluir todas as alterações importantes	BAI06.02	✓
113	Documentar (de forma detetável e auditável) quaisquer alterações relevantes para a cibersegurança, incluindo mudanças nos negócios	BAI06.04	✓
114	Identificar e contribuir com infraestruturas relacionadas com o risco de cibersegurança e vulnerabilidades e ameaças (gerindo as instalações e energia dos equipamentos) especialmente para as que possam ser um alvo	DSS01.05	-
115	Fazer cruzamento apropriado entre referencias de políticas e procedimentos de cibersegurança. Incluir cenários apropriados na política de BC (*business continuity*)	DSS04.01	✓
116	Desenvolver, alinhar e testar os BCP's (business continuity plan) para cenários relacionados à cibersegurança. Incluir acordos incidentais no ciclo PDCA	DSS04.03 DSS04.04 DSS04.05	✓
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;			

Tabela 37 - Práticas associadas ao processo de mudança/ melhoria contínua, adaptado da publicação COBIT5TC

Dentro daquilo que foi possível observar na organização, a definição de processo de melhoria contínua é feita através de um processo ao qual chamam de *change management development*. Neste sentido, e tal como indica no ponto número 111, 112 e 116 da tabela 37, a organização avalia todo o tipo de possíveis alterações de cibersegurança, com base em ataques e violações reais, definindo um conjunto de metas a alcançar como parte do

processo de transformação geral. Aquando de se verificarem necessidades de transformação, estas são devidamente documentadas e incorporadas no processo geral de cibersegurança.

No sentido de procurar a constante melhoria dos processos, é também feito o cruzamento apropriado entre referências de políticas e procedimentos de cibersegurança. Tendo em conta a política de continuidade do negócio, também realizam a prática de desenvolver, alinhar e testar os BCP's (*business continuity plan*) para cenários relacionados à cibersegurança.

4.1.2. Princípios de cibersegurança

Atendendo ao facto das práticas recomendadas pela publicação COBIT5TC relativamente aos princípios e políticas, serem muito repetitivas às práticas recomendadas nos diferentes processos, o objetivo nesta etapa do trabalho, foi conseguir associar quais as práticas associadas aos processos comprovariam o cumprimento das práticas associadas aos princípios e políticas. Assim sendo, e após uma comparação exaustiva entre o conjunto coletivo das práticas da check list, foi possível concretizar a tarefa. Deste modo, é apresentado na tabela 38 o conjunto dos princípios recomendados pelo ISACA (2012a)(primeira coluna) o seu objetivo a nível funcional (segunda coluna), e por fim, a ligação aos números das práticas observadas nos pontos anteriores (terceira coluna).

A título de melhor compreensão, analisando a terceira linha da tabela 41, é afirmável que a organização cumpre o princípio do "Foco no negócio" se for verificável o cumprimento das práticas atribuídas aos números 16, 24 e 107 dos pontos discutidos anteriormente.

Princípio	Objetivo	Check list	
Suporte ao Negócio			
1 - Foco no negócio	Garantir que a segurança da informação esteja integrada nas atividades essenciais do negócio	16; 24; 107	✓
2- Fornecer qualidade e valor aos stakeholders	Garantir que a segurança da informação oferece valor e atende aos requisitos do negócio	35; 36; 44; 51;	✓
3- Cumprir com os requisitos legais e regulamentares relevantes	Garantir que as obrigações legais sejam cumpridas, as expectativas dos stakeholders sejam geridas e as penalidades civis ou criminais sejam evitadas	2; 26; 36; 43	✓
4- Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação	Apoiar os requisitos do negócio e gerir o risco de informação.	35; 50; 54; 63;	✓
5- Avaliar atuais e futuras ameaças à informação	Analisar e avaliar as ameaças emergentes à segurança da informação, de modo a que as ações sejam informadas em tempo útil e oportunas para mitigar riscos.	6; 22; 55	✓
6- Promover a melhoria contínua da segurança da informação	Reduzir os custos, melhorar a eficiência e eficácia e promover uma cultura de melhoria contínua na segurança da informação	24; 108; 109	+
Defender o Negócio			
7- Adotar uma abordagem baseada no risco	Certificar-se de que o risco seja tratado de forma consistente e eficaz.	3; 20; 21; 22; 23; 26; 27; 35; 55	✓
8- Proteger a informação confidencial	Impedir a divulgação de informações classificadas (por exemplo, confidenciais ou sensíveis) a pessoas não autorizadas.	76; 78; 80; 81; 82; 83	✓
9- Concentrar-se nas aplicações críticas de negócio	Priorizar recursos escassos de segurança da informação, protegendo as aplicações do negócio nos quais um incidente de segurança da informação teria o maior impacto.	18; 27; 48; 52; 60; 61; 62; 87	✓
10- Desenvolver sistemas de forma segura	Criar qualidade, sistemas de custo-benefício nos quais os empresários possam confiar (por exemplo, consistentemente robustos, precisos e confiáveis).	45; 74; 75; 105	+
Promover um comportamento responsável de segurança de informação			
11- Agir de forma ética e profissional	Certificar-se de que as atividades relacionadas à segurança da informação sejam realizadas de forma fiável, responsável e efetiva.	1; 2; 4; 73; 95; 96; 99; 100	+
12- Fomentar uma cultura de segurança da informação positiva	Fornecer uma influência positiva de segurança da informação sobre o comportamento dos usuários finais, reduzir a probabilidade de ocorrência de incidentes de segurança da informação e limitar seu potencial impacto no negócio.	40; 107	✓
✓ Verifica-se a prática; ✗ - não se verifica a prática; + - verifica-se parcialmente a prática ; Relativamente à cor em que se apresentam os números da terceira coluna se for: verde – verifica-se a prática; vermelho – não se verifica a prática ; amarelo – verifica-se parcialmente a prática			

Tabela 38 - Princípios associados à cibersegurança, adaptado da publicação COBIT5TC

A análise do cumprimento/ incumprimento dos princípios recomendados pelo COBIT5TC encontra-se abaixo, enumerada à semelhança da primeira coluna da tabela 38:

1 – Foco no negócio – através da análise das práticas realizadas pela organização, é notável a preocupação em garantir que a cibersegurança se encontre integrada nas atividades de negócio. Nesta perspetiva de negócio, é estabelecido o nível de tolerância face aos ataques e violações assim como, são feitas análises de risco aos ataques e violações que possam afetar os processos normais de negócio. O objetivo desta política é cobrir, ao nível do negócio, todas a necessidades de cibersegurança existentes.

2- Fornecer qualidade e valor aos stakeholders – Este fornecimento de qualidade traduz-se no comprometimento da organização em garantir que a segurança da informação, neste caso a cibersegurança, oferece valor e consegue atender aos requisitos do negócio. Atendendo ao objetivo, e apesar da organização não estabelecer corretamente a definição dos seus stakeholders em relação à informação de cibersegurança, verifica-se, através das práticas assocadas a este princípio, que este é cumprido.

3 – Cumprir com os requisitos legais e regulamentares relevantes – Cumprir estes requisitos é essencial para que a governo da organização seja funcional. Assim sendo, e assim como constatado anteriormente, a organização cumpre plenamente este princípio, uma vez que tem o cuidado de identificar todas as leis, regulamentos e regras assim como os requisitos a cumprir. A par do referido anteriormente, a organização não só procede à identificação das leis, regulamentos e regras, como também transmite os requisitos e seus componentes ao longo de todo o sistema de cibersegurança, assim como é recomendado pela publicação COBIT5TC.

4- Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação - O principal objetivo deste princípio é a realização de práticas que apoiem os requisitos do negócio, sugerindo o estabelecimento de indicadores ou pontos chave de desempenho de cibersegurança, assim como o reporte regular destas análises. Neste sentido, verifica-se na organização em estudo, o cumprimento desta prática uma vez que esta desenvolve uma linha base de recursos para cibersegurança, incluindo critérios e indicadores de desempenho (KPI's), com o objetivo de atender a todas as necessidades de cibersegurança. A par disto realizam-se análises de desempenho assim como relatórios regulares de desempenho de cibersegurança. A organização procede ainda à definição e

comunicação metas e objetivos de cibersegurança ao nível estratégico e inclui-os na estratégia de segurança.

5- Avaliar atuais e futuras ameaças à informação – Este princípio defende que a organização deve analisar e avaliar convenientemente todas as ameaças que sejam emergentes à cibersegurança a fim de que as ações correspondentes sejam implementadas em tempo útil e consideradas oportunas para mitigar os riscos. Neste sentido, comprova-se a prática desta política uma vez que a organização em estudo tem a preocupação de identificar, avaliar, tratar todas as ameaças existente. Uma das principais práticas é a coleta de dados e evidências sobre incidentes de cibersegurança assim como a identificação das ameaças para toda a organização. Nesta coleta de dados são aplicadas técnicas detalhadas de análise de dados podendo obter-se assim uma visão mais aprofundada sobre o futuro da cibersegurança. Todo este estudo ao nível das ameaças, permite à organização antecipar ameaças futuras que possam surgir.

6- Promover a melhoria contínua da segurança da informação – No contexto deste princípio, o pressuposto é que a organização promova uma cultura de melhoria continua de cibersegurança, reduzindo os custos, mas tornando os processos eficientes e eficazes. Neste sentido foi possível observar que a organização tem a preocupação em estabelecer um processo de melhoria contínua, tendo em conta as experiências passadas e as tendências futuras. Observa-se ainda a tentativa de estabelecer e manter uma cultura que promova a melhoria e o pensamento adaptativo tolerante a falhas e erros que possam ocorrer.

7- Adotar uma abordagem baseada no risco – Este princípio é aquele que garante que a organização faça de forma consciente e eficaz o tratamento do risco. Neste sentido, constatou-se que a organização define de forma apropriada o processo de identificação e avaliação do risco assim como as correspondentes opções de tratamento. Esta avaliação do risco de cibersegurança tem incorporadas análises a incidentes passados e consequentes aprendizagens organizacionais e técnicas. Todas as estratégias de análise e gestão de risco encontram-se alinhadas com as políticas adotadas na estratégia de governo do sistema de cibersegurança da organização.

8 – Proteger a informação confidencial – é essencial que uma organização saiba como impedir a divulgação da informação a pessoas não autorizadas, tendo em conta a sua classificação. Relativamente a este princípio, foi possível observar que a organização faz

uma devida gestão da informação, classificando e tratando-a de forma correta, gerindo, em função disso, a permissão de acesso à mesma. Assim sendo, e tendo em conta a gestão de identidades alinhadas ao governo do sistema de cibersegurança, todos os usuários têm direitos de acesso à informação de acordo com os requisitos do negócio.

9- Concentrar-se nas aplicações de críticas de negócio– O objetivo desta política é que a organização priorize recursos escassos de segurança da informação, protegendo as aplicações do negócio nos quais um incidente de segurança da informação teria o maior impacto. A publicação COBIT5TC recomenda que, em primeiro lugar, a organização tenha definidas, na perspetiva de cibersegurança, todas as aplicações críticas de negócio, analisando detalhadamente todas as dependências e pontos de entrada potencialmente relevantes. Com base no estudo à organização, verifica-se o cumprimento do referido anteriormente, assim como a respetiva alocação de recursos e financiamentos de acordo as prioridades, tendo em conta as ameaças reais.

10- Desenvolver sistemas de forma segura - O pressuposto para cumprir esta política, segundo a publicação COBIT5TC, traduz-se na definição de um processo de administração de cibersegurança para todas as aplicações e sistemas potencialmente críticos assim como o estabelecimento de controlos ao ciclo de vida dos softwares para aplicações autodesenvolvidas e personalizadas. Esta política defende ainda como fundamental a participação dos fornecedores no processo de gestão das vulnerabilidades e pontos de entrada assim como no alcance de novos controlos de cibersegurança. Posto isto, e tendo em conta a organização em estudo, é conclusivo que esta prática não é muito desenvolvida, uma vez que não existe a participação dos fornecedores no processo de gestão e definição dos controlos de cibersegurança, a não ser que estejamos a falar de fornecedores de softwares para deteção de vulnerabilidades, onde é considerado que isso influência a gestão dos pontos de entrada e vulnerabilidades.

Relativamente à gestão dos sistemas e softwares para aplicações autodesenvolvidas, esta política não se enquadra ao contexto do departamento de cibersegurança, mas sim ao departamento que gere as infraestruturas da organização.

11 - Agir de forma ética e profissional – Segundo a publicação COBIT5TC este princípio tem como objetivo certificar-se que as atividades relacionadas à cibersegurança sejam realizadas de forma fiável, responsável e efetiva. Neste sentido, e atendendo às práticas

analisadas nos pontos anteriores, verifica-se por parte da organização o cumprimento parcial deste princípio. Associado a este, é necessário analisar o sistema de governo de cibersegurança, assim como todas as práticas associadas às contratações de recursos humanos e serviços necessários. Posto isto, e assim como recomendado, a organização suporta um conjunto de documentos criados onde se podem encontrar definidas políticas, práticas, procedimentos e outros elementos de orientação com base no risco de cibersegurança e o modelo geral de governo da organização, através do uso de OKR's (*objectives and Key Results*). Com base nisso, ocorre uma monitorização e avaliação contínua, incluindo autoavaliações de controlo de cibersegurança (CSA's), e elaboração de relatórios de ataques/fraquezas/falhas ou outras atividades suspeitas. Relativamente à componente associada aos recursos humanos, e assim como referido anteriormente, está definida uma equipa destinada a diferentes funções, nomeadamente à função de cibersegurança. Os elementos da equipa cumprem um conjunto de requisitos necessários, sendo dada especial atenção às contratações para posições sensíveis. No final de cada contratação a organização procede automaticamente aos procedimentos definidos e implementados de *off – boarding*, a fim de assegurar a confidencialidade e proteção da informação.

O único ponto que falha para não atribuir o cumprimento total deste princípio, é o facto de a organização não atribuir qualquer tipo de reconhecimento apropriado ou incentivo, pela boa prática das ações de cibersegurança implementadas, uma vez que é do princípio que cada colaborador é automaticamente responsável por praticar corretamente as ações de cibersegurança definidas.

12 - Fomentar uma cultura de segurança da informação positiva – O principal objetivo deste princípio é o fornecimento de uma influência positiva de cibersegurança sobre comportamentos a fim de reduzir a probabilidade de ocorrência de incidentes, limitando o potencial impacto no negócio. Assim como referido anteriormente, a organização desenvolve programas de consciencialização e instrução de cibersegurança, onde apresenta exemplos práticos de ataques / ameaças, com o objetivo de fornecer informação sempre atual e útil que possa apoiar as medidas e métricas utilizadas no contexto da cibersegurança. Neste contexto, e por forma a influenciar esta mudança de comportamentos, são apresentadas avaliações de impacto para processos de TI e do negócio. Relativamente aos comportamentos de cibersegurança a adotar, estes são devidamente testados, aprovados e inseridos nos planos de resposta a incidentes com

medidas corretivas e consequente transformação do processo geral da cibersegurança da organização.

4.1.3. Políticas de cibersegurança

Da mesma forma que se encontram apresentados os princípios orientadores de cibersegurança, apresenta-se na tabela 39 o conjunto das políticas sugeridas pelo ISACA (2012a)(primeira ferrcoluna), assim como, a ligação aos números das práticas associadas (segunda coluna). Assim como referido no ponto 2.2.1 do presente trabalho de projeto, as políticas, fornecem orientações mais detalhadas relativamente à forma como se deve pôr em prática os princípios seguidos pela organização.

Uma vez mais, e a título de melhor compreensão, analisando a segunda linha da tabela 39, é afirmável que a organização cumpre a política de "segurança da informação" se for verificável o cumprimento das práticas atribuídas aos números 24, 35, 38, 55, 107 e 108 das tabelas 15 à 37.

Políticas	Check list	
1- Segurança da informação	24; 35; 38; 55; 107; 108	✓
2- Controlo de acesso	15; 70; 71; 72; 76; 77; 78; 79	+
3- Segurança da informação do pessoal	79; 94; 95; 99	+
4- Segurança da informação física e ambiental	83; 114	+
5- Resposta a incidentes	13; 44; 45; 105; 106	+
6- Continuidade do negócio e recuperação de desastres	20; 27; 115; 116	✓
7- Gestão de ativos	22; 80; 81; 82; 83	✓
8- Regras de comportamento	24; 108; 109	+
9- Adquirir sistemas de informação, desenvolvimento e manutenção de software	45; 74; 75; 105	+
10- Gestão de Fornecedores	75; 102	✗
11- Gestão das operações e da comunicação	22; 26; 76	✓
12- Conformidade	4; 47; 54; 59; 63; 73; 95; 100	+
13- Gestão de Risco	3; 6; 24; 26; 54; 55; 63; 69	+
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ; ✗ - não se verifica a prática; Relativamente à cor em que se apresentam os números da segunda coluna se for: verde – verifica-se a prática; amarelo – verifica-se parcialmente a prática; vermelho – não se verifica a prática		

Tabela 39 - Políticas associados à cibersegurança, adaptado da publicação COBIT5TC

Assim como realizado anteriormente na discussão do cumprimento dos princípios de cibersegurança, a análise do cumprimento/ incumprimento das políticas sugeridas pelo COBIT5TC encontram-se abaixo, enumeradas pela ordem da primeira coluna da Tabela 39:

1- Segurança da informação – O cumprimento desta política implica que organização assuma objetivos de cibersegurança assim como o compromisso de responsabilidade do seu cumprimento. Neste sentido observa-se por parte da organização a definição clara do plano de cibersegurança acompanhada de metas e objetivos a cumprir, assim como métricas adequadas que expliquem a visão e cultura de cibersegurança presente. Esta política engloba um aglomerado de outras políticas assim como práticas e princípios, tais como a gestão de dados, avaliação de risco da informação, gestão de custos e o cumprimento das obrigações legais, regulamentares e contratuais. Neste sentido é possível afirmar o cumprimento geral desta política, tendo em conta todos os resultados anteriormente referidos.

2- Controlo de acesso – Esta política tem como objetivo o fornecimento de acesso adequado aos stakeholders quer internos quer externos. É uma política geral a todas as unidades de negócio. Seguindo a análise da organização em estudo, o controlo de acessos é feito sendo apenas atribuído o acesso à informação, caso a função ou responsabilidade justifique. As conclusões relativas o ao ponto "Acessos/ Identidade" complementam as conclusões a retirar sobre esta política de controlo de acesso.

3- Segurança da informação do pessoal – esta política recomenda a execução de verificações de antecedentes a todos os colaboradores com posições-chave. Neste sentido é verificável a preocupação da organização em contratar colaboradores altamente qualificados aos cargos a ocupar, tendo por base a análise e verificação completa de antecedentes. É também feita a certificação de que a equipa de cibersegurança possui habilidades atuais e pertinentes assim como todas a certificações necessárias.

4- Segurança da informação física e ambiental - o objetivo desta política é fornecer orientação sobre a proteção dos locais físicos, com base em controlos ambientais. Uma vez que o contexto deste estudo está focado para a cibersegurança, e não na segurança da informação de forma generalizada, não foram verificadas as práticas associadas à proteção física referida nesta política.

5- Resposta a incidentes – O objetivo desta política é cobrir a necessidade de responder aos incidentes em tempo útil a fim de ainda conseguir recuperar a atividade sem grande impacto. Neste sentido, aquando a ocorrência de um incidente, a política recomenda que se faça a sua identificação, declarando a forma como o incidente será tratado, a equipa que responderá ao incidente (mencionando funções e responsabilidades) assim como

documentar procedimentos e diretrizes para o seu tratamento. Neste sentido, e com base nas práticas analisadas ao longo deste projeto, é possível concluir que esta política é seguida.

6- Continuidade do negócio e recuperação de desastres - Recuperar de um desastre, segundo esta política, implica a realização de análises de impacto (BIA), planos de recuperação com base nas vulnerabilidades e correta alocação de recursos e fundos. Na perspetiva de cibersegurança é possível a verificação do cumprimento das práticas associadas a esta política, nos pontos 20; 27; 115; 116 das tabelas 15 à 37.

7- Gestão de ativos – Segundo a publicação COBIT5TC o cumprimento desta política, recomenda o estabelecimento e correta classificação dos dados, em relação ao risco de cibercrime ou ciberguerra, assim como o seu armazenamento. Neste sentido, é verificável que a organização em estudo tem a preocupação existente de coletar dados sobre riscos, ataques, violações e incidentes relacionados à cibersegurança, incluindo dados externos se apropriado, como é verificável na prática número 22 da tabela 18. Relativamente à gestão dos dados é possível observar no ponto "classificação e tratamento da informação", que toda a informação é classificada e processada em função da sua necessidade de confidencialidade. A informação específica relacionada com ataques e violações é avaliada e utilizada para solucionar situações futuras, como por exemplo na deteção de fraudes.

No contexto dos ativos não é verificável a gestão do ciclo de vida de proteção, nem são projetadas pelos responsáveis de cibersegurança medidas de proteção de ativos.

8- Regras de comportamento – Através da análise dos pontos "4.2.1.5. Métricas e medidas de consciencialização" e "4.1.1.21. Mudança/ Melhoria contínua" assim como às conclusões retiradas sobre o cumprimento do princípio "6- Promover a melhoria contínua da segurança da informação" é possível verificar a preocupação existente da organização, em desenvolver uma cultura empresarial que promova a melhoria contínua e o pensamento adaptativo, assim como definir orientação comportamental de cibersegurança e consciencialização para a preocupação de cibercrime e ciberguerra.

9- Adquirir sistemas de informação, desenvolvimento e manutenção de software – Atendendo às práticas concretas de cibersegurança, esta política não é cumprida na sua totalidade no sentido em que não são estabelecidos quaisquer controlos de cibersegurança

ao nível do acompanhamento dos softwares utilizados. Todos os procedimentos de cibersegurança associados a um software, são realizados a priori da sua aquisição, quando são verificados os requisitos necessários para que a aquisição seja aprovada.

10- Gestão de Fornecedores – esta política salienta a importância de uma organização, em conjunto com os fornecedores, gerir as vulnerabilidades e pontos de entrada assim como a definição de controlos de cibersegurança. No entanto, e à semelhança daquilo que foi referido no princípio 10 "Desenvolver sistemas de forma segura", não existe a participação dos fornecedores no processo de gestão e definição dos controlos de cibersegurança.

11- Gestão das operações e da comunicação – No contexto desta política, a publicação COBIT5TC recomenda a coleta de dados e evidências sobre incidentes de cibersegurança, seguida da adequada análise destes a fim de obter uma visão razoavelmente sólida sobre o futuro da cibersegurança. Esta política submete ainda à identificação e avaliação de riscos decorrentes do cibercrime e ciberguerra assim como também remete ao fornecimento de informações relacionadas à cibersegurança para a gestão de acessos e identidade no geral. Neste sentido, e uma vez que se observou a prática destas ações por parte da organização em estudo, é afirmável o cumprimento desta política.

12- Conformidade – Verificar a conformidade da cibersegurança traduz-se na análise à presença de regulamentação, quer a nível legal quer regulatório e definir requisitos de cibersegurança a partir destes. Posteriormente, é necessária a transmissão desses requisitos ao longo do sistema geral de cibersegurança e aplica-los às políticas e normas seguidas. Por forma a não tornar repetitiva a descrição do cumprimento desta política, é aceitável dizer-se que é cumprida, através das práticas mencionadas anteriormente com os números 4; 47; 54; 63; 67; 77; 99; 104 encontradas da tabela 15 à 37.

13- Gestão de Risco – No seguimento desta política é conclusivo que se encontra em cumprimento pela organização, uma vez que esta suporta metodologias para avaliar o alcance e âmbito do risco, papeis e responsabilidades de tratamento, ferramentas e técnicas de mitigação, assim como planos de resposta a incidentes, como recomenda a publicação COBIT5TC. Serve ainda de conclusão ao cumprimento desta política os resultados referidos nas práticas do ponto "4.1.1.3. Risco, apetite pelo risco e tolerância ao mesmo "assim como no princípio "7- Adotar uma abordagem baseada no risco".

4.1.4. Estruturas Organizacionais

Dada a importância que a atribuição de funções e responsabilidades ocupa numa organização, achou-se pertinente verificar quais as estruturas organizacionais existentes assim as responsabilidades associadas.

Segundo a publicação COBIT5TC e bastante diferente daquilo que é recomendado na publicação do ISACA (2012a), é bastante frequente que a maioria das pequenas e médias empresas atribuam a responsabilidade pela cibersegurança a um elemento pertencente à área de TI, principalmente, à estrutura ISM (*Information security Manager).* Em ambientes organizacionais maiores, já é comum a existência de atribuição da responsabilidade de cibersegurança associada a um *Cybersecurity specialist profile.*

No seguimento da entrevista, constatou-se que as estruturas organizacionais recomendadas não são cumpridas pela organização. Neste sentido, observou-se a presença da existência de um ISO *(Information Security Officer)* associado a uma equipa de segurança da informação *(Information Security Team)*. Assim sendo, todas as responsabilidades inerentes à cibersegurança estão atribuídas ao ISO, uma vez que é o único elemento existente com poder de tomada de decisão. Estas responsabilidades, podem de certa forma ser transferidas, podendo este passar a responsabilidade de uma prática a um elemento da *Information Security Team* no seguimento da atribuição de tarefas associado ao plano de trabalho diário.

4.1.5. Cultura, Ética e Comportamento

No contexto da Cultura, Ética e Comportamento, o ISACA (2012a) define um conjunto de comportamentos modelo e valores culturais, assumindo a sua aplicação como fundamental ao processo de gestão de cibersegurança.

Assim como menciona a publicação COBIT5TC, a gestão de cibersegurança é baseada na conformidade, usando um modelo de comportamentos e resiliência organizacional, para combater possíveis ataques e violações. Dependendo da cultura organizacional predominante, este processo de cultura de comportamentos pode levar um tempo considerável para ser implementado.

Assim sendo, segue-se na tabela abaixo, o conjunto de modelos comportamentais recomendados pelo COBIT5TC:

Modelo de comportamentos - Aplicabilidade ao nível da Cibersegurança	
A segurança da informação é praticada nas operações diárias	
Os princípios e práticas de cibersegurança são aplicados às operações diárias.	+
Todos os associados compreendem e aplicam cibersegurança em tempo útil.	✓
As pessoas respeitam a importância das políticas e princípios de cibersegurança	
Todos os usuários compreendem as prioridades definidas na cibersegurança assim como a aplicabilidade no seu ambiente de TI pessoal e empresarial.	✓
Todos os usuários da informação estão conscientes e ativamente envolvidos, sugerindo/definindo princípios e políticas de cibersegurança.	+
Os princípios, políticas, padrões e KOPs de cibersegurança são atualizados com frequência para refletir a realidade do dia a dia e a experiência da organização	+
As pessoas recebem orientações de segurança da informação suficientes e detalhadas e são encorajadas a participar e desafiar a situação atual de segurança da informação.	
A cibersegurança é um processo de transformação com desafios regulares em todas as partes da organização.	+
A orientação para cibersegurança é simples e relaciona-se com o risco típico do dia-a-dia.	✓
A situação em relação à cibersegurança é avaliada de forma contínua e conjunta por usuários e gestores da segurança.	+
Todos são responsabilizados pela proteção da informação, dentro da organização	
Os gestores da segurança e os usuários compartilham a responsabilidade pela cibersegurança. Isso inclui o uso comercial, uso em viagens e uso doméstico	✓
Os usuários têm uma compreensão clara de sua responsabilidade e atuam de forma responsável.	✓
A organização opera num ambiente tolerante a falhas/ tolerância a erros e evita o bode expiatório.	✓
Os stakeholders estão cientes de como identificar e responder às ameaças da organização	
Todos os usuários são stakeholders na cibersegurança, independentemente do seu nível hierárquico dentro da organização.	✓
Os usuários estão suficientemente conscientes dos riscos, ameaças e vulnerabilidades associados a ataques / infrações.	✓
A resposta a ameaças e incidentes é bem compreendida, exercida com frequência e auditável.	✓
A gestão de topo apoia e antecipa inovações de forma proativa	
A gestão da segurança e usuários finais identificam, testam e adotam a inovação de cibersegurança.	+
A administração e os usuários finais identificam e adotam novos casos de negócios para tecnologia, práticas de segurança e outros tipos de valor agregado na cibersegurança.	+
A organização visa explicitamente manter-se na frente, no que toca a cibersegurança	✓
A gestão do negócio empenha-se na obtenção de uma colaboração interfuncional continua	
Os programas de cibersegurança estão em vigor e fazem parte da estratégia geral de inovação.	✓
As inovações de segurança são incorporadas como projetos-chave.	✓
As funções de negócios cooperam com a segurança da informação para maximizar a eficiência e eficácia da cibersegurança.	+
A gestão executiva reconhece o valor que segurança da informação tem no negócio	
Os gerentes executivos atuam como usuários finais e reconhecem o valor da cibersegurança	✓
Eles participam ativamente de atividades de instrução e conscientização.	+
✓ verifica-se a prática; + - verifica-se parcialmente a prática; ✗ - não se verifica a prática;	

Tabela 40 - Modelo de comportamentos associado à cibersegurança, adaptado da publicação COBIT5TC

Dado que o preenchimento desta tabela se encontrou ao cargo do entrevistado, o responsável pela cibersegurança na organização, não poderá ser feita uma análise tão detalhada, à semelhança dos pontos anteriores.

No entanto, apesar da liberdade de preenchimento atribuída a esta tabela, em função daquilo que o entrevistado consideraria como comportamentos que se verificam na organização ao nível da cibersegurança, este foi capaz de assumir que nem todos os comportamentos observados na tabela 40 se cumprem por completo. Assim sendo, é notável a consciência que a organização tem face aos comportamentos dos indivíduos.

Segundo as conclusões dos pontos mencionados anteriormente, já seria constatável que nem todos os comportamentos desejáveis seriam cumpridos, e face a isso, é que se optou por deixar ao preenchimento do entrevistado, para analisar a postura e consciência deste.

Capítulo V – Conclusão

5.1. Conclusão do trabalho de projeto

Atendendo à realidade atual da sociedade, e observando o mundo tecnológico em que cada vez mais nos tornamos, apostar na Cibersegurança, assim como recomenda a publicação COBIT5TC, poderá ser considerado uma mais valia. Tornar efetivo um sistema de cibersegurança requer, na sua aplicação, quatro passos essenciais: planeamento, ação, verificação e revisão. No entanto, torna-lo dinâmico e atual requer uma constante evolução, análise e melhoria.

Com o objetivo de tornar este projeto o mais próximo da realidade, desenvolveu-se um estudo de caso numa e-commerce, baseado no normativo do COBIT5SI mas focado numa das publicações do ISACA aplicado à Cibersegurança (COBIT5TC). Neste estudo fez-se a análise do cumprimento de práticas associadas aos processos, princípios e políticas de cibersegurança, assim como quais as estruturas organizacionais existentes e o conjunto de comportamentos associados à cultura de cibersegurança presente na organização.

Através deste estudo de caso conseguiu-se verificar, à parte do contexto teórico, a forma como a cibersegurança é encarada no mundo empresarial dos dias atuais. Foi também possível praticar algumas técnicas associadas à profissão de um auditor, podendo observar a forma como esta se aplica em contexto real.

Constatou-se que, para a ocorrência do correto funcionamento em qualquer que seja a organização, é essencial que haja documentos que expliquem os diferentes processos, princípios, políticas, recursos, servições, estruturas e respetivas responsabilidades. Só desta forma é possível avaliar se o modelo de gestão e governo, é feito de forma correta.

5.2. Discussão dos resultados obtidos

Relativamente à análise do estudo prático realizado, e tendo em conta a informação recolhida no decorrer da entrevista, é possível concluir que, de um modo geral, a organização pratica nas suas operações diárias e planos de trabalho, a maioria das recomendações assinaladas no COBIT5TC. Com base na check list elaborada (situada no anexo II), foi-nos possível uma análise pormenorizada acerca do cumprimento, cumprimento parcial e não cumprimento de todas as práticas associadas aos processos, princípios e políticas presentes na publicação.

Neste sentido, constatou-se o cumprimento parcial e incumprimento de algumas práticas pertencentes à check list, o que nos sugere, de imediato, a existência de algumas melhorias que a organização deve incorporar, a fim de melhorar o governo e gestão do sistema de cibersegurança presente.
Face aos resultados apresentados no ponto 4.1 deste relatório, enumeram-se de seguida um conjunto de propostas de melhoria, nomeadamente:

1: Dada a sua ausência física e reconhecida a sua grande importância, recomenda-se a criação de um modelo de governo do sistema de cibersegurança que compreenda todo o conjunto de políticas, princípios, práticas, procedimentos outros elementos de orientação, com base em disposições legais e regulamentares existentes de cibersegurança.

2: No contexto da análise e gestão de risco de cibersegurança, recomenda-se a introdução da prática de definir e manter cenários de risco de cibersegurança. Esta prática permite a antecipação da organização não nível dos riscos que não comporta, mas que pode vir a assumir.

3: No sentido de prever e antecipar possíveis falhas ou inconformidades das medidas e métricas já estabelecidas, recomenda-se a realização de verificações e avaliações rotineiras de conformidade. Evitando o hábito de apenas intervir aquando de uma já ocorrência de inconformidade, como é observável. O mesmo se deve aplicar aos controlos de cibersegurança definidos e implementados pela organização.

4: Dado que nem todos os controlos existentes se encontram listados e respetivamente associados aos riscos que pretendem diminuir, recomenda-se a identificação e listagem de todos os controlos existentes e inclusão deles no tratamento e plano de risco de segurança da informação.

5: No contexto do controlo dos ativos existente, e tendo em conta que não é da direta responsabilidade do departamento de cibersegurança, salienta-se a importância de uma prática incumprida que é o estabelecimento de controlos de ciclo de vida de software para aplicações autodesenvolvidas e personalizadas.

6: No contexto da relação que a organização mantem com os fornecedores, verifica-se que não há grande comunicação entre estes, no contexto de melhorar as práticas de cibersegurança. Neste sentido, e uma vez que não se verificou a prática, recomenda-se

que a organização tenha uma participação mais ativa com os fornecedores para gerir vulnerabilidades e pontos de entrada e alcançar controlos de cibersegurança.

7: No contexto da identificação de identidades, verificou-se que apesar da organização verificar os antecedentes para indivíduos que entram em áreas sensíveis, não efetua essa prática com visitantes. Deste modo, recomenda-se a prática.

8: Relativamente aos recursos humanos que operam numa organização, é muito importante que estes tenham plena noção das suas funções e responsabilidades operacionais. Deste modo, e uma vez que não foi observável a sua existência, recomenda-se que organização defina claramente todas as obrigações, responsabilidades e tarefas de cibersegurança assim como outras estruturas organizacionais. O mesmo se aplica à identificação e definição formal dos direitos de decisão para a organização de cibersegurança.

9: Relativamente ao facto de apenas se observar a existência de um ISO (*Information Security Officer*) associado a uma equipa de cibersegurança (*Information Security Team*) e face ao facto de todas as responsabilidades inerentes à cibersegurança serem atribuídas ao ISO, uma vez que é o único elemento existente com poder de tomada de decisão, sugere-se uma alteração da estrutura organizacional. A recomendação passa pela criação de um comité ao nível da cibersegurança (ISSC), existência de um ISM (*Information security Manager*) ou *Cybersecurity specialist profile* abaixo da função do ISO.

5.3. Dificuldades e limitações do trabalho

Como limitação pode-se referir que uma das principais deste estudo de caso esteve na compreensão dos vários conceitos e conhecimento técnico alusivos à temática da Cibersegurança, nomeadamente à vertente tecnológica que requer algum conhecimento de conceitos.

Outra limitação foi a falta de matérias e literaturas associadas à cibersegurança uma vez que é uma temática bastante recente.

No contexto mais prático do trabalho, uma das principais limitações foi a interpretação do COBIT5TC, dada a não familiarização com este tipo de publicações, o que tornou mais difícil a análise e compreensão, assim como também o facto de não se conseguir obter a versão gratuita escrita em Português. Ainda neste contexto e dada a dimensão da

publicação COBIT5TC, considerou-se como dificuldade conseguir sintetizar todas as práticas recomendadas numa única check list.

No contexto das entrevistas, uma das limitações foi tentar fazer a ponte de ligação entre as recomendações do COBIT5TC com as práticas em contexto real e associadas à organização em estudo. Uma vez a publicação é adaptável a qualquer organização, a principal limitação é enquadrar as características especificas de uma organização a uma publicação tão abrangente.

5.4. Propostas de trabalhos futuros

No contexto de trabalhos futuros, existem várias abordagens que podem ser tomadas:

Analisar, através de entrevistas realizadas a outros colaboradores da organização em estudo, de que forma é feita a comunicação das políticas, princípios e processos de cibersegurança observadas anteriormente, avaliando a forma como todos estes elementos são conhecidos e aplicados.

Fazer a análise completa às práticas de cibersegurança, tendo em conta os habilitadores que não foram estudados, dada a dificuldade que implicaria a sua análise. Neste sentido preceder-se-ia à análise dos tipos de informação relacionadas à cibersegurança, os stakeholders da mesma o existente catálogo de serviços e os skills/ competências associadas às estruturas organizacionais.

Utilizar a mesma metodologia e abordagem para avaliar outras organizações do tipo e-commerce, para se conseguir entender um padrão na forma como a gestão da cibersegurança está a ser efetuada e gerida em organizações deste tipo.

Dar continuidade a este estudo de caso, fazendo mais duas análises: uma com base na norma internacional ISO27001, e outra com base no framework ITIL. Dessa forma, poder-se-ia fundamentar ou confrontar as conclusões teóricas com uma componente prática.

Utilizar a mesma metodologia e abordagem para outros estudos de caso do contexto académico semelhantes, em organizações distintas.

5.5. Considerações finais

Este caso de estudo revelou-se numa mais valia para mim tanto a nível pessoal, como a nível profissional, pois possibilitou-me uma visão mais abrangente sobre o conceito de Cibersegurança, a sua importância e aplicabilidade no contexto organizacional.

É de realçar que com a realização do caso estudo, foi possível por em prática os conhecimentos adquiridos ao longo do mestrado de Auditoria, no contexto de trabalho de pesquisa, preparação, execução e análise de dados, como também, me proporcionou um enriquecimento desses conhecimentos.

Referências Bibliográficas

Alter, S. (1992). *Information Systems : A Management Perspective.* Addison- Wesley.

Amaral, L., & Varajão, J. (2007). *Planeamento de sistemas de informação.* FCA - Editora Informática, Lda.

Anthony, R. N. (1965). *Planning and Control Systems : a Framework for Analysis.* Cambridge: Harvard University Press.

Arora, V. (2010). *Comparing different information security standards: COBIT vs. ISO 27001.* Qatar.

AXELOS. (2017). *ITIL What is ITIL ?* Obtido de https://www.axelos.com/best-practice-solutions/itil

Baptista, C. S., & Sousa, M. J. (2011). *Como Fazer Investigação, Dissertações, Tese e Relatórios - Segundo Bolonha.* Lisboa: Pactor.

Bartens, Y., Haes, S. D., Eggert, L., Heilig, L., Maes, K., Schulte, F., & VoB , S. (2014). A visualization approach for reducing the perceived complexity of COBIT 5. *International Conference on Design Science Research in Information Systems in Lecture Notes in Computer Science*, (pp. 403 - 407).

Bauer, M. W., & Gaskell, G. (2017). *Pesquisa qualitativa com texto, imagem e som - tradução de Pedrinho Guareschi.* Petrópoolis: Vozes.

Bhattacherjee, A. (2012). *Social Science Research: Principles, Methods, and Practices.* USA .https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks: Textbooks Collection .

bmc. (2017). *ITIL® Information Security Management*. Obtido de ITIL® Information Security Management

Bourdieu, P. (1999). *A miséria do mundo. Tradução de Mateus S. Soares.* Petrópolis: Vozes.

Bretschneider, S., & Wittmer, D. (1993). *Organizational Adoption of Microcomputer Technology: The Role of Sector.*

Buckinham, R. A., Hirschheim, R. A., Land, F. F., & Tully, C. J. (1987). *Information systems curriculum: a basis for course design.*

Caldeira, M. (2008). *Sistemas de Informação para a gestão.* Universidade aberta.

Cannon, D. L. (2008). *Certified Information Systems Auditor - Study Guide.* Wiley Publishing.

Carneiro, A. (2009). *Auditoria e Controlo de Sistemas de Informação.* FCA - Editora Informática.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J., & Rance, S. (2007). The IT Infrastructure Library - An Introductory Overview of ITIL® V3. *The IT Service Management Forum.*

Cascarino, R. E. (2007). *Auditor's Guide to Information Systems Auditing.* John Wiley & Sons.

Champlain, J. J. (2003). *Auditing Information Systems.* John Wiley & Sons.

Costa, C. B. (2010). *Auditoria Financeira - Teoria & Prática.* Rei dos Livros.

Diehl, A. A., & Tatim, D. C. (2004). *Pesquisa em ciências sociais aplicadas: métodos e técnicas.* São Paulo: Prentice Hall.

Earl, M. J. (1988). *Exploiting IT for Strategic Advantage - A framework of frameworks.* Oxford Institute of Information Management.

FFIEC. (2016). *FFIEC Information Technology Examination Handbook: Information Security.* Obtido de Federal Financial Institutions Examination Council: https://www.ffiec.gov/press/pdf/ffiec_it_handbook_information_security_booklet.pdf

Fortin, M. F. (1999). *O Processo de Investigação: da concepção à realização, 2ª Edição.* Lusociência.

Gaivéo, J. M. (2008). As pessoas nos sistemas de gestão da segurança da informação. *Tese de Doutoramento*.

Gantz, S. D. (2014). *The Basis of IT Audits - Purposes, Processes, and Practical Information.*

Gomes, J., & Romão, M. (2012). Seleção de uma abordagem de gestão de investimentos. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*.

Grilo, R. (2008). *Investigação em sistemas de informação organizacionais em Portugal: Caracterização do periodo de 2004 a 2007.* thesis.

Haguette, T. M. (1997). *Metodologias qualitativas na Sociologia.* Petrópolis: Vozes.

IDN-CESEDEN. (2013). *Estratégia da Informação e Segurança no Ciberespaço.* Lisboa: Instituto da Defesa Nacional - https://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf.

IIA, T. (2004). *The Role of Internal Auditing in Enterprise-wide Risk Management.* Florida: The Institute of Internal Auditors.

ISACA. (2010). *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals.*

ISACA. (2012a). *COBIT 5 for Information Security.*

ISACA. (2012b). *CoBIT 5 - A Business Framework for the Governance and Management of Enterprise IT.*

ISACA. (2013a). *COBIT 5: Enabling Information.*

ISACA. (2013b). *Transforming Cybersecurity: Using COBIT® 5*, pp. ISBN: 978-1-60420-342-4.

ISACA. (2016). *A HISTORICAL TIMELINE- The COBIT® Framework*. Obtido de http://www.isaca.org/COBIT/Documents/COBIT-20-Timeline.PDF

ISACA. (2017). *About COBIT 5 | What is COBIT 5 ?* Obtido de https://cobitonline.isaca.org/about

ISO, I. O. (2018). *ISO/IEC 27001 Information security*. Obtido de International Organization for standartization (ISO): https://www.iso.org/isoiec-27001-information-security.html

ITGI. (2005). *Aligning COBIT, ITIL and ISO17799 for Business Benefit: Management* .

ITGI. (2007). *COBIT 4.1.* USA: IT Governance Institute.

ITGI. (2014). *COBIT 4.1 Executive Summary.* Obtido de http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

itSMF-12ª Conferência Anual. (2015). Para além do ITIL: Tradição e Novas Tendências. *itSMF-12ª Conferência Anual.* Lisboa.

ITU. (2009). *Understanding Cybercrime: A Guide for Developing Countries. Technical report.*

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Roning, J. (2007). Information Security Standards and Global Business. *IEEE International Conference on Industrial Technology.* Mumbai, India.

Keyes - Pearce, S. V. (2005). *IT Value Management in Leading Firms: The Fit Between Theory and Practice.* University of Sydney.

King, J. L., & Kraemer, K. L. (1988). Information Resource Management: Is it Sensible and Can It Work? Em *Information & Management* (pp. 7-14).

Knapp, K. J., Marshall, T. E., Byrd, T. A., & Morris, R. F. (2009). *Information security policy: An organizational-level process model.* Computers & Security.

Kruger, H. A., & Kearney, W. D. (2008). *Consensus Rankink - An ICT security awareness case study* . Computers & Security.

Lakatos, E. M., & Marconi, M. d. (1996). *Técnicas de pesquisa.* São Paulo: Editora Atlas.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). *Threats to information systems: today's reality, yesterday's understanding.* MIS Quarterly.

Lucey, T. (2005). *Management Information Systems.* Thomson.

Maes, K., Bruyn, P. D., Oorts, G., & Huysmans, P. (2014). On the need for evolvability assessment in value management. *47th Hawaii International Conference on System Science*, (pp. 4406 - 4415).

Marchand, D. A. (2000). *Competing with Information: A Manager's Guide to Creating Business Value with Information Content.* New York: John Wiley & Sons.

McNamee, D., & Selim, G. M. (1998). *Risk Management: Changing the Internal Auditor's Paradigm.* Florida: The Institute of Internal Auditors Research Foundation.

Mendes, R. R., Oliveira, R. R., Costa, A. F., & Gomes, R. (2015). Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002. *Revista Principia - Divulgação Científica e Tecnológica do IFPB*, 69-80.

Minayo (Org), M. C. (2010). *PESQUISA SOCIAL: Teoria, método e criatividade.* Petrópolis, Rio de Janeiro: Editora vozes.

Moeller, R. R. (2013). *Executive's Guide to IT Governance.* Hoboken, New Jersey: John Wiley & Sons.

Musaji, Y. F. (2001). *Auditing and Security.* John Wiley & Sons.

NIST. (2017). *National Institute of Standards and Technology*. Obtido de http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf - National Institute of Standards and Technology

NP ISO/IEC 27000. (2014). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* .

NP ISO/IEC 27001. (2013). *Tecnologias de Informação. Técnicas de Segurança. Sistemas de gestão de segurança da informação – Requisitos - Norma Portuguesa. Instituto Português da Qualidade.* Caparica.

NP ISO/IEC 27002. (2013). *Information Technology - Security Techniques: Code of practice for information security management. International Standard.*

Oliveira, A. (1994). O valor da informação. Em *Sistemas de informação.*

Oliveira, A. (1998/9). A importancia dos Sistemas de Informação para a indústria. *Revista Estudos de Gestão*.

Oliveira, J. A. (2006). *Método de Auditoria a Sistemas de Informação.* Porto Editora, S.A.

Oz, E. (2009). *Management Information Systems* . Thomson.

Pereira, C., & Ferreira, C. (2015). Indentificação de Práticas e Recursos de Gestão do Valor das TI no COBIT 5. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*.

Piattini, M. (2000). *Auditing Information Systems.* Idea Group Publishing.

Pimenta, A. M., & Quaresma, R. F. (2016). *A segurança dos sistemas de informação e o comportamento dos usuários : Information Systems Security and Users Behavior.* Revista de Gestão da Tecnologia e Sistemas de Informação.

Porter, M. E. (1985). *Competitive Advantage.* New York: The Free Press.

Raposo, R. G. (2016). *GESTÃO DO RISCO E GARANTIA DA INFORMAÇÃO: A INFLUÊNCIA DO FATOR HUMANO E DA ÉTICA NA SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA NAS ORGANIZAÇÕES.* Lisboa: Thesis.

Ray, A. K., & Acharya, T. (2004). *Information Technology: Principles and Applications.* Prentice Hall of India Private Limited.

Resolução da Assembleia da Repúblicanº 63/2015. (12 de Junho de 2015). Resolução da Assembleia da Repúblicanº 63/2015 - Diário da República, 1.ª série — N.º 113 — 12 de junho de 2015. pp. 3738-3742.

Rivas, F. G.-P. (1984). *Estruturas Organizativas e Information en la Empresa.* Madrid: Association para el Progreso de la Direction.

Ronen, B., & Spiegler, I. (1991). Information as inventory: A new conceptual view. Em *Information & Management* (pp. 239-247).

Rouse, M. (2009). *Security Information Management (SIM).* Search Security - TechTarget.

Silva, P. T., Carvalho, H., & Torres, C. B. (2003). *Segurança dos Sistemas de Informação: Gestão Estratégica da Segurança Empresarial.* Centro Atlântico.

Sousa, J. P., Moreira, S. V., & Vieria (Org), J. P. (2006). *A prática antes da teoria e o foco no objetivo: uma proposta para oensino universitário de jornalismo.* Intercon/UERJ: São Pulo/Rio de Janeiro.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*.

Sutter, É. (1993). *Maitriser l'information pour garantir la qualité.* Paris: Afnor.

Teixeira, M. d. (2006). Dissertação de Mestrado em Contabilidade e Auditoria. *Contributo da auditoria interna para uma gestão eficaz.*, pp. 72-75.

Thomas, M. (13 de Abril de 2015). *Pulicações centrais do COBIT: Uma rápida visão*. Obtido de ISACA: http://www.isaca.org/COBIT/focus/Pages/the-core-cobit-publications-a-quick-glance-portuguese.aspx

Wadlow, T. A. (2000). *The process of network security: designing and managing a safe network.* Addison - Wesley Professional .

Ward, J., Griffiths, P., & Whitmore, P. (1990). *Strategic planning for information systems.* Chichester, West Sussex, England Wiley.

Whitman, M. E., & Mattord, H. J. (2008). *Principles os Information Security.*

Wilkin, C., Campbell, J., Moore, S., & Grembergen, W. V. (2013). Co-Creating Value from IT in a Contracted Public Sector Service Environment: Perspectives on COBIT and Val IT. *Journal of Information Systems*, 283-306.

Workman, M., Bommer, W. H., & Straub, D. (2008). *Security lapses and the omission of information security measures: A threat control model and empirical test.* Security lapses and the omission of information security measures: A threat control model and empirical test.

Yin, R. K. (2009). *Case study research: design and methods.* Thousand Oaks: SAGE Publications. Obtido de http://www.madeira-edu.pt/LinkClick.aspx?fileticket=Fgm4GJWVTRs%3D&tabid=3004

Zorrinho, C. (1991). *Gestão da Informação.* Lisboa: Editorial presença.

Anexos

Anexo I - Transforming cybersecurity using COBIT 5

No presente anexo, encontra-me as tabelas retiradas do COBIT5TC que serviram como base para a elaboração da check list. **As tabelas que encontram neste anexo resultam apenas de uma tradução às tabelas encontradas no documento original.**

Nas tabelas 41 e 42 encontram-se representados os princípios (primeira coluna) associados ao seu objetivo (segunda coluna) e o conjunto de procedimentos aplicados à cibersegurança (terceira coluna).

Princípio	Objetivo	Cibersegurança
Suporte ao Negócio		
Foco no negócio	Garantir que a segurança da informação esteja integrada nas atividades essenciais do negócio	• Analisar o risco do negócio face a ataques/ falhas nos processos de negócio e priorizar de acordo com a cibersegurança. • Estabelecer o nível de tolerância de ataques e violações, através da perspetiva do negócio.
Fornecer qualidade e valor aos stakeholders	Garantir que a segurança da informação oferece valor e atende aos requisitos do negócio	Realizar análise de stakeholders (interna e externa) e obter requisitos para a cibersegurança. • Realizar análise de requisitos do negócio (legais/ regulatórios, internos e externos) e obter requisitos específicos para cibersegurança. • Definir objetivos de alto nível de cibersegurança e obter o sinal da gestão sênior.
Cumprir com os requisitos legais e regulamentares relevantes	Garantir que as obrigações legais sejam cumpridas, as expectativas dos stakeholders sejam geridas e as penalidades civis ou criminais sejam evitadas	• Identificar leis, regulamentos e regras de governança para a cibersegurança e seus requisitos a cumprir. • Transmitir esses requisitos e seus componentes ao longo do sistema geral de cibersegurança.
Fornecer informações oportunas e precisas sobre o desempenho da segurança da informação	Apoiar os requisitos do negócio e gerir o risco de informação.	• Estabelecer indicadores chave de desempenho de cibersegurança (KPIs) e relatórios regulares. • Estabelecer pontos chave de risco de cibersegurança (KRIs) e relatórios regulares.
Avaliar atuais e futuras ameaças à informação	Analisar e avaliar as ameaças emergentes à segurança da informação, de modo a que as ações sejam informadas em tempo útil e oportunas para mitigar riscos.	• Identificar ameaças para todas as partes da empresa. • Antecipar ameaças futuras através do cibercrime e da ciberguerra. • Coletar dados e evidências sobre incidentes de cibersegurança, ataques e violações. • Aplicar técnicas detalhadas de análise de dados para obter uma visão razoavelmente sólida sobre o futuro da cibersegurança. • Aproveitar os conhecimentos externos, caso seja apropriado.
Promover a melhoria contínua da segurança da informação	Reduzir os custos, melhorar a eficiência e eficácia e promover uma cultura de melhoria contínua na segurança da informação	• Estabelecer um processo de melhoria contínua, com base na experiência passada e nas tendências futuras. • Estabelecer um processo de cibersegurança tolerante a falhas / erros. • Estabelecer uma cultura que promova a melhoria e o pensamento adaptativo.

Tabela 41 - Princípios do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

Defender o Negócio		
Adotar uma abordagem baseada no risco	Certificar-se de que o risco seja tratado de forma consistente e eficaz.	• Definir um processo apropriado de identificação e avaliação de risco. • Validar as opções de tratamento de risco na cibersegurança. • Alinhar o risco com o modelo geral de governança selecionado. • Incluir incidentes passados e aprendizagens técnicas/organizacionais. • Identificar e avaliar o novo risco decorrente do cibercrime e da ciberguerra.
Proteger a informação confidencial	Impedir a divulgação de informações classificadas (por exemplo, confidenciais ou sensíveis) a pessoas não autorizadas.	• Estabelecer a classificação de dados no que diz respeito ao cibercrime e à ciberguerra. • Incluir armazenamento e serviços baseados na cloud, bem como dados que residem ou fluem e dispositivos móveis ou públicos. • Fornecer informações relacionadas à cibersegurança para identidade geral e gestão de acessos
Concentrar-se nas aplicações de negócio críticas	Priorizar recursos escassos de segurança da informação, protegendo as aplicações do negócio nos quais um incidente de segurança da informação teria o maior impacto.	• Identificar aplicações críticas no negócio executando uma análise de impacto no negócio (BIA) com uma perspetiva de cibersegurança. • Executar uma análise detalhada da dependência das aplicações críticas para identificar pontos de entrada potencialmente vulneráveis. • Alocar recursos e financiamentos de acordo com as ameaças reais de cibercrime e ciberguerra, e considerar vetores e abordagens de ataque indiretos.
Desenvolver sistemas de forma segura	Criar qualidade, sistemas de custo-benefício nos quais os empresários possam confiar (por exemplo, consistentemente robustos, precisos e confiáveis).	• Estabelecer controlos de ciclo de vida de software para aplicações auto- desenvolvidas e personalizadas. • Definir um processo de administração de cibersegurança para aplicações e sistemas potencialmente críticos. • Participar com os fornecedores para alcançar os controlos de cibersegurança a montante. • Envolver-se com os fornecedores para gerir vulnerabilidades e pontos de entrada.
Promover um comportamento responsável de segurança de informação		
Agir de forma ética e profissional	Certificar-se de que as atividades relacionadas à segurança da informação sejam realizadas de forma fiável, responsável e efetiva.	• Aplicar governança às políticas de cibersegurança, normas e procedimentos chave de operacionalidade. • Introduzir rotinas de auto- avaliação e avaliação por pares, para o pessoal exposto (garantia de integridade). • Executar verificações de antecedentes (com base em opt-in) para o pessoal da cibersegurança. • Definir e implementar verificações adequadas para novas contratações em posições sensíveis. • Definir e implementar procedimentos adequados para o final da contratação. •Assegurar o reconhecimento do pessoal através de incentivos e reconhecimento apropriados.
Fomentar uma cultura de segurança da informação positiva	Fornecer uma influência positiva de segurança da informação sobre o comportamento dos usuários finais, reduzir a probabilidade de ocorrência de incidentes de segurança da informação e limitar seu potencial impacto no negócio.	• Definir comportamentos de cibersegurança • Promover a conscientização sobre cibersegurança e cibercrime. • Fornecer exemplos práticos e casos de ataques / ameaças. • Destacar o impacto no negócio dos ataques / falhas.

Tabela 42 - Princípios do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

Nas tabelas 43, 44 e 45 encontram-se representados as políticas (primeira coluna) associados ao seu objetivo no contexto do COBIT5 (segunda coluna) e o conjunto de procedimentos aplicados à cibersegurança (terceira coluna).

Políticas	COBIT 5	Cibersegurança
Segurança da informação	Definição de segurança da informação e responsabilidades associadas. Visão em relação à segurança da informação, acompanhada de metas e métricas adequadas e uma explicação de como a visão é apoiada pela cultura e consciência de segurança da informação. Explicação de como a política de segurança da informação se alinha com outras políticas de alto nível. Elaboração de tópicos específicos, tais como gestão de dados, avaliação de risco de informação e cumprimento das obrigações legais, regulamentares e contratuais	Definir objetivos de alto nível de cibersegurança e obter a aprovação da gestão sênior. Estabelecer um processo de melhoria contínua com base na experiência passada e nas tendências futuras. Estabelecer um processo de cibersegurança tolerante a falhas / erros. Fornecer exemplos práticos e casos de ataques / violações. Destacar o impacto dos ataques / falhas no negócio Vincular aos princípios orientadores para a cibersegurança.
Controlo de acesso	A política de controlo de acesso fornece acesso adequado aos stakeholders internos e externos para atingir os objetivos do negócio. Além disso, esta política deve garantir que o acesso de emergência seja apropriadamente permitido e revogado em tempo util. Esta política destina-se a todas as unidades do negócio, fornecedores e terceiros correspondentes.	Isso pode ser medido através de métricas, como: • Número de violações de acesso que excedem o valor permitido; • Quantidade de interrupção do trabalho devido a direitos de acesso insuficientes; • Número de segregação de incidentes de deveres ou resultados de auditoria; • Número de solicitações de acesso de emergência; • Número de contas de emergência ativas em excesso de prazos aprovados;
Segurança da informação do pessoal	Executar verificações de antecedentes regulares de todos os funcionários e pessoas com posições-chave. Adquirir informações sobre o pessoal-chave nas posições de segurança da informação. Desenvolver um plano de sucessão para todas as principais posições de segurança da informação	Verificações completas de antecedentes para o pessoal-chave. Verificar o pessoal em posições-chave em que não ocorre rotação de acordo com a frequência predefinida. Listar todas as posições críticas de segurança da informação que não possuem pessoal de backup. Verificar se toda a equipa de segurança da informação possui as habilidades atuais e pertinentes necessárias e as certificações relacionadas.
Segurança da informação física e ambiental	O objetivo desta política é fornecer orientação sobre a proteção dos locais físicos e controlos ambientais que fornecem recursos para suportar operações	A segurança da localização física pode ser medida pelo número de vulnerabilidades exploráveis identificadas e / ou incidentes atribuídos a ameaças de localização física (riscos criminais, de transporte e industriais, ameaças naturais). Os controlos ambientais podem ser verificados medindo o número de vulnerabilidades exploráveis identificadas e / ou incidentes atribuídos aos sistemas de controlo ambiental.
Resposta a incidentes	Esta política cobre a necessidade de responder aos incidentes em tempo util para recuperar as atividades do negócio. A política deve incluir: •A definição de incidente de segurança da informação e como serão tratados. • Requisitos para o estabelecimento da equipa de resposta a incidentes, com funções e responsabilidades organizacionais • Requisitos para a criação de um plano testado de resposta a incidentes, que fornecerá procedimentos documentados e diretrizes.	Verificação de procedimentos documentados e diretrizes para: - Crítica dos incidentes - Relatórios e processo de escalonamento - Recuperação (incluindo): objetivos de tempo de recuperação (RTOs) para retornar ao estado fiável; investigação e preservação do processo; testes e prática - Reuniões pós-incidente para documentar análise de causas raiz e aprimoramentos de documentos de práticas de segurança da informação para evitar futuros eventos semelhantes. - Documentação e encerramento de incidentes

Tabela 43 - Políticas do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

Políticas	COBIT 5	Cibersegurança
Continuidade do negócio e recuperação de desastres	A política deve incluir: • Análise do impacto no negócio (BIA) • Planos de contingência empresarial com recuperação fiável • Requisitos de recuperação para sistemas críticos • Limites e disparadores definidos para contingências, escalada de incidentes • Plano de recuperação de desastres (DRP) • Testes e prática	Identificar aplicações criticas do negócio executando uma BIA na perspetiva de cibersegurança. Executar uma análise de dependência detalhada a partir das aplicações críticas do negócio para identificar pontos de entrada potencialmente vulneráveis. Alocar recursos e fundos de acordo com as ameaças reais de cibercrime e ciberguerra, e considerar vetores de ataque indiretos e abordagens de ataque. Adotar a mentalidade do maior estrago do atacante com o menor esforço.
Gestão de ativos	Estabelecer: • Classificação de dados • Propriedade de dados • Classificação do sistema e propriedades • Utilização de recursos e priorização • Gestão do ciclo de vida do ativo • Medidas de proteção de ativos	Estabelecer a classificação de dados em relação ao cibercrime e ciberguerra. Incluir armazenamento e serviços baseados na cloud, bem como dados que residem ou fluem através de dispositivos móveis ou públicos.
Regras de comportamento	• Usos e comportamentos aceitáveis no trabalho: - Expectativa de privacidade - Uso de sistemas e ativos empresariais - Internet; email; mensagem instantânea; acesso remoto; dispositivos móveis e uso da câmara; uso da impressora, scanner e fax; uso de computadores pessoais para atividades empresariais • Uso e comportamentos aceitáveis fora do local: Redes sociais; blogs	Promover uma cultura que promova a melhoria e o pensamento adaptativo. Definir orientação comportamental de cibersegurança. Fomentar a conscientização sobre cibersegurança e cibercrime.
Adquirir sistemas de informação, desenvolvimento e manutenção de software	• Segurança da informação no processo do ciclo de vida • Processo de definição de requisitos de segurança da informação • Segurança da informação dentro do processo de aquisição • Práticas de codificação seguras • Integração da segurança da informação com a gestão de mudanças e de configuração	Aproveitar os conhecimentos externos, conforme apropriado. Estabelecer controlos no ciclo de vida do software para aplicações auto-desenvolvidas e personalizadas. Definir o processo de instalação de cibersegurança para aplicações e sistemas potencialmente críticos.
Gestão de Fornecedores	• Gestão de contratos: - Termos e condições de segurança da informação - Avaliação da segurança da informação - Acompanhamento de contratos de segurança da informação	Interagir com os fornecedores para alcançar os controlos de cibersegurança. Interagir com os fornecedores para gerir vulnerabilidades e pontos de entrada
Gestão das operações e da comunicação	Arquitetura de segurança de informações de TI e design de aplicativos: - Comitê de direção - Padrões - Diretrizes • SLA: - Operações internas - Operações externas • Procedimentos operacionais de segurança de informação de TI	Coletar dados e evidências sobre incidentes de cibersegurança, ataques e violações Aplicar técnicas detalhadas de análise de dados para obter uma visão razoavelmente sólida sobre o futuro da cibersegurança. Incluir incidentes passados e aprendizagens técnicas / organizacionais. Identificar e avaliar novos riscos decorrentes do cibercrime e da ciberguerra. Fornecer informações relacionadas à cibersegurança para identidade geral e gestão de acessos.

Tabela 44 - Políticas do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

Políticas	COBIT 5	Cibersegurança
Conformidade	• Processo de avaliação de conformidade de segurança de informações de TI: - Regulamentação - Contractual - Empreendimento • Desenvolvimento de métricas • Repositórios de avaliação: - Público - Conteúdo - Estrutura - Acompanhamento	Identificar leis, regulamentos e regras de governança para a cibersegurança e definir requisitos . Transmitir esses requisitos ao longo do sistema geral de cibersegurança e seus componentes. Estabelecer KPIs de cibersegurança e relatórios regulares. Aplicar governança às políticas de cibersegurança, normas e KOPs. Introduzir autoavaliação e rotinas de avaliação por pares para pessoal exposto (garantia de integridade). Executar verificações de antecedentes (com base em opt-in) para pessoal da cibersegurança. Definir e implementar verificações adequadas para novas contratações das posições sensíveis. Definir e implementar procedimentos adequados para o encerramento das posições Assegurar o reconhecimento do pessoal de cibersegurança através de incentivos e reconhecimento apropriados
Gestão de Risco	• Plano de gestão do risco organizacional: - Âmbito/alcance - Papéis e responsabilidades - Metodologias - Ferramentas e técnicas - Processos de repositório • Perfil de risco de informação	Analisar o risco de ataques / falhas aos processos do negócio e priorizar de acordo com a cibersegurança. Estabelecer o nível de tolerância de ataques e violações, na perspetiva do negócio. Executar análise de stakeholders (interna e externa) e obter requisitos para a cibersegurança. Estabelecer KRIs de cibersegurança e relatórios regulares. Identificar ameaças a todas as partes da empresa. Antecipar ameaças futuras através do cibercrime e da ciberguerra. Definir o processo adequado de identificação e avaliação de riscos. Validar as opções de tratamento de risco na cibersegurança. Alinhar o risco com o modelo geral de governança selecionado.

Tabela 45 - Políticas do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

Tal como referido já anteriormente, o modelo de referência de processos do COBIT5 está dividido em duas áreas principais de atividade – governação e gestão, divididas em domínios de processos e subdividido em 37 processos.

Quanto aos cinco processos da área de governação, estes estão associados ao domínio avaliar, dirigir e monitorizar (*EDM - Evaluate, Direct and Monitor*). Em relação aos trinta e dois da área da gestão, estes dividem-se pelos domínios alinhar, planear e organizar (*APO - Align, Plan and Organize*), construir, adquirir e implementar (*BAI - Build, Acquire and Implement*), entrega, serviço e suporte (DSS - *Deliver, Service and Support)* e monitorizar, avaliar e aferir (*MEA - Monitor, Evaluate and Assess*) (ISACA, 2012b).

Nas tabelas 46 à 51, apresentam-se a descrição dos processos e subprocessos da área de governação associados ao domínio avaliar, dirigir e monitorizar (*EDM - Evaluate, Direct and Monitor*). Na tabela são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT 5	Cibersegurança
EDM01 Assegurar a definição e manutenção de um framework de governança	Analisar e articular os requisitos de governança de TSI da organização, executar e manter estruturas, princípios, processos e práticas base eficazes, havendo claridade no que diz respeito às responsabilidades e autoridades associadas, para se conseguir atingir a missão, meta e objetivos da entidade.	
EDMO1.01 Avaliar o sistema de Governança	Fatores ambientais internos e externos (legal, regulatório, contratual). Identificar tendências que influenciem o desenvolvimento da Governança	• Rever disposições legais e regulamentares relativas ao cibercrime e ciberguerra • Identificar e validar o modelo de governança para a cibersegurança ("tolerância zero" versus "viver com ela") • Identificar adaptabilidade, capacidade de resposta e resiliência do modelo de governança em termos de ataques/violações de cibersegurança • Identificar quaisquer elementos de governança rígidos / frágeis que, inadvertidamente, possam conduzir ao cibercrime e à ciberguerra
	A medida em que a segurança da informação atende às necessidades empresariais de conformidade e regulamentares	Validar as necessidades do negócio (expressas e implícitas) em relação a ataques e violações • Categorizar ataques e ameaças, em termos de conformidade e necessidades regulatórias - identificar lacunas e deficiências • Documentar deficiências sistêmicas na cibersegurança no que diz respeito ao negócio e seus impulsionadores de lucro
	Determinar o modelo ideal de tomada de decisão para a segurança da informação.	Determinar um modelo de tomada de decisão para a cibersegurança • Prever respostas a ciberataques específicos

Tabela 46 - Processo EDMO1 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT 5	Cibersegurança
EDM01.02 Dirigir o sistema de Governança	Obter o compromisso da alta administração com a segurança e gestão de risco da informação	• Identificar o nível de tolerância da alta administração em relação a ataques e violações. • Obter compromisso de gestão para o modelo de governança selecionado. • Obter gestão formal do apetite pelo risco em termos de cibercrime e ciberguerra.
	Mandato de uma função de segurança da informação da empresa.	Atribuir uma função de cibersegurança apropriada, incluindo resposta a incidente e ataques. • Estabelecer comunicação entre a função de cibersegurança e outras funções de segurança da informação
	Mandato de um comitê de direção de segurança da informação (ISSC).	• Assegurar a participação do comitê de direção ao nível da cibersegurança • Incorporar atividades de transformação de cibersegurança na agenda do comitê de direção.
	Implementar informações hierárquicas e escala de procedimentos de decisão	• Estabelecer escala de pontos para ataques, infrações e incidentes. • Definir escala de etapas para atividades de cibersegurança e etapas de transformação (ex, novas vulnerabilidades e ameaças). • Estabelecer procedimentos de decisão em modo rápido
	Alinhar a estratégia de segurança da informação com a estratégia do negócio	• Alinhar, na medida apropriada, a cibersegurança com segurança genérica da informação. • Destacar áreas de cibersegurança que são deliberadamente mantidas separadas e distintas.
	Promover uma cultura e ambiente de segurança da informação.	• Definir a cultura alvo para a cibersegurança • Definir o cenário para a conscientização cibercrime / ciberguerra. • Desenvolver orientação apropriada para associados.
EDM01.03 Monitorizar o sistema de Governança	Monitorizar mecanismos regulares e rotineiros para garantir que o uso de sistemas de medição de segurança da informação esteja em conformidade com legislação e regulamentação.	• Integrar medidas e métricas de cibersegurança em mecanismos de verificação de conformidade rotineira. • Monitorar a conformidade das medidas de cibersegurança que não fazem parte de mecanismos regulares e rotineiros.
	Analisar as implicações gerais da mudança da paisagem de ameaças.	• Avaliar as ameaças e vulnerabilidades relevantes para a cibersegurança cibernética. • Incorporar a mudança da paisagem da ameaça na governança de transformação da cibersegurança • Identificar e articular qualquer mudança de jogo ou mudanças de paradigma na cibersegurança

Tabela 47- Processo EDMO1 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT 5	Cibersegurança
EDM02 Assegurar a entrega de benefícios	Otimizar a contribuição de valor a partir dos processos de negócio, dos serviços e ativos de TSI, resultante de investimentos realizados pela área de TSI a custos aceitáveis.	
EDM02.01 Avaliar a otimização de valor	Identificar e registrar os requisitos dos stakeholders para proteger os seus interesses e fornecer valor através da atividade de segurança da informação.	Identificar e registar dados de casos do negócio em relação ao impacto/ dano contra o investimento em cibersegurança • Identificar e registar os requisitos dos stakeholders em termos de ataques, ameaças e incidentes. • Integrar a direção da cibersegurança na direção geral da segurança da informação.
EDM02.02 Otimização direta do valor	Estabelecer um método para demonstrar o valor da segurança da informação para assegurar o uso eficiente dos ativos existentes relacionados	• Estabelecer um método para demonstrar o valor da cibersegurança dentro da segurança da informação. • Estender esse método para demonstrar o valor direto para o negócio
	Assegurar o uso de medidas financeiras e não financeiras para descrever o valor agregado das iniciativas de segurança da informação.	Incluir medidas financeiras (impacto, danos) e não financeiras (legal, reputação, operacional, outras) para descrever o valor agregado das iniciativas de cibersegurança
	Usar métodos de reporte focados no negócio sobre o valor agregado das iniciativas de segurança da informação.	Incorporar o reporte de cibersegurança nos métodos genéricos de segurança da informação.
EDM02.03 Monitorizar a otimização de valor	Acompanhar os resultados das iniciativas de segurança da informação e comparar com as expectativas para garantir a entrega de valor em relação aos objetivos do negócio.	• Acompanhar os resultados e efeitos da cibersegurança, relativamente às mudanças nos ataques, ameaças e incidentes. • Comparar os resultados com as expectativas iniciais (estado atual) e futuro (estado do alvo). • Comparar resultados com etapas de transformação e marcos.

Tabela 48- Processo EDMO2 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT 5	Cibersegurança
EDM03 Assegurar a otimização do risco	Garantir que o apetite e a tolerância de risco da organização são compreendidos, articulados e comunicados, e que o risco associado ao uso de TSI é identificado e gerido.	
EDM03.01 Avaliar a gestão de risco	Determinar o apetite de risco empresarial	• Determinar os níveis de apetite / tolerância ao risco para ataques e violações • Combinar os níveis de tolerância em relação ao modelo geral de governança ("tolerância zero" versus "viver com ele"). • Comparar os níveis de tolerância ao risco e comparar inconsistências entre a segurança da informação e a cibersegurança.
	Medir o nível de integração da informação acerca da gestão de risco com o modelo geral ERM	Medir o nível de integração da avaliação e gestão de risco de cibersegurança com gestão geral de risco de informação.
EDM03.02 Gestão de risco direta	Integrar a gestão de riscos da informação no modelo geral ERM.	Integrar a avaliação e gestão de riscos de cibersegurança na gestão geral de segurança da informação.
EDM03.03 Monitorizar a gestão de riscos	Acompanhar o perfil de risco da informação empresarial ou o apetite de risco para alcançar o equilíbrio ideal entre riscos e oportunidades do negócio.	• Monitorizar o perfil de risco para ataques /ameaças e o apetite de risco correspondente para alcançar um equilíbrio ótimo entre riscos de cibersegurança e as oportunidades de negócios. • Alinhar o risco em termos do modelo geral de governança ("tolerância zero" versus "viver com ele").
	Incluir os resultados dos processos de gestão de risco de informação como inputs para o painel global de risco de negócios.	Incluir avaliação e gestão de riscos de cibersegurança como inputs para o risco geral de informações.

Tabela 49- Processo EDMO3 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT 5	Cibersegurança
EDM04 Assegurar a otimização de recursos	Garantir que estejam disponíveis recursos adequados e suficientes relacionados a TSI (pessoas, processos e tecnologia), que apoiem os objetivos da organização de forma eficaz a um custo ideal.	
EDM04.01 Avaliar a gestão dos recursos	Avaliar a eficácia dos recursos de segurança da informação em termos de provisão, prática, conscientização e competências dos recursos necessários em comparação com as necessidades do negócio.	Avaliar a eficácia dos recursos de cibersegurança em comparação com as necessidades de segurança da informação e risco de informação. • Incluir recursos externos na avaliação.
EDM04.02 Dirigir a gestão de recursos	Garantir que a gestão de recursos de segurança da informação esteja alinhada às necessidades do negócio.	• Certificar-se de que a gestão de recursos de cibersegurança esteja alinhada às necessidades de segurança de informações abrangentes. • Validar recursos de cibersegurança em termos de metas e objetivos específicos. • Incluir gestão de recursos externos.
EDM04.03 Monitorizar a gestão de recursos	Medir a eficácia, eficiência e capacidade dos recursos de segurança da informação contra as necessidades do negócio.	Medir a eficácia dos recursos de cibersegurança (interna e externa) relativamente às necessidades, objetivos e metas definidos pela segurança da informação.

Tabela 50- Processo EDMO4 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT 5	Cibersegurança
EDM05 Assegurar a transparência dos Stakeholders	Garantir que a medição e relatórios de desempenho e conformidade da área de TSI são transparentes, e que existe a aprovação dos stakeholders nas metas, métricas e ações corretivas necessárias.	
EDM05.01 Avaliar os requisitos do relatório dos stakeholders	Determinar o público, incluindo indivíduos internos, externos ou grupos, para comunicação e relatórios.	• Determinar o público interno e externo (geralmente restrito) para comunicar e informar sobre a cibersegurança. • Incorporar as necessidades de confidencialidade e sigilo no processo de identificação.
	Identificar requisitos para relatórios sobre segurança da informação para os stakeholders.	• Identificar os requisitos de relatórios para a cibersegurança (conteúdo, detalhes). • Alinhar requisitos de relatórios às necessidades dos stakeholders internos e externos (público definido).
	Identificar os meios e canais para comunicar problemas de segurança da informação.	• Identificar os meios e canais para comunicar questões e informações de cibersegurança
EDM05.02 Dirigir a comunicação e reporte aos stakeholders	Priorizar os relatórios sobre questões de segurança da informação aos stakeholders	• Priorizar relatórios de cibersegurança para os stakeholders. • Aplicar os princípios de menos privilégio e necessidade de conhecer as prioridades de relatórios de cibersegurança.
	Realizar auditorias internas e externas para avaliar a eficácia do programa de governança de segurança da informação.	• Realizar auditorias internas e externas para avaliar a eficácia do programa de governança da cibersegurança • Definir claramente e articular instâncias de dependência do trabalho de terceiros (para auditores externos). • Definir e observar formalmente os requisitos de confidencialidade e sigilo para auditores externos.
	Produzir relatórios de status de segurança de informações regulares para os stakeholders.	Produzir relatórios de status da cibersegurança regulares para os stakeholders, tendo em consideração as restrições a serem aplicadas.
EDM05.03 Monitorizar a comunicação com os stakeholders	Estabelecer monitorização e relatórios para segurança de informações e gestão de riscos de informações, com base no domínio MEA	Estabelecer a monitorização da cibersegurança, com base no domínio MEA.

Tabela 51- Processo EDMO5 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Apesar de existirem processos destinados à gestão e outros à governação, existem alguns que são comuns aos dois, como é o caso do processo APO01 e APO02, associados aos domínios alinhar, planear e organizar (*APO - Align, Plan and Organize)*. Nas tabelas 52 e 53, apresenta-se a descrição desses processos e subprocessos na vertente de governação. Na tabela são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT 5	Cibersegurança
APO01 Gerir o framework de gestão de TSI	Esclarecer e preservar a missão e visão da governança de TSI. Implementar e manter mecanismos e jurisdição que tratem da gestão da informação e do uso de TSI na organização e que sustentem os objetivos de gestão, cumprindo com os princípios e políticas delineados.	
APO01.01 Definir a estrutura organizacional	Alinhar a organização relacionada à segurança da informação com modelos organizacionais de arquitetura corporativa.	• Alinhar a organização à cibersegurança nas funções de segurança da informação e de risco da informação. • Definir modelo RACI de alto nível para a função de cibersegurança, incluindo recursos externos. • Destacar qualquer obstáculo ou outra segregação organizacional de deveres / informações. • Estabelecer uma plataforma / comitê apropriado para cibersegurança.
	Estabelecer um ISSC (ou equivalente).	
	Definir a função de segurança da informação, incluindo funções internas e externas, recursos e direitos de decisão necessários.	• Definir a organização da cibersegurança em termos de capacidades, baseada no RACI. • Identificar e definir formalmente os direitos de decisão para a organização de cibersegurança. • Incluir e considerar quaisquer direitos de decisão estendidos que possam ser aplicáveis em situações tratamento de crises / incidentes
APO01.02 Estabelecer funções e responsabilidades	Determinar as obrigações de segurança da informação de outras funções organizacionais.	• Determinar obrigações, responsabilidades e tarefas de cibersegurança de outras funções organizacionais.
APO01.04 Comunicar os objetivos e direções de gestão	Definir as expectativas em relação à segurança da informação, incluindo ética e cultura organizacional específicas.	• Definir as expectativas em relação à cibersegurança, incluindo ética e cultura. • Destacar claramente como essas expectativas correspondem ao modelo geral de governança (“tolerância zero” versus “viver com isso”). • Destacar quaisquer descontinuidades éticas / culturais que existam ou surjam.
	Desenvolver um programa de consciencialização de segurança da informação	• Desenvolver um programa de consciencialização sobre cibersegurança.
APO01.08 Manter a conformidade com políticas e procedimentos	Agendar e realizar avaliações regulares para determinar a conformidade com políticas e procedimentos de segurança da informação	• Agendar e realizar avaliações regulares para determinar a conformidade da cibersegurança • Identificar e anotar quaisquer exceções à conformidade que possam ser necessárias na cibersegurança.

Tabela 52- Processo APO01 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT 5	Cibersegurança
APO02 Gestão Estratégica	Fornecer uma visão holística do negócio, do ambiente de TSI, do sentido a tomar na organização e das iniciativas necessárias para migrar do estado atual para o ambiente futuro desejado. Alavancar os elementos essenciais e componentes da arquitetura da organização, incluindo os serviços prestados externamente e recursos relacionados, com vista a atingir uma resposta ágil, fiável e eficiente aos objetivos estratégicos.	
APO02.01 Entender a direção da organização	Entender como a segurança da informação deve suportar os objetivos corporativos gerais e proteger os interesses dos stakeholders	Entender como a cibersegurança deve suportar os objetivos corporativos gerais e proteger os interesses dos stakeholders.

Tabela 53 - Processo APO02 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Tal como referido na revisão da literatura, no COBIT 5, os processos *APO13 Manage security, e DSS05 Manage security services* fornecem orientação básica sobre como definir, operar e monitorar um sistema de gestão de segurança geral.

Nas tabelas 54 e 55 são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT5	Cibersegurança
APO13 Gestão da Segurança	Definir, operacionalizar e monitorizar um sistema para a gestão de segurança da informação.	
APO13.01 Estabelecer e manter um sistema de gestão de segurança da informação (SGSI).	Estabelecer e manter um SGSI que forneça uma abordagem padrão, formal e contínua, à gestão de segurança da informação, facultando uma tecnologia segura e processos de negócio alinhados com os requisitos do negócio e gestão de segurança corporativa.	• Incorporar controlos relacionados à cibersegurança dentro do SGSI geral. • Definir relação entre os controlos de cibersegurança e controlos genéricos de segurança de informações (SGSI).
APO13.02 Definir e gerir um plano de tratamento de riscos de segurança da informação	Manter um plano que descreva como o risco de segurança da informação deve ser gerido e alinhado à estratégia corporativa e à arquitetura corporativa. Garantir que as recomendações para implementar melhorias de segurança sejam baseadas em casos do negócio aprovados e implementadas como parte integrante do desenvolvimento de serviços e soluções	• Identificar e categorizar o risco relacionado à cibersegurança e as opções de tratamento. • Incorporar tratamento de risco de cibersegurança no plano geral de segurança da informação. • Justificar as opções de tratamento em termos do business case selecionado. • Identificar e listar todos os controlos existentes e inclui-los no tratamento e plano de risco de segurança da informação.
APO13.03 Monitorar e rever o SGSI.	Manter e comunicar regularmente a necessidade e os benefícios da melhoria contínua de segurança da informação. Coletar e analisar dados sobre o SGSI e melhorar a sua eficiência. Corrigir não conformidades para evitar recorrência. Promover uma cultura de segurança e melhoria contínua.	• Definir processo de melhoria contínua para cibersegurança • Definir o mecanismo de análise de lacunas para o risco de cibersegurança vs. tratamento / controlos existentes. • Incorporar processos de gestão de mudança organizacional. • Incluir melhoria contínua nos conjuntos de controlo corporativo e social.

Tabela 54- Processo APO13 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
DSS05 Gerir Serviços de segurança	Proteger a informação da organização para manter o nível de risco de segurança da informação aceitável, de acordo com a política de segurança. Estabelecer e manter as funções de segurança da informação e os direitos de acesso, e realizar a monitorização de segurança.	
DSS05.01 Proteger contra malware.	Implementar e manter medidas preventivas, de deteção e corretivas em toda a organização para proteger os sistemas de informação e tecnologia contra malware (por exemplo, vírus, worms, spyware, spam).	• Implementar processo de reconhecimento e tratamento de exploits. • Implementar processo de reconhecimento de padrões (a todos os níveis) apontando para ataques / violações. • Incluir heurísticas baseadas em não assinatura para reconhecimento de malware.
DSS05.02 Gerir segurança de rede e conectividade	Usar medidas de segurança e procedimentos de gestão relacionados para proteger a informação sobre todos os métodos de conectividade.	• Identificar o conjunto de controlos existentes • Definir uma abordagem de proteção adequada a todos os níveis e topologia da rede. • Identificar potenciais pontos de entrada e combina-los com os controlos existentes.
DSS05.03 Gerir a segurança do terminal.	Garantir que os pontos de extremidade (por exemplo, laptop, desktop, servidor e outros dispositivos móveis ou de rede ou software) sejam protegidos num nível que seja igual ou superior aos requisitos de segurança definidos das informações processadas, armazenadas ou transmitidas.	• Categorizar endpoints e controlos relacionados (existentes). • Recolher potenciais pontos de entrada em todos os níveis (técnicas, sociais, etc.). • Analisar a atratividade do alvo para cada endpoint. • Comparar com qualquer histórico conhecido de ataques / violações.
DSS05.04 Gerir a identidade do usuário e acesso lógico.	Assegurar que todos os usuários tenham direitos de acesso à informação de acordo com seus requisitos de negócio e que sejam coordenados com as unidades de negócio que gerem os seus próprios direitos de acesso	• Ajustar os requisitos de negócio de acordo com os princípios de menor privilégio e necessidade de conhecimento. • Alinhar a gestão de identidade com o modelo de governança selecionado. • Identificar potenciais pontos de ataque numa perspetiva social e técnica. • Verificar os controlos existentes, particularmente no que diz respeito à segregação de funções • Analisar (baseado em cenário) o potencial de cibercrime e ciberguerra baseado em roubo de identidade e abuso de identidade.
DSS05.05 Gerir o acesso físico aos ativos de TI.	Definir e implementar procedimentos para conceder, limitar e revogar o acesso a instalações, edifícios e áreas de acordo com as necessidades do negócio, incluindo emergências. O acesso a instalações, edifícios e áreas deve ser justificado, autorizado, registrado e monitorizado. Isso deve aplicar-se a todas as pessoas que entram nas instalações, incluindo funcionários efetivos e temporários, clientes, fornecedores, visitantes ou qualquer outro terceiro.	• Identificar os controlos existentes sobre o acesso físico, combinados com a gestão de identidades. • Definir verificações de antecedentes para indivíduos que entram em áreas sensíveis, particularmente para funcionários temporários e visitantes. • Verificar os controlos sobre potenciais ataques, infiltração e violações. • Verificar a análise de registos e rever as práticas. • Definir rotinas de verificação / verificação aleatórias, conforme apropriado
DSS05.06 Gerir documentos e dispositivos de saída sensíveis.	Estabelecer proteções físicas, práticas contabilísticas e gestão de inventário apropriados em relação a ativos de TI confidenciais, como formulários especiais, instrumentos negociáveis, e impressoras com finalidades especiais ou tokens de segurança.	• Verificar o catálogo de documentos e dispositivos sensíveis. • Identificar os controlos existentes com relação ao acesso físico, utilização, aprovação, etc. • Verificar os controlos dos tokens de segurança (emissão, monitoramento, descarte, etc.)
DSS05.07 Monitorar a infraestrutura para eventos relacionados à segurança.	Usar ferramentas de deteção de intrusão, monitorar a infraestrutura para acesso não autorizado e garantir que todos os eventos sejam integrados ao monitoramento geral de eventos e à gestão de incidentes	• Identificar e categorizar os controlos existentes sobre intrusões, incluindo deteção técnica, reconhecimento de padrões pela equipa, relatórios e escalonamento • Verificar se há algum controlo sobre técnicas de invasão avançadas e não padronizadas

Tabela 55- Processo DSS05 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Nas tabelas 56 à 63, apresenta-se a descrição dos processos e subprocessos da área de gestão associados ao domínio (*APO - Align, Plan and Organize*). Nas tabelas são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT5	Cibersegurança
APO01 Gerir o Framework de gestão de IT	Esclarecer e manter a governança da missão e visão de TI da organização. Implementar e manter mecanismos e autoridades para gerir a informação e o uso de TI, em apoio aos objetivos de governança, de acordo com princípios e políticas orientadores.	Incorporar a cibersegurança dentro da estrutura de gestão de TI. Componente do processo para monitorar a conformidade com a cibersegurança
APO01.02 Estabelecer funções e responsabilidades	Estabelecer, acordar e comunicar funções e responsabilidades do pessoal de TI, bem como de outros stakeholders com responsabilidades corporativas, que reflitam claramente as necessidades gerais do negócio e os objetivos, autoridade e responsabilidades.	Definir como se organiza a cibersegurança, alinhando funções e responsabilidades com a segurança geral da informação.
APO01.03 Manter os facilitadores do sistema de gestão.	Manter os facilitadores do sistema de gestão e do ambiente de controlo para a TI corporativa e garantir que eles estejam integrados e alinhados com a filosofia de administração e gestão e o estilo operacional da organização. Esses facilitadores incluem a comunicação clara de expectativas / requisitos. O sistema de gestão deve encorajar a cooperação entre divisões e o trabalho em equipa, promover a conformidade e a melhoria contínua	Fornecer política de cibersegurança (gestão) e padrão (s) subsidiário (s), alinhados e integrados com o conjunto geral de políticas de segurança da informação
APO01.04 Comunicar objetivos e direções de gestão	Comunicar a consciencialização e a compreensão dos objetivos e da direção de TI para os stakeholders e usuários apropriados em toda a organização.	Desenvolver programas de consciencialização e instrução em cibersegurança, incluindo elementos baseados em riscos.
APO01.06 Definir informações (dados) e propriedade do sistema	Definir e manter responsabilidades pela propriedade da informação (dados) e sistemas de informação. Assegurar que os proprietários tomem decisões sobre a classificação da informação e sistemas e proteja-la de acordo com essa classificação.	Definir funções e responsabilidades de cibersegurança Fornecer diretrizes relacionadas à cibersegurança sobre o significado da informação "sensível" e "pessoal", especificamente em relação a ataques e violações.
APO01.07 Gerir a melhoria contínua dos processos.	Avaliar, planear e executar a melhoria contínua dos processos e sua maturidade para garantir que eles sejam capazes de transmitir os objetivos corporativos, de governança, gestão e controlo. Considerar a orientação de implementação, os padrões emergentes, os requisitos de conformidade, as oportunidades de automação e o feedback dos usuários do processo, da equipa do processo e de outros stakeholders. Atualizar o processo	Fornecer plano e perspetiva para melhorar a gestão de cibersegurança, incluindo padrões emergentes e requisitos de conformidade Conduzir à prática de cibersegurança de acordo com o programa de consciencialização e instrução e oferecer caminhos de educação específicos para especialistas em cibersegurança.
APO01.08 Manter a conformidade com políticas e procedimentos.	Implementar procedimentos para manter a conformidade e a medição do desempenho de políticas e outros facilitadores da estrutura de controlo e aplicar as consequências da não conformidade ou do desempenho inadequado. Acompanhar as tendências e o desempenho e considerar isso no futuro design e melhoria da estrutura de controlo	Definir e executar revisões de conformidade relacionadas à cibersegurança no cronograma geral de avaliações

Tabela 56- Processo APO01 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO02 Gestão da estratégia	Fornecer uma visão holística do negócio e do ambiente de TI atual, da direção futura e das iniciativas necessárias para alcançar o ambiente futuro desejado. Aproveitar os componentes e componentes básicos da arquitetura empresarial, incluindo serviços fornecidos externamente e recursos relacionados, para permitir uma resposta ágil, fiável e eficiente aos objetivos estratégicos.	Alinhar a estratégia de cibersegurança com a estratégia geral de segurança da informação. Componente de processo para análise de lacunas na cibersegurança
APO02.02 Avaliar o ambiente atual, capacidades e desempenho.	Avaliar o desempenho do negócio interno, recursos de TI atuais e serviços de TI externos e desenvolver um entendimento da arquitetura corporativa em relação às TI. Identificar os problemas que atuais e desenvolver recomendações em áreas que poderiam beneficiar da melhoria. Considerar os diferenciais e opções dos prestadores de serviços, o impacto financeiro e os possíveis custos e benefícios do uso de serviços externos	Desenvolver uma linha de base de recursos para cibersegurança, incluindo critérios e indicadores de desempenho.
APO02.03 Definir os recursos futuros de TI.	Definir os negócios futuros, recursos de TI e os serviços de TI necessários. Isso deve ser baseado no entendimento do ambiente e dos requisitos da organização, na avaliação do atual processo de negócios e ambiente e questões de TI e tendo em consideração de padrões de referência, melhores práticas e tecnologias emergentes validadas ou propostas de inovação.	Definir estados-alvo, como parte da transformação geral, para cibersegurança em intervalos regulares (por exemplo, anualmente) e em função de ataques e violações reais.
APO02.04 Realizar uma análise de lacunas.	Identificar as lacunas entre os ambientes atuais e os futuros e considerar o alinhamento de ativos (os recursos que suportam serviços) para otimizar o investimento e a utilização da base de ativos interna e externa. Considerar os fatores críticos de sucesso para apoiar a execução da estratégia	Realizar marca de referência regular (por exemplo, trimestral) para cibersegurança Corrigir / fechar lacunas através de um processo formal de gestão de mudanças na cibersegurança
APO02.05 Definir o plano estratégico e o roteiro.	Criar um plano estratégico que defina, em cooperação com os stakeholders relevantes, como as metas relacionadas às TI contribuirão para os objetivos estratégicos da organização. Incluir programas de investimento, processos de negócios, serviços, ativos. Direcionar as TI para definir as iniciativas que serão necessárias para fechar as lacunas, a estratégia de sourcing e as medições a serem usadas para monitorar o alcance das metas, priorizar as iniciativas e combina-las	Definir e incluir metas e objetivos de cibersegurança ao nível estratégico e incluí-los na estratégia de segurança. Fornecer e incluir marcos e datas de conclusão para metas e objetivos de cibersegurança.

Tabela 57- Processo APO02 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO03 Administrar a estrutura organizacional	Estabelecer uma arquitetura comum constituída pelos processos de negócio, informação, aplicativos e arquitetura de tecnologia para a realização efetiva e eficiente de estratégias corporativas e de TI, criando modelos e práticas chave que descrevam as arquiteturas de linha de base e de destino. Definir requisitos para taxonomia, padrões, diretrizes, procedimentos, modelos, ferramentas e fornecer uma ligação para esses componentes. Melhorar o alinhamento, aumentar a agilidade, melhorar a qualidade da informação e gerir economias potenciais de custos por meio de iniciativas como a reutilização de componentes de blocos de construção.	Definir e incorporar componentes arquitetónicos da cibersegurança como parte da arquitetura geral relacionada à segurança da informação
APO03.03 Selecionar oportunidades e soluções.	Racionalizar as lacunas entre as arquiteturas de linha de base e de destino, assumindo perspetivas comerciais e técnicas e agrupando-as logicamente em pacotes de trabalho de projeto. Integrar o projeto a qualquer programa de investimento relacionado às TI para garantir que as iniciativas de arquitetura estejam alinhadas e possibilitem essas iniciativas como parte da mudança geral da empresa. Colaborar com os principais stakeholders e TI, para avaliar a prontidão de transformação da organização e identificar oportunidades, soluções e todas as restrições de implementação.	Verificar todo e qualquer risco arquitetural decorrente de problemas relacionados à cibersegurança, incluindo visão sistêmica sobre migração.

Tabela 58- Processo APO03 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO04 Gerir a Inovação	Manter a noção de tecnologias das informação e tendências de serviços relacionados, identificar oportunidades de inovação e planear possíveis benefícios da inovação em relação às necessidades do negócio. Analisar quais as oportunidades de inovação ou melhorias que podem ser criadas por tecnologias emergentes, serviços ou inovação habilitada por TI, bem como por meio de tecnologias já estabelecidas. Influenciar o planeamento estratégico e as decisões de arquitetura corporativa.	Componente do processo para monitorar e analisar o ambiente da tecnologia; Componente adicional para monitorar o uso de tecnologias e inovações emergentes
APO04.01 Criar um ambiente propício à inovação.	Criar um ambiente propício à inovação, considerando questões como cultura, recompensa, colaboração, fóruns de tecnologia e mecanismos para promover e capturar ideias.	Incluir inovação na gestão da cibersegurança como parte da inovação geral de segurança da informação.
APO04.02 Manter um entendimento do ambiente corporativo.	Trabalhar com stakeholders relevantes para entender os seus desafios. Manter uma compreensão adequada da estratégia empresarial e do ambiente competitivo ou outras restrições, de modo que as oportunidades possibilitadas pelas novas tecnologias possam ser identificadas.	Avaliar potenciais vulnerabilidades, ameaças e risco associado de novas iniciativas.
APO04.03 Monitorizar e examinar o ambiente tecnológico.	Trabalhar com os stakeholdes para entender seus desafios. Manter uma compreensão adequada da estratégia empresarial e do ambiente competitivo ou outras restrições, de modo que as oportunidades possibilitadas pelas novas tecnologias possam ser identificadas.	Pesquisar e identificar tendências emergentes no cibercrime, ciberguerra e medidas de segurança relacionadas.
APO04.04 Avaliar o potencial de tecnologias emergentes e ideias de inovação.	Analisar as tecnologias emergentes identificadas e / ou outras sugestões de inovação de TI. Trabalhar com os stakeholders para validar as hipóteses sobre o potencial das novas tecnologias e inovação.	Verificar o impacto potencial da cibersegurança em relação às tecnologias e inovações emergentes e incluir riscos e problemas conhecidos
APO04.05 Recomendar iniciativas adicionais apropriadas.	Avaliar e monitorizar os resultados das iniciativas de prova de conceito e, se favorável, gerir recomendações para outras iniciativas e obter o apoio dos stakeholders	Fornecer aconselhamento baseado no risco em relação a possíveis ataques ou violações, sugerindo etapas e medidas de cibersegurança necessárias

Tabela 59- Processo APO04 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO05 Gestão de Portfólio	Executar a estratégia definida para investimentos em linha com a visão de arquitetura empresarial e as características desejadas dos portfólios de investimento e serviços relacionados, e considerar as diferentes categorias de investimentos, restrições de recursos e financiamento. Avaliar, priorizar e equilibrar programas e serviços, gerindo a procura dentro de restrições de recursos e financiamento, com base no alinhamento com os objetivos estratégicos, o valor e o risco da organização. Mover os programas selecionados para o portfólio de serviços ativos para execução. Monitorizar o desempenho do portfólio geral de serviços e programas, propondo ajustes conforme necessário em resposta ao desempenho do programa e do serviço ou alterando prioridades	Processo subsidiário para identificar e obter financiamento para gestão de cibersegurança
APO05.01 Estabelecer o mix de investimentos alvo	Rever e garantir a clareza da organização, das estratégias de TI e serviços atuais. Definir um mix de investimentos adequado com base no custo, alinhamento com a estratégia e medidas financeiras, como custo e ROI esperado durante todo o ciclo de vida econômico, grau de risco e tipo de benefício para os programas no portfólio. Ajustar as estratégias corporativas e de TI, quando necessário.	Determinar uma apropriada gestão dos investimentos de cibersegurança no contexto sistêmico.
APO05.02 Determinar a disponibilidade e fontes de recursos	Determinar fontes potenciais de recursos, diferentes opções de financiamento e as implicações da fonte de financiamento nas expectativas de retorno do investimento.	Garantir que haja financiamento apropriado para cibersegurança; obter as aceitações de risco exigidas quando o financiamento é insuficiente
APO05.06 Gerir a realização de benefícios.	Monitorizar os benefícios de fornecer e manter serviços e recursos de TI apropriados, com base no atual caso acordado	Verificar e atualizar o perfil de risco de cibersegurança, com base em dados de ataque / violação / incidente e respetiva resposta.

Tabela 60- Processo APO05 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO06 Gestão de orçamentos e custos	Gerir as atividades financeiras relacionadas às funções do negócio e de TI, cobrindo orçamento, gestão de custos, benefícios e priorização de gastos por meio do uso de práticas formais de orçamento e um sistema justo e equitativo de alocação de custos. Consultar os stakeholders para identificar e controlar os custos e benefícios totais dentro do contexto dos planos estratégicos e táticos de TI e iniciar ações corretivas quando necessário.	Orçamento subsidiado relativo à cibersegurança, incluindo o financiamento de contingência para situações reais de ataque / violação
APO06.02 Priorizar a alocação de recursos.	Implementar um processo de tomada de decisão para priorizar a alocação de recursos e regras para investimentos discriminados por unidades de negócio individuais. Incluir o uso potencial de fornecedores de serviços externos e considerar as opções de compra, desenvolvimento e aluguer.	Priorizar as iniciativas de cibersegurança e os recursos necessários em um contexto sistêmico.
APO06.03 Criar e manter orçamentos.	Preparar um orçamento que reflita as prioridades de investimento que apoiam os objetivos estratégicos com base no portfólio de programas e serviços de TI.	Preparar e manter um orçamento de cibersegurança
APO07 Gestão dos Recursos humanos	Fornecer uma abordagem estruturada para garantir melhor posicionamento, direitos de decisão e habilidades de recursos humanos. Isso inclui comunicar os papéis e responsabilidades definidos, os planos de aprendizagem e crescimento e as expectativas de desempenho, apoiados por pessoas competentes e motivadas.	Processo subsidiário para a instrução de pessoal de TI e usuários em cibersegurança Componente do processo para monitorizar a conformidade do contrato de pessoal
APO07.01 Manter pessoal adequado e apropriado	Avaliar os requisitos de pessoal regularmente ou em grandes mudanças nos ambientes corporativos, operacionais ou de TI, para garantir que a organização tenha recursos humanos suficientes para dar suporte às metas e objetivos. O pessoal inclui recursos internos e externos.	Definir requisitos para a equipa de cibersegurança
APO07.O3 Manter as habilidades e competências do pessoal.	Definir e gerir as habilidades e competências requeridas do pessoal. Verificar regularmente se o pessoal tem as competências necessárias para cumprir suas funções com base na sua formação, instrução e/ou experiência, e verificar se essas competências se mantêm, usando programas de qualificação e certificação, quando apropriado. Fornecer aos colaboradores uma aprendizagem contínua e oportunidades para manter seus conhecimentos, habilidades e competências	Definir um plano de instrução em cibersegurança Desenvolver um programa de conscientização sobre cibersegurança

Tabela 61- Processo APO06 e APO07 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO09 Administrar acordos de serviços	Alinhar os serviços e os níveis de serviço habilitados por TI às necessidades e expectativas da organização, incluindo identificação, especificação, design, publicação, contrato e monitorização de serviços de TI, níveis de serviço e indicadores de desempenho.	Processo para SLS de cibersegurança e acordos de nível operacional (OLAs), de acordo com o cenário geral de governança selecionado Componente do processo para rever os acordos em termos de requisitos de cibersegurança
APO09.02 Catálogo de serviços de TI.	Definir e manter um ou mais catálogos de serviços para grupos-alvo relevantes. Publicar e manter serviços ativados por TI nos catálogos de serviços.	Adicionar serviços relacionados à cibersegurança para catalogar conforme apropriado.
APO09.03 Definir e preparar contratos de serviço.	Definir e preparar contratos de serviço com base nas opções dos catálogos de serviços. Incluir acordos operacionais internos	Avaliar os níveis de serviço do fornecedor em relação a critérios e requisitos de cibersegurança. Definir níveis operacionais para serviços relacionados à cibersegurança
APO09.04 Monitorizar e relatar os níveis de serviço.	Monitorizar os níveis de serviço, relatar as conquistas e identificar tendências. Fornecer as informações de gestão apropriadas para auxiliar a gestão de desempenho.	Preparar relatórios de desempenho de cibersegurança (de fornecedores).
APO09.05 Rever os acordos e contratos de serviços	Realizar revisões periódicas dos contratos de serviço quando necessário	Analisar as cláusulas relacionadas à cibersegurança nos contratos, conforme apropriado, e atualizar os SLAs conforme necessário.
APO10 Gerir Fornecedores	Gerir serviços relacionados a TI fornecidos por todos os tipos de fornecedores para atender aos requisitos da organização, incluindo a seleção de fornecedores, gestão de relacionamentos e de contratos e revisão e monitorização do desempenho do fornecedor quanto à eficácia e conformidade	Elementos de processo adicionados para a gestão de terceiros e fornecedores em relação à cibersegurança Componente do processo para monitorizar a conformidade do fornecedor com as disposições de cibersegurança
APO10.04 Gerir o risco de fornecedor	Identificar e gerir os riscos relacionados à capacidade dos fornecedores de fornecer continuamente uma prestação de serviços segura, eficiente e eficaz.	Atualizar a classificação de risco para todos os fornecedores sujeitos a requisitos de cibersegurança
APO10.05 Monitorizar o desempenho e a conformidade do fornecedor.	Rever periodicamente o desempenho geral dos fornecedores, a conformidade com os requisitos do contrato e a relação custo-benefício e resolver os problemas identificados.	Avaliar e rever fornecedores para conformidade e desempenho em cibersegurança

Tabela 62- Processo APO09 e APO10 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
APO12 **Gestão de risco**	Identificar, avaliar e reduzir continuamente o risco relacionado às TI dentro dos níveis de tolerância definidos pela gestão executiva corporativa	Identificação, avaliação e processo de risco de cibersegurança subsidiária Componente de processo para manter um perfil de risco de cibersegurança com base em indicadores de monitorização
APO12.01 Coletar dados	Identificar e coletar dados relevantes para permitir a identificação, análise e relatório de riscos relacionados às TI.	Coletar dados sobre riscos, ataques, violações e incidentes relacionados à cibersegurança, incluindo dados externos, se apropriado.
APO12.02 Analisar o risco	Desenvolver informações úteis para apoiar decisões de risco que levem em consideração a relevância comercial dos fatores de risco	Analisar o risco de cibersegurança Definir e manter cenários de risco relacionados à cibersegurança
APO12.03 Manter um perfil de risco	Manter um inventário dos atributos conhecidos de risco (incluindo a frequência esperada, impacto potencial e respostas) e dos recursos, capacidades e atividades de controlo atuais relacionados.	Manter e transformar um perfil de risco de cibersegurança
APO12.04 Risco articulado	Fornecer informações sobre o estado atual de exposições e oportunidades relacionadas às TI para todo o tipo de stakeholders.	Desenvolver e comunicar estratégias de resposta para ataques, violações e incidentes; integrar-se ao risco geral de segurança da informação e à resposta a incidentes.
APO12.05 Definir um portfólio de ações de gestão de risco.	Gerir oportunidades para reduzir o risco a um nível aceitável com o portfólio.	Definir propostas de projetos de cibersegurança e casos de negócio correspondentes.
APO12.06 Responder ao risco	Responder em tempo útil com medidas eficazes para limitar a magnitude da perda de eventos relacionados as TI	Definir práticas de mitigação e resposta de cibersegurança que incluam ataque / manipulação de violações, análise forense e investigação.

Tabela 63- Processo APO12 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Nas tabelas 64 à 71, apresenta-se a descrição dos processos e subprocessos da área de gestão associados ao domínio construir, adquirir e implementar (*BAI - Build, Acquire and Implement*) Nas tabelas são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT5	Cibersegurança
BAI01 Gestão de programas e de projetos	Gerir todos os programas e projetos do portfólio de investimentos em alinhamento com a estratégia da organização, de forma coordenada. Iniciar, planear, controlar e executar programas e projetos e terminar o processo com uma revisão pós-implementação.	
BAI01.02 Iniciar um programa.	Iniciar um programa para confirmar os benefícios esperados e obter autorização para prosseguir. Isso inclui concordar com o orçamento do programa, confirmar o mandato do programa, nomear o comitê ou membros do comitê, elaborar o resumo do programa, rever e atualizar o caso de negócio, desenvolver um plano de realização de benefícios e obter a aprovação dos financiadores para prosseguir.	Definir o caso de negócio e o programa de cibersegurança com base em medidas de segurança obrigatórias e prioridades críticas de negócios.
BAI01.08 Planear projetos.	Estabelecer e manter um plano de projeto integrado formal e aprovado (cobrindo recursos de negócio e de TI) para orientar a execução e o controlo do projeto durante toda a vida do projeto. O âmbito dos projetos deve ser claramente definido e vinculado à construção ou ao aprimoramento da capacidade do negócio.	Planear projetos relacionados à cibersegurança de acordo com o programa.
BAI01.11 Monitorizar e controlar projetos.	Medir o desempenho do projeto em relação aos principais critérios de desempenho do projeto, como cronograma, qualidade, custo e risco. Identificar quaisquer desvios daquilo que é esperado. Avaliar o impacto dos desvios no projeto e no programa geral e relatar os resultados aos principais stakeholders	Fornecer relatórios sobre projetos de cibersegurança, com referência específica a pontos fracos decorrentes de novas formas de cibercrime e ciberguerra

Tabela 64- Processo BAI01 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI02 Gerir a definição de requisitos	Identificar soluções e analisar os requisitos antes da aquisição ou criação, para garantir que estejam alinhados com os requisitos estratégicos da organização, abrangendo processos de negócio, aplicativos, informação/dados, infraestrutura e serviços. Coordenar com os stakeholders afetados a revisão de opções viáveis, incluindo custos e benefícios relativos, análise de risco e aprovação de requisitos e soluções propostas.	Processo subsidiário para definir requisitos de cibersegurança
BAI02.01 Definir e manter requisitos funcionais e técnicos de negócios.	Com base no negócio, identificar, priorizar, especificar e concordar com os requisitos de informações comerciais, funcionais, técnicas e de controlo que abrangem o âmbito/entendimento de todas as iniciativas necessárias para alcançar os resultados esperados	Definir requisitos de cibersegurança como um subconjunto de requisitos gerais de segurança da informação.
BAI02.03 Gerir risco de requisitos.	Identificar, documentar, priorizar e mitigar o risco funcional, técnico e relacionado ao processamento de informação, associado aos requisitos da organização e à solução proposta.	Definir e documentar o risco associado às soluções, incluindo o risco residual após a mitigação e exposição a ataques e violações.
BAI02.04 Obter aprovação de requisitos e solução.	Coordenar o feedback dos stakeholders afetados e, em estágios-chave predeterminados, obter aprovação do financiador ou do proprietário do produto e assinar os requisitos funcionais e técnicos, estudos de viabilidade, análises de risco e soluções recomendadas.	Obter aprovações necessárias para soluções, medidas e requisitos de cibersegurança; incluindo aceitações de risco para exposição remanescente a ataques, violações e incidentes.

Tabela 65- Processo BAI02 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI03 Administrar a identificação e construção de soluções	Estabelecer e manter soluções identificadas de acordo com os requisitos corporativos que abrangem o projeto, desenvolvimento, suprimento / terceirização e parceria com fornecedores. Gerir a configuração, preparação de testes, testes, requisitos e manutenção de processos de negócio, aplicativos, informações / dados, infraestrutura e serviços.	Processo subsidiário para identificação de soluções específicas relacionadas à cibersegurança
BAI03.01 Projetar soluções de alto nível	Desenvolver e documentar projetos de alto nível usando técnicas de desenvolvimento ágeis, apropriadas e rápidas. Garantir o alinhamento estratégico de TI e a arquitetura corporativa. Reavaliar e atualizar os projetos quando ocorrerem problemas significativos durante o projeto detalhado ou nas fases de construção ou conforme a solução evolui. Assegurar que os stakeholders participem ativamente no projeto e aprovem cada versão.	Desenvolver especificações de cibersegurança de alto nível de acordo com o modelo de segurança e a dinâmica do sistema
BAI03.02 Projetar componentes detalhadas de solução.	Desenvolver, documentar e elaborar progressivamente projetos detalhados usando técnicas de desenvolvimento ágeis, apropriadas e rápidas, abordando todos os componentes (processos de negócio e controlos manuais e automatizados relacionados, suportando aplicativos de TI, serviços de infraestrutura, produtos de tecnologia e parceiros / fornecedores). Certificar se o design detalhado inclui SLAs e OLAs internos e externos.	Desenvolver etapas, ações e medidas detalhadas de cibersegurança para abordar o risco e incorpora-las ao sistema de cibersegurança
BAI03.10 Manter soluções	Desenvolver e executar um plano para a manutenção de componentes de solução e infraestrutura. Incluir revisões periódicas em relação às necessidades de negócio e requisitos operacionais	Atualizar as soluções de cibersegurança de acordo com as necessidades do negócio e requisitos operacionais.

Tabela 66- Processo BAI03 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI04 Gestão de disponibilidade e de capacidade	Equilibrar as necessidades atuais e futuras de disponibilidade, desempenho e capacidade com prestação de serviços económica. Incluir a avaliação das capacidades atuais, a previsão das futuras com base nos requisitos do negócio, a análise dos impactos e a avaliação do risco para planear e implementar ações de forma a atender aos requisitos identificados.	
BAI04.01 Avaliar a disponibilidade, desempenho e capacidade atuais e criar uma linha de base	Avaliar a disponibilidade, o desempenho e a capacidade dos serviços e recursos para garantir que a capacidade e o desempenho estejam disponíveis para dar suporte às necessidades do negócio. Criar linhas de base de disponibilidade, desempenho e capacidade para comparação futura	Definir e incluir quaisquer problemas relacionados à cibersegurança, especificamente ataques e violações relacionados à disponibilidade, desempenho e capacidade.
BAI04.02 Avaliar o impacto no negócio	Identificar e mapear os serviços importantes para organização, recursos para processos de negócio e identificar dependências. Assegurar que o impacto dos recursos indisponíveis seja totalmente acordado e aceite pelo cliente. Certificar-se que, para funções vitais do negócio, os requisitos de disponibilidade de SLA possam ser atendidos.	Realizar avaliações de impacto para processos de TI e do negócio potencialmente afetados por ataques e violações; alinhar com o BCM e outras avaliações acordadas

Tabela 67- Processo BAI04 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI05 Gerir a habilitação para a mudança organizacional	Maximizar a probabilidade de implementar com sucesso a mudança organizacional sustentável em toda a organização de forma rápida e com risco reduzido, cobrindo o ciclo de vida completo da mudança e todos os stakeholders afetados no negócio e TI.	Vincular a transformação da cibersegurança e incorporar etapas de transformação na gestão geral de mudanças
BAI05.01 Estabelecer a vontade de mudar	Entender o âmbito e o impacto da mudança prevista e a prontidão / disposição para mudança. Identificar ações para motivar os stakeholders a aceitar e querer que a mudança funcione com sucesso	Definir e planear comunicações sobre cibersegurança assim como etapas e medidas relacionadas; criar gestão sênior consciente e obter apoio para a cibersegurança
BAI05.04 Capacitar o papel dos agentes e identificar vitórias de curto prazo.	Capacitar aqueles com funções de implementação, garantindo que as responsabilidades sejam atribuídas, fornecendo instrução e alinhando estruturas organizacionais e processos de RH. Identificar e comunicar vitórias de curto prazo que podem ser atingidas e podem ser importantes para a perspetiva de ativação de mudança.	Priorizar planos e projetos de cibersegurança num cronograma e identificar objetivos e benefícios de curto prazo, ou seja, ações imediatas para reduzir o número de ataques e violações.
BAI05.05 Ativar operação e uso.	Planear e implementar todos os aspetos técnicos, operacionais e de uso, de modo que todos aqueles que estão envolvidos no futuro ambiente do estado possam exercer a sua responsabilidade.	Planear e implementar ações com vista no futuro, como parte da transformação da cibersegurança, destacando o aspeto transformacional.
BAI05.07 Sustentar mudanças	Sustentar mudanças através da instrução efetiva de novos funcionários, campanhas de comunicação contínuas, compromisso contínuo da alta administração, monitorização de adoção e partilha de lições aprendidas em toda a organização.	Integrar revisões operacionais com monitorização e controlo de cibersegurança

Tabela 68- Processo BAI05 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI06 Gerir mudanças	Gerir todas as alterações de maneira controlada, incluindo alterações padrão e manutenção de emergências relacionadas a processos, aplicativos e infraestrutura do negócio. Incluir padrões e procedimentos de mudança, avaliação de impacto, priorização e autorização, mudanças de emergência, rastreamento, relatórios, fecho e documentação.	Processo subsidiário para mudanças de emergência na cibersegurança
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Avaliar todas as solicitações de mudança para determinar o impacto nos processos de negócio e nos serviços de TI e avaliar se as alterações afetarão negativamente o ambiente operacional ou apresentem riscos inaceitáveis. Garantir que as alterações sejam registadas, priorizadas, categorizadas, avaliadas, autorizadas, planeadas e programadas	Avaliar as alterações de cibersegurança do ponto de vista da transformação; incorporar mudanças relacionadas à gestão geral de mudanças.
BAI06.02 Gerir mudanças de emergência	Gerir com cuidado as mudanças de emergência para minimizar mais incidentes e certificar que a alteração seja controlada e ocorra com segurança. Verificar se as alterações de emergência são devidamente avaliadas e autorizadas após a alteração.	Rever e consolidar quaisquer mudanças de emergência relacionadas à cibersegurança; Incluir quaisquer alterações importantes, como desligar sistemas, etc.
BAI06.04 Fechar e documentar as alterações	Sempre que as alterações forem implementadas, atualizar adequadamente a documentação da solução e do usuário e os procedimentos afetados pela alteração.	Documentar (de forma auditável e detetável) quaisquer alterações relevantes para a cibersegurança, incluindo mudanças nos negócios.

Tabela 69- Processo BAI06 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI07 Gerir a aceitação e a transição da mudança	Aceitar formalmente e implementar novas soluções operacionais, incluindo planeamento de implementação, conversão de dados e sistemas, testes de aceitação, comunicação, preparação, promoção para produção de processos de negócio e serviços de TI novos ou alterados, suporte à produção inicial e revisão pós-implementação	Conectar para a transformação da cibersegurança e incorporar etapas de transformação dentro de mudanças gerais.
BAI07.04 Estabelecer um ambiente de teste.	Definir e estabelecer um ambiente de teste seguro, representativo do processo de negócio e ambiente de operações de TI planeados, desempenho e capacidade, segurança, controlos internos, práticas operacionais, requisitos de privacidade, qualidade de dados e cargas de trabalho.	Estabelecer teste apropriados, incluindo ambientes de área restrita, para testar ações relacionadas à cibersegurança, bem como ataques e violações

Tabela 70- Processo BAI07 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
BAI08 Gestão de conhecimento	Manter a disponibilidade de conhecimento relevante, atual, validado e fiável para suportar todas as atividades do processo e facilitar a tomada de decisão. Planear a identificação, coleta, organização, manutenção, uso e retirada do conhecimento.	Processo de gestão do conhecimento subsidiário para cibersegurança
BAI08.02 Identificar e classificar fontes de informação.	Identificar, validar e classificar diversas fontes de informação internas e externas necessárias para permitir o seu uso e operação eficaz de processos de negócio e serviços de TI.	Identificar e classificar fontes de informações de cibersegurança, inteligência externa e serviços relacionados e estatísticas de ataque / violação
BAI08.05 Avaliar e retirar informações.	Medir o uso e avaliar o valor e a relevância da informação. Retirar informações obsoletas.	Avaliar a informação relacionada a ataques, violações, TI em geral, alvos potenciais e retirar informações obsoletas.
BAI10 Gerir a configuração	Definir e manter descrições e relações entre os principais recursos e as capacidades necessárias para prestar serviços de TI, incluindo a coleta de informação de configuração, o estabelecimento de linhas de base, verificação e auditoria de informações de configuração e atualizar o repositório de configuração.	
BAI10.02 Estabelecer e manter um repositório de configuração e linha de base.	Estabelecer e manter um repositório de gestão de configuração e criar linhas de base de configuração controladas	Definir vulnerabilidades relacionadas à cibersegurança e integra-las nos relatórios de vulnerabilidade.

Tabela 71- Processo BAI08 e BAI10 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Nas tabelas 72 à 76, apresenta-se a descrição dos processos e subprocessos da área de gestão associados ao entrega, serviço e suporte (DSS - *Deliver, Service and Support).* Nas tabelas são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT5	Cibersegurança
DSS01 Gestão de Operações	Coordenar e executar as atividades e procedimentos operacionais necessários para fornecer serviços de TI internos e terceirizados, incluindo a execução de procedimentos operacionais, padrões predefinidos e atividades exigidas.	Processo de operações subsidiárias para cibersegurança, vinculado a operações gerais de TI, incluindo serviços terceirizados e monitorização de infraestruturas críticas
DSS01.02 Gestão serviços de TI terceirizados	Gerir a operação de serviços de TI terceirizados para manter a proteção das informações corporativas e a fiabilidade da prestação de serviços.	Inserir requisitos de cibersegurança em níveis e contratos de serviços de terceiros; incluir requisitos de cibersegurança e testes em planos de garantia de terceiros.
DSS01.03 Monitorizar a infraestrutura de TI	Monitorizar a infraestrutura de TI e eventos relacionados. Armazenar informações cronológicas suficientes nos registos de operações para permitir a reconstrução, revisão e exame das sequências de tempo das operações e das outras atividades que envolvem ou suportam as operações.	Estender as regras de monitorização para cobrir todos os requisitos de cibersegurança; incluir especificamente a monitorização de ataques e violações potenciais ou reais.
DSS01.04 Gerir o ambiente	Manter medidas de proteção contra fatores ambientais. Instalar equipamentos e dispositivos especializados para monitorizar e controlar o ambiente	Fornecer informações sobre serviços, equipamentos e dispositivos especializados para monitorizar e controlar o ambiente.
DSS01.05 Gerir instalações	Gerir instalações, incluindo energia e equipamentos de comunicação, de acordo com as leis e regulamentos, requisitos técnicos e de negócio, especificações do fornecedor e diretrizes de saúde e segurança.	Identificar e contribuir com instalações relacionadas com o risco de cibersegurança e vulnerabilidades / ameaças, especificamente para infraestruturas técnicas que possam ser um alvo

Tabela 72 - Processo DSS01 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
DSS02 Gerir solicitações de serviços e administrar incidentes	Fornecer resposta rápida e eficaz às solicitações dos usuários e resolução de todos os tipos de incidentes. Restaurar o serviço normal; atender às solicitações de usuários; registar, investigar, diagnosticar, encaminhar e resolver incidentes.	Processo de cibersegurança subsidiária para identificar, classificar e gerir incidentes relacionados Componente de processo para integrar a resposta de incidentes com gestão geral de incidentes / gestão de crises
DSS02.02 Registar, classificar e priorizar solicitações e incidentes.	Identificar, registar e classificar solicitações e incidentes de serviços e atribuir uma prioridade de acordo com a importância do negócio e os contratos de serviço	Desenvolver critérios de classificação relacionados com a cibersegurança e alinhá-los com o registo e classificação geral de incidentes; fornecer dados atuais sobre incidentes relevantes para a cibersegurança
DSS02.04 Investiga, diagnosticar e alocar incidentes.	Identificar e registar sinais de incidentes, determinar possíveis causas e alocar para resolução	Identificar os incidentes relevantes para a cibersegurança, proteger os dados e todas as evidências potenciais; seguir as regras da cadeia de custódia e regras de descoberta eletrônica;
DSS02.05 Resolver e recuperar de incidentes	Documentar, aplicar e testar as soluções ou hipóteses alternativas identificadas e executar ações de recuperação para restaurar o serviço relacionado às TI.	Desenvolver resposta de cibersegurança de acordo com a preparação, investigação, remediação e erradicação de causas raiz.
DSS02.07 Rastrear status e produzir relatórios	Analisar e relacionar as tendências de atendimento a incidentes e pedidos de informação para melhoria contínua.	Consolidar dados e evidências de incidentes; obter lições aprendidas para cibersegurança; definir melhorias e necessidades de transformação.

Tabela 73 - Processo DSS02 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
DSS03 Gestão de problemas	Identificar e classificar problemas e suas principais causas e fornecer uma resolução oportuna para evitar incidentes recorrentes. Fornecer recomendações para melhorias	Processo de cibersegurança subsidiária para identificação de causas raiz, prevenção de ocorrências e recomendação de melhorias
DSS03.01 Identificar e classificar problemas	Definir e implementar critérios e procedimentos para relatar problemas identificados, incluindo classificação, categorização e priorização de problemas.	Incluir critérios relacionados a problemas de cibersegurança
DSS03.02 Investigar e diagnosticar problemas	Investigar e diagnosticar problemas usando especialistas relevantes para avaliar e analisar as causas raiz.	Investigar e diagnosticar ataques, violações e incidentes; incluir quase-falhas e tentativas frustradas; estabelecer a causa raiz, se possível, e deduzir características comuns.
DSS03.03 fazer o levantamento dos erros conhecidos	Assim que as causas dos problemas forem identificadas, criar registos de erros conhecidos assim como identificar uma solução alternativa apropriada	Fazer o levantamento de problemas conhecidos de cibersegurança; especificamente aqueles que incluem fraquezas sistêmicas

Tabela 74 - Processo DSS03 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
DSS04 Gestão da continuidade	Estabelecer e manter um plano para permitir que o negócio e as TI respondam a incidentes e interrupções, a fim de continuar a operação de processos críticos de negócio e serviços de TI necessários e manter a disponibilidade da informação a um nível aceitável para a organização.	Componente de processo para integrar a resposta, recuperação e retomada de incidentes com BCM geral
DSS04.01 Definir a política de continuidade de negócio, objetivos e âmbito.	Definir a política de continuidade de negócio e o seu âmbito, alinhados com os objetivos da organização e dos stakeholders.	Cruzar apropriadamente referências entre as políticas e procedimentos de cibersegurança; incluir cenários apropriados de cibercrime / ciberguerra na política da BC
DSS04.02 Manter uma estratégia de continuidade.	Avaliar as opções de gestão de continuidade do negócio e escolher uma estratégia de continuidade económica e viável que garanta a recuperação e a continuidade da empresa diante de um desastre, um grande incidente ou interrupção.	Integrar estratégias e táticas de cibersegurança para lidar com ataques/ violações para incidentes crescentes; atualizar BIA e avaliação de risco para vulnerabilidades/ameaças de cibersegurança e risco associado.
DSS04.03 Desenvolver e implementar uma resposta de continuidade de negócio	Desenvolver um plano de continuidade de negócio (BCP) com base na estratégia que documenta os procedimentos e as informações em prontidão para uso num incidente, a fim de permitir que a organização continue com suas atividades críticas.	Desenvolver e alinhar os BCP's para cenários relacionados à cibersegurança.
DSS04.04 Exercitar, testar e rever o BCP.	Testar os programas continuidade regularmente para exercitar os planos de recuperação contra resultados predeterminados, para permitir que soluções inovadoras sejam desenvolvidas e ajudar a verificar, com tempo, que o plano funcionará como previsto.	Testar BCPs relacionados à cibersegurança e acordos incidentais
DSS04.05 Rever, manter e melhorar o plano de continuidade.	Realizar uma revisão da gestão da capacidade de continuidade em intervalos regulares para garantir a sua adequação, sustentabilidade e efetividade contínuas. Gerir as alterações no plano de acordo com o processo de controlo de alterações para garantir que o plano de continuidade seja mantido atualizado. Refletir continuamente sobre os requisitos reais de negócio.	Incluir BCPs relacionados à cibersegurança e acordos incidentais no ciclo PDCA.

Tabela 75 - Processo DSS04 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Processo	COBIT5	Cibersegurança
DSS05 Gerir serviços de segurança	Proteger a informação da organização para manter o nível de risco aceitável de segurança de acordo com a política de segurança. Estabelecer e manter funções de segurança da informação e privilégios de acesso e realizar monitorização de segurança	
DSS05.01 Proteger contra malware.	Implementar e manter em vigor medidas preventivas, de deteção e corretivas em toda a organização para proteger os sistemas de informação e tecnologia contra malware	Alinhar políticas, padrões e KOPs de cibersegurança com políticas gerais de segurança de informações e vice-versa. Avaliar ameaças específicas, como explorações, malware de nível militar e ferramentas de ataque APT.
DSS05.02 Gerir segurança de rede e conectividade.	Usar medidas de segurança e procedimentos de gestão para proteger a informação sobre todos os métodos de conectividade.	Identificar e inserir componentes de rede propensos a ataques / violações, incluindo explorações do tipo dia zero e APT. Realizar testes de penetração apropriados em componentes de rede propensos a ataques; restringir ao nível técnico para distinguir as perspetivas genéricas de segurança da informação e cibersegurança
DSS05.03 Gerir terminal de segurança de	Assegurar que os pontos de extremidade (por exemplo, laptop, desktop, servidor e outros dispositivos móveis ou de rede ou software) estejam protegidos a um nível igual ou superior aos requisitos definidos de segurança da informação processados, armazenados ou transmitidos.	Incluir ataques / violações de terminais e ataques de APT conhecidos.
DSS05.07 Monitorizar a infraestrutura para eventos relacionados à segurança	Usando ferramentas de deteção de invasão, monitorizar a infraestrutura para o acesso não autorizado e garantir que todos os eventos sejam integrados à monitorização geral de eventos e gestão de incidentes.	Avaliar tickets de incidentes para indicações de cibercrime ou ciberguerra; Avaliar se os incidentes são relevantes para a cibersegurança ou se os incidentes podem ser tratados usando procedimentos e ações gerais de segurança da informação. Estabelecer mecanismos de análise e revisão relacionados à cibersegurança

Tabela 76 - Processo DSS05 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

Na tabela 77, apresenta-se a descrição dos processos e subprocessos da área de gestão associados ao monitorizar, avaliar e aferir (*MEA - Monitor, Evaluate and Assess*). Nas tabelas são apresentados os processos e subprocessos (primeira coluna), a descrição de cada um em função do COBIT5 (segunda coluna) e as práticas de cibersegurança associadas (terceira coluna).

Processo	COBIT5	Cibersegurança
MEA01 Monitorizar, avaliar e aferir o desempenho e a conformidade	Coletar, validar e avaliar metas e métricas do processo de negócio e TI. Avaliar a conformidade dos processos em relação às metas e métricas de desempenho acordadas e fornecer relatórios sistemáticos e oportunos.	Processo subsidiário para a monitorização da cibersegurança (dentro dos limites legais e regulatórios)
MEA01.03 Coletar e processar dados de desempenho e conformidade	Coletar e processar dados oportunos e precisos, alinhados a abordagens corporativas	Definir requisitos de monitorização, indicadores, conjuntos de dados e métodos de coleta para monetização de cibersegurança; definir métodos analíticos apropriados
MEA01.05 Garantir a implementação de ações corretivas.	Ajudar os stakeholders a identificar, iniciar e rastrear ações corretivas para lidar com anomalias	Definir ações corretivas relacionadas a ataques / violações / incidentes; incorporar quaisquer ações corretivas e planeamentos relacionados com a transformação geral de cibersegurança
MEA02 Monitorizar, avaliar e aferir o sistema de controlo interno	Monitorar e avaliar continuamente, o ambiente de controlo, incluindo autoavaliações e análises de avaliações independentes. Permitir que a gestão identifique deficiências e ineficiências de controlo e iniciar ações de melhoria. Planear, organizar e manter padrões para avaliação do controlo interno e atividades de garantia	Processo subsidiário para autoavaliações de controlo (CSAs) na cibersegurança, incluindo relatórios de ataques / falhas e outras atividades suspeitas
MEA02.04 Identificar e relatar deficiências de controlo.	Identificar deficiências de controlo, analisar e identificar as principais causas subjacentes. Enumerar as deficiências de controlo e informar os stakeholders.	Identificar as fraquezas do controlo na cibersegurança, numa perspetiva baseada no risco e destacar quaisquer efeitos em cadeia na dinâmica do sistema
MEA02.05 Garantir que as garantias de fornecedores sejam independentes e qualificadas.	Assegurar que as entidades que executam a garantia sejam independentes no âmbito da função, grupos ou organização. As entidades que executam a garantia devem demonstrar uma atitude e aparência apropriadas, competência, conhecimentos necessários para realizar a garantia e aderência aos códigos de ética e padrões profissionais.	Avaliar garantia de fornecedores para cibersegurança; reunir inteligência apropriada e realizar verificações de antecedentes conforme apropriado.
MEA03 Monitorizar, avaliar e aferir a conformidade com requisitos externos	Avaliar se as TI e processos do negócio suportados pelas TI estão em conformidade com as leis, regulamentos e exigências contratuais. Obter a garantia de que os requisitos foram identificados e cumpridos e integra-los em conformidade com o cumprimento global da organização	Processo subsidiário para identificar e interpretar os requisitos de conformidade externa na cibersegurança
MEA03.01 Identificar os requisitos de conformidade externos.	Numa base contínua, identificar e monitorar as mudanças nas leis, regulamentos e outros requisitos externos locais e internacionais que devem ser cumpridos numa perspetiva de TI.	Identificar quaisquer leis ou regulamentos que afetem a cibersegurança; incluir disposições específicas no âmbito da prerrogativa de segurança nacional (ou equivalente); incluir quaisquer requisitos relacionados à ciberguerra

Tabela 77 - Processo MEA01, MEA02, MEA03 e subprocessos do COBIT5 - aplicabilidade à cibersegurança (extraído do COBIT5TC)

No que toca ao habilitador *Estrutura Organizacional*, é de referir que as estruturas organizacionais são consideradas as entidades chave para a tomada de decisão dentro da organização. Este habilitador pretende que seja executado um conjunto de práticas associadas às diferentes funções, que ofereçam como resultado à organização a tomada de boas decisões. O COBIT5TC, sugere a existência de certas funções ou estruturas dentro da organização que estejam diretamente relacionadas com a segurança da informação, especificadas na tabela 78, assim como a descrição das diferentes funções/ estruturas organizacionais

Estrutura Organizacional	Responsabilidade da Estrutura
CISO (Chief Information Security Officer)	Responsabilidade geral pelo programa de segurança da informação da organização.
ISSC (Information Security Steering Committee)	Garantir, através de monitorização e avaliação, que são aplicadas boas práticas de segurança da informação de forma eficaz e consistente em toda a empresa.
ISM (Information Security Manager)	Responsabilidade geral pela gestão dos esforços desenvolvidos na área de segurança da informação.
ERM (Enterprise Risk Management)	Responsabilidade pela tomada de decisão na organização para avaliar, controlar, otimizar, financiar e monitorizar o risco de todas as fontes, com a finalidade de aumentar o valor da organização para os seus stakeholders a curto e longo prazo.
Cybersecurity Specialist	Responsabilidade pela gestão operacional da cibersegurança

Tabela 78 - Estruturas organizacionais do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

No que diz respeito ao habilitador de *Cultura, Ética e Comportamento*, este visa que os comportamentos devem ser medidos ao longo do tempo para se conseguir, desta forma, aferir a cultura de segurança na organização. Na tabela 79 encontra-se uma lista de comportamentos sugeridos que influenciam positivamente a cultura de cibersegurança, A descrição dos diferentes comportamentos desejados encontra-se na primeira coluna, e na segunda coluna encontra-se a sua aplicabilidade ao nível da cibersegurança

Modelo de Comportamentos	Aplicabilidade ao nível da Cibersegurança
Segurança da informação é praticada diariamente nas operações	• Os princípios e práticas de cibersegurança são aplicados às operações diárias. • Todos os associados compreendem e aplicam cibersegurança em tempo útil.
As pessoas respeitam a importância das políticas e princípios de segurança da informação	• Todos os usuários compreendem as prioridades definidas na cibersegurança assim como a aplicabilidade no seu ambiente de TI pessoal e empresarial. • Todos os usuários da informação estão conscientes e ativamente envolvidos, definindo princípios e políticas de cibersegurança. • Os princípios, políticas, padrões e KOPs de cibersegurança são atualizados com frequência para refletir a realidade do dia a dia e a experiência da organização.
As pessoas recebem orientação suficiente e detalhada acerca de segurança da informação e são encorajadas a participar e desafiar a atual situação de segurança da informação	• A cibersegurança é um processo de transformação com desafios regulares em todas as partes da organização. • A orientação para cibersegurança é simples e relaciona-se com o risco típico do dia-a-dia. • A situação em relação à cibersegurança é avaliada de forma contínua e conjunta por usuários e gestores da segurança.
Todos são responsáveis pela proteção da informação dentro da organização.	• Os gestores da segurança e os usuários compartilham a responsabilidade pela cibersegurança. Isso inclui o uso comercial, uso em viagens e uso doméstico. • Os usuários têm uma compreensão clara de sua responsabilidade e atuam de forma responsável. • A organização opera num ambiente tolerante a falhas/ tolerância a erros e evita o bode expiatório.
Os Stakeholders estão cientes de como identificar e responder a ameaças da organização.	• Todos os usuários são stakeholders na cibersegurança, independentemente do seu nível hierárquico dentro da organização. • Os usuários estão suficientemente conscientes dos riscos, ameaças e vulnerabilidades associados a ataques / infrações. • A resposta a ameaças e incidentes é bem compreendida, exercida com frequência e auditável.
A gestão apoia e antecipa inovações de segurança da informação e comunica isso à organização. A organização explica e lida com novos desafios de segurança da informação.	• A gestão da segurança e usuários finais identificam, testam e adotam a inovação de cibersegurança. • A administração e os usuários finais identificam e adotam novos casos de negócios para tecnologia, práticas de segurança e outros tipos de valor agregado na cibersegurança. • A organização visa explicitamente manter-se na frente, no que toca a cibersegurança.
A gestão de negócios envolve uma colaboração contínua e multifuncional para permitir programas de segurança da informação eficientes e eficazes.	• Os programas de cibersegurança estão em vigor e fazem parte da estratégia geral de inovação. As inovações de segurança são incorporadas como projetos-chave. • As funções de negócios cooperam com a segurança da informação para maximizar a eficiência e eficácia da cibersegurança.
A gestão executiva reconhece o valor comercial da segurança da informação.	• Os gerentes executivos atuam como usuários finais e reconhecem o valor da cibersegurança. Eles participam ativamente de atividades de instrução e conscientização.

Tabela 79 - Modelo de comportamentos do COBIT5 e aplicabilidade à cibersegurança (extraído do COBIT5TC)

Anexo II – Check list de verificação às práticas do COBIT5TC

Tal como referido anteriormente, e observando todas as práticas sugeridas pelo COBIT 5TC do anexo I, foi possível sintetizar todos as práticas recomendadas associadas aos princípios, políticas e processos, numa única check list com apenas 116 práticas. A check list encontra-se apresentada da tabela 80 à 85.

Nº	Requisito de Cibersegurança	Processo COBIT5
	Disposições legais e governo do sistema de cibersegurança	
1	Identificar e validar o modelo de governo do sistema de cibersegurança	EDM01.01
2	Identificar/Rever disposições legais e regulamentares existentes que possam influenciar no desenvolvimento do governo do sistema de cibersegurança, assim como os requisitos a cumprir, relativos a ocorrências que afetem a cibersegurança.	EDM01.01 MEA03.01
3	Alinhar o risco de cibersegurança de acordo com o modelo de governo geral da organização	EDM03.03
4	Aplicar normas e procedimentos chave de operacionalidade (KOP's)	Princípio 11
5	Obter compromisso de gestão para o modelo de governo ou de gestão selecionado	EDM01.02
	Ataques, ameaças e vulnerabilidades	
6	Avaliar as ameaças e vulnerabilidades relevantes para a cibersegurança	EDM01.03
7	Categorizar ataques e ameaças em termos de conformidade e necessidades regulatórias	EDM01.01
8	Estabelecer escala de pontos para ataques, infrações e incidentes	EDM01.02 DSS02.02
9	Identificar adaptabilidade, capacidade de resposta e resiliência em termos de ataques/violações de cibersegurança	EDM01.01
10	Fornecer aconselhamento baseado no risco em relação a possíveis ataques ou violações, sugerindo etapas e medidas de cibersegurança necessárias	APO04.05
11	Definir vulnerabilidades relacionadas à cibersegurança e integrá-las nos relatórios de vulnerabilidade	BAI10.02
12	Identificar os incidentes relevantes para a cibersegurança, proteger dados e todas as evidências potenciais	DSS02.04
13	Investigar e diagnosticar ataques, violações e incidentes; incluir quase falhas e tentativas frustradas; estabelecer a causa raiz, se possível, e deduzir características comuns	DSS03.02
14	Comparar acontecimentos atuais com o histórico de conhecimentos de ataques e violações	DSS05.03
	Necessidades, lacunas, deficiências, fragilidades	
15	Identificar quaisquer elementos /frágeis ou lacunas que possam conduzir ao cibercrime ou ciberguerra	EDM01.01 DSS05.04
16	Verificar as necessidades do negócio em relação a ataques e violações	EDM01.01
17	Documentar deficiências sistémicas na cibersegurança	EDM01.01
18	Definir o mecanismo de análise de lacunas para o risco de cibersegurança vs tratamento / controlos existentes	APO13.03
19	Corrigir/ fechar lacunas através do processo formal de gestão de mudanças de cibersegurança.	APO02.04
	Modelo de tomada de decisão	
20	Determinar um modelo de tomada de decisão para a cibersegurança – prever respostas/recuperação ciberataques específicos (preparação, investigação, correção e erradicação de causas raiz)	EDM01.01 EDM01.02 APO12.05 DSS02.07
21	Definir/planear propostas de projetos de cibersegurança (portfólio de ações)	APO12.05 BAI01.08

Tabela 80 - Check list de práticas de cibersegurança - elaboração própria com base no COBIT5TC

Nº	Requisito de Cibersegurança	Processo COBIT5
	Tolerância, apetite pelo risco, risco	
22	Coletar dados sobre riscos, ataques, violações e incidentes relacionados à cibersegurança, incluindo dados externos se apropriado	APO12.01 DSS02.02 DSS02.07
23	Manter e transformar um perfil de risco de cibersegurança	APO12.03
24	Identificar o nível de tolerância da organização em relação a ataques e violações	EDM01.02 EDM03.01
25	Comparar os níveis de tolerância ao risco e comparar inconsistências entre a segurança da informação e a cibersegurança.	EDM03.01
26	Identificar e categorizar o risco relacionado à cibersegurança e as opções de tratamento	APO13.02 APO03.03 APO05.06 APO12.02 BAI02.03
27	Realizar e atualizar BIA (Business impact analysis) e avaliação de risco para vulnerabilidades /ameaças de cibersegurança e risco associado	DSS04.02
28	Incorporar o tratamento de risco de cibersegurança no plano geral de segurança da informação	APO13.02
29	Definir e manter cenários de risco de cibersegurança	APO12.02
	Cibersegurança e segurança da informação	
30	Estabelecer e assegurar a participação do comité ao nível da cibersegurança (ISSC)	EDM01.02 APO01.01
31	Integrar a direção da cibersegurança na direção geral de segurança da informação	EDM02.01
32	Estabelecer ligação/comunicação entre a função de cibersegurança e outras funções de segurança da informação (Alinhar as duas funções)	EDM01.02 APO01.01
33	Atribuir a organização, função e responsabilidades de cibersegurança apropriada (uso do RACI – matriz das responsabilidades)	EDM01.02 APO01.01 APO01.02 APO01.06
34	Identificar e definir formalmente os direitos de decisão para a organização de cibersegurança, incluindo os que possam ser aplicáveis em situações de tratamento de crises /incidentes	APO01.01
35	Definir e comunicar metas e objetivos de cibersegurança ao nível estratégico e inclui-los na estratégia de segurança. Fornecer e incluir marcos e datas de conclusão para metas e objetivos de cibersegurança	APO02.05 APO12.04 BAI05.01
36	Definir requisitos de cibersegurança como um subconjunto de requisitos gerais de segurança da informação	BAI02.01
37	Fornecer política de cibersegurança e padrões subsidiários alinhados e integrados com o conjunto geral de políticas de segurança da informação	APO01.03
38	Interligar as políticas de segurança da informação aos princípios orientadores para a cibersegurança	Política 1

Tabela 81- Check list de práticas de cibersegurança - elaboração própria com base no COBIT5TC

Nº	Requisito de Cibersegurança	Processo COBIT5
	Consciencialização, métricas e medidas	
39	Definir o cenário para consciencialização de cibercrime e ciberguerra	EDM01.02
40	Desenvolver um programa de consciencialização e instrução sobre cibersegurança, incluindo elementos baseados no risco	APO01.04 APO07.03
41	Integrar medidas e métricas de cibersegurança em mecanismos de verificação e avaliação rotineira da conformidade. Identificar e anotar exceções à conformidade que possam ser necessárias.	EDM01.03 APO01.08
42	Incluir medidas financeiras (impacto, danos) e não financeiras (legal, reputação, operacional, outras) para descrever o valor agregado das iniciativas de cibersegurança	EDM02.02
43	Obter aprovações necessárias para soluções, medidas e requisitos de cibersegurança; incluindo aceitações de risco para exposição remanescente a ataques, violações e incidentes (junto de quem financia assim como os stakeholders – estudos de viabilidade, análises de risco, etc)	BAI02.04
44	Atualizar as soluções de cibersegurança de acordo com as necessidades do negócio e requisitos operacionais (planos de manutenção/ revisões periódicas)	BAI03.10
45	Desenvolver etapas, ações e medidas detalhadas de cibersegurança para abordar o risco e incorporá-las ao sistema de cibersegurança (iniciativas)	BAI03.02 BAI05.05
46	Estabelecer testes apropriados, incluindo os ambientes de área restrita, para testar ações relacionadas à cibersegurança	BAI07.04
47	Definir ações corretivas relacionadas a ataques/violações/ incidentes; incorporar quaisquer ações corretivas e planos relacionados com a transformação geral de cibersegurança	MEA01.05
48	Adotar a mentalidade do atacante – maior estrago com menor esforço	Princípio 9
	Reporte e relatórios	
49	Identificar os meios e canais para comunicar questões e soluções de cibersegurança	EDM05.01
50	Incorporar o reporte de cibersegurança nos métodos genéricos de segurança da informação	EDM02.02
51	Identificar os requisitos que devem compor um relatório de cibersegurança	EDM05.01
52	Alinhar e priorizar os requisitos de relatórios às necessidades dos stakeholders internos e externos	EDM05.01 EDM05.02
53	Fornecer relatórios sobre projetos de cibersegurança, com referência específica a pontos fracos decorrentes de novas formas de cibercrime e ciberguerra	BAI01.11
54	Preparar relatórios de desempenho de cibersegurança	APO09.05
	Monitorização	
55	Acompanhar os resultados e efeitos da cibersegurança, relativamente às mudanças nos ataques, ameaças e incidentes. Comparar os resultados com as expectativas iniciais (atualidade) e futuro e outros marcos passados	EDM02.03
56	Integrar e medir o nível de integração da avaliação e gestão de risco de cibersegurança com gestão geral de risco de informação.	EDM03.01 EDM03.02 EDM03.03
57	Monitorizar a conformidade das medidas e métricas de cibersegurança que não fazem parte dos mecanismos regulares e rotineiros	EDM01.03
58	Monitorizar o perfil de risco para ataques/ameaças e o apetite de risco correspondente para alcançar um equilíbrio ótimo entre riscos de cibersegurança e as oportunidades de negócio	EDM03.03
59	Estender as regras de monitorização para cobrir todos os requisitos de cibersegurança; Definir métodos analíticos apropriados para coletar dados de desempenho e conformidade e incluir especificamente a monitorização de ataques e violações reais ou potenciais.	DSS01.03 MEA01.03
	Recursos	
60	Avaliar a eficácia dos recursos de cibersegurança, em comparação com as necessidades de segurança da informação e risco da informação (incluindo recursos externos)	EDM04.01 EDM04.02
61	Validar recursos de cibersegurança em termos de metas e objetivos específicos (incluindo recursos externos)	EDM04.02
62	Medir a eficácia dos recursos de cibersegurança (interna e externa) relativamente às necessidades, objetivos e metas definidas pela segurança da informação	EDM04.03
63	Desenvolver uma linha base de recursos para cibersegurança, incluindo critérios e indicadores de desempenho (KPI's)	APO02.02

Tabela 82- Check list de práticas de cibersegurança - elaboração própria com base no COBIT5TC

Nº	Requisito de Cibersegurança	Processo COBIT5
	Confidencialidade e sigilo	
64	Incorporar as necessidades de confidencialidade e sigilo no processo de identificação dos stakeholders	EDM05.01
65	Definir e observar formalmente os requisitos de confidencialidade e sigilo para auditores externos	EDM05.02
	Auditorias internas e externas	
66	Realizar auditorias internas e externas para avaliar a eficácia do programa de governança de cibersegurança.	EDM05.02
67	Definir e articular as instâncias de dependência do trabalho de terceiros (para auditores externos)	EDM05.02
	Controlos	
68	Definir relação entre os controlos de cibersegurança e os controlos genéricos de segurança da informação e incorporá-los no SGSI geral	APO13.01
69	Identificar e listar todos os controlos existentes e inclui-los no tratamento e plano de risco de segurança da informação	APO13.02
70	Recolher potenciais pontos de entrada (conectividade) a todos os níveis e tipologias de rede, categorizá-los e identificar os controlos relacionados existentes	DSS05.02 DSS05.03 DSS05.04 DSS05.05 DSS05.06
71	Definir rotinas de verificação/verificações aleatórias, conforme apropriado (controlos – acesso físico aos ativos)	DSS05.05
72	Identificar e categorizar os controlos existentes sobre intrusões, incluindo deteção técnica, reconhecimento de padrões, técnicas de invasão avançadas e não padronizadas.	DSS05.07
73	Monitorizar e avaliar continuamente, incluindo autoavaliações de controlo (CSA's) na cibersegurança, incluindo relatórios de ataques/fraquezas/falhas e outras atividades suspeitas, baseadas no risco	MEA02.04
74	Estabelecer controlos de ciclo de vida de software para aplicações auto desenvolvidas e personalizadas	Princípio 10
75	Participar com os fornecedores para alcançar os controlos de cibersegurança a montante	Princípio 10
	Acesso / identidade	
76	Assegurar que todos os usuários tenham direitos de acesso à informação de acordo com os requisitos do negócio, assim como, é feita uma adequada segregação das funções	DSS05.04
77	Alinhar a gestão de identidade ao modelo de governança selecionado	DSS05.04
78	Identificar controlos existentes sobre o acesso físico, combinados com a gestão de identidades.	DSS05.05
79	Definir verificações de antecedentes para indivíduos que entram em áreas sensíveis, particularmente para funcionários temporários e visitantes.	DSS05.05
	Informação	
80	Fornecer diretrizes relacionadas à cibersegurança sobre o significado de informação sensível e pessoal, assim como a respetiva classificação da informação no que toca a ataques e violações	APO01.06
81	Identificar e classificar fontes de informação de cibersegurança, inteligência externa e serviços relacionados e estatísticas de ataques/violações	BAI08.02
82	Avaliar a informação relacionada a ataques e violações, TI em geral, potenciais alvos e retirar informações obsoletas	BAI08.05
83	Fornecer informações sobre serviços, equipamentos e dispositivos para monitorizar e controlar o ambiente	DSS01.04
	Inovação	
84	Incluir inovação na gestão de cibersegurança como parte a inovação geral de segurança da informação	APO04.01
85	Avaliar potenciais vulnerabilidades, ameaças e risco associado de novas iniciativas	APO04.02
86	Verificar o impacto potencial de cibersegurança em relação às tecnologias e inovações emergentes e incluir os seus riscos e problemas associados	APO04.04
87	Priorizar as iniciativas de cibersegurança e os recursos necessários	APO06.02
88	Pesquisar e identificar tendências emergentes no cibercrime e ciberguerra e medidas de segurança relacionadas	APO04.03

Tabela 83- Check list de práticas de cibersegurança - elaboração própria com base no COBIT5TC

Nº	Requisito de Cibersegurança	Processo COBIT5
	Investimentos	
89	Determinar uma apropriada gestão dos investimentos de cibersegurança no contexto sistémico	APO05.01
90	Garantir que haja financiamento apropriado para cibersegurança	APO05.02
91	Obter as aceitações de risco quando o financiamento é insuficiente	APO05.02
92	Preparar e manter um orçamento de cibersegurança	APO06.03
	Recursos humanos	
93	Determinar obrigações, responsabilidades e tarefas de cibersegurança de outras funções organizacionais	APO01.02
94	Definir equipa de cibersegurança assim como requisitos necessários para a mesma	APO07.01
95	Definir e implementar procedimentos adequados para o final da contratação	Princípio 11
96	Assegurar o reconhecimento do pessoal da cibersegurança através de incentivos e reconhecimento apropriados	Princípio 11
	Serviços	
97	Definir/Adicionar serviços necessários, relacionados à cibersegurança e catalogá-los conforme apropriado	APO09.02
98	Avaliar os níveis de serviços do fornecedor em relação a critérios e requisitos de cibersegurança e definir os níveis operacionais	APO09.03
99	Analisar as cláusulas/requisitos relacionadas à cibersegurança nos contratos e atualizar os SLA's conforme necessário	APO09.05 DSS01.02
	Fornecedores	
100	Atualizar a classificação de risco para todos os fornecedores sujeitos a requisitos de cibersegurança. Avaliar a garantia, reunindo informação apropriada para verificações de antecedentes	APO10.04 MEA02.05
101	Avaliar e rever fornecedores para conformidade e desempenho de cibersegurança	APO10.05
102	Comunicar com os fornecedores para gerir as vulnerabilidades e pontos de entrada	Princípio 10
	Programas	
103	Definir casos de negócio e respetivo programa de cibersegurança com base em medidas de segurança obrigatórias e prioridades críticas de negócio	BAI01.02
104	Priorizar planos e projetos de cibersegurança num cronograma e identificar objetivos e benefícios de curto prazo, ou seja, ações imediatas para reduzir o número de ataques e violações	BAI05.04
105	Desenvolver e documentar projetos com especificações de cibersegurança de alto nível de acordo com o modelo de segurança e a dinâmica do sistema	BAI03.01
	Disponibilidade	
106	Definir e incluir quaisquer problemas/ameaças relacionados à cibersegurança, especificamente ataques e violações que ponham em causa a disponibilidade, desempenho e capacidade dos serviços; Fazer o levantamento daqueles que incluem fraquezas sistémicas	BAI04.01 DSS03.01 DSS03.03
107	Realizar avaliações de impacto para processos de TI e do negócio potencialmente afetados por ataques e violações	BAI04.02

Tabela 84- Check list de práticas de cibersegurança - elaboração própria com base no COBIT5TC

Nº	Requisito de Cibersegurança	Processo COBIT5
	Mudança / melhoria	
108	Definir o processo de melhoria contínua para cibersegurança	APO13.03 APO01.07 DSS02.07
109	Implementar um processo de reconhecimento de padrões (a todos os níveis) apontado para ataques e violações	DSS05.01 APO01.07
110	Definir metas como parte da transformação geral, para cibersegurança, em intervalos regulares e em função de ataques e violações reais	APO02.03
111	Avaliar as alterações de cibersegurança do ponto de vista da transformação; incorporar essas mudanças à gestão geral de mudanças	BAI06.01
112	Rever e consolidar quaisquer mudanças de emergência relacionadas à cibersegurança: Incluir todas as alterações importantes	BAI06.02
113	Documentar (de forma detetável e auditável) quaisquer alterações relevantes para a cibersegurança, incluindo mudanças nos negócios	BAI06.04
114	Identificar e contribuir com infraestruturas relacionadas com o risco de cibersegurança e vulnerabilidades e ameaças (gerindo as instalações e energia dos equipamentos) especialmente para as que possam ser um alvo	DSS01.05
115	Fazer cruzamento apropriado entre referencias de políticas e procedimentos de cibersegurança. Incluir cenários apropriados na política de BC (business continuity)	DSS04.01
116	Desenvolver, alinhar e testar os BCP's (business continuity plan) para cenários relacionados à cibersegurança. Incluir acordos incidentais no ciclo PDCA	DSS04.03 DSS04.04 DSS04.05

Tabela 85- Check list de práticas de cibersegurança - elaboração própria com base no COBIT5TC