iscac Politécnico de Coimbra

O modelo de Gestão de Riscos e o Sistema de Controlo Interno Integrado no Instituto Politécnico de Coimbra

David Miguel Ramos Marques

ISCAC | 2022

Instituto Superior
de Contabilidade
e Administração
Politécnico de Coimbra

David Miguel Ramos Marques

O modelo de Gestão de Riscos e o Sistema de Controlo Interno Integrado no Instituto Politécnico de Coimbra

Coimbra, novembro de 2022

Instituto Superior de Contabilidade e Administração
Politécnico de Coimbra

David Miguel Ramos Marques

O modelo de Gestão de Riscos e o Sistema de Controlo Interno Integrado no Instituto Politécnico de Coimbra

Trabalho de projeto submetido ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Auditoria Empresarial e Pública com especialização em Auditoria de Conformidade**, realizado sob a orientação da Professora Maria Georgina da Costa Tamborino Morais.

Coimbra, novembro de 2022

TERMO DE RESPONSABILIDADE

Declaro ser o autor deste projeto, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação do presente projeto.

"*Não se limite a ser apenas melhor do que os seus contemporâneos ou antepassados. Tente superar-se a si mesmo".*

William Faulkner

AGRADECIMENTOS

O meu agradecimento a todos aqueles que contribuíram para que a execução deste trabalho fosse possível.

Agradeço ao Instituto Politécnico de Coimbra, pela oportunidade de desenvolver o presente trabalho. Para a realização deste trabalho foi determinante o apoio de algumas pessoas, que contribuíram de uma forma positiva para execução deste projeto.

Agradeço os ensinamentos dos Professores que integram o curso de mestrado em Auditoria Empresarial e Pública, ministrado pelo Instituto de Contabilidade e Administração de Coimbra do Instituto Politécnico de Coimbra. Igualmente agradeço à supervisora deste projeto, Daniela Ferreira da Cunha e particularmente à Professora Maria Georgina da Costa Tamborino Morais, por todo o apoio demonstrado durante a parte letiva e posteriormente na parte não letiva, através da orientação deste trabalho.

Um especial agradecimento à minha família, pela compreensão e apoio.

RESUMO

A evolução da sociedade traz ao ensino superior e às suas instituições inúmeros desafios. As mudanças são constantes e diárias, seja derivada do local onde estão inseridas, do contexto socioeconómico dos estudantes, do uso da tecnologia, do aumento da regulação e mesmo das próprias necessidades e expetativas de outras partes interessadas que fazem parte destas organizações, dando origem a riscos. Estes associados à sua atividade, refletidos no seu próprio contexto, desde a decisão da criação da oferta formativa até à empregabilidade dos estudantes. Neste sentido, é fundamental que as Instituições de Ensino Superior (IES) identifiquem e enraízem o risco inerente à sua atividade. Por outro lado, estas entidades têm, na sua grande maioria, Sistemas Internos de Garantia da Qualidade (SIGQ) acreditados pela Agência de Acreditação e Avaliação do Ensino Superior (A3ES) e obrigatoriedade de disporem de um plano de Gestão de Riscos (GR) e Sistema de Controlo Interno (SCI) que englobe toda a organização. Este projeto tem como objetivo propor um modelo integrado, no Instituto Politécnico de Coimbra (IPC) com gestão de riscos (GR) e controlo interno (CI), baseado nas orientações técnicas e recomendações que constam nos seguintes documentos: *Enterprise Risk Management – Integrated Framework* e *Internal Control Integrated Framework* da autoria do *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), bem como os referenciais da A3ES. Nesse sentido, este projeto fornece uma abordagem sobre a GR e CI através de modelos reconhecidos internacionalmente, efetuando a sua integração com o próprio SIGQ.

A realização deste trabalho permite indicar que apesar da estrutura deste modelo ter sido desenvolvida, deve ser garantida a sua monitorização e avaliação da sua aplicabilidade e eficácia, com vista à melhoria institucional. As principais limitações estão associadas ao enquadramento teórico do modelo, dado desconhecer-se na prática algum caso que tivesse sido anteriormente desenvolvido, o que o torna um projeto pioneiro. Quanto a propostas futuras sugere-se a aplicação do projeto e identificação de riscos associados a todo IPC, desde a governação, passando pela conceção dos cursos e comparação com organizações congéneres. Em suma, a concretização deste projeto permitiu consolidar o conhecimento sobre a temática da GR, CI e executar, com êxito a proposta, criando as bases para a propor um modelo de GR e CI integrado no IPC, efetuando a ligação com o seu SIGQ.

Palavras-chave: Ensino Superior; Gestão de Risco, Controlo Interno, Qualidade.

ABSTRACT

The evolution of society brings numerous challenges to higher education and its institutions. Changes are constant and daily, whether derived from the place where they are inserted, the socioeconomic context of the students, the use of technology, the increase in regulation and even the needs and expectations of other stakeholders that are part of these organizations, giving rise to scratchs. These associated with its activity, reflected in its own context, from the decision to create the training offer to the employability of students. In this sense, it is essential that Higher Education Institutions (HEIs) identify and root the risk inherent in their activity. On the other hand, these entities have, for the most part, Internal Quality Assurance Systems (IQAS) accredited by the Higher Education Accreditation and Assessment Agency (HEAAA) and the obligation to have a Risk Management (RM) and Internal Control System (ICS) that encompasses the entire organization. This project aims to propose an integrated model, at the Polytechnic Institute of Coimbra (PIC) with risk management (RM) and internal control (IC), based on the technical guidelines and recommendations contained in the following documents: Enterprise Risk Management – Integrated Framework and Internal Control Integrated Framework by Committee of Sponsoring Organizations of the Treadway Commission (COSO), as well as the HEAAA references. In this sense, this project provides an approach on RM and IC through internationally recognized models, integrating them with IQAS.

Carrying out this work indicates that, despite the structure of this model having been developed, its monitoring and evaluation of its applicability and effectiveness must be ensured, with a view to institutional improvement. The main limitations are associated with the theoretical framework of the model, given that no case that had been previously developed was known in practice, which makes it a pioneering project. As for future proposals, it is suggested the application of the project and identification of risks associated with every PIC, from governance, passing through the design of courses and comparison with similar organizations.In short, the implementation of this project allowed consolidating knowledge on the theme of RM, IC and successfully executing the proposal, creating the bases for proposing a model of RM and IC integrated in the PIC, making the connection with its IQAS.

Keywords: Higher education; Risk Management, Internal Control, Quality.

ÍNDICE GERAL

ÍNDICE DE QUADROS

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS, ACRÓNIMOS E SIGLAS

A3ES	Agência de Acreditação e Avaliação do Ensino Superior
AI	Auditoria interna
AICPA	*American Institute of Certified Publics Accountants*
CAE	Comissão de Avaliação Externa
CCDRC	Comissão de Coordenação de Desenvolvimento Regional do Centro
CI	Controlo Interno
CIM	Comunidade Internacional
CTeSP	Cursos Técnicos Superiores Profissionais
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
CPC	Conselho de Prevenção da Corrupção
ERM	*Enterprise Risk Management*
FERMA	*Federation of European Risk Management Associations*
GR	Gestão de Riscos
ICIF	*Internal Control Integrated Framework*
IES	Instituições de Ensino Superior
IFAC	*Internacional Federations of Accounts*
IIA	*Institute of Internal Auditors*
IPC	Instituto Politécnico de Coimbra
ISA	*International Standard on Auditing*
ISO	*International Organization for Standardization*
MP	Macroprocesso
PI	Partes Interessadas
RGPD	Regime Geral de Proteção de Dados
RJIES	Regime Jurídico das Instituições de Ensino Superior
SASIPC	Serviços de Ação Social do Instituto Politécnico de Coimbra
SC	Serviços Centrais
SCI	Sistema de Controlo Interno
SIGQ	Sistema Interno de Garantia da Qualidade
UO	Unidades Orgânicas
UOA	Unidade Orgânica de Apoio
UOE	Unidade Orgânica de Ensino
UOI	Unidade Orgânica de Investigação

INTRODUÇÃO

As organizações estão em constante mudança, derivado muitas vezes das alterações complexas e imprevisíveis que ocorrem no mundo, trazendo cada vez mais riscos aos ambientes em que estas estão inseridas. Segundo (Moeller, 2011) quer seja a sua finalidade, lucrativa ou não lucrativa, existem para fornecer valor às suas partes interessadas, nos quais se incluem os trabalhadores e acionistas para uma empresa comercial ou os eleitores para uma entidade do setor público. Neste sentido, de acordo Hopkin (2010), o risco está presente em toda a parte e deriva diretamente da imprevisibilidade. Por sua vez, torna-se fundamental que as organizações, independentemente do seu âmbito de atuação, adotem práticas de gestão que assegurem a sua continuidade, nomeadamente, gerir os riscos inerentes ao seu funcionamento de uma forma consciente e sistematizada (Hill, 2006; Ching, 2011). Consequentemente a Gestão do Risco (GR), tem evoluído nos últimos tempos, que na opinião de Rodrigues (2013) deriva de vários fatores, estes externos e internos, como é caso da globalização, liberalização; da instabilidade, da crescente preocupação relativamente aos aspetos legais e regulamentares e ao governo societário; do progresso tecnológico e a maximização de riqueza das partes interessadas (PI). Em consonância, (Purdy, 2010; Frigo e Anderson, 2011) referem que a exposição das organizações ao risco é inevitável, mas se estas quiserem assegurar o seu desenvolvimento há que potenciar oportunidades e minimizar as ameaças. No caso das IES, estas enfrentam uma indeterminada quantidade de riscos de origem externa e interna. Historicamente, a GR nestas instituições tem-se concentrado, principalmente nos riscos associados às áreas académica, financeira e recursos humanos. No entanto, os desafios da atividade das IES são inúmeros e permanentes, o que origina mudanças na sua governação e consequentemente na GR. A GR Empresarial (*Enterprise Risk Management* – ERM) permite, de forma integrada nos processos de gestão e de tomada de decisão, abordar todos os tipos de risco a que estas organizações estão expostas.

A ERM é, atualmente, um modelo de GR que apresenta vantagens reconhecidas internacionalmente. Neste sentido, gerir riscos *possibilita às empresas se beneficiarem de um enfoque integrado que desvie seu foco de uma situação defensiva de mitigação de risco para estratégia e de agregação de valor aos acionistas* (Ching 2011, p.257). Por outro lado, a publicação do Decreto-Lei n.º 109-E/2021 de 9 de dezembro, exige que as

entidades públicas tenham em funcionamento a GR. Por sua vez, no âmbito da mesma legislação existe a obrigatoriedade de terem Sistema de Controlo Interno (SCI). Em suma, os SCI devem ter por base modelos adequados de GR. Neste sentido, constitui objetivo do presente trabalho, propor um modelo de GR cruzado com o SCI do IPC, integrando a nível de riscos e controlos com o SIGQ, visando um modelo integrado que deriva destas três estruturas. Assim propõe-se: verificar se existem mecanismos e instrumentos de GR implementados na IES; propor um modelo de GR baseado no modelo ERM do COSO 2017 com o cruzando do modelo ICIF do COSO 2013, integrando-o no IPC, juntamente com a ligação ao SIGQ; aferir sobre o grau de maturidade do modelo ERM do COSO, operacionalização do Plano de GR e contributo para a instituição. Considerando os objetivos do Projeto, são recolhidos e tratados os dados, efetuado um enquadramento do IPC e descrita a metodologia a aplicar, finalizando-se com a proposta do modelo integrado e análise critica.

Em relação à estrutura deste projeto, o atual documento começa por fazer uma revisão da literatura direcionada para a temática da GR e CI, realizando a inserção de conceitos essenciais para a compreensão exata dos dados que suportam a atual GR e SCI do IPC. É efetuado um levantamento de conceitos e elencado benefícios e limitações dos modelos aceites internacionalmente e implementados nas organizações. No terceiro capítulo deste projeto é caraterizado o IPC, seguindo-se uma descrição do processo a propor, nomeadamente: um modelo de GR e o SCI integrado na IES. Sobre o CI, os componente e princípios previstos no modelo ICIF do COSO 2013, apresentam-se como complementares, não só pela convergência com os princípios estabelecidos pelo modelo ERM do COSO 2017, mas também porque é considerada uma referência mundial para auxiliar as organizações a atenderem aos requisitos associados a um controlo interno eficaz.

Importa então criar e propor um modelo de GR que assente no cumprimento de requisitos legais e simultaneamente normativos. Mais do que apresentar um modelo complexo, ambiciona-se um modelo útil à gestão pública e adaptável à realidade das diversas entidades. Neste contexto surge o presente projeto com o tema: O modelo de Gestão de Riscos e o Sistema de Controlo Interno Integrado no Instituto Politécnico de Coimbra. A atualidade e inovação do tema, a existência de poucos trabalhos em relação à proposta de um modelo de GR ligado com o SCI, tornando integrado e com base no SIGQ, no domínio

de atuação pública, a disponibilidade e a possibilidade de participar diretamente no desenvolvimento do estudo revelam-se como as principais razões para a escolha desta temática.

O tema apresentado indica que as opções metodológicas convergem para um estudo de caso. O IPC encontra-se acreditado no âmbito do SIGQ pela A3ES. Neste sentido, a delineação de um modelo de GR, deve assentar na integração dos princípios e orientações previstos nos modelos ERM do COSO 2017 e ICIF do COSO 2013 e nas práticas de gestão desta IES. Desta forma, evidencia-se a contribuição deste trabalho no sentido de se constituir como uma orientação para a aplicação deste processo no IPC.

1 A GESTÃO DE RISCOS

O mundo está constantemente com alterações, estas derivam de impactos e incertezas que todos os dias a sociedade se depara, ou seja, mudanças que trazem consigo alguns perigos, mas também oportunidades para serem geridas. O termo "risco" tem sido usado em inúmeras situações ao longo dos tempos, é criado ou modificado em todas as tomadas de decisão que, por sua vez, constituem parte integrante do quotidiano das organizações. No entanto, parece não existir, ainda, uma definição universal. Neste sentido, este capítulo está estruturado com uma breve contextualização do risco, nomeadamente definição, seguindo a identificação dos tipos de riscos. A GR nas organizações; os principais modelos e comparação entre eles; o caso do setor público, nomeadamente o ensino superior, são as restantes partes deste capítulo que pretendem demonstrar a GR como um forte instrumento a nível organizacional.

1.1 Contextualização do risco - definição

O significado de risco não é universal. Da pesquisa efetuada é possível referir que o termo de "risco" adquire, na sua globalidade, um cariz negativo. No dicionário Priberam da língua portuguesa indica *perigo, inconveniente* e no dicionário de língua portuguesa da Porto editora, significa *possibilidade de um acontecimento futuro e incerto; diferença entre o retorno esperado e o retorno obtido*. Por outro lado, a terminologia "risco" deriva do italiano antigo *risicare,* que significa ousar. Hill (2006); Rendóm e Garcia (2015) consideram que todos temos um conceito diferente do que é o risco, todos o gerimos, ainda que não seja de forma estruturada e planeada. Neste sentido, o risco é uma opção e não um destino (Bernnein, 1996). Por sua vez, segundo Valente (2000), todos partilhamos da opinião de que estamos perante uma situação de risco *quando existe a probabilidade de uma determinada situação ter um resultado que não é o desejado*. (p. 2). Assim, o risco *consiste num conjunto de circunstâncias que impedem a realização dos objetivos* por parte das organizações (Griffiths, 2006, p.2). A nível de negócios, a *International Standard on Auditing* 315 [ISA 315 do IFAC] - *Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment*, estipula o risco como o resultado de condições, acontecimentos, circunstâncias, ações […] que podem afetar adversamente a capacidade de uma entidade para atingir os seus objetivos

e executar suas estratégias (IFAC, 2010a). Deste modo, o risco consiste no pressuposto de ocorrer um acontecimento que causa algum tipo de dano numa organização, seja este humano, patrimonial, financeiro ou de imagem. Em relação ao perigo, é a fonte de ocorrência potencial, onde o risco mede a possibilidade da sua ocorrência e estima a gravidade do seu impacto. Em síntese, o significado para o termo risco, não é consensual, deriva da probabilidade de uma ocorrência que pode causar algum tipo de nocividade nas organizações.

1.1.1 Tipos de riscos

As organizações durante o seu percurso de vida estão expostas a inúmeros riscos, alguns suscetíveis de controlo, ou seja, o risco é inevitável e proteger-se de todos é impraticável. Por conseguinte, o exercício do estabelecimento de objetivos atendendo aos riscos e implementação de controlos necessários de modo a mitigar os mesmos, é uma prática cada vez mais adotada, não só pelas organizações que visam o lucro, mas também por aquelas que desenvolvem uma atividade exclusivamente direcionada para a prossecução de objetivos de carácter social (Rodrigues, 2013). Assim, as organizações estão expostas a inúmeros riscos, podendo ser categorizados por tipologia, conforme demonstrado no quadro 1.1, como por exemplo: financeiros, operacionais, relacionados com delegação de autoridade, relacionados com o processamento da informação, tecnológicos, relacionados com a prática de fraude e atos ilegais, estratégicos.

Quadro 1.1 - Tipologia de riscos

Tipologia de riscos
financeiros
operacionais
relacionados com a delegação de autoridade (*empowerment risks*)
relacionados com o processamento da informação
tecnológicos
relacionados com a prática de fraude e atos ilegais
estratégicos

Fonte: adaptado, Linsley e Shrives (2006)

Os riscos financeiros abrangem o risco de crédito, ou seja, a probabilidade de não obter crédito junto da banca ou de outros financiadores e de não cumprir com as obrigações que derivam das flutuações do valor dos instrumentos de dívida (Lopez & Saidenberg, 2000), bem como o risco associado à liquidez da organização, às flutuações das taxas de juro e de câmbio (Linsley & Shrives, 2006). Por sua vez, em relação aos riscos operacionais, segundo o COSO (2013); Linsley e Shrives (2006); Wei e Lewis (2003) dizem respeito a situações associadas aos processos produtivos, à produção/desenvolvimento de bens e serviços, à satisfação dos clientes, à reputação da organização, entre outras. O processo de gestão e liderança da organização e a forma como a delegação de autoridade é exercida ao longo da estrutura hierárquica da entidade está associado aos riscos relacionados com a delegação de autoridade (*empowerment risks*) (Linsley & Shrives, 2006). Relativamente aos riscos relacionados com o processamento da informação, deriva da possibilidade das demonstrações financeiras e outros documentos que suportam o processo de comunicação da entidade, conterem distorções, erros ou omissões materialmente relevantes, não detetadas oportunamente pelos sistemas de monitorização (COSO, 2013). Em relação aos riscos tecnológicos, Linsley e Shrives (2006) referem que estão relacionados com a volatilidade crescente ao nível das tecnologias, a dificuldade no acesso às mesmas, bem como a integridade das tecnologias instaladas. Sobre os riscos relacionados com a prática de fraude e atos ilegais, Linsley e Shrives (2006) consideram que estão incluídos os riscos de fraude ou atos ilegais por parte da gestão de topo, gestão dos empregados da organização, assim como os riscos que derivam dos danos na reputação da organização por via dessas práticas ilegais. Os riscos estratégicos consistem em obstáculos de sustentabilidade que provocam impactos na prossecução da missão e dos objetivos estratégicos, nomeadamente no posicionamento no mercado, nas relações com os investidores e na comunicação com as partes interessadas nos negócios da entidade (COSO, 2013; Emblemsvåg & Kjølstad, 2002). Em relação aos impactos, segundo Krane, Rolstadås e Olsson, (2010), os possíveis eventos que poderão provocar tais impactos são a implementação inapropriada de uma ou mais decisões e ainda a falta de resposta à volatilidade do ambiente.

Aos riscos mencionados, o COSO (2013), acrescenta os de conformidade, podendo estes ser vários e distribuídos por diversas áreas: segurança e saúde no trabalho, direitos humanos, leis laborais e ambientais. Por outro lado, no âmbito do meio envolvente, de acordo com a IFAC (2010b) os riscos devem ser agregados de acordo com a sua origem,

ou seja, internos e externos. Nos riscos internos, estão englobados: operacionais; relacionados com o *staff*; de saúde ocupacional e segurança; de localização e premissas de negócio; relacionados com o *goodwill* e com a reputação advindos de fraude e/ou má publicidade e, por último, os associados com a evolução das tecnologias de informação. Em relação aos externos, estes agrupam os riscos associados aos mercados, aos clientes, bem como os que possam advir dos investidores, entre outros.

A nível de dimensões, os riscos podem ser desagregados três categorias: macroambiental, industrial e corporativa Haley (2003). A macroambiental refere-se aos eventos políticos (revoluções e guerras), regulamentares (reformas legais e fiscais), macroeconómicos (inflação e impostos), sociais (estilos de vida) e ambientais (desastres naturais). A industrial está relacionada com a cadeia de produção (qualidade), na procura (preferências dos clientes e/ou potenciais clientes) e na relação com a concorrência (inovação dos produtos dos principais concorrentes). Por último, a corporativa compreende todas as funções do nível hierárquico superior, isto é, as funções da produção, da tecnologia, financeiras, gestão e as competências dos membros que constituem a organização.

Em suma, os tipos de risco que as organizações estão sujeitas foram descritos, exemplificando cada um deles. O próximo ponto aborda a GR nas organizações e os diversos modelos que estão associados a esta temática.

1.2 Gestão de riscos nas organizações

No contexto organizacional a temática da GR é algo que tem vindo a assumir considerável importância no seio das organizações, pois está diretamente relacionada com a sua capacidade de subsistir (Morais, 2008). Historicamente, a GR tendeu a ser informal e motivada, quase exclusivamente, pela conformidade com os regulamentos e leis vigentes (Barton, Shenkir e Walker, 2002). Hardy (2015) considera que embora a gestão tradicional do risco tenha os seus méritos, carateriza-se por ser executada sob a forma de silos, deixando-se "espaços em branco" entre funções organizacionais e sem que seja possível interpretar a transversalidade do seu impacto. Assim, impõe-se, um novo modelo no qual a GR que esteja integrado e seja coordenado ao longo de toda a organização, enraizando, na cultura organizacional, uma consciência de prevenção de riscos (Barton, Shenkir e Walker, 2002). Por sua vez, segundo Fraser e Simkins (2010), a ERM pode ser vista como uma evolução natural do processo tradicional GR.

> *No contexto atual, em que a natureza dos riscos que as organizações enfrentam muda rapidamente, os métodos utilizados para gerir os riscos também mudam, pelo que é previsível que as empresas sigam incorporando progressivamente a gestão de riscos na sua organização até chegar a uma gestão centralizada e integral. Desta forma, muitas das maiores organizações internacionais estão a instituir uma cultura de risco para a implementação com sucesso do processo de ERM* […]. (Castanheira & Rodrigues, 2006, p. 58)

Resumidamente, ao longo do tempo, a GR tem evoluído na sequência das mudanças ocorridas nas organizações, de modo a criar valor adicional a estas. Por outro lado, segundo Beja (2004) a GR como sendo um conjunto de meios utilizados na identificação, avaliação e relato do risco empresarial surgiu nos Estados Unidos da América em meados do século XX. No entanto, só no final do século XX é que a GR foi considerada como um elemento importante e essencial na gestão empresarial passando a fazer parte das boas práticas de gestão e apoiando a tomada de decisão. Neste sentido Castanheira e Rodrigues (2006) referem que a visão tradicional do risco tem vindo a sofrer alterações e a ganhar novas formas começando a dar cada vez maior importância ao conceito de GR. Assim, a abordagem tradicional do risco que assentava numa gestão informal e descentralizada onde cada área da organização gere os seus próprios riscos torna se cada vez menos frequente.

1.2.1 Conceito de gestão de riscos

Todas as organizações enfrentam uma variedade de riscos internos e externos, tanto a nível estratégico como a nível operacional. Cada risco tem uma probabilidade de ocorrência e um impacto de maior ou menor intensidade. As organizações devem identificar e avaliar sistematicamente estes riscos tentando gerir os mesmos através da implementação de medidas apropriadas de prevenção e contingência. Neste sentido, o processo de GR tem como objetivo minimizar o risco de um determinado evento a um nível aceitável em termos da probabilidade de ocorrência e do impacto das suas consequências. A nível de conceito, as definições relatadas na literatura são várias, seja mencionado pelos diversos organismos, normativos e investigadores da área. Hopkin (2010) considera GR, o conjunto de atividades dentro de uma organização que é realizado para entregar o resultado mais favorável e reduzir a volatilidade ou a variabilidade desse resultado. Por sua vez, os normativos definem diversos conceitos, nomeadamente o

modelo ERM do COSO (2004) refere que é um processo desenvolvido pelo conselho de administração, órgãos de gestão e outros elementos e que deve abranger toda a organização, aplicada na definição da estratégia a seguir pela organização.

O processo de GR deve ser projetado para identificar eventos potenciais que possam afetar a entidade e que permita gerir o risco dentro do apetite de risco definido, isto é o risco que podem ou querem suportar, de forma a proporcionar uma garantia razoável quanto à obtenção dos objetivos definidos pela entidade, nomeadamente a criação de valor. A *International Organization for Standardization* (ISO) através da norma ISO 31000 *"Risk management – Guidelines"*, estabelece a GR como atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco. Este *deve ser um processo contínuo e em constante desenvolvimento, aplicado à estratégia da organização (...). Deve analisar metodicamente todos os riscos inerentes às atividades passadas, presentes e, em especial, futuras de uma organização.* (FERMA, 2003, p. 3)

Para o Instituto de Gestão de Risco (IRM) de Londres: *é o processo que pretende ajudar as organizações a compreender, avaliar e atuar sobre todos os seus riscos, para aumentar a probabilidade de sucesso e reduzir a de fracasso* (Willsher, 2007, p. 45). Significa tomar ações corretivas para mudar a probabilidade de ocorrência dos riscos de forma a aumentar a probabilidade de ocorrência de resultados positivos e diminuir as de resultados negativos. Para a alcançar essa meta a GR deve adotar como estratégias de decisão a prevenção, a criação, a compra ou venda, a diversificação, a concentração e compensação e o impulsionamento dos riscos (Beja, 2004). Neste sentido deverá ser um processo organizado, sólido e constante ao longo de toda a organização para identificar, avaliar e reportar internamente as oportunidades e ameaças face à concretização dos objetivos da organização. Por sua vez a principal diferença entre o processo de GR e as outras formas tradicionais de GR é que o processo de GR adota uma perspetiva que coordena a GR ao longo de toda a organização em vez de cada área da organização gerir os seus próprios riscos (Banham, 2004). Um processo de transformação que altera a forma como as organizações gerem o risco, permitindo-lhes avaliar os riscos de forma continuada e identificar as medidas a tomar e os recursos a alocar na mitigação do risco (Funston, 2003). Vem representar um avanço na centralização da função de riscos, pois o que se pretende é integrar a gestão especializada dos diversos riscos numa única visão que abarque todas as interdependências, ou seja, as correlações dos diferentes riscos com

o objetivo de agregar o risco total da organização num único número e construir a partir desse número uma única estratégia de cobertura (Fuente & Veja, 2003). O processo de GR empresarial

> *inicia-se com a identificação e priorização numa base consistente de todos os riscos enfrentados pela organização. Numa segunda fase, segue-se a avaliação e mitigação dos principais riscos, sendo que os mesmos devem ser priorizados atendendo à sua probabilidade, ao valor atual do seu impacto e à qualidade dos controlos já implementados. Por último, o passo final no processo de ERM é a monitorização contínua dos riscos.* (Castanheira, 2007, p. 20)

Em síntese, a GR é descrita por inúmeros autores, cuja todas as definições têm a ideia subjacente de que as organizações que implementem processos de GR terão uma maior probabilidade de sucesso na identificação e controlo da ocorrência e tratamento dos riscos de impacto potencialmente negativo e de tirar vantagens e oportunidades dos riscos potencialmente positivos, tendo como principal objetivo a criação de valor.

1.2.2 Benefícios e limitações da gestão de riscos

As organizações têm, como objetivos, entre outros, a potencialização do seu valor para as suas partes interessadas. O valor pode, certamente, ser criado ou deflacionado por decisões de negócios tomadas a partir do topo, mas também pode ser criado, conservado ou corroído por decisões de rotina que ocorrem em todos os níveis dentro da organização. A ERM apoia a criação e/ou preservação de valor, ajudando a gestão a lidar eficazmente com potenciais eventos futuros que criam incerteza e a responder de forma a reduzir a probabilidade de resultados que levariam à erosão desse valor. Uma GR eficaz apoia o alinhamento da estratégia da entidade e os seus objetivos com o plano de gestão de riscos, facilitando a sua comunicação por toda a organização, e promove uma maior responsabilidade e propriedade dos controlos internos em toda a organização. O valor real da ERM é evidenciado quando as organizações olham para além da avaliação do risco com a única finalidade de atender a requisitos regulamentares mínimos (Marchetti, 2012).

Na opinião de Chapman (2011) a ERM poderá beneficiar as organizações, melhorando a sua capacidade em: aumentar a probabilidade de realização dos objetivos de negócio; construir uma maior confiança das partes interessadas; cumprir com os requisitos legais e regulamentares aplicáveis; melhorar a resiliência organizacional; melhorar o governo

corporativo; incorporar o processo de GR em toda a organização; minimizar surpresas e perdas operacionais; melhorar as decisões de resposta ao risco; otimizar a alocação de recursos; relacionar crescimento, risco e retorno; racionalizar capital; aproveitar oportunidades; melhorar a aprendizagem organizacional.

A ERM permite que a gestão opere de forma mais eficaz num ambiente de negócios onde o perfil de exposição ao risco organizacional está em constante mutação. Todavia, não existe um processo de GR que possa criar um ambiente livre de riscos (Chapman, 2011). Por outro lado, segundo Barton, et al, (2002) a incipiente ou má GR pode acarretar um preço enorme, designadamente, consideráveis perdas financeiras, diminuição do valor do acionista, dano na reputação, despedimento de quadros superiores e, em alguns casos, a destruição do negócio. Por sua vez, a GR pode ser gerida com base em diversos modelos, estando elencados alguns exemplos de estruturas conceptuais no quadro 1.2, como é caso, entre outras, do *Orange Book*; ISO 31000; *Enterprise Risk Management – Integrating with Strategy and Performance;* ISO 9001. Neste quadro está descrito a designação do modelo, descrição geral, autoria e ano.

Quadro 1.2 - Estruturas conceptuais de Gestão do Risco

Modelo	Descrição Geral	Autor	Ano
Orange Book	Atualiza a versão de 2004. Estabelece os princípios essenciais e de suporte para a GR no governo. Considera a eficácia da GR, avaliando a conformidade com os requisitos do Código de Governança Corporativa.	*Her Majesty's Treasure*	2020
ISO 31000	Documento para ser utilizado por pessoas que criam e protegem valor nas organizações, da tomada de decisões, do estabelecimento e consecução de objetivos e da melhoria do desempenho.	ISO	2018
Enterprise Risk Management – Integrating with Strategy and Performance	Atualização do modelo ERM integrando a estratégia e performance.	COSO	2017
ISO 9001	Referencial de Gestão da Qualidade, que apresenta como principal inovação, a abordagem ou conceito de pensamento baseado no risco.	ISO	2015
Integrated Framework Executive Summary	Complementa o *COSO Enterprise Risk Management – Integrated Framework*, emitido em 2004. É mais exigente que o anterior em matéria de avaliação, pois passou a ser obrigatória a autoavaliação por parte dos gestores sobre o CI da organização.	COSO	2013
Enterprise Risk Management – Integrated Framework	Introduz os conceitos de apetite pelo risco e visão integrada dos riscos (*Enterprise Risk Management-ERM*).	COSO	2004
FERMA	Estrutura para difusão da disciplina de GR na Europa a partir de uma visão objetiva do processo de GR.	*Federation of European Risk Managers Association*	2002

Fonte: atualizado e adaptado de Macieira (2008) e Magalhães (2017)

1.3 Modelos de gestão de riscos

A utilização da GR é preconizada por diversos modelos. Estes reconhecidos mundialmente, dos quais se destaca: a norma de GR da *Federation of European Risk Management Associations* (FERMA) de 2002; a GR Empresarial (ERM) – *Enterprise Risk Management – Integrating with Strategy and Performance*, emitido pelo COSO, de 2017; e a ISO 31000 da *International Organization for Standardization* de 2018. No quadro 1.3 são descritas as principais especificidades dos três modelos referidos.

Quadro 1.3 – Modelos de GR e suas especificidades

Modelo	Principais especificidades
FERMA	Esta norma não foi projetada tendo em mente um processo prescritivo para a GR empresarial. No entanto, descreve os componentes necessários para uma estrutura de GR empresarial, representando as melhores práticas para as organizações se medirem.
ERM do COSO	Coloca um maior grau de responsabilidade no órgão de gestão, exigindo que a administração não só apoie a GR empresarial, como também se envolva diretamente no processo.
ISO 31000	A principal diferença é a alteração de foco do evento para o efeito que o risco e a GR tem sobre os objetivos de uma organização. Sendo que os objetivos são normalmente articulados de forma mais clara e precisa. Coloca ênfase diretamente sobre a GR como disciplina estratégica, ajustada para a tomada de decisões sobre o risco.

Fonte: adaptado de (Hardy, 2015, p.127)

Independentemente do modelo de GR que se implemente, este não será capaz de garantir, com uma segurança absoluta, o cumprimento dos objetivos da organização, contribuindo, apenas, para a existência de uma segurança razoável na sua concretização. Acresce que, a GR é realizada por pessoas, o que determina, por si só, a existência de determinados riscos inerentes, como sejam, a título de exemplo, a possibilidade de ocorrência de erros ou lapsos, a subjetividade associada ao processo de tomada de decisões, o incumprimento doloso ou negligente dos processos de CI e das políticas de GR.

1.3.1 Modelo do *Comittee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management* (ERM do COSO)

O modelo ERM do COSO surgiu em 2004, desenvolvido em parceria com a PWC, sob supervisão da COSO, e incorporava dentro de si o modelo de CI COSO de 1992, para satisfazer as necessidades decorrentes de uma preocupação e focalização crescentes na GR, permitindo que as organizações adotassem este modelo com vista a satisfazerem as necessidades do seu SCI progredindo para um processo de GR.

O modelo de GR proposto pelo COSO é um modelo de referência, caracterizando-se por ser abrangente e completo, por ser a metodologia mais divulgada e reconhecida internacionalmente e a mais utilizada pelos profissionais de auditoria. Este modelo define GR como parte integrante do CI e preconiza a agregação dos riscos e uma visão global dos mesmos a partir do topo, ao contrário de muitas organizações que procedem à GR ao nível da subdivisão. O risco, interno e/ou externo à organização, deve ser parte relevante para a determinação da estratégia da entidade para alcançar os seus objetivos. O CI é também parte desse processo em que as estruturas de controlo e os procedimentos internos são essenciais para garantir que estes objetivos sejam alcançados.

1.3.1.1 O processo de gestão de riscos do modelo do COSO - Enterprise Risk Management and performance

O modelo ERM do COSO é uma estrutura para apoiar as organizações a perceber o que é o risco. De que modo é que ele está presente nas instituições e de que forma é que pode afetar de forma contrária os objetivos estratégicos da organização e a criação de valor, para identificar determinados acontecimentos que possam afetar a instituição. Destina-se a identificar, avaliar e gerir o risco de modo a fornecer uma segurança razoável quanto à realização dos objetivos da organização (COSO, 2004). A formulação deste modelo é baseada a partir da ideia de risco em vez da de CI. Neste sentido, desenvolve de forma sistemática todos os aspetos relevantes para uma GR e tem vindo a ser alterado desde a sua criação em 1992, sendo a última revisão ocorrida em 2017.

A abordagem do ERM do COSO deve ser incorporada na gestão estratégica e nos processos de gestão das organizações e englobar aspetos mais amplos do CI e não apenas aqueles que diretamente estão relacionados com o relato financeiro. Consequentemente, os responsáveis pela gestão devem adotar uma abordagem baseada no risco para avaliação do CI relativamente à sua eficácia. Este modelo deverá ser avaliado e implementado em toda a organização, partindo de um nível mais elevado (entidade) até chegar ao nível mais básico (atividades). Face às incertezas e diversidade de riscos que as organizações enfrentam os desafios colocados à gestão são o de determinar qual é o nível de incerteza que a empresa está preparada para aceitar e quais os riscos que enfrentam de modo a identificá-los, mensurá-los e priorizá-los.

Dada a relação entre risco e CI o objetivo principal do CI é auxiliar a gerir e a controlar o risco a que as organizações estão expostas e não de o eliminar, assumindo, por isso, um papel importante no auxílio à gestão e controlo do risco, na medida que pode transformar os riscos em oportunidades. Um bom SCI dependerá, então, de uma avaliação cuidada e regular da natureza e da dimensão dos riscos a que a empresa está exposta. Segundo o COSO (2004) toda a estrutura de GR é definida com o fim de alcançar os objetivos de uma organização que são classificados em quatro categorias, nomeadamente os objetivos estratégicos, operacionais, relato e conformidade.

A versão do modelo ERM do COSO de 2004, acrescentou relativamente ao COSO de 1992 mais uma categoria de objetivos, designada de objetivos estratégicos que operam a um nível superior em relação aos outros objetivos e que resultam da missão ou visão da organização com as quais deveriam estar alinhados os objetivos operacionais, de informação e de conformidade e inclui também o conceito de apetite ao risco e tolerância ao risco. Este conceito define o nível de apetite ao risco tolerado pela organização no sentido de lhe incrementar valor, ou seja, deverá ser quantificado o risco que está disposta a aceitar para assim perseguir um determinado objetivo.

A nova versão, do modelo ERM do COSO, passou a designar-se de gestão de riscos empresarial – integrado com estratégia e performance (*Enterprise Risk Management - Integrating with Strategy and Performance*), esta de 2017. Esta revisão, reduziu para cinco, os anteriores oito componentes definidos em 2004, apresentando diferentes pontos

de vistas e estruturas operacionais, melhorando estratégias e tomadas de decisão. A nova versão do modelo dá relevância à GR na parte do planeamento estratégico, sendo este incorporado em toda a organização, ou seja, o risco influencia e alinha a estratégia e desempenho em todas as funções e departamentos. Em resumo, esta atualização de acordo com o COSO (2017, p.V): elucida o valor da GR ao estabelecer e executar uma estratégia; intensifica o alinhamento entre performance e GR empresarial, com o objetivo de aperfeiçoar a definição de metas de performance e o entendimento do impacto do risco sobre a performance; contempla as expectativas relativas a governança e supervisão; reconhece a globalização dos mercados e das operações e a necessidade de aplicar uma abordagem comum; apresenta novas formas de interpretar riscos ao definir e atingir objetivos no contexto de maior complexidade dos negócios; amplia os aspetos de divulgação dos riscos para atender às expectativas das PI em relação a maior transparência; contempla tecnologias evolutivas e a proliferação de dados e análises de dados (*analytics*) que suportam no apoio à tomada de decisões; estabelece definições básicas, componentes e princípios para todos os níveis da organização envolvidos na conceção, implementação e execução das práticas de GR corporativas.

No âmbito da tomada de decisão, d*efinir uma estratégia implica fazer escolhas e aceitar trade-offs* (COSO, 2017, p.4). Por sua vez, o risco deve ter em consideração diversos processos de definição estratégica. A sua escolha é apenas um dos aspetos a considerar. O modelo ERM do COSO 2017, destaca dois outros aspetos que podem ter um efeito maior sobre o valor da organização: a possibilidade de desalinhamento e as implicações da estratégia escolhida. O primeiro está relacionado com a estratégia, missão, visão e os valores fundamentais da organização. A estratégia escolhida necessita do suporte da missão e a visão da entidade. Uma estratégia desalinhada aumenta a probabilidade de a instituição não conseguir concretizar a sua missão e visão, ou por em causa os seus valores. Por outro lado, as implicações da estratégia podem originar um desalinhamento nos riscos que estão associados aos objetivos operacionais (COSO, 2017).

A gestão de riscos empresarial – integrado com estratégia e performance, é uma estrutura aplicada a todas as organizações, independente da sua dimensão e demonstra de que maneira a integração das práticas de GR ajudam a acelerar o crescimento e melhorar a performance, instituindo princípios que podem ser aplicados desde a tomada de decisões estratégicas até à performance (COSO, 2017, p.1), conforme elencado na figura 1.1, com

este processo a iniciar com a missão, visão e valores fundamentais, dando seguimento à parte estratégica e da performance da organização.

Figura 1.1 - Representação gráfica do modelo ERM 2017 envolvendo a estratégia

Fonte: COSO (2017)

A GR tem apoiado muitas organizações a identificar, avaliar e gerir os riscos estratégicos. No entanto, as causas mais importantes de destruição de valor residem na possibilidade estratégica de não suportar a missão e visão da organização e nas implicações decorrentes da estratégia escolhida. A definição de uma estratégia requere um processo de decisão estruturado que analise os riscos e alinhe os recursos com a missão e a visão da organização. Este modelo de GR, integrado com estratégia e performance, é um modelo orientado, com realce para a importância da GR no planeamento estratégico e da sua incorporação em toda a organização, uma vez que o risco influência e alinha estratégia e performance em todos os departamentos e funções (COSO, 2017, pp. 5-6). A nova versão do ERM do COSO de 2017, passou de uma representação tridimensional, ilustrada num cubo (ERM do COSO de 2004), para um modelo com um conjunto de princípios, organizados em cinco componentes, nomeadamente: governança e cultura; estratégia e definição de objetivos; desempenho; análise e revisão; informação, comunicação e reporte, que estão inter-relacionados em forma de espiral, demonstrado na figura 1.2.

Figura 1.2 - Componentes do modelo ERM do COSO 2017

Fonte: adaptado de COSO (2017)

O modelo ERM do COSO de 2004, com a revisão ocorrida em 2017, sofreu alterações. O quadro 1.4 compara as principais modificações, através componentes dos modelos ERM do COSO 2017 e 2004 e princípios que continuam na estrutura conceptual.

Quadro 1.4 – Comparação entre modelo ERM do COSO 2017 e 2004

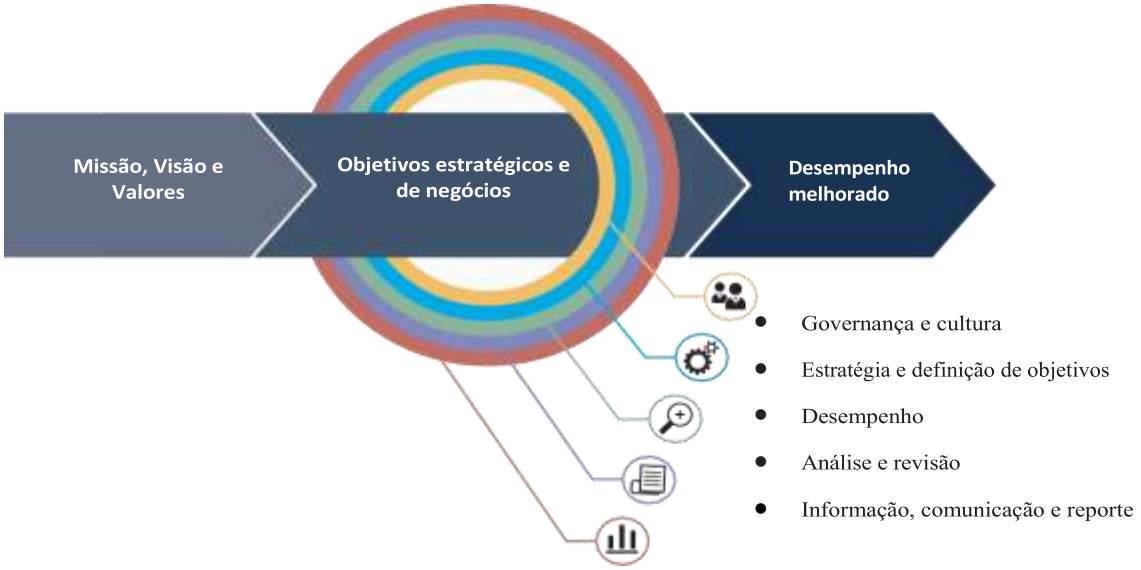
Componentes 2017	#	Princípios do modelo ERM COSO - 2017	Incluído no modelo 2004?	Componentes 2004
Governo e Cultura (*Governance and Culture*)	1	Supervisão dos Riscos através do Conselho de Administração	✓	Ambiente interno
	2	Estabelece estruturas operacionais	✓	
	3	Define a Cultura desejada	✓	
	4	Demonstra compromisso com os valores essenciais	✓	
	5	Atraí, desenvolve e retém profissionais qualificados	✓	
Estratégia e definição de objetivos (*Strategy and Objective-Setting*)	6	Analisa o contexto de negócios	✓	Definição de objetivos
	7	Define o apetite ao risco	✓	
	8	Avalia estratégias alternativas	ø	
	9	Formula objetivos de negócios	≠	
Desempenho (*Performance*)	10	Identifica o risco	✓	Identificação do evento
	11	Avalia a severidade do risco	≠	Avaliação de risco
	12	Prioriza os riscos	✓	
	13	Implementa resposta aos riscos	✓	Resposta ao risco e atividades de controlo
	14	Desenvolve uma visão de portfólio	✓	Resposta ao risco
Análise e revisão (*Review and Revion*)	15	Avalia mudanças significativas	✓	Monitorização
	16	Analisa riscos e desempenho	✓	
	17	Procura a melhoria da gestão de riscos de negócios	✓	
Informação, comunicação e reporte (*Information, Communication, and Reporting*)	18	Aproveita os sistemas de informação	✓	Informação e comunicação
	19	Comunica informações de riscos	✓	
	20	Divulga informações de risco, cultura e desempenho	✓	

Legenda: |✓tópico incluído| ≠ faltam alguns conceitos-chave| Ø faltam a maioria do conceitos-chave|

Fonte: adaptado, Terry e Prewett 2018)

Esta atualização efetua uma ligação mais clara entre a GR e expectativas das PI; posiciona o risco no contexto da performance da organização, e não como foco de um raciocínio isolado; permite às organizações antecipar-se ao risco. Igualmente dá maior ênfase na forma como a GR influencia a estratégia e a sua execução (COSO, 2017). A figura 1.3 demonstra a envolvência do modelo com os cinco componentes.

Figura 1.3 – Ilustração do modelo ERM do COSO 2017



Fonte: adaptado, https://commsrisk.com/new-coso-erm-framework-out-for-comment

O quadro 1.5 salienta a ligação dos cinco componentes do modelo ERM do COSO 2017 com os seus vinte princípios, com a descrição inerente a cada componente. A adoção dos princípios pode dar segurança à administração, na medida em que a organização é capaz de gerir aceitavelmente os riscos associados à estratégia e aos objetivos de negócios.

Quadro 1.5 – Modelo ERM do COSO 2017 – componentes e princípios

Componentes do modelo ERM do COSO 2017		#	Princípios
Governança e Cultura	A governança determina o tom da organização e reforça a importância da responsabilidade de supervisionar a GR na organização. Quanto à cultura, está relacionada aos valores éticos, comportamentos desejados e compreensão dos riscos na organização. O conselho de administração, através do seu papel de supervisão, é responsável por apoiar a criação de valor na organização e evitar seu declínio, pois o papel de supervisão é representado pela supervisão dos riscos.	1	Supervisão dos riscos através do Conselho de Administração
		2	Estabelece estruturas operacionais
		3	Define a cultura desejada
		4	Demonstra compromisso com os valores essenciais
		5	Atraí, desenvolve e retém profissionais qualificados
Estratégia e definição de objetivos	A GR da organização, as estratégias e a definição de objetivos fazem parte do processo de planeamento estratégico em que a empresa determina a sua disposição de assumir riscos e coordena a estratégia. Os objetivos colocam a estratégia em prática e servem de base para identificar, avaliar e responder aos riscos. Existem três tipos de riscos que devem ser considerados como parte do processo de planeamento: • Riscos relacionados com a estratégia escolhida. • A possibilidade de incompatibilidade da estratégia com a missão, visão e valor central da organização. • Implicações para a estratégia escolhida.	6	Analisa o contexto de negócios
		7	Define o apetite ao risco
		8	Avalia estratégias alternativas
		9	Formula objetivos de negócios
Desempenho	Os riscos que afetam o alcance da estratégia e dos objetivos de negócios da empresa devem ser identificados e avaliados, e os riscos devem ser priorizados de acordo com o grau de risco no contexto do desejo de risco da empresa. A empresa aposta no conceito de risco e escolhe a mais adequada para o risco. Os resultados desse processo são reportados aos principais *stakeholders* do risco.	10	Identifica o risco
		11	Avalia a severidade do risco
		12	Prioriza os riscos
		13	Implementa resposta aos riscos
		14	Desenvolve uma visão de portfólio
Análise e revisão	Como parte da revisão do desempenho da organização, a administração deve considerar, ao longo do tempo, a qualidade do trabalho dos componentes de GR na organização no caso de existir mudanças fundamentais, porque a administração deve ter em consideração as revisões necessárias.	15	Avalia mudanças significativas
		16	Analisa riscos e desempenho
		17	Procura a melhoria da gestão de riscos de negócios
Informação, comunicação e reporte	A GR da organização inclui um processo contínuo de obtenção das informações necessárias de fontes internas e externas e compartilhamento com as partes interessadas. A comunicação deve fluir para cima e para baixo e por toda a organização	18	Aproveita os sistemas de informação
		19	Comunica informações de riscos
		20	Divulga informações de risco, cultura e desempenho

Fonte: elaboração própria, adaptado de COSO 2017 e COSO 2020a

Sobre os vinte princípios, enumera-se as suas especificidades:

1. Exerce supervisão do risco por intermédio do conselho — O conselho de administração supervisiona a estratégia e cumpre responsabilidades de governança para ajudar a administração a atingir a estratégia e os objetivos de negócios.

2. Estabelece estruturas operacionais — A organização estabelece estruturas operacionais para atingir a estratégia e os objetivos de negócios.

3. Define a cultura desejada — A organização define os comportamentos esperados que caracterizam a cultura desejada pela entidade.

4. Demonstra compromisso com os valores fundamentais — A organização demonstra compromisso com os valores fundamentais da entidade.

5. Atrai, desenvolve e retém pessoas capazes — A organização tem o compromisso de formar capital humano de acordo com a estratégia e os objetivos de negócios.

6. Analisa o contexto de negócios — A organização leva em conta os possíveis efeitos do contexto de negócios sobre o perfil de riscos.

7. Define o apetite a risco — A organização define o apetite a risco no contexto da criação, da preservação e da realização de valor.

8. Avalia estratégias alternativas — A organização avalia estratégias alternativas e seu possível impacto no perfil de riscos.

9. Formula objetivos de negócios —A organização considera o risco enquanto estabelece os objetivos de negócios nos diversos níveis, que se alinham e suportam a estratégia.

10. Identifica o risco — A organização identifica os riscos que impactam a execução da estratégia e os objetivos de negócios.

11. Avalia a severidade do risco — A organização avalia a severidade do risco.

12. Prioriza os riscos — A organização prioriza os riscos como base para a seleção das respostas a eles.

13. Implementa respostas aos riscos — A organização identifica e seleciona respostas aos riscos.

14. Adota uma visão de portfólio — A organização adota e avalia uma visão consolidada do portfólio de riscos.

15. Avalia mudanças importantes — A organização identifica e avalia mudanças capazes de afetar de forma relevante a estratégia e os objetivos de negócios.

16. Analisa riscos e performance — A organização analisa a performance da entidade e considera o risco como parte desse processo.

17. Busca o aprimoramento no gerenciamento de riscos corporativos — A organização busca o aprimoramento contínuo do gerenciamento de riscos corporativos.

18. Alavanca sistemas de informação — A organização maximiza a utilização dos sistemas de informação e tecnologias existentes na entidade para impulsionar o gerenciamento de riscos corporativos.

19. Comunica informações sobre riscos — A organização utiliza canais de comunicação para suportar o gerenciamento de riscos corporativos.

20. Divulga informações de riscos, cultura e performance — A organização elabora e divulga informações sobre riscos, cultura e performance abrangendo todos os níveis e a entidade como um todo. (COSO 2017, p.10)

1.3.1.2 Benefícios e limitações ao modelo ao modelo ERM do COSO

O modelo ERM do COSO tem recebido ao longo dos últimos anos, diversas análises que apontam os seus benefícios e limitações, apresentados no quadro 1.6.

Quadro 1.6 – Principais benefícios e limitações do modelo ERM do COSO

	Benefícios	Limitações
Modelo ERM do COSO	Harmonização internacional dos processos de GR, proporcionando os princípios e orientações genéricas sobre a sua aplicação	Subjetividade inerente ao processo de tomada de decisões pode enviesar as respostas aos riscos
	Identificação, visualização integral e responsabilização dos riscos nas organizações	Uma efetiva GR apenas proporcionará uma segurança razoável à administração e ao conselho de administração quanto ao cumprimento dos objetivos da organização
	Eficiência através da adoção de medidas de ações corretivas	Deve-se avaliar a relação custo/benefício relativa à implementação de controlos ou de ações corretivas
	Maior probabilidade de atingir objetivos	O risco de acontecimentos negativos poder ocorrer causados por erros ou omissões humanas que, quando agregados, podem tornar-se significativos
	Melhor compreensão dos principais riscos e das suas implicações	O risco dos processos de CI poderem ser contornados pelo conluio
	Maior informação sobre os riscos e tomada de decisão	O risco da gestão ter a possibilidade e a capacidade de ignorar as decisões da organização em termos de GR

Fonte: adaptado Santos (2013); IIA (2004)

Em síntese, no que concerne a benefícios destaca-se: aumento do leque de oportunidades; identificação e gestão do risco na entidade como um todo; aumento dos resultados positivos e da vantagem com a diminuição das surpresas negativas; diminuição da oscilação da performance; melhor distribuição de recursos; aumento da resiliência da empresa (COSO, 2017).

1.3.2 Modelo da *Internacional Organization for Standardization* - ISO

A necessidade da criação uma norma internacional específica para a GR, resultou do facto da ISO ter constatado que existiam diversos grupos de trabalho que desenvolviam normas e procedimentos sobre GR e que utilizavam conceitos, terminologias, processos e pressupostos diferentes, criando muitas inconsistências e ambiguidades entre os diferentes normativos. Com base nessa informação foi criada a ISO 31000 com o objetivo de integrar e padronizar todos esses conceitos, terminologias, regulamentação e modelos anteriormente publicados, através de um processo consistente e uma estrutura abrangente, e de estabelecer os princípios e orientações genéricas sobre a estrutura e a implementação de um sistema de GR de forma a ajudar as organizações a gerir o risco de forma eficaz, eficiente e coerentemente.

1.3.2.1 Princípios para a gestão de riscos da norma ISO 31000

A norma ISO 31000 recomenda as organizações a desenvolver, implementar e melhorar continuamente um sistema de GR como uma componente integral do seu sistema de gestão. Nesse sentido, pode ser adotada por todo o tipo de organizações e dimensões, qualquer que seja o sector de atividade em que está inserida, podendo ser aplicada a toda a organização e para uma ampla gama de atividades, processos, funções, projetos, produtos, serviços, ativos, operações e decisões. Trata-se, portanto, de um modelo abrangente que tem como principal objetivo ajudar os responsáveis no desenvolvimento de políticas de GR das organizações a assegurar que os riscos são eficazmente geridos. A norma vem assim ajudar as organizações a desenvolver, programar e melhorar continuamente uma estrutura com a finalidade de integrar o processo de GR no governo, estratégia, gestão, processos e na cultura de toda a organização.

A ISO 31000 recomenda a adoção de processos consistentes dentro de uma estrutura própria para análise e gestão integrada dos riscos de uma organização, exigindo-se que as organizações procurem internamente harmonizar seus padrões, políticas e diretrizes

relacionadas com a GR, permitindo a otimização de tempo e de recursos para criar valor para a organização. A inovação deste modelo é a inclusão de princípios de gestão e a ênfase que é dada ao risco. O risco é definido como o efeito da incerteza sobre os objetivos e não apenas como um evento.

1.3.2.2 Benefícios e limitações à norma ISO 31000

O quadro 1.7 apresenta os principais benefícios e limitações da ISO 31000.

Quadro 1.7 – Benefícios e limitações ao normativo ISO 31000

	Benefícios	Limitações
Modelo ISO 31000	-Aumentar a probabilidade de atingir os objetivos; -Incentivar a gestão pró-ativa; -Consciencializar da necessidade de identificar e tratar o risco em toda a organização; -Melhorar: a identificação de oportunidades e ameaças; o reporte da informação financeira; a governação; a confiança dos *stakeholders*; os controlos; a eficácia e a eficiência operacional; o desempenho em segurança e proteção ambiental; a prevenção de perdas e a gestão de incidentes; a aprendizagem organizacional e capacidade de superar as adversidades organizacionais. -Cumprir os requisitos legais e regulamentares e as normas internacionais; -Estabelecer uma base confiável para a tomada de decisão e planeamento; -Utilizar eficazmente recursos para tratamento de riscos; De acordo com Leitch (2010): -A norma salienta, a importância de a GR fazer parte integrante do processo de gestão, a todos os níveis da organização, embora não forneça orientações específicas sobre a forma como se processa essa integração; destaca a importância de se considerar a interdependência dos diferentes riscos e das suas origens; afirma que a análise de risco pode ser tomada para diferentes níveis de detalhe, dependendo do risco; -A organização deve considerar e divulgar a confiança nas avaliações de risco efetuadas.	Segundo Purdy (2010): -os conceitos de apetite ao risco e tolerância ao risco são confusos e ambíguos, não havendo uma clara definição dos dois termos nem a evidência da diferença entre eles; -Resposta sobre até que ponto o tratamento do risco deve continuar quando se atinge algum critério de risco definido ou quando a relação custo/benefício é benéfica mesmo para os riscos com menor probabilidade de ocorrência e se deve haver lugar a um tratamento de risco adicional; -Embora a descrição da GR, existente na cláusula 4 da norma, ser bastante sucinta há alguns elementos que poderiam ser simplificados para que a estrutura e a sua implementação se tornassem mais compreensíveis, mais simples e menos onerosa para as organizações mais pequenas. De acordo com Leitch (2010): -Não ser clara, na medida que usa terminologia e definições complexas, ambíguas, pouco claras e compreensíveis; -O risco é também definido como podendo ser uma potencial surpresa agradável, no entanto a norma é descrita como se apenas potenciais surpresas desagradáveis fossem aí compreendidas e só sugere tratamentos para os riscos negativos; -Algumas das orientações levam a decisões ilógicas; -A norma inclui alguns requisitos idealistas que, seguidos literalmente, são impossíveis de cumprir; -As orientações não têm uma base matemática, nomeadamente quanto a probabilidades, tratamentos de dados ou modelos.

Fonte: adaptado de Santos (2013); Caetano (2017)

1.3.3 Norma de gestão de riscos da *Federation of European Risk Management Associations* - FERMA

A norma de GR da FERMA é a consequência do trabalho desenvolvido por uma equipa com elementos das principais organizações de GR do Reino Unido: *The Institute of Risk Management*; *The Association of Insurance and Risk Managers* e *The National Forum for Risk Management in the Public Sector*. Esta norma estipula que a GR:

> *protege e acrescenta valor à organização e aos diversos intervenientes, apoiando da seguinte forma os seus objetivos: criação de uma estrutura na organização que permita que a atividade futura se desenvolva de forma consistente e controlada; melhoria da tomada de decisões, do planeamento e da definição de prioridades, através da interpretação abrangente e estruturada da atividade do negócio, da volatilidade dos resultados e das oportunidades/ameaças do projeto; […]; redução da volatilidade em áreas de negócio não essenciais; proteção e melhoria dos ativos e da imagem da empresa;[…]; otimização da eficiência operacional*. (FERMA 2003, pp.3-5)

1.3.4 Comparação das principais normas e modelos

No quadro 1.8 é apresentada a comparação das principais normas e modelos, nomeadamente: FERMA; ISO 31000 e ERM do COSO.

Quadro 1.8 – Comparação das principais normas e modelos

		FERMA	ISO 31000	ERM do COSO
Âmbito		A GR não é apenas um tema para empresas ou organizações públicas, mas também para qualquer atividade ou projeto de curto ou longo prazo.	A norma fornece princípios e diretrizes genéricas sobre GR. Pode ser usada por qualquer organização.	Centra-se diretamente na realização dos objetivos fixados por uma entidade e proporciona uma base para a definição de GR empresariais.
Definições	Gestão de risco	Processo através do qual as organizações analisam metodicamente os riscos inerentes às respetivas atividades.	Atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco.	É um processo, aplicado na definição da estratégia e a toda a empresa, destinado a identificar potenciais eventos que possam afetar a entidade e gerir o risco dentro de seu apetite pelo risco.
	Risco	Combinação da probabilidade de um acontecimento e das suas consequências.	Efeito da incerteza sobre objetivos.	Possibilidade de um evento ocorrer e afetar adversamente a realização dos objetivos.
	Apetite pelo risco	Potencial de perda e impacto financeiro do risco Valor em risco (*value at risk*) Probabilidade e dimensão de perdas/ganhos potenciais.	Quantidade e tipo de riscos que uma organização está disposta a prosseguir ou reter.	Quantidade ampla de riscos que uma entidade está disposta a aceitar na prossecução da sua missão ou visão.
	Avaliação de risco	A avaliação de riscos é definida pelo documento ISO/IEC *Guide* 73 como o processo geral de análise de riscos e estimativa de riscos.	Processo global de identificação, análise e avaliação do risco.	Os riscos são analisados em função da sua probabilidade e impacto. Avaliados como sendo inerentes ou residuais.

Fonte: adaptado – Gjerdrum, *et al* (2011)

1.3.5 A gestão de riscos no setor público

A GR no setor público em Portugal tem vindo a ser implementada através de vários mecanismos. Em 1 de julho de 2009, o Conselho de Prevenção da Corrupção (CPC) aprovou a Recomendação relativa à elaboração e aplicação de planos de prevenção de riscos de corrupção e infrações conexas, publicada sob o n.º1/2009, no Diário da República (DR), 2.ª série, n.º 140, de 22 de julho de 2009. Esta recomendação dirigida aos órgãos dirigentes máximos das entidades gestoras de dinheiros, valores ou património públicos, seja qual for a sua natureza, administrativa ou empresarial, de direito público ou de direito privado. Recentemente através da aprovação do Decreto-Lei nº 109-E/2021, torna obrigatório que as entidades tenham plano de prevenção de riscos de corrupção e infrações conexas. Por sua vez:

> *1 — As entidades abrangidas adotam e implementam um PPR que abranja toda a sua organização e atividade, incluindo áreas de administração, de direção, operacionais ou de suporte, e que contenha: a) A identificação, análise e classificação dos riscos e das situações que possam expor a entidade a atos de corrupção e infrações conexas, incluindo aqueles associados ao exercício de funções pelos titulares dos órgãos de administração e direção, considerando a realidade do setor e as áreas geográficas em que a entidade atua; b) Medidas preventivas e corretivas que permitam reduzir a probabilidade de ocorrência e o impacto dos riscos e situações identificados. 2 — Do PPR devem constar: a) As áreas de atividade da entidade com risco de prática de atos de corrupção e infrações conexas; b) A probabilidade de ocorrência e o impacto previsível de cada situação, de forma a permitir a graduação dos riscos; c) Medidas preventivas e corretivas que permitam reduzir a probabilidade de ocorrência e o impacto dos riscos e situações identificados; d) Nas situações de risco elevado ou máximo, as medidas de prevenção mais exaustivas, sendo prioritária a respetiva execução; e) A designação do responsável geral pela execução, controlo e revisão do PPR, que pode ser o responsável pelo cumprimento normativo.* (artigo 6º do Decreto-Lei nº 109-E/2021)

1.3.5.1 Plano de gestão de riscos e corrupção e infrações conexas

O CPC, em reunião de 7 de abril de 2010, aprova, em complemento da Recomendação de 1 de julho de 2009, a Recomendação n.º1/2010, publicada no DR, 2.ª série, n.º 71, de 13 de abril de 2010, que recomenda:

> *Os órgãos dirigentes máximos das entidades gestoras de dinheiros, valores ou património públicos, seja qual for a sua natureza, administrativa ou empresarial, de direito público ou de direito privado, devem publicitar no sítio da respetiva entidade na Internet o plano de prevenção de riscos de corrupção e infracções conexas.*

Em dezembro de 2012, a Recomendação n.º 5/2012, de 7 de novembro do CPC, publicada no DR nº 219, 2ª série, de 13 de novembro 2012, consagra novas atividades e medidas por forma a servir de mecanismos de acompanhamento e de gestão de conflitos de interesses, devidamente publicitados, que incluam também o período que sucede ao exercício de funções públicas, com indicação das consequências legais. A recomendação sobre a gestão de conflitos de interesses de 8 de janeiro 2020, estipula que haja:

> *Identificação e caracterização de áreas de risco, designadamente as que resultem das situações de acumulação de funções, cujo tratamento de funções, cujo tratamento deve ser efetuado no âmbito e nos mesmo termos do Plano de Gestão de Riscos de Corrupção e infrações conexas"; "Identifiquem a caraterizem áreas de risco, designadamente as que resultem das situações de acumulação de funções, cujo tratamento deve ser efetuado no âmbito e nos mesmo termos do Plano de Gestão de Riscos Corrupção e infrações conexas.*

A 1 de abril de 2022, a CPC sobre práticas de Cibersegurança, recomenda que as entidades públicas reúnam os meios técnicos adequados para garantir um elevado nível de Cibersegurança, dando cumprimento ao estabelecido no Decreto-Lei nº 65/2021, de 30 de julho, e no Regulamento n.º 183/2022, de 21 de fevereiro, nomeadamente:

> *a) Implementação de mecanismo adequados de governação, risco e compliance; […] e) Cumprimento das medidas técnicas e organizativas destinadas a gerir os riscos que se colocam à segurança das redes, e dos sistemas de informação que utilizam; f) Realização de uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, ainda, aos ativos que garantam a prestação do serviço.*

Em suma, o setor público está legalmente obrigado a ter no seu quotidiano em toda a organização e atividade, incluindo as áreas de administração, direção, operacionais ou de suporte, GR.

1.3.5.2 A gestão de riscos nas Instituições de Ensino Superior

As Instituições de Ensino Superior (IES) estão reguladas pelo Regime Jurídico das Instituições de Ensino Superior (RJIES), por sua vez a recomendação do CPC de 1 de julho de 2009 fez com que estas organizações tivessem mecanismos de prevenção de riscos. Segundo Marques e Morais (2022a) a maioria das IES tem um plano, incluindo os de corrupção e infrações conexas e é objeto de auditoria interna (AI). Por sua vez, Machado, et al (2017) mencionam que os objetivos mais atribuídos à AI foram a melhoria dos processos e operações, bem como a avaliação e melhoria da eficácia dos processos de controlo e GR. Ribeiro (2016); Marques e Morais (2022b) mencionam que a maior parte das IES possuem um plano de GR, incluindo os de corrupções e infrações conexas, tendo como objetivo promover os sistemas de controlo interno (SCI), sendo as suas áreas de intervenção com maior incidência, a académica e os recursos humanos. Por outro lado, referem que a maior parte das instituições relata que a atividade de AI contribui para a identificação, avaliação e nomeação para ações de melhoria e prevenção dos riscos. Em suma, a GR e o CI geram valor às organizações, no caso das IES, aumentam a sua qualidade seja através da mitigação dos riscos ou mesmo na diminuição da fraude e corrupção (Marques e Morais, 2022b).

2 O CONTROLO INTERNO

O segundo capítulo deste projeto está estruturado da seguinte forma: definição de CI; tipificação de controlos; modelos de CI e CI no setor público.

2.1 Definição de controlo interno

Para o IIA (2012) o conceito de controlo está associado a qualquer ação desenvolvida pela gestão, pelo conselho e outras entidades, para aperfeiçoar a GR e a consecução dos objetivos da organização. A gestão planeia, organiza e dirige a realização das ações que assegurem com razoabilidade a consecução das metas e dos objetivos da organização.

Não existe uma única linha de pensamento para a definição de CI, apesar da evolução verificada quanto à perceção da sua importância para uma organização. Frequentemente imagina-se que o CI é um sinónimo de AI. Esta ideia é desacertada pois a AI, em termos gerais, equivale a uma atividade de apreciação independente, criada dentro de uma organização, a fim de examinar e avaliar as suas atividades, enquanto que o CI se refere a procedimentos adotados como planos permanentes e sistemáticos da organização. Assim:

> *devem os auditores ter consciência de que os controlos são adequados e úteis apenas se tiverem sido estabelecidos para atingir um objetivo determinado. E, como se compreende, os objetivos a atingir devem ser estabelecidos antes que possam ser implantadas as respetivas medidas*. (Carvalho, 1995, p. 46)

O *American Institute of Certified Publics Accountants* (AICPA) foi o primeiro organismo a definir CI, em 1934, SAS11 nº 1, usada pela SEC12, que definia:

> *o controlo interno compreende um plano de organização e coordenação de todos os métodos e medidas, adotadas num negócio a fim de garantir a salvaguarda de ativos, verificar a adequação e confiabilidade dos dados contabilísticos, promover a eficiência operacional e encorajar a adesão às políticas estabelecidas pela gestão.* (Morais & Martins 2013, p. 28)

Por sua vez, Attie (2000) defende que para melhor se perceber o conceito de CI este deve ser estudado profundamente, sobretudo quanto à sua plenitude e real significado. Neste sentido é fundamental os seguintes aspetos: plano de organização; métodos e medidas; salvaguarda de ativos; adequação e confiabilidade dos dados contabilísticos; eficiência operacional; políticas estabelecidas pela gestão, apresentados no quadro 2.1.

Quadro 2.1 – Principais aspetos do controlo interno

Aspetos	Descrição
Plano de organização	Modo pelo qual se organiza um sistema. A estrutura organizacional necessita corresponder a uma divisão de trabalho de forma que sejam estabelecidas as relações de autoridade e responsabilidade entre os vários níveis, para a consecução dos objetivos da organização de modo a serem claramente definidas as responsabilidades e autoridades dos diversos níveis.
Métodos e medidas	Procedimentos que estabelecem os caminhos e os meios de comparação e julgamento para se chegar a um determinado fim, mesmo que não tenham sido pré-estabelecidos formalmente. A organização, como um todo, pode ser caracterizada como a conjugação de vários subsistemas. Cada um dos subsistemas, por sua vez, compõem-se de uma cadeia de procedimentos destinados a gerar e a registar informações finais. O planeamento de um sistema deve ter em conta a definição de procedimentos especificamente destinados para promover o controlo sobre as operações e as atividades preferencialmente formalizadas através de manuais.
Salvaguarda de ativos	Compreende a forma pela qual são salvaguardados e defendidos os bens e direitos da organização. A definição e determinação da independência das funções de execução operacional (posse, controlo e contabilização dos bens patrimoniais, conjugada a um sistema de autorizações, de acordo com as responsabilidades e riscos envolvidos) possibilitam um eficiente e salutar meio de salvaguardar os interesses da organização.
Adequação e confiabilidade dos dados contabilísticos	Verificar se os dados contabilísticos correspondem com adequada precisão aos elementos constantes na contabilidade. A classificação dos dados dentro de uma estrutura formal de contas, seguida da existência de um plano de contas que facilite o registo, preparação e contabilização em tempo útil, a utilização de um manual descritivo do uso das contas conjugado à definição de procedimentos que possibilitem a análise, a conciliação e a solução tempestiva de quaisquer divergências, são elementos para a apresentação da imagem verdadeira e apropriada da situação financeira da organização.
Eficiência operacional	Compreende a ação a ser posta em prática nas transações realizadas pela organização. A definição de um adequado plano aliado aos métodos e procedimentos bem definidos, assim como a observação de normas no cumprimento dos deveres e funções com a existência de pessoal qualificado, treinado para desenvolver as atividades com adequada supervisão por parte dos seus responsáveis, tendem a implementar a desejada eficiência nas operações.
Políticas estabelecidas pela gestão	Compreendem o sistema de regras relativas à direção dos negócios e à prática dos princípios, normas e funções para a obtenção de determinado resultado. As políticas representam as direções de raciocínio, planeadas para a tomada de decisões em níveis inferiores e aplicáveis às situações repetitivas, de forma a canalizar as decisões para o objetivo que afetam tanto o comportamento da organização (política estratégica) quanto as regras de trabalho (políticas operacionais).

Fonte: adaptado de Attie, (2000, pp. 110-112)

Em resumo,

> *o controlo interno compreende todos os meios de planeamento de numa entidade para dirigir, restringir, governar e conferir as várias atividades com o propósito de fazer cumprir os seus objetivos. Os meios de controlo incluem, entre outros, a forma de organização, as políticas, os sistemas, os procedimentos, os registos, os métodos, a segregação de funções e o sistema de autorização e aprovação.* (Attie, 2000, p. 112).

Para o Tribunal de Contas (1999) é um modo de organização que presume a existência de planeamento e sistemas coordenados, estes destinados a prevenir a ocorrência de erros e irregularidades, maximizando o desempenho da entidade. Por sua vez, a organização do CI varia em função de fatores como a dimensão e a natureza da entidade, o número de unidades operacionais e a sua dispersão geográfica ou distribuição espacial (Tribunal de Contas, 1999, p. 47). Por outro lado, o IIA (2012) determina que a auditoria interna deverá contribuir para a instituição criar controlos efetivos, através da sua eficiência e eficácia, visando um aperfeiçoamento contínuo, nomeadamente com controlos eficazes onde a administração/gestão possa dirigir os sistemas para assegurar que os objetivos e metas estabelecidos da organização sejam cumpridos.

2.2 Tipificação de controlos

Os controlos podem ser classificados de acordo com diversos fatores, nomeadamente se tratar de questões preventivas, detetivas, que envolvam correções, orientações ou mesmo compensações. Neste sentido apresenta-se, no quadro 2.2, tipificação, finalidade e exemplos destes tipos de controlos.

Quadro 2.2 – Tipificação dos controlos

Categorização	Finalidade	Exemplificação
Preventivos	Impedir que factos indesejáveis ocorram. São considerados controlos à *priori,* que entram imediatamente em funcionamento, impedindo que determinados factos indesejáveis se processem.	Obter lista de fornecedores aprovada.
Detetivos	Detetar ou corrigir factos indesejáveis que já tenham ocorrido. São considerados controlos à *posteriori*.	Efetuar contagens físicas.
Corretivos	Retificar problemas identificados.	Relatórios de atrasos de cobrança de dívidas.
Orientativos	Provocar ou encorajar a ocorrência de um facto desejável, isto é, para produzir efeitos "positivos", porque boas orientações previnem que más aconteçam.	Estabelecer determinados requisitos para o recrutamento de pessoal.
Compensatórios	Compensar eventuais fraquezas de controlo noutras áreas da organização.	O total dos salários processados pelo serviço de recursos humanos pode ser cruzado com o total dos créditos feitos à segurança social através da contabilidade.

Fonte: Adaptado de Morais e Martins (2013)

2.3 Modelos de controlos interno

A aplicação de metodologias organizacionais para o CI tem vindo a ser desenvolvidas através de diversos modelos, como é o caso do ICIF do COSO; *Turnbull's Report Frameworks* e COBIT. Estes são usados na execução de políticas organizacionais internas relativamente à adoção de CI. O presente projeto irá incidir no ICIF do COSO.

2.3.1 *Internal Control Integrated Framework* - Modelo ICIF do COSO

No âmbito do CI, o modelo ICIF do COSO é representado através de uma matriz tridimensional, conforme é exemplificado na figura 2.1. Acrescenta três novos componentes em relação ao modelo de 1992, nomeadamente a definição de objetivos, a identificação dos eventos e a resposta aos riscos. Existe uma relação direta entre objetivos, que são as metas a alcançar pelas organizações, e componentes de GR, que são os meios necessários para atingir esses objetivos.

Figura 2.1 – Modelo ICIF do COSO

Fonte: COSO (2020b)

O quadro 2.3 demonstra os dezassete princípios do modelo ICIF do COSO e os cinco componentes associados a esta estrutura.

Quadro 2.3 – Componentes e princípios do modelo ICIF do COSO

Componentes	Princípios
Ambiente de controlo (*control environment*)	1. A organização demonstra ter comprometimento com a integridade e os valores éticos.
	2. O órgão de gestão de topo demonstra independência em relação aos seus executivos e supervisiona o desenvolvimento e o desempenho do controlo interno.
	3. O órgão de gestão de topo demonstra independência em relação aos seus executivos e supervisiona o desenvolvimento e o desempenho do controlo interno.
	4. A organização demonstra comprometimento para atrair, desenvolver e reter talentos competentes, em linha com seus objetivos.
	5. A organização faz com que as pessoas assumam responsabilidade pelas suas funções de controlo interno na busca pelos objetivos.
Avaliação de riscos (*risk assessment*)	6. A organização especifica os objetivos com clareza suficiente, a fim de permitir a identificação e a avaliação dos riscos que lhes estão associados.
	7. A organização identifica os riscos, em todos os níveis, que podem afetar a realização dos seus objetivos e analisa-os de modo a determinar a forma como devem ser geridos.
	8. A organização considera o potencial para a fraude na avaliação dos riscos que podem afetar a realização dos objetivos.
	9. A organização identifica e avalia as mudanças que poderiam afetar, de forma significativa, o sistema de controlo interno.
Atividades de controlo (*control activities*)	10. A organização seleciona e desenvolve atividades de controlo que contribuem na redução, para níveis aceitáveis, dos riscos que podem afetar a realização dos objetivos.
	11. A organização seleciona e desenvolve atividades gerais de controlo sobre a tecnologia para apoiar a realização dos objetivos.
	12. A organização estabelece atividades de controlo através de políticas que instituem aquilo que é esperado e os respetivos procedimentos que permitem a operacionalização daquelas políticas.
Informação e comunicação (*information and communication*)	13. A organização obtém ou gera e utiliza informações significativas e de qualidade para apoiar o funcionamento do controlo interno.
	14. A organização transmite internamente as informações necessárias para apoiar o funcionamento do controlo interno, incluindo os objetivos e as responsabilidades pelo controlo.
	15. A organização comunica com os públicos externos sobre assuntos que afetam o funcionamento do controlo interno.
Atividades de monitorização (*monitoring*)	16. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou independentes para se certificar da presença e do funcionamento dos componentes do controlo interno.
	17. A organização avalia e comunica, em tempo útil, aos responsáveis por tomar ações corretivas, incluindo o órgão de gestão de topo, deficiências no controlo interno.

Fonte: Adaptado de (Deloitte, 2014, p. 56 e COSO, 2019)

2.4 Controlo Interno no Setor Público

O CI é essencial ao funcionamento e à concretização dos objetivos de qualquer entidade. No âmbito de um sistema de informação contabilística é importante identificar e avaliar, de forma inequívoca, o SCI. Por sua vez, os serviços públicos devem dispor de um SCI atuante em duas vertentes: administrativa e financeira ou contabilística. A vertente administrativa ocupa-se dos procedimentos e registos relacionados com o processo de decisão que conduzem às autorizações das transações e operações. Consequentemente deverá ser um processo integrado e estruturado. Este efetuado pela administração e pelos seus colaboradores. Sendo desenhado para enfrentar os riscos, dar uma confiança aceitável na consecução da missão da entidade e alcance dos seus objetivos. Em relação à vertente financeira ou contabilística, está relacionada com a proteção dos ativos e informação fidedigna dos registos contabilísticos. Por outro lado, conforme estipulado pela ISA 315 do IFAC, o CI é o processo concebido, implementado e mantido pelos encarregados da governação, pela gerência e por outro pessoal para proporcionar segurança razoável acerca da consecução dos objetivos de uma entidade com respeito à fiabilidade do relato financeiro, eficácia e eficiência das operações, e conformidade com leis e regulamentos aplicáveis (IFAC, 2010a).

2.4.1 Controlo Interno nas Instituições de Ensino Superior

O SCI nas IES tem por base adequados sistemas de modelos de GR, informação e de comunicação, bem como um processo de monitorização que assegure a respetiva adequação e eficácia em todas as suas áreas de intervenção. Por sua vez, Marques e Morais (2022a) referem que as IES possuem normas e procedimentos de CI. Por outro lado, Saraiva (2010) relata que devem promover com regularidade revisões aos seus manuais de CI e verificar se os mesmos são conhecidos pelos seus utilizadores. Neste sentido, segundo Onescu (2018) a falta de CI ou a aplicação incorreta dos seus princípios constitui um dos principais riscos que levam ao incumprimento dos requisitos contratuais estabelecidos pelas entidades públicas. Por outro lado, de acordo com Sá (2018) um bom CI ajuda bastante a instituição a atingir os seus objetivos de uma forma eficaz e eficiente e previne a fraude. No entanto, o CI não se deve cingir à prevenção, verificação e correção de erros, mas fortalecer a gestão de desempenho das entidades, para garantir a realização de metas de desempenho (Huang, 2018), podendo prevenir mais fraudes do que os auditores (Arens et al., 2011). Por sua vez, as IES deveriam possuir um SCI que tenha

por base um modelo adequado de GR e serem avaliados através de AI (Marques & Morais, 2022b), que devem passar pela adoção de boas práticas organizacionais e modelos internacionalmente reconhecidos, mas igualmente pelo definido por lei.

A nível legislativo, os SCI no ensino superior derivam da existência de uma abordagem ao controlo interno, através da legislação que criou os planos setoriais.

O Decreto-Lei n.º 109-E/2021 de 9 de dezembro, cria o Mecanismo Nacional Anticorrupção e estabelece o regime geral de prevenção da corrupção, reforçando a obrigatoriedade das IES possuírem SCI e GR, nomeadamente ao estipular que:

> *1 — As entidades públicas abrangidas implementam um sistema de controlo interno […] que tenha por base modelos adequados de gestão dos riscos, de informação e de comunicação, em todas as áreas de intervenção, designadamente as identificadas no respetivo PPR. […] 3 — O sistema de controlo interno visa garantir, designadamente: […] d) A adequada gestão e mitigação de riscos, tendo em atenção o PPR; […] f) A prevenção e deteção de situações de ilegalidade, corrupção, fraude e erro; […] 5 — Para efeitos de avaliação da respetiva adequação e eficácia, as entidades públicas abrangidas promovem o acompanhamento regular da implementação do sistema de controlo interno, designadamente através da realização de auditorias aleatórias, reportando superiormente os seus resultados e eventuais condicionantes, e implementam as necessárias medidas corretivas ou de aperfeiçoamento. (artigo 15º, Decreto-Lei n.º 109-E/2021 de 9 de dezembro).*

Em resumo, as IES têm vários normativos que ligam a GR e o CI, incluindo os próprios sistemas de certificação e legislação do RGPD.

3 A GESTÃO DE RISCOS E O SISTEMA DE CONTROLO INTERNO NO INSTITUTO POLITÉCNICO DE COIMBRA

3.1 Caraterização do Instituto Politécnico de Coimbra

O Instituto Politécnico de Coimbra (IPC) é uma pessoa coletiva de direito público, provida de autonomia estatutária, pedagógica, científica, cultural, administrativa, financeira, disciplinar e patrimonial. Integra Unidades Orgânicas de Ensino (UOE) e uma Unidade Orgânica de Investigação (UOI), que dispõem de autonomia estatutária, pedagógica, científica, cultural, administrativa e disciplinar.

A definição dos objetivos e programa de ensino e de investigação, é da competência dos órgãos próprios do IPC e das suas Unidades Orgânicas (UO,) gerindo os seus recursos financeiros de acordo com critérios estabelecidos pelo Conselho Geral e Conselho de Gestão, incluindo os montantes atribuídos no Orçamento do Estado.

3.1.1 Objeto e Área de Influência

O ensino superior enfrenta um conjunto de riscos e oportunidades que resultam das profundas alterações ocorridas ao longo da última década, nomeadamente: alternações demográficas; persistentes disparidades sociais; desenvolvimentos científicos e tecnológicos e a digitalização; sustentabilidade ambiental; restrições orçamentais e o subfinanciamento; alterações no contexto geopolítico (IPC, 2021, p. 9). No âmbito do subsistema do ensino politécnico, o IPC, tem as seguintes atribuições: realizar ciclos de estudos visando a atribuição de graus académicos, bem como de outros cursos pós-secundários, de cursos de formação pós-graduada e outros, nos termos da lei; criar um ambiente educativo apropriado às suas finalidades; realizar investigação e o apoiar e participar em instituições científicas; transferir e valorizar económica e social o conhecimento científico e tecnológico; realizar ações de formação profissional; prestar serviços à comunidade; cooperar no intercâmbio cultural, científico e técnico com instituições congéneres, nacionais e estrangeiras; contribuir, no seu âmbito de atividade, para a cooperação internacional e para a aproximação entre os povos, com especial destaque para os países de língua portuguesa e os países europeus; produzir e difundir o conhecimento e cultura. Ao IPC compete, ainda, nos termos da lei, a concessão de creditações, equivalências e o reconhecimento de graus e habilitações académicos. (IPC, 2020, p. 12)

3.1.2 Missão, Visão, Objetivos

O IPC, de acordo com os seus Estatutos, é uma IES globalmente orientada para a prossecução dos objetivos do ensino politécnico, mais precisamente: formar alunos com elevado nível de exigência qualitativa, nos aspetos humanístico, cultural, científico, artístico, tecnológico e profissional; prepara os seus estudantes para a sua inserção e integração no mundo do trabalho e para um desempenho profissional de sucesso; formar profissionais com competências de resolução de problemas, de trabalho cooperativo e de liderança, desenvolvendo-lhes o compromisso com o comportamento ético e com o respeito pelos outros e pela sociedade, preparando-os para serem cidadãos exigentes, informados, produtivos, responsáveis e ativamente envolvidos no desenvolvimento cultural, educacional, económico, científico, social e político da comunidade; realizar atividades de pesquisa e investigação aplicada; prestar serviços à comunidade, tendo em vista a transferência de conhecimentos e a valorização recíproca; intercâmbio com instituições, nacionais, estrangeiras e internacionais; contribuir, no seu âmbito de atividades, para a cooperação internacional e para o encontro entre povos e comunidades; criar um ambiente de debate e de troca aberta de ideias, onde a criatividade, a descoberta e o desenvolvimento pessoal e social de todos os seus membros possa ocorrer. (IPC 2020, p.12). Por outro lado, tem definido no seu Plano Estratégico 2021-2025, um conjunto de cinco eixos estratégicos: 1 - Escola IPC; 2 - Inserção Territorial; 3 – Internacionalização; 4 – Investigação; 5 – Responsabilidade Social e Solidariedade.

No âmbito do primeiro eixo, o IPC deverá formar profissionais de qualidade; organizar-se para uma formação de elevada exigência; criar sinergias com as empresas e instituições; incentivar e intensificar o diálogo; continuar a criar na comunidade um sentido de pertença e de identidade com a instituição; continuar a criar ambientes felizes, integradores, atrativos; continuar a construir a marca Politécnico de Coimbra. Relativamente ao segundo eixo, o IPC deverá continuar a construir alternativas para se afirmar como parte indispensável no desenvolvimento da região; continuar a desenvolver parcerias com empresas e instituições do setor público, privado e social; aprofundar a relação com a CIM-Região de Coimbra e a CCDRC. Em relação à internacionalização (eixo 3), o IPC deverá privilegiar o espaço europeu para a criação de projetos de intervenção e de investigação e captação de fundos comunitários; continuar a apostar nas ligações aos países lusófonos; continuar a desenvolver relações com o espaço

iberoamericano; reforçar as ligações à diáspora lusa; continuar o trabalho desenvolvido na captação de estudantes internacionais; continuar a apostar na mobilidade de estudantes. Sobre a investigação (eixo 4), o IPC deverá: prosseguir com a organização interna do Instituto de Investigação Aplicada; aproveitar as oportunidades para a investigação, cocriação e transferência de conhecimento associadas ao Plano de Recuperação e Resiliência; aumentar o número de centros de investigação partilhados com a Universidade de Coimbra e com outras instituições do ensino superior politécnico; criar grupos sólidos de investigadores, que envolvam grandes equipas transdisciplinares e multicêntricas de forma a possibilitar uma maior atratividade da instituição relativamente a quem nos procura. Com o eixo cinco, o IPC deverá: ser solidário com os mais desprotegidos; promover o acesso à cultura e ao desporto através da disponibilização de uma oferta de atividades de cariz social e cultural, da promoção de atividades lúdicas de cariz cultural; fomentar a criação de mecanismos de apoio à inserção profissional e ao empreendedorismo; dar continuidade à implementação de projetos e ações no domínio da sustentabilidade ambiental; capacitar e ampliar as estruturas de alimentação e de alojamento (IPC, 2021, pp. 19-27).

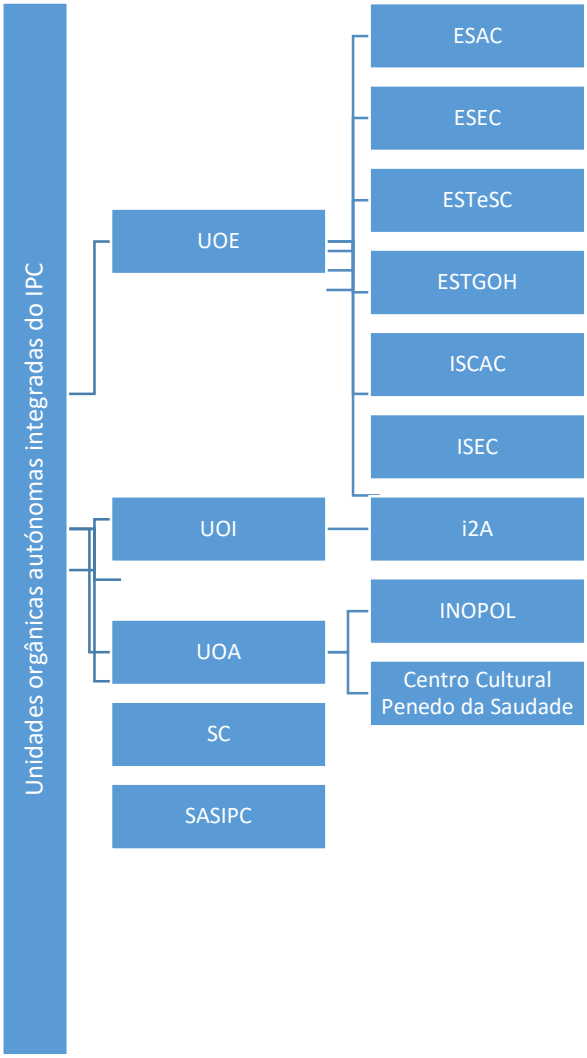
A operacionalização destes eixos estratégicos é proposta através da formulação estratégica. Esta, descrita no mapa estratégico, sustenta-se na definição dos objetivos estratégicos e interliga os eixos estratégicos com os objetivos a alcançar, de acordo com quatro perspetivas: Impacto; Processos internos e inovação; Capacitação; Financeira. A perspetiva *Impacto* abrange os resultados que derivam da estratégia da instituição; Em relação a *Processos internos e inovação*, abrange os processos e a inovação que a instituição terá de desenvolver para gerar os resultados da perspetiva anterior; a *Capacitação* abrange a criação de capacidade para, através dos recursos físicos e humanos de que dispõe, a instituição atingir os objetivos das restantes perspetivas; A *Financeira* abrange a captação dos recursos financeiros necessários à prossecução dos objetivos das restantes perspetivas (IPC, 2021, p.29).

3.1.3 Estrutura interna

O IPC integra unidades orgânicas autónomas, com pessoal próprio, nomeadamente: seis Unidades orgânicas de ensino ou de ensino e investigação (UOE), as quais compreendem a Escola Superior Agrária do IPC (ESAC), a Escola Superior de Educação do IPC (ESEC), a Escola Superior de Tecnologia da Saúde do IPC (ESTeSC), a Escola Superior

de Tecnologia e Gestão do IPC (ESTGOH), o Instituto Superior de Contabilidade e Administração do IPC (ISCAC), o Instituto Superior de Engenharia do IPC (ISEC); uma unidade orgânica de investigação (UOI), nomeadamente o Instituto de Investigação Aplicada (i2A); duas Unidades Orgânicas de Apoio à Formação e ao Desenvolvimento (UOA), o INOPOL (Academia de Empreendedorismo) e o Centro Cultural Penedo da Saudade; os Serviços Centrais (SC) e os Serviços de Ação Social (SASIPC).

Figura 3.1- Estrutura interna do IPC



Fonte: elaboração própria

A nível de dimensão, de acordo com o relatório de atividades de 2021, no período de referência 2020/21, o IPC tinha 9180 estudantes de licenciatura (1º ciclo), 1.880 de mestrado (2º ciclo) e 541 frequentaram os Cursos Técnicos Superiores Profissionais

(CTeSP). No que concerne aos recursos humanos (RH) (docentes e não docentes), a 31/12/2021 estavam afetos 995,5 ETI (equivalente a tempo integral). Destes, 61% eram docentes, 35% eram não docentes, 3% eram dirigentes e 0,2% eram investigadores. Em comparação com ano de 2020, o IPC registou um aumento total de 63,5 ETI. Os SASIPC a 31/12/2021 tinham afetos 52 trabalhadores, dos quais 94% eram não docentes e 6% eram dirigentes. Em relação à execução do orçamento, as receitas do IPC geradas em 2021 atingiram os 49,4 M€, mais 1,8 M€ do que em 2020. As receitas dos SASIPC geradas em 2021 atingiram 2,0 M€, menos 0,1 M€ do que em 2020.

3.2 Processo da Gestão de Riscos e a ligação ao Controlo Interno

3.2.1 Enquadramento contextual

O objeto de estudo foi definido. Posteriormente foi desenvolvida a pesquisa em relação à literatura científica. A fase seguinte, identifica quais as opções metodológicas com vista à recolha de informação e dados mais apropriados, bem como o seu tratamento. Deste modo, o presente projeto final de mestrado, estudo de caso, apresenta um tema específico e propõe-se a atingir os seguintes objetivos: (1) verificar se existem mecanismos e instrumentos de GR implementados no IPC; (2) verificar se estão previstas práticas de controlo interno na IES; (3) propor um modelo de GR, integrando-o no IPC através do modelo ERM do COSO 2017 em conjunto com o modelo ICIF do COSO 2013 (integração de modelos), tendo por base o SIGQ e (4) aferir sobre o grau de maturidade e a operacionalização do Plano de Gestão de Riscos de Corrupção e Infrações Conexas e seu contributo para a gestão do IPC.

3.2.2 Metodologia adotada

A notoriedade da investigação de estudos de caso, tem vindo a crescer. Meirinhos e Osório (2010) referem que o estudo de caso proporciona a integração com *múltiplas fontes de evidência (qualitativas e quantitativas) e enquadra-se numa lógica de construção de conhecimento, incorporando a subjetividade do investigador* (p. 64). Por sua vez, de acordo com Barata (2013) este método é útil quando o fenómeno a ser estudado é amplo e complexo e não pode ser estudado fora do contexto em que ocorre.

Considerando os objetivos propostos a alcançar, o estudo de caso será sobre um organismo público, o IPC, pelo qual os seus serviços prosseguem, nos termos da lei, fins de interesse público. O modelo integrado de GR e a sua ligação ao SCI nesta organização da administração pública, revela-se um tema atual e inovador. Por sua vez, o intuito de responder à pergunta de partida – O modelo de GR e o SCI Integrado no IPC? – fundamentam a presente opção metodológica – estudo de caso. Neste sentido, será desenvolvido um projeto, com um objeto de estudo claramente definido, tendo como suporte diversas fontes de informação. Além disso, será importante salientar que a oportunidade concedida para a realização deste projeto e a possibilidade de acrescentar conhecimento e valor ao IPC relativamente ao Sistema Interno da Garantia da Qualidade (SIGQ), às práticas de GR e CI revela-se um desafio. Por outro lado, este projeto implica a recolha de dados para o seu posterior tratamento. Em consonância, para este projeto sugere-se a apresentação do seguinte planeamento: 1-Recolha da documentação interna do IPC; 2-Aplicação de questionários; 3-Análise dos dados; 4-Elaboração de proposta de modelo a implementar: O modelo de Gestão do Risco com Sistema de Controlo Interno Integrado no IPC. Em síntese, este modelo tem por base a execução de um conjunto de etapas, nas quais se desenvolve as tarefas necessárias para prossecução dos objetivos definidos.

Etapas para preparação do modelo de GR e SCI Integrado no IPC:

Etapa I – Recolha, tratamento e análise de documentação externa e interna do IPC;

Etapa II – Criação de uma base de dados, efetuando o cruzamento com a norma de CI e o plano GR existentes no IPC (com validação posterior pela gestão de topo);

Etapa III – Estabelecimento dos objetivos do questionário, envio e tratamento de dados. (se o IPC tem implementado a GR e CI e aferir o grau de maturidade da GR do IPC, considerando os pressupostos do modelo ERM do COSO 2017);

Etapa IV – Elaboração de proposta a adotar relativa à integração de um modelo integrado.

Em suma e no seguimento das opções e procedimentos metodológicos anteriormente mencionados e metodologia aplicada no desenvolvimento do presente projeto, consultou-se determinadas fontes documentais, das quais destaca-se as apresentadas no quadro 3.1.

Quadro 3.1 – Principais fontes documentais do IPC consultadas

Designação	Informação Obtida
Despacho n.º 2008/2021	Alteração ao Regulamento Interno dos Serviços Centrais do Instituto Politécnico de Coimbra
Despacho Normativo n.º 21/2021	Alterações aos Estatutos do Instituto Politécnico de Coimbra.
Despacho SC/184/2022	Alteração ao Manual da Qualidade do IPC.
Estatutos do Instituto Politécnico de Coimbra	Hierarquia da estrutura organizacional e atribuições e competências das respetivas Unidades Orgânicas.
Manual de Qualidade	Meios adotados para assegurar a manutenção do SIGQ, âmbito de aplicação, procedimentos documentados e interação dos processos.
Norma de Controlo Interno	Princípios e procedimentos de controlo interno associados ao IPC.
Plano de Gestão de Riscos 2021-2023	Diretrizes sobre a identificação, avaliação e identificação dos responsáveis pelas atividades de GR organizacionais.
Plano Estratégico 2021-2025	Estratégia do IPC para o período 2021-2025.
Regulamento Interno dos Serviços Centrais do Instituto Politécnico de Coimbra (Despacho n.º 5110/2020)	Funcionamento orgânico do IPC a nível Responsabilidades e autoridades dos dirigentes.
Relatório anual de revisão 2020	Execução da situação do SIGQ do IPC.
Relatório de Atividades do Instituto Politécnico de Coimbra - 2021	Dimensão do IPC: estrutura interna; número de alunos; recursos humanos (docentes e não docentes); orçamento.
Relatório de Execução do Plano de Gestão de Riscos do IPC – ano de 2021	Avaliação da conformidade, estado de implementação e monitorização do plano de gestão dos riscos da organização. Grau de execução das ações desenvolvidas para tratamento dos riscos organizacionais.
Relatório de revisão pela gestão 2018 e 2019	Execução da situação do SIGQ do IPC.
Relatório final da CAE - ASIGQ/20/00001	Apreciação do grau de desenvolvimento do sistema interno de garantia da qualidade

Fonte: Elaboração própria

Em síntese, a nível de metodologia adotada, foi considerado o estipulado no Plano de Gestão de Riscos do IPC – 2021-2023, datado de novembro 2020 (riscos associados ao processo; nível de risco; situações que poderão originar o risco; medidas de controlo implementadas), cruzando com a norma de controlo interno, proposta apresentada e aprovada em reunião de Conselho de Gestão de 11 de janeiro 2018. De igual modo, foi efetuado uma ligação com o SIGQ, nomeadamente aos seus sete macroprocessos que estão definidos manual da qualidade com a alteração do despacho SC/184/2022. Um macroprocesso de gestão estratégia, governação e garantia da qualidade; quatro macroprocessos de missão (nucleares) e dois macroprocessos de suporte. Posteriormente os dados foram enviados e validados por parte da Presidência do IPC, sendo transpostos para o modelo proposto.

3.3 Estabelecimento do contexto

O IPC tem o seu SIGQ estruturado em sete macroprocessos: um macroprocesso de gestão estratégia, governação e garantia da qualidade (MP01 – Governação); quatro macroprocessos de missão (MP02 – Ensino/Aprendizagem; MP03 – Internacionalização; MP04 – Investigação; MP05 – Relação com a comunidade) estes considerados nucleares porque sistematizam as componentes centrais do IPC e dois macroprocessos de suporte (MP06 – Recursos Humanos; MP07 – Recursos Materiais e Serviços). Igualmente tem um plano de GR e SCI. No entanto, estes sistemas e estruturas estão isoladas, originando muitas vezes que se efetue um trabalho redundante dentro da organização, ou seja, esta IES necessita de integrar estes sistemas num só modelo.

3.3.1 Questionário: objetivos e resultados

O questionário (ver apêndice 1) irá contribuir para um melhor entendimento sobre a importância que é dada à GR e SCI no IPC. Igualmente saber o que é o IPC tem definido e contemplado para a sua governação. A obtenção de respostas sobre se o IPC tem implementado a GR e CI são conclusões que se pretendem ser retiradas. Em suma, tem como objetivo efetuar o respetivo diagnóstico, aferir junto do IPC sobre o cruzamento entre o CI e GR e aferir o seu grau de maturidade considerando o modelo ERM do COSO. Encontra-se dividido em cinco partes: dados de quem está a responder ao questionário; relação com SCI; gestão do risco; relação entre CI e GR; avaliação do grau de maturidade no IPC. O inquérito foi elaborado através da plataforma *GoogleDocs* e enviado para preenchimento ao membro da presidência com competência e dirigente intermédio para o devido efeito em relação aos sete Macroprocessos que constituem o SIGQ.

A recolha dos dados foi realizada entre os dias três e trinta e um de outubro de 2022, foram enviados a um total de sete dirigentes, nomeadamente: Vice-Presidência, Chefes de Divisão de gestão académica; da gestão financeira; gestão de recursos humanos e Coordenação de Serviços da comunicação e imagem, todos com responsabilidades inerentes aos macroprocessos. Devido a um número baixo de respostas, reforçou-se o pedido, com objetivo de obter-se um maior número de respostas possível. No entanto, obteve-se no total, duas respostas, representando uma taxa de 28,57%, das quais inconclusivas no que concerne à última parte do questionário, que permitiria aferir numa primeira abordagem o

grau de maturidade do modelo ERM do COSO 2017, ou seja, através das práticas já existentes de GR no IPC, replicando o estudo elaborado em 2021, pelo Instituto de Auditores Internos de Espanha: *"Auditoria Interna y gestión de riesgos"* e efetuando um diagnóstico sobre o atual estado de arte da GR no IPC, permitiria obter resultados com indicações sobre que medidas a IES deve tomar no sentido de melhorar a sua organização neste âmbito.

Das respostas obtidas, a totalidade pertence ao MP01 – Governação e referem que o IPC possui normas e procedimentos de CI, estando as seguintes áreas contempladas: financeira, recursos humanos, académica, proteção de dados e segurança da informação, contração pública e organização na globalidade. Sobre os meios de CI que existem no IPC, responderam que: Definição de autoridade e delegação de responsabilidades, segregação de deveres e funções; Confronto das contagens de caixa, títulos, ativos e existência com os registos contabilísticos; Verificação e conferência de registos e realização de conciliações; Meio de prevenção de erros e/ou procedimentos ilegais ou fraudulentos; Restrição do acesso físico direto aos ativos e registos; Aprovação e controlo de documentos; Comparação de informação com fontes externas de informação; Manual de procedimentos, formulários e documentos; Controlo de contas e balancetes de verificação; Rotinas de validação.

Em relação à GR e ao IPC ter implementado um processo formal, incluindo Plano de Corrupção e Infrações Conexas, assinalaram que sim, com a finalidade de *Estabelecer uma estratégia de prevenção do risco e comunicá-la à organização* e *Preventiva*. De igual modo, o IPC tem compreensão exata e abrangente dos riscos que atualmente enfrenta. No que concerne às áreas de intervenção previstas no plano de GR, indicaram as seguintes: Académica; Proteção de dados (RGPD); Contratação pública; Recursos humanos; Receita; Património; Propriedade intelectual; Segurança da informação (tecnologia); *Benefícios concedidos, orçamental*; *Todas as áreas de atuação que obedecem a normativos legais e/ou aplicáveis*.

Sobre as ações/procedimentos de intervenção previstos no plano, a totalidade respondeu: promover ações de formação de sensibilização dos trabalhadores para o risco de corrupção e infrações conexas; identificar as medidas implementadas para prevenir a ocorrência de riscos; desenvolver a atividade de auditoria interna; avaliar a segregação de funções e promover sistemas de controlo interno. Por sua vez, consideram o plano como

ferramenta essencial de prevenção de possíveis erros e/ou omissões. Em relação ao se assumir riscos é considerado uma estratégia de gestão, as respostas dividem-se. No que respeita às seguintes questões: se estão definidos e corretamente implementados controlos que mitiguem eficazmente os riscos identificados no IPC, de modo a não colocar em causa a concretização dos objetivos definidos pela gestão; se existem meios ou técnicas para identificar potenciais eventos que poderão originar riscos ou oportunidades; se os processo de GR são acompanhados pela gestão de modo a garantir que as respostas e as ações desenvolvidas para controlar ou eliminar os riscos são eficazes e estão em linha com os objetivos da organização; se periodicamente são analisados e reavaliados os riscos a que o IPC está exposta e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos; a totalidade respondeu que sim. Por outro lado, o IPC realiza acompanhamento do CI e GR com recurso às novas tecnologias de informação.

3.3.2 Identificação, avaliação e tratamento dos Riscos

A identificação inicial dos riscos pressupõe o envolvimento de diversas partes interessadas para a organização. Após esta identificação, na fase da avaliação dos riscos, se existirem alguns que ainda necessitem de tratamento por estarem acima do apetite ao risco da organização, novos controlos poderão ser abrangidos e os controlos existentes poderão ser complementados. Deste modo, ao realizar uma avaliação de risco, o primeiro passo é identificar o risco inerente e, em seguida, considerar os controlos eficazes e eficientes para chegar ao risco residual. Em termos de definições considera-se risco inerente, aquele que representa a quantidade de risco que existe com os controlos existentes no momento da identificação dos riscos, enquanto que risco residual é a quantidade de risco que permanece ou que aparece após a inclusão dos controlos adicionais e/ou ajustes dos controlos existentes.

A avaliação de riscos pode ser efetuada com base em diversas metodologias. No caso do IPC, foi utilizado como matriz: probabilidade X impacto (3 X 3, com a classificação do risco: reduzido; moderado; elevado). Por outro lado, a graduação dos riscos assenta no conceito de risco inerente. No âmbito do tratamento dos riscos, deve-se ter em consideração a identificação e implementação de planos de ação adequados aos riscos que são considerados críticos, ou seja, tratar riscos implica a escolha de determinadas

estratégias e planeamento para a sua concretização. Desde modo, com base na gravidade e avaliação dos riscos, a sua consequência poderá passar por: aceitar/prevenir; prevenir/transferir; investigar/evitar/partilhar, conforme demonstrado na figura 3.2. No entanto, não foram identificadas no plano de GR do IPC as consequências com finalidade do seu tratamento.

Figura 3.2 – Tratamento de riscos

Moderado Prevenir/Transferir	**Elevado** Investigar/Evitar/Partilhar	**Elevado** Investigar/Evitar/Partilhar
Fraco/reduzido Aceitar/Prevenir	**Moderado** Prevenir/Transferir	**Elevado** Investigar/Evitar/Partilhar
Fraco/reduzido Aceitar/Prevenir	**Fraco/reduzido** Aceitar/Prevenir	**Moderado** Prevenir/Transferir

Fonte: elaboração própria

A nível da identificação e análise dos riscos, a figura 3.3 apresenta através de uma matriz, os riscos identificados, sendo posteriormente cruzados e elencados neste projeto por processo do SIGQ. A valorização dos riscos na maior parte dos macroprocessos foi avaliada como reduzida. Sobre a classificação do risco como moderado, esta encontra-se nos macroprocessos: MP05, MP06 e MP07. O MP07 – *Recursos materiais e serviços*, tem igualmente riscos avaliados como elevado, nomeadamente em cinco processos da área *proteção de dados e de segurança da informação*.

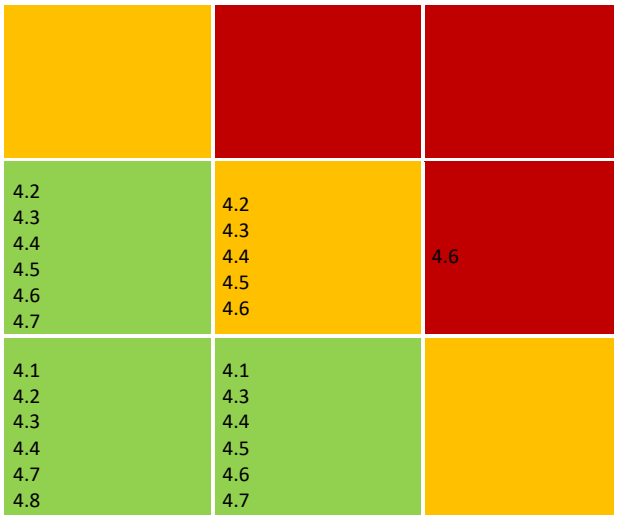
Figura 3.3 – Mapa de riscos – SIGQ do IPC

MP01 MP05 MP06 MP07	MP05 MP06 MP07	MP07
MP01 MP02 MP04 MP05 MP06 MP07	MP01 MP02 MP05 MP07	

Fonte: elaboração própria

Na figura 3.4 estão identificados e elencados os riscos de forma numérica, conforme definido no plano de GR 2021-2023 do IPC. A avaliação de risco "moderado" foi efetuada em cinco áreas conforme demonstrado. Contudo, a maioria dos riscos identificados do IPC, foram classificados como fraco/reduzido.

Figura 3.4 – Mapa de riscos do plano de GR do IPC



Fonte: elaboração própria

Os riscos foram identificados e resumidos, com a sua valorização, nas matrizes conforme demonstrado nas figuras 3.3 e 3.4, efetuando a sua ligação ao SIGQ através dos macroprocessos. Por outro lado, a nível do cruzamento com o SCI, não existe uma ligação com o plano de GR do IPC.

O quadro 3.2 demonstra a ligação proposta entre os dois modelos, ERM do COSO – 2017 com o ICIF do COSO 2013.

Quadro 3.2 – Integração dos modelos ERM do COSO 2017 e ICIF 2013

Componentes do modelo ERM do COSO 2017	Componentes do modelo ICIF do COSO 2013
Governança e Cultura	Ambiente de controlo
Estratégia e definição de objetivos	
Desempenho	Avaliação de riscos
	Atividades de controlo
Análise e revisão	Atividade de monitorização
Informação, comunicação e reporte	Informação e comunicação

Fonte: elaboração própria

3.4 O modelo de Gestão de Riscos e o Sistema de Controlo Interno Integrado no Instituto Politécnico de Coimbra

As IES têm uma importância fundamental no desenvolvimento nacional e nas comunidades onde estão inseridas. Estas são reguladas pelo Regime Jurídico das Instituições de Ensino Superior (RJIES). Por outro lado, o seu funcionamento está ligado à Agência de Avaliação e Acreditação do Ensino Superior (A3ES) e consequentemente aos SIGQ, que têm trazido mudanças relevantes para no seu funcionamento. Em relação ao seu desenvolvimento,

> *nos últimos anos, o sistema de ensino superior português registou uma evolução que merece ser referida. Uma enorme alteração resultou do aumento do fluxo de jovens que pretendem frequentar o ensino superior. Portugal registou um novo máximo histórico, atingindo 411 995 estudantes inscritos no ensino superior no último ano letivo (2020/21), mais 15 mil estudantes do que no ano letivo anterior, de acordo com a Direção-Geral de Estatísticas de Educação e Ciência, representando uma subida de 4% em relação ao ano anterior* (A3ES, 2021a, p.5).

A A3ES estipula a utilização de treze referenciais para os SIGQ. Estes estão assentes em cinco vetores e são a base para a certificação e acreditação das IES. Segundo a A3ES (2016) os vetores são:

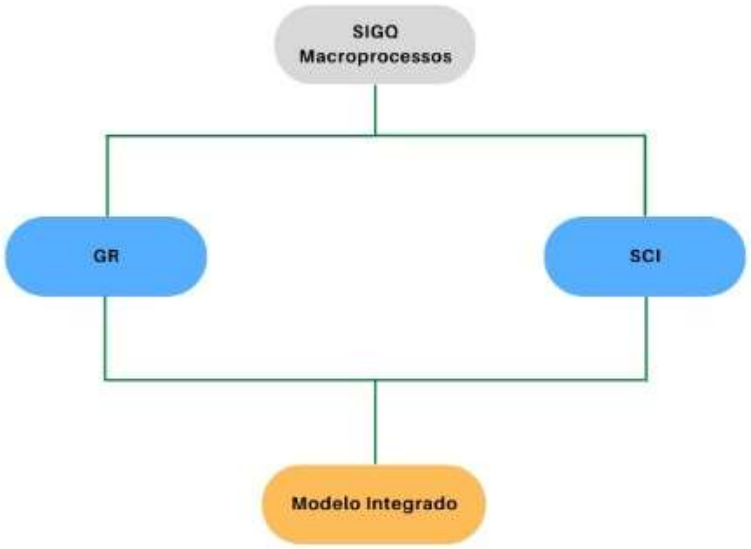
> *política para a garantia da qualidade*; *a garantia da qualidade nos processos nucleares da missão institucional*; *garantia da qualidade na gestão dos recursos e serviços de apoio*; *gestão e publicitação da informação*; *avaliação externa periódica*. (p. 1)

Em relação aos trezes referenciais, conforme estipulado pela A3ES (2016, pp. 1-7) são os seguintes: referencial 1 - *adoção de política para a garantia da qualidade e prossecução de objetivos de qualidade*; referencial 2 - *conceção e aprovação da oferta formativa*; referencial 3 - *ensino, aprendizagem e avaliação centrados no estudante*; referencial 4 - *admissão de estudantes, progressão, reconhecimento e certificação*; referencial 5 - *monitorização contínua e revisão periódica dos cursos*; referencial 7 - *colaboração interinstitucional e com a comunidade*; referencial 8 - *internacionalização*; referencial 9 - *recursos humanos*; referencial 10 - *recursos materiais e serviços*; referencial 11 - *gestão da*

informação; referencial 12 - *informação pública*; referencial 13 - *caracter cíclico da garantia externa da qualidade*. Por sua vez, a A3ES avalia externamente a qualidade dos cursos e nesta sequência a própria IES no seu todo através dos seus SIGQ. Internamente as IES também são auditadas, permitindo em primeira instância aferir a qualidade dos seus ciclos de estudos e fazer recomendações, proporcionando uma gestão mais eficaz e eficiente, ajudando no apoio à governação destas entidades. Sobre a GR e o CI, estes são elementos essenciais na governação das IES (Marques e Morais, 2022). Por sua vez, a insuficiência de procedimentos de CI leva ao incumprimento dos requisitos estabelecidos pelas entidades públicas (Onescu, 2018).

O modelo proposto para este projeto teve por base o SIGQ do IPC, nomeadamente os seus sete macroprocessos, efetuando a ligação com a GR e SCI, dando origem a um modelo integrado conforme figura 3.5. Igualmente está estruturado conforme as estruturas dos modelos ERM 2017 e ICIF 2013 do COSO.

Figura 3.5 – Esquematização do modelo GR e SCI Integrado no IPC



Fonte: elaboração própria

A ligação realizada dos referenciais da A3ES ao SIGQ, GR e SCI do IPC é demonstrado no quadro 3.3.

Quadro 3.3 – Ligação do SIGQ do IPC aos referenciais da A3ES, GR e SCI

A3ES Referenciais	IPC		
	SIGQ Macroprocessos	Plano de GR (áreas)	SCI
Referencial 1 - *Adoção de política para a garantia da qualidade e prossecução de objetivos de qualidade.*	**MP01** - Governação	- Sem informação	- Sem informação
Referencial 2 – *Conceção e aprovação da oferta formativa*; **Referencial 3** – *Ensino, aprendizagem e avaliação centrados no estudante;* **Referencial 4** – *Admissão de estudantes, progressão, reconhecimento e certificação*; **Referencial 5** – *Monitorização contínua e revisão periódica dos cursos.*	**MP02** – Ensino/Aprendizagem	- Académica; - Benefícios concedidos.	- Sem informação
Referencial 6 – *Investigação e desenvolvimento / Investigação orientada e desenvolvimento profissional de alto nível*	**MP04** - Investigação	- Património, infraestruturas e equipamentos	- Sem informação
Referencial 7 – *Colaboração interinstitucional e com a comunidade*	**MP05** – Relação com a comunidade	- Património, infraestruturas e equipamentos; - Aquisição de bens e serviços	- Artigos 9º; 10º e 12º da norma de CI do IPC
Referencial 8 – *Internacionalização*	**MP03** - Internacionalização	- Sem informação	- Sem informação
Referencial 9 – *Recursos humanos*	**MP06** – Recursos humanos	- Recursos humanos	- Artigo 11º da norma de CI do IPC
Referencial 10 – *Recursos materiais e serviços*	**MP07** – Recursos materiais e serviços	- Património, infraestruturas e equipamentos; - Aquisição de bens e serviços; - Área orçamental e financeira; - Proteção de dados e segurança da informação; - Benefícios concedidos.	- Artigos 7º; 8º; 9º; 10º; 12º; 16º e 17º da norma de CI do IPC
Referencial 11 – *Gestão da informação;* **Referencial 12** – *Informação pública;* **Referencial 13** – *Caracter cíclico da garantia externa da qualidade.*	**MP01** - Governação	- Informação e comunicação	- Artigo 19º da norma de CI do IPC

Fonte: elaboração própria

Em relação ao modelo da GR e o SCI Integrado no IPC, este está estruturado da seguinte forma: a integração da GR e o SCI no IPC, tem por base os documentos anteriormente referidos, adaptando-os aos modelos ERM do COSO - 2017 e ICIF do COSO - 2013. O

macroprocesso *Governação* está ligado com a componente do modelo ERM do COSO 2017 *Governança e Cultura* e cruza com a componente *Ambiente de controlo* referente ao modelo ICIF do COSO 2013, e assim sucessivamente conforme identificado nos *templates* que representam a vertente prática deste projeto. No que concerne à valorização do risco, deu-se continuidade ao estipulado no Plano de GR do IPC, nomeadamente a matriz três por três (3X3). Em relação à estrutura (*template*) proposta (ver apêndice 2), é composta por três partes, nomeadamente: objetivo; riscos e medidas de controlo.

Na primeira parte é elencada a designação da atividade/processo, de acordo com o estipulado no plano de GR do IPC, cruzando com os macroprocessos do SIGQ. Posteriormente deverá ser descrito o objetivo da atividade/processo, definir o indicador de cumprimento e responsável para a sua concretização. Igualmente deverá ser assinalada os componentes dos modelos e objetivos do ERM do COSO 2017 e ICIF do COSO 2013, respetivamente; nível de risco (cálculo efetuado no plano GR do IPC por uma matriz 3X3, com a seguinte valorização: 1 e 2 – reduzido; 3 e 4 – moderado; 5 e 6 – elevado). Na segunda parte são descritos os riscos associados ao processo; situações que poderão originar o risco; resposta ao risco inerente (aceitar/prevenir; prevenir/transferir; investigar/evitar/partilhar). No que concerne à terceira parte, o modelo está estruturado para o controlo, com medidas de controlo a implementar e medidas de controlo implementadas, onde deverá ser descrito o tipo de controlo (preventivo detetivos, corretivos, orientativos, compensatórios). Contempla um campo para efetuar o cruzamento com o SCI do IPC (identificando o artigo da norma de CI do IPC que contempla estes controlos). De igual o início, revisão, periodicidade de execução e indicador de eficácia também está previsto. Quando for realizada a passagem das medidas de controlo a implementar (estas associadas ao risco inerente), na seção seguinte (medidas de controlo implementadas) deverá ser colocada a classificação do risco residual (quantidade de risco que permanece ou que aparece após a inclusão dos controlos adicionais e/ou ajustes dos controlos existentes); resposta ao risco; tipo de controlo; cruzamento com o SCI do IPC (identificando o artigo da norma de CI do IPC que contempla estes controlos); início, revisão, periodicidade de execução e indicador de eficácia. O modelo a implementar encontra-se demonstrado na figura 3.6, que contempla o *template* proposto.

Figura 3.6 – Modelo proposto a implementar

PRIMEIRA PARTE DO MODELO

MP0X – "identificar macroprocesso"

Área: "descrever a área"
Atividade: "identificar atividade"

Objetivo

Descrição: [descrever objetivo]	**Indicador de cumprimento**	**Responsável**	[definir responsável]
	[definir objetivo]		

Componentes da gestão de riscos e controlo interno

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
- [descrever área]	☑	☑	☑	☑	☑	**Valorização do risco**	☑	☑	☑	☑	☑	☑	☑	☑

SEGUNDA E TERCEIRA PARTE DO MODELO

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- [descrever riscos]	- [descrever situações que poderão originar o risco]	[Aceitar/Prevenir/…]
Medidas de controlo a implementar	- [descrever medidas de controlo a implementar]	
Tipo de controlo		
[…]	SCI – [identificação do normativo associado a este controlo]	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[definir indicador]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo			
[…]	SCI – [identificação do normativo associado a este controlo]		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

No âmbito do *MP01 – Governação* e cruzamento com a GR do IPC, foi identificada a área de *Informação e comunicação*. Os riscos associados a esta área estão divididos por sete processos (os processos são considerados como atividades no *template* proposto), nomeadamente: *comunicação interna intra unidade orgânica*; *Comunicação interna inter unidades orgânica*; *Comunicação externa – Conteúdos*; *Comunicação externa - promoção da imagem institucional*; *Comunicação externa - utilização do nome «Instituto Politécnico de Coimbra» por terceiros em ações externas*; *Comunicação externa - utilização do nome «Instituto Politécnico de Coimbra» por terceiros em redes sociais*; *Comunicação externa - utilização da imagem corporativa*. Dos quais apenas a *Comunicação interna inter unidades orgânica* foi identificada com medidas de controlo a implementar através SCI do IPC, nomeadamente através do estipulado no artigo 19º, subcapítulo X da norma do controlo interno do IPC.

MP01 – Governação

Área: *Informação e comunicação*
Atividade: *Comunicação interna intra unidade orgânica*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**1- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Comunicação inadequada na Instituição (falha de articulação entre os diversos serviços).	- Ausência de procedimentos.	**[…]**

Medidas de controlo a implementar	- Implementar procedimentos de articulação inter serviços.

Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

A atividade *Comunicação interna inter unidades orgânicas* em termos do modelo ERM do COSO 2017 está associada à componente *Informação e reporte* cruzando com o modelo ICIF do COSO 2013 na componente *Informação e comunicação*. Por outro lado, a sua ligação da GR ao SCI é efetuada (em termos contabilísticos) através do definido entre o nº1 e nº 7 do artigo 19º da norma de CI do IPC, ao estipular no nº1 que:

> *Na comunicação entre as unidades orgânicas utilizar-se-á a plataforma de gestão documental em vigor".* […] *O circuito documental, bem como a forma de arquivo de todos os documentos de suporte e registo das operações contabilísticas, será o estipulado em regulamento próprio, de acordo com o processo de gestão documental em uso nas Instituições. Não obstante, todos os documentos devem passar por esse circuito, sendo que o seu original, com excepção dos documentos associados a projectos, deverá permanecer na unidade orgânica de origem*. […] *Os acessos e as permissões por utilizador à aplicação informática de gestão documental deverá ser sujeita a validação de serviço ou trabalhador designado para o efeito.* […] *Para as reafectações orçamentais, deverão ser criados processos onde serão inseridos os documentos que contêm as propostas de cada unidade orgânica aprovadas pelos respectivos órgãos de gestão. Depois de reunidas todas as propostas das unidades intervenientes, a proposta global é remetida ao Conselho de Gestão e, após a respectiva apreciação, é devolvida ao departamento de gestão financeira para inserção no software de gestão*.

Área: *Informação e comunicação*
Atividade: *Comunicação interna inter unidades orgânicas*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**2- reduzido**	☑						☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Comunicação inadequada entre UO;	- Ausência de procedimentos; - Ocorrência de falhas nos sistemas informáticos.	
Medidas de controlo a implementar	- Implementar procedimentos de articulação inter UO; - Implementar medidas que garantam a segurança e proteção da informação.	**[…]**
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo X – Arquivo, Artigo 19º (Procedimentos)	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Informação e comunicação*
Atividade: *Comunicação externa - Conteúdos*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**2- reduzido**	☑						☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Risco de incorreção e desatualização dos conteúdos da internet; **- Risco de erros e falhas nas publicações.**	- Falta de acompanhamento sistemático; - Falta de comunicação por parte dos serviços competentes.	
Medidas de controlo a implementar	- Acompanhar sistematicamente os conteúdos da internet; - Verificar periodicamente de conteúdos por elementos distintos dos que fazem o acompanhamento sistemático; - Definir circuitos de informação.	**[…]**

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Informação e comunicação*
Atividade: *Comunicação externa - promoção da imagem institucional*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**1- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Promoção inadequada da imagem da Instituição.	- Falta de comunicação por parte de entidades externas ao IPC | GCII	
Medidas de controlo a implementar	- Acompanhar e supervisionar todos os materiais/suportes/conteúdos; - Preparar atempada e exaustiva das diversas matérias a abordar, nomeadamente prestação de esclarecimento aos Media.	**[…]**
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Informação e comunicação*
Atividade: *Comunicação externa - utilização do nome «Instituto Politécnico de Coimbra» por terceiros em ações externas*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**1- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Utilização do nome do IPC indevidamente em ações externas (ex.: angariação de fundos, campanhas de solidariedade).	- Ausência de regras para a promoção da imagem da instituição.	**[…]**
Medidas de controlo a implementar	- Em caso de difamação, encaminhamento para o Departamento Jurídico; - Preparar e enviar *press-release*/comunicado institucional de forma a esclarecer qualquer mal-entendido, caso necessário.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Informação e comunicação*
Atividade: *Comunicação externa - utilização do nome «Instituto Politécnico de Coimbra» por terceiros em redes sociais*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**1- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Divulgação e utilização indevida do nome da instituição em redes sociais, por terceiros.	- Falta de comunicação por parte de entidades externas/particulares ao IPC | GCII	
Medidas de controlo a implementar	- Monitorizar acompanhar constante nas redes sociais; - Antecipar de possíveis reações em situações mais críticas (prestação de esclarecimentos, filtragem de comentários, etc.).	**[…]**
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Informação e comunicação*
Atividade: *Comunicação externa - utilização da imagem corporativa*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Informação e comunicação					☑	**1- reduzido**	☑						☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Utilização inadequada da imagem corporativa da instituição (logótipos, fotografias, documentos disponibilizados ao exterior, etc.).	- Falta de comunicação por parte de entidades internas e externas ao IPC.	**[…]**
Medidas de controlo a implementar	- Disponibilizar manual de normas gráficas no portal da instituição; - Disponibilizar Despacho orientador sobre a comunicação, com a definição de regras de utilização, no portal da instituição.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Posteriormente são demonstrados os riscos que foram identificados no plano de GR do IPC para a área académica e associados neste projeto ao *MP02 – Ensino/Aprendizagem*, integrando e ligando assim o SIGQ com a GR e SCI dos modelos ERM do COSO 2017 e ICIF do COSO 2013.

MP02 – Ensino/Aprendizagem

Em relação ao macroprocesso *MP02 – Ensino/aprendizagem*, foi associado às áreas *Académica* e *Benefícios concedidos*, cruzado com um total de nove processos. Oito processos que suportam a área académica, nomeadamente: *Processos transversais à gestão académica*; *Emissão de Certidões/Certificados/Diplomas/Cartas de Curso*; *Lançamento de classificações*; *Creditação de formação*; *Seriação dos candidatos a processos de concursos*; *Avaliação de conhecimentos*; *Matricula de inscrição*; *Atribuição de Estatutos Especiais* e um processo a área dos benefícios concedidos, mais precisamente: *Bolsas de estudo e outros benefícios sociais/ Bolsas de mérito/ Apoio à publicação científica*. Dos quais não foram identificadas medidas de controlo a implementar no SCI do IPC.

Área: *Académica*
Atividade: *Processos transversais à gestão académica*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Componentes da gestão de riscos e controlo interno

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑				**1- reduzido**	☑		☑	☑	☑	☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Violação do princípio da legalidade.	- Possibilidade de aplicação incorreta dos critérios legal e regularmente estabelecidos.	
Medidas de controlo a implementar	- Publicitar e disseminar internamente e através dos meios adequados informação útil aos serviços.	**[…]**

Tipo de controlo			
[preventivo]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**

Tipo de controlo			
[…]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Académica*
Atividade: *Emissão de Certidões/ Certificados/ Diplomas/ Cartas de Curso*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑				**2- reduzido**	☑			☑		☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- - Abuso de poder; **- Falsificação de documentos;** **- Corrupção passiva;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Obtenção de benefício económico ilícito para o próprio;** **- Favorecimento de terceiros.**	- Falsificação de documentos; - Ausência e incorreção dos pressupostos administrativos associados à emissão de certidões.	**[…]**
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo; - Emitir automaticamente documentos com recurso a meios informáticos e mediante critérios pré-definidos informaticamente validadas com minimização da intervenção humana; - Criar duas versões dos ficheiros relativos às Cartas de Curso (uma para controlo, assinada digitalmente, outra para envio ao fornecedor). A fidedignidade da documentação recebida do fornecedor será aferida a partir da comparação entre a versão de controlo assinada digitalmente e a documentação efetivamente recebida.	

Tipo de controlo	
[preventivo]	**SCI – por identificar na norma de controlo interno do IPC**

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	Classificação do risco residual	Resposta ao risco	[…]
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Académica*
Atividade: *Lançamento de classificações*

Objetivo

Descrição:	Indicador de cumprimento	Responsável	[…]
	[…]		

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	Nível do risco	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑	☑			**2- reduzido**	☑			☑	☑	☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Abuso de poder. **- Falsificação de documentos.** **- Corrupção passiva.** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo).** **- Obtenção de benefício económico ilícito para o próprio.** **- Favorecimento de terceiros.**	- Por acordo entre o estudante e o docente poderá ser efetuado o registo de uma classificação ou pedido de retificação da mesma que não corresponda ao valor obtido na avaliação; - Por acordo entre o estudante e o funcionário poderá ser efetuada a retificação incorreta de uma classificação.	**[…]**
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo; - Publicitar notas e creditações.	

Tipo de controlo [preventivo]	SCI – por identificar controlos a implementar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Académica*
Atividade: *Creditação de formação*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑	☑			**2- reduzido**	☑			☑	☑	☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Abuso de poder; **- Corrupção passiva;** **- Tráfico de Influência;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Discricionariedade;** **- Favorecimento de terceiros.**	- Por acordo entre o estudante e o funcionário docente/ não docente pode haver lugar à creditação de competências não homologadas ou superiores às homologadas pelos órgãos competentes.	**[…]**
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo - Aplicar critérios definidos de forma clara, com menor possibilidade de discricionariedade e com recurso a meios informáticos; - Fundamentar a atribuição da classificação e respetiva divulgação	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Académica*
Atividade: *Seriação dos candidatos a processos de concursos*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente Nível do risco	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑	☑			**1- reduzido**	☑			☑		☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Abuso de poder; **- Corrupção passiva;** **- Tráfico de Influência;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Discricionariedade;** **- Favorecimento de terceiros;** **- Violação de dados pessoais.** **- Discricionariedade;** **- Favorecimento de terceiros;** **- Violação de dados pessoais..**	- Por acordo entre o candidato e o funcionário poderá ser efetuada a candidatura fora de prazo; - Por acordo entre o candidato e o funcionário docente ou não docente poderão ser admitidos documentos ou candidatos em desconformidade com a lei e regulamentos em vigor; - Poderão ser alteradas decisões de júris na transcrição das decisões com o intuito de beneficiar determinado candidato.	**[…]**
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo; - Aplicar de critérios definidos de forma clara, com menor possibilidade de discricionariedade; - Restringir de acesso à plataforma informática; - Identificar automaticamente os responsáveis pelos acessos e registos; - Seriar e creditar via plataforma informática; - Fundamentar a atribuição da classificação e respetiva divulgação.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Académica*
Atividade: *Avaliação de conhecimentos*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Intervenção em impedimento; **- Favorecimento de terceiros;** **- Violação dos deveres gerais do trabalhador (imparcialidade e isenção).**	- Conhecimento prévio do teor da prova de avaliação de conhecimentos; - Intervenção em processo em que estejam presentes situações de impedimento.	
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo; - Fundamentar a atribuição da classificação e respetiva divulgação; - Publicitar os júris das provas públicas; - Dever de comunicação, por parte de um funcionário, de que um seu familiar frequenta o IPC, e assunção do compromisso de suscitar o impedimento.	**[…]**

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Académica*
Atividade: *Matrícula e renovação de inscrição*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder. **- Falsificação de documentos.** **- Corrupção passiva.** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo).** **- Obtenção de benefício económico ilícito para o próprio.** **- Favorecimento de terceiros.**	- Por acordo entre o estudante e o funcionário poderá ser efetuada a matrícula/renovação de inscrição de um estudante com matrícula e inscrição prescrita no ano letivo anterior; - Por acordo entre o funcionário e o candidato, pode ser aceite a matrícula/ renovação de inscrição sem apresentação de documentos obrigatórios ao ato.	**[…]**
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo; - Realizar matrícula/ renovação de inscrição com recurso a meios informáticos que incluam validações automáticas segundo critérios pré-definidos.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Académica*
Atividade: *Atribuição de Estatutos Especiais*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Processos**	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
		Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Académica	Atribuição de Estatutos Especiais		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Corrupção passiva;** **- Tráfico de Influência;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Discricionariedade;** **- Favorecimento de terceiros..**	- Por acordo entre o estudante e o funcionário pode haver lugar à atribuição de estatutos especiais não estando reunidas condições para tal.	**[…]**
Medidas de controlo a implementar	- Assegurar a segregação de funções na distribuição de tarefas associadas ao processo; - Recorrer a meios informáticos para inserção de documentos necessários à análise de candidaturas, sem a qual não seja possível a emissão de despacho de atribuição de estatuto especial; - Aplicar de forma clara de critérios pré-definidos nas decisões com apoio dos meios informáticos.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Benefícios concedidos*
Atividade: *Bolsas de estudo e outros benefícios sociais/ Bolsas de mérito/ Apoio à publicação científica*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Benefícios concedidos		☑		☑		**1- reduzido**	☑	☑		☑				☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder. Corrupção passiva para ato ilícito. **- Favorecimento de terceiros;** **- Tráfico de Influência;** **- Violação dos deveres gerais do trabalhador (zelo, imparcialidade e isenção);** **- Obtenção de benefício económico ilícito para terceiros.**	- Aplicação indevida da legislação e regulamentos de atribuição de bolsas de estudo e outros benefícios sociais/ bolsas de mérito; - Alteração das condições que levaram à atribuição do benefício; - Favorecimento de estudante na atribuição do benefício.	**[…]**
Medidas de controlo a implementar	- Aplicar critérios de atribuição de benefícios com recurso a meios informáticos parametrizados com os respetivos critérios de atribuição, que permitam identificar o trabalhador responsável pela respetiva aplicação; - Integrar sistemas de informação académica do IPC com os sistemas de informação dos SASIPC; - Verificar periodicamente e aleatoriamente processos por trabalhadores distintos dos responsáveis pela aplicação dos critérios de atribuição de benefícios/ por auditores contratados para o efeito.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

O processo *Bolsas de estudo e outros benefícios sociais/ Bolsas de mérito/ Apoio à publicação científica* poderá estar associado igualmente ao *MP04 – Investigação*, mais concretamente na relação que existe com o apoio à publicitação científica. Em relação ao *MP02 – Ensino/Aprendizagem*, foram identificados riscos para este macroprocesso e medidas de controlo a implementar. No entanto, no SCI do IPC nada consta sobre esta temática para estes dois macroprocessos. Posteriormente é demonstrada a estrutura proposta para o *MP03 – Internacionalização*.

MP03 – Internacionalização

No âmbito do *MP03 – Internacionalização*, não foram identificadas áreas que estivessem definidas no plano de GR do IPC. Consequentemente não foram identificados riscos que possam ser associados a estes macroprocessos. De igual modo também na norma de controlo interno do IPC nada está estipulado para este efeito. Por outro lado, este macroprocesso liga com o componente do modelo ERM do COSO 2017 *Estratégia e estabelecimento de objetivos*, que cruza com o componente *Ambiente de controlo* referente ao modelo ICIF do COSO 2013 e o tipo de objetivo é *operacional*. Posteriormente são demonstrados os riscos que foram identificados e consequentemente associados através deste trabalho ao *MP04 – Investigação*.

MP04 – Investigação

No âmbito do *MP04 – Investigação* e cruzamento com a GR do IPC, foi identificada a área de *Património, infraestruturas e equipamentos*. Os riscos associados a esta área estão identificados num processo, nomeadamente: *Propriedade Intelectual, Patentes e Transferência do Conhecimento*. Contudo não foi evidenciado no SCI medidas para controlar esta atividade.

Área: *Património, infraestruturas e equipamentos*
Atividade: *Propriedade Intelectual, Patentes e Transferência do Conhecimento*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑		☑	**1- reduzido**		☑			☑	☑	☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Favorecimento de terceiros; **- Intervenção em impedimento;** **- Violação de direitos de autor;** **- Peculato;** **- Participação económica em negócio;** **- Abuso de poder.**	- Licenciamento, registo e/ou adulteração por terceiros de marcas/ desenhos/ patentes resultantes de investigação ou trabalhos desenvolvidos com os recursos do IPC; - Utilização de informação privilegiada referente a processos de registo de propriedade intelectual para favorecimento de terceiros e possível inviabilização de registo; - Apropriação indevida de proveitos por parte de investigadores/inventores.	**[…]**
Medidas de controlo a implementar	- Elaborar Regulamento Interno de Procedimentos de Transferência de Tecnologia; - Aprovar e implementar Manual/Regulamento da Propriedade Intelectual do IPC; - Obrigar a assinatura de um acordo de confidencialidade entre os investigadores envolvidos e o IPC.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno

Início dd-mm-aaaa	Revisão dd-mm-aaaa	Periodicidade de execução […]	Indicador de eficácia […]

No *MP05 – Relação com a comunidade* foram associadas duas áreas: *património, infraestruturas e equipamentos* e *aquisição de bens e serviços*. Em relação à área do *património, infraestruturas e equipamentos*, esta está ligada ao processo (atividade) *exploração agropecuária*, a qual a nível de valorização do risco não contém elementos no plano de GR do IPC. Por sua vez, a área *aquisição de bens e serviços* liga-se ao processo (atividade) *Prestação de serviços*. No âmbito deste projeto verifica-se que estão definidos controlos no SCI do IPC que cruzam com a GR, nomeadamente de acordo dos artigos 10º e 12º da norma de CI do IPC.

MP05 – Relação com a comunidade

A atividade *Exploração agropecuária* em termos do modelo ERM do COSO 2017 está associada à componente *Estabelecimento de objetivos estratégicos* e *Desempenho* cruzando com o modelo ICIF do COSO 2013 na componente *Ambiente de controlo* e *Avaliação de riscos*. Por outro lado, a sua ligação entre a GR ao SCI é efetuada (em termos contabilísticos) através dos artigos 10º e 12º da norma de CI do IPC. O artigo 10º estipula que:

> *Cada local de armazenagem de existências terá de possuir um responsável nomeado para o efeito* […] *Trimestralmente deverá ser realizada a inventariação física às existências.* […]; *Deverão ser adoptados procedimentos que visem uma correcta gestão de stocks, no sentido de se evitarem desperdícios e permitirem uma utilização eficiente dos bens* […]; *As existências obsoletas e depreciadas, devem ser prontamente comunicadas ao sector de aprovisionamento e de contabilidade.*

Em continuidade para efeitos de CI, o artigo 12º define que:

> *deve remeter mensalmente ao serviço responsável pelo Inventário, através da gestão documental em vigor, cópia das facturas referentes à aquisição de bens duradouros que devam ser objecto de inventariação, acompanhada da respectiva notade lançamento na contabilidade.* […] *A alteração da localização de bens deverá ser dada a conhecer ao responsável pelo Inventário.* […].

Área: *Património, infraestruturas e equipamentos*
Atividade: *Exploração agropecuária*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos		☑	☑			**Sem elementos**	☑	☑	☑	☑	☑			

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Peculato; **- Abuso de Poder;** **- Corrupção passiva para ato ilícito;** **- Tráfico de influência;** **- Participação económica em negócio;** **- Violação do princípio da onerosidade.**	- Desvio de bens para uso privado (ferramentas, fertilizantes, adubos, sementes, animais, rações, produção agrícola e silvícola, combustíveis); - Utilização de terrenos para fins privados sem contrapartida; - Venda de produtos agrícolas, silvícolas ou pecuários a preços diferentes dos aprovados pelos órgãos de gestão; - Perdas em resultado de mau acondicionamento de produtos/ animais; ausência de maneios apropriados; ausência de colheitas atempadas; etc.	**[…]**
Medidas de controlo a implementar	- Inventariar os equipamentos, do material e do efetivo agrícola e pecuário; - Manter livro de registos do efetivo pecuário atualizado com recurso a software específico; - Colocar dispositivos identificadores dos animais (brincos, anilhas, chips, etc.); - Definir programas de maneio animal e de manutenção de espaços agrícolas e florestais; - Registar existências e de gestão de stocks com apoio de software específico; - Usar generalizadamente requisições de material integradas em software de gestão específico; - Definir politicas específicas de gestão e controlo de stocks e de armazém; - Registo sistemático das entradas e saídas de armazém; - Usar generalizadamente guias de remessa integrado com o software de gestão específico; - Faturar de forma adequada, designadamente quanto à especificação, quantidade e preço unitário do produto; - Utilizar generalizadamente talões de pesagem; - Segregar funções entre a produção, o armazenamento, a faturação e cobrança; - Publicitar os preços no site da instituição e nos locais de venda; - Publicitar avisos relativos à apresentação de propostas para arrendamento ou cedência de espaços com especificação dos critérios de estabelecimento de renda/ prestação e dos critérios para admissão e seleção dos candidatos; - Aprovar manual de procedimentos para a cedência de bens móveis e imóveis; - Aprovar manual de procedimentos para a exploração agropecuária.	
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo V – Existências (artigo 10º e subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)	

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno		

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade "Prestação de serviços" da área "Aquisição de bens e serviços", em termos do modelo ERM do COSO 2017 está associada à componente "Estabelecimento de objetivos estratégicos" e "Desempenho" cruzando com o modelo ICIF do COSO 2013 na componente "Ambiente de controlo"; "Avaliação de riscos" e "Atividades de controlo". Por outro lado, a sua ligação da GR ao SCI é efetuada (em termos contabilísticos) através do definido nos artigos 9º e 10º da norma de CI do IPC.

Área: *Aquisição de bens e serviços*
Atividade: *Prestação de serviços*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Aquisição de bens e serviços		☑	☑			**4- moderado**	☑			☑	☑	☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Violação da LGTFP; **- Favorecimento de terceiros;** **- Abuso de poder;** **- Corrupção passiva para ato ilícito;** **- Intervenção em impedimento;** **- Tráfico de Influência.**	- Recurso à contratação da prestação de serviços para satisfazer necessidades permanentes.	**[…]**

Medidas de controlo a implementar	- Levantamento regular anual das necessidades de pessoal de carácter permanente; - Fundamentar detalhadamente a necessidade de recurso à prestação de serviços e do não enquadramento na contratação de pessoal.

Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo IV – Aquisições (Artigo 9º) e subcapítulo V – Existências (artigo 10º)		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Posteriormente são demonstrados os riscos que foram identificados e associados à estrutura proposta para o *MP06 – Recursos Humanos*, designadamente na área *recursos humanos*, estando divididos por onze processos: *Recrutamento por concurso (pessoal docente)*; *Recrutamento por concurso (Pessoal não docente e bolseiros)*; *Recrutamento de docentes convidados*; *Processamento de remunerações*; *Análise de justificações das faltas*; *Análise de requerimentos de equiparação a bolseiro*; *Comunicação externa - utilização da imagem corporativa*; *Acumulação de funções*; *Elaboração do mapa de férias*; *Seleção de candidatos a programas de mobilidade*; *Formação Profissional ministrada pela instituição*. A área *recursos humanos* e os onze processos foram identificados com medidas de controlo a implementar, cruzando com o SCI do IPC, nomeadamente através do estipulado nos artigos 6º e 11º, da norma do controlo interno do IPC.

MP06 – Recursos Humanos

A atividade *Recrutamento por concurso (pessoal docente)* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, sobre a sua ligação da GR ao SCI, não constam controlos no SCI do IPC. No entanto, no plano GR foram definidas medidas de controlo a implementar.

Área: *Recursos humanos*
Atividade: *Recrutamento por concurso (pessoal docente)*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**1- reduzido**	☑					☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Corrupção passiva para ato ilícito;** **- Favorecimento de terceiros;** **- Intervenção em impedimento;** **- Tráfico de Influência.**	- Favorecimento/ Desfavorecimento de candidato; - Intervenção em processo em situação de impedido.	**[…]**
Medidas de controlo a implementar	- Recorrer preferencialmente a membros dos júris externos; - Aprovação de Manual de Procedimentos relativo à tramitação dos processos de recrutamento por concurso; - Densificar os critérios de seleção e respetiva publicitação; - Verificar periodicamente e aleatória de processos por pessoal não envolvido na tramitação do procedimento.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade *Recrutamento por concurso (pessoal não docente e bolseiros)* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento*

de objetivos cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, em relação à sua ligação da GR ao SCI, não constam controlos no SCI do IPC. No entanto, no plano GR foram definidas medidas de controlo a implementar.

Área: *Recursos humanos*
Atividade: *Recrutamento por concurso (Pessoal não docente e bolseiros)*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**2- reduzido**	☑					☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Corrupção passiva para ato ilícito;** **- Favorecimento de terceiros;** **- Intervenção em impedimento;** **- Tráfico de Influência.**	- Favorecimento/ Desfavorecimento de candidato; - Intervenção em processo em situação de impedido.	**[…]**
Medidas de controlo a implementar	- Recorrer preferencialmente a membros dos júris externos; - Nomear júris diferenciados para cada concurso; - Aprovação de Manual de Procedimentos relativo à tramitação dos processos de recrutamento por concurso; - Densificar os critérios de seleção e respetiva publicitação; - Verificar periódica e aleatória de processos por pessoal não envolvido na tramitação do procedimento.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade *Recrutamento de docentes convidados* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, em relação à sua ligação da GR ao SCI, não constam controlos no SCI do IPC. Contudo, no plano GR foram definidas medidas de controlo a implementar.

Área: *Recursos humanos*
Atividade: *Recrutamento de docentes convidados*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos						**4- moderado**								

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Intervenção em impedimento;** **- Tráfico de Influência.**	- Favorecimento/ Desfavorecimento de candidato; - Intervenção em processo em situação de impedido.	**[…]**
Medidas de controlo a implementar	- Existir Regulamento de Docentes Convidados com normas claras dos procedimentos a seguir; - Constituir uma base de recrutamento do IPC nos termos do art.º 8º-A do ECPDESP e publicitação da mesma, recorrendo para o efeito a uma solução desmaterializada; - Densificar os critérios de seleção e respetiva publicitação; - Verificar periodicamente e aleatoriamente processos por pessoal não envolvido na tramitação do procedimento; - Aprovar o Manual de Procedimentos relativo à tramitação dos processos de recrutamento de docentes convidados.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

A atividade *Processamento de remunerações* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, a sua ligação da GR ao SCI é efetuada de acordo com o estipulado nos artigos 6º e 11º da norma de CI do IPC.

Área: *Recursos humanos*
Atividade: *Processamento de remunerações*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Corrupção ativa para ato ilícito; **- Peculato;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Obtenção de benefício económico ilícito para terceiros.**	- Pagamentos indevidos a troco, ou não, de benefícios pessoais ou de terceiros - Utilização abusiva do recurso a horas extraordinárias.	**[…]**

Medidas de controlo a implementar	- Distribuir o processo de processamento de remunerações por diversos intervenientes e por fases de validação intermédia com recurso a meios informáticos; - Controlar a assiduidade através de sistemas biométricos com integração automática no software de processamento de remunerações; - Parametrizar o software de processamento de forma a minimizar a realização de cálculos de forma manual; - Segregar funções ou Rotatividade de funções/tarefas; - Conferir sistematicamente a folha de processamento de remunerações; - Aprovar Manual de Procedimentos relativo ao processamento de remunerações; - Formar regularmente pessoal envolvido no processamento de remunerações; - Verificar periodicamente e aleatoriamente processos de processamento por pessoal não envolvido na tramitação do procedimento.
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo I – Procedimentos Gerais, Artigo 6º; subcapítulo VI – Recursos Humanos, Artigo 11º.

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade *Análise de justificação das faltas* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, sobre a sua ligação da GR ao SCI é efetuada de acordo com o estipulado no artigo 11º da norma de CI do IPC.

Área: *Recursos humanos*
Atividade: *Análise de justificações das faltas*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Concussão; **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Obtenção de benefício económico ilícito para terceiros;** **- Corrupção.**	- Considerar indevidamente uma falta como justificada; - Não considerar de forma adequada os tempos efetivos de trabalho.	
Medidas de controlo a implementar	- Controlar a assiduidade através de sistemas biométricos com integração automática no software de processamento de remunerações; - Distribuir o processo de verificação da assiduidade por diversos intervenientes e por fases de validação intermédia com recurso a meios informáticos; - Parametrizar o software de processamento de forma a minimizar a introdução de registos de forma manual; - Identificar os responsáveis pelas validações intermédias no software de processamento de remunerações de forma automática; - Segregar funções ou Rotatividade de funções/tarefas; - Verificar periodicamente e aleatoriamente processos de assiduidade por pessoal não envolvido na tramitação do procedimento; - Aprovar Manual de Procedimentos relativo ao controlo e verificação da assiduidade.	**[…]**
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VI – Recursos Humanos, Artigo 11º (Procedimentos)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

A atividade *Análise de requerimento de licenças sem vencimento* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, em relação à sua ligação da GR ao SCI, esta efetuada apenas na parte da segregação de funções, mais precisamente com o estipulado nos artigos 6º da norma de CI do IPC.

Área: *Recursos humanos*
Atividade: *Análise de requerimentos de licenças sem vencimento*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Concussão; **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Obtenção de benefício económico ilícito para terceiros;** **- Corrupção.**	- Considerar indevidamente que se encontram cumpridos os requisitos.	**[…]**
Medidas de controlo a implementar	- Validar com recurso a meios informáticos; - Segregar funções ou Rotatividade de funções/tarefas; - Verificar periodicamente e aleatoriamente processos por pessoal não envolvido na tramitação do procedimento; - Publicitar das decisões; - Aprovar de Manual de Procedimentos relativo aos requerimentos de licenças sem vencimentos.	

Tipo de controlo	
[preventivo]	SCI – norma de controlo interno do IPC, subcapítulo I – Procedimentos Gerais, Artigo 6º (apenas a parte da segregação de funções).

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade *Análise de requerimentos de equiparação a bolseiro* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, sobre a sua ligação da GR ao SCI, não constam controlos no SCI do IPC. No entanto, no plano GR foram definidas medidas de controlo a implementar.

Área: *Recursos humanos*
Atividade: *Análise de requerimentos de equiparação a bolseiro*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**						**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte			Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑					**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Concussão; **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Obtenção de benefício económico ilícito para terceiros;** **- Corrupção.**	- Considerar indevidamente que se encontram cumpridos os requisitos; - Ausência de implementação de medidas na sequência de incumprimento dos deveres do bolseiro; - Acumulação da equiparação a bolseiro com outros benefícios não permitidos por lei; - Não verificação dos pressupostos que conduziram à concessão da equiparação; - Acumulação de funções públicas ou privadas em situação de impedimento; - Ausência de implementação de medidas na sequência de incumprimento dos deveres do equiparado a bolseiro.	**[…]**
Medidas de controlo a implementar	- Validar com recurso a meios informáticos - Segregar funções ou rotatividade de funções/tarefas - Verificar periodicamente e aleatoriamente processos por pessoal não envolvido na tramitação do procedimento;	

Tipo de controlo			
[preventivo]	SCI – por identificar na norma de controlo interno do IPC		
Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

A atividade *Acumulação de funções* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*, sendo definidas medidas no plano de GR a implementar. Contudo, nada consta na norma de CI do IPC para o seu cruzamento.

Área: *Recursos humanos*
Atividade: *Acumulação de funções*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**4- moderado**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Exercício de funções em incompatibilidade; **- Obtenção de benefício económico ilícito para terceiros;** **- Comprometimento do dever de imparcialidade;** **- Recebimento indevido de vantagem;** **- Concussão;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Corrupção.**	- Considerar indevidamente que se encontram cumpridos os requisitos; - Considerar indevidamente que se encontram cumpridos os requisitos; - Incompatibilidades; - Violação do regime de exclusividade; - Acumulação de funções sem prévia autorização.	**[…]**

Medidas de controlo a implementar	- Validar com recurso a meios informáticos; - Segregar funções ou Rotatividade de funções/tarefas; - Verificar periódica e aleatória de processos por pessoal não envolvido na tramitação do procedimento; - Condicionar a decisão à entrega de declaração de compromisso de honra por parte do interessado; - Publicitar as decisões; - Solicitar documento que faça prova dos rendimentos auferidos no ano civil anterior relativos à categoria A (trabalho dependente) e B (empresariais e profissionais); - Assinar declaração de compromisso de respeito pelo regime de incompatibilidades, impedimentos e escusa; - Amplificar a divulgação do regime de acumulações; - Aprovar de Manual de Procedimentos relativo aos requerimentos e exercício de acumulação de funções.
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade *Elaboração do mapa de férias* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. Por outro lado, a sua ligação da GR ao SCI é efetuada de acordo com o estipulado no artigo 11º da norma de CI do IPC.

Área: *Recursos humanos*
Atividade: *Elaboração do mapa de férias*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo); **- Corrupção;** **- Favorecimento de terceiros.**	- Atribuição de dias de férias superiores aos que o trabalhador tem direito; - Favorecimento na escolha dos dias de férias.	
Medidas de controlo a implementar	- Emitir mapa de forma automática a partir de software de gestão de recursos humanos; - Validar com recurso a meios informáticos; - Identificar responsáveis pelas validações intermédias no software de gestão de recursos humanos de forma automática; - Rodar funções; - Publicitar do mapa de férias; - Verificar periodicamente e aleatoriamente processos por pessoal não envolvido na tramitação do procedimento; - Aprovar Manual de Procedimentos relativo à elaboração e validação do mapa de férias.	**[…]**

Tipo de controlo			
[preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VI – Recursos Humanos, Artigo 11º (Procedimentos)		
Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**

Tipo de controlo			
[…]	SCI – por identificar na norma de controlo interno do IPC		
Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

A atividade *Seleção de candidatos a programas de mobilidade* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo*. No que concerne à sua ligação da GR ao SCI nada consta na norma de CI do IPC. No entanto, foram definidas medidas de controlo a implementar no plano de GR do IPC.

Área: *Recursos humanos*
Atividade: *Seleção de candidatos a programas de mobilidade*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente / Nível do risco	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- - Abuso de poder; **- Corrupção;** **- Tráfico de Influência;** **- Favorecimento de terceiros;** **- Intervenção em impedimento.**	- Favorecimento de candidatos; - Intervenção em processo em situação de impedido.	
Medidas de controlo a implementar	- Subscrever uma Declaração de Compromisso relativa a incompatibilidades, impedimentos ou escusa pelos trabalhadores do IPC; - Existir Regulamento relativo à admissão e seleção de candidatos a programas de mobilidade com normas claras dos procedimentos a seguir; - Densificar os critérios de seleção e respetiva publicitação; - Publicitar as decisões relativas à admissão e seleção de candidatos; - Aprovar de Manual de Procedimentos relativo à tramitação dos processos de admissão e seleção de candidatos a programas de mobilidade; - Verificar periódica e aleatória de processos por pessoal não envolvido na tramitação do procedimento.	**[…]**
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

A atividade *Formação Profissional ministrada pela instituição* em termos do modelo ERM do COSO 2017 está associada à componente *Estratégia e estabelecimento de objetivos* cruzando com o modelo ICIF do COSO 2013 na componente *Atividades de controlo* e objetivos *operacionais*. Em relação à sua ligação da GR ao SCI nada consta na norma de CI do IPC. No entanto, foram definidas medidas de controlo a implementar no plano de GR do IPC.

Área: *Recursos humanos*
Atividade: *Formação Profissional ministrada pela instituição*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Processos**	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
		Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Recursos humanos	Formação Profissional ministrada pela instituição		☑				**1- reduzido**	☑			☑				

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Falsificação de documentos;** **- Corrupção passiva;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Obtenção de benefício económico ilícito para o próprio;** **- Favorecimento de terceiros.**	- Falsificação de documentos; - Cobrança indevida de inscrições; - Com ou sem acordo entre o formando e o funcionário pode haver lugar a emissão de certificados de presença sem a frequência da ação de formação; - Por acordo entre o formando e o funcionário pode haver lugar a emissão de documentos quando existam valores em débito, ou haver lugar a regularização fictícia de débitos; - Frequência de ação de formação sem pagamento da respetiva inscrição.	**[…]**
Medidas de controlo a implementar	- Inscrever através de formulário eletrónico, condicionada ao pagamento da mesma sempre que aplicável; - Publicitar valores de inscrição; - Emitir certificado com recurso a meios informáticos e condicionado ao registo de presenças; - Identificar automaticamente com recurso a meios informáticos dos funcionários responsáveis pela emissão dos certificados; - Aprovar Manual de Procedimentos relativo à tramitação dos processos de inscrição, frequência e certificação de presença e ações de formação; - Verificar periódica e aleatória de processos por pessoal não envolvido na tramitação do procedimento.	
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VI – Recursos Humanos, Artigo 11º (Procedimentos)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

No âmbito do *MP06 – Recursos humanos*, foram identificados riscos para este macroprocesso e medidas para a sua mitigação, assim como estão definidos controlos, de acordo com o estipulado nos artigos 6º e 11º da norma de controlo interno do IPC. Posteriormente são demonstrados os riscos que foram identificados e associados à estrutura proposta para o *MP07 – Recursos Materiais e Serviços*. Os riscos associados a este macroprocesso foram divididos por cinco áreas, nomeadamente: *património, infraestruturas e equipamentos*; *aquisição de bens e serviços*; *área orçamental e financeira*; *Proteção de dados e de segurança da informação* e *apoios concedidos*. Estão definidas, para além das identificadas no plano de GR do IPC e demonstrados nos *templates* associados ao MP07, medidas de controlo através dos artigos 7º, 8º, 9º, 10º, 12º, 16º e 17º da norma do controlo interno do IPC.

MP07 – Recursos materiais e serviços

Área: *Património, infraestruturas e equipamentos*
Atividade: *Processos transversais à gestão do património, infraestruturas e equipamentos*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑		☑	**1- reduzido**		☑	☑		☑	☑	☑	

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Violação do princípio da legalidade	- Possibilidade de aplicação incorreta dos critérios legal e regularmente estabelecidos.	
Medidas de controlo a implementar	- Publicitar e disseminar internamente e através dos meios adequados informação útil aos serviços.	**[…]**
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)	

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Inventariação de bens móveis e salvaguarda de ativos*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente / Nível do risco	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑		☑	**4- moderado**		☑	☑		☑	☑	☑	

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Violação do CIBE; **- Violação das normas previstas no SNC-AP quanto ao Cadastro dos Ativos Fixos Tangíveis e Propriedades de Investimento;** **- Peculato;** **- Peculato de uso;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Abuso de poder.**	- Ausência de inventariação completa e integral segundo as normas previstas no CIBE e no SNC-AP; - Ausência de etiquetagem e de identificação da localização dos bens; - Apropriação de bens públicos para fins privados; - Transferência de bens sem autorização; - Cedência de bens sem competência para o efeito; - Utilização indevida de equipamentos e de equipamentos e de materiais; - Alienação de bens com valor histórico.	
Medidas de controlo a implementar	- Registar sistematicamente bens cadastráveis com recurso a software integrado com a contabilidade; - Reconciliar regularidade não superior a 1 ano dos registos contabilísticos com os registos de inventário; - Segregar funções entre quem efetua o registo de inventário, quem efetua o registo contabilístico, quem efetua a etiquetagem dos bens e quem efetua as verificações; - Controlar acessos aos bens de maior valor, ou cuja utilização exija normas de segurança reforçada dada a sua natureza e impacto sobre a organização (ex.: servidores, veículos, materiais de laboratório, obras bibliográficas, obras de interesse cultural etc.); - Generalizar o uso de requisições internas e de guias de entrega com recurso a meios informáticos que permitam a rápida localização do bem e a identificação do requisitante; - Realizar verificações físicas regulares dos bens; - Realizar verificações regulares ao Cadastro dos Ativos Fixos Tangíveis e Propriedades de Investimento.	**[…]**
Tipo de controlo […]	SCI – norma de controlo interno do IPC, subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)	

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC		

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Bens Imóveis*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente Nível do risco	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑		☑	**4- moderado**		☑	☑		☑	☑	☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Violação do CIBE; **- Violação das normas previstas no SNC-AP quanto ao Cadastro dos Ativos Fixos Tangíveis e Propriedades de Investimento;** **- Peculato;** **- Peculato de uso;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **-- Desperdício de recursos;** **- Subutilização da capacidade instalada;** **- Segurança de pessoas, bens e instalações.**	- Ausência de inventariação completa e integral segundo as normas previstas no CIBE e no SNC-AP - Valorização incompleta ou incorreta dos bens imóveis - Apropriação de bens públicos para fins privados - Existência de bens imóveis por registar na conservatória do registo predial - Cedência de bens sem competência para o efeito - Ausência de normas e procedimentos internos relativos ao cadastro, utilização, segurança, manutenção e preservação de imóveis - Alienação de bens com valor histórico.	**[…]**
Medidas de controlo a implementar	- Aprovar regulamento com normas e procedimentos relativos ao cadastro, utilização, segurança, manutenção e cedência de imóveis; - Efetuar um levantamento da situação do património; - Avaliar a utilização dos edifícios; - Promover a avaliação e registo na conservatória dos imóveis por avaliar/ registar. - Centralizar o registo da informação relativa a imóveis em plataforma única que permita: • integrar informação com o software de contabilidade e com o Cadastro de Ativos Fixos e Propriedades de Investimento; • gerir os prédios rústicos e urbanos (características, estado de conservação, manutenção, segurança, planos de intervenção, execução dos planos de intervenção, etc.); • controlar e acompanhar a utilização dos prédios rústicos e urbanos; • controlar os imóveis cedidos; • celebrar prestação de informação aos órgãos de gestão e ao exterior. - Segregar funções entre quem promove o registo predial, quem efetua o registo de inventário, quem efetua o registo contabilístico e quem efetua as verificações; - Realizar verificações regulares ao Cadastro dos Ativos Fixos Tangíveis e Propriedades de Investimento.	
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo **[…]**	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Doações à instituição*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos					☑	**1- reduzido**			☑				☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Violação das normas previstas no SNC-AP quanto ao Cadastro dos Ativos Fixos Tangíveis e Propriedades de Investimento;** **- Violação do CIBE;** **- Peculato;** **- Peculato de uso;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo).**	- Ofertas à instituição sem a existência de um processo formal de aceitação e com a ausência de cadastro dos bens doados, criando as condições para a apropriação de bens públicos ou para a utilização de bens públicos para fins privados; - Utilização da doação como aliciamento da instituição para aquisições futuras.	**[…]**
Medidas de controlo a implementar	- Registar sistematicamente bens doados no software de cadastro de ativos fixos tangíveis e propriedades de investimento; - Realizar verificações físicas regulares dos bens, com a periodicidade mínima do ano civil; - Realizar verificações regulares ao cumprimento dos procedimentos de aceitação e cadastro dos bens doados, com a periodicidade mínima do ano civil; - Realizar verificações regulares ao Cadastro dos Ativos Fixos Tangíveis e Propriedades de Investimento, com a periodicidade mínima do ano civil.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Abates, alienações e transferência/ cedência de bens*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑		☑	**2- reduzido**		☑	☑			☑	☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Violação das normas previstas no SNC-AP quanto ao Cadastro dos Ativos Fixos Tangíveis, bens imóveis e Propriedades de Investimento; **- Violação do CIBE;** **- Peculato;** **- Peculato de uso;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Apropriação indevida de bens públicos;** **- Desaparecimento do bem;** **- Desatualização das fichas dos bens;** **- Abuso de poder.**	- Abates e alienações sem autorização do órgão competente; - Utilização indevida de bem abatido/ alienado documentalmente sem confirmação do abate/ alienação físico do bem; - Insuficiente descrição do cadastro do bem; - Transferência de bens sem comunicação ou autorização.	**[…]**

Medidas de controlo a implementar	- Elaborar listagem anual de bens abatidos/ transferidos/ cedidos devidamente assinada pelo órgão com competência para autorizar; - Exigir fundamentação dos autos de abate/ cedência/ transferência e exigência de autorização de abate/ cedência/ transferência pelo órgão competente, conforme com os requisitos legais, antes da respetiva comunicação ao serviço responsável pelo Património e ao serviço responsável pelo seu registo no software integrado de gestão de ativos fixos; - Isolar os bens a abater em local de acesso restrito e controlado; - Realizar conferências físicas periódicas para verificar se os bens abatidos ainda se encontram no local; se a autorização de abate/ cedência/ transferência foi proferida pelo órgão com competências para o efeito; se os abates se encontram devidamente fundamentados e se os demais procedimentos foram respeitados.

Tipo de controlo	
[preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: "Património, infraestruturas e equipamentos"
Atividade: "Cedência de espaços"

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑			**2- reduzido**	☑				☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Violação do princípio da onerosidade; - Peculato; - Peculato de uso;	- Cedência de espaços sem contrapartida ou com contrapartida insuficiente.	**[…]**

- Abuso de poder; - Participação económica em negócio; - Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo).	
Medidas de controlo a implementar	- Fazer depender a utilização externa de espaços de autorização do órgão com competência para o efeito (Conselho Geral, Conselho de Gestão ou Conselho Administrativo) e da emissão de auto de cedência; - Aprovar em órgão próprio das regras de utilização e cedência de espaços, zelando pelo princípio da onerosidade; - Realizar verificações regulares relativas à utilização dos espaços e às contrapartidas financeiras associadas à sua cedência.

Tipo de controlo	
[preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Arquivo e Bibliotecas*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos		☑			☑	**4- moderado**	☑		☑	☑			☑	

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Perda de obras; - Peculato; - Desperdício de recursos; - Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo); - Apropriação indevida de bens.	- Risco de degradação dos documentos não decorrente da ação humana; - Risco de degradação dos documentos decorrente da ação humana, nomeadamente: • Dano ou desperdício do património arquivístico ou com interesse histórico; • Extravio de obras bibliográficas; • Duplicação de acervo bibliográfico decorrente da ausência de gestão integrada; • Empréstimos não devolvidos.	
Medidas de controlo a implementar	- Relativamente aos riscos de degradação dos documentos não decorrente da ação humana: • manter regularmente as infraestruturas onde se encontra acondicionada a documentação, assegurando a sua estanquicidade face aos elementos atmosféricos e de origem animal; • realizar de rotinas de controlo de pragas, insetos ou roedores; • Promoção da limpeza regular dos depósitos, evitando a acumulação de poeiras; • controlar os níveis de humidade relativa e temperatura, tendo em vista a manutenção dos níveis adequados consoante o suporte da documentação (papel, fotografia, CD-ROM, etc.); • implementar os procedimentos de prevenção e proteção face a sinistros naturais (agravados ou não pela ação humana). - Relativamente aos riscos de degradação dos documentos decorrente da ação humana: • Realizar, com regularidade, ações de tratamento e avaliação de documentação acumulada; • Desenvolver e aplicar instrumentos de boa gestão documental, em ambiente analógico ou digital; • Respeitar o grau de conservação e manuseio da documentação, utilizando sistemas de acondicionamento adequados; • Promover o restauro e conservação preventiva dos documentos; • Gerir a utilização interna e externa das obras solicitadas para consulta.	**[…]**
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Viaturas de Serviço*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente / Nível do risco	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑	☑		**4- moderado**	☑		☑		☑	☑		☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Recebimento indevido de vantagem; **- Peculato;** **- Subutilização ou desperdício de recursos;** **- Acidente;** **- Apropriação indevida de bens.**	- Utilização indevida de viaturas; - Aquisição de combustíveis para uso próprio; - Deficiente manutenção das viaturas; - Ausência de Gestão Integrada de Frota.	**[…]**
Medidas de controlo a implementar	- Inventariar de forma completa e sistemática as viaturas existentes no IPC; - Efetuar o registo sistemático e com o apoio de meios informáticos, da agenda de utilização de viaturas; dos percursos percorridos e respetiva quilometragem, dos abastecimentos de combustíveis e das manutenções/ reparações efetuadas; - Segregar funções entre quem conduz as viaturas e quem gere a sua utilização; - Recorrer a soluções de pagamento de combustíveis associados a cartões frota que permitam o controlo sistemático das quantidades de combustíveis consumidas por viatura; - Verificar periodicamente e aleatoriamente processos por pessoal não envolvido na tramitação do procedimento.	
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VII - Imobilizado - Património, Infraestruturas e Equipamentos (Artigo 12º)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Património, infraestruturas e equipamentos*
Atividade: *Património histórico e cultural*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |componentes|					Classificação do risco inerente Nível do risco	Modelo ICIF do COSO - 2013 |tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos			☑		☑	**4- moderado**			☑					☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Perda de património; **- Peculato;** **- Desperdício de recursos;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Apropriação indevida de bens.**	- Risco de degradação do património não decorrente da ação humana; - Risco de degradação do património decorrente da ação humana, nomeadamente: • Dano ou desperdício do património; • Extravio.	**[…]**
Medidas de controlo a implementar	- Relativamente aos riscos de degradação não decorrentes da ação humana: • manter as infraestruturas, assegurando a sua estanquicidade face aos elementos atmosféricos e de origem animal; • realizar rotinas de controlo de pragas, insetos ou roedores; • promover limpeza regular dos depósitos, evitando a acumulação de poeiras; • controlar níveis de humidade relativa e temperatura, tendo em vista a manutenção dos níveis adequados; • implementar procedimentos de prevenção e proteção face a sinistros naturais (agravados ou não pela ação humana). - Relativamente aos riscos de degradação decorrentes da ação humana: • realizar, com regularidade, ações de tratamento e avaliação do património histórico e cultural; • respeitar o grau de conservação e manuseio do património histórico e cultural, utilizando sistemas de acondicionamento adequados; • promover o restauro e conservação preventiva; • gerir a utilização interna e externa do património histórico e cultural.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Em relação á área *Aquisição de bens e serviços*, no âmbito do MP07, foram associadas as seguintes atividades: *Planeamento da contratação e avaliação das necessidades*; *Procedimentos pré-contratuais; Verificação material da recepção e entrega de bens e serviços*; *Gestão e renovação dos contratos*; *Avaliação de fornecedores*; *Publicitação de procedimentos de aquisição*; *Execução Orçamental*; *Emissão de faturas e cobrança de receita*; *Registo de faturas de despesa e pagamentos*; *Fundo de Maneio*. Sobre o *Planeamento da contratação e avaliação das necessidades*, o SCI o IPC tem definido medidas de controlo a aplicar na instituição.

Área: *Aquisição de bens e serviços*
Atividade: *Planeamento da contratação e avaliação das necessidades*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Aquisição de bens e serviços			☑			**1- reduzido**		☑			☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Corrupção passiva; **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Violação do CCP;** **- Obtenção de benefício económico ilícito para o próprio;** **- Favorecimento de terceiros;** **- Fracionamento da despesa;** **- Tráfico de influência;** **- Alocação desnecessária de recursos aos procedimentos de aquisição;** **- Deficiente desempenho da missão da instituição;** **- Restituição de fundos comunitários associados ao financiamento de projetos.**	- Pedido de aquisição de bens para uso exclusivamente pessoal e/ou com vista a obter vantagem com a aquisição dos mesmos; - Deficiente planeamento das necessidades subjacentes e insuficiente previsão dos bens e serviços necessários à prossecução da missão da instituição; - Realização de trabalhos a mais sem prévia autorização do órgão competente/ sem abertura de novo procedimento.	**[…]**

Medidas de controlo a implementar	- Elaborar Manual de Procedimentos que preveja a tramitação a seguir no levantamento de necessidades, a respetiva fundamentação, a periodicidade da respetiva realização, revisão e acompanhamento e a segregação de funções entre a proposta de aquisição, a prévia verificação de contrato em vigor/ existência de bens em stock para a necessidade requerida e a aprovação do início do procedimento; - Criar uma ferramenta informática transversal a todo o IPC e integrada no software em uso de levantamento agregado de necessidades e do respetivo acompanhamento - Promover a segregação de funções entre os responsáveis pelos procedimentos pré- contratuais, o gestor do contrato e a fiscalização das empreitadas; - Recorrer a equipas multidisciplinares especializadas na conceção do caderno de encargos.
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo IV – Aquisições (Artigo 9º) e subcapítulo V – Existências (artigo 10º)

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Aquisição de bens e serviços*
Atividade: *Procedimentos pré-contratuais*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Aquisição de bens e serviços			☑			**2- reduzido**			☑		☑	☑	☑	

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Corrupção passiva; **- Violação do Código dos Contratos Públicos e do Regime de Administração Financeira do Estado** **- Participação económica em negócio;** **- Tráfico de Influência;** **- Violação dos deveres gerais do trabalhador (imparcialidade, isenção, prossecução do interesse público e zelo);** **- Aquisição de bens/ serviços que, pela economia, eficiência ou eficácia, comprometam o desempenho da missão da instituição;** **- Restituição de fundos comunitários associados ao financiamento de projetos.**	- Inexistência de mecanismos que possam identificar situações de conluio entre os adjudicatários e os funcionários/ Intervenção em processo em situação de impedimento; - Supressão de fases do procedimento necessárias à realização da despesa (ex. cabimentação e autorização prévias da despesa pelas entidades competentes; verificação de fundos disponíveis); - Fracionamento da despesa; - Inexistência de competência própria ou delegada para aprovação do procedimento; - Quebra do dever de sigilo com consequências sobre os resultados do procedimento (preço base, adjudicação, etc.); - Favorecimento de fornecedores com objetivo de obter vantagem; - Incorreta verificação dos documentos de habilitação (Apresentação de documentos falsos; apresentação de documentos fora de prazo; inadequada análise dos documentos).	
Medidas de controlo a implementar	- Assinar declaração tipo, com compromisso de suscitar impedimento, escusa e suspeição caso se verifique; - Promover, sempre que possível, da consulta a mais do que um fornecedor nas situações fora do âmbito do concurso público, fundamentando sempre a escolha dos mesmos; - Promover aa redução do número de procedimentos, através da agregação das aquisições inter e intra UO, assente no levantamento de necessidades e no recurso à contratação por lotes; - Promover a redução dos procedimentos por ajuste direto e consulta prévia; - Promover a avaliação de fornecedores e do recurso à mesma na fundamentação da escolha de fornecedores, quando aplicável; - Verificar aleatoriamente procedimentos por trabalhadores distintos dos que tiveram a responsabilidade pela tramitação pré-contratual; - Realizar preferencialmente consultas ao mercado via recolha de preços disponibilizados na Internet; - Promover a rotatividade dos trabalhadores no acompanhamento dos procedimentos pré-contratuais; - Formar os trabalhadores no âmbito da contratação pública e das fases da realização da despesa; - Verificar periodicamente e aleatoriamente do cumprimento da delegação de competências; - Elaborar manuais de procedimentos relativos à tramitação da contratação pública e à tramitação das várias fases da despesa.	**[…]**
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo IV – Aquisições (Artigo 9º) e subcapítulo V – Existências (artigo 10º)	

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Aquisição de bens e serviços*
Atividade: *Verificação material da receção e entrega de bens e serviços*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Aquisição de bens e serviços			☑	☑	☑	**2- reduzido**	☑	☑	☑		☑	☑	☑	☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Corrupção passiva;** **- Favorecimento de terceiros;** **- Conluio;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Peculato;** **- Obtenção de benefício económico ilícito para o próprio/ terceiros;** **- Tráfico de Influência;** **- Aquisição de bens/ serviços que, pela economia, eficiência ou eficácia, comprometam o desempenho da missão da instituição;** **- Desvio ou não verificação da quantidade e qualidade de bens.**	- Desvio de material para uso próprio ou de terceiros; - Controlo deficiente dos bens e serviços recebidos no que respeita à quantidade, qualidade e preço; - Não ativação das garantias bancárias/ penalizações previstas contratualmente em caso de deficiente fornecimento sistemático.	**[…]**
Medidas de controlo a implementar	- Manter registos de controlo de economato atualizados; - Aposição sistemática na fatura e nos registos informáticos de informação relativa à conformidade dos bens e serviços recebidos com a encomenda; - Elaborar notas de encomenda com a integral/completa especificação dos bens e serviços a adquirir (descrição, quantidade, preço de acordo com o contratualizado); - Segregar funções entre pessoal responsável pela encomenda e pessoal responsável pela receção e verificação dos bens existentes em stock; - Verificar periodicamente o fornecimento de serviços de acordo com as especificações contratualizadas e recurso a trabalhadores especializados para verificar o adequado fornecimento de bens e serviços sempre que a sua complexidade o justifique; - Distribuir internamente bens mediante preenchimento prévio, preferencialmente com recurso a formulário eletrónico, de requisição e aposição de informação de confirmação da sua receção no momento da entrega pelo requisitante;	

	- Monitorizar as garantias bancárias relativas a empreitadas e aquisição de bens e serviços e respetiva ativação, quando aplicável; - Prever penalizações no caderno de encargos em caso de incumprimento contratual; - Elaborar instruções de serviço relativas à verificação material da receção de bens e serviços.
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo IV – Aquisições (Artigo 9º) e subcapítulo V – Existências (artigo 10º)

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Aquisição de bens e serviços*
Atividade: *Gestão e renovação dos contratos*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Património, infraestruturas e equipamentos		☑	☑			**1- reduzido**	☑			☑	☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Corrupção passiva; **- Favorecimento de terceiros;** **- Violação do Código dos Contratos Públicos;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Participação económica em negócio;**	- Inexistência de alerta atempado para o termo dos contratos, quer o mesmo resulte de ação voluntária, quer o mesmo resulte de ação involuntária do trabalhador.	**[…]**

- Tráfico de Influência; **- Deficiente desempenho da missão da instituição.**	
Medidas de controlo a implementar	- Existir um software que apoie a verificação de contratos cujo términus ocorra no ano seguinte de forma efetuar planeamento e abertura de novos procedimentos; - Emitir alertas por software com a antecedência considerada adequada, para avaliação da renovação ou denúncia dos contratos e verificação, durante o último trimestre, dos contratos cujo términus ocorra durante o ano seguinte, de forma a efetuar planeamento atempado e providenciar abertura de novos procedimentos.

Área: *Aquisição de bens e serviços*
Atividade: *Avaliação de fornecedores*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Aquisição de bens e serviços		☑	☑			**2- reduzido**	☑	☑		☑	☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Corrupção passiva;** **- Tráfico de Influência;** **- Participação económica em negócio;** **- Favorecimento de terceiros;** **- Violação do CCP.**	- Ausência de avaliação sistemática de fornecedores; - Ausência de rotatividade dos trabalhadores responsáveis pela tramitação administrativa dos procedimentos; - Ausência de controlo sistemático e sucessivo por trabalhadores não envolvidos na tramitação contratual.	**[…]**
Medidas de controlo a implementar	- Promover a avaliação sistemática de fornecedores através de ferramenta informática apropriada e da exigência de fundamentação da escolha do fornecedor baseada, sempre que aplicável, nomeadamente na avaliação prévia de fornecedores; - Promover a rotatividade de fornecedores, quando aplicável; - Promover a rotatividade de trabalhadores responsáveis pela instrução de procedimentos; - Elaborar instruções de trabalho relativas à tramitação da contratação pública que abranjam estes processos; - Realizar testes de conformidade periódicos por trabalhadores não envolvidos na tramitação contratual.	
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo IV – Aquisições (Artigo 9º) e subcapítulo V – Existências (artigo 10º)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	[…]

Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Aquisição de bens e serviços*
Atividade: *Publicitação de procedimentos de aquisição*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	[…]

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Aquisição de bens e serviços			☑		☑	**4- moderado**			☑		☑	☑	☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Ineficácia dos contratos; **- Pagamentos ilegais, nos termos do CCP;** **- Responsabilidade financeira decorrente da realização de pagamentos ilegais.**	- Não publicitação dos procedimentos de aquisição; - Pagamentos sem a publicitação do procedimento na Base Gov.	
Medidas de controlo a implementar	- Garantir a transparência dos procedimentos de contratação pública através do cumprimento de publicitação no portal da contratação pública.	**[…]**

Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo IV – Aquisições (Artigo 9º) e subcapítulo V – Existências (artigo 10º)		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

A área *Orçamental e financeira* tem associadas quatro atividades, nomeadamente: *execução orçamental*; *emissão de faturas e cobrança de receita*; *registo de faturas de despesa e pagamentos*; *fundo de maneio*.

Área: *Orçamental e financeira*
Atividade: *Execução Orçamental*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Orçamental e financeira			☑			**4- moderado**			☑		☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Transversais às diversas áreas **o Incumprimento da Lei de Enquadramento Orçamental;** **o Incumprimento da Lei de Orçamento;** **o Violação do Regime de Administração Financeira do Estado;** **o Deficiente prestação de contas;** **o Responsabilidade financeira reintegratória;** **o Responsabilidade financeira sancionatória;** **o Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **o Dificuldade em satisfazer obrigações perante terceiros;** **o Deficiente desempenho da missão da instituição.**	- Deficiente processo de planeamento; - Incumprimento das fases de realização da despesa (cabimento, compromisso após verificação de fundos disponíveis, obrigação, pagamento); - Incumprimento das fases de realização da receita; - Registo insuficiente de compromissos; - Ausência de segregação de funções; - Existência de atrasos na tramitação administrativa e financeira; - Deliberações relativas à despesa e receita por órgãos sem competência própria ou delegada para o efeito; - Registos incompletos ou incorretos; - Ausência de acompanhamento regular e sistemático da execução orçamental com disponibilização de relatórios periódicos de suporte à tomada de decisão.	**[…]**

Medidas de controlo a implementar	- Processar um planeamento financeiro rigoroso, sistemático e participado; - Existir sistemas informáticos que garantam e apoiem o cumprimento dos requisitos inerentes a cada uma das fases da despesa (ex.: impossibilidade de registar cabimentos sem dotação disponível; impossibilidade de emitir compromissos sem a existência de cabimento prévio, autorização de despesa e informação relativa a fundos disponíveis; impossibilidade de registar faturas sem prévia emissão de nota de encomenda; impossibilidade de realizar pagamentos sem a respetiva autorização); - Existir sistemas informáticos que garantam e apoiem o cumprimento dos requisitos inerentes a cada fase da receita (ex.: impossibilidade de registo de cobrança sem prévio/simultâneo registo da liquidação); - Elaborar relatórios periódicos de acompanhamento da execução orçamental; - Verificar periodicamente e sistemática da tramitação administrativa e financeira da execução orçamental por trabalhadores/ entidades não intervenientes no processo devidamente habilitadas; - Verificar periodicamente da competência própria ou delegada associada às decisões por trabalhadores/ entidades não intervenientes no processo devidamente habilitadas; - Segregar funções entre quem executa, autoriza e regista e entre os diversos intervenientes de cada fase orçamental; - Promover de medidas visando a completa implementação do SNC-AP; - Manter de norma de controlo interno atualizada e verificação periódica da respetiva implementação; - Elaborar de manuais de procedimentos detalhados que complementem a norma de controlo interno; - Formação regular dos trabalhadores.
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo VIII – Contabilidade Orçamental, Patrimonial e Analítica (Artigo 16º e 17º)

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Orçamental e financeira*
Atividade: *Emissão de faturas e cobrança de receita*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Orçamental e financeira			☑			**2- reduzido**			☑		☑	☑		

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Abuso de poder; **- Corrupção passiva;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Peculato;** **- Obtenção de benefício económico ilícito para o próprio / terceiros;** **- Sanções tributárias;** **- Responsabilidade financeira sancionatória e reintegratória.**	- Não emissão ou anulação indevida de recibos de forma a eliminar a cobrança de receita e beneficiar do desvio da mesma; - Emissão de faturas, faturas-recibo e cobrança de valores desconformes com as condições contratuais subjacentes (quantidade, qualidade e preço unitário estabelecidos); - Aplicação incorreta das taxas de IVA em vigor; - Emissão incorreta de faturas ou não emissão de faturas/ faturas-recibo; - Uso próprio dos valores em caixa na Tesouraria.	
Medidas de controlo a implementar	- Emitir faturas/ faturas-recibos com recurso a software certificado e na sequência de respetivamente, registos de liquidação e cobrança; - Fundamentar a anulação de faturas e comunicação ao superior hierárquico; - Segregar funções entre quem procede à emissão de faturas e à cobrança de receita; - Registar sistematicamente os valores faturados e cobrados; - Emitir automaticamente e diária de folhas de caixa com detalhe dos valores entrados, saídos e do saldo, a partir do software de contabilidade; - Conferir diariamente os valores em caixa com as folhas de caixa; - Conferir com periodicidade mensal da folha de caixa com os valores em caixa por funcionário distinto do responsável pelo manuseamento de valores; - Conciliar contas bancárias mensalmente; - Publicitar na página da instituição e em local bem visível os preços praticados; - Emitir faturas a partir de tabelas de artigos/serviços do software de contabilidade previamente parametrizadas por funcionário distinto do responsável pela emissão de faturas, com descritivo do artigo/serviço e preço unitário; - Verificar periodicamente a conformidade das faturas emitidas (preços unitários, descritivos, quantidades, preços totais, cliente e taxas de IVA) por trabalhadores exteriores ao serviço emitente; - Promover o recurso à cobrança através de multibanco, transferência bancária ou *e-banking*, de forma a minimizar o uso de numerário; - Recolher periodicamente informação de cliente (circularização de clientes); - Identificar automática dos responsáveis pelos registos; - Elaboração de manual de procedimentos relativo à liquidação e cobrança de receita.	**[…]**
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo II – Disponibilidades (Artigo 7º) e subcapítulo III – Terceiros (artigo 8º)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Em relação à atividade *Registo de faturas de despesa e pagamentos*, foram identificados sete riscos e verificada que a norma de CI do IPC prevê mecanismos para a sua mitigação, nomeadamente no artigo 7º, *subcapítulo II – Disponibilidades*.

Área: *Orçamental e financeira*
Atividade: *Registo de faturas de despesa e pagamentos*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Orçamental e financeira			☑			**2- reduzido**			☑		☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Abuso de poder; **- Corrupção passiva;** **- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo);** **- Peculato;** **- Obtenção de benefício económico ilícito para o próprio / terceiros;** **- Sanções tributárias;** **- Responsabilidade financeira sancionatória e reintegratória.**	- Processamento de faturas sem prévia conferência da conformidade dos bens recebidos/ serviços prestados com nota de encomenda; - Processamento de faturas desconformes com a legislação em vigor (código de IVA/ outra); - Registo de valores de despesa diferentes do documento de suporte; - Incorreta classificação contabilística da despesa; - Registo da fatura com contrapartida distinta do respetivo fornecedor; - Realização de pagamentos em numerário; - Realização de pagamentos através de cheque; - Realização de pagamentos sem prévia verificação e registo da fatura; - Realização de pagamentos sem prévia autorização do órgão competente; - Autorização de pagamentos sem prévio registo da fatura; - Utilização indevida de fundo de maneio.	**[…]**
Medidas de controlo a implementar	- Existir mecanismos de bloqueio informático do registo da fatura sem prévio registo de informação relativa à respetiva conformidade com a nota de encomenda e com os bens/ serviços recebidos; do registo de pedido de autorização de pagamento sem prévio registo da fatura; - Segregar funções entre quem emite a nota de encomenda; quem confere os bens/ serviços recebidos; quem regista; quem emite os pedidos de autorização de pagamento; quem autoriza os pagamentos; quem submete ficheiros para pagamento; quem paga e quem regista os pagamentos; - Reforçar medidas de controlo interno garantindo-se a verificação de que os pagamentos são efetuados exclusivamente com suporte numa ordem de pagamento devidamente autorizada, a qual pressupõe a assinatura de pelo menos dois representantes legais da instituição; - Minimizar o recurso a pagamentos em numerário ou cheque, privilegiando-se os pagamentos por ficheiro em sistema de *homebanking*; - Circularização periódica de fornecedores; - Identificação automática dos responsáveis pelos registos; - Conciliação bancária mensal realizada por trabalhadores distintos dos que efetuam ou registam movimentos financeiros; - Elaborar de manual de procedimentos relativo ao processamento de faturas e pagamentos; - Realizar auditorias periódicas por trabalhadores/ entidades externas ao DGF.	
Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo II – Disponibilidades (Artigo 7º)	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início dd-mm-aaaa	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Em relação à atividade "Fundo de Maneio", foram identificados quatro riscos e verificada que a norma de controlo interno do IPC prevê mecanismos para a sua mitigação, mais concretamente no artigo 7º, subcapítulo II – Disponibilidades.

Área: *Orçamental e financeira*
Atividade: *Fundo de Maneio*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Orçamental e financeira			☑			**2- reduzido**			☑		☑	☑		

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Violação dos deveres gerais do trabalhador (prossecução do interesse público e zelo); **- Peculato;** **- Obtenção de benefício económico ilícito para o próprio / terceiros;** **- Responsabilidade financeira sancionatória e reintegratória.**	- Utilização indevida do fundo de maneio para a realização de despesas; - Reconstituição do fundo de maneio sem apresentação de documentos de suporte da despesa; - Não liquidação periódica do fundo de maneio.	**[…]**

Medidas de controlo a implementar	- Publicitar regulamento de fundo de maneio onde estejam previstos os procedimentos e regras a seguir na constituição, reconstituição e liquidação do FM, bem como as despesas abrangidas pelo mesmo; - Realizar de auditorias periódicas às despesas por fundo de maneio.

Tipo de controlo [preventivo]	SCI – norma de controlo interno do IPC, subcapítulo II – Disponibilidades (Artigo 7º)		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Sobre a área *Proteção de dados e de segurança da informação* de referir que estão associados quinze processos, associados ao MP07, mais precisamente:

> *Gestão de acessos a informação por intermédio de sistemas informáticos – atribuição de acessos*; *Gestão de acessos a informação por intermédio de sistemas informáticos – Utilização de acessos*; *Gestão de acessos físicos a áreas de armazenamento e processamento de informação – acesso às áreas técnicas*; *Gestão de acessos físicos a áreas de armazenamento e processamento de informação - acesso a áreas de arquivo físico de informação*; *Tratamento de informação - tratamento de dados*; *Tratamento de informação - direitos à Informação*; *Gestão de repositórios de informação - perda de informação*; *Gestão de repositórios de informação – conformidade da utilização de repositórios externos à instituição com o RGPD*; *Gestão de repositórios de informação – Acesso a informação através de repositórios externos à instituição*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos em situação de catástrofe*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos - acesso a informação e serviços informáticos e infraestruturas elétricas e/ou de climatização de centros de dados associadas*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos e os sistemas de comunicação de*

dados associados; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos e os sistemas servidores*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - sistemas de armazenamento de informação*; *Gestão de segurança de informática*.

Em relação à atividade: *Gestão de acessos a informação por intermédio de sistemas informáticos – atribuição de acessos* e a sua ligação com o SCI do IPC verificou-se que não se encontram definidos controlos associados a este processo.

Área: *Proteção de dados e de segurança da informação*
Atividade: "*Gestão de acessos a informação por intermédio de sistemas informáticos – atribuição de acessos*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**2- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Atribuição indevida de acessos.	- Ausência ou falhas de comunicação dos acessos a atribuir aos recursos humanos para exercício das suas funções; - Ausência ou falhas de comunicação aquando a cessação ou alteração de funções dos recursos humanos; - Erros na atribuição ou remoção de acessos, por parte dos serviços responsáveis; - Proliferação de aplicações cujo acesso não é efetuado através de credenciais geridas centralmente; - Existência de várias credenciais de acesso para o mesmo sistema informático, atribuídas ao mesmo recurso humano.	**[…]**

Medidas de controlo a implementar	- Reforçar divulgação e disponibilização dos procedimentos de atribuição e remoção de acessos a recursos informáticos; - Registar no sistema de informação institucional de gestão de RH todos os recursos humanos do IPC (incluindo prestadores de serviço na modalidade de tarefa ou avença), garantindo a necessária qualidade dos dados relativos ao início, alteração e cessão de funções; - Implementar mecanismos automáticos que, fazendo uso da informação mantida na medida 2, procedam à "Revisão de direitos de acesso de utilizadores em intervalos regulares" e "Restrição de acesso à informação baseado no princípio necessidade de conhecer", de acordo com os níveis de conformidade exigidos na RCM n.º 41/2018, que define, no âmbito do Regulamento Geral de Proteção de Dados (RGPD), a "Arquitetura de segurança das redes e sistemas de informação" para todos os serviços e entidades da Administração direta e indireta do Estado; - Reduzir ao mínimo indispensável de sistemas informáticos cujas credenciais de acesso utilizadas não possam ser geridas centralmente no sistema de gestão de identidade e de acessos; - Reduzir ao mínimo indispensável da utilização de múltiplas credenciais de acesso para o mesmo recurso humano.
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de acessos a informação por intermédio de sistemas informáticos – Utilização de acessos*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**6- elevado**	☑						☑	

Riscos associados ao processo	Situações que poderão originar o risco |Causas possíveis|	Resposta ao risco inerente
- Utilização indevida de acessos, com potenciais impactos na integridade, confidencialidade, autenticidade e disponibilidade da informação.	- Computadores com sessões desbloqueadas e aplicações abertas com passwords memorizadas; - Partilha de credenciais de acesso; - Registo descuidado de credencias de acesso em suportes desadequados (post its, ficheiros de texto, etc.); - Utilizadores expostos a fraudes informáticas com recurso a esquemas de engenharia social (phishing, etc.); - Acumulação de perfis em simultâneo (um estudante que pode ser cumulativamente trabalhador e vice-versa); - Utilização de acessos a sistemas e aplicações com privilégios mais elevados do que os necessários para desenvolver as atividades laborais.	**[…]**
Medidas de controlo a implementar	- Definir e implementar políticas que reforcem a segurança das credenciais de acesso utilizadas (ex.: aumento do número mínimo de caracteres, obrigatoriedade de alteração periódica); - Implementar, sempre que possível, de mecanismos de autenticação forte (e.g. cartão cidadão/certificados digitais, impressão digital ou autenticação duplo fator) em aplicações e sistemas informáticos críticos; - Divulgar normas de segurança e formação aos utilizadores sobre cibersegurança (Ciber Higiene); - Ativar registos de atividade (logs) de todos os sistemas e aplicações que disponham destes mecanismos; - Minimizar situações conducentes a acumulação de perfis que possam resultar em conflito de interesses; - Definir formalmente políticas de segurança que sustentem a implementação de medidas com vista à "Restrição de acesso à informação baseado no princípio necessidade de conhecer"; - Eliminar utilização de credenciais de acesso partilhadas por mais do que um recurso humano.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno	

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	Revisão	Periodicidade de execução	Indicador de eficácia
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de acessos físicos a áreas de armazenamento e processamento de informação – acesso às áreas técnicas*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	Modelo ERM do COSO - 2017 |Componentes|					Classificação do risco inerente / Nível do risco	Modelo ICIF do COSO - 2013 |Tipo de objetivo|			Modelo ICIF do COSO - 2013 |componentes |				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**6- elevado**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Acesso indevido a áreas técnicas onde se encontram alojados equipamentos informáticos, com possibilidade de vandalismo desses mesmos equipamentos, resultando em consequências diretas na integridade e disponibilidade da informação (por ex. perda total de informação e/ou sistemas informáticos indisponíveis).	- Chaves de acesso a áreas técnicas expostas em locais sem um controlo de acesso minimamente robusto (chaves colocadas em caixas guardadas em armários, etc.); - Inexistência ou desadequação de mecanismos de controlo de acesso a algumas áreas técnicas; - Inexistência de mecanismos que garantam o registo de acesso a áreas técnicas.	**[…]**
Medidas de controlo a implementar	- Definir procedimentos formais para controlo do acesso físico às áreas técnicas; - Salvaguardar chaves de acesso aos locais recorrendo a mecanismos mais robustos (cofres com controlo de acesso por PIN ou biométricos, entre outros); - Implementar mecanismos de controlo de acesso mais robustos nas áreas técnicas mais críticas (por ex. centro de dados); - Implementar sistemas de videovigilância nas áreas técnicas mais críticas; - Implementar mecanismos de registo automático de acessos às áreas mais críticas, preferencialmente com alarmística.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de acessos físicos a áreas de armazenamento e processamento de informação - acesso a áreas de arquivo físico de informação*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**4- moderado**	☑						☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Acesso indevido a áreas de arquivo físico de informação (documentação de gestão académica, financeira, recursos humanos, entre outras), como potenciais riscos para a integridade, confidencialidade, autenticidade e disponibilidade da informação armazenada nessas áreas.	- Chaves de acesso às áreas de arquivo expostas em locais sem um controlo de acesso minimamente robusto (chaves colocadas em caixas guardadas em armários, etc.); - Inexistência ou desadequação de mecanismos de controlo de acesso a algumas áreas de arquivo; - Inexistência de mecanismos que garantam o registo de acessos às áreas de arquivo.	**[…]**
Medidas de controlo a implementar	- Definir procedimentos formais para controlo do acesso físico às áreas de arquivo; - Salvaguardar as chaves de acesso aos locais recorrendo a mecanismos mais robustos (cofres com controlo de acesso por PIN ou biométricos, entre outros); - Implementar mecanismos de controlo de acesso mais robustos nas áreas de arquivo; - Implementar sistemas de videovigilância nas áreas de arquivo consideradas mais críticas; - Implementar mecanismos de registo automático de acessos às áreas mais críticas, preferencialmente com alarmística.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Tratamento de informação - tratamento de dados*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**4- moderado**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Tratamento incorreto de dados com consequências para a execução dos processos administrativos e de tomada de decisão.	- Erros cometidos nos procedimentos manuais de inserção e atualização de dados nos sistemas de informação institucionais; - Manutenção por vários serviços de múltiplas bases de dados descentralizadas em vários formatos (folhas de cálculo, ficheiros MS Access, etc.), muitas vezes com o mesmo objetivo, conduzindo a cenários de redundância dos dados, incorreções no seu tratamento e desatualização dos mesmos; - Alteração incorreta de dados extraídos de sistemas de informação institucionais, com o objetivo de os melhor adequar a um determinado propósito (produção de relatórios, entre outros), podendo conduzir a visões inconsistentes e desvirtuadas da informação contida nas fontes originais.	**[…]**
Medidas de controlo a implementar	- Criar formalmente uma política de informação institucional, que defina que apenas a informação proveniente de sistemas de informação disponibilizados centralmente e definidos como institucionais, seja considerada como a única fonte oficial para todos os propósitos de entrega de informação. Defina também que, os utilizadores desses sistemas são responsáveis pela inserção e modificação dos dados contidos nos mesmos e, por conseguinte, pelo seu conteúdo, consistência e validade, bem como pela sua privacidade e reserva das suas fontes; - Automatizar processos de transferência de dados entre sistemas de informação, reduzindo ao mínimo indispensável a intervenção humana; - Melhorar o processo de verificação da qualidade dos dados existentes nos sistemas de informação institucionais.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Tratamento de informação - direitos à Informação*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**4- moderado**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Violação dos direitos à Informação (artigo 12.º), acesso (artigo 15.º) e retificação (artigo 16.º) por parte dos titulares dos dados no âmbito do Regulamento Geral de Proteção de Dados (RGPD).	- Manutenção por vários serviços de múltiplas bases de dados descentralizadas em vários suportes (folhas de cálculo, ficheiros MS Access, etc.), muitas vezes com o mesmo objetivo, conduzindo a cenários de redundância de dados, incorreções e desatualização dos mesmos; - A manutenção de múltiplas bases de dados descentralizadas e em vários suportes pelos serviços, dificultam o registo escrito, incluindo em formato eletrónico, de todas as atividades de tratamento de dados, nos termos do artigo 30.º do RGPD, de acordo com o qual, cada responsável pelo tratamento de dados tem de conservar, um registo de todas as atividades de tratamento sob a sua responsabilidade por forma a comprovar a observância do regulamento e facultar esse registo à autoridade de controlo sempre que lhe seja solicitado.	**[…]**
Medidas de controlo a implementar	- Criar/Definir políticas corporativas de tratamento de dados pessoais, no que diz respeito: (1) à seleção de subcontratantes; (2) à segurança no tratamento de dados pessoais; (3) ao tratamento de dados não autorizados; (3) políticas contra perdas ou destruição de dados; (4) riscos do tratamento; (5) controlo da quantidade e qualidade dos dados; (6) segregação de acessos; e (7) segregação de funções; - Promover ações de sensibilização e formação a todos os colaboradores da instituição nas temáticas da privacidade e da proteção de dados pessoais.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de repositórios de informação - perda de informação*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**2- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Perda de informação por inexistência de mecanismos que garantam a redundância da mesma.	- Informação relevante para a instituição mantida unicamente em unidades de armazenamento locais de postos de trabalho, não abrangidas pelos os procedimentos de backup, sob a forma de folhas de cálculo, documentos de texto, bases de dados locais, entre outros. Em situação de avaria das unidades de armazenamento dos postos de trabalho, a informação pode ser totalmente ou parcialmente perdida; - Informação armazenada em unidades de armazenamento móveis, tais como discos externos e *pen drives*, suscetíveis a furtos e avarias.	**[…]**
Medidas de controlo a implementar	- Definir uma política de segurança informática que restrinja a utilização de repositórios locais de informação; - Reforço dos recursos TIC internos que suportam o armazenamento centralizado da informação; - Promover ações de sensibilização direcionadas, com enfoque nos riscos da utilização de repositórios locais; - Implementar controles lógicos nos computadores que equipam os postos de trabalho que reduzam as possibilidades de se utilizarem as unidades de armazenamento locais.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de repositórios de informação – conformidade da utilização de repositórios externos à instituição com o RGPD*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**2- reduzido**			☑				☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Não conformidade com o RGDP por utilização inadequada de repositórios externos à instituição.	- Utilização de repositórios de informação fornecidos por entidades externas à instituição, sem qualquer contrato de prestação de serviços associado (serviços Google ou Microsoft geridos com contas pessoais, entre outros) com o objetivo de armazenar e processar informação institucional, em particular informação contendo dados pessoais.	**[…]**
Medidas de controlo a implementar	- Definir uma política de segurança informática que impeça a utilização de repositórios de informação fornecidos por entidades externas à instituição, sem qualquer contrato de prestação de serviços associado; - Implementação de recursos informáticos que minimizem a necessidade de recorrer a repositórios externos; - Implementar mecanismos de verificação da conformidade com a política de segurança.	

Tipo de controlo	
[preventivo]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo	
[…]	SCI – por identificar na norma de controlo interno do IPC

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de repositórios de informação – Acesso a informação através de repositórios externos à instituição*

Objetivo

Descrição:	**Indicador de cumprimento** […]	**Responsável**	**[…]**

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**2- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Perda de acesso a informação por utilização inadequada de repositórios externos à instituição.	- Recursos humanos que cessam funções e mantêm em repositórios de informação externos à instituição (serviços Google ou Microsoft geridos com contas pessoais, entre outros) versões únicas de informação relevante para a instituição; - Recursos humanos que perdem acesso a repositórios de informação externos à instituição, onde mantinham armazenada informação relevante para a instituição.	**[…]**
Medidas de controlo a implementar	- Definir uma política de segurança informática que impeça a utilização de repositórios de informação fornecidos por entidades externas à instituição, sem qualquer contrato de prestação de serviços associado; - Implementar recursos informáticos que minimizem a necessidade de recorrer a repositórios externos; - Implementar mecanismos de verificação da conformidade com a política de segurança.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos em situação de catástrofe*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**6- elevado**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Impossibilidade de acesso a informação e serviços informáticos, devido a situações de catástrofe, resultando na destruição de equipamentos e instalações em centros de dados.	- Desastres naturais (tremores de terra, inundações, tempestades, entre outros) com consequências para as instalações dos centros de dados; - Incêndios provocados por sobreaquecimento de equipamentos e/ou curtos circuitos nas instalações elétricas; - Inundações nas áreas técnicas dos centros de dados; - Outros eventos que resultem na destruição irreparável de equipamentos e instalações.	**[…]**
Medidas de controlo a implementar	- Criar um plano de continuidade de negócio, baseado nas recomendações da norma internacional ISO/IEC 27031; - Implementar um centro de dados destinado a sustentar processos de recuperação de desastre (*Disaster Recovery*), como parte integrante do plano de continuidade de negócio.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos - acesso a informação e serviços informáticos e infraestruturas elétricas e/ou de climatização de centros de dados associadas*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**4- moderado**	☑						☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Impossibilidade de acesso a informação e serviços informáticos, devido a problemas nas infraestruturas elétricas e/ou de climatização de centros de dados.	- Infraestruturas de alimentação elétrica desajustadas ou subdimensionados face às necessidades atuais; - UPS com baterias em fim de vida, incapazes de garantir o fornecimento elétrico durante intervalos de tempo minimamente aceitáveis; - Climatização deficiente por falta de manutenção dos AC; - Incapacidade de manter a alimentação elétrica de forma ininterrupta em centros de dados críticos para a instituição, em cenários de problemas de fornecimento elétrico da rede ou manutenção demorada (mais de 20 minutos) das instalações elétricas.	**[…]**
Medidas de controlo a implementar	- Rever as instalações elétricas dos centros de dados e, caso se mostre necessário, proceder à sua reestruturação de forma a garantir, no mínimo, a segregação do circuito de alimentação elétrica do centro de dados dos restantes circuitos; - Implementar um processo de manutenção periódica das UPS; - Assegurar a existência de contratos de manutenção para os sistemas de AC e a sua adequada utilização; - Instalar geradores em centros de dados críticos cujo impacto de desativação resulta num prejuízo considerável nas atividades operacionais.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos e os sistemas de comunicação de dados associados*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**4- moderado**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Impossibilidade de acesso a informação e serviços informáticos devido a problemas nos sistemas de comunicação de dados.	- Quebra no meio físico (cabos UTP, fibras óticas, etc.) que suportam ligações de dados; - Avaria de equipamentos ativos de rede; - Funcionamento deficiente das redes de dados por má utilização das mesmas, seja de forma não intencional ou propositada (criação de *loops*, etc.).	**[…]**
Medidas de controlo a implementar	- Instalar caminhos físicos alternativos, redundantes, para interligação de sistemas mais críticos; - Criar mecanismos de redundância ao nível dos ativos de rede, em particular para os que suportam comunicações entre sistemas mais críticos; - Implementar segmentação adequada das redes e controles lógicos para segregação de tráfego e mitigação de problemas de má utilização.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos e os sistemas servidores*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação					☑	**2- reduzido**		☑					☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Impossibilidade de acesso a informação e serviços informáticos por falha nos sistemas servidores.	- Servidores físicos com avarias de *hardware*; - Servidores com recursos computacionais esgotados; - Problemas com software de sistema, decorrentes de processos de atualização; - Problemas de software decorrentes de erros de configuração.	**[…]**
Medidas de controlo a implementar	- Definir e implementar planos de manutenção de hardware; - Definir e implementar planos de manutenção de software; - Implementação de sistemas de monitorização de recursos dos servidores; - Criar ambientes de teste que permitam a avaliação prévia do impacto de configurações e atualizações mais críticas em sistemas servidores.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - sistemas de armazenamento de informação*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação				☑	☑	**6- elevado**		☑					☑	☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Perda de informação por avaria de sistemas de armazenamento.	- Avaria de *hardware* nos sistemas de armazenamento e ausência de cópias de segurança (*backups*) atualizadas; - Problemas de software nos sistemas de armazenamento e ausência de cópias de segurança atualizadas; - Destruição de sistemas de armazenamento por vandalismo ou desastre.	**[…]**
Medidas de controlo a implementar	- Definir e implementar planos de manutenção de hardware; - Definir e implementar planos de manutenção de software; - Implementar planos de *backup* e de replicação da informação, que garantam objetivos de recuperação devidamente ajustados à criticidade dos sistemas; - Replicar a informação para sistemas de armazenamento deslocalizados de forma a garantir resiliência da informação em caso de destruição dos sistemas de armazenamento principais.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas

- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Gestão de segurança de informática*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Proteção de dados e de segurança da informação				☑	☑	**6- elevado**		☑					☑	☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Ataques aos sistemas informáticos com potenciais consequências na integridade, confidencialidade, autenticidade e disponibilidade da informação.	- Equipamentos ativos de rede com vulnerabilidades passíveis de serem exploradas; - Deficiente segmentação de redes e segregação de tráfego, conduzindo à exposição de sistemas críticos; - Sistemas servidores com vulnerabilidades passíveis de serem exploradas; - Computadores de postos de trabalho comprometidos e suscetíveis de perpetrarem ataques informáticos; - Utilizadores expostos a fraudes informáticas com recurso a esquemas de engenharia social (*phishing*, etc.); - Falhas nos controles lógicos conduzindo a cenários de violação de dados e/ou manipulação de políticas de segurança.	**[…]**
Medidas de controlo a implementar	- Definir formalmente e operacionalizar uma estrutura de suporte às questões relacionadas com a segurança informática (SI), que atue ao nível de toda a instituição e que esteja devidamente dotada dos meios humanos e materiais, necessários para: • Coordenar e apoiar as várias unidades orgânicas na reposta a incidentes de segurança informática e respetiva articulação com o CERT.PT, CNCS e CNPD (no caso de violações de dados pessoais); • Promover ações de esclarecimento e sensibilização à comunidade na área da ciber segurança; • Implementar mecanismos de segurança passíveis de serem utilizados por todas as UO (dns firewall, entre outros); • Auditar serviços e redes informáticas, com o objetivo de identificar potenciais falhas e aconselhar a mitigação das mesmas; • Definir políticas de segurança.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo […]	SCI – por identificar na norma de controlo interno		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Área: *Proteção de dados e de segurança da informação*
Atividade: *Processos transversais à atribuição de benefícios*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Benefícios concedidos					☑	**1- reduzido**			☑				☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Violação do princípio da legalidade; **- Abuso de poder. Corrupção passiva para ato ilícito;** **- Favorecimento de terceiros;** **- Tráfico de Influência;** **- Violação dos deveres gerais do trabalhador (zelo, imparcialidade e isenção);** **- Obtenção de benefício económico ilícito para terceiros.**	- Possibilidade de atribuição de benefícios sem suporte legal para o efeito; - Possibilidade de aplicação incorreta dos critérios legal e regularmente estabelecidos; - Possibilidade de atribuição de benefícios em substituição da celebração de contrato público de aquisição de bens ou serviços sem aplicação do Código de Contratos Públicos; - Não salvaguarda de situações de conflito de interesse..	**[…]**
Medidas de controlo a implementar	- Publicitar e disseminar internamente e através dos meios adequados informação útil aos serviços; - Assinar, quando aplicável, por parte da entidade beneficiada, declaração que ateste a inexistência de contrapartidas abrangidas pelo Código de Contratos Públicos.	

Tipo de controlo			
[preventivo]	SCI – por identificar na norma de controlo interno do IPC		
Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		

Tipo de controlo			
[…]	SCI – por identificar na norma de controlo interno do IPC		
Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

Sobre a área dos *Benefícios concedidos*, estão associadas duas atividades: Processos transversais à atribuição de benefícios; Publicitação dos benefícios concedidos.

Área: *Benefícios concedidos*
Atividade: *Publicitação dos benefícios concedidos*

Objetivo

Descrição:	**Indicador de cumprimento**	**Responsável**	**[…]**
	[…]		

Áreas	**Modelo ERM do COSO - 2017 |Componentes|**					**Classificação do risco inerente**	**Modelo ICIF do COSO - 2013 |Tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte	**Nível do risco**	Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
Benefícios concedidos					☑	**1- reduzido**			☑				☑	

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- Responsabilidade disciplinar, civil e financeira do dirigente e cessação da respetiva comissão de serviço; **- A retenção de 15 % na dotação orçamental, ou na transferência do Orçamento do Estado, subsídio ou adiantamento para entidade obrigada, no mês ou meses seguintes ao incumprimento, excecionando-se as verbas destinadas a suportar encargos com remunerações certas e permanentes.**	- Não publicitação dos benefícios concedidos nos termos previstos na Lei 64/2013, de 27 de agosto.	**[…]**
Medidas de controlo a implementar	- Incluir campo no processo de autorização de despesa relativo à obrigatoriedade de publicitação, quando aplicável; - Emitir alertas informáticos relativos à necessidade de publicitação; - Emitir mapas para publicitação, gerados automaticamente a partir dos sistemas informáticos.	
Tipo de controlo [preventivo]	SCI – por identificar na norma de controlo interno do IPC	

Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Medidas de controlo implementadas			
- […]	**Classificação do risco residual** […]	**Resposta ao risco**	**[…]**
Tipo de controlo […]	SCI – por identificar na norma de controlo interno do IPC		
Início **dd-mm-aaaa**	**Revisão** dd-mm-aaaa	**Periodicidade de execução** […]	**Indicador de eficácia** […]

Em síntese, no que concerne ao *MP07 – Recursos Materiais e Serviços*, foram identificados e associados riscos a este macroprocesso, que derivam do plano de GR do IPC. Por outro lado, através do estipulado nos artigos 7º, 8º, 9º, 10º, 12º, 16º e 17º do SCI do IPC estão elencadas medidas de controlo. No entanto, nas áreas:

> *Património, infraestruturas e equipamentos* (atividades: *arquivo de bibliotecas e Património histórico e cultural*) *Proteção de dados e segurança da informação* (atividades: *Gestão de acessos a informação por intermédio de sistemas informáticos – atribuição de acessos*; *Gestão de acessos a informação por intermédio de sistemas informáticos – Utilização de acessos*; *Gestão de acessos físicos a áreas de armazenamento e processamento de informação – acesso às áreas técnicas*; *Gestão de acessos físicos a áreas de armazenamento e processamento de informação - acesso a áreas de arquivo físico de informação*; *Tratamento de informação - tratamento de dados*; *Tratamento de informação - direitos à Informação*; *Gestão de repositórios de informação – conformidade da utilização de repositórios externos à instituição com o RGPD*; *Gestão de repositórios de informação – Acesso a informação através de repositórios externos à instituição*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos em situação de catástrofe*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos - acesso a informação e serviços informáticos e infraestruturas elétricas e/ou de climatização de centros de dados associadas*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos e os sistemas de comunicação de dados associados*; *Gestão de infraestruturas tecnológicas de suporte a sistemas informáticos - acesso a informação e serviços informáticos e os sistemas servidores*; *Gestão de infraestruturas tecnológicas de suporte a*

sistemas informáticos - sistemas de armazenamento de informação; *Gestão de segurança de informática*,

não constam controlos através do SCI do IPC. Igualmente na área dos *Benefícios concedidos*, nas seguintes atividades: *Processos transversais à atribuição de benefícios* e *Publicitação dos benefícios concedidos* não foram evidenciados controlos que estejam associados ao SCI do IPC.

3.5 Análise crítica

Em termos de análise crítica, depois de aplicado o modelo integrado aos diversos documentos existentes, permitiu identificar as seguintes oportunidades de melhoria: falta de controlos que estejam definidos no SCI do IPC (aqueles que estão regulamentados são direcionados essencialmente para a área contabilística, que abrange desde a tesouraria até aos recursos humanos, passando pelas medidas de controlo na parte do património). Por outro lado, no plano de GR também não estão identificados todos os riscos para poder-se efetuar o cruzamento na integra com os macroprocessos do SIGQ e não se encontra contemplado o tratamento para os riscos que foram identificados, conforme matriz proposta.

No *MP01 – Governação*, apenas estão definidos riscos para a área *informação e comunicação*, faltando a identificação em relação aos estratégicos. Sobre o *MP02 – Ensino/Aprendizagem*, foram identificados para as áreas académica e benefícios concedidos. No entanto, a ligação com os referenciais traduz-se na ausência de riscos associados à conceção e aprovação da oferta formativa e na monitorização contínua e revisão periódica dos cursos. Em relação ao *MP03 – Internacionalização*, nada consta quer termos de SCI e GR do IPC. No que concerne ao *MP04 – Investigação* e *MP05 – Relação com a comunidade*, foram identificados riscos, definidos no plano de GR do IPC. No *MP06 – Recursos humanos* e *MP07 – Recursos materiais e serviços*, estão evidenciados também controlos através do SCI do ICP.

A abordagem por macroprocessos permite continuar a verificar a falta de medidas tanto da parte da GR como do CI não sendo evidenciados riscos e medidas de controlo do SCI.

O IPC necessita de definir riscos e controlos associados à sua estratégia, com objetivo de otimizar a estratégia e a performance. Neste sentido, esta proposta de integração em todo

o IPC, traz benefícios, nomeadamente ao serem avaliados riscos durante o processo de definição da estratégia e dos objetivos de operacionais, ajudando na otimização dos resultados. Por sua vez, a proposta deste modelo integrado, permite referir que irá reduzir a redundância inicial que deriva de diversos documentos, incluindo os estratégicos, trazendo relatórios integrados ao IPC. Segundo Dees e Llamas (2021, p.9) os relatórios integrados têm como benefícios a melhoria da transparência e fomentam a comunicação exterior com as PI.

Em síntese, com a otimização de recursos, neste caso públicos, o IPC elimina as redundâncias, com ganhos de eficiência e eficácia, com informação mais fidedigna e ainda no cumprimento do estipulado por lei, normas e regulamentos, nomeadamente a obrigatoriedade de GR e SCI que englobe toda a organização, através de um modelo integrado ligação ao seu SIGQ e estruturas de GR e CI do COSO internacionalmente reconhecidas, dando igualmente resposta às recomendações da Comissão de Avaliação Externa (CAE) da A3ES, nomeadamente de acordo com a A3ES (2021b, p. 5) *é fundamental a atualização do Plano de Gestão de Riscos de Corrupção e Infrações Conexas, em conformidade com legislação e alinhamento com mecanismos do SIGQ*.

CONCLUSÃO

O risco é inerente à própria vida e ao próprio ser humano, consequentemente está no seio das organizações. Qualquer ação que realizamos tem um risco associado. Em termos organizacionais os riscos podem ser categorizados como estratégicos, financeiros, operacionais, tecnológicos e relacionados com: delegação de autoridade e prática de fraude e atos ilegais, sendo que estes necessitam de ser geridos. A nível histórico a tendência para a GR era numa vertente informal e motivada essencialmente pela conformidade de questões legais. No entanto, as expetativas das PI são cada vez mais elevadas, traduzindo-se na necessidade por parte das organizações terem uma gestão mais eficaz e processos organizados no que concerne à GR. O processo de GR é um processo estruturado e contínuo, transversal a toda a organização. Existem vários modelos reconhecidos internacionalmente. Este projeto assentou nos princípios definidos do modelo ERM do COSO.

No âmbito das IES, gerir riscos revela-se um enorme desafio, devido à adoção de procedimentos por inerência da A3ES e consequentemente através de mecanismos internos seja com equipas multidisciplinares, estas envolvidas e enquadradas com o seu ambiente organizacional, no sentido de identificar, detetar, tratar e posteriormente mitigar um conjunto diverso de riscos associados às questões académicas. Por outro lado, em relação ao CI é essencial que estas entidades ao implementar um SCI englobe o plano da organização, políticas, métodos; mecanismos, procedimentos e boas práticas de controlo e também de combate à fraude e corrupção. As IES devem dispor de um plano de GR que seja transversal a toda a organização e meios para os controlar através de um SCI, permitindo eliminar redundâncias através de uma gestão eficaz dos seus recursos.

A integração da ERM na cultura organizacional cruzando com o SCI e SIGQ permite ter uma gestão integrada e suprir redundâncias que ocorrem através de sistemas separados. Em relação ao IPC, com a frequência de milhares de estudantes nos seus cursos, que passam pelo ensino e aprendizagem, investigação, internacionalização e utilizam recursos humanos e materiais, torna-se essencial não só por exigência legislativa, mas igualmente por motivos de uma gestão eficaz na utilização de recursos públicos, a existência de controlos adequados que vão na direção da obtenção de resultados e ao encontro das necessidades e expetativas das suas partes interessadas. Desde modo, o IPC tem três documentos para este efeito: manual da qualidade, plano de GR e uma norma de CI.

Em relação aos objetivos do projeto passaram por: (1) verificar se existem mecanismos e instrumentos de GR implementados no IPC; (2) verificar se estão previstas práticas de CI na IES; (3) elaborar um modelo de GR, integrando-o no IPC através do modelo ERM do COSO 2017 em conjunto com o modelo ICIF do COSO 2013 (integração de modelos), tendo por base o SIGQ; (4) aferir sobre o grau de maturidade da GR e o seu contributo para a gestão do IPC. Por sua vez, um dos contributos deste projeto foi igualmente a elaboração de artigos científicos (em anexo): "*Auditoria interna e o uso das novas tecnologias no ensino superior*", este artigo desenvolvido com o propósito de demonstrar se são usadas novas tecnologias nas auditorias internas realizadas nas IES, aceite e apresentado na 17.ª CISTI, Conferência Ibérica de Sistemas e Tecnologias de Informação, associado ao WICTA (*Workshop on ICT for Auditing & Accounting 2022*) e indexado na Scopus; "*Auditoria Interna nas Instituições de Ensino Superior e o Sistema Interno de Garantia da Qualidade*", artigo aceite e apresentado no XII Encontro de investigadores da Qualidade.

Sobre a existência de mecanismos e instrumentos de GR e prática de CI na IES, a resposta é sim. O IPC tem um plano de GR e SCI, este derivado de uma norma de CI direcionada essencialmente para as questões contabilísticas. No que concerne à elaboração do modelo, este foi construído com base na pesquisa efetuada e contexto organizacional da instituição. Em relação ao grau de maturidade, das respostas obtidas torna-se inconclusiva a obtenção de resultados, uma vez que os respondentes ou não responderam totalmente ou só responderam a metade dessa parte do questionário.

A GR e SCI integrado num modelo tendo por base o seu SIGQ numa IES apresenta-se como uma vantagem competitiva. O trabalho desenvolvido teve como principal objetivo a elaboração de um modelo de GR com o SCI numa IES, realizando a ligação ao SIGQ. Atendendo aos objetivos deste projeto, optou-se por um estudo de caso, designadamente através de um organismo público – O Instituto Politécnico de Coimbra.

A proposta do modelo apresentada teve em consideração a integração do SIGQ, GR e SCI do IPC. Os resultados obtidos permitem concluir que: os princípios e orientações previstos no modelo ERM do COSO (2017) apresentam-se complementares e convergentes com os requisitos do modelo ICIF do COSO (2013). Neste sentido, das melhorias apresentadas pelo modelo proposto destaca-se: identificação dos riscos tendo em conta os objetivos estratégicos; definição de estratégias para o tratamento dos riscos

considerando os fatores de risco; proposta para implementar a vertente prática do risco residual; reformulação e integração do Plano de GR e do SCI, juntamente com o SIGQ, integrando estes sistemas num Sistema Integrado de Gestão; aferição do grau de maturidade do modelo ERM do COSO. Consequentemente, o IPC com este modelo incorpora um SCI com o modelo de GR que engloba o plano da organização; políticas; métodos; procedimentos e boas práticas de controlo.

Em relação a limitações que decorreram deste projeto, destaca-se a obtenção de um número baixo de respostas relativamente à auscultação da maturidade da GR. No que concerne a orientações e propostas para trabalhos futuros, considera-se ser necessário melhorar o entendimento da GR e CI no contexto da administração pública. Sugere-se igualmente o alargamento do âmbito deste trabalho, replicando-o a outras IES e a outras entidades públicas, nomeadamente organismos pertencentes à administração local. Propõe-se também a criação de parcerias entre diversas entidades públicas com o objetivo de realizar partilha de boas práticas e comparação de metodologias em termos de GR e CI, nomeadamente no âmbito da monitorização, que poderia ser desenvolvida também interpares.

Em suma, o modelo proposto de GR e SCI Integrado do IPC, é um sistema de melhoria, de mudança, exclusivo e específico. Aprofunda a cultura institucional para a qualidade, controlo e risco. Assim, o modelo de GR e SCI Integrado pode contribuir positivamente para a eficácia do IPC. Tendo por base o SIGQ, torna-o como um importante instrumento de apoio à gestão, deixando assim de existir tantas redundâncias quer em questões estratégicas, quer em questões operacionais, trazendo uma gestão mais eficiente e eficaz, através de sistemas totalmente integrados.

REFERÊNCIAS BIBLIOGRÁFICAS

A3ES (2016). Referenciais para os sistemas internos de garantia da qualidade nas instituições de ensino superior. Lisboa: Agência de Avaliação e Acreditação do Ensino Superior.

A3ES (2021a). Relatório de monitorização da avaliação do ensino superior em Portugal.

A3ES (2021b). ASIGQ/20/00001 — Relatório final da CAE.

Arens, A., Elder, R. & Beasley, M. (2011). *Auditing and assurance services: An integrated approach*, 14nd edition, Prentice Hall.

Attie, W. (2000). Auditoria: Conceitos e Aplicações. São Paulo: Atlas.

Banham, R. (2004). *Enterprising views of risk management*, Journal of Accountancy, Jun, pp. 65-71.

Barata, A. M. S. (2013). Corrupção e poder local – transparência dos sítios web: estudo de caso. Dissertação de Mestrado. Departamento de Ciências Sociais, Políticas e do Território, Universidade de Aveiro.

Barton, T., Shenkir, W., & Walker, P. (2002). *Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management*. Upper Saddle River, NJ: Financial Times/Prentice Hall PTR.

Beja, R. (2004). *Risk Management* – Gestão, Relato e Auditoria dos Riscos do Negócio; Áreas Editora, S.A.

Bernnein, P. (1996). *Against the gods: The remarkable story of risk. Hoboken*, New Jersey: John Wiley & Sons, Inc.

Caetano, F. (2017). Implementação de um modelo de gestão de risco não clínico na ULSNA, EPE. Trabalho de projeto de mestrado. Instituto de Contabilidade de Administração de Coimbra, Instituto Politécnico de Coimbra.

Carvalho, A. A. (1995). Elementos de Auditoria. Gráfica Claret.

Castanheira, N., & Rodrigues, L. (2006). Gestão de risco: Da abordagem tradicional à gestão de risco empresarial (ERM). Revista Revisores & Empresas > Julho/Setembro 2006, pp. 58-61.

Castanheira, N. M. C. (2007). Auditoria interna baseada no risco – estudo do caso português. Dissertação de Mestrado. Escola de Economia e Gestão, Universidade do Minho.

Chapman, R. (2011). *Simple Tools and Techniques for Enterprise Risk Management* (2ª ed.). West Sussex, United Kingdom: John Wiley & Sons Ltd.

Ching, H. Y. (2011). Contribuição das boas práticas do mercado para a eficiência na gestão de risco corporativo. Revista Brasileira de Estratégia, Curitiba, vol. 4, n.º 3, pp. 257-273, setembro/dezembro.

COSO (1992). *Internal Control – Integrated Framework.* AICPA.

COSO (2004). *Enterprise Risk Management – Integrated Framework*. AICPA.

COSO (2013). *Integrated Framework Executive Summary*. AICPA.

COSO (2017). *Enterprise Risk Management Integrating with Strategy and Performance*. AICPA.

COSO (2019). *COSO Internal Control – Integrated Framework: An Implementation Guide for the Healthcare Provider Industry*. AICPA.

COSO (2020a). *Compliance Risk Management: Applying the COSO ERM Framework*. AICPA.

COSO (2020b). *Blockchain and Internal Control.* AICPA.

Decreto-Lei n.º 109-E/2021 de 9 de dezembro - Mecanismo Nacional Anticorrupção e regime geral de prevenção da corrupção.

Dees, M., Llamas, S. (2021). *Integrated Reporting in the European Public Sector: It's time to act!* ECIIA & EUROSAI.

Deloitte (2014). Nova framework COSO 2013: O que mudou e como aplicar nas organizações. XXI CONFERÊNCIA ANUAL: Auditoria Interna - Controlo Interno e Governação. Instituto Português de Auditoria Interna.

Dicionário de Língua Portuguesa da Porto Editora. (s.d.). Definição de "*risco*".

Dicionário Priberam da Língua Portuguesa. (s.d.). Definição de *"risco"*.

Emblemsvåg, J., & Kjølstad, L. E. (2002). *Strategic risk analysis – a field version*. Management Decision, 40 (9), 842-852.

Ferma (2003). Norma de Gestão de Riscos, *Federation of European Risk Management Associations. Bélgica: The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC)* e *ALARM The National Forum for Risk Management in the Public Sector.*

Fraser, J., & Simkins, B. (2010). *Enterprise risk management: today's leading research and best practices for tomorrow's executives*. Hoboken, New Jersey: JohnWiley & Sons, Inc.

Frigo, M. L. & Anderson, R. J. (2011). *Strategic risk management: A foundation for improving enterprise risk management and governance*. The Journal of Corporate Accounting & Finance, pp. 81-88, march/april.

Fuente, L. & Vega, G (2003). *La gestión de riesgos en empresas no financieras,* Partida Doble, Diciembre, pp. 54-60.

Funston, R. (2003). *Creating a risk-intelligent organization, The Internal Auditor*, April, pp. 59-63.

Gjerdrum, D., & Peter, M. (Março de 2011). *The New International Standard on the on the Practice of Risk Management – A Comparison of ISO 31000:2009 and the COSO ERM Framework.*

Griffiths, D. (2006). *Risk based internal auditing – an introduction*. Acesso em 20 maio de 2022, em: http://www.internalaudit.biz

Haley, U. C. (2003). *Assessing and controlling business risks in China*. Journal of International Management, 9 (3), 237-252.

Hardy, K. (2015). *Enterprise Risk Management: A Guide for Government Professionals*. San Francisco, CA: John Wiley & Sons, Inc.

Hill, S. (2006). Guia sobre a gestão de riscos no serviço público. Brasília: Escola Nacional de Administração Pública.

Hopkin, P. (2010). *Fundamentals of risk management: understanding, evaluating, and implementing effective risk management*. London, United Kingdom: Kogan Page Limited.

Huang, X. (2018). *The Party's Inspection and the Analysis of Effectiveness of Internal Control in Public Colleges and Universities.* Advances in Intelligent Systems Research, 163, pp.1131-1135

IFAC (2010a). Manual das Normas Internacionais de Controlo de Qualidade, Auditoria, Revisão, Outros Trabalhos de Garantia de Fiabilidade e Serviços Relacionados. Lisboa: OROC.

IFAC (2010b). *Guide to Practice Management for Small* - and Medium-Size Practices. New York: IFAC.

IIA (2004). *The Role of Internal Auditing in Enterprise-wide Risk Management*.

IIA (2012). *International Standards for the Professional Practice of Internal Auditing*. Altamonte Springs, Florida: The Institute of Internal Auditors.

Instituto de Auditores Internos de Espanha (2021*). Auditoría Interna y gestión de riesgos*. ISBN: 978-84-122588-4-4

IPC (2020). Plano de Gestão de Riscos do Instituto Politécnico de Coimbra – 2021-2023.

IPC (2021). Plano Estratégico 2021-2025 | Instituto Politécnico de Coimbra. ISBN 978-989-8649-18-8.

ISO (2018). ISO 31000: 2018 Gestão do risco Linhas de orientação. Instituto Português da Qualidade.

Krane, H. P., Rolstadås, A. & Olsson, N. O. (2010). *Categorizing risks in seven large projects- Which risks do the projects focus on?* Project Management Journal, 41 (1), 81-86.

Leitch, M. (2010). ISO 31000:2009 — *The New International Standard on Risk Management*. Risk Analysis, Vol. 30, No. 6, pp. 887-892.

Linsley, P. M. & Shrives, P. J. (2006). *Risk reporting: A study of risk disclosures in the anual reports of UK companies*. The British Accounting Review, 38 (4), 387-404.

Lopez, J. A. & Saidenberg, M. R. (2000). *Evaluating credit risk models*. Journal of Banking & Finance, 24 (1), 151-165.

Machado, S.; Serra S.; Gomes, P.(2017). Auditoria interna nas instituições públicas de ensino superior: Estudo empírico no contexto português. Dos Algarves: A Multidisciplinary e-Journal, 29, 31-48. doi: 10.18089/DAMeJ.2017.29.2

Macieira, A. (2008). Gestão Baseada em Riscos – Reinventando o papel da gestão de riscos integrada ao negócio. ELO Group, pp. 1-13.

Magalhães, M. (2017). Modelo Integrado de Gestão do Risco para o Sector Público Português. Estudo de Caso: O Município da Maia. Trabalho de Projeto. Instituto Politécnico do Porto.

Marchetti, A. (2012). *Enterprise risk management best practices: from assessment to ongoing compliance*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Marques, D.; Morais, G. (2022a) Auditoria interna e o uso das novas tecnologias no ensino superior, junho 2022. DOI: 10.23919/CISTI54924.2022.9820269

Marques, D.; Morais, G. (2022b) Auditoria Interna nas Instituições de Ensino Superior e o Sistema Interno de Garantia da Qualidade, Livro de atas do XII ENCONTRO da RIQUAL - Rede de Investigadores da Qualidade.

Meirinhos, M. & Osório, A. (2010). O estudo de caso como estratégia de investigação em educação. Revista de Educação – Inovação, Investigação em Educação, vol. 2, n.º 2, pp. 49-65.

Moeller, R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes* (2 ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

Morais, G., & Martins, I. (2013). Auditoria Interna: Função e Processo (4ª ed.). Lisboa: Áreas Editora.

Morais, M. G. C. T. (2008). A importância da auditoria interna para a gestão: caso das empresas portuguesas. Brasil: Gramado/Rio Grande do Sul.

Onescu, L. (2018). *Audit And Internal Control Indispensable Tools In Successful Implementation Of Eu Projects*. Internal Auditing and Risk Management, 52(4), pp. 22-33.

Purdy, G. (2010). ISO 31000:2009 - *Setting a New Standard for Risk Management. Risk*.

Rendón, M. E. M. & García, M. L. S. (2015). *El gobierno corporativo y el comité de auditoría en el marco de la responsabilidade social empresarial*. Revista Contaduría y Administración, Universidad Nacional Autónoma de México, n.º 60, pp. 486-506.

Ribeiro, A. (2016). O Papel da Auditoria Interna nas Instituições Públicas de Ensino Superior em Portugal Continental – Universidades e Politécnicos. (Dissertação de Mestrado). ISCAL, Lisboa, Portugal.

Rodrigues, S. M. C. E. (2013). A gestão de risco – Estudo da sua influência na competitividade dos municípios portugueses. Dissertação de Mestrado. Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria.

Santos, M. (2013). O controlo interno e a gestão de risco nas empresas da área metropolitana do Porto. Dissertação de Mestrado. Instituto Superior de Contabilidade e Administração do Porto. Instituto Politécnico do Porto.

Saraiva, E. (2010). A Auditoria Interna em Instituições de Ensino Superior - O Caso do Ensino Público Politécnico (Projecto de Mestrado). IPCV, Viseu, Portugal.

Sá, S. (2018). Avaliação da auditoria interna e do sistema de controlo interno nas Instituições de Ensino Superior – Estudo de caso: Universidades e Politécnicos (Dissertação de Mestrado). ISCAP, Porto, Portugal.

Terry, A.; Prewett, K. (2018) *COSO's Updated Enterprise Risk Management Framework— A Quest For Depth And Clarity*. The Journal of Corporate Accounting & Finance / July 2018 Published online in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/jcaf.22346

Tribunal de Contas (1999). Manual de Auditoria e de Procedimentos (Vol. I). Lisboa. Documento disponível em: https://www.tcontas.pt/pt-pt/NormasOrientacoes/ ManuaisTC/Documents/Manual_vol1.pdf.

Valente, R.M.C. (2000). O porquê da cobertura de risco. Cadernos do Mercado de Valores Mobiliários, n.º 8. Lisboa: CMVM.

Wei, R., & Lewis, C. M. (2003*). Operational risks in the insurance industry*. Philadelphia. University of Pennsylvania, The Wharton School, Department of Insurance and Risk Management.

Willsher, R. (2007), Um negócio arriscado; Revista Exame World Business; Agosto/Setembro/Outubro, pp..42- 47.

APÊNDICES

APÊNDICE 1 - INQUÉRITO POR QUESTIONÁRIO

Inquérito por questionário: O modelo de Gestão de Riscos (GR) e o Sistema de Controlo Interno (SCI) Integrado no Instituto Politécnico de Coimbra (IPC).

Inquérito por questionário

O presente inquérito insere-se no projeto final, do mestrado em Auditoria Empresarial e Pública ministrado pelo Instituto de Contabilidade e Administração de Coimbra com o tema: "O modelo de Gestão de Riscos e o Sistema de Controlo Interno Integrado no Instituto Politécnico de Coimbra". O objetivo é efetuar o respetivo diagnóstico, aferir junto do IPC sobre o cruzamento entre o controlo interno (CI) e GR desta instituição e seu grau de maturidade.

Nota: NS/NA - Não sei/Não se aplica

1. 1. Dados de quem está a responder ao questionário.
   1.1. Cargo

   Marcar apenas uma oval.

   - ◯ Presidência
   - ◯ Chefia intermédia
   - ◯ Outra: _____

2. 1.2. Estrutura/serviço do IPC que pertence?

   Marcar apenas uma oval.

   - ◯ Conselho de Gestão
   - ◯ Outra: _____

3. 1.3. Instituição: Sistema Interno de Garantia da Qualidade (SIGQ).
No âmbito da SIGQ, indique qual o processo a que pertence.

Marcar apenas uma oval.

- ◯ MP01 - Governação
- ◯ MP02 - Ensino/Aprendizagem
- ◯ MP03 - Internacionalização
- ◯ MP04 - Investigação
- ◯ MP05 - Relação com a comunidade
- ◯ MP06 - Recursos Humanos
- ◯ MP07 - Recursos Materiais e Serviços
- ◯ NS/NA

2. Esta seção destina-se a questões em relação ao SCI.

4. 2..1. O IPC possui normas e procedimentos de CI?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ NS/NA

5. 2.2. Se respondeu sim, à questão anterior, quais as áreas que o IPC tem contempladas:

Marcar tudo o que for aplicável.

- ☐ Área financeira
- ☐ Recursos humanos
- ☐ Área académica
- ☐ Proteção de dados e segurança da informação
- ☐ Contratação pública
- ☐ Organização na globalidade
- ☐ Outra: _____

6. 2.3. Que meios de CI existem no IPC. Assinale as suas opções:

Marcar tudo o que for aplicável.

- [ ] Definição de autoridade e delegação de responsabilidades, segregação de deveres e funções
- [ ] Confronto das contagens de caixa, títulos, ativos e existência com os registos contabilísticos
- [ ] Verificação e conferência de registos e realização de conciliações
- [ ] Meio de prevenção de erros e/ou procedimentos ilegais ou fraudulentos
- [ ] Restrição do acesso físico direto aos ativos e registos
- [ ] Aprovação e controlo de documentos
- [ ] Comparação de informação com fontes externas de informação
- [ ] Manual de procedimentos, formulários e documentos
- [ ] Controlo de contas e balancetes de verificação
- [ ] Rotinas de validação
- [ ] Outra: _____

3. Gestão do Risco

7. 3.1. O IPC tem implementado um processo formal de GR, incluindo Plano de Corrupção e Infracções Conexas?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Em fase de implementação

8. 3.2.1. Se respondeu **Sim**, por favor responda às questões seguintes.

Marcar apenas uma oval por linha.

	Sim	Não
Sabe qual a finalidade do Plano de Gestão de Risco de Corrupção e Infrações Conexas?	◯	◯

9. 3.2.1.1. Sim, Qual?

_____

10. 3.3. O IPC tem compreensão exata e abrangente dos riscos que atualmente enfrenta?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ Apenas de alguns riscos

11. 3.3.1. Quais as áreas de intervenção previstas no plano:

Marcar tudo o que for aplicável.

- [ ] Académica
- [ ] Proteção de dados (RGPD)
- [ ] Contratação pública
- [ ] Recursos humanos
- [ ] Receita
- [ ] Património
- [ ] Propriedade intelectual
- [ ] Segurança da informação (tecnologias)
- [ ] Outra: _____

12. 3.4. Quais as ações/procedimentos de intervenção previstos no plano?

Marcar tudo o que for aplicável.

- [ ] Promover ações de formação de sensibilização dos trabalhadores para o risco de corrupção e infrações conexas
- [ ] Identificar as medidas implementadas para prevenir a ocorrência de riscos
- [ ] Desenvolver a atividade de auditoria interna
- [ ] Avaliar a segregação de funções
- [ ] Promover sistemas de controlo interno
- [ ] Outra: _____

13. 3.5. Considera este Plano como ferramenta essencial de prevenção de possíveis erros e/ou omissões?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ NS/NA

14. 3.6. O IPC desenvolveu, nos últimos 3 anos, alguma sessão informativa sobre este Plano?

Marcar apenas uma oval.

- Sim
- Não
- NS/NA

15. 3.7. Tem conhecimento se o IPC possui uma estrutura que monitorize este Plano?

Marcar apenas uma oval.

- Sim
- Não
- NS/NA

16. 3.8. GR no IPC

Marcar apenas uma oval por linha.

	Sim	Não
3.8.1. Assumir riscos é considerado uma estratégia de gestão?	◯	◯
3.8.2. Estão definidos e corretamente implementados controlos que mitiguem eficazmente os riscos identificados no IPC, de modo a não colocar em causa a concretização dos objetivos definidos pela gestão?	◯	◯
3.8.3. Existem meios ou técnicas para identificar potenciais eventos que poderão originar riscos ou oportunidades?	◯	◯
3.8.4. Os processo de GR são acompanhados pela gestão de modo a garantir que as respostas e as ações desenvolvidas para controlar	◯	◯

ou eliminar os riscos são eficazes e estão em linha com os objetivos da organização?		
3.8.5. Periodicamente são analisados e reavaliados os riscos a que o IPC está exposta e estabelecidas medidas que reduzam a probabilidade de ocorrência de perdas futuras e/ou potenciem ganhos?		

4. Relação entre CI e GR

17. 4.1. Utilizando a seguinte escala, exprima a sua opinião sobre cada um dos aspetos abaixo indicados. Responda ao seguinte grupo de questões numa escala de intensidade – Likert – com concordo totalmente, concordo, nem concordo nem discordo, discordo ou discordo totalmente.

Marcar apenas uma oval por linha.

	Discordo totalmente	Discordo	Nem concordo, Nem discordo	Concordo	Concordo totalmente
4.1.1. Um processo de GR deverá ser implementado independentemente da existência de um SCI	⬭	⬭	⬭	⬭	⬭
4.1.2. Cada departamento de uma organização deverá ter um responsável pelo CI, não cabendo apenas à gestão de topo essa responsabilidade	⬭	⬭	⬭	⬭	⬭
4.1.3. A auditoria interna deverá ser o órgão responsável por estruturar e implementar um processo de GR numa organização	⬭	⬭	⬭	⬭	⬭
4.1.4. A auditoria interna deverá ter apenas o papel de supervisão e avaliação num processo de GR e de CI	⬭	⬭	⬭	⬭	⬭
4.1.5. A GR relaciona-se com a gestão de ameaças e oportunidades, enquanto o sistema de controlo interno	⬭	⬭	⬭	⬭	⬭

é projetado para gerir eficazmente essas ameaças e oportunidades					
4.1.6. O objetivo do CI é o de auxiliar a gerir e a controlar o risco de forma adequada e não de o eliminar	⬭	⬭	⬭	⬭	⬭
4.1.7. Um CI eficaz permite criar vantagens competitivas para a organização permitindo-lhe assumir riscos adicionais com vista à criação e preservação de valor para as suas partes interessadas.	⬭	⬭	⬭	⬭	⬭
4.1.8. A GR e o CI não garantem que os objetivos de uma organização sejam todos atingidos, apenas dão uma segurança razoável de que tais objetivos possam ser alcançados.	⬭	⬭	⬭	⬭	⬭
4.1.9. A existência de fluxos de informação e relato entre os órgãos de gestão e as unidades operacionais são fundamentais para que a informação chegue, de forma tempestiva e exata, a todos os colaboradores do IPC.	⬭	⬭	⬭	⬭	⬭

4.1.10. Um bom SCI é essencial e uma GR eficiente	⬭	⬭	⬭	⬭	⬭

18. 4.2. Considerando o Regulamento de CI do IPC (serviço onde exerce as suas funções) responda ao seguinte grupo de questões numa escala de intensidade – Likert – com concordo totalmente, concordo, nem concordo nem discordo, discordo ou discordo totalmente.

Marcar apenas uma oval por linha.

	Discordo totalmente	Discordo	Nem concordo, Nem discordo	Concordo	Concordo totalmente
4.2.1. Considera o Regulamento de CI como uma ferramenta essencial para o controlo e prevenção da ocorrência de possíveis erros e fraudes.	⬭	⬭	⬭	⬭	⬭
4.2.2. Recorre ao Regulamento de CI sempre que surge uma questão/ dúvida à qual não tem solução.	⬭	⬭	⬭	⬭	⬭
4.2.3. O Regulamento de CI é atualizado sempre que as exigências assim o determinem.	⬭	⬭	⬭	⬭	⬭
4.2.4. A existência do Regulamento de CI contribui para	⬭	⬭	⬭	⬭	⬭

um acatamento mais eficiente do cumprimento das normas de ética pelos trabalhadores.					
4.2.5. Considera, no caso específico do IPC, o Regulamento de Controlo Interno uma importante ferramenta de prevenção.	◯	◯	◯	◯	◯

19. 4.3. O IPC realiza acompanhamento do controlo interno e GR com recurso às novas tecnologias de informação?

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não
- ◯ NS/NA

20. 4.3.1. Se sim, quais?

_____

Modelo ERM do COSO - 2017: avaliação do grau de maturidade no IPC.

O modelo ERM COSO é um modelo de gestão de riscos reconhecido internacionalmente. Em 2017, foi alterado, passando a ser composto por 5 componentes (**Governo e Cultura**; **Estratégia e definição de objetivos**; **Desempenho**; **Análise e revisão**; **Informação, comunicação e reporte**) e 20 princípios.
Com o objetivo de adoção do modelo, responda às questões seguintes, assinalando consoante a atual adequação ao IPC.

1- Ad hoc (A abordagem para determinar requisitos de controlo interno e gestão de risco é ad hoc e desorganizado, sem atividades de comunicação ou monitorização).
2 - Fragmentado (Controlos existem, mas não são documentados. O seu funcionamento depende do conhecimento e motivação dos colaboradores).
3 - Global (Os controlos existem e são devidamente documentados. A eficácia operacional é avaliada periodicamente. No entanto, o processo de avaliação não está documentado).
4 - Integrado (Existe um ambiente de controlo, gestão interna e de risco. A avaliação de controlos formais e documentados é realizado com frequência. Muitos controlos são automatizados com o uso a estratégia de tecnologia).
5 - Estratégico (Existe um programa completo controlo interno e gestão risco ao nível do IPC. A avaliação do ambiente de controlo é contínua, baseada nas autoavaliações, análise e análise de lacunas da causa principal).

21. **5.1. Governo e Cultura** (componente)

Supervisionar Riscos através do Conselho de Administração (Principio 1.)

Marcar apenas uma oval por linha.

	1. Ad hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
1.1. O Regulamento do Conselho de Gestão estabelece as suas competências em matéria de supervisão da gestão de risco?	⬭	⬭	⬭	⬭	⬭
1.2. Os membros do Conselho de Gestão recebem formação personalizada para o cumprimento das suas funções de supervisão da gestão de risco?	⬭	⬭	⬭	⬭	⬭
1.3. Existe uma Política de Gestão de Riscos, aprovada pelo Conselho de Gestão, onde são estabelecidos os principais papéis, responsabilidades e competências?	⬭	⬭	⬭	⬭	⬭
1.4. A Política de gestão de risco é consistente com outras estruturas relacionadas (por exemplo, segurança, qualidade, conformidade, etc.)?	⬭	⬭	⬭	⬭	⬭

22. **5.2. Governo e Cultura** (componente)
Estabelecer Estruturas Operacionais (Principio 2.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
2.1. O IPC articulou uma estrutura formal de gestão de risco?	⬭	⬭	⬭	⬭	⬭
2.2. A estrutura é consistente com outras estruturas relacionadas (por exemplo, segurança, qualidade, conformidade, etc.)?	⬭	⬭	⬭	⬭	⬭
2.3. A estrutura de gestão de risco foi amplamente divulgada a todo o IPC?	⬭	⬭	⬭	⬭	⬭
2.4. Os fluxos de aprovação e relatórios estão claramente estabelecidos na gestão de riscos?	⬭	⬭	⬭	⬭	⬭
2.5. Existe uma função de gestão de risco independente da administração?	⬭	⬭	⬭	⬭	⬭
2.6. Os agentes da 1ª, 2ª e 3ª Linha	⬭	⬭	⬭	⬭	⬭

de Defesa estão claramente identificados nas principais áreas do IPC?					
2.7. Existe Comité de Risco ou esses assuntos são tratados em algum dos Comités existentes?	⬭	⬭	⬭	⬭	⬭
2.8. Os gestores de risco das áreas/linhas de negócio (eg Segurança, Cliente, RH, Jurídico, etc.) aparecem regularmente no referido Comité?	⬭	⬭	⬭	⬭	⬭

23. **5.3. Governo e Cultura** (componente)
Definir Cultura desejada (Principio 3.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
3.1. Existe um Código de Ética?	◯	◯	◯	◯	◯
3.2. O IPC adapta a sua estrutura de gestão de riscos com base na sua cultura?	◯	◯	◯	◯	◯
3.3. A Política de Riscos reflete os princípios de comportamento esperado, de acordo com as disposições do Código de Ética do IPC?	◯	◯	◯	◯	◯

24. **5.4. Governo e Cultura** (componente)

Demonstrar compromisso com os Valores Fundamentais (princípio 4)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
4.1. Os principais valores da organização são disponibilizados ao público, tanto interno quanto externo?	◯	◯	◯	◯	◯
4.2. A Gestão de Topo demonstra com seu comportamento seu comprometimento com os valores do IPC (tone at the top)?	◯	◯	◯	◯	◯
4.3. A Gestão de Topo demonstra através do seu comportamento o seu compromisso com o ERM (tone at the top)?	◯	◯	◯	◯	◯
4.4. Os membros do Comité de Riscos promovem ativamente a cultura de gestão de riscos entre o pessoal das suas áreas de responsabilidade?	◯	◯	◯	◯	◯
4.5. O processo de entrada de novos funcionários inclui formação/sensibilização sobre riscos?	◯	◯	◯	◯	◯
4.6. São realizadas medições/avaliações do nível de cultura de risco entre os colaboradores regularmente?	◯	◯	◯	◯	◯

25. **5.5. Governo e Cultura** (componente)
Atrair, desenvolver e reter profissionais qualificados (Principio 5.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
5.1. Existe um programa de gestão de talentos?	◯	◯	◯	◯	◯
5.2. Existe uma política do IPC que apoie o seu compromisso com o desenvolvimento dos funcionários, um sistema de remuneração justa, diversidade e respeito aos direitos humanos?	◯	◯	◯	◯	◯
5.3. O pessoal da gestão de risco possui as habilitações e conhecimentos necessários para realizar as suas tarefas	◯	◯	◯	◯	◯
5.4. Os objetivos da equipa de gestão de risco estão alinhados com os da função de ERM	◯	◯	◯	◯	◯
5.5. Existe um plano de sucessão para os principais cargos de gestão de risco?	◯	◯	◯	◯	◯

26. **5.6. Estratégia e Definição de Objetivos** (componente)
Análisar o contexto de negócios (Principio 6.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
6.1. Existe um Plano Estratégico aprovado pelo Conselho de Gestão?	◯	◯	◯	◯	◯
6.2. O registo/inventário de riscos reflete os fatores internos e externos que podem afetar os objetivos do IPC (estratégicos, operacionais, etc.)?	◯	◯	◯	◯	◯
6.3. As informações externas são sistematicamente analisadas para identificar mudanças relevantes no contexto de negócios e identificar riscos emergentes?	◯	◯	◯	◯	◯
6.4. As informações internas são sistematicamente analisadas para identificar mudanças relevantes no contexto de negócios e identificar riscos emergentes?	◯	◯	◯	◯	◯

27. **5.7. Estratégia e Definição de Objetivos** (componente)
Definir apetite de risco (Principio 7.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
7.1. Existe uma "declaração de apetite ao risco" devidamente formalizada?	◯	◯	◯	◯	◯
7.2. A definição do apetite ao risco é de competência exclusiva do Conselho de Gestão?	◯	◯	◯	◯	◯
7.3. É ativamente promovido que a Gestão de Topo e os principais agentes de ERM conheçam o apetite de risco do IPC?	◯	◯	◯	◯	◯
7.4. O apetite ao risco é considerado nos processos de tomada de decisão?	◯	◯	◯	◯	◯
7.5. O Conselho de Gestão está envolvido na tomada de decisões que possam implicar o	◯	◯	◯	◯	◯

incumprimento do apetite de risco estabelecido?					
7.6. A conformidade com o apetite ao risco é monitorizada ativamente?					

28. **5.8. Estratégia e Definição de Objetivos** (componente)
Avaliar estratégias alternativas (Principio 8.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
8.1. A estratégia do IPC está alinhada com sua missão, visão e valores?	◯	◯	◯	◯	◯
8.2. No processo de planeamento estratégico, as estratégias alternativas são avaliadas, analisando os riscos e oportunidades associados com base em metodologias comprovadas (por exemplo, técnicas estatísticas, matrizes de correlação, etc.)?	◯	◯	◯	◯	◯
8.3. Os principais intervenientes de ERM ou o Comité de Risco participam sistematicamente do processo de planeamento estratégico?	◯	◯	◯	◯	◯

29. **5.9. Estratégia e Definição de Objetivos** (componente)
Formular objetivos de negócios (Principio 9.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
9.1. Os objetivos estratégicos do IPC estão alinhados com o apetite de risco estabelecido?	⬭	⬭	⬭	⬭	⬭
9.2. Os objetivos estratégicos são desenvolvidos em objetivos operacionais, financeiros, de conformidade, etc.?	⬭	⬭	⬭	⬭	⬭
9.3. Os objetivos dos colaboradores estão alinhados com os objetivos estratégicos do IPC?	⬭	⬭	⬭	⬭	⬭
9.4. Os níveis de tolerância ao risco são definidos e atualizados para todos os principais riscos com a aprovação do Conselho de Gestão?	⬭	⬭	⬭	⬭	⬭

9.5. Os níveis de tolerância ao risco são considerados nos processos de tomada de decisão?	⬭	⬭	⬭	⬭	⬭
9.6. O cumprimento dos níveis de tolerância ao risco é monitorizado ativamente?	⬭	⬭	⬭	⬭	⬭
9.7. As exceções ao cumprimento da tolerância ao risco são geridas caso a caso e requerem aprovação da Gestão de Topo e/ou do Conselho de Gestão?	⬭	⬭	⬭	⬭	⬭

30. **5.10. Desempenho** (componente)
Identificar o risco (Principio 10.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
10.1. Existem processos para identificar sistematicamente os principais riscos e oportunidades que afetam o alcance dos objetivos estratégicos e de negócios?	⬭	⬭	⬭	⬭	⬭
10.2. Os riscos são identificados e avaliados periodicamente, pelo menos anualmente?	⬭	⬭	⬭	⬭	⬭
10.3. Existe uma taxonomia de risco para classificar os riscos por tipologia?	⬭	⬭	⬭	⬭	⬭
10.4. São definidos KRIs (Key Risk Indicators) para identificar proativamente riscos crescentes ou emergentes?	⬭	⬭	⬭	⬭	⬭

31. 5.11. **Desempenho** (componente)
Avaliar a gravidade do risco (Principio 11.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
11.1. O impacto e a probabilidade dos riscos identificados são avaliados usando critérios homogéneos pré-estabelecidos?	⬭	⬭	⬭	⬭	⬭
11.2. O impacto económico dos riscos é quantificado, sempre que possível?	⬭	⬭	⬭	⬭	⬭
11.3. O impacto reputacional dos riscos é considerado?	⬭	⬭	⬭	⬭	⬭
11.4. A gravidade do risco é determinada com técnicas de análise determinística (por exemplo, análise de sensibilidade)?	⬭	⬭	⬭	⬭	⬭
11.5. A gravidade do risco é determinada com técnicas de análise probabilística	⬭	⬭	⬭	⬭	⬭

(por exemplo, simulação de Monte Carlo)?					

32. **5.12. Desempenho** (componente)
Priorizar riscos (Principio 12.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
12.1. Os riscos são priorizados com base em seu impacto e probabilidade de ocorrência?	⬭	⬭	⬭	⬭	⬭
12.2. Os riscos estão representados em um mapa de risco (por exemplo, mapa de calor) que permite sua priorização?	⬭	⬭	⬭	⬭	⬭
12.3. É monitorizado sistematicamente se a gravidade dos riscos atende ao apetite/tolerância de risco estabelecido?	⬭	⬭	⬭	⬭	⬭

33. **5.13. Desempenho** (componente)
Implementar respostas aos risco (Principio 13.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
13.1. Os planos são definidos para gerir todos os riscos identificados (ou seja, aceitar, evitar, mitigar ou transferir)?	◯	◯	◯	◯	◯
13.2. É atribuído um responsável e uma data de execução para gerir cada um dos riscos identificados?	◯	◯	◯	◯	◯

34. **5.14. Desempenho** (componente)

Desenvolver uma visão no nível do portfólio (Principio 14.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
14.1. Existe um registo/inventário de riscos centralizado no nível da unidade de negócios?	⬭	⬭	⬭	⬭	⬭
14.2. As possíveis interdependências entre os riscos identificados em cada unidade de negócio são analisadas para se obter uma visão do portfólio naquele nível?	⬭	⬭	⬭	⬭	⬭
14.3. Existe um registo/inventário de risco centralizado no nível de unidade da entidade?	⬭	⬭	⬭	⬭	⬭
14.4. É desenvolvida uma visão integrada ao nível da entidade dos riscos identificados nas diferentes unidades de negócio através da aplicação de metodologias comprovadas (por exemplo, técnicas estatísticas, análise de sensibilidade, simulação de Monte Carlo,	⬭	⬭	⬭	⬭	⬭

matrizes de correlação, etc.)?

35. **5.15. Análise e Revisão** (componente)
Avaliar mudanças significativas (Principio 15.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
15.1. Existe um processo de monitorização para identificar periodicamente mudanças no contexto do negócio (ou seja, fatores internos e externos) com possível impacto no alcance dos objetivos do IPC?	⬭	⬭	⬭	⬭	⬭
15.2. O registo/inventário de riscos do IPC é atualizado regularmente, incorporando questões emergentes ou mudanças no contexto de negócios?	⬭	⬭	⬭	⬭	⬭
15.3. O Comité de Riscos se reúne periodicamente para analisar, concluir e atualizar o Perfil de Riscos do IPC?	⬭	⬭	⬭	⬭	⬭
15.4. Existe um processo de relatório de emergência ou exceção (ou seja, fora do cronograma de relatório	⬭	⬭	⬭	⬭	⬭

formalmente estabelecido)?

36. **5.16. Análise e Revisão** (componente)
Rever o risco e Desempenho (Principio 16.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
16.1. O IPC monitoriza periodicamente o grau de desempenho para os principais objetivos estabelecidos	◯	◯	◯	◯	◯

37. **5.17. Análise e Revisão** (componente)
Procurar a melhoria da Gestão de Riscos de Negócios (Principio 17.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
17.1. O IPC revê a adequação e atualiza a sua estrutura de gestão de riscos periodicamente (por exemplo, auditorias)?	⬭	⬭	⬭	⬭	⬭
17.2. Foram implementadas melhorias significativas no processo de gestão de riscos no último ano?	⬭	⬭	⬭	⬭	⬭

38. **5.18. Informação, comunicação e reporte** (componente)
Aproveitar a informação e a tecnologia (Principio 18.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
18.1. Os membros do Comité de Risco têm acesso direto às Informações de Risco de que precisam para cumprir suas responsabilidades de supervisão	◯	◯	◯	◯	◯
18.2. Existe uma ferramenta de software ERM disponível?	◯	◯	◯	◯	◯
18.3. Os agentes da 1ª. e 2a. Linha de Defesa tem acesso direto à ferramenta para upload, análise e reporte dos riscos sob sua responsabilidade?	◯	◯	◯	◯	◯
18.4. As ferramentas de última geração (por exemplo, análise de dados, big data, inteligência artificial) são usadas para complementar as atividades de ERM?	◯	◯	◯	◯	◯

39. **5.19. Informação, comunicação e reporte** (componente)
Informar sobre riscos de comunicações (Principio 19.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
19.1. Os fluxos de aprovação e relatórios para informações de risco estão claramente estabelecidos?	⬭	⬭	⬭	⬭	⬭
19.2. Os principais riscos da organização são reportados periodicamente (no mínimo anualmente) ao Conselho de Gestão por meio do Comité de Auditoria?	⬭	⬭	⬭	⬭	⬭

40. **5.20. Informação, comunicação e reporte** (componente)
Reportar sobre Risco, Cultura e Desempenho (Principio 20.)

Marcar apenas uma oval por linha.

	1. Ad-hoc	2. Fragmentado	3. Global	4. Integrado	5. Estratégico
20.1. Existem processos de relatórios personalizados nos diferentes níveis organizacionais?	◯	◯	◯	◯	◯
20.2. O processo de GR fornece as informações necessárias para a divulgação de informações públicas (por exemplo, Contas Anuais, Relatório Anual de Governança Corporativa etc.)?	◯	◯	◯	◯	◯
20.3. As métricas de monitorização de risco (Key Risk Indicators ou KRIs) são usadas para alertar sobre riscos crescentes ou emergentes?	◯	◯	◯	◯	◯
20.4. É uma avaliação qualitativa (tendência histórica, perspetiva futura, nível de seguro, etc.) e	◯	◯	◯	◯	◯

quantitativa (nível de exposição, nível máximo, análise de sensibilidade e teste de stress, etc.) dos principais riscos reportados?					
20.5. Os riscos materializados e o seu real impacto nos objetivos do IPC são relatados?	⬭	⬭	⬭	⬭	⬭
20.6. A cultura de risco é relatada?	⬭	⬭	⬭	⬭	⬭

Muito obrigado pelas respostas e colaboração neste trabalho!

APÊNDICE 2 – EXEMPLIFICAÇÃO DO MODELO INTEGRADO NO IPC

MP0X – "identificar macroprocesso"

Área: "descrever a área"
Atividade: "identificar atividade"

Objetivo

Descrição: [descrever objetivo]	**Indicador de cumprimento**	**Responsável**	[definir responsável]
	[definir objetivo]		

Componentes da gestão de riscos e controlo interno

Áreas	**Modelo ERM do COSO - 2017 |componentes|**					**Classificação do risco inerente** / **Nível do risco**	**Modelo ICIF do COSO - 2013 |tipo de objetivo|**			**Modelo ICIF do COSO - 2013 |componentes |**				
	Governança e Cultura	Estratégia e estabelecimento de objetivos	Desempenho	Revisão e monitorização	Informação e reporte		Operacionais	Reporte	Conformidade	Ambiente de controlo	Avaliação de riscos	Atividades de controlo	Informação e comunicação	Monitorização
- [descrever área]	☑	☑	☑	☑	☑	**Valorização do risco**	☑	☑	☑	☑	☑	☑	☑	☑

Riscos associados ao processo	**Situações que poderão originar o risco |Causas possíveis|**	**Resposta ao risco inerente**
- [descrever riscos]	- [descrever situações que poderão originar o risco]	[Aceitar/Prevenir/…]
Medidas de controlo a implementar	- [descrever medidas de controlo a implementar]	
Tipo de controlo		
[…]	SCI – [identificação do normativo associado a este controlo]	

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[definir indicador]

Medidas de controlo implementadas

- […]	**Classificação do risco residual**	**Resposta ao risco**	**[…]**
	[…]		
Tipo de controlo			
[…]	SCI – [identificação do normativo associado a este controlo]		

Início	**Revisão**	**Periodicidade de execução**	**Indicador de eficácia**
dd-mm-aaaa	dd-mm-aaaa	[…]	[…]

ANEXOS

ANEXO 1 – PLANO DE GESTÃO DE RISCOS DO IPC

PLANO DE GESTÃO DE RISCOS DO IPC 2021-2023

Disponível em: https://www.ipc.pt/ipc/wp-content/uploads/2021/06/Plano-de-Gestao-de-Riscos-do-IPC-2021-a-2023-v2.pdf

ANEXO 2 – NORMA DE CONTROLO INTERNO DO IPC e SASIPC

NORMA DE CONTROLO INTERNO – IPC E SASIPC

Disponível em: https://www.ipc.pt/ipc/wp-content/uploads/2020/03/37_norma_controlo_interno_ipc_e_sas.pdf

ANEXO 3 – ELABORAÇÃO DE ARTIGOS

No âmbito da atividade não letiva foram desenvolvidas quatro publicações, que contribuíram para aprofundar conhecimentos a aplicar neste projeto. Artigo aceite e apresentado no XI Encontro de investigadores da Qualidade: "*A importância da auditoria interna no Sistema Interno de Garantia da Qualidade nas Instituições Públicas de Ensino Superior Politécnico – estado da arte*"; Publicação aceite e apresentado no Congresso internacional: Desafios da Qualidade nas IES: "*Ensino superior e auditoria interna aos sistemas internos de garantia da qualidade*"; Artigo desenvolvido com o propósito de demonstrar se são usadas novas tecnologias nas auditorias internas realizadas nas IES, aceite e apresentado na 17.ª CISTI, Conferência Ibérica de Sistemas e Tecnologias de Informação, associado ao WICTA (*Workshop on ICT for Auditing & Accounting 2022*) e indexado na Scopus (DOI: 10.23919/CISTI54924.2022.9820269): "*Auditoria interna e o uso das novas tecnologias no ensino superior*"; e artigo aceite e apresentado no XII Encontro de investigadores da Qualidade: "*Auditoria Interna nas Instituições de Ensino Superior e o Sistema Interno de Garantia da Qualidade*".

A importância da auditoria interna no Sistema Interno de Garantia da Qualidade nas Instituições Públicas de Ensino Superior Politécnico – estado da arte

David Marques
dmrmarques@gmail.com
Coimbra Business School – ISCAC/IPC

Georgina Morais
mmorais@iscac.pt
Coimbra Business School – ISCAC/IPC

Resumo:

O presente artigo contribui para um melhor entendimento da importância que é dada à auditoria interna realizada aos Sistemas Internos de Garantia da Qualidade (SIGQ) nas Instituições Públicas de Ensino Superior Politécnico. Os SIGQ e os referenciais da Agência de Avaliação e Acreditação do Ensino Superior trouxeram mudanças nas estruturas e estratégias internas destas instituições, muitas com boas práticas já instituídas que advêm de outras normas de certificação como é o caso da ISO 9001.
A informação proporcionada no âmbito das auditorias internas é reconhecida como uma melhoria da eficácia da gestão e permite ajudar na tomada de decisões. A estratégia para a qualidade, tem em consideração a avaliação regular que é feita pelas auditorias internas e monitorização da implementação de melhorias resultantes desta avaliação.
Para analisar empiricamente a relação entre auditoria interna nos SIGQ, este estudo baseia-se na análise de resultados divulgados e de um questionário enviado aos órgãos de gestão destas instituições.
Estas instituições de ensino ao criarem um gabinete de auditoria interna ou aprimorar o papel de um gabinete já existente, desenvolvem as atividades desse serviço para que se torne um instrumento para apoiar a boa governança da organização. Podemos referir que a auditoria interna tem cada vez mais importância no seio destas instituições e dos SIGQ.

Palavras-chave: Auditoria interna, melhoria contínua, qualidade, SIGQ.

Abstract:

This article contributes to a better understanding of the importance given to the internal audit carried out on the Internal Quality Assurance Systems (SIGQ) in Public Institutions of Polytechnic Higher Education. The SIGQ and the references of the Agency for Assessment and Accreditation of Higher Education brought changes in the structures and internal strategies of these institutions, many with good practices already in place that come from other certification standards such as ISO 9001.

Ensino superior e auditoria interna aos sistemas internos de garantia da qualidade

David Marques
dmrmarques@gmail.com
Coimbra Business School, Instituto Politécnico de Coimbra, Portugal

Georgina Morais
mmorais@iscac.pt
Coimbra Business School, Instituto Politécnico de Coimbra, Portugal

Resumo:

As instituições de ensino superior (IES) através dos Sistemas Internos de Garantia da Qualidade (SIGQ) têm realizado mudanças internas, tanto a nível estratégico como estrutural, as quais têm dado continuidade às boas condutas organizacionais que já tinham sido introduzidas, por algumas, da implementação e certificação destas entidades por outros normativos, como é o caso da ISO 9001. Por sua vez, as auditorias internas têm permitido ajudar na tomada de decisões e são reconhecidas como uma melhoria para a economia, eficiência e eficácia das organizações.

A estratégia para a qualidade no ensino superior é uma realidade, tem em consideração a avaliação regular que é feita pelas auditorias internas e respetiva monitorização da implementação de melhorias, muitas destas, resultantes das avaliações aos SIGQ.

O ensino superior e auditoria interna aos SIGQ, é um estudo empírico que tem em consideração a análise dos resultados divulgados por outros estudos desenvolvidos e pelos resultados de um questionário que foi submetido a estas entidades. A presente pesquisa permite contribuir para uma melhor perceção sobre a forma e importância que as auditorias internas realizadas aos SIGQ das IES são consideradas e a sua adequação aos referenciais da Agência de Avaliação e Acreditação do Ensino Superior (A3ES).

As IES ao começarem a ter consciência da importância do desenvolvimento de auditorias internas nas suas organizações, seja através da criação de uma estrutura que as realiza, seja com o aperfeiçoamento de uma já existente e a desenvolver as atividades desse serviço, permitem que estas se tornem um instrumento cada vez mais de apoio à boa governança destas entidades. Pode-se assim mencionar que no ensino superior a auditoria interna é muito importante para os SIGQ e consequentemente para a melhoria institucional.

Palavras-chave: auditoria interna, ensino superior, melhoria, qualidade

Auditoria interna e o uso das novas tecnologias no ensino superior

Internal audit and the use of new technologies in higher education

David Marques
Coimbra Business School | ISCAC,
Polytechnic of Coimbra,
Coimbra, Portugal
dmrmarques@gmail.com

Georgina Morais
Coimbra Business School | ISCAC,
Polytechnic of Coimbra,
Coimbra, Portugal
mmorais@iscac.pt

Resumo — **A auditoria interna tem contribuído para a melhoria institucional das organizações. O atual contexto que resulta da transformação e transição digital implica o uso das novas tecnologias. Neste sentido, o presente artigo tem como propósito demonstrar se são usadas novas tecnologias nas auditorias internas nos Institutos Politécnicos Públicos e contribuir para um melhor entendimento da importância que é dada à auditoria interna realizada aos Sistemas Internos de Garantia da Qualidade (SIGQ). O Ensino Superior, ao consciencializar-se da relevância do uso das novas tecnologias de informação nas auditorias internas às suas instituições, poderá encará-las como um contributo adicional ao avanço da atual transição digital nas Instituições de Ensino Superior (IES). Estas ferramentas tornam-se cada vez mais importantes no seu seio das IES e no apoio à boa governação destas organizações face à complexidade dos atuais sistemas de informação. Por sua vez, estas são utilizadas na auditoria interna.**

Palavras Chave - Auditoria Interna, Instituições de Ensino Superior, Sistemas de Informação, Tecnologias de Informação para auditoria.

Abstract — **Internal Internal audit has contributed to the institutional improvement of organizations. The current context resulting from digital transformation and transition implies the use of new technologies. In this sense, this article aims to demonstrate whether new technologies are used in internal audits in Public Polytechnic Institutes and to contribute to a better understanding of the importance given to the internal audit performed to Internal Quality Assurance Systems (IQAS). Higher Education, by becoming aware of the relevance of the use of new information technologies in internal audits of their institutions, can see them as an additional contribution to the advancement of the current digital transition in Higher Education Institutions (HEIs). These tools are becoming increasingly important within the HEIs and in supporting the good governance of these organizations given the complexity of current information systems. In turn, these are used in internal auditing.**

Keywords - Internal Audit, Higher Education Institutions, information systems, computer-assisted audit tools.

I - INTRODUÇÃO

O contexto atual das organizações é refletido em inúmeros desafios, muitos destes derivam da própria globalização e consequentemente do atual uso das novas tecnologias. Por sua vez, os auditores internos têm de estar adaptados à constante mudança que as inovações tecnológicas trazem às instituições, traduzindo-se na realização de auditorias internas através do uso de novas tecnologias.

As auditorias internas têm permitido ajudar na tomada de decisões e são reconhecidas como uma melhoria para a economia, eficiência e eficácia destas organizações.

O uso das novas ferramentas informáticas com as auditorias internas no contexto de auditoria interna nas IES é algo que necessita, face ao atual cenário, de ser percecionado como uma mais-valia devido a poder melhorar o trabalho do auditor interno, com a redução de processos manuais para processos automatizados através da aplicação das inovações tecnológicas nas auditorias internas. Assim, com este artigo pretende-se perceber o grau de utilização das TI em Auditoria Interna nas IES, em especial de Ensino Superior Politécnico Público e qual a importância que é dada à auditoria interna realizada aos Sistemas Internos de Garantia da Qualidade.

Pretende-se dar resposta aos objetivos anteriormente descritos com a revisão da literatura e resultados de um questionário administrado às IES de Ensino Superior em Portugal.

Este artigo encontra-se organizado da seguinte forma: a seção I e II contempla a introdução e a revisão da literatura, respetivamente. O estudo empírico: metodologia e análise dos resultados está relatado na seção III. A seção IV contém a conclusão deste artigo.

II - REVISÃO LITERATURA

Nas últimas décadas, a auditoria tem vindo a evidenciar a sua importância para a sociedade e para as organizações. Tem sido atribuída uma importância crescente à realização de auditorias, tendo em conta a classificação quanto ao sujeito que as realiza, uma vez que as ações desenvolvidas interna e externamente

Auditoria Interna nas Instituições de Ensino Superior e o Sistema Interno de Garantia da Qualidade

David Marques
dmrmarques@gmail.com
Coimbra Business School – ISCAC/IPC

Georgina Morais
mmorais@iscac.pt
Coimbra Business School – ISCAC/IPC

Resumo:
O Sistema Interno de Garantia da Qualidade (SIGQ) no seio das Instituições de Ensino Superior (IES) tem trazido mudanças estruturais para estas organizações que derivam entre outras da realização de auditorias internas. Por outro lado, a gestão de risco (GR) e o controlo interno (CI) são elementos essenciais na governação das organizações.
A auditoria interna (AI) nas IES e o SIGQ é o tema deste artigo com o propósito de dar continuidade ao estudo efetuado sobre a importância das auditorias internas realizadas aos SIGQ.
A obtenção de respostas sobre se as IES têm nas suas organizações estruturas de AI bem como a adoção da GR e CI são conclusões que pretendem ser respondidas. Este estudo irá contribuir para um melhor entendimento da importância que é dada à AI, GR e CI no seio das IES.
Para analisar empiricamente a ligação entre AI e o SIGQ, este artigo baseia-se na análise de resultados divulgados e de um questionário enviado aos órgãos de gestão a todas as IES em Portugal.
A AI e o relato que é obtido da sua avaliação é reconhecido como uma melhoria da eficácia da gestão que permite ajudar na tomada de decisões no âmbito do SIGQ.

Palavras-chave: Auditoria interna, controlo interno, gestão de riscos, instituições de ensino superior, qualidade.

Abstract:
The Internal Quality Assurance System (IQAS) within Higher Education Institutions (HEI) has brought structural changes to these organizations that derive, among others, from the performance of internal audits. On the other hand, risk management (RM) and internal control (IC) are essential elements in the governance of organizations.
The internal audit (IA) in HEI and the IQAS is the subject of this article with the purpose of continuing the study carried out on the importance of internal audits carried out on IQAS.
Obtaining answers on whether HEIs have internal audit structures in their organizations as well as the adoption of RM and IC are conclusions that intend to be answered. This study will