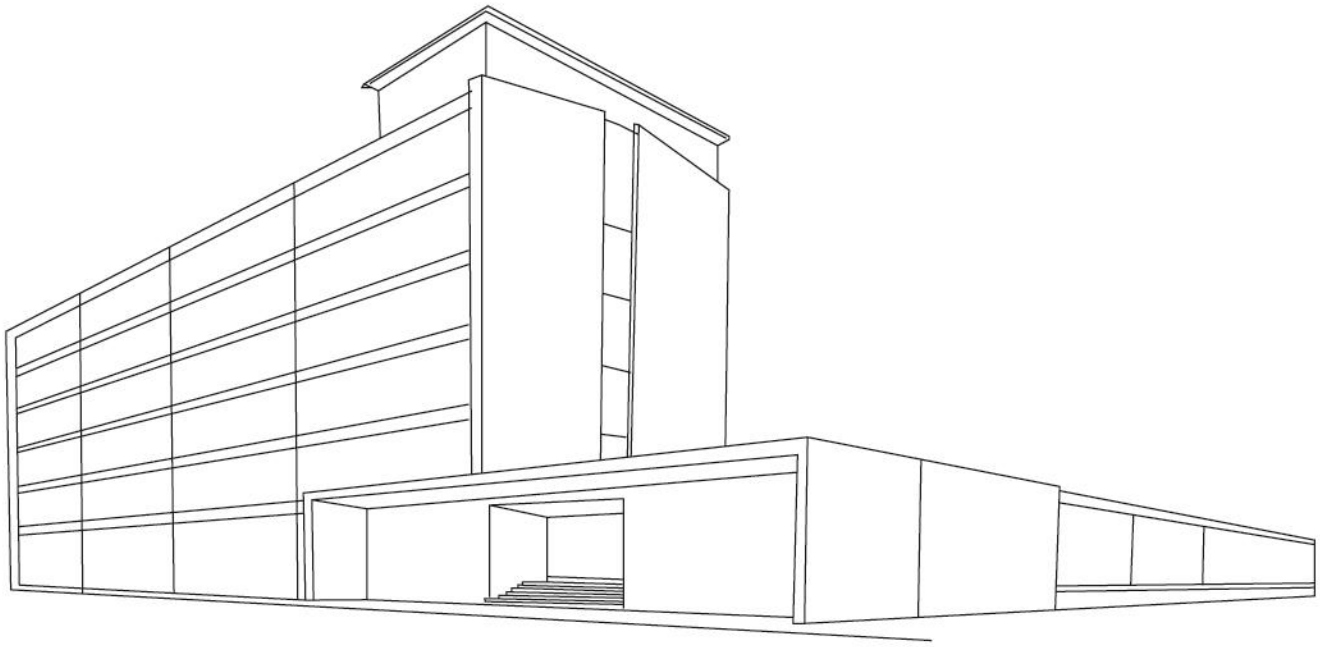

PLANO DE GESTÃO DE
RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

2017

Abreviaturas

APR	▸ Aprovisionamento
CGR	▸ Centro de gestão de recursos
CIT	▸ Centro de informática e técnico
CMM	▸ Controlo de meios monetários
COC	▸ Controlo orçamental e contabilidade
CPA	▸ Código do Procedimento Administrativo
CPC-ESEP	▸ Comissão de Prevenção da Corrupção da ESEP
EAM	▸ Expediente, arquivo e museu
ESEP	▸ Escola Superior de Enfermagem do Porto
PGRCIC	▸ Plano de Gestão de Riscos de Corrupção e Infrações Conexas
SAAE	▸ Serviços académicos e de apoio ao estudante

1. Caracterização da ESEP

1.1 Identidade

A Escola Superior de Enfermagem do Porto[1] (ESEP) é uma pessoa coletiva de direito público, dotada de personalidade jurídica e de autonomia estatutária, científica, pedagógica, cultural, disciplinar, administrativa, financeira e patrimonial que se identifica como uma instituição pública não integrada de ensino superior politécnico com elementos distintivos no plano nacional e internacional ao nível da excelência da formação de enfermeiros e da criação, transmissão e difusão da cultura, do saber e da ciência e tecnologia, através da articulação do estudo, do ensino e da investigação.

1.2 Missão

A ESEP tem por missão proporcionar ciclos de estudos, bem como outros programas de formação, orientados para o desenvolvimento de competências no domínio da Enfermagem. Paralelamente, promove investigação e programas de desenvolvimento geradores, quer de novo conhecimento disciplinar, quer de inovação em saúde.

1.3 Estrutura organizacional

Os órgãos de governo da Escola Superior de Enfermagem do Porto, de acordo com os estatutos são:

a) Conselho geral;
b) Presidente;
c) Conselho de gestão;
d) Conselho consultivo;
e) Conselho técnico-científico;
f) Conselho pedagógico.

[1] Com estatutos homologados pelo Despacho normativo n.º 26/2009, publicado no Diário da República, *2.ª série*, n.º 136, de 16 de julho de 2009.

2. Metodologia

O Plano de Gestão de Riscos de Corrupção e Infrações Conexas (PGRCIC) da ESEP assenta em três vertentes estruturantes: a primeira, de âmbito geral, formativo e de sensibilização dos seus trabalhadores e agentes; a segunda, de identificação de riscos e determinação de medidas e ações concretas de prevenção à ocorrência de situações de corrupção e de infrações conexas; e, a terceira, de controlo e acompanhamento da implementação e efetivo cumprimento do plano.

Como referenciais no desempenho das suas atribuições, a ESEP adota, com primazia, os princípios constantes da Constituição da República Portuguesa, do Código do Procedimento Administrativo, da Lei Geral dos Trabalhadores em Funções Públicas e da Carta Ética da Administração Pública.

Tomou-se como noção de risco, o resultado da combinação entre a probabilidade de ocorrência, aleatória e futura, de um desvio às melhores práticas na atuação administrativa e o impacto dele resultante.

Para dar início à configuração do PGRCIC, e no intuito de diagnosticar necessidades, procedeu-se a um levantamento do que, nos processos e operações administrativas da ESEP, poderia configurar risco de desvio quanto aos deveres éticos e funcionais legalmente impostos à Administração Pública e aos seus agentes.

Nesse levantamento, constatou-se que um número muito significativo de riscos é transversal aos diferentes serviços e procedimentos. Acresce que, estes riscos transversais surgem associados, não tanto à atividade específica de cada um dos serviços, mas, antes, à atuação dos diferentes trabalhadores enquanto agentes da Administração Pública.

Num plano mais estrito, e tomando-se por referência os documentos e as orientações do Tribunal de Contas, identificaram-se e autonomizaram-se os serviços que desenvolvem atividades consideradas de maior risco, nomeadamente, a gestão estratégica, a administração económica/financeira e a gestão de recursos humanos (desenvolvidas pelo Centro de Gestão de Recursos) e as tecnologias de informação (desenvolvidas pelo Centro de Informática e Técnico). Em paralelo, identificaram-se os serviços que, por via da especialização e tecnicidade das suas atribuições, encerram riscos e necessidades específicas de prevenção (os Serviços Académicos e de Apoio ao Estudante e o serviço de Expediente, Arquivo e Museu).

Para uma melhor organização do plano, procedeu-se ao agrupamento das diferentes atividades e procedimentos que partilham os mesmos riscos e são alvo das mesmas medidas preventivas.

3. Implementação do plano

A implementação do PGRCIC da ESEP inclui:

A. A criação da Comissão de Prevenção da Corrupção da ESEP (CPC-ESEP), composta por quatro elementos, a designar pelo Presidente da ESEP;
    a. À CPC-ESEP incumbirá a coordenação e a aplicação do PGRCIC, bem como o acompanhamento e a monitorização da respetiva implementação e cumprimento;
    b. A CPC-ESEP elaborará um relatório anual, com base nas informações disponibilizadas pelos serviços e pelo Gabinete de apoio à qualidade e à avaliação, a submeter à apreciação do Conselho de gestão. O relatório anual deverá ser entregue até ao final do mês de fevereiro do ano seguinte àquele a que diz respeito;
    c. Para a avaliação qualitativa dos riscos será tomada como referência a Norma FERMA. Esta avaliação será efetuada no primeiro relatório, podendo ser revista anualmente.
B. A apropriação do PGRCIC da ESEP pelos trabalhadores:
    a. Divulgação, através de informação a enviar por correio eletrónico e a publicar no sítio da ESEP na Internet, do PGRCIC e da respetiva implementação, bem como dos princípios éticos adotados como referência pela ESEP;
    b. Ações de formação interna sobre as medidas de prevenção de riscos de corrupção e infrações conexas que aproximem os trabalhadores do Plano e facilitem a sua implementação.
C. Ações de auditoria à implementação e execução do PGRCIC da ESEP.

Plano de Gestão de Riscos de Corrupção e Infrações Conexas

ÁREA: "TRANSVERSAL"[2] Atividades sensíveis	RISCOS DE CORRUPÇÃO E DE INFRAÇÕES CONEXAS	PROCEDIMENTOS PREVENTIVOS A ADOTAR
▸ Procedimentos que envolvem a interação direta da ESEP com os particulares e em que está em causa o interesse público.	▸ Risco de violação dos princípios e valores gerais da atividade administrativa; ▸ Risco de violação dos deveres funcionais de responsabilidade, transparência, isenção, imparcialidade e confidencialidade; ▸ Risco de incompatibilidade e conflito de interesses; ▸ Risco de utilização indevida de bens públicos; ▸ Risco de violação do princípio da prossecução do interesse público; ▸ Risco de violação do sigilo profissional e procedimental; ▸ Risco de erro na informação prestada no atendimento aos clientes (internos e externos); ▸ Risco de erro na emissão de certificados, diplomas e outras certidões; ▸ Risco de erro na informação registada nas bases de dados; ▸ Risco de omissão, erros ou desatualização dos conteúdos institucionais divulgados nos locais de estilo, nomeadamente no sítio da ESEP na Internet;	▸ Atualizar os trabalhadores em matérias de ética e deveres funcionais, com ações de formação periódicas; ▸ Acompanhar e supervisionar o cumprimento das orientações e da observância dos princípios éticos no exercício de funções dos trabalhadores, pelos respetivos responsáveis; ▸ Implementar medidas conducentes à prevenção da quebra de sigilo, designadamente restringindo o acesso aos dados que integram os processos individuais de estudantes e trabalhadores, nas suas diferentes etapas; ▸ Implementar a obrigatoriedade de os trabalhadores declararem, individual e expressamente, em determinadas intervenções procedimentais, eventuais conflitos de interesse e impedimentos. ▸ Disponibilizar formação a todos os trabalhadores sobre o CPA, legislação e regulamentos pertinentes para o exercício das suas funções; ▸ Incentivar à frequência de cursos/formações sobre atendimento ao público; ▸ Difundir as melhores práticas e novos conhecimentos com vista à sua adoção pelos diferentes serviços e trabalhadores; ▸ Dinamizar momentos de partilha de conhecimentos, de experiências e de informação técnica;

[2] Riscos gerais aplicáveis a todos os trabalhadores independentemente da atividade exercida, inclui diferentes serviços, órgãos ou gabinetes.

	▸ Risco de redução da qualidade e fiabilidade dos estudos e pareceres; ▸ Risco de redução da qualidade do serviço prestado ao cliente; ▸ Risco de extravio ou de inutilização de documentos e equipamentos, por ação humana ou causas naturais; ▸ Risco de descoordenação na relação entre os serviços; ▸ Apropriação ou uso ilegítimo, de bens, fundos ou valores confiados aos trabalhadores em razão das suas funções.	▸ Implementar mecanismos de articulação, comunicação e divulgação da informação técnica entre serviços e gabinetes; ▸ Manter a informação científica atualizada; ▸ Promover a revisão das publicações por elementos externos aos trabalhos de edição; ▸ Promover a troca de informação interna e externa; ▸ Conferir a informação intermédia e final; ▸ Acompanhar, de forma sistemática, os conteúdos contantes do sítio da internet da ESEP, com sistemas de alertas; ▸ Acompanhar e supervisar os técnicos e equipas de trabalho; ▸ Adotar a colegialidade na realização das ações, com especial relevância nas de controlo, e na tomada de decisão; ▸ Mobilizar os trabalhadores entre os diferentes serviços, de acordo com a natureza das funções a desempenhar e as respetivas competências e condições; ▸ Supervisar os procedimentos adotados e rever, por amostragem aleatória, os trabalhos realizados; Promover a segregação de funções e estabelecer a responsabilidade pelas operações; ▸ Implementar mecanismos de aferição externa aos comportamentos adotados no exercício das funções; ▸ Verificar, com regularidade, o cumprimento das regras de manuseamento e utilização de equipamentos;

		▸ Criar instruções e formulários e definir prazos obrigatórios para a recolha de informação; ▸ Triangular dados com origem em fontes distintas e realizar testes de conformidade e cumprimento procedimental; ▸ Criar sistemas de controlo interno: conferência, de forma aleatória, numa base de amostragem, a um número mínimo mensal/anual de documentos emitidos.
▸ Planeamento e gestão de atividades	▸ Risco de afastamento e inexecução do plano estratégico aprovado para a ESEP; ▸ Risco de inadequação dos perfis técnicos e comportamentais ao exercício de funções; ▸ Risco de falhas na implementação, aplicação e uniformização das normas, orientações, métodos e procedimentos; ▸ Risco de promoção inadequada da imagem institucional e ausência de informação de suporte.	▸ Implementar reuniões periódicas de planeamento e acompanhamento das atividades; ▸ Definir prioridades de acordo com o plano estratégico; ▸ Planear a adoção de planos operacionais e definir objetivos de curto prazo; ▸ Promover a motivação individual e dos grupos de trabalho; ▸ Adequar as necessidades formativas ao perfil exigido; ▸ Definir níveis de responsabilidade; ▸ Acompanhar e controlar a execução das medidas previstas na norma de controlo interno; ▸ Estabelecer mecanismos de uniformização de metodologias de promoção da imagem institucional; ▸ Promover ações de sensibilização da imagem institucional.

ÁREA: CGR-RECURSOS HUMANOS Atividades sensíveis	RISCOS DE CORRUPÇÃO E DE INFRAÇÕES CONEXAS	PROCEDIMENTOS PREVENTIVOS A ADOTAR
▸ Procedimentos de recrutamento e seleção de pessoal.	▸ Risco de violação dos deveres de transparência, isenção e imparcialidade; ▸ Risco de erro na informação de disponibilidade para contratação de docentes convidados; ▸ Erro na elaboração de documentos inerentes à contratação.	▸ Colegialidade na tomada de decisões; ▸ Nomeação de júris diferenciados para cada procedimento concorrencial, com rotatividade; ▸ Publicitação dos documentos de decisão, designadamente atas, do procedimento; ▸ Adequação fundamentada dos métodos de seleção ao perfil do posto de trabalho/cargo a ocupar; ▸ Atualização do manual que proceda à definição detalhada da tramitação de todo procedimento; ▸ Regulamentação do recrutamento de docentes convidados, com estabelecimento de critérios objetivos de recrutamento e privilegiando a criação de bolsas de recrutamento concorrenciais; ▸ Medidas de segurança relativamente ao acesso ao mapa-base de contratação de docentes convidados restrito a um número limitado e reduzido de trabalhadores.

▸ Processamentos diversos no âmbito de remunerações, abonos variáveis, descontos e contribuições.	▸ Risco do deficiente processamento das remunerações, abonos variáveis, descontos e contribuições, nomeadamente através de pagamentos indevidos.	▸ Promoção de sistemas de controlo interno: folha de processamento dos vencimentos e de ajudas de custo deve ser objeto de conferência, intermédia e final, numa base de amostragem, em meses sorteados, no sentido de confirmar a adequação das remunerações processadas e dos respetivos descontos; ▸ Validação do processamento com os valores cabimentados e com os processamentos anteriores, ao nível do CGR-COC e do CGR-RH, respetivamente; ▸ Promoção e divulgação entre os trabalhadores das regras legais aplicáveis anualmente ao abrigo da Lei do Orçamento de Estado; ▸ Definição detalhada, através da normalização de procedimentos aprovados, da tramitação dos processos.
▸ Instrução de requerimentos dos trabalhadores, nomeadamente, justificações de faltas, requerimentos de licenças, requerimentos de acumulação de funções, requerimentos de equiparação a bolseiro, entre outros.	▸ Risco de redução da qualidade e erro na informação prestada e no apoio técnico e administrativo com vista à tomada de decisão pelo órgão competente.	▸ Promoção de sistemas de controlo interno: conferência das análises aos pedidos, numa base de amostragem; ▸ Definição detalhada da tramitação dos processos; ▸ Distribuição dos processos por várias fases e intervenientes; ▸ Formação contínua dos trabalhadores na área de legislação laboral; ▸ Segregação de funções quanto à temática a tratar.

▸ Elaboração do mapa de pessoal; ▸ Elaboração do mapa de férias; ▸ Elaboração de mapas de reporte interno e externo; ▸ Controlo das situações acumulação de funções e de dedicação exclusiva; ▸ Controlo e verificação das deslocações em serviço.	▸ Risco de falhas no registo da informação nas bases de dados do pessoal; ▸ Risco de redução da qualidade e erro na informação prestada e no apoio técnico e administrativo com vista à tomada de decisão pelo órgão competente; ▸ Risco do deficiente processamento dos valores devidos a título de ajudas de custo e deslocações, nomeadamente através de pagamentos indevidos.	▸ Promoção de sistemas de controlo interno: conferência, numa base de amostragem; ▸ Definição detalhada da tramitação dos processos; ▸ Elaboração de normas que fixem os procedimentos e condições de autorização dos pedidos; ▸ Ampla divulgação dos regimes de acumulações de funções e de dedicação exclusiva; ▸ Cruzamento de informação.
▸ Gestão dos processos individuais dos trabalhadores; ▸ Organização e manutenção dos processos internos de âmbito laboral.	▸ Risco de falhas no registo de informação nas bases de dados dos processos individuais dos trabalhadores; ▸ Risco de acesso indevido às informações pessoais e quebra de sigilo.	▸ Implementação de medidas de segurança nos arquivos físicos e informáticos dos processos individuais; ▸ Acesso restrito dos processos individuais aos trabalhadores do CGR-RH.

ÁREA: CGR-APR, CMM, COC Atividades sensíveis	**RISCOS DE CORRUPÇÃO E DE INFRAÇÕES CONEXAS**	**PROCEDIMENTOS PREVENTIVOS A ADOTAR**
▸ Elaboração do orçamento e outros documentos de prestação de contas; ▸ Elaboração de pedidos de libertação de crédito; ▸ Elaboração das relações de documentos de despesa a submeter a aprovação.	▸ Risco da perda de qualidade da informação prestada, com possibilidade de erro, e do apoio técnico e administrativo prestado com vista à tomada de decisão pelos órgãos de gestão; ▸ Risco de deficiente qualidade da informação financeira prestada a entidades externas; ▸ Risco de falhas na aplicação de normas, procedimentos e regulamentos de natureza financeira; ▸ Risco de afetação da qualidade de prestação de contas e da informação contabilística.	▸ Adotar sistemas de controlo interno: conferência, de forma aleatória, numa base de amostragem, aos documentos financeiros; ▸ Promover a conferência da informação intermédia e final; ▸ Analisar e rever a execução dos procedimentos legais e dos de controlo interno; ▸ Acompanhar, supervisar e controlar a execução das medidas previstas nos procedimentos de controlo interno; ▸ Promover a segregação de funções e estabelecer a responsabilidade pelas operações; ▸ Estabelecer medidas de controlo de prazos.
▸ Controlo da regularidade financeira das receitas e despesas; ▸ Controlo das operações bancárias; ▸ Conferências de valores; ▸ Pagamentos e arrecadação de receita.	▸ Risco de perda de valores ativos; ▸ Risco de desvio de dinheiro e valores; ▸ Risco de falhas na aplicação de normas, procedimentos e regulamentos de natureza financeira.	▸ Conferir, diariamente, os valores recebidos, com folhas de caixa discriminativas, pelo coordenador do serviço ou trabalhador designado para tal, que não tenha efetuado recebimentos; ▸ Promover a conferência da informação intermédia e final; ▸ Promover sistemas automáticos de controlo, com verificação aleatória de registos.

▸ Planificação, organização e coordenação da execução da contabilidade, segundo os planos de contas oficialmente aplicáveis.	▸ Risco do deficiente processamento das operações contabilísticas; ▸ Risco de falhas na aplicação de normas, procedimentos e regulamentos de natureza financeira;	▸ Promover a conferência da informação intermédia e final; ▸ Estabelecer medidas de controlo de prazos; ▸ Acompanhar e supervisar os procedimentos e operações contabilísticas; ▸ Promover a formação contínua dos trabalhadores.
▸ Assegurar a gestão previsional de stocks; ▸ Elaborar e atualizar o inventário.	▸ Risco de ineficácia no cumprimento dos objetivos dos órgãos, serviços e gabinetes; ▸ Risco de perda de valores ativos.	▸ Analisar e rever a execução dos procedimentos estabelecidos no sistema de controlo interno; ▸ Promover a segregação de funções e a responsabilidade das operações relativas a stocks e inventário; ▸ Validar periodicamente o inventário; ▸ Acesso restrito aos materiais e equipamentos em stock armazenados.
▸ Instrução de procedimentos pré-contratuais de aquisição ou alienação de bens e serviços; ▸ Acompanhamento da execução dos contratos.	▸ Risco de violação dos deveres de transparência, isenção e imparcialidade; ▸ Risco de supressão de fases do procedimento necessários (ex. cabimentação e autorização prévias da despesa pelas entidades competentes); ▸ Risco de deficiente gestão dos processos de aquisição de bens / serviços;	▸ Promover a colegialidade na tomada de decisões; ▸ Nomear júris diferenciados e com rotatividade em cada procedimento concorrencial; ▸ Atualizar o manual que procede à definição detalhada da tramitação de todos os procedimentos; ▸ Publicitar os documentos de tomada de decisão, designadamente atas relativas ao procedimento;

	▸ Risco de erro na elaboração de documentos inerentes à contratação; ▸ Risco de ineficácia no cumprimento dos objetivos dos órgãos, serviços e gabinetes.	▸ Adequar os métodos de seleção das candidaturas/propostas a cada procedimento; ▸ Verificação aleatória de procedimentos; ▸ Medidas de segurança relativamente ao acesso às plataformas eletrónicas de contratação a um número limitado e reduzido de trabalhadores; ▸ Proceder à avaliação de fornecedores.
▸ Organizar e manter atualizados os processos e documentos de âmbito contabilístico; ▸ Elaboração de mapas de reporte interno e externo.	▸ Risco de falhas no registo da informação contabilística; ▸ Risco de redução da qualidade e erro na informação prestada e no apoio técnico e administrativo com vista à tomada de decisão pelos órgãos de gestão e entidades externas.	▸ Promover sistemas de controlo interno: conferência das análises aos pedidos, numa base de amostragem; ▸ Triangular a informação relevante relacionada com os processos contabilísticos; ▸ Implementar medidas de segurança nos arquivos físicos e informáticos dos processos contabilísticos; ▸ Limitar o acesso dos processos contabilísticos aos trabalhadores do CGR-APR, CMM, COC.

ÁREA: SAAE Atividades sensíveis	**RISCOS DE CORRUPÇÃO E DE INFRAÇÕES CONEXAS**	**PROCEDIMENTOS PREVENTIVOS A ADOTAR**
▸ Emissão de documentos.	▸ Risco de falhas e erro nos dados certificados documentalmente.	▸ Elaborar e atualizar procedimentos e normas para a emissão de declarações e certidões; ▸ Promover a segregação de funções entre o trabalhador que redige o documento e o que o confere e assina; ▸ Concentrar a maior quantidade possível de informação numa única base, de acesso e consulta simplificada; ▸ Adotar sistemas de controlo interno: conferência, de forma aleatória, numa base de amostragem, a um número mínimo mensal/anual de documentos emitidos.
▸ Receção de candidaturas; ▸ Efetivação de matrículas e inscrições de estudantes; ▸ Registo de classificações; ▸ Aplicação do regime de prescrição da matrícula; ▸ Registo de creditações.	▸ Risco de falhas no registo da informação nas bases de dados académicas; ▸ Risco de redução da qualidade e erro na informação prestada e no apoio técnico e administrativo com vista à tomada de decisão pelo órgão competente; ▸ Risco de erro no procedimento com efeitos jurídicos relevantes para a instituição e para o estudante.	▸ Adotar sistemas de controlo interno: conferência, de forma aleatória, numa base de amostragem; ▸ Detalhar a tramitação dos processos; ▸ Elaborar normas que fixem os procedimentos e as condições de autorização dos requerimentos; ▸ Divulgar os regimes aplicáveis aos estudantes; ▸ Concentrar, numa única base, a maior quantidade possível de informação; ▸ Simplificar o acesso e consulta às bases de dados existentes; ▸ Promover a colaboração e troca de informação interna entre serviços e gabinetes; ▸ Triangular a informação disponível.

▸ Instrução e tratamento de requerimentos de âmbito académico	▸ Risco de redução da qualidade e erro na informação prestada e no apoio técnico e administrativo com vista à tomada de decisão pelo órgão competente.	▸ Adotar sistemas de controlo interno: conferência, de forma aleatória, numa base de amostragem, aos requerimentos académicos tratados; ▸ Detalhar a tramitação dos processos; ▸ Promover a segregação de funções nas várias fases dos processos de âmbito académico; ▸ Promover formação contínua dos trabalhadores na área de gestão académica e ensino superior.

ÁREA: EAM Atividades sensíveis	**RISCOS DE CORRUPÇÃO E DE INFRAÇÕES CONEXAS**	**PROCEDIMENTOS PREVENTIVOS A ADOTAR**
▸ Conservação da documentação	▸ Risco de deterioração dos documentos, por agentes naturais.	▸ Controlar os níveis de temperatura e humidade ambiental; ▸ Monitorizar as rotinas periódicas de controlo de pragas e de aspiração de pós e poeiras nos arquivos de documentação; ▸ Monitorizar o funcionamento dos sistemas de alerta contra incêndios.
	▸ Risco de deterioração dos documentos por ação humana.	▸ Acondicionar os documentos, utilizando sistemas e materiais adequados ao manuseamento e consulta dos mesmos; ▸ Acondicionar, conservar e restaurar os documentos com valor histórico.

ÁREA: CIT Atividades sensíveis	**RISCOS DE CORRUPÇÃO E DE INFRAÇÕES CONEXAS**	**PROCEDIMENTOS PREVENTIVOS A ADOTAR**
▸ Autenticação e autorização de acesso a serviços e a bases de dados	▸ Risco de perda, modificação ou adulteração de informação por intrusão no sistema.	▸ Monitorizar os procedimentos de autenticação e de controlo dos acessos aos recursos e serviços de tecnologias de informação disponibilizados; ▸ Centralizar a gestão do controlo de acessos e autenticação numa ferramenta de gestão de identidades; ▸ Rever, periodicamente, os critérios de definição dos perfis de acesso recursos e serviços; ▸ Classificar a informação em termos de confidencialidade e divulgação; ▸ Assegurar a autorização, autenticidade e não repudiação de transações eletrónicas com terceiros; ▸ Estabelecer e investir de forma continuada numa infraestrutura de prevenção, deteção e correção de software; ▸ Aplicar medidas de segurança aos pontos de controlo de rede e de regulação do tráfego de dados; ▸ Implementar mecanismos de autenticação forte (certificados digitais) e outras medidas que reforcem a segurança das credenciais de acesso utilizadas; ▸ Definir e implementar sistemas de garantia de integridade de logs.

▸ Administração e manutenção de suporte, sistemas, redes e comunicações	▸ Risco de acesso indevido a informação, por intrusão; ▸ Adulteração e destruição de dados; ▸ Adulteração das políticas de segurança.	▸ Definir políticas para a contratação de sistemas tecnológicos; ▸ Definir e implementar sistemas de garantia de integridade de logs; ▸ Definir metodologias de controlo e de delegação de acessos em multicamadas.
	▸ Risco de não contratualização de níveis de serviço necessários em áreas tecnológicas dependentes de infraestruturas externas.	▸ Rever de forma continuada os níveis de serviços com entidades/fornecedores externos tendo por base requisitos de disponibilidade, continuidade e segurança; ▸ Monitorizar e comunicar as vulnerabilidades encontradas no cumprimento dos níveis de serviço acordados/contratualizados; ▸ Utilizar ferramentas automáticas de deteção e comunicação de incidentes, de acordo com os níveis de serviço definidos.
	▸ Risco de perda do controlo sobre os recursos disponibilizados pelas tecnologias de informação; ▸ Risco de interrupção de serviço contínuo e consequente perda de informação; ▸ Risco de perda do controlo do meio físico e ambiental que rodeia e protege os recursos tecnológicos de acidentes.	▸ Definir os processos e as ferramentas adequadas à medição da utilização e do desempenho dos sistemas e comunicações; ▸ Gerir os ciclos de vida das infraestruturas tecnológicas, para aquisição, manutenção e abate das mesmas; ▸ Identificar, classificar e monitorizar os componentes mais críticos da infraestrutura tecnológica; ▸ Estabelecer sistemas de redundância; ▸ Controlar, monitorizar e corrigir as condições do meio físico e ambiental para o data center;

- Assegurar o controlo dos acessos físicos ao data center, bem como a realização de inspeções físicas regulares aos sistemas de deteção de incidentes e de controlo do meio ambiente;
- Definir procedimentos de salvaguarda (backup) e de recuperação/reconstrução (restore) da informação relevante;
- Assegurar os procedimentos de segurança de acesso no que toca ao armazenamento dos meios de salvaguarda;
- Testar periodicamente os sistemas redundantes a falhas.