PLANO DE PREVENÇÃO DE RISCOS DE GESTÃO

(INCLUINDO OS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS)

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data: 2022-01-14

ÍNDICE

1. INTRODUÇÃO

Todas as organizações estão sujeitas a fatores, internos ou externos, cuja ocorrência pode gerar incertezas na implementação da estratégia e na concretização dos seus objetivos. Quando o efeito desta incerteza compromete a concretização dos objetivos da organização está-se perante um "risco". Este conceito está subjacente à definição de risco apresentada pelo ***Committee of Sponsoring Organizations of the Treadway Commission*** **(COSO)**, que considera o risco como a *possibilidade de ocorrência de um evento que afete negativamente o cumprimento de objetivos e que impeça a criação de valor ou mesmo a destruição daquele existente*.

Todas as entidades, independentemente do seu setor de atividade, enfrentam diversas incertezas, que tanto geram riscos, como oportunidades. Nas instituições de saúde, o efeito negativo destas incertezas é mais impactante, atendendo àquele que é o seu *core business*: **a prestação de cuidados de saúde, com eficiência, qualidade, em tempo útil e a custos socialmente comportáveis, à população da sua área de influência e a todos os cidadãos em geral**.

Nestas instituições, a dimensão do risco não se limita fundamentalmente à manutenção da sua viabilidade financeira, existindo outras dimensões de risco que podem condicionar o cumprimento do seu *major* objetivo (a prestação de cuidados de saúde), nomeadamente a regulamentação legal, muitas vezes restritiva na área financeira e de recursos humanos, as alterações nas condições demográficas, que determinam mudanças nas áreas de prestação de cuidados, ou ainda a obrigação de prestar assistência ao utente, independentemente da capacidade deste em pagar os atos médicos associados.

É neste contexto, que a gestão de riscos constitui um elemento fundamental na gestão estratégica de qualquer organização, em particular nas instituições de saúde, na medida em que permite identificar, avaliar e gerir riscos, num ambiente de incertezas, minimizando as consequências negativas no seu desempenho e, consequentemente, assegurando um nível razoável de garantia na concretização dos seus objetivos.

O ***Plano de Prevenção de Riscos de Gestão (incluindo os Riscos de Corrupção e Infrações Conexas)*** (PPRG) do Centro Hospitalar Universitário Cova da Beira, EPE (CHUCB, EPE) foi desenvolvido por forma a dar cumprimento à **Recomendação n.º 3/2015, de 1 de julho**, que estabelece a identificação exaustiva dos riscos de gestão, incluindo os riscos de corrupção e infrações conexas, bem como as correspondentes medidas preventivas.

Pretende-se com este documento:

- Assegurar a implementação da Recomendação n° 3/2015, de 1 de julho, do Conselho de Prevenção da Corrupção;
- Implementar um modelo de gestão de riscos tendo por base a **Estrutura Integrada de Gestão de Riscos Empresariais (ERM)[1] do COSO**[2];
- Gerir os riscos operacionais e de gestão mais expressivos, incluindo, os riscos de corrupção e infrações conexas, relativamente a cada atividade;
- Apresentar medidas que visem a mitigação dos riscos identificados, no sentido do cumprimento dos objetivos do CHUCB;
- Identificar os responsáveis envolvidos na gestão do plano.

O presente PPRG entra em vigor após aprovação do Conselho de Administração do CHUCB, EPE.

[1] Tradução livre: *Enterprise Risk Management* (ERM)

[2] *Committee of Sponsoring Organizations of the Treadway Commission* (COSO).

2. ENQUADRAMENTO, METODOLOGIA E ESTRUTURA

O PPRG constitui uma ferramenta de reforço ao **Sistema de Controlo Interno** do Centro Hospitalar Universitário Cova da Beira, EPE, assumindo um carácter transversal à instituição no âmbito da eliminação e prevenção de riscos de gestão em todas as áreas em que se identifica a sua necessidade, bem como dos riscos das atividades no âmbito da corrupção, infrações conexas, de situações que possam consubstanciar eventuais conflitos de interesse e de outros que, por ação ou omissão dos membros dos órgãos estatutários, trabalhadores ou fornecedores, possam indiciar violação de princípios e disposições legais, regulamentares e deontológicas, comprometer o património da instituição ou dos utentes ou a imagem do CHUCB.

O Sistema de Controlo Interno (SCI) compreende um conjunto de estratégias, políticas, processos, regras e procedimentos que garantam um desempenho eficiente da atividade e a utilização racional dos recursos, bem como o respeito pelas disposições legais e regulamentares aplicáveis, pelas regras internas e estatutárias, com base num adequado **Sistema de Gestão de Risco** (SGR), assegurando a respetiva adequação e eficácia em todas as áreas de intervenção.

No sentido de garantir uma atividade de âmbito nacional no âmbito da prevenção da corrupção e infrações conexas, foi criado o Conselho de Prevenção da Corrupção (CPC), uma entidade administrativa independente que funciona junto do Tribunal de Contas e tem como fim desenvolver uma atividade exclusivamente orientada para a prevenção da corrupção (artigo 1º da Lei nº 54/2008, de 4 de setembro) e que emitiu, em julho de 2009, a **Recomendação n.º 1/2009**, vinculando os órgãos máximos das entidades gestoras de dinheiros, valores ou patrimónios públicos, independentemente da sua natureza, a elaborar Planos de Prevenção de Riscos de Corrupção e Infrações Conexas. A esta recomendação seguiu-se a determinação da obrigatoriedade de publicitação desses planos no sítio da internet das entidades, através da **Recomendação do CPC n.º 1/2010**, de 7 de abril.

A 7 de Novembro de 2012,0 CPC divulgou a **Recomendação n.º 5/2012**, em que alerta para a necessidade de existência de mecanismos de acompanhamento e de gestão de conflitos de interesses, instrumento fundamental na promoção de uma cultura de rigor e transparência, tendo como intuito prevenir a ocorrência de situações de risco desta natureza.

Em 2013 são reforçadas as determinações das Recomendações do CPC, relativamente ao dever de cumprir a legislação e a regulamentação em vigor relativas à prevenção da corrupção, com a publicação do Decreto-Lei n.º 133/2013[3], de 3 de outubro, (**art.º 46, do DL 133/2013, de 3 de Outubro, alterado pela Lei n.º 42/2016, de 28 de dezembro)** ao determinar o cumprimento deste desiderato pelas empresas públicas, estabelecendo ainda a obrigatoriedade de elaboração anual de um relatório identificativo das ocorrências, ou risco de ocorrências, dos factos[4] mencionados na alínea a) do n.º 1 do artigo 2.º da Lei n.º 54/2008, de 4 de setembro, bem como a sua publicitação no sítio da Internet dessas entidades.

Outra matéria objeto de recomendações pelo CPC foi a área da contratação pública, que na sua **Recomendação n.º 1/2015**, de 7 de Janeiro, especificamente dirigida às entidades com responsabilidades na celebração de contratos públicos, sublinha a necessidade de reforçar a prevenção de riscos de corrupção na contratação pública, através da identificação, prevenção e gestão de riscos de corrupção e infrações conexas nos contratos públicos, quanto à sua formação e execução, salvaguardar a transparência nos procedimentos de contratação pública, reduzindo o recurso ao ajuste direto, bem como a implementação de mecanismos de controlo de eventuais conflitos de interesses.

Incentivando ao reforço de uma cultura de prevenção de riscos e incremento da transparência e do rigor, na gestão pública e na qualidade do serviço público, o CPC aprovou a **Recomendação n.º 3/2015**, de 1 de julho, que reitera a necessidade de adoção e divulgação dos Planos de Prevenção de Riscos de Corrupção e Infrações Conexas, considerando que estes "***devem identificar de modo exaustivo os riscos de gestão, incluindo os de corrupção, bem como as correspondentes medidas preventivas***." Esta recomendação determina ainda a identificação dos riscos relativamente às funções, ações e procedimentos realizados por todas as unidades da estrutura orgânica das entidades, estabelecendo ainda que os Planos devem designar responsáveis setoriais e um responsável geral pela sua execução e monitorização, bem como pela elaboração dos correspondentes relatórios anuais.

[3] Regime Jurídico do Setor Público Empresarial

[4] "Factos de corrupção activa ou passiva, de criminalidade económica e financeira, de branqueamento de capitais, de tráfico de influência, de apropriação ilegítima de bens públicos, de administração danosa, de peculato, de participação económica em negócio, de abuso de poder ou violação de dever de segredo, bem como de aquisições de imóveis ou valores mobiliários em consequência da obtenção ou utilização ilícitas de informação privilegiada no exercício de funções na Administração Pública ou no sector público empresarial"

Para além de dar cumprimento às recomendações do CPC, o presente **Plano de Prevenção de Riscos de Gestão** (PPRG) constitui um reforço do alinhamento do Sistema de Controlo Interno do CHUCB, com o Sistema de Gestão de Riscos da instituição, estabelecendo uma adequada gestão e controlo dos riscos da atividade, por forma a garantir, com razoabilidade, a continuidade, segurança e qualidade da prestação de cuidados de saúde, utilizando eficazmente os seus ativos e recursos.

Nesse sentido, e em conformidade com o disposto na **Recomendação n.º 3/2015**, de 1 de julho, foram identificadas como áreas de maior exposição a potenciais riscos operacionais, de corrupção, de infrações conexas e de conflito de interesses, as seguintes:

- Financeiros;
- Higiene, Saúde e Segurança no Trabalho;
- Instalações e Equipamentos;
- Logística Hospitalar;
- Recursos Humanos;
- Sistemas e Tecnologias da Informação.

Para estes Serviços são identificados os riscos das atividades no âmbito da corrupção, infrações conexas, de situações que possam consubstanciar eventuais conflitos de interesse e de outros que, por ação ou omissão dos membros dos órgãos estatutários, trabalhadores ou fornecedores, possam comprometer os processos de gestão e de tomada de decisão, o cumprimento de disposições legais, regulamentares e deontológicas, a salvaguarda do património da instituição ou dos utentes ou constituir um prejuízo à imagem do CHUCB.

Os riscos identificados são avaliados de acordo com a sua probabilidade de ocorrência e impacto previsto, descrevendo-se os procedimentos estabelecidos para monitorizar e mitigar potenciais eventos de risco, com respetiva identificação dos responsáveis pela sua execução, processo este suportado numa ferramenta de controlo e avaliação de riscos (Matriz de Riscos e Controlos).

Esta matriz elenca a relação de todos os controlos que visam mitigar os riscos associados a cada processo de negócio e de suporte, possibilitando a definição do grau de importância dos riscos avaliados, em função da análise da capacidade de os controlos adotados mitigarem os riscos, constituindo um instrumento de suporte à decisão e gestão dos riscos, pelo Conselho de Administração, e uma ferramenta de monitorização da eficácia da gestão de risco, pelos Serviços.

O Sistema de Gestão de Risco proposto ao Conselho de Administração tem por base por base as orientações técnicas emanadas pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), concretamente, as vertidas no documento intitulado "*Enterprise Risk Management* (ERM)— *Integrated Framework*", de 2004.

Foram ainda considerados os referenciais de gestão de risco da NP ISO 31000:2009 (norma portuguesa de Gestão do Risco – Princípios e linhas de orientação) e da FERMA (*Federation of European Risk Management Associations*).

Em termos de estrutura, na elaboração do PPRG foram adotadas, com a respetiva adequação, as orientações plasmadas no Guião do CPC, de Janeiro de 2015, para os Planos de Prevenção de Riscos, documento que propõe a seguinte disposição:

- ✓ **Atribuições da entidade, organograma e identificação dos responsáveis:**

"Caracterização genérica das atribuições da entidade (a razão da sua existência) e da estrutura orgânica que apresenta, com identificação dos responsáveis."

- ✓ **Identificação dos riscos de corrupção e infrações conexas:**

"Tendo em conta as funções da entidade, devem ser identificados e caracterizados por unidade orgânica os respetivos potenciais riscos de corrupção e infrações conexas.
Estes riscos devem ser classificados segundo uma escala de risco (…), em função dos graus de probabilidade de ocorrência e de gravidade da consequência (…). Por sua vez, esta classificação deverá ser aferida a partir da própria caracterização de cada uma das funções."

- ✓ **Medidas preventivas dos riscos:**

"Identificados os riscos, devem ser indicadas as medidas que previnam a sua ocorrência, tais como mecanismos de controlo interno, segregação de funções, declarações de interesses, definição prévia de critérios gerais e abstratos de concessão de benefícios públicos, criação de gabinetes de auditoria interna em especial nas entidades de maior dimensão, controlo efetivo das situações de acumulações de funções públicas com atividades privadas e respetivos conflitos de interesses. (…) Neste âmbito podem ser consideradas as orientações técnicas de gestão de risco da FERMA, do COSO, bem como de outros organismos cujas indicações possam ser consideradas de utilidade."

- ✓ **Estratégias de aferição da efetividade, utilidade, eficácia e eventual correção das medidas propostas:**

"Os Planos de Prevenção de Riscos de Corrupção e Infrações Conexas são instrumentos de gestão dinâmicos, pelo que devem ser acompanhados na sua execução, elaborando-se, pelo menos anualmente, um relatório de execução e refletindo-se sobre a necessidade da sua atualização."

Considerando a abrangência do PPRG, em consonância com as Recomendações do CPC, e a especificidade das áreas envolvidas, bem como a transversalidade dos riscos na instituição, este plano foi elaborado com a participação dos responsáveis pelos diversos Serviços, cujo envolvimento em todo o processo pode contribuir para uma ação mais efetiva e atempada na prevenção dos riscos operacionais ou dos riscos apercebidos de corrupção, de infrações conexas e de conflito de interesses.

Em termos de operacionalização do PPRG, a responsabilidade é partilhada pelos vários intervenientes, da forma como a seguir se define:

a) O Conselho de Administração, a quem compete, enquanto órgão de gestão de topo, a aprovação do modelo, das regras e dos critérios de gestão dos riscos;
b) O Serviço de Auditoria Interna, a quem, por Lei, incumbe a avaliação e melhoria contínua de todos os processos de controlo interno e de gestão de riscos nos domínios contabilístico, financeiro, operacional, informático e de recursos humanos;

c) Os responsáveis dos Serviços, a quem cabe a definição e uniformização das políticas e procedimentos, a utilização racional de recursos e a gestão operacional da respetiva unidade orgânica, com o dever de identificar os riscos que afetam as atividades do serviço, a avaliação dos níveis de exposição a esses riscos e a definição de planos de melhoria, que conduzam a um ambiente de controlo adequado;

d) Todos os colaboradores, em geral, que pelo cumprimento dos deveres e valores a que estão vinculados pela relação jurídica de emprego de que são titulares, devem reportar superiormente, os riscos e irregularidades identificados no desempenho das suas funções ou para os quais sejam alertados por colegas, utentes ou outros, contribuindo dessa forma para a identificação ou avaliação de riscos, ou adoção de outras medidas necessárias à realização da gestão de riscos.

Importa ainda realçar que a abrangência do presente PPRG não se restringe às áreas consideradas, mas que apenas foram contemplados os aspetos julgados mais relevantes nesta matéria, salvaguardando-se a tomada de decisões em função da legislação vigente, dos procedimentos em vigor e das obrigações contratuais a que a instituição está vinculada.

3. OPERACIONALIZAÇÃO, DIVULGAÇÃO E MONITORIZAÇÃO DO PLANO

Atendendo à sua importância enquanto instrumento de gestão, a operacionalização do PPRG incumbe às direções de cada Serviço, com as seguintes responsabilidades:

a) A sua implementação e manutenção, na parte que lhe corresponde, com a respetiva elaboração de um relatório anual, a remeter ao Conselho de Administração e Serviço de Auditoria Interna, que deve reportar as seguintes informações:

   i. Identificação das medidas de prevenção e mitigação de riscos adotadas e aquelas a implementar, relativamente ao período em análise;

   ii. Avaliação da adequabilidade e eficácia das medidas, analisando o efeito obtido ao nível da probabilidade de ocorrência e do impacto previsto;

   iii. Justificação de eventuais atrasos face à previsão da introdução das medidas ou da sua não implementação;

iv. Identificação e avaliação de novos fatores de risco, em função de alterações nos objetivos ou na estratégia, ou ainda resultantes da introdução de atividades, com a respetiva definição das medidas a adotar na prevenção e mitigação desses novos riscos.

b) A iniciativa de apresentação ao Serviço de Auditoria Interna, de propostas de correção e atualização do PPRG, quando se considerar necessário.

A eficácia da gestão de riscos está dependente da qualidade da informação produzida e comunicada para suporte à tomada de decisões, em particular no que concerne à gestão e controlo das atividades da organização, e nas funções e responsabilidades de todos os colaboradores nas respostas aos riscos. Como tal, deve promover-se a comunicação e divulgação do presente PPRG, transversalmente a toda a instituição, sensibilizando os colaboradores para as matérias relacionadas com a prevenção de riscos operacionais, de conflitos de interesse, de corrupção e infrações conexas. Por conseguinte, são de realçar, designadamente, as seguintes medidas:

- Disponibilização do PPRG no portal da intranet e no sítio da internet do Centro Hospitalar Universitário Cova da Beira, EPE;
- Promoção de ações de divulgação do PPRG, com a respetiva sensibilização para as matérias aí plasmadas.

Para efeitos de monitorização e aferição da efetividade, utilidade e eficácia do PPRG, este será objeto de acompanhamento anual pelo Serviço de Auditoria Interna, com as seguintes responsabilidades:

i. Elaboração de um relatório anual de execução do PPRG, com base na informação prestada pelos Serviços, a remeter ao Conselho de Administração do Centro Hospitalar Universitário Cova da Beira, EPE, ao Conselho de Prevenção da Corrupção e à Tutela.

ii. Atualização do PPRG, em função dos desajustamentos identificados pelos Serviços, e pelas ações de avaliação desenvolvidas pelo Serviço de Auditoria Interna, bem como pela identificação de necessidades de melhoria do mesmo, em função da evolução dos resultados alcançados, ou de alterações decorrentes de normativos legais, de orientações internas, ou determinadas por alterações às atividades e respetivos riscos.

iii. Publicitação do relatório de execução do PPRG no sítio da internet do Centro Hospitalar Universitário Cova da Beira, EPE, após sua aprovação pelo Conselho de Administração.

4. CARACTERIZAÇÃO DO CENTRO HOSPITALAR UNIVERSITÁRIO COVA DA BEIRA, EPE

4.1 Identificação da Instituição

O Centro Hospitalar Cova da Beira, SA foi criado a 17 de janeiro de 2000, através do Decreto-Lei nº 426/99 de 21 de Outubro, passando a Sociedade Anónima de capitais exclusivamente públicos, pelo Decreto-Lei nº 288/2002 de 10 de dezembro, tendo sido posteriormente transformado em Entidade Pública Empresarial, pelo Decreto-Lei n.º 93/2005 de 7 de junho, com efeitos a partir de 29 de dezembro de 2005, e Decreto-Lei n.º 233/2005, de 29 de dezembro.

O Centro Hospitalar Universitário Cova da Beira, EPE rege-se pelo seu Regulamento Interno e pela seguinte legislação:

- Regime jurídico e estatutos aplicáveis às unidades de saúde do serviço nacional de saúde (Decreto-Lei nº 18/2017, de 10 de fevereiro);
- Regime jurídico do setor público empresarial (Decreto-Lei n.º 133/2013, de 03 de outubro, com as respetivas alterações);
- Lei de Bases da Saúde (Lei nº 27/2002, de 8 de novembro; Decreto-Lei nº 11/93, de 15 de janeiro, com as respetivas alterações);
- Estatuto do gestor público (Decreto - Lei n.º 71/2007, de 27 de março, com as respetivas alterações);
- Lei geral do trabalho em funções públicas (Lei n.º 35/2014, de 20 de junho, com as respetivas alterações);
- Código do Trabalho (Lei n.º 7/2009, de 12 de fevereiro, com as respetivas alterações);
- Código das Sociedades Comerciais;
- Outras normas especiais e gerais decorrentes do seu objeto social e da Lei.

O Centro Hospitalar Universitário Cova da Beira, E.P.E. é uma unidade do Serviço Nacional de Saúde português composta por duas unidades hospitalares:

- Hospital Pêro da Covilhã, na Covilhã, que integra num edifício adjacente o Departamento de Psiquiatria e Saúde Mental;
- Hospital do Fundão, no Fundão.

Hospital Pêro da Covilhã

Departamento de Psiquiatria e Saúde Mental

Hospital do Fundão

O Centro Hospitalar Universitário Cova da Beira é uma instituição moderna e inovadora, de referência na prestação de cuidados de saúde de excelência às populações residentes nos Concelhos de Belmonte, Covilhã, Fundão e parte do Concelho de Penamacor, em cumprimento do estabelecido na Carta de Referência Hospitalar do Ministério da Saúde.

Contudo, o Centro Hospitalar Universitário Cova da Beira atende nos seus serviços todos os cidadãos que desejem ser tratados nesta instituição, o que se traduz na população residente no território nacional.

População abrangida:

População Residente		
Censos 2011[5]	Continente	10.047.621
	Centro	2.327.755
	Cova da Beira	87.869
	Área Influência CHCB	93.551
	Penamacor	5.682
	Belmonte	6.859
	Covilhã	51.797
	Fundão	29.213

De acordo com o Protocolo nº 11/2001, publicado em Diário da República, II Série de 16 de abril de 2001, o Centro Hospitalar Universitário Cova da Beira apresenta-se como Hospital Nuclear da Faculdade de Ciências da Saúde da Universidade da Beira Interior (UBI), passando o seu compromisso pelo desenvolvimento de ensino e investigação de alta responsabilidade e qualidade. O seu comprometimento revela-se também na participação no ensino pré e pós-graduado em colaboração com as Escolas Superiores de Enfermagem e Escolas Superiores de Tecnologia de Saúde e promoção, acompanhamento, e desenvolvimento de projetos de investigação clínica em colaboração com entidades externas.

4.2 Missão, Princípios, Valores e Visão

Tendo por base os seus princípios e valores, que se encontram difundidos pelos colaboradores, o Centro Hospitalar Universitário Cova da Beira assume-se como uma Instituição de referência, pela qualidade das práticas clínicas e como um centro integrado de prestação de cuidados e de promoção de competências, na investigação e no ensino das ciências da saúde.

[5] Fonte: INE: Censos 2011. Resultados definitivos.

O trabalho contínuo pela qualidade pretende contribuir para alcançar aquela que é a sua **Visão**: "***Ser uma Instituição de referência a nível regional e nacional, pela qualidade na prestação dos cuidados de saúde e pelo seu contributo para a investigação e o ensino na área da saúde***".

A missão, princípios e valores do Centro Hospitalar Universitário Cova da Beira encontram-se plasmados no seu Regulamento Interno, e que se traduzem nas seguintes asserções:

Missão

Prestar cuidados de saúde com eficiência, qualidade, em tempo útil e a custos socialmente comportáveis, à população da sua área de influência, e a todos os cidadãos em geral; desenvolver ensino de alta qualidade como Hospital Nuclear da Faculdade de Ciências da Saúde da Universidade da Beira Interior; participar no ensino pré e pós graduado, em colaboração com as Escolas Superiores de Enfermagem e Escolas Superiores de Tecnologia de Saúde e outras com as quais venham a ser celebrados Protocolos, proporcionando um ensino de excelência nas várias áreas de prestação de cuidados de saúde; promover, acompanhar e desenvolver projetos de investigação clínica de iniciativa própria ou em colaboração com entidades externas.

Princípios

Legalidade, Igualdade, Proporcionalidade, Colaboração e da Boa-fé; Humanismo; Respeito pela dignidade humana; Qualidade na ação, assegurando os melhores níveis de serviço e resultados; Competência e responsabilidade.

Valores

A atitude centrada no doente e na promoção da saúde da comunidade, respeitando os valores do doente da família; a cultura de excelência técnica, científica e do conhecimento, como um valor a prosseguir continuamente; a cultura interna de multidisciplinaridade e de bom relacionamento no trabalho e a Responsabilidade Social, contribuindo para a otimização na utilização dos recursos e da capacidade instalada.

4.3 Órgãos de Administração, Controlo e Supervisão

A estrutura organizativa dos órgãos de administração, controlo e supervisão encontra-se prevista nos termos do disposto no Capítulo II, do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro, que estabelece os princípios e regras aplicáveis às unidades de saúde que integram o Serviço Nacional de Saúde, com a natureza de entidade pública empresarial, bem como os estatutos destas entidades.

4.3.1 Conselho de Administração

O Conselho de Administração do Centro Hospitalar Universitário Cova da Beira é constituído por um Presidente, que acumula as funções de Diretor Clínico, dois Vogais Executivos e um Enfermeiro Diretor, tendo sido nomeados pela Resolução do Conselho de Ministros n.º 99/2019, de 25 de junho de 2019, publicada no Diário da República, 1.ª Série, n.º 119, para um mandato de três anos, "*sob proposta dos Ministros das Finanças e da Saúde",* João José Casteleiro Alves (diretor clínico), Vítor Manuel Alves Mendes da Mota, Sandra Maria Nunes Duarte e Ana Paula Salgueiro Fava de Freitas Rodrigo (enfermeira diretora), respetivamente, para os cargos de presidente e vogais executivos do conselho de administração do Centro Hospitalar Universitário da Cova da Beira, EPE *"cuja idoneidade, experiência e competências profissionais para o desempenho dos cargos são evidenciados nas respetivas notas curriculares, que constam do anexo à presente resolução, dela fazendo parte integrante*."

As competências deste órgão, sem prejuízo de outras competências que lhe sejam conferidas por lei, estão definidas nos art.º 7º a 10º, do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro.

4.3.2 Revisor Oficial de Contas e Fiscal Único

Nos termos do disposto na Secção II, do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro, encontram-se regulados os mandatos do revisor oficial de contas e do fiscal único, estando as suas competências definidas nos artigos 16º e 18º, da referida secção do mesmo decreto-lei, respetivamente.

Contudo, à data atual, não existe nomeação para ROC ou SROC.

4.3.3 Serviço de Auditoria Interna

Os requisitos e competências do Serviço de Auditoria Interna encontram-se determinados na Secção III, do Anexo II do Decreto-Lei n.º 18/2017, de 10 de fevereiro, estando ainda regulada a atividade e funções do Serviço no procedimento interno CHCB.PI.CHCB.172 e nas "Normas Internacionais para a Prática Profissional da Auditoria Interna" do *The Institute of Internal Auditors* (IIA).

4.4 Estrutura Organizacional

O Centro Hospitalar Universitário Cova da Beira, EPE organiza-se em cinco áreas de atuação:

i. Área de Prestação de Cuidados;
ii. Área de Suporte à Prestação de Cuidados;
iii. Área de Apoio à Gestão e Logística Geral;
iv. Área de Inovação, Ensino e Formação;
v. Área de Consultoria.

A **Área de Prestação de Cuidados** está organizada em Departamentos, Serviços e Unidades, sendo cada uma dirigida por responsável próprio, englobando as seguintes funções de prestação de cuidados:

- Internamento (médico e cuidados agudos);
- Cirurgias (em Ambulatório e Bloco Operatório);
- Consultas Externas;
- Hospital de Dia;
- Urgência (Geral e Pediátrica);
- Cuidados Domiciliários;
- Meios Complementares de Diagnóstico e Terapêutica;
- Farmácia;
- Outras prestações de cuidados, designadamente, de Consulta de Telemedicina e Psicologia Clínica.

A **Área de Suporte à Prestação de Cuidados** contempla as seguintes intervenções de apoio:

- Arquivo Clínico;
- Serviço Social;
- Serviços Religiosos.

A Área de Apoio à Gestão e Logística Geral encontra-se organizada por Serviços, contemplando as seguintes estruturas:

- Expediente;
- Financeiros;
- Higiene, Saúde e Segurança no Trabalho;
- Instalações e Equipamentos;
- Logística Hospitalar;
- Recursos Humanos;
- Sistemas e Tecnologias da Informação.

A **Área de Inovação, Ensino e Formação** está organizada em quatro serviços, designadamente:

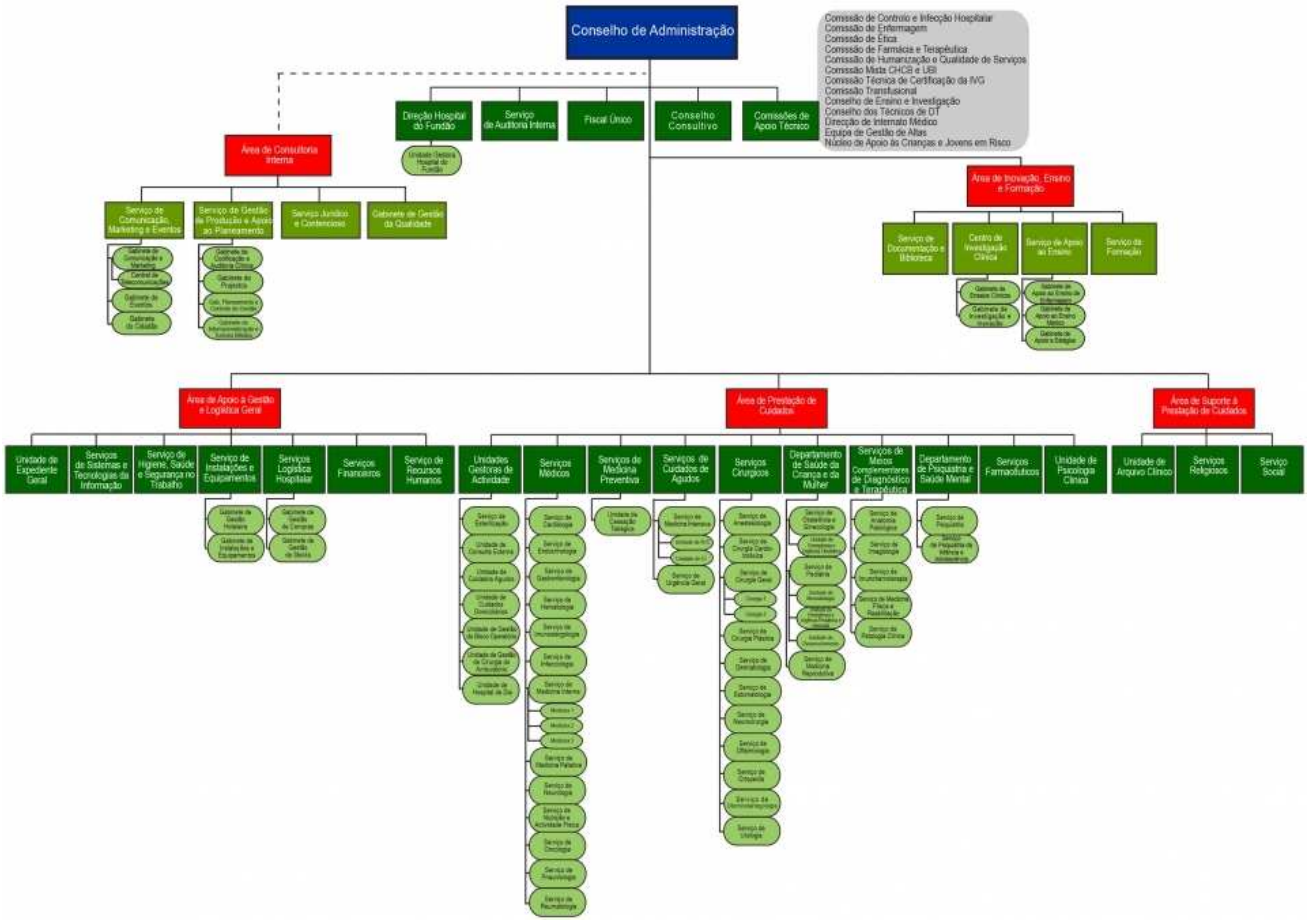
- Serviço de Documentação e Biblioteca;
- Centro de Investigação Clínica;
- Serviço de Apoio ao Ensino;
- Serviço de Formação.

A **Área de Consultoria Interna** é composta pelos seguintes serviços:

- Serviço de Comunicação, Marketing e Eventos;
- Gabinete do Cidadão;
- Serviços de Gestão da Produção e Apoio ao Planeamento;
- Serviço Jurídico e Contencioso;
- Serviço de Gestão da Qualidade.

4.5 Organograma

Na figura seguinte pode ver-se o organograma do Centro Hospitalar Universitário Cova da Beira, homologado pela Administração Regional de Saúde do Centro, em 8 de janeiro de 2015.



5. MODELO DE GESTÃO DE RISCOS

5.1 Enquadramento conceptual

Por forma a garantir a homogeneidade na abordagem a realizar junto dos vários Serviços, considera-se pertinente clarificar e tipificar os conceitos no âmbito da gestão, identificação e avaliação de riscos, incluindo os de corrupção e infrações conexas, bem como do próprio modelo que serve de suporte à metodologia adoptada.

5.1.1 Corrupção e Infrações Conexas

Os Organismos Estratégicos do Controlo Interno da Comunidade dos Países de Língua Portuguesa (OECI - CPLP) elaboraram, em novembro de 2011, um **Guião de boas práticas para a prevenção e combate à corrupção na Administração Pública**, onde consideram que a corrupção "*consiste no uso ilegal (ou socialmente imoral) por parte dos titulares de cargos públicos e dos funcionários públicos ou equiparados do poder político, administrativo, judicial e financeiro que detêm, com o objectivo de transferir valores financeiros ou outras vantagens/benefícios indevidos para determinados indivíduos ou grupos, obtendo por isso qualquer vantagem ilícita (ou socialmente imoral).*".

Neste documento, também se define corrupção, do ponto de vista criminal, como "*A prática de um qualquer acto ou a sua omissão, seja lícito ou ilícito, contra o recebimento ou a promessa de uma qualquer compensação que não seja devida, para o próprio ou para terceiro.*"

Nos termos do Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, alterado e republicado pela Lei n.º 60/2013, de 23 de agosto, indicam-se de seguida os principais ilícitos que podem ser cometidos no exercício de funções públicas e que constituem crimes de corrupção e infrações conexas, previstos e punidos:

1. **Recebimento indevido de vantagem (art.º 372 do Código Penal)**

"1 - O funcionário que, no exercício das suas funções ou por causa delas, por si, ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, que não lhe seja devida, (…).

2 - Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer a funcionário, ou a terceiro por indicação ou conhecimento daquele, vantagem patrimonial ou não patrimonial, que não lhe seja devida, no exercício das suas funções ou por causa delas, (…)."

2. **Corrupção passiva (art.º 373 do Código Penal)**

"1 - O funcionário que por si, ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, ou a sua promessa, para a prática de um qualquer ato ou omissão contrários aos deveres do cargo, ainda que anteriores àquela solicitação ou aceitação (…)"

3. **Corrupção ativa (art.º 374 do Código Penal)**

"1 - Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer a funcionário, ou a terceiro por indicação ou com conhecimento daquele, vantagem patrimonial ou não patrimonial com o fim indicado no n.º 1 do artigo 373.º (…)"

Além destes, o Código Penal prevê ainda outros crimes conexos, destacando-se as infrações conexas que poderão ocorrer no exercício de funções públicas:

4. **Administração danosa no setor público ou cooperativo (art.º 235 do Código Penal)**

"1 - Quem, infringindo intencionalmente normas de controlo ou regras económicas de uma gestão racional, provocar dano patrimonial importante em unidade económica do sector público ou cooperativo (…).

2 - A punição não tem lugar se o dano se verificar contra a expectativa fundada do agente."

5. **Tráfico de influência (art.º 335 do Código Penal)**

"1 - Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, ou a sua promessa, para abusar da sua influência, real ou suposta, junto de qualquer entidade pública, (…).

2 - Quem, por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer vantagem patrimonial ou não patrimonial às pessoas referidas no número anterior para os fins previstos na alínea a) (…).”

6. Peculato (art.º 375 do Código Penal)

“1 - O funcionário que ilegitimamente se apropriar, em proveito próprio ou de outra pessoa, de dinheiro ou qualquer coisa móvel, pública ou particular, que lhe tenha sido entregue, esteja na sua posse ou lhe seja acessível em razão das suas funções, (…).”

7. Peculato de uso (art.º 376 do Código Penal)

“1 - O funcionário que fizer uso ou permitir que outra pessoa faça uso, para fins alheios àqueles a que se destinem, de veículos ou de outras coisas móveis de valor apreciável, públicos ou particulares, que lhe forem entregues, estiverem na sua posse ou lhe forem acessíveis em razão das suas funções, (…).

2 - Se o funcionário, sem que especiais razões de interesse público o justifiquem, der a dinheiro público destino para uso público diferente daquele a que está legalmente afetado, (…).”

8. Participação económica em negócio (art.º 377 do Código Penal)

“1 - O funcionário que, com intenção de obter, para si ou para terceiro, participação económica ilícita, lesar em negócio jurídico os interesses patrimoniais que, no todo ou em parte, lhe cumpre, em razão da sua função, administrar, fiscalizar, defender ou realizar, (…).

2 - O funcionário que, por qualquer forma, receber, para si ou para terceiro, vantagem patrimonial por efeito de acto jurídico-civil relativo a interesses de que tinha, por força das suas funções, no momento do acto, total ou parcialmente, a disposição, administração ou fiscalização, ainda que sem os lesar, (…).

3 – (…) funcionário que receber, para si ou para terceiro, por qualquer forma, vantagem patrimonial por efeito de cobrança, arrecadação, liquidação ou pagamento que, por força das suas funções, total ou parcialmente, esteja encarregado de ordenar ou fazer, posto que não se verifique prejuízo para a Fazenda Pública ou para os interesses que lhe estão confiados.”

9. Concussão (art.º 379 do Código Penal)

"1 - O funcionário que, no exercício das suas funções ou de poderes de facto delas decorrentes, por si ou por interposta pessoa com o seu consentimento ou ratificação, receber, para si, para o Estado ou para terceiro, mediante indução em erro ou aproveitamento de erro da vítima, vantagem patrimonial que lhe não seja devida, ou seja superior à devida, nomeadamente contribuição, taxa, emolumento, multa ou coima, (…)".

10. Abuso de poder (art.º 382 do Código Penal)

"O funcionário que, fora dos casos previstos nos artigos anteriores, abusar de poderes ou violar deveres inerentes às suas funções, com intenção de obter, para si ou para terceiro, benefício ilegítimo ou causar prejuízo a outra pessoa, (…)".

11. Violação de segredo por funcionário (art.º 383 do Código Penal)

"1 - O funcionário que, sem estar devidamente autorizado, revelar segredo de que tenha tomado conhecimento ou que lhe tenha sido confiado no exercício das suas funções, ou cujo conhecimento lhe tenha sido facilitado pelo cargo que exerce, com intenção de obter, para si ou para outra pessoa, benefício, ou com a consciência de causar prejuízo ao interesse público ou a terceiros, (…).

2 - Se o funcionário praticar o facto previsto no número anterior criando perigo para a vida ou para a integridade física de outrem ou para bens patrimoniais alheios de valor elevado (…).

3 - O procedimento criminal depende de participação da entidade que superintender no respetivo serviço ou de queixa do ofendido."

Numa outra vertente, destaca-se o risco de conflitos de interesses no setor público, sendo expectável que os agentes públicos desempenhem os seus deveres com integridade e imparcialidade, não permitindo que os seus interesses privados, preferências ou simpatias influenciem ou comprometam a sua atuação, decisão ou gestão pública.

Nesse sentido, o Conselho de Prevenção da Corrupção (CPC) emitiu uma Recomendação estabelecendo que todas as entidades com natureza pública, ainda que constituídas sob a forma de direito privado, devem dispor de mecanismos de acompanhamento e de gestão de conflito de interesses.

De acordo com essa recomendação considera-se como conflito de interesses no setor público:

12. Conflitos de interesses (Recomendação do CPC n.º 1/2012, de 7 de novembro)

"(…) qualquer situação em que um agente público (…) tenha de tomar decisões ou tenha contacto com procedimentos administrativos de qualquer natureza, que possam afetar, ou em que possam estar em causa, interesses particulares seus ou de terceiros e que por essa via prejudiquem ou possam prejudicar a isenção e o rigor das decisões administrativas que tenham de ser tomadas, ou que possam suscitar a mera dúvida sobre a isenção e o rigor que são devidos ao exercício de funções públicas."

5.1.2 Riscos de Gestão

Atendendo a que o presente PPRG abrange, em cumprimento das orientações do CPC, os riscos de gestão mais relevantes, é pertinente a sua caracterização, para a qual foram adotados os conceitos vertidos no **Modelo de Avaliação de Riscos (MAR) do Banco de Portugal**[6], e que servem de suporte à categorização dos riscos de gestão, decorrentes da possibilidade de ocorrência de perdas de ativos, deficiências ou inadequação dos processos internos, pessoas ou sistemas, falhas de segurança, eventos externos, legais e contenciosos, que se repercutam na redução, degradação ou interrupção, parcial ou total, das atividades da instituição, com impacto negativo na sua imagem ou ativos.

Para efeitos de operacionalização do presente PPRG, identificam-se, e categorizam-se, os seguintes riscos de gestão:

a. Risco de Estratégia

"*Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de decisões estratégicas inadequadas, da deficiente implementação das decisões ou da incapacidade de resposta a alterações do meio envolvente, bem como a alterações no ambiente de negócios da instituição."*

[6] Consulta do Banco de Portugal n.º 2/2007 - Modelo de Avaliação de Riscos - MAR – Metodologia *"que estabelece critérios e procedimentos, objectivos e sistematizados, para avaliar a magnitude dos riscos subjacentes à actividade desenvolvida por cada instituição (…) de todas as dimensões do risco intrínseco das instituições"*

b. Risco Operacional

"*Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de falhas na análise, processamento ou liquidação das operações, de fraudes internas e externas, da actividade ser afectada devido à utilização de recursos em regime de "outsourcing", da existência de recursos humanos insuficientes ou inadequados ou da inoperacionalidade das infra-estruturas*."

c. Risco de Sistemas de Informação

"*Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, em consequência da inadaptabilidade dos sistemas de informação a novas necessidades, da sua incapacidade para impedir acessos não autorizados, para garantir a integridade dos dados ou para assegurar a continuidade do negócio em caso de falha, bem como devido ao prosseguimento de uma estratégia desajustada nesta área*."

d. Risco de Compliance

"*Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes de violações ou desconformidades relativamente às leis, regulamentos, contratos, códigos de conduta, práticas instituídas ou princípios éticos. Pode traduzir-se em sanções de carácter legal ou regulamentar, na limitação das oportunidades de negócio, na redução do potencial de expansão ou na impossibilidade de exigir o cumprimento de obrigações contratuais*."

e. Risco de Reputação

"*Probabilidade de ocorrência de impactos negativos nos resultados ou no capital, decorrentes duma percepção negativa da imagem pública da instituição, fundamentada ou não, por parte de clientes, fornecedores, analistas financeiros, colaboradores, investidores, órgãos de imprensa ou pela opinião pública em geral*."

5.2 Metodologia ERM do COSO

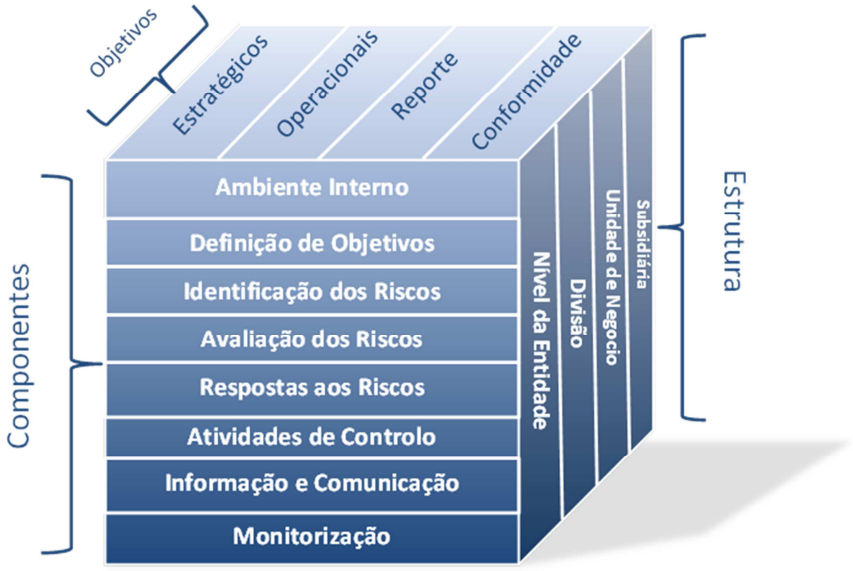
O Plano de Prevenção de Riscos de Gestão, a par da existência de manuais de procedimentos, atividades de controlo, da divulgação de informação relevante sobre os vários tipos de risco e respetivas medidas de mitigação, bem como o acompanhamento da eficácia destas medidas, constituem instrumentos que minimizam a ocorrência dos riscos, em geral, e a prática de corrupção ou infrações conexas, em particular.

Com o objetivo de uniformizar a gestão de riscos na instituição, e em particular, nos serviços abrangidos pelo PPRG, adotou-se o modelo de Gestão de Riscos Empresariais do COSO, de acordo com o qual o **risco** pode ser entendido como *a possibilidade da ocorrência de um evento que possa ter efeito redutor no alcance de objetivos*.

O COSO define a **Gestão de Riscos** como *um processo conduzido pelo Conselho de Administração, direção do serviço e restantes colaboradores, aplicado no estabelecimento de uma estratégia transversal à organização, formulada para identificar potenciais eventos ou situações que possam afetá-la, e gerir os riscos de modo a mantê-los num nível tolerado (apetite pelo risco), de forma a fornecer uma segurança razoável de que os objetivos da organização serão alcançados*.

A metodologia **ERM do COSO** é representada por uma matriz tridimensional (figura seguinte), que relaciona os objetivos e estratégia da organização, com as componentes que suportam a gestão de risco, aplicadas a todos os níveis e áreas da sua estrutura organizacional, e que é necessário gerir para providenciar uma segurança razoável no cumprimento dos objetivos organizacionais.

Figura 1 – Representação da matriz tridimensional ERM do COSO



Fonte: Adaptado de Estrutura Integrada de Gestão de Riscos Empresariais (ERM) do COSO

Trata-se pois de um processo contínuo e dinâmico, desenvolvido por todos os colaboradores, em todos os níveis da organização, objetivando a identificação, análise e tratamento dos riscos, salvaguardando a prossecução da missão, estratégia e objetivos do Centro Hospitalar Cova da Beira, suportado e conduzido pelo órgão de administração.

5.2.1 Componentes da Gestão de Riscos

Ambiente Interno

O Ambiente Interno compreende a forma como o risco é identificado e tratado, a sensibilidade ao risco estabelecida pelo órgão de gestão, assim como a percepção do sistema de controlo interno, pela entidade e todos os colaboradores, constituindo a base para todos as outras componentes da gestão do risco, influenciando a forma como:

- A estratégia e os objetivos são definidos;
- As atividades são estruturadas, desenhadas e realizadas;
- Os riscos são identificados, avaliados e geridos;
- Os sistemas de informação e comunicação são desenhados e funcionam;
- As atividades de monitorização são desenhadas e realizadas.

Definição de Objetivos

A definição de objetivos constitui um requisito para a identificação, avaliação e definição da reposta aos riscos, razão pela qual os objectivos definidos devem servir de suporte e estar alinhados com a missão da instituição. Por sua vez, os objetivos estratégicos estabelecem a base para a definição dos objetivos operacionais, de reporte e de conformidade e devem estar alinhados com os níveis de tolerância a riscos[7] estabelecidos, o que determina a definição de indicadores de medida para os mesmos.

No âmbito da metodologia ERM do COSO, constituem objetivos organizacionais, os seguintes:

Quadro 1 – Tipologia de Objetivos Organizacionais

[7] A tolerância a risco é o nível de variação aceitável quanto à realização de um determinado objetivo.

Objetivos	Definição
Estratégicos	Objetivos de alto nível alinhados com a missão e visão
Operacionais	Objetivos relacionados com a eficácia e eficiência das operações, que constituem uma referência na alocação dos recursos
Reporte	Objetivos relacionados com reportes externos ou internos, contendo informação fiável, de natureza financeira ou não financeira
Conformidade	Objetivos relacionados com o cumprimento de legislação e regulamentação, à qual a Instituição se encontra obrigada

Fonte: Adaptado de Estrutura Integrada de Gestão de Riscos Empresariais (ERM) do COSO

Identificação dos Riscos

Os eventos, de origem interna e externa[8], cuja ocorrência possa afetar a implementação da estratégia e a concretização dos objetivos, devem ser identificados, de forma contínua e interativa, e diferenciados em ameaças, oportunidades, ou ambos, conforme o seu efeito seja negativo ou positivo.

Quando o seu impacto é negativo, estes eventos resultam em riscos (de gestão e/ou de corrupção e infrações conexas), devendo ser classificados conforme a tipologia identificada e descrita nos pontos 5.1.1 e 5.1.2 do presente PPRG.

Avaliação dos Riscos

A avaliação de risco permite estabelecer o grau pelo qual os eventos potenciais terão um resultado na realização dos objetivos, de acordo com a sua probabilidade[9] e impacto[10], considerando ainda os seus efeitos inerentes e residuais.

[8] Estes eventos são considerados como fatores potenciadores do risco, podendo resultar de fatores económicos, ambientais, políticos, sociais, tecnológicos, estratégicos, estruturais, de recursos humanos, processos, entre outros.

[9] Possibilidade de determinado evento ocorrer.

[10] Representa o efeito da ocorrência de um evento.

Deve ser considerado como risco inerente aquele que existe antes da implementação de quaisquer controlos ou medidas que possam reduzir a sua probabilidade de ocorrência ou impacto. O risco residual é o risco remanescente após a definição de respostas ao risco. Numa fase inicial, a avaliação do risco deve ser efetuada considerando os riscos inerentes e, após a implementação de respostas ao risco, deve ser efetuada para os riscos residuais, tendo por base os critérios de avaliação que a seguir se apresentam.

Quadro 2 – Critérios de Avaliação do Risco Inerente

Avaliação do Risco Inerente			
Probabilidade de Ocorrência (P)	**Rara (1)**	**Possível (2)**	**Frequente (3)**
	Possibilidade de ocorrência de determinado evento ou a frequência com que este possa ocorrer, num determinado período de tempo, é relativamente baixa.	Possibilidade de ocorrência de determinado evento ou a frequência com que este possa ocorrer, num determinado período de tempo, é média.	Forte possibilidade de ocorrência de determinado evento, ou a sua ocorrência frequente, em determinado período de tempo.
Impacto (I)	**Menor (1)**	**Médio (2)**	**Severo (3)**
	A situação de risco não tem potencial para provocar prejuízos financeiros e/ou outros para a organização, não sendo os danos comprometedores da eficiência e eficácia dos processos ou da imagem da instituição.	A situação de risco pode comportar prejuízos financeiros e/ou outros, para a organização e comprometer a eficiência e eficácia dos processos, afetando o funcionamento dos serviços e o alcance dos objetivos.	A situação de risco pode resultar em prejuízos financeiros e/ou outros significativos para a organização, comprometendo a eficiência e eficácia dos processos, o alcance dos objetivos e comprometimento da missão da organização e da sua imagem.

A magnitude do risco[11] é determinada em função da ponderação resultante da classificação atribuída à probabilidade da ocorrência e ao impacto previsto, de acordo com os critérios definidos na matriz seguinte:

[11] Magnitude do risco também pode ser entendida como a sensibilidade ao risco.

Quadro 3 – Matriz de classificação dos riscos

Sensibilidade ao Risco (PxI)				
Probabilidade de Ocorrência (P)	3	Elevado	Muito Elevado	Extremo
	2	Moderado	Elevado	Muito Elevado
	1	Baixo	Moderado	Elevado
		1	2	3
		Impacto (I)		

A avaliação do risco residual é determinada pela ponderação da avaliação ao risco inerente e aos controlos/medidas de resposta implementados, e que alterem a probabilidade e/ou impacto dos eventos.

Nesse sentido, a avaliação do risco residual deve ser efetuada de acordo com os seguintes critérios:

Quadro 4 – Critérios de Avaliação do Risco Residual

Avaliação do Risco Residual			
Sensibilidade ao risco	**Baixa/Moderada (1)**	**Elevada (2)**	**Muito elevada/Extrema (3)**
	Possibilidade de risco, mas o controlo existente é suficiente para obviar/mitigar o risco	Possibilidade de risco, mas o controlo existente não é suficiente para obviar/mitigar o risco, havendo necessidade de decisões e ações adicionais	Forte possibilidade de ocorrência, mas limitadas formas de obviar/mitigar o risco, mesmo com decisões e ações adicionais
Avaliação dos controlos	**Eficaz (1)**	**Não eficaz (2)**	**Inexistente (3)**
	Controlo formalizado e implementado, com evidências de que mitiga o risco	Controlo razoavelmente implementado, mas pode falhar por não contemplar todos os aspetos relevantes do risco	Controlo inexistente ou não funcional/não implementado

Respostas aos Riscos

Após a avaliação dos riscos, deverá ser determinada uma resposta apropriada, tendo em consideração o processo em causa e o efeito sobre a probabilidade de ocorrência ou impacto do risco, assim como os custos ou benefícios inerentes à resposta tomada. A decisão tomada deverá garantir que o risco residual é tolerável, devendo a sua implementação ser suportada num conjunto de atividades de controlo.

Os critérios de decisão das respostas a aplicar encontram-se suportados numa graduação de risco entre 1 e 9 que agrupa as respostas ao risco nas seguintes categorias: Aceitar, Monitorizar, Reduzir, Partilhar e Eliminar.

Quadro 5 – Estratégias de respostas aos riscos

Graduação da resposta ao risco	Estratégia	Ação
1	Aceitar	Não requer medidas específicas
2	Aceitar e Monitorizar	Não são necessários controlos adicionais. Deve proceder-se a monitorizações periódicas, de forma a assegurar que se mantém o controlo.
3 a 4	Reduzir	Devem ser implementadas medidas de redução da probabilidade de ocorrência ou impacto do risco.
6	Reduzir e Partilhar	A atividade pode ser suspensa até que se proceda à redução do risco. São tomadas medidas para reduzir a probabilidade de ocorrência ou impacto, podendo inclusive proceder-se à sua transferência ou partilha de parte do risco.
9	Eliminar	A atividade não deve ser iniciada, ou deve ser interrompida, até serem tomadas medidas de eliminação/redução do risco.

Fonte: Adaptado de Estrutura Integrada de Gestão de Riscos Empresariais (ERM) do COSO

Atividades de Controlo

Constituem atividades de controlo o conjunto de práticas e procedimentos estabelecidos para monitorizar e mitigar potenciais eventos de risco, pressupondo a execução de ações para assegurar com segurança razoável o cumprimento dos objetivos, executadas aos vários níveis da organização.

Estas atividades podem compreender procedimentos relacionados com segregação de funções, autorizações, verificações, reconciliações ou aprovações, podendo as próprias atividades de controlo constituir respostas a riscos.

Para efeitos de operacionalização do PPRG classificaram-se os controlos em função de constituírem atividades preventivas ou detetivas, ainda que combinando controlos de natureza manual (executados por pessoas de forma manual (total ou parcialmente), ainda que com o auxilio de aplicações informáticas) ou automática (executados por uma aplicação, apresentando um carácter mecânico).

Quadro 6 – Tipificação dos controlos

Controlos	Definição
Preventivos	Visam prevenir a ocorrência de eventos indesejáveis que comprometam o alcance dos objetivos.
Detetivos	Permitem detetar e identificar eventos indesejáveis que tenham ocorrido.

Fonte: Adaptado de Estrutura Integrada de Gestão de Riscos Empresariais (ERM) do COSO

Informação e Comunicação

A qualidade da informação afeta a capacidade de tomada de decisões apropriadas na gestão e controlo das atividades da organização, pelo que a informação considerada pertinente deve ser identificada, avaliada e comunicada de forma coerente e atempada, transversalmente pela organização, permitindo que cada um desempenhe as suas responsabilidades nas respostas aos riscos.

Ela será tanto mais eficaz, na medida em que fluir de forma correta, com a complexidade necessária, dirigida às pessoas certas e na ocasião oportuna, quer internamente, quer com terceiros, nomeadamente, clientes, fornecedores, órgãos reguladores e acionistas.

A comunicação deve ocorrer de forma a permitir transmitir, eficazmente:

- A estratégia e os objetivos institucionais;
- A importância e a pertinência da gestão de riscos;

- O nível de tolerância dos riscos;
- Uma linguagem comum no que concerne à gestão de riscos;
- A definição das funções e responsabilidades dos Serviços e colaboradores na gestão de riscos.

Monitorização

A monitorização visa assegurar que o processo de gestão de riscos e respetivas componentes continuam a operar de forma efetiva, devendo ser ajustado sempre que necessário, em função de alterações nos objetivos ou na estratégia, na medida em que as respostas ao risco que antes eram efetivas poderão tornar-se irrelevantes e as atividades de controlo poderão tornar-se menos eficazes ou deixar de ser efetuadas.

Nesse sentido, podem ser efetuadas atividades contínuas de monitorização, realizadas permanentemente pelos Serviços, ou avaliações periódicas realizadas pelo Serviço de Auditoria Interna ou entidades externas. As atividades realizadas continuamente pelos Serviços para monitorizar a eficácia da gestão de risco estão integradas nas sua atividades correntes, onde se incluem, entre outras, atividades regulares de gestão e supervisão, comparações, reconciliações e outras ações de rotina, permitindo reagir proativamente a alterações ou potenciais fatores de risco.

A monitorização dos riscos e controlos internamente pelos Serviços, permite uma intervenção mais efetiva e atempada a possíveis alterações estruturais e processuais e de forma mais preventiva à ocorrência de erros ou irregularidades, sendo mais efetivas que as avaliações periódicas, que são tendencialmente mais reativas.

Não obstante, o recurso combinado às duas formas de monitorização contribuirá para assegurar maior eficácia do processo de gestão de riscos, ao longo do tempo.

6. MATRIZES DE RISCOS E CONTROLOS DOS SERVIÇOS

O processo de gestão de riscos adotado encontra-se suportado numa ferramenta de controlo e avaliação de riscos (Matriz de Riscos e Controlos), desenvolvida de acordo com a metodologia ERM do COSO, no sentido de constituir um instrumento quer de auto avaliação da eficácia do controlo interno de cada serviço, quer de monitorização da eficácia da gestão de riscos, sustentando dessa forma a tomada de decisões com vista à mitigação dos riscos que comprometem o alcance dos objetivos de cada processo.

Nesse sentido, a Matriz de Riscos e Controlos elenca os riscos associados a cada processo, que se encontram avaliados em função da sua probabilidade de ocorrência e impacto, descrevendo-se os procedimentos estabelecidos para monitorizar e mitigar os potenciais eventos de risco. É igualmente analisada a capacidade dos controlos adotados mitigarem os riscos, com respetiva identificação dos responsáveis pela sua execução. Essa análise determina a necessidade (ou não) de implementação de medidas de controlo que permitam reduzir a exposição aos riscos, cuja eficácia será monitorizada periodicamente.

Nas páginas seguintes apresentam-se sumariamente as matrizes de riscos e controlos dos serviços abrangidos no âmbito do presente PPRG, que prestaram a informação constante das mesmas e que é da sua exclusiva responsabilidade.

6.1 Serviços Financeiros

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Contabilidade e Reporte	Elaboração do orçamento anual	Orçamento desadequado	Estratégia; Operacional	Elevado	• Levantamento anual de necessidades a todos os serviços; • Validação do orçamento pelo CA; • Parecer do órgão de fiscalização	Conselho de Administração; Serviços; Órgão de Fiscalização	Aceitar e Monitorizar	• Obrigatoriedade de Plano de Atividades por serviço; • Validação das necessidades identificadas pelos serviços, a ser feita pelo SIE, RH e Logística
	Controlo e execução orçamental	Inadequada classificação contabilística	Estratégia	Moderado	• Verificação e comparação mensal dos registos de cabimentos e compromissos, no que respeita a alterações de encomendas	Serviços Financeiros	Reduzir	• Monitorização mensal dos encargos plurianuais. • Elaboração de mapa mensal de execução orçamental.
		Desvios orçamentais não autorizados	Operacional	Elevado	• Relatório de Execução Trimestral	Serviços Financeiros		
		Incumprimento legal	Compliance	Elevado	-	Serviços Financeiros		

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Contabilidade e Reporte	LCPA	Assunção de despesas sem Fundos Disponíveis	Operacional	Muito Elevado	• Parecer prestado pelo S. Financeiros, a cada processo de aquisição, em que informa da inexistência de fundos disponíveis.	Serviços Financeiros	Aceitar e Monitorizar	• Determinação mensal dos Fundos Disponíveis e comunicação ao CA • Checklist de informação de reporte
		Incumprimento legal	Compliance	Muito Elevado		Serviços Financeiros		
	Contabilidade Geral e de Custos	Não comunicação tempestiva, atempada e correta da informação de relato (ao Conselho de Administração, à tutela e demais entidades)	Operacional Compliance	Elevado	• Verificação e comparação mensal dos registos contabilísticos com os períodos anteriores • Avisos informáticos automáticos dos sistemas de informação • Conferência de listagens das aplicações de origem • Revisão de Contas pelos ROC	Serviços Financeiros	Aceitar e Monitorizar	• Checklist de procedimentos a efetuar/efetuados • Checklist de informação de reporte
Compras e Contas a Pagar	LCPA	Penalidades por incumprimento da LCPA	Compliance	Muito Elevado	• Parecer prestado pelo S. Financeiros, a cada processo de aquisição, em que informa da inexistência de fundos disponíveis.	Serviços Financeiros	Aceitar	• Informação mensal da execução orçamental

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Compras e Contas a Pagar	Contas a pagar	Pagamentos indevidos/incorretos ou ausência de pagamentos	Operacional	Elevado	• Requisitos mínimos na criação de uma nova entidade • Conferência de extratos de conta corrente	Serviços Financeiros	Aceitar e Monitorizar	• Definição da política de pagamentos pela tutela
		Demonstrações Financeiras adulteradas (com omissão de passivos/ responsabilidades)	Operacional	Elevado	• Conferência de extratos de conta corrente • Revisão de Contas pelos ROC	Serviços Financeiros	Aceitar e Monitorizar	• Centralizar a receção de faturas nos Serviços Financeiros • Circularização amostral de fornecedores (por forma a ser feita a reconciliação anual de todos com a conta corrente) • Validação amostral, com periodicidade trimestral, das anulações de faturas de fornecedores (com verificação do suporte documental)

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Faturação e Contas a Receber	Taxas Moderadoras	Prestações de serviços clínicos não faturados na totalidade, com perda de receitas de taxas moderadoras	Operacional	Elevado	• Verificação e comprovação dos dados pessoais e da situação do utente face ao dever de pagamento de taxas moderadoras e respectiva cobrança	Serviços Financeiros	Aceitar e Monitorizar	• Avaliação periódica (trimestral), tendo por base uma amostra aleatória, à aplicação e cumprimento dos regimes especiais de benefícios previstos no âmbito do regime de taxas moderadoras • Comunicar trimestralmente ao CA os atrasos na faturação • Monitorizar e cruzar o sonho com restantes aplicações de suporte (trimestralmente)
	Faturação de prestações de cuidados (contrato programa /seguradoras /outras)	Prestações de serviços clínicos não faturados na totalidade, comprometendo a faturação no âmbito do contrato-programa	Operacional	Elevado	• Conferência mensal de valores por facturar • Conferência trimestral de contas correntes	Serviços Financeiros	Aceitar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Faturação e Contas a Receber	Faturação de prestações de cuidados (contrato programa /seguradoras /outras)	Os saldos de clientes não refletem a totalidade dos direitos da instituição	Operacional	Elevado	• Encontro de contas com outras instituições (Cleaninghouse) e SAFT • Análise mensal de antiguidade de saldos de clientes	Serviços Financeiros	Aceitar	-
		Prescrição de dívidas	Operacional	Elevado	-	Serviços Financeiros	Aceitar e Monitorizar	• Verificação trimestral de facturas superiores a 3 UC por enviar para Contencioso
	Outras faturações (ensaios clínicos, seminários….)	Perda de receitas	Operacional	Moderado	-	Serviços Financeiros	Aceitar e Monitorizar	• Elaboração de ficheiro partilhado para controlo de outras faturações, com monitorização semanal
Tesouraria	Gestão de Pagamentos	Desvio de fundos	Operacional	Moderado	-	Serviços Financeiros	Aceitar e Monitorizar	• Promover reduções no prazo de conferência interna das facturas
		Penalizações/juros por atraso nos pagamentos	Operacional	Elevado	-	Serviços Financeiros	Aceitar e Monitorizar	• Reduzir o número de adiantamentos • Efetuar processos globais de pagamentos de facturas
		Favorecimentos na gestão de pagamentos	Operacional	Elevado	-	Serviços Financeiros	Aceitar e Monitorizar	

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Tesouraria	Gestão de Recebimentos	Desvio de fundos	Operacional	Elevado	-	Serviços Financeiros	Aceitar	• Confrontação trimestral da lista de recibos do sonho com a contabilidade
	Gestão de fundos de maneio e caixa	Gestão de tesouraria inexistente ou ineficaz	Operacional	Moderado	• Planeamento mensal das necessidades de tesouraria	Serviços Financeiros	Aceitar	• Validação diária da folha de caixa pelo Diretor de Serviço
Gestão de Recursos Humanos no Serviço	Exercício de funções dos colaboradores dos Serviços Financeiros	Contágio COVID-19 em contexto laboral	Operacional	Elevado	• Face às atualizações da situação epidemiológica da COVID 19, monitorizar de forma contínua a equipa de colaboradores, de forma a que exerçam funções cumprindo as directrizes da DGS de distanciamento físico e protecção individual, no âmbito da COVID- 19	Serviços Financeiros	Aceitar e Monitorizar	-

6.2 Serviço de Higiene, Saúde e Segurança no Trabalho

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Vigilância da Saúde	Admissão na consulta não presencial / presencial	Acesso à ficha do trabalhador errado	Operacional	Elevado	• Confirmação da identificação do trabalhador para a consulta (2 elementos de identificação)	Assistente Técnico	Aceitar e Monitorizar	-
		Acesso não autorizado a informação confidencial	Sistemas de Informação	Elevado	• Acesso restrito aos processos	Assistente Técnico	Aceitar e Monitorizar	-
	Avaliação de enfermagem	Acesso à ficha do trabalhador errado	Operacional	Elevado	• Chamada para a consulta enfermagem	Enfermeiro	Aceitar e Monitorizar	-
		Incumprimento das ações preconizadas por parte do trabalhador	Operacional	Elevado	• Na consulta médica ou na próxima consulta	Enfermeiro	Aceitar e Monitorizar	-
		Acesso não autorizado a informação confidencial	Sistemas de Informação	Elevado	• Restrição de acessos pelo Serviço de Tecnologias de Informação	Informático	Aceitar e Monitorizar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Vigilância da Saúde	Consulta médica	Acesso à ficha do trabalhador errado	Operacional	Baixo	• Confirmação da identificação do trabalhador para a consulta (2 elementos de identificação) • Chamada para a consulta	Médico	Aceitar	-
		Insatisfação do trabalhador/ Possíveis efeitos negativos da saúde do trabalhador pela não realização de Consulta de Medicina do Trabalho	Compliance	Extremo	• Marcação para posterior consulta	Médico	Aceitar e Monitorizar	-
		Acesso não autorizado a informação confidencial	Sistemas de Informação	Elevado	• Restrição de acessos pelo Serviço de Tecnologias de Informação	Informático	Aceitar e Monitorizar	-
		Incumprimento do programa de vigilância da saúde programada para o ano	Compliance	Elevado	• Validação do Protocolo na consulta médica ou na próxima consulta	Médico	Aceitar e Monitorizar	-
	Prestação de cuidados	Tratamento inadequado	Operacional	Elevado	• Trabalhador ou outro prestador de cuidados na avaliação dos registos de prestação de cuidados	Médico	Aceitar e Monitorizar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
		Incumprimento das ações preconizadas por parte do trabalhador/Agravamento das condições clínicas do trabalhador	Operacional	Elevado	• Outro prestador de cuidados na avaliação dos registos de prestação de cuidados	Médico	Aceitar e Monitorizar	-
Vigilância da Saúde	Prescrição e administração de terapêutica	Tratamento inadequado	Operacional	Elevado	• Validação de fármacos	Diretora da Farmácia	Aceitar e Monitorizar	-
		Incumprimento das ações preconizadas por parte do trabalhador/Agravamento das condições clínicas do trabalhador	Operacional	Elevado	• Outro profissional de saúde a comunicar a terapêutica	Médico	Aceitar e Monitorizar	-
Inspeção das Instalações	Implementação das medidas	Medidas propostas não implementadas por restrições financeiras	Operacional	Elevado	• Verificação na próxima auditoria	Técnico Superior de Higiene e Segurança do Trabalho Diretor do SIE Responsáveis de Serviço	Aceitar e Monitorizar	-

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
	Inspeção das instalações	Riscos não identificados/ avaliados/tratados/eliminados	Operacional	Elevado	• Verificação na próxima auditoria	Técnico Superior de Higiene e Segurança do Trabalho Diretor do SIE Responsáveis de Serviço	Aceitar e Monitorizar	-
	Verificação das medidas	Agravamento das situações pela não implementação das medidas propostas ou pela sua ineficácia	Operacional	Elevado	• Verificação na próxima auditoria /Revisão de medidas implementadas nos Serviços / Reporte dos Serviços	Técnico Superior de Higiene e Segurança do Trabalho Diretor do SIE CA	Aceitar e Monitorizar	-
Gestão de Riscos Profissionais	Análise do risco no posto de trabalho	Não identificação da totalidade dos riscos presentes no posto de trabalho pela complexidade dos postos de trabalhos e novas actividades	Operacional	Elevado	• Avaliação anual de riscos profissionais, no decorrer das inspeções, relato de incidentes e/ou eventos adversos, auditorias	Técnico Superior de Higiene e Segurança do Trabalho	Aceitar e Monitorizar	-
	Controlo do risco	Riscos não controlados	Operacional	Elevado	• Avaliação anual de riscos profissionais, no decorrer	Técnico Superior de Higiene e	Aceitar e Monitorizar	-

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
		Agravamento dos riscos	Operacional	Elevado	das inspeções, relato de incidentes e/ou eventos adversos, auditorias	Segurança do Trabalho		
Acidentes de Trabalho	Implementação de acção correctiva / preventiva (se necessário)	Medidas propostas não implementadas por restrições financeiras	Operacional	Elevado	• Registo de não conformidade/Evento Adverso	Técnico Superior de Higiene e Segurança do Trabalho / CA / Responsáveis Serviço / Gabinete da Qualidade	Aceitar e Monitorizar	-
		Agravamento das situações pela não implementação das medidas propostas ou pela sua ineficácia	Operacional	Elevado	• Registo de não conformidade/Evento Adverso • Revisão de medidas implementadas nos Serviços • Reporte dos Serviços		Aceitar e Monitorizar	-
Gestão de Recursos Humanos no Serviço	Exercício de funções dos colaboradores do Serviço de HSST	Contágio COVID-19 em contexto laboral	Operacional	Elevado	• Face às atualizações da situação epidemiológica da COVID 19, monitorizar de forma contínua a equipa de colaboradores, de forma a que exerçam funções cumprindo as directrizes da DGS de distanciamento físico e protecção individual, no âmbito da COVID- 19	SHSST	Aceitar e Monitorizar	-

6.3 Serviço de Instalações e Equipamentos

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Instalações e Equipamentos	AVAC	Tratamento ineficaz/inadequado ou inexistente	Operacional	Elevado	• Análises à qualidade do ar interior	Director do Serviço	Aceitar e monitorizar	• Ensaios de controlo de Qualidade do ambiente interior (BO, UMR, Ambulatório, Farmácia)
		Temperaturas elevadas provocam reações adversas na população do serviço	Operacional	Elevado	• Monitorização da temperatura nos picos de verão; • Reformulação do sistema AVAC	Director do Serviço	Aceitar e monitorizar	-
		Situação anómala no ar que provoca reações adversas na população do serviço	Operacional	Elevado	• Verificação de sistema AVAC, rede esgotos, integridade das infraestruturas de alvenaria, zonas circundantes	Director do Serviço/Entidade Externa	Aceitar e monitorizar	
		Ausência de ar condicionado nos serviços críticos	Operacional	Elevado	• Monitorização permanente na GTC, do funcionamento dos equipamentos;	Técnico da GTC e Técnico de AVAC, Electricista	Aceitar e monitorizar	• Execução da Manutenção ao Sistema de Aquecimento e Ventilação e Ar Condicionado- • Inspeção aos aparelhos de ar condicionado

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Instalações e Equipamentos	Gases	Inoperacionalidade dos equipamentos de gás	Operacional	Elevado	• Monitorização permanente na GTC, do funcionamento dos equipamentos. • Deteção por parte do operador dos equipamentos. • Ordens de trabalho (MAC).	Técnico da GTC e Assistente Operacional da Secção de Gases Medicinais	Aceitar e monitorizar	-
		Impossibilidade de dispensa de cuidados assistenciais	Operacional	Elevado	• Monitorização dos alarmes da central de gases.	Técnico da GTC, Assistente Operacional da Secção de GM e entidade externa	Aceitar e monitorizar	• Execução da Manutenção à rede de gases Medicinais
	Rede Hidráulica	Falha no fornecimento de água da rede externa.	Operacional	Elevado	• Execução de Manobras de suporte a um corte de abastecimento de água - CHCB.PO.DAH.03	Assistente Operacional da Secção de Canalização	Aceitar e monitorizar	-

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Instalações e Equipamentos		Fornecimento de água contaminada	Operacional	Elevado	• Análises às águas de consumo; • Manutenção às linhas de abastecimento de água (CHCB.PO.DAH.13); • Monitorização da qualidade da água de acordo com o procedimento CHCB.PO.DAH.12	Responsável da Qualidade; Assistente Operacional da Secção de Canalização.	Aceitar e monitorizar	-
		Interrupção de serviços assistenciais e de suporte	Operacional	Elevado	• Execução da Manutenção às linhas de abastecimento de água (CHCB.PO.DAH.13). • Inspeções às instalações.	Assistente Operacional da Secção de Canalização	Aceitar e monitorizar	-
	Estruturas	Anomalias com forte potencial de risco de acidentes	Operacional	Elevado	• Inspecções às instalações. • Requisições de trabalho	Director do SIE	Aceitar e monitorizar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Instalações e Equipamentos	Electricidade	Inoperacionalidade de equipamentos e sistemas suportados por energia eléctrica	Operacional	Muito Elevado	• Monitorização permanente na GTC, do funcionamento dos equipamentos. • Manobras de suporte a um corte de energia eléctrica • Monitorização dos quadros eléctricos	Técnico de GTC e Assistente Operacional da Secção de Electricidade	Reduzir	• Monitorização dos quadros eléctricos. • Manutenção semanal aos grupos electrogéneos. • Manutenção Trimestral aos grupos electrogéneos (em carga) por entidade externa.
	Equipamentos Médicos	Validação de equipamento não conforme	Operacional	Elevado	• Manutenção preventiva e/ou manutenção correctiva e/ou calibração	Director do SIE	Aceitar e monitorizar	-
	Segurança	Roubo, extravio, rapto ou outra anomalia decorrente de comportamentos indevidos	Operacional	Elevado	• Monitorização da segurança e controlo de acessos nos três edifícios • Incidentes e eventos adversos	Director do SIE; Empresa de segurança	Aceitar e monitorizar	-
	Resíduos	Não recolha dos resíduos para tratamento, provocando acumulação dos mesmos na Central	Operacional	Elevado	• Monitorização de contrato	Director do SIE	Aceitar e monitorizar	-

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão Hoteleira	Alimentação	Consumo de alimentos não conformes	Operacional	Elevado	• Monitorização de contrato	Gabinete Hoteleiro, Director do SIE	Aceitar e monitorizar	-
	Tratamento e Fornecimento de Roupa Hospitalar	Fornecimento inadequado de roupa hospitalar	Operacional	Elevado	• Análises microbiológicas; • Incidente e eventos adversos, Auditorias	Gabinete Hoteleiro, Director do SIE	Aceitar e monitorizar	-
Geral	Geral	Incumprimento das ações preconizadas	Operacional	Baixo	• Repetição das informações e pedidos formalizados	Gabinete Hoteleiro, Director do SIE	Aceitar e Monitorizar	-
		Fuga de informação	Operacional	Baixo	• Assinatura de contrato, formações e panfletos	Chefia direta	Aceitar e Monitorizar	-
		Não cumprimento do plano de formação proposto devido à pandemia	Operacional	Baixo	• Reagendamento de todo a formação e proposta de alteração para aumentar o prazo de cumprimento.	Director do SIE	Aceitar e Monitorizar	-
		Colaborador com possibilidade de disseminar infeção por COVID-19	Operacional	Elevado	• Realização de teste COVID 19	Director do SIE	Aceitar e Monitorizar	-

6.4 Serviço de Logística Hospitalar

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Compras	Pedido de compra	Encomenda de artigos ou quantidades erradas podendo originar excesso de existências, que se poderão tornar inutilizáveis ou obsoletas (prazo de validade), ou ruptura de existências.	Operacional	Elevado	• Validação do pedido de aquisição pelo Conselho de Administração • Elaboração obrigatória de informação que expressa a necessidade de aquisição • Validação da satisfação da necessidade pela direção do serviço (considerando a expressão da necessidade real do serviço utilizador e o montante disponível em rubrica orçamental) • Alerta automático da aplicação informática relativamente ao nível mínimo de stocks	Direção do Serviço Logística Hospitalar Gestão de Compras	Aceitar e Monitorizar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Compras	Autorização da despesa e escolha do procedimento	Compras de existências e contratação de serviços não autorizadas e/ou que não cumprem os procedimentos e regulamentação sobre aquisições	Operacional Compliance	Elevado	• Dar cumprimento ao código de conduta ética. • Dar cumprimento ao manual de Boas Praticas em Contratação Pública • Dar cumprimento à legislação em vigor • Elaboração obrigatória de informação que expressa a necessidade de aquisição • Nomeação de Gestor de contrato • Utilização preferencial da plataforma electrónica de contratação pública • Inclusão no caderno de encargos de cláusulas sobre penalizações por incumprimento e aplicação das mesmas • Aprovação da minuta do contrato por parte da entidade adjudicante • Elaboração de mapas comparativos	Conselho de Administração Direção do Serviço Logística Hospitalar Gestão de Compras Gabinete Técnico Jurídico	Reduzir	• Emissão de parecer jurídico relativo à conformidade legal e administrativa dos procedimentos contratuais • Avaliação das últimas aquisições por fornecedor e por objecto. • Validação da Checklist em anexo ao Manual de Boas Práticas para cada procedimento • Não inclusão de elementos da Gestão de Compras em júris de procedimentos. • Preenchimento obrigatório de declaração de inexistência de conflitos de interesse para cada procedimento • Pedido de parecer ao SRH sobre existência de impedimentos e/ou conflitos de interesses para cada elemento de júri nomeado para o procedimento concursal • Análise semestral do cumprimento dos contratos (com reporte ao SLH)

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Compras	Gestão da encomenda	Ruptura de stocks por não satisfação de encomendas	Operacional	Elevado	• Validação diária das Notas de Encomenda a receber	Direção do Serviço Logística Hospitalar Gestão de Compras	Aceitar e Monitorizar	-
		Inadequabilidade dos produtos/serviços adquiridos por encomenda incorreta	Operacional	Elevado	• Validação pelo CA que a informação constante da NE (fornecedor, material, quantidade, prazo de entrega, valor) corresponde à autorização de compra • Manter registo dos contratos adjudicados com os fornecedores descrevendo as condições de fornecimento concordadas, de modo a facilitar a emissão de notas de encomenda		Aceitar e Monitorizar	-
Gestão de Stocks	Receção e Conferência	Receções de materiais e bens/serviços não conformes, não registadas e não contabilizadas correta e oportunamente	Operacional	Moderado	• Dupla validação: pela receção e pelos armazéns • Verificação documental, quantitativa e qualitativa, com base na Guia de Entrada e Nota Encomenda • Segregação de funções entre quem receciona/confere e quem regista • Colocação de material em zona de devolução • Conferência mensal das devoluções	Direção do Serviço Logística Hospitalar Gestão de Stocks	Aceitar e Monitorizar	• Identificação por número mecanográfico de quem validou a receção e de quem efetuou o registo • Estabelecimento de critérios de aceitação de encomendas

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Stocks	Armazenamento	Desvio ou deterioração de existências	Operacional	Elevado	• Verificação documental, quantitativa e qualitativa, com base na Guia de Entrada e Nota Encomenda • Circuito de armazenagem (armazéns centrais e avançados), que permite a movimentação eficiente e eficaz dos materiais, tendo em consideração os requisitos de armazenagem dos mesmos • Condições de armazenamento (temperatura) e restrição de acessos físicos definidos, com verificações periódicas das instalações físicas • Verificações periódicas aos armazéns e materiais, respeitando a segregação de funções • Contagens mensais físicas na totalidade, respeitando a segregação de funções (equipa com 1 elemento do armazém e 1 elemento do setor de aquisições) • Análise mensal dos consumos previstos e dos reais • Atualização mensal dos indicadores de gestão: stock máximo, mínimo, ponto de encomenda	Direção do Serviço Logística Hospitalar Gestão de Stocks	Aceitar e Monitorizar	• Identificação por número mecanográfico de quem validou a receção e de quem efetuou o registo • Definição dos critérios a observar na verificação física das existências • Verificação anual de existências com rotação reduzida ou obsoleta
		Valorização incorreta de existências	Operacional	Elevado		Direção do Serviço Logística Hospitalar Gestão de Stocks	Aceitar e Monitorizar	

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Stocks	Distribuição	Quebra dos níveis mínimos de stocks	Operacional	Elevado	• Mapa de aviamentos	Direção do Serviço Logística Hospitalar Gestão de Stocks	Aceitar e Monitorizar	-
		Desvios entre o inventário físico das existências e o stock contabilístico	Operacional	Elevado	• Rotatividade dos Colaboradores na reposição e distribuição • As saídas de armazém (por requisição interna) são devidamente aprovadas e validadas documentalmente (por quem entrega e por quem recebe) e automaticamente registada a saída na aplicação informática aquando do aviamento em armazém	Direção do Serviço Logística Hospitalar Gestão de Stocks	Aceitar e Monitorizar	-

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Património	Inventário, Cadastro e Registo	Cadastro de imobilizado desatualizado e/ou valorizado incorretamente	Operacional	Elevado	-	Direção do Serviço Logística Hospitalar Património	Reduzir ou Partilhar	• Segregação de funções entre quem regista e quem procede à inventariação • Verificação semestral dos bens (de forma amostral) - verificação física vs cadastro • Realização do inventário de bens de imobilizado de 2 em 2 anos • Elaboração de lista de material inventariado por serviço (datada e assinada por responsável do património e do serviço), procedendo à respetiva atualização anual • Responsabilização dos serviços pela salvaguarda dos bens sob a sua custódia, através da validação e confirmação da existência dos bens afetos ao serviço pelo respectivo responsável, com periodicidade anual

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Património	Transferência de bens	Cadastro de imobilizado desatualizado	Operacional	Elevado	-	Direção do Serviço Logística Hospitalar Património	Reduzir ou Partilhar	• Obrigatoriedade de pedido de autorização de transferência do bem (ficha de transferência) ao Serviço de Logística e CA
	Abates de imobilizado	Cadastro de imobilizado desatualizado e/ou valorizado incorretamente	Operacional	Elevado	• Submeter todos os abates e vendas de imobilizado à aprovação do CA, após parecer do diretor do Serviço de Instalações e Equipamentos e do diretor do Serviço de Logística Hospitalar	Direção do Serviço Logística Hospitalar Património SIE	Aceitar e Monitorizar	• Avaliação anual dos pedidos para abate de imobilizado e respetivo registo
	Avarias/ Reparações	Custos indevidos com ações de manutenção e reparação de equipamentos	Operacional	Elevado	• Identificação dos registos de inventário relativo ao bem a ser reparado externamente • Validação pelo património e pela direção de serviço de Logística Hospitalar da garantia/contrato de manutenção do equipamento/serviço • Avaliação da necessidade de reparação externa pelo SIE, com a respetiva fundamentação • Informação partilhada sobre pedidos de reparação ao exterior (SLH/SIE)	Direção do Serviço Logística Hospitalar Património SIE	Aceitar e Monitorizar	• Conferência semanal dos pedidos de reparação externa
		Comprometimento da atividade dos serviços por atrasos ou não realização de reparações	Operacional	Elevado			Aceitar e Monitorizar	

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Património	Demonstração /Empréstimo	Custos financeiros inerentes a uma avaria ou desaparecimento de bem em regime de demonstração/ empréstimo ou de consumos associados	Operacional	Elevado	• Submissão a autorização do CA o pedido de demonstração /empréstimo e respectiva validação. • Listagem/relação de bens em regime de empréstimo/demonstração	Conselho de Administração Direção do Serviço Logística Hospitalar Serviço Requisitante	Reduzir	• Conferência mensal da situação de bens em regime de empréstimo/demonstração
Gestão de Recursos Humanos no Serviço	Exercício de funções dos colaboradores do Serviço de LH	Contágio COVID-19 em contexto laboral	Operacional	Elevado	• Face às atualizações da situação epidemiológica da COVID 19, monitorizar de forma contínua a equipa de colaboradores, de forma a que exerçam funções cumprindo as directrizes da DGS de distanciamento físico e protecção individual, no âmbito da COVID- 19	SLH	Aceitar e Monitorizar	-

6.5 Serviço de Recursos Humanos

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Necessidade de admissão e início de funções	Seleção e Recrutamento	Quadro de pessoal insuficiente ou inadequado	Operacional	Muito Elevado	• Os Serviços com carência de pessoal manifestam a necessidade através de fundamentação escrita de forma objetiva, com apresentação de dados da produção, nº de elementos a trabalhar na função onde há carência e a melhoria dos resultados com a contratação do novo elemento, horário pretendido para o novo elemento, bem como a descrição de funções (em impresso próprio), a ser entregue no Serviço de Recursos Humanos • Check list dos atos a realizar no processo de recrutamento e selecção • Consulta de base de dados para suprir a necessidade internamente • <u>Definição de medidas de gestão específicas, caso a caso</u>	CA RH Serviços	<u>Aceitar</u>	• Levantamento dos constrangimentos em termos de suficiência e adequabilidade da dotação das equipas de RH, bem como do recurso sistemático a trabalho extraordinário, com reporte ao CA, identificando as situações críticas
		Recurso a trabalho extraordinário	Compliance	Muito Elevado		CA RH Serviços	<u>Aceitar</u>	

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Necessidade de admissão e início de funções	Contratação e Integração	Inadaptação do colaborador ao posto de trabalho	Operacional	Elevado	• Checklist de documentos obrigatórios a entregar pelo colaborador • Avaliação pela Medicina do Trabalho da aptidão do colaborador • Comunicação encaminhada ao serviço de destino do colaborador recrutado e aos serviços de Informática, SHST, Central telefónica, Aprovisionamento e SIE, para os respectivos acessos e fardamento • Sessão de integração do colaborador com divulgação de procedimentos, manuais, regulamentos, códigos instituídos	CA RH Serviços	Aceitar	-
		Incumprimento no desempenho das funções	Operacional	Elevado		CA RH Serviços	Aceitar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Remunerações e prestações sociais	Remunerações, contribuições e impostos	Vencimentos, contribuições e impostos calculados com erro e/ou não verificados e contabilizados oportunamente	Operacional	Elevado	• Gestão mensal de ficheiros informáticos de processamento de trabalho suplementar/extraordinário e prevenções. • Elaboração mensal de mapas associados a cada escala que implique horas extraordinárias e prevenções para autorização do Conselho de Administração • Conferência de todas as alterações realizadas no mês em curso • Recolha dos registos de trabalho suplementar/extraordinário realizado pelos enfermeiros para assegurar o acompanhamento de doentes ao exterior e remessa para a secção de vencimentos para processamento. • Recolha dos Boletins de ajudas de custo e envio para autorização do Conselho de Administração e respetivo processamento • Submissão de ficheiros de acordo com calendário acordado com a SPMS	RH/ vencimentos CA	Aceitar	• Processamento das alterações de informação dos colaboradores associadas a processamento remuneratório e envio para Conselho de Administração para autorização de processamento.
		Acréscimo de custos não contemplado no orçamento	Operacional	Elevado		RH/ vencimentos CA	Aceitar	
		Não pagamento atempado de vencimentos	Operacional	Elevado		RH/ vencimentos CA	Aceitar	

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Assiduidade e Pontualidade	Assiduidade e Pontualidade	Registo das alterações mensais (faltas, horas extra, remunerações não regulares) não efetuado, ou efetuado de forma errada para efeito de processamento das remunerações	Operacional	Elevado	• Regulamento do horário de trabalho e assiduidade • Sistema de registo automático através de tecnologia de identificação biométrica (Sistema de Registo Biométrico), com interface funcional com a aplicação SISQUAL, para registo da assiduidade e pontualidade • Controlo e validação de assiduidade e pontualidade dos trabalhadores, pelas chefias/gestores de escala da sua dependência hierárquica • Contabilização mensal do tempo de trabalho prestado pelo colaborador, até ao dia 5 • Verificação de todas as escalas pelo SRH com o propósito de detetar possíveis irregularidades ou incumprimentos do Regulamente de Horário de Trabalho e Assiduidade • Auditoria trimestral por amostra às escalas para verificação de cumprimento do RHTA	Chefias Gestores de escala RH	Aceitar e Monitorizar	-
		Ausências que podem colocar em risco a dotação mínima dos serviços e a consequente prestação de cuidados	Compliance	Elevado		Chefias Gestores de escala RH	Aceitar e Monitorizar	-

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Carreiras e exercício funcional	Férias, faltas e mobilidades	Recurso a trabalho extraordinário	Operacional Estratégia	Elevado	• Emissão anual de Circular Informativa com procedimentos a cumprir na elaboração dos planos de férias. • Verificação da legalidade de todos os mapas e envio para o Conselho de Administração para aprovação. • O SRH verifica e valida o enquadramento legal de todas as ausências dos colaboradores. • Tipificação das ausências e reporte anual ao CA	RH CA	Aceitar e Monitorizar	-
Acumulação de funções, incompatibilidades e impedimentos	Acumulação de Funções	Incumprimento legal	Compliance	Muito Elevado	• Emissão anual de Circular Informativa sobre normativos legais para a acumulação de funções/exercício de outra atividade profissional • Entrega de requerimento obrigatório para a acumulação de funções, públicas ou privadas, de acordo com requisitos definidos	RH CA	Aceitar e Monitorizar	• Consulta do sítio da Entidade Reguladora da Saúde com periodicidade trimestral, e de forma amostral, para averiguar a existência de situações de acumulação de funções não autorizadas/comunicadas

Elaborado por: Serviço de Auditoria Interna

(Não carece de assinatura)

Data: 2021-06-21

Aprovado por: Conselho de Administração

Assinatura:

Data:

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Acumulação de funções, incompatibilidades e impedimentos	Acumulação de Funções	Comprometimento da segurança do profissional e do utente decorrente da acumulação de funções/exercício de outra atividade profissional	Operacional	Muito Elevado	• Verificação do cumprimento das normas legais aplicáveis aos vários grupos profissionais e ao regime de CIT e CTFP • Anualmente é cruzada informação com as entidades públicas e privadas nas quais os colaboradores declaram exercer actividade em acumulação de funções	RH CA	Aceitar e Monitorizar	• Revisão do procedimento CHUCB.IMP.DRH.46 - Requerimento de autorização do regime de acumulação de funções
	Incompatibili-dades e impedimentos	Incumprimento legal no exercício de funções	Operacional Compliance	Elevado	• Verificação da existência de incompatibilidades e proibições específicas no âmbito da acumulação de funções/exercício de outra atividade profissional, que requeiram procedimento especial • Parecer do SRH quando à existência de incompatibilidades e proibições específicas dos membros dos júris/comissões de escolha dos processos de aquisição de bens, serviços e empreitadas (a pedido do Serviço de Logística Hospitalar)	RH CA	Aceitar e Monitorizar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Avaliação de desempenho	SIADAP	Não reconhecido o mérito e desempenho dos colaboradores	Compliance	Elevado	• Emissão bianual de Circular Informativa com procedimentos a cumprir no processo de avaliação de desempenho. • Avaliações com menção de desempenho excelente, relevante e inadequado são remetidas para o Conselho Coordenador de Avaliação para validação, parecer e homologação. • Verificação da ficha de avaliação nos seguintes parâmetros: Nº de objetivos; Nº de Competências; Quadro da avaliação global de desempenho. • Após homologação, comunicação ao colaborador da menção atribuída e respetiva validação.	Serviços RH CA	Aceitar e Monitorizar	-
		Não progressão na carreira	Compliance	Elevado		Serviços RH CA	Aceitar e Monitorizar	-

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Cessação de funções	Cessação de funções do colaborador por iniciativa do colaborador/ entidade	Acréscimo de custos por indemnizações devidas por incumprimento legal	Compliance	Elevado	• Verificação mensal de prazos para a cessação da relação jurídica de emprego • Após deliberação autorizadora do Conselho de Administração no pedido de cessação de funções do trabalhador o SRH informa: ✓ O próprio para fazer entrega do cartão de identificação; ✓ Diretores de Departamento/Serviço; ✓ Sector de Tratamento de Roupa para este solicitar a devolução da farda; ✓ Serviço de Aprovisionamento, no caso de possuir telemóvel de serviço (VPN); ✓ Serviços Financeiros	RH CA Serviços	Aceitar e Monitorizar	-
		Insuficiência de colaboradores que pode comprometer a dotação mínima dos serviços	Compliance	Elevado			Aceitar e Monitorizar	-
	Aposentações	Quadro de pessoal insuficiente	Estratégia	Muito Elevado	• Após deferimento da aposentação o SRH informa o colaborador da data de término de exercício de funções e os serviços da instituição • Comunicação da aposentação às instituições externas em que o colaborador acumula funções.	RH CA Serviços	Aceitar e Monitorizar	• Solicitação à Tutela de contratação de colaborador que assegure as funções de carácter permanente exercidas pelo colaborado aposentado
		Insuficiência de colaboradores que pode comprometer a dotação mínima dos serviços	Estratégia	Muito Elevado			Aceitar e Monitorizar	

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Recursos Humanos no Serviço	Exercício de funções dos colaboradores do Serviço de RH	Contágio COVID-19 em contexto laboral	Operacional	Elevado	• Face às atualizações da situação epidemiológica da COVID 19, monitorizar de forma contínua a equipa de colaboradores, de forma a que exerçam funções cumprindo as directrizes da DGS de distanciamento físico e protecção individual, no âmbito da COVID- 19	Serviço de Recursos Humanos	Aceitar e Monitorizar	-

6.6 Serviço de Sistemas e Tecnologias de Informação

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Acessos dos colaboradores	Activação	Inacessibilidade do colaborador as aplicações para desempenhar a sua função no dia que vai necessitar. Não serem atribuídos todos os níveis de acesso ao colaborador.	Operacional	Elevado	• Circuito de informação em articulação com o Serviço de Recursos Humanos, o qual comunica todas a entradas e saídas de funcionários e as suas mobilidades entre serviços, através de e-mail, de forma a serem ajustados os acessos. • Verificação constante das requisições para triagem • Matriz de acessos aos colaboradores	Recursos Humanos Responsável de serviço SSTI	Aceitar e Monitorizar	• Implementar um regime de prevenção para o STI • As requisições não triadas aparecem no início • Identificação do erro de atribuição por parte da área

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
	Desactivação	Ficar um acesso não autorizado activo, possibilitando acessos indevidos ao sistema.	Operacional	Elevado	• Validação da desactivação por todas as áreas do STI envolvidas • Prazos definidos para a finalização das requisições • Análise semestral pelo SSTI do reporte de saídas de colaboradores da instituição, remetido pelo SRH, procedendo à desativação de acessos de colaboradores que ainda se mantenham ativos, através do procedimento instituído	Recursos Humanos Responsável de serviço SSTI	Reduzir ou Partilhar	• Comunicação periódica (a definir) para efeitos de controlo de saídas de colaboradores a ser remetida pelo Serviço de Recursos Humanos

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão de Alertas	Tratamento de Alertas (deteção, análise, notificação)	Anomalia ou inoperacionalidade de um sistema.	Operacional	Moderado	• O alerta gera o envio de e-mail automático para informatica@chcbeira.min-saude.pt, procedendo-se à sua formalização através de requisição informática	Direção de Serviço/Help Desk	Aceitar	• Requisição não é finalizada enquanto a anomalia persistir
Gestão de Incidentes	Comunicação de problemas/ avarias	Anomalia ou inoperacionalidade de um sistema por comunicação inadequada ou não ser feita em tempo útil.	Operacional	Elevado	• As requisições não triadas aparecem no início	Serviço Requisitante	Aceitar	• Verificação permanente das requisições para triagem
	Triagem da requisição e resolução	Não resolução de uma anomalia, ou resolução ineficaz, que pode originar falha ou inoperabilidade de um sistema.	Operacional	Elevado	• Alerta por parte do utilizador	Direção de Serviço/Help Desk	Aceitar	• Designar dois colaboradores do serviço de STI responsáveis pela validação das requisições e sua monitorização.

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
Gestão da Segurança	Políticas de Segurança	Fuga e uso indevido de informação	Operacional	Elevado	• CHCB.PL.CHCB.06 - Política de segurança da informação do Centro Hospitalar Cova da Beira	SSTI	Reduzir	• Elaboração de impresso para conhecimento dos colaboradores das regras de segurança e confidencialidade dos dados.
		Acessos indevidos aos sistemas	Operacional	Muito Elevado	• Controlo de acessos a internet através do ISA; • Procedimento de controlo de acesso por níveis de autorização (CHCB.PI.CHCB.11, CHCB.PI.CHCB.225); • Regulamento das condições de utilização da infraestrutura da RIS para efeitos de manutenção remota	SSTI	Aceitar	• As passwords de acesso as aplicações, são dadas pessoalmente aos utilizadores, e sempre que solicitado superiormente, são validados os responsáveis por alguns registos • Após comunicação pelo Serviço de Recursos Humanos, das entradas e saídas de funcionários e das suas mobilidades entre serviços, através de e-mail, são criados, revistos, atualizados ou cessados os acessos

Processo	Atividade	Descrição do Risco	Tipologia do Risco	Avaliação do Risco Inerente	Descrição do Controlo	Responsáveis/ Intervenientes	Avaliação do Risco Residual	Atividades de Controlo
	Salvaguarda da informação dos dados	Riscos de perda, modificação ou adulteração de informação por intrusão e de perda do controlo do meio físico e ambiental que protege e rodeia os recursos tecnológicos	Sistemas de Informação	Moderado	• Acesso restrito ao Data Center; • Existe um cofre anti-fogo em localização diferente do data Center; • Plano de Contingência.	SSTI	Aceitar e Monitorizar	• Realização de backups, de forma automática através de ferramentas apropriadas de backups, e também manualmente por colaboradores da área. O procedimento inclui, também, transporte e armazenamento em localizações físicas separadas
Gestão de Recursos Humanos no Serviço	Exercício de funções dos colaboradores do Serviço de STI	Contágio COVID-19 em contexto laboral	Operacional	Elevado	• Face às atualizações da situação epidemiológica da COVID 19, monitorizar de forma contínua a equipa de colaboradores, de forma a que exerçam funções cumprindo as directrizes da DGS de distanciamento físico e protecção individual, no âmbito da COVID- 19	SSTI	Aceitar e Monitorizar	-

Esta página foi intencionalmente deixada em branco.