

PLANO DE GESTÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS



SPMS_{EPE}
Serviços Partilhados do Ministério da Saúde

Índice

Sumário Executivo	3
Caracterização da SPMS	4
Sistema de Controlo Interno da SPMS.....	6
Gestão do Risco	8
Metodologia.....	11
Monitorização do Plano.....	13
Revisão do Plano	14
Identificação dos riscos e medidas preventivas a adotar	15
Transversais a toda a organização.....	15
Conselho de Administração	16
Direção de Administração Geral	17
Direção de Assuntos Jurídicos e Contencioso.....	18
Direção Financeira.....	19
Direção de Recursos Humanos.....	20
Direção de Planeamento e Desenvolvimento Organizacional	21
Direção de Comunicação e Relações Públicas	22
Gabinete de Apoio ao Conselho de Administração	22
Unidade de Projetos e Relações Internacionais	23
Unidade de Auditoria Interna	23
Unidade de Proteção de Dados e Cibersegurança	24
Centro de Contacto do SNS	24
Centro Nacional de Telessaúde	25
Centro de Controlo e Monitorização do SNS	26
Direção de Sistemas de Informação I.....	27
Direção de Sistemas de Informação II	28
Direção de Sistemas de Informação III	28
Central de Compras da Saúde.....	29
Unidade de Marketing, Serviços Partilhados e Gestão de Clientes	30

Sumário Executivo

De acordo com a recomendação do Conselho de Prevenção da Corrupção (CPC), de 1 de julho de 2009, os órgãos dirigentes máximos das entidades gestoras de dinheiros, valores ou património públicos, seja qual for a sua natureza, devem elaborar Planos de Gestão de Riscos de Corrupção e Infrações Conexas (PGRIC), bem como um relatório anual sobre a execução do plano.

Decorrente da aprovação da alteração ao Regulamento Interno da SPMS, homologado pelo Secretário de Estado da Saúde, em 25 de setembro de 2020, e revista a respetiva estrutura organizativa, verificou-se a necessidade de atualização do Plano de Gestão de Riscos de Corrupção e Infrações Conexas (PGRIC), de modo a refletir a nova orgânica. Adicionalmente, procedeu-se a um ajustamento relativamente aos riscos inerentes à qualidade de beneficiário direto e final do Plano de Recuperação e Resiliência.

Por outro lado, na elaboração do relatório de execução do PGRIC, foram, simultaneamente, avaliados os riscos identificados no PGRIC vigente, no sentido de aferir a sua manutenção no próximo Plano, a respetiva graduação, em termos de matriz de risco, e a eventual revisão.

De um modo geral, os responsáveis das áreas consideraram que as medidas de prevenção, então em vigor, se revelam adequadas. Não obstante, em algumas áreas foram sugeridas novas ações corretivas e identificados novos fatores de risco, demonstrando, desta forma, a preocupação de obter uma maior eficácia no controlo interno da instituição e na gestão do risco, em particular.

O presente documento procede, assim, à atualização do Plano de Gestão de Riscos de Corrupção e Infrações Conexas, tendo sido identificadas, face ao PGRIC aprovado em 10 de setembro de 2019, mais 44 riscos, bem como mais 64 medidas de prevenção ou mitigação.

Caracterização da SPMS

A SPMS, E.P.E. é uma pessoa coletiva de direito público de natureza empresarial, dotada de personalidade jurídica, autonomia administrativa e financeira e de património próprio, estando sujeita à tutela dos membros do Governo responsáveis pelas áreas das finanças e da saúde e ao regime jurídico do sector empresarial do Estado, aprovado pelo Decreto-Lei n.º 133/2013, de 3 de outubro. Rege-se pelo regime jurídico aplicável às entidades públicas empresariais, com as especificidades previstas nos seus Estatutos, aprovados pelo Decreto-Lei n.º 19/2010, de 22 de março, e no seu regulamento interno.

De acordo com o quadro jurídico estabelecido pelo Decreto-Lei n.º 19/2010, de 22 de março, alterado pelos Decretos-Leis n.ºs 108/2011, de 17 de novembro, 209/2015, de 25 de setembro, 32/2016, de 28 de junho, e 69/2017, de 16 de junho, 38/2018, de 11 de junho, e 75/2020, de 25 de setembro, tem vindo a assistir-se ao reforço das competências e atribuições da SPMS em matéria de prestação de serviços partilhados específicos da área da saúde aos estabelecimentos e serviços do Serviço Nacional de Saúde (SNS), independentemente da sua natureza jurídica, bem como aos órgãos e serviços do Ministério da Saúde (MS) e a quaisquer outras entidades, quando executem atividades específicas da área da saúde.

Constituem atribuições da SPMS a prestação de serviços partilhados nas áreas de compras e logística, serviços financeiros, recursos humanos e sistemas e tecnologias de informação e comunicação; o funcionamento do Centro de Contacto do Serviço Nacional de Saúde (SNS24) e do Centro Nacional de Telessaúde (CNTS); e, no âmbito dos serviços partilhados de conferência de faturas de medicamentos, de meios complementares de diagnóstico e terapêutica e de outras áreas de prestações de saúde, cabe, ainda, à SPMS assegurar a atividade e a gestão do Centro de Controlo e Monitorização do SNS (CCMSNS).

Em termos organizacionais, a SPMS apresenta uma estrutura composta por 13 Direções e 5 unidades de coordenação autónomas, diretamente dependentes do Conselho de Administração, que desenvolvem atividade quer em áreas de negócio (compras e logística, financeiros, recursos humanos, sistemas e tecnologias de informação e comunicação, bem como serviços de comunicação e media, e gestão e operação do SNS24 e CCMSNS), quer em áreas de suporte às demais Direções, conforme organograma infra.



Sistema de Controlo Interno da SPMS

O Committee of Sponsoring Organizations of the Treadway Commission (COSO) define o controlo interno como “um processo, efetuado por pessoas da direção, da gestão e outro pessoal designado, para fornecer uma certeza razoável acerca do cumprimento dos objetivos quanto à eficácia e eficiência das operações, à fiabilidade dos relatórios e contas e ao cumprimento das leis e regulamentos” (COSO, 2013).

Numa perspetiva mais contabilística, embora com reflexos em toda a atividade de uma organização, o SNC-AP, aprovado pelo Decreto-Lei n.º 192/2015, de 11 de setembro, estabelece no seu artigo 9º que as entidades públicas devem adotar um sistema de controlo interno que englobe, nomeadamente, “...o plano de organização, as políticas, os métodos e os procedimentos de controlo, bem como todos os outros métodos e procedimentos definidos pelos responsáveis que contribuam para assegurar o desenvolvimento das atividades de forma ordenada e eficiente, incluindo a salvaguarda dos ativos, a prevenção e deteção de situações de ilegalidade, fraude e erro, a exatidão e a integridade dos registos contabilísticos e a preparação oportuna de informação orçamental e financeira fiável”.

Neste sentido, devem as organizações desenvolver um sistema de controlo interno adaptado aos seus ambientes institucionais e operacionais, que permita mitigar riscos de ocorrência de erros ou de irregularidades e assegurando que as operações ou os processos sejam executados e decorram em conformidade com o previsto.

O Controlo Interno da SPMS está assente no seu modelo organizativo, em cumprimento do princípio da segregação de funções de administração executiva e de fiscalização, cujas identidades, responsabilidades específicas, remunerações e demais benefícios são divulgados publicamente, tendo, igualmente, criado um modelo de governação ajustado ao controlo interno dos projetos financiados por fundos europeus, no cumprimento do acordo celebrado com a Recuperar Portugal.

O órgão executivo é o Conselho de Administração, composto por 3 membros, com um mandato de 3 anos.

O Conselho Fiscal é o órgão responsável pelo controlo da legalidade, da regularidade e da boa gestão financeira e patrimonial da SPMS.

Na perspetiva de ambiente de controlo, nos termos preconizados pelo COSO, ou seja, o conjunto de normas, processos e estruturas que providenciam a base para

o desenvolvimento do controlo interno da organização, constituem garante do controlo interno a cultura ética e de integridade da instituição, bem como a respetiva regulamentação, constante do Código de Conduta.

O modelo de controlo interno encontra-se suportado no conjunto de normas internas, no repositório de processos internos e formulários e de deliberações do Conselho de Administração, que permitem a clarificação de instruções, estabelecem níveis de responsabilização e implementam medidas para validação de processos e procedimentos.

Na vertente das atividades de controlo, ou sejam as ações estabelecidas através de políticas e procedimentos que permitem assegurar o cumprimento das diretrizes da administração para mitigar os riscos subjacentes à concretização dos objetivos da entidade, nomeadamente no contexto das novas exigências da Cibersegurança, importa referir a importância das Políticas de Segurança de Informação; complementarmente, foi nomeado o Encarregado de Proteção de Dados, por deliberação do Conselho de Administração da SPMS, de 3 de fevereiro de 2021, permitindo o robustecimento da conformidade em matéria de RGPD.

Por outro lado, têm especial relevância enquanto instrumentos de controlo nas áreas de negócio da SPMS: na área das Compras, os procedimentos de compras, que estabelecem os princípios gerais pelos quais se devem reger todos os elementos que integram a área das Compras; na área Financeira, o Manual de Procedimentos de Gestão de Ativos, que integra as regras de classificação e os procedimentos atinentes à gestão patrimonial; na área de Recursos Humanos, o Guia de Acolhimento, enquanto documento orientador das normas internas e da organização, e o Manual de Funções, que constitui o sumário das tarefas, objetivos e responsabilidades exigidos para o desempenho das funções de forma adequada; no Centro de Controlo e Monitorização do SNS, o Manual de Operações do CCM-SNS, enquanto mecanismo de orientação e descrição das atividades de toda a operação, e o Manual de Controlo interno do CCM-SNS, que define os controlos e procedimentos a observar para mitigação dos riscos identificados em cada uma das áreas de atividade da operação.

No âmbito da componente de atividades de monitorização, assumem especial relevância, após a definição de objetivos para os diferentes níveis da organização, explanados no Plano de Atividades, Investimento e Orçamento anual, e em decorrência do Plano Estratégico da instituição, o controlo e monitorização da atividade interna e contratualizada, que é realizada quer através do acompanhamento periódico, em reuniões de Direção, quer através da produção de indicadores e relatórios trimestrais de

execução da atividade; bem como a avaliação da satisfação dos clientes, stakeholders e colaboradores, através de questionários aplicados periodicamente.

Por último, cumpre referir a Unidade de Auditoria Interna e Prevenção da Fraude (AUDIT), enquanto responsável por avaliar o sistema de controlo interno, competindo-lhe comunicar a sua avaliação e recomendar ações corretivas ou de melhoria que devem ser consideradas e implementadas pela administração.

No âmbito da Auditoria Interna, a AUDIT tem como missão proporcionar um serviço independente e objetivo destinado a acrescentar valor e melhorar as operações da organização, designadamente a eficácia dos processos de gestão do risco, de controlo e de governação. Nesta matéria, compete, em especial, à AUDIT, avaliar e monitorizar a eficácia das práticas de gestão de risco implementadas, no sentido de garantir uma gestão eficaz dos riscos associados à missão e objetivos da instituição, constituindo o principal instrumento para este efeito o PGRCIC e o respetivo Relatório de Execução.

Gestão do Risco

O risco, de acordo com a definição do Institute of Internal Auditors (IIA), consiste na “possibilidade da ocorrência de um evento que possa ter impacto sobre o alcance de objetivos. O risco é medido em termos de impacto e probabilidade de ocorrência”, e podem ter origem em fatores internos ou externos à empresa.

São vários os fatores potenciadores de situações que levam a que o desenvolvimento de uma atividade comporte um maior ou menor risco de gestão e de corrupção ou outras infrações conexas, designadamente:

- Qualidade da gestão – idoneidade dos gestores e decisores;
- A ética e conduta da empresa e dos seus trabalhadores;
- O ambiente propício;
- Motivação dos trabalhadores;
- A desadequação do sistema de controlo interno.

De acordo com a definição da ERM-Enterprise Risk Management do Committee of Sponsoring Organizations of the Treadway Commission (COSO), a gestão do risco

é definida como “um processo desenvolvido pela administração, diretores e demais colaboradores de uma organização, aplicado na definição de uma estratégia transversal a toda empresa, concebido para identificar eventos potenciais que possam afetar a organização, e gerir o risco, dentro do nível de risco que a organização está disposta a aceitar, de forma a assegurar um nível de confiança razoável dentro do cumprimento dos objetivos da organização.”

O Conselho de Administração e os dirigentes da SPMS assumem a responsabilidade de promover elevados padrões de ética e integridade e de estabelecer uma cultura na organização que demonstre a todos colaboradores a importância dos controlos internos.

O Conselho de Administração tem a responsabilidade de aprovar e rever as estratégias e as políticas relevantes da SPMS, de compreender os maiores riscos da empresa, estabelecer níveis aceitáveis para tais riscos e assegurar que os dirigentes tomam as medidas necessárias a identificar, medir, monitorizar e controlar tais riscos.

Os riscos são identificados e validados pelos dirigentes, que têm a responsabilidade de implementar as estratégias e as políticas aprovadas pelo Conselho de Administração, de desenvolver processos para medir, monitorizar e controlar os riscos identificados e de manter uma estrutura organizacional que permita identificar claramente as responsabilidades.

A avaliação dos vários componentes de controlo interno e dos mecanismos de controlo instituídos, a confiança e integridade da informação, a conformidade com os planos, procedimentos e regulamentos, a salvaguarda dos ativos e o uso económico e eficiente dos recursos são efetuados de forma sistemática pela função de auditoria interna.

Procurou-se uma análise mais abrangente dos riscos transversais, em função das competências exercidas pela SPMS, mas também dos novos desafios resultantes do recentemente aprovado Regime Geral de Prevenção da Corrupção, através do Decreto-Lei 109-E/2021, de 9 de dezembro, que no seu artigo 5º estabelece a obrigatoriedade de as entidades abrangidas adotarem e implementarem um programa de cumprimento normativo que inclua, pelo menos, um plano de prevenção de riscos de corrupção e infrações conexas, um código de conduta, um programa de formação e um canal de denúncias.

Procurou-se, assim, alinhar este conjunto de documentos, permitindo começar a desenhar o que será o futuro Programa de Cumprimento Normativo, através da

agregação dos riscos transversais em: riscos Estratégicos, riscos Legais e de Compliance, e riscos Operacionais.

Os riscos Estratégicos decorrem de iniciativas que visam aumentar os resultados da organização, quer pela utilização de novas fontes de financiamento, consubstanciadas no PRR, quer no conjunto dos projetos que comportam uma forte componente de inovação.

Os riscos Legais e de Compliance correspondem ao conjunto de riscos que se baseia no cumprimento de regras, tendo por fonte quer a legislação, quer os processos e procedimentos internos aprovados.

Os riscos operacionais compreendem as atividades, funções, tarefas e operações que possam pôr em risco a prossecução da missão e dos objetivos da SPMS, sendo de destacar como principal medida mitigadora o Plano de Continuidade de Negócio.

Foram avaliadas todas as áreas de atividade da SPMS, sejam áreas de negócio ou áreas de apoio interno que, pela sua natureza intrínseca, apresentam vulnerabilidades que podem consubstanciar riscos de gestão, de fraude e de corrupção, articulando com os riscos ligados ao cumprimento normativo, também na vertente de ética e integridade.

Cumprir realçar que o critério adotado na identificação das áreas assentou unicamente na circunstância das mesmas comportarem, em abstrato, a potencialidade da verificação de situações de risco e não na deteção, passada ou presente, de casos suscetíveis de serem qualificados como casos de desvios indesejáveis às regras aplicáveis.

Cada área específica foi objeto de uma apreciação conjunta através de reuniões e entrevistas, nas quais foram identificadas as situações de risco, bem como as medidas de mitigação da probabilidade da sua ocorrência.

No quadro seguinte são identificados os intervenientes, as respetivas funções e responsabilidades, no âmbito da Gestão do Risco, e do presente Plano, em particular.

Decisor	Função e Responsabilidades
Conselho de Administração (CA)	<ul style="list-style-type: none"> • É o gestor do Plano • Estabelece a arquitectura e os critérios de gestão de risco, determinando a revisão do Plano quando necessária.
Diretores e Coordenadores	<ul style="list-style-type: none"> • São os responsáveis pela organização, aplicação e acompanhamento do Plano na parte respetiva; • Responsabilizam-se pela eficácia das medidas de controlo do risco na sua esfera de atuação; • Identificam e comunicam ao CA qualquer ocorrência de risco elevado ou novos que importe prevenir.
Coordenador da Unidade de Auditoria Interna e Prevenção da Fraude	<ul style="list-style-type: none"> • Promove a comunicação com os outros departamentos no âmbito da gestão de riscos; • Acompanha a execução das medidas previstas no Plano; • Desenvolve o acompanhamento através de inquéritos e ações de auditoria específicas; • Procede à revisão do Plano.
Colaboradores	<ul style="list-style-type: none"> • Devem ter consciência da existência de riscos, conhecer o nível de responsabilidade associada e contribuir para a melhoria contínua da gestão de riscos; • Devem comunicar à respetiva Direção/Unidade, de forma sistemática e imediata, todos os riscos ou falhas identificadas nas medidas de controlo existentes.

Metodologia

Para a elaboração do presente Plano foram considerados:

- a)** Recomendações do Conselho de Prevenção da Corrupção, designadamente as de 1.07.2009, de 7.04.2010 (relativa à publicidade dos PGRCIC), de 7.01.2015, sobre a Contratação pública e de 1.07.2015;
- b)** Relatório de execução do Plano de Gestão de Riscos de Corrupção e Infrações Conexas, aprovado pelo C.A. da SPMS em 27.05.2021;
- c)** Regime Geral de Prevenção da Corrupção, aprovado pelo Decreto-Lei 109-E/2021, de 9 de dezembro.

Os riscos foram classificados segundo uma escala: elevado, moderado e fraco, em função do grau de probabilidade de ocorrência e da gravidade/impacto das suas consequências.

Probabilidade de ocorrência:

- **BAIXA:** Possibilidade de ocorrência, mas com hipótese de obviar o evento com o controlo existente para o tratar;
- **MÉDIA:** Possibilidade de ocorrência, mas com hipóteses de obviar o evento através de decisões e ações adicionais;
- **ALTA:** Forte possibilidade de ocorrência e escassez de hipóteses de obviar o evento mesmo com decisões e ações adicionais essenciais.

Impacto previsível:

- **BAIXO:** Afetação da otimização do desempenho ou das atividades operacionais, querendo revisão de procedimentos ou de calendarizações;
- **MÉDIO:** Impacto moderado na imagem institucional ou sobre o desempenho e atividades operacionais querendo reorganização de processos ou recursos;
- **ALTO:** Prejuízo na imagem e reputação institucional, ou impacto significativo sobre a estratégia, o desempenho e atividades operacionais.

Do cruzamento das variáveis probabilidade e impacto resulta a seguinte matriz de risco, que é aplicada a cada um dos riscos potenciais identificados para a organização.

Matriz de Risco		Impacto		
		BAIXO	MÉDIO	ALTO
PROBABILIDADE	BAIXO	FRACO	FRACO	MODERADO
	MÉDIO	FRACO	MODERADO	ELEVADO
	ALTO	MODERADO	ELEVADO	ELEVADO

Para cada risco potencial, foram identificadas medidas preventivas que se destinam a:

- EVITAR o risco, eliminando a sua causa;
- PREVENIR o risco, procurando minimizar a probabilidade de ocorrência do risco ou do seu impacto negativo;
- ACEITAR o risco e os seus efeitos;
- TRANSFERIR o risco para terceiros.

Pese embora sejam utilizadas diferentes formulações, as medidas preventivas/de mitigação correspondem, na generalidade dos casos, aos seguintes meios de defesa e controlo:

- a)** Monitorização do Código de Conduta e respetivas normas de operacionalização;
- b)** Preparação e tomada de decisões assente numa estrutura mista, combinando validações hierárquicas com incorporação de especialistas e stakeholders na gestão dos riscos estratégicos;
- c)** Aplicação, na validação de processos, do princípio da segregação de funções entre os diversos intervenientes e entre vários níveis hierárquicos;
- d)** Aplicação de controlos gerais dos sistemas informáticos e de controlos aplicativos;
- e)** Existência ou necessidade de elaboração de procedimentos ou manuais de boas práticas.

Monitorização do Plano

A AUDIT procede ao acompanhamento periódico do Plano, elaborando, para o efeito, um relatório anual.

O acompanhamento anual do Plano deve basear-se na análise das respostas das Direções/Unidades envolvidas, através de formulários e ações específicas, elaboradas pela AUDIT.

O processo de acompanhamento deve garantir que são implementados os mecanismos

de controlo adequados para as atividades da empresa e que os procedimentos sejam compreendidos e seguidos em todos os níveis organizacionais.

No âmbito da gestão dos riscos associados à inovação podem ser criadas novas modalidades de avaliação de risco, partilhadas com grupos de especialistas dos stakeholders ou da academia.

Para além da periodicidade das revisões e atualizações acima indicadas, os Diretores/ Coordenadores responsáveis devem informar o CA sempre que surjam riscos elevados ou novos que importe prevenir.

Revisão do Plano

O Plano de Gestão de Riscos será revisto sempre que se verifiquem alterações legislativas aplicáveis à SPMS, designadamente aquelas que tenham impacto na sua orgânica, atribuições, objetivos, ou alteração de atividades, serviços, instalações, ou sempre que sejam identificados novos riscos ou a necessidade da sua reavaliação ou da sua significância, em função do resultado do relatório de execução anual ou de outros mecanismos de acompanhamento a criar .

Identificação dos riscos e medidas preventivas a adotar

Transversais a toda a organização

	RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Riscos Estratégicos	Não execução de projetos, no âmbito do Contrato Programa com a ACSS, do PRR, ou outros	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Elaboração do Plano Estratégico Garantir o alinhamento e a definição de prioridades nos projetos 	CA e DPDO
	Orçamento insuficiente para as aquisições necessárias ao cumprimento das competências das Direções, das atribuições da SPMS e dos requisitos legais	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Identificação das prioridades na atividade das várias Direções, em face das disponibilidades financeiras Diversificação de fontes de financiamento, através do PRR Revisão das necessidades aquisitivas de bens e serviços 	CA e DPDO DAG
	Inadequada partilha de responsabilidades na gestão da inovação	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Utilização de grupo de especialistas, sempre que aplicável, quer no decurso do projeto, quer na gestão e mitigação dos riscos que lhe estão associados. Estabelecimento de parcerias com a Academia como método preferencial de mitigação dos riscos de reputação associados a projetos com potenciais impactos disruptivos 	DCNTS, SNS 24, DSI DCCM
Riscos Legais e de Compliance	Ausência ou falta de uniformização de procedimentos	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Identificação de práticas não normalizadas Modelação e caracterização de processos internos das práticas não normalizadas 	CA e DPDO DPDO
	Falta de cumprimento dos procedimentos internos aprovados pelo CA	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Promover a implementação dos processos internos à medida que vão sendo aprovados pelo CA, através de reuniões internas para apresentação, sensibilização e esclarecimento de dúvidas Divulgação por email e publicação na intranet de todos os processos internos existentes bem como de uma grelha síntese (nome, descrição sumária, etc.) 	DPDO e AUDIT DCRP
	Conflito de interesses, quer no exercício de funções, quer após a respetiva cessação	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Assinatura de Declaração de Conhecimento e Compromisso do Código de Conduta por todos os que desenvolvem atividade na SPMS ou para a SPMS (colaboradores internos e prestadores de serviços externos, membros de júri, etc.). Realização de procedimentos de controlo, nos termos das normas de operacionalização do Código de Conduta. Cumprimento de procedimento obrigatório de submissão de pedido anual por parte dos trabalhadores que pretendam acumular funções. 	Todas as Direções envolvidas CA e DRH
	Ocorrência de situações integráveis no conceito de fraude	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Assinatura, pelo CA, de Declaração de Política Antifraude no âmbito da gestão de projetos financiados por fundos comunitários. Elaboração de Manual de Gestão e Avaliação do Risco de Fraude, incluindo os riscos inerentes ao PRR. 	CA AUDIT
	Fuga de informação, violação de segredo, quebra de confidencialidade ou utilização indevida de informação sigilosa	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Assinatura de Acordo de Confidencialidade, por entidades e colaboradores externos, sempre que esteja em causa o acesso a informação sigilosa e sensível. Implementação de Políticas de Utilização Aceitável no contexto das Políticas de Segurança da Informação. Definição dos processos internos para cedência de informação (universidades, instituições do MS, autoridades judiciais, de fiscalização e auditoria), em conformidade com o Regulamento Geral de Proteção de Dados 	DAG DSI DPDO
	Falta de cumprimento dos prazos e procedimentos inerentes às formalidades administrativas internas (ex.: informações a CA, submissão de boletins de itinerário, pedido para realização de trabalho suplementar, pedidos de autorização prévia, etc.)	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Alargamento da plataforma de gestão documental a todas as unidades orgânicas da organização, que permita rastrear todos os procedimentos inerentes às formalidades administrativas Desmaterialização de todo o processo relacionado com as informações a CA (desde a elaboração, aprovação e produção de ata). Publicação de informação (FAQ's na intranet, por exemplo) com descrição de direitos e deveres, normas e procedimentos inerentes a direitos e deveres dos colaboradores (ajudas de custo, trabalho suplementar, deslocações, parentalidade, etc.) 	DSI DRH
	Assunção de despesa sem prévia autorização	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração de processo que defina as diferentes fases de autorização/execução da despesa, assegurando a segregação de funções e rastreabilidade de decisões, e que integre as aplicações informáticas utilizadas 	DF
	Inconformidade legal dos procedimentos de contratação	MÉDIA	ALTO	MODERADO	<ul style="list-style-type: none"> Criar condições para garantir a segregação de funções sempre que exista a necessidade de obter parecer jurídico ou segunda apreciação em especial na área da Contratação Pública 	CA, DAJC, DAG, CCS
	Dissimulação ou não deteção de comportamentos de trabalhadores não conformes aos princípios éticos do Código de Conduta	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Realização de ações de sensibilização a dirigentes e trabalhadores sobre riscos de corrupção e medidas de prevenção Publicitação do Regulamento de Comunicação de Irregularidades, no site institucional e intranet 	AUDIT

RISCO POTENCIAL		PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Riscos Operacionais	Inadequada gestão da continuidade de negócio	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Análise de impacto de negócio Análise de risco Identificação de cenários de risco Sessões de awareness para sensibilização e aumento do nível de maturidade organizacional no âmbito da continuidade de negócio 	Todas as áreas envolvidas
	Inadequada gestão dos contratos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração de "Guia Prático da Boa Gestão Contratual", a desenvolver conjuntamente entre as diferentes Direções. Este guia deve ser divulgado por todos os colaboradores e prestadores de serviços em funções e pelas novas contratações (internos e externos). Envio do contrato e respetiva parte integrante ao responsável pela validação e conferência das faturas associadas Monitorização do prazo médio de validação de faturas, por colaborador. Reporte dos incumprimentos parciais ou totais dos contratos de modo a ser possível acionar as devidas penalizações 	Todas as áreas envolvidas DAG DF DAG
	Dificuldade de retenção de colaboradores	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Criar as condições para assegurar uma adequada motivação dos colaboradores e respetiva gestão de carreira 	CA e DRH
	Elevada dependência de recursos externos para o cumprimento dos objetivos das Direções	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Criação de procedimentos internos e de métodos de trabalho em equipa que permitam a disseminação e retenção do conhecimento 	Todas as áreas envolvidas

Conselho de Administração

RISCO POTENCIAL+B3:G15	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Sujeição da atuação CA a pressões externas	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Envolvimento de todos os colaboradores na elaboração final dos Planos de cariz estratégico e Planos anuais de Atividade através do envio pelo CA da versão preliminar com pedido de contributos. Realização de reuniões internas periódicas de acompanhamento, avaliação e monitorização dos objetivos, metas e resultados. Avaliação e monitorização dos programas de financiamento, de acordo com os modelos de governação aprovados. Ampla divulgação interna e publicação na intranet do Contrato Programa com a ACS, demais contratos com restantes clientes, bem como parcerias e contratos interadministrativos e contratos de financiamento comunitário. 	Conselho de Administração
Utilização indevida de recursos ou de competências, para finalidades diferentes das atribuições legais da organização	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Delegação de competências dos membros do CA devidamente identificada e publicada no site da SPMS e intranet, constituindo-se também como repositório. Processos validados por vários intervenientes de vários níveis hierárquicos 	
Ausência de uniformização de procedimentos, normas, métodos, técnicas ou atuação da organização relativamente a atividades críticas ou prioritárias	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Promoção da documentação e comunicação generalizada dos procedimentos, normas, métodos e técnicas a adotar na organização. Acompanhamento e supervisão hierárquica da atividade. 	
Não cumprimento do Plano anual de atividades da organização e/ou outros específicos de cada Direção (Plano de Compras, Plano de Comunicação, Plano de Auditorias, etc.)	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Acompanhamento dos relatórios de execução com identificação precisa do motivo que originou o não cumprimento das atividades planeadas bem como capítulo com a descrição das atividades extra-Plano realizadas. 	
Utilização/divulgação indevida de informação privilegiada	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Cumprimento dos princípios e regras do Código de Conduta, promovendo uma cultura de compromisso permanente com a integridade 	
Deliberações não conformes com a legalidade ou procedimentos internos	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Remessa, para auscultação ou esclarecimento pelas Direções, das informações submetidas a CA, sempre que suscitada dúvida sobre alguma matéria Deliberação pelo C.A., por regra, apenas sobre os documentos e informações constantes da agenda da reunião, e cujo envio seja efetuado até ao prazo constante de procedimento interno aprovado, garantindo um melhor conhecimento por todos os membros do CA das respetivas matérias 	

Direção de Administração Geral

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Favorecimento ilícito de fornecedores	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> • Informar todas as Direções e unidades da SPMS sobre fornecedores, cujo preço contratual acumulado seja igual ou superior aos limites legalmente estabelecidos, para o ajuste direto • Segregação de funções entre quem executa os procedimentos aquisitivos e quem verifica os documentos de habilitação. • Criação de equipas multidisciplinares para Procedimentos de TI com especial complexidade • Definição das especificações do objeto e parte técnica de forma concreta, objetiva e pormenorizada • Garantir a rotatividade dos elementos do júri, nos procedimentos de contratação, aumentando o número de vogais do júri da área que solicitou a aquisição • Recurso ao critério de avaliação da proposta economicamente mais vantajosa nas modalidades monofactor ou multifactor, adequando à necessidade da entidade adjudicante, com fatores objetivos de qualidade 	DAG
<p>Conflito de interesses nos procedimentos de contratação pública, que se pode expressar através de:</p> <ul style="list-style-type: none"> - Favorecimento de interesses alheios ao procedimento; - Fuga de informação; - Incorrecta apreciação das capacidades dos proponentes. 	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> • Subscrição por parte de todos os trabalhadores de declarações de inexistência de conflitos de interesse relativamente a cada procedimento que lhe seja confiado no âmbito das suas funções, e no qual, de algum modo, tenha influência • Divulgação do Código de Conduta da SPMS e das normas de operacionalização e realização de ações de sensibilização para o seu cumprimento • Desenvolvimento de ações de controlo para verificação do cumprimento das várias fases dos procedimentos contratuais, em especial as que envolvem uma apreciação sobre a capacidade do candidato ou podem levar à exclusão do procedimento, bem como para o cumprimento das normas de operacionalização do Código de Conduta 	AUDIT
Atraso na tramitação dos procedimentos inerentes à formação de contratos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> • Atualização do Manual de Boas Práticas de Contratação Pública da SPMS • Automatização dos procedimentos associados à formação de contratos. • Uniformização de Procedimentos das Equipas relativos às Comunicações e Notificações a efetuar na Plataforma Eletrónica de Contratação. • Elaboração e monitorização do Plano anual de Compras. • Redução de tempos de tramitação interna (esclarecimentos sobre especificações técnicas, avaliação de propostas, documentos financeiros) • Controlo dos prazos de envio de processos para o Tribunal de Contas. Resposta às questões dentro dos prazos. 	DAG
Inconformidade legal dos procedimentos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> • Elaboração do Manual de Boas Práticas de Contratação Pública da SPMS • Garantir a segregação de funções sempre que exista a necessidade de obter parecer jurídico ou segunda apreciação sobre a mesma questão 	DAG, CCS DAG, DAJC
Deficiente gestão/acompanhamento da execução de contratos	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> • Segregação de Funções entre Procedimento de Compra e Execução do Contrato, através do Núcleo próprio, que assegura o controle e monitorização da execução do contrato. • Integração de Equipa multidisciplinar segregada, no contexto da execução dos contratos financiados por programas comunitários 	DAG DAG, DF e DPDO
Perda ou extravio de documentação relativa aos procedimentos aquisitivos	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> • Assegurar que a divulgação de informação interna de procedimentos de aquisição com outras Direções ocorre com o conhecimento do Coordenador ou Diretor, promovendo a cedência de documentação por email ou outra ferramenta análoga (one drive), com responsabilidade institucional. 	
Sub ou sobreavaliação das necessidades reais de consumíveis para o regular funcionamento da instituição	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> • Existência de histórico relativo a aquisições, gastos e consumos de consumíveis, por rubricas (eletricidade, limpeza, vigilância, economato, máquinas purificadoras de água, gasóleo, limpeza de esgotos, limpeza ar condicionado, etc.). • Assegurar a segregação de funções entre o responsável pelo levantamento das necessidades (UAG) e pela elaboração das peças procedimentais para contratação de bens e/ou serviços (DAG-UAP) e acompanhamento da execução do contrato (DAG-NEC). 	DAG

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Uso indevido de instalações, equipamentos e veículos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Obrigatoriedade de autorização prévia da UAG para entrada nos edifícios fora do horário regular de trabalho. Esta informação deve ser veiculada por Circular Interna a todos os colaboradores da SPMS, com esclarecimento de conceitos e todos os procedimentos necessários. Todas as entradas e saídas nos edifícios da SPMS fora do horário regular de trabalho devem constar do relatório de segurança. Garantir o devido cumprimento do Regulamento de Utilização da Garagem Monitorização da execução do Regulamento relativo à atribuição e utilização de telemóveis. Registo de todos os telemóveis que são disponibilizados aos colaboradores, em articulação com a DRH para que aquando a saída do colaborador da instituição seja devolvido todo o material que lhe foi atribuído e com a DF para efeitos de inventário. Apoiar a DF na gestão dos ativos, nomeadamente na etiquetagem e deslocação de material dentro do edifício, sinalizando essa deslocação para o email dos ativos. Garantir a segurança e usabilidade do material à sua guarda 	DAG
Falta de garantia da segurança e higiene no trabalho	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Desenvolvimento de Plano anual de Intervenção na área da segurança e higiene no trabalho e respetivo Plano de Execução a apresentar a CA e a publicar no site da SPMS e intranet. Garantir formação dos colaboradores na área da segurança e higiene no trabalho. 	
Falta de garantia de segurança nos edifícios	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Divulgação do Plano de Segurança e Normas de Segurança dos Edifícios a todos os colaboradores, publicação na intranet e promoção de formação nesta área a todos os colaboradores. Desencadear Auditorias regulares à segurança dos edifícios, com relatório de inconformidades e recomendações. Desenvolvimento de Relatórios de execução detalhados relativos às recomendações identificadas nos Relatórios de auditorias/vistorias realizadas aos edifícios. 	
Produção de resíduos e sua incorrecta segregação, não contribuindo para uma política ambiental sustentável	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Disponibilização preferencial de documentos por via eletrónica e utilização preferencial de plataformas digitais, incluindo comunicação de e para o exterior Disponibilização de dispensadores de água, de forma a evitar a aquisição de garrafas de água Colocação de contentores específicos para pilhas em local visível Gestão de resíduos, segregação, encaminhamento e retoma 	DAG e DSI DAG

Direção de Assuntos Jurídicos e Contencioso

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Ausência de imparcialidade e rigor na emissão de pareceres de modo a favorecer ou prejudicar intencionalmente algum(ns) colaborador(es)	MÉDIA	ALTO	MODERADO	<ul style="list-style-type: none"> Garantir que a estrutura hierarquizada de decisão permite vários níveis de análise sobre as mesmas matérias. 	DAJC
Fuga de informação confidencial	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Implementação de medidas que garantam a privacidade das reuniões presenciais e teleconferências Participação em Políticas de Segurança da Informação, designadamente na prática selectiva de procedimentos de credenciação Criação de sistema de alerta para data de término dos prazos 	DAJC, DSI I, UPDCS, AUDIT
Não cumprimento de prazos de resposta às solicitações internas ou entidades externas	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Monitorização da demora média de resposta e dias de resposta acrescidos em relação ao prazo estipulado, no que respeita a pedidos de parecer internos Consulta diária ao Diário da República online e/ou outras Bases de Dados Jurídicas e compilação da informação relevante para a organização Envio diário a todas as Direções e publicação na intranet de legislação com relevância para a SPMS 	DAJC
Desconhecimento da publicação de diplomas legais e jurisprudência de interesse para a SPMS	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Envio diário a todas as Direções e publicação na intranet de legislação com relevância para a SPMS 	DAJC, DCRP
Apropriação indevida de Propriedade intelectual	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Adopção de procedimentos de registo, se aplicável, para garantia da proteção de direitos de propriedade intelectual 	DSI, DAJC
Incorrecta gestão dos protocolos elaborados na SPMS	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Revisão e atualização do procedimento relativo à elaboração, execução e gestão de protocolos 	DAJC, DPDO
Inconformidade legal dos procedimentos de contratação	MÉDIA	ALTO	MODERADO	<ul style="list-style-type: none"> Garantir a segregação de funções sempre que exista a necessidade de obter parecer jurídico ou segunda apreciação sobre a mesma questão relativamente à área da Contratação Pública 	DAJC, DAG, AUDIT

Direção Financeira

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Falhas intencionais nas transações financeiras (pagamentos, recebimentos)	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Garantir a segregação de funções, entre quem processa no sistema de informação e quem confere Garantir que a aplicação informática de gestão financeira permite integrar as diferentes fases de autorização/ execução da despesa em ordem a assegurar segregação de funções e rastreabilidade de decisões Garantir que a autorização para pagamento apenas é desencadeada quando existe comprovativo de devida validação da fatura Validação prévia de faturas provisórias de clientes antes de passagem a definitiva Proceder mensalmente à reconciliação de contas (Clientes e Fornecedores) por profissional não afeto a esta tarefa 	DF
Utilização indevida do cartão de crédito	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Assegurar a segregação de funções entre o colaborador com autorização para efetuar pagamentos com cartão de crédito da empresa e o colaborador responsável pelo controlo dos despesas efetuadas e cruzamento da informação dos processos de compras 	
Assunção de compromissos sem fundos disponíveis	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Assegurar que não são autorizadas despesas sem validação financeira, mediante prévia obtenção de comprovativo de suficiência orçamental para a despesa em apreço 	CA e DF
Falhas intencionais nas diferentes fases do ciclo de gestão de ativos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Cumprimento rigoroso do processo interno "Gestão de Ativos", publicado em Circular Interna nº1/2017, de modo a garantir-se uma correta gestão de ativos, designadamente o seu registo, controlo e gestão de ciclo de vida Etiquetagem e registo imediato dos novos artigos rececionados 	DF
				<ul style="list-style-type: none"> Desenvolvimento de inventários físicos periódicos conjuntos entre a DF/UAG (bens gerais) e DF/DSI (material informático), com identificação da localização Reporte semestral ao CA dos equipamentos que não estão a ser utilizados para que este determine o fim a dar aos mesmos 	DF, DAG
				<ul style="list-style-type: none"> Articulação com a DAG para que esta unidade orgânica avise a DF da data de chegada dos bens, para imediata inventariação Migração para o sistema de gestão financeira (SICC) da informação relativa à gestão de ativos 	
Reduzido acompanhamento do trabalho dos Auditores Externos/Inspetores ou prestação de informação pouco rigorosa ou falsa	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Criação de perfis de acesso à aplicação informática de gestão financeira (SICC), de acordo com as responsabilidades e âmbito de auditoria/inspeção 	DF
Pagamentos em atraso	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Controlo periódico dos tempos de pagamentos através de relatórios extraídos da aplicação informática de Contabilidade e do MySPMSdoc Melhoria das taxas de entregáveis a clientes com impacto na antecipação da receita, indispensável para que a estimativa mensal de Fundos Disponíveis seja a mais real possível 	DPDO, DSI
Falta de prestação atempada e/ou correta de informação contabilística e fiscal (ex. Entrega não atempada ou incorreta de declarações fiscais, atraso nos pagamentos à Autoridade Tributária e Segurança Social, incumprimento de obrigações legais e de reporte a entidades externas).	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Elaboração anual de calendário com prestações de informação contabilística e fiscal já previstas Atualização deste calendário à medida que são cumpridas as obrigações, com a identificação da data em que foram efetivadas, e submissão a CA trimestralmente 	DF
				<ul style="list-style-type: none"> Estabelecimento de diferentes níveis de validação e aprovação da informação 	
Deficiente controlo financeiro na execução de projetos no âmbito de fundos comunitários	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Integração de Equipa multidisciplinar segregada, no contexto da execução dos contratos financiados por programas comunitários 	DF, DAG e DPDO
Falta de prestação atempada de informação no âmbito dos projetos comunitários	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Definição de normas de operacionalização de cada projeto, com identificação de ações, responsabilidades e tempos de resposta 	DF, UPRI
Falta de prestação atempada de informação no âmbito do SITAM (ex. Não garantia dos pagamentos com regularidade)	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Definição de normas de operacionalização de cada projeto, com identificação de ações, responsabilidades e tempos de resposta 	DF
Inadequado processo de registo de todas as operações ao longo do ciclo de despesa, desde o processo de tomada de decisão ao pagamento	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração conjunta de processo com definição das responsabilidades, registo e circularização da informação de todo o ciclo da despesa, que permita uma adequada rastreabilidade para efeitos de auditoria 	DF, DAG e DPDO

Direção de Recursos Humanos

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Favorecimento ilícito na escolha de recursos humanos a contratar	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Definição de critérios objetivos e precisos, com reduzida margem de discricionariedade, aplicável quer ao curriculum vitae (CV) quer à entrevista Constituição de júri para avaliação de candidatos (CV e entrevista) Composição do júri deve variar de processo para processo e ser composto por elementos da DRH e outros (s) responsáveis ou técnicos da área do posto de trabalho a ocupar Divulgação, no site da SPMS, das regras aplicáveis aos processos de recrutamento e seleção na SPMS 	DRH
Fuga de informação dos processos individuais dos colaboradores	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Definição e divulgação aos colaboradores da DRH dos procedimentos/normas internas de segurança a adotar no que respeita à preservação da informação constante nos processos internos dos colaboradores 	
Erros intencionais no processamento de vencimentos, abonos ou descontos	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Segregação de funções entre colaboradores responsáveis pelo registo da informação necessária para o devido processamento de remunerações, outros abonos e descontos e o responsável pelo processamento em si mesmo Garantir a devida gestão de acessos às aplicações de suporte à atividade da DRH (RHV, SGA, etc.) - perfis de acessos de acordo com as funções a desempenhar e histórico de acessos 	
Favorecimento de entidades formadoras	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Elaboração, até ao final do ano anterior, de um Plano Anual de Formação de acordo com as necessidades formativas identificadas no plano individual de formação dos colaboradores Elaboração, até ao final do ano anterior, de matriz com a identificação dos cursos, o número de propostas recebidas e os critérios de seleção do fornecedor para a realização da formação Efetuar consulta ao mercado para desenvolvimento de formação profissional certificada, para dar resposta ao Plano de Formação anual, de forma a obter as condições mais vantajosas 	
Dificuldade de retenção de colaboradores	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Elaborar propostas de medidas com reflexos na motivação, baseados em inquéritos de satisfação Elaboração de proposta de sistema de avaliação, em articulação com um modelo de progressão de carreiras 	
Não suprimento de saída de colaboradores	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Garantir a adequada instrução (técnica, estratégica e legal) dos pedidos de autorização para recrutamento dirigido à Tutela. 	
Inadequado alinhamento dos objetivos individuais com os objetivos estratégicos da organização	MÉDIA	BAIXO	FRACO	<ul style="list-style-type: none"> Elaboração e implementação de um regulamento de avaliação de desempenho adequado e aplicável a todos os trabalhadores da SPMS Elaboração/revisão de manual de análise e descrição de funções. 	

Direção de Planeamento e Desenvolvimento Organizacional

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Gestão/monitorização deficiente dos Contratos Programa	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Cumprimento do processo estabelecido, que permite rastrear todo o processo de gestão e execução do contrato programa, desde a expressão da necessidade, preparação do contrato, identificação do grau de execução das metas e ordem de faturação ou cobrança. Reporte mensal ao Conselho de Administração e às Unidades de Negócio da execução dos projetos, com base na monitorização feita previamente. 	DPDO
Dificuldade na gestão de projetos no âmbito do PRR	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Garantir o adequado funcionamento do Modelo de Governação. Promover o cumprimento das melhores práticas e metodologia de Gestão de Projetos. Incorporar uma metodologia de monitorização de resultados, para efeitos de avaliação global de cada projeto. Revisão das versões finais dos documentos por outros elementos da equipa e/ou stakeholders envolvidos (internos e externos). 	
Produção de documentos com informação falsa ou inexata	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Assegurar o sistema de reporte da atividade interna e validação dos dados comunicados, procurando automatizar o sistema existente. Reporte periódico ao Conselho de Administração, dos resultados da atividade interna. 	
Gestão/monitorização deficiente da atividade interna	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Catálogo de instrumentos de gestão, onde consta a calendarização para a sua elaboração ou revisão e respetivos responsáveis Assegurar a coordenação da aplicação de questionários de satisfação. Envolvimento de clientes, stakeholders e utentes nas etapas dos projetos consideradas relevantes. 	
Incumprimento dos prazos na elaboração dos documentos institucionais	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Disponibilização do catálogo dos processos a toda a organização. 	
Ausência de informação relativamente à satisfação dos clientes, stakeholders e utentes da SPMS	BAIXA	BAIXO	FRACO		
Desconhecimento Interno dos Processos estabelecidos pela SPMS	BAIXA	BAIXO	FRACO		

Direção de Comunicação e Relações Públicas

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Prestação de informação inexacta aos órgãos de comunicação social	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Garantir que a informação enviada para o exterior é sempre escrita e validada pelo Diretor de Comunicação e Relações Públicas e pelos membros do CA 	DCRP
Publicação de conteúdos inexactos ou de informação com erros	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Elaboração de manual de procedimentos que contemple o estabelecimento de diferentes níveis de validação e aprovação da informação a publicar 	
Comunicação extemporânea de informação em situações de crise	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Cumprimento do disposto no capítulo sobre Gestão de Crise no âmbito do Plano de Contingência 	
Ausência de uniformização e identificação das linhas gráficas dos portais das entidades do Ministério da Saúde	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Implementação das guidelines de uniformidade gráfica e boas práticas de webdesign para a criação dos portais do SNS e das entidades do Ministério da Saúde 	
Falta de planeamento da atividade, que conduza a uma deficiente avaliação das necessidades de aquisição de serviços.	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Desenvolvimento de Plano anual de Comunicação, que inclua as necessidades de aquisição de forma a privilegiar a adoção de procedimentos de aquisição concorrenciais 	
Deficiente avaliação das necessidades aquisitivas de serviços, devido à dificuldade de planeamento exaustivo das ações de comunicação anuais, atenta a imprevisibilidade de algumas atividades	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração de procedimento interno que preveja prazos mínimos para solicitação dos serviços internos da DCRP Levantamento de necessidades aquisitivas atempado, articulado com o Plano de Compras 	
Incumprimento do prazo estipulado de resposta às solicitações das unidades orgânicas internas e/ou entidades externas	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Desenvolvimento de Plano anual de Comunicação Desenvolvimento de processo interno relativo ao tratamento de pedidos/respostas a unidades orgânicas internas e/ou entidades externas que permita fazer uma uniformização e priorização dos mesmos 	
Ineficiente organização/gestão de eventos	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Criação de comissões organizadoras dos eventos, representativas das diferentes áreas de negócio envolvidas 	
Cumprimento da Lei n.º 95/2015, de 17 de agosto, na realização de campanhas de publicidade institucional do Estado	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Elaboração de checklist para validação do cumprimento da Lei sobre Publicidade institucional do Estado 	DCRP, DAIC

Gabinete de Apoio ao Conselho de Administração

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Ineficiente triagem de expediente com consequências na demora nos tempos de resposta a pedidos externos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração/revisão de processo sobre fluxo do expediente e aprovação de documentos internos 	GAC
Ocultação, desvio ou incorreto encaminhamento de documentação com fins ilícitos	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Enviar sempre para o redator do ofício cópia do mesmo após aposição de carimbo de saída. Cumprimento do procedimento sobre fluxo do expediente e aprovação de documentos internos 	
Ineficiente controlo de aprovação de atos pelos membros do CA, no âmbito da delegação de competências	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Verificação, pela Coordenação da Unidade, da aprovação de atos administrativos, em cumprimento da delegação de competências do CA 	
Erros/falhas na elaboração/ transmissão das deliberações ou atas das reuniões do CA	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Agendamento das reuniões do Conselho de Administração pelo secretariado do CA, através de sistema de correio eletrónico Revisão do texto das atas das reuniões do Conselho de Administração por jurista do GAC 	

Unidade de Projetos e Relações Internacionais

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Rejeição da candidatura, não participação ou devolução do financiamento dos custos por parte da Comissão Europeia, na altura do reporte ou em resultado de uma possível auditoria	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Melhor articulação entre as várias unidades da SPMS envolvidas no processo de reporte financeiro (UPRI, DF, DRH, DCRP, DAG, etc.) e também com as empresas empregadoras dos recursos externos Automatização do report de horas global por parte dos colaboradores (internos e externos) que colaborem nos projetos nacionais e/ou internacionais 	UPRI, DF, DRH, DCRP, DAG
Ineficiente acesso, utilização de financiamento e participação em projetos internacionais	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Envolvimento das unidades orgânicas na conceção, candidatura e desenvolvimento dos projetos internacionais 	

Unidade de Auditoria Interna

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Ausência de efetiva monitorização de todas as atividades de controlo interno	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Elaboração de um Plano Anual de Auditorias para o ano seguinte, a apresentar até ao final do ano anterior Planeamento de ações de follow up às áreas auditadas Elaboração de relatório anual de execução do Plano de Gestão de Riscos Corrupção e Infrações Conexas e sua atualização/revisão, sempre que necessário 	AUDIT
Falta de isenção e imparcialidade técnica nas atividades de auditoria	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Realização de trabalho de campo por 2 técnicos da AUDIT Validação do relatório de auditoria por outro técnico que não o redator 	
Utilização/divulgação de informação privilegiada ou confidencial para benefício próprio ou de terceiros	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Elaboração de Manual de Auditoria Interna, incorporando a descrição das fases da Auditoria e o estatuto dos colaboradores, que desenvolvem atividade na Unidade de Auditoria e Prevenção da Fraude 	
Utilização de modelos risco desatualizados na monitorização da despesa e prevenção da fraude do SNS	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Revisão e atualização contínua dos modelos de risco e monitorização, de acordo com a legislação em vigor e com as melhores práticas em matéria de prevenção da fraude Realização de reuniões regulares com stakeholders (Entidades Inspetivas, de fiscalização, Judiciais ou de Auditoria interna) 	
Baixa qualidade de dados que servem de análise às atividades de exploração de informação, o que potencia falha na monitorização e na identificação de riscos de fraude	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Intervenção da Unidade de Auditoria e Prevenção da Fraude por via de testes substantivos Recomendações de melhoria da qualidade dos dados, resultante de testes efectuados 	
Não cumprimento dos prazos de resposta adequados aos pedidos provenientes de entidades externas	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Aprovação de processo interno que defina as responsabilidades das várias unidades orgânicas, tratamento e confidencialidade, bem como cumprimento dos prazos de resposta 	
Favorecimento de interesses pessoais, familiares, de terceiros ou uso indevido de informação privilegiada	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Automatização da aplicação do modelo de risco, reduzindo a intervenção humana na produção de resultados Elaboração de procedimentos internos que contemplem as atividades e matriz de responsabilidades da análise de risco no âmbito da prevenção da fraude Constituição de equipa de trabalho maioritariamente por recursos internos da SPMS 	

Unidade de Proteção de Dados e Cibersegurança

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Quebra de segurança associada ao comportamento do utilizador	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Ações de sensibilização e ações de formação aos utilizadores, no âmbito do Programa de Awareness and Training do Núcleo de Cibersegurança 	UPDCS, Academia
Incumprimento dos prazos de resposta a pedidos remetidos por entidades externas (Titular dos Dados, Autoridade de Controlo, Clientes e Fornecedores)	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Desenvolver um sistema de alertas relativo à tramitação dos processos Estabelecimento de prazos máximos de resposta no âmbito do procedimento criado para "Avaliar pedidos de cedência de dados" 	UPDCS
Inexistência de registo de tratamento de dados pessoais	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Definição de Procedimento para o registo de tratamento de dados pessoais Implementação de sistema de registo de tratamento de dados pessoais 	
Ausência de avaliações de impacto na proteção de dados (DPIA)	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Definição de Procedimentos para elaboração de DPIA dos tratamentos de dados pessoais Inventariação atualizada dos tratamentos de dados pessoais 	
Atraso na comunicação à CNPD de situações de violação de dados pessoais	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Implementação dos controlos técnicos para deteção de situações de violação de dados pessoais Definição de processo de comunicação à CNPD 	
Incumprimento da obrigação de comunicação ao titular dos dados de situações de violação de dados pessoais	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Definição de processo de comunicação de situação de violação de dados pessoais aos titulares dos dados 	
Inexistência de registo dos pedidos dos titulares dos dados e da garantia da sua autenticidade	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Definir processo para a disponibilização da informação solicitada pelos titulares dos dados Disponibilizar plataforma para pedidos no âmbito do exercício de direitos, garantindo a autenticidade dos titulares 	
Dificuldade na implementação das alterações legislativas no âmbito da Cibersegurança e da Diretiva NIS	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Integração dos Sistemas de Informação da SPMS com o Sistema de Gestão de Eventos de Segurança (SIEM) 	
Atraso na comunicação de Incidentes de Cibersegurança	ALTA	ALTO	ELEVADO	<ul style="list-style-type: none"> Definição de processo de comunicação ao CNCS dos Incidentes de Cibersegurança 	
Intrusão ou ataque informático	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Monitorização e deteção proativa de ataques de cibersegurança através da equipa CSIRT SPMS Implementação do Plano Operacional da ENSC 2.0 - Estratégia Nacional da Segurança do Ciberespaço Realização de auditorias de verificação de vulnerabilidades dos sistemas, em termos de segurança de informação 	

Centro de Contacto do SNS

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Gestão/monitorização irregular do Contrato com fornecedor do Centro de Contacto	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Criar as condições adequadas para proceder ao cálculo de SLA's pela entidade adjudicante. Apresentação de documentação de suporte à validação de faturas. 	Centro de Contacto do SNS
Desenho incompleto ou incorrecto de novos serviços, devido à urgência na sua implementação	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Formalização da comunicação dos pedidos de novos serviços ao operador Validação da implementação dos novos serviços Fundamentação da utilização da bolsa de horas do contrato com o fornecedor do Centro de Contacto 	
Publicação de conteúdos desatualizados no site do SNS 24	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Cumprimento dos protocolos celebrados com sociedades científicas ou stakeholders institucionais Criação e gestão de alertas de necessidade de atualização de conteúdos 	
Incapacidade para contribuir para a melhoria contínua e proactiva dos serviços implementados	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Utilização da gestão de reclamações para efeitos de introdução de melhorias 	

Centro Nacional de Telessaúde

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Favorecimento na produção de pareceres técnicos no âmbito da TeleSaúde	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Formulação de pareceres gerais, que possam ser remetidos a instituições ou empresas com as mesmas características 	CNTS
Favorecimento de fornecedores na aquisição de equipamentos e serviços	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Definição das especificações do objeto e parte técnica de forma concreta, objetiva e pormenorizada 	CNTS e DAG
Favorecimento na disponibilização de serviços de telessaúde	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Definição de critérios para a disponibilização do serviço e atribuição de equipamentos 	CNTS
Falta de transparência no relacionamento com fornecedores	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Comunicação por e-mail com conhecimento de endereço de e-mail geral da direção / coordenação ou outro elemento da equipa Realização de reuniões com fornecedores apenas nas instalações da SPMS, salvo situações devidamente justificadas 	
Produção intencional de documentos com informação falsa ou inexata	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Envio de documentos finais em PDF, preferencialmente por via digital, com conhecimento do endereço de e-mail geral da direção / coordenação ou outro elemento da equipa. 	

Centro de Controlo e Monitorização do SNS

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Indisponibilidade dos sistemas	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Planeamento mensal de intervenções críticas para garantir a divulgação atempada das respetivas intervenções junto dos clientes Assessment e disponibilização de relatórios de disponibilidade por cada um dos sistemas críticos da sua responsabilidade. 	DCCM, DSI I, DSI II e DSI III
Fraca/moderada robustez das aplicações informáticas por incumprimento/relacionadas com as boas práticas de desenvolvimento de software	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração de Manual de Desenvolvimento de Software e do ciclo de vida dos sistemas de informação Adopção de Manual de Gestão de Projetos Compilação de boas práticas de realização de testes sobre os sistemas ou funcionalidades desenvolvidas 	DCCM, DSI II e DSI III
Tratamento preferencial no Suporte interno e externo (clientes, stakeholders e utilizadores)	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Monitorização dos tempos de resposta aos pedidos que dão entrada no Servicedesk relativamente a cada um dos sistemas da DCCM 	DCCM
Dificuldade em integrar os profissionais de saúde no modelo participativo no desenvolvimento dos projetos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Inclusão, no Manual de Gestão de Projeto, de modelo de indicação de profissionais para participação no desenvolvimento de projetos, com o respetivo registo da sua atividade. 	DCCM e DPDO
Equipa de operações com remunerações baixas e tarefas rotineiras, atreita à prática de erros, fruto da repetição de tarefas operacionais	BAIXA	MÉDIO	FRACO	<ul style="list-style-type: none"> Desenvolvimento de tarefas em regime de rotatividade entre equipas 	DCCM
Ausência de controlo de acesso físico e lógico à área de operações	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Implementação de controlo de acesso físico ao edifício da SPMS Maia na área de operações Implementação de controlo e registo de acesso lógico 	DCCM, DAG
Deficiente controlo do acesso na recepção de documentos e correspondência	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Implementação de barreiras físicas e de controlo de acesso físico, no que refere à recepção da documentação entregue pelo prestador 	DCCM
Incorreções na atividade de conferência (prescrição, dispensa e despesa do SNS com medicamentos, MCDTs e outras áreas de prescrição complementares)	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Realização de auditorias internas pela equipa DCCM, no procedimento de conferência 	DCCM
Erro humano na conferência	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Aumento da desmaterialização: elaboração conjunta entre Direções de proposta legislativa de alteração do regime jurídico que regula a prescrição de medicamentos, no sentido de controlar a prescrição manual Formação aos médicos inadaptados; Segregação de funções entre diferentes áreas na conferência 	DCCM, DAIC
Manutenção de todas as componentes do Centro e da Solução de Conferência: Perda de know how estratégico para o Ministério da Saúde	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Reforço e retenção dos recursos internos afetos à operação e consolidação dos procedimentos das diferentes áreas de atuação. 	
Falha nas aplicações de negócio e sistemas de informação, decorrente das alterações legais, da introdução de novos tipos de conferência ou da alteração das regras de conferência, se não existir constante manutenção evolutiva	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Revisão e atualização contínua dos manuais de relacionamento onde se encontram definidas as regras de conferência utilizadas no processo 	DCCM
Produção de informação de suporte à gestão do processo de conferência, para utilização pelo próprio centro, para a gestão das ARS, ACSS e de outras instituições do SNS: monitorização da atividade e cumprimento dos SLAs	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Manutenção de controlos para o cumprimento dos prazos definidos para a conferência 	
Vulnerabilidades nos sistemas fonte de informação derivadas da ausência de qualidade na informação	BAIXA	ALTO	MODERADO	<ul style="list-style-type: none"> Implementação de controlo de verificação nos sistemas fonte de suporte à operação do CCMSNS (por exemplo, no momento da emissão de recetivário) 	

Direção de Sistemas de Informação I

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Perda, modificação ou adulteração de informação por intrusão nos sistemas de informação	MÉDIA	ALTO	ELEVADO	• Política de acessos e operações em ambiente de produção restrita	DSI I/UPDCS
				• Atribuição de computadores fornecidos pela SPMS para todos os colaboradores internos e máquinas virtuais para prestadores de serviços externos;	DSI I
				• Política de Recursos Humanos para Entrada e Saída de colaboradores	DSI I/ DRH/ DAG/UPDCS
				• Implementação de processo de gestão de identidades com suporte numa ferramenta de Gestão de Identidades (IAM)	DSI I/ DSI III
Alteração nas condições ambientais das salas de Data Center	MÉDIA	ALTO	ELEVADO	• Definição de procedimento de acesso a posto de trabalho por via de "autenticação forte" (dois factores de identificação)	DSI I/UPDCS
				• Política de acesso a salas de sistemas e instalação de controladores eletrónicos (duplo factor)	DSI I/UPDCS
Indisponibilidade dos sistemas	MÉDIA	ALTO	ELEVADO	• Medidas de controlo e salvaguarda de tratamento de ar e energia	DSI I/ DAG
				• Alargamento do processo de monitorização da performance e níveis de serviço das aplicações	DSI I
				• Divulgação atempada junto dos clientes das intervenções críticas a executar	
Desadequada gestão do parque informático e software, quer em número (excedente ou insuficiente) quer em atualização.	MÉDIA	MÉDIO	MODERADO	• Revisão da Política de Continuidade de Negócio.	DSI, DRH, DF, DAG
				• Adaptação da metodologia de continuidade de negócio ao PRR	
Tratamento preferencial no Suporte interno e externo (clientes)	MÉDIA	MÉDIO	MODERADO	• Auditoria anual ao parque informático.	DSI I
				• Registo de todo o material consumível que é disponibilizado aos colaboradores (teclados, ratos, mochilas de portátil, bases para portátil, etc.), devendo haver articulação com a DRH para que aquando a saída do colaborador da instituição seja devolvido todo o material que lhe foi atribuído.	
Conceção de sistemas insuficientes ou desadequados que propiciem falhas no controlo da informação	MÉDIA	ALTO	ELEVADO	• Monitorização dos tempos de resposta aos pedidos que dão entrada no Servicedesk e disponibilização mensal na intranet.	DSI I
				• Garantia de formação dos colaboradores da área do atendimento e suporte.	
Perda de informação e registos por avaria irrecoverável dos computadores e/ou das aplicações	MÉDIA	MÉDIO	MODERADO	• Segregação física e lógica do acesso a informação	DSI I, UPDCS, DAIC
				• Criação de mecanismos de acesso restrito a processos confidenciais	
Falhas na atribuição de acessos à rede informática	BAIXA	BAIXO	FRACO	• Revisão da política de backups e de inventariação de activos críticos	DSI I
				• Revisão periódica da cadeia de responsabilização para atribuição de acessos	DSI I

Direção de Sistemas de Informação II

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Indisponibilidade dos sistemas	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Planeamento mensal de intervenções críticas para garantir a divulgação atempada das respetivas intervenções junto dos clientes Assessment e disponibilização de relatórios de disponibilidade por cada um dos sistemas críticos da sua responsabilidade. 	DSI II e DSI I
Fraca/moderada robustez das aplicações informáticas por incumprimento/relacionadas com as boas práticas de desenvolvimento de software	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração de Manual de Desenvolvimento de Software e do ciclo de vida dos sistemas de informação Adopção de Manual de Gestão de Projetos Compilação de boas práticas de realização de testes sobre os sistemas ou funcionalidades desenvolvidas 	DSI II e DSI III DSI II DSI II
Tratamento preferencial no Suporte interno e externo (clientes, stakeholders e utilizadores)	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Monitorização dos tempos de resposta aos pedidos que dão entrada no Servicedesk relativamente a cada um dos sistemas da DSI II 	DSI II e DSI I
Dificuldade em integrar os profissionais de saúde no modelo participativo no desenvolvimento dos projetos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Inclusão, no Manual de Gestão de Projeto, de modelo de indicação de profissionais para participação no desenvolvimento de projetos, com o respetivo registo da sua atividade. 	DSI II e DPDO

Direção de Sistemas de Informação III

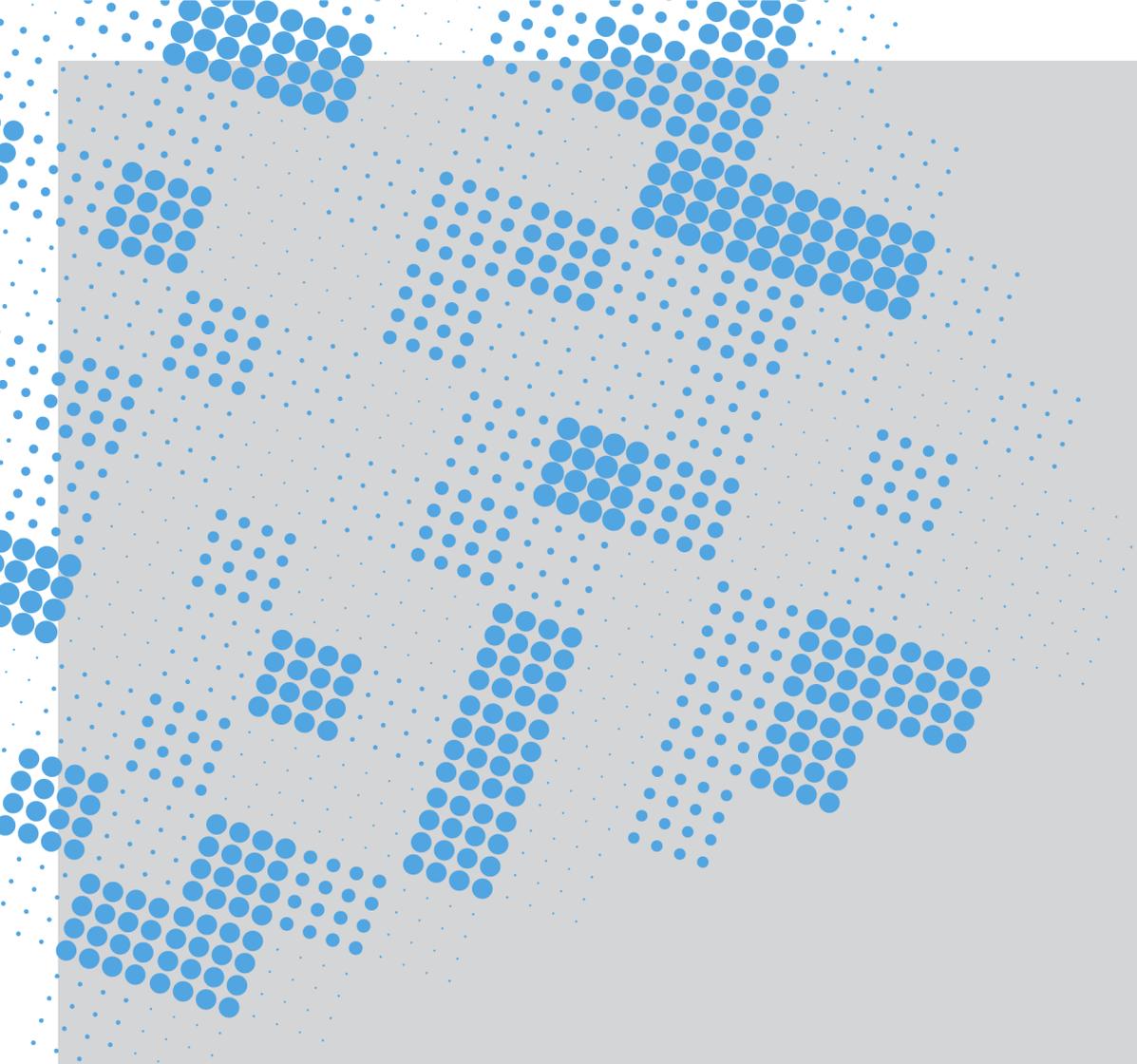
RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Perda, modificação ou adulteração de informação por intrusão nos sistemas de informação	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Implementação de processo de gestão de identidades com suporte numa ferramenta de Gestão de Identidades (IAM) 	DSI I/ DSI III
Indisponibilidade dos sistemas críticos	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Assessment e disponibilização de relatórios de disponibilidade por cada um dos sistemas críticos da sua responsabilidade Desenvolvimento de, pelo menos, um processo de alarmística por cada um dos sistemas críticos da sua responsabilidade 	DSI III
Mecanismos de interoperabilidade inadequados ou limitados entre os componentes dos Sistemas de Informação da Saúde	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Definição de políticas, normas, guidelines, em alinhamento com a estratégia TIC para a AP 	DSI III
Tratamento preferencial no Suporte interno e externo (clientes, utentes etc.)	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Monitorização dos tempos de resposta aos pedidos que dão entrada no Servicedesk relativamente a cada um dos sistemas da DSI III 	Todas as DSI
Ausência de condições para verificação de requisitos de conformidade dos sistemas	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Realização de levantamento do sistema de <i>compliance</i>, na componente de fornecedores de softwares privados Criação de automatismos para verificação de conformidade 	DSI III e AUDIT DSI III
Dificuldade na gestão de projetos no âmbito do PRR	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Coordenação técnica dos projetos que constam do PRR, nos termos definidos no Modelo de Governação 	
Fraca/moderada robustez das aplicações informáticas por incumprimento/relacionadas com as boas práticas de desenvolvimento de software	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Elaboração de Manual de Desenvolvimento de Software e do ciclo de vida dos sistemas de informação Adopção de Manual de Gestão de Projetos Inclusão, no Manual de Gestão de Projeto, de modelo de indicação de profissionais e entidades utilizadoras para participação no desenvolvimento de projetos, com o respetivo registo da sua atividade. 	DSI III

Central de Compras da Saúde

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Favorecimento ilícito de fornecedores	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Criação de equipas multidisciplinares para Procedimentos de TI com especial complexidade Segregação de funções entre quem executa os procedimentos aquisitivos e quem verifica os documentos de habilitação. Disponibilização de Acordos Quadro em categorias de utilização interna da SPMS. Assegurar que estão devidamente definidas as especificações do objeto e parte técnica de forma concreta, objetiva e pormenorizada Garantir a rotatividade dos elementos do júri, nos procedimentos de contratação, aumentando o número de vogais do júri da área que solicitou a aquisição Assegurar a assinatura de Declaração de Inexistência de Conflitos de Interesses por todos os elementos do júri e participantes no procedimento Recurso ao critério de avaliação da proposta economicamente mais vantajosa nas modalidades monofactor ou multifactor, adequando à necessidade da entidade adjudicante 	Central de Compras
Atraso na tramitação dos procedimentos inerentes à formação de contratos	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Promover a atualização dos colaboradores das Direções de Compras na área da Contratação Pública em relação a procedimentos de autorização de despesa Atualização do Manual de Boas Práticas de Contratação Pública da SPMS Automatização dos procedimentos associados à formação de contratos. Divulgação por todos os colaboradores das Direções de Compras (em funções e novos) dos documentos relativos à Uniformização de Procedimentos das Equipas relativos às Comunicações e Notificações a efetuar na Plataforma Eletrónica de Contratação. 	
Assegurar o princípio da transparência na elaboração de acordos quadro	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Efetuar consultas públicas e/ou anúncios de pré-informação no âmbito da formação de novos acordos quadro 	
Não cumprimento da Estratégia Nacional para as Compras Públicas Ecológicas	MÉDIA	BAIXO	MODERADO	<ul style="list-style-type: none"> Incluir critérios ecológicos nos procedimento de contratação pública para as categorias cujos manuais sejam disponibilizados pela ENCEPE 	
Não utilização dos Acordos Quadro	ALTA	BAIXO	MODERADO	<ul style="list-style-type: none"> Garantir a divulgação dos acordos quadro transversais no site da SPMS Disponibilizar um canal de comunicação próprio para esclarecimento de dúvidas sobre acordos quadro 	
Perda de informação por ausência de software de procurement na área transversal para a comunicação com as entidades do MS e SNS	MÉDIA	ELEVADO	ELEVADO	<ul style="list-style-type: none"> Desenvolvimento de uma área transversal no Catálogo eletrónico da SPMS 	
Não cumprimento do planeamento das aquisições centralizadas por falta de documentação/resposta das entidades do MS e SNS	BAIXA	ELEVADO	MODERADO	<ul style="list-style-type: none"> Divulgar o planeamento anual das aquisições centralizadas Informar os prazos limite para respostas, por forma a permitir a conclusão da tramitação processual no prazo estimado Oficializar a falta de resposta para o Conselho de Administração/ Diretivo, após 5 insistências sem resposta 	
Assegurar o princípio da transparência na elaboração de acordos quadro	BAIXA	BAIXO	FRACO	<ul style="list-style-type: none"> Efetuar consultas públicas e/ou anúncios de pré-informação no âmbito da formação de novos acordos quadro 	
	MÉDIA	ALTO	MODERADO	<ul style="list-style-type: none"> Verificar a legalidade dos procedimentos de formação de acordos quadro ou sistemas de aquisição dinâmicos 	

Unidade de Marketing, Serviços Partilhados e Gestão de Clientes

RISCO POTENCIAL	PROBABILIDADE	IMPACTO	GRADUAÇÃO DO RISCO	MEDIDA PREVENTIVA	RESPONSÁVEL PELA GESTÃO DO RISCO
Perda de receita potencial por falta de colaboração interna no processo de disponibilização de produtos e serviços da SPMS	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Report trimestral da atualização do portfolio de produtos e serviços e da execução dos contratos com clientes. 	Clientes
Tabela de preços desadequada face à nomenclatura e variabilidade dos produtos e serviços	MÉDIA	MÉDIO	MODERADO	<ul style="list-style-type: none"> Participação de todas as áreas envolvidas na disponibilização de produtos e prestação de serviços na elaboração de proposta de revisão da tabela de custos 	DPDO, DSI, Clientes, DF, CCMSNS
Falta de informação que prejudique a disseminação dos produtos e serviços da SPMS bem como o reconhecimento da sua qualidade	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Criação de equipa de gestão de clientes Realização de visitas e acompanhamento regular dos clientes 	Clientes
Favorecimento de clientes	MÉDIA	ALTO	ELEVADO	<ul style="list-style-type: none"> Propostas são elaboradas e revistas por vários níveis hierárquicos diferentes e direções e assinadas sempre pelos membros do CA 	



SPMS_{EPE}
Serviços Partilhados do Ministério da Saúde