Versão Retificada a 29-6-2017

CONCURSO PÚBLICO COM PUBLICAÇÃO NO JOUE PARA A CELEBRAÇÃO DE ACORDO QUADRO PARA A PRESTAÇÃO DE SERVIÇOS DE *CYBERSEGURANÇA* PARA A ÁREA DA SAÚDE

REF. UAQT2017002

CADERNO DE ENCARGOS

Índice

PARTE I - Do acordo quadro

Secção I

Disposições gerais

Cláusula 1.ª Definições

Para efeitos do presente Caderno de Encargos, apresentam-se ou adotam-se as seguintes definições:

a) Acordo Quadro – significa o contrato celebrado entre a SPMS, EPE e uma ou mais entidades, com vista a disciplinar relações contratuais futuras relativas à prestação de serviços de *Cybersegurança* na área da saúde, a estabelecer ao longo de um determinado período de tempo, mediante a fixação antecipada dos respetivos termos.

b) SPMS, EPE – Serviços Partilhados do Ministério da Saúde, Entidade Pública Empresarial, criada pelo Decreto-Lei n.º 19/2010, de 22 de março, alterado pelo Decreto-Lei n.º 108/2011, de 17 de novembro, pelo Decreto-Lei nº 209/2015, de 25 de setembro, e pelo Decreto-Lei nº 32/2016, de 28 de junho, com o objeto e atribuições conforme definidos nos seus Estatutos, publicados em anexo ao referido diploma;

c) Contratos – significam os contratos a celebrar entre as entidades adquirentes e os Prestadores de Serviços, nos termos do presente caderno de encargos;

d) Cocontratantes - Os adjudicatários do acordo quadro e dos contratos de prestação de serviços a celebrar ao seu abrigo.

e) Gestor do Contrato – Responsável em cada cocontratante pela gestão do acordo quadro e dos contratos celebrados ao abrigo do mesmo;

f) Gestor de categoria - Responsável pela gestão dos contratos celebrados ao abrigo do acordo quadro;

g) Entidade adquirente – Qualquer organismo do Ministério da Saúde ou entidade do Serviço Nacional de Saúde, bem como qualquer das entidades compradoras voluntárias que venha a celebrar contratos de adesão com a SPMS, EPE, cujo objeto compreenda os serviços incluídos no presente acordo quadro.

Cláusula 2.ª Tipo de procedimento, designação e objeto

1. O concurso é designado como "Concurso público com publicação no JOUE para a celebração de Acordo Quadro para a prestação de serviços de *Cybersegurança* na área da saúde".

2. O presente concurso tem por objeto a seleção de cocontratantes para a celebração de um Acordo Quadro para a prestação de serviços de *Cybersegurança* na área de saúde.
3. O acordo quadro resultante do presente procedimento disciplinará as relações contratuais futuras a estabelecer entre os cocontratantes e os Serviços Partilhados do Ministério da Saúde, E.P.E. (SPMS, EPE), entidades adquirentes vinculadas e/ou voluntárias, tal como definidas no Decreto-Lei n.º 19/2010, de 22 de março, alterado pelo Decreto-Lei n.º 108/2011, de 17 de novembro, pelo Decreto-Lei 209/2015, de 25 de setembro, e pelo Decreto-Lei nº 32/2016, de 28 de junho.

Cláusula 3.ª Caraterização dos lotes do Acordo Quadro

1. O acordo-quadro em apreço encontra-se dividido em 25 (vinte e cinco) lotes de serviço *Cybersegurança*, constituídos da seguinte forma:
   a) Categoria I - Governo da segurança e gestão do risco
      I. Lote 1 – Estratégia e plano de ação de segurança
      II. Lote 2 – Análise de risco
      III. Lote 3 – Políticas e normas de segurança
      IV. Lote 4 – Avaliação de desempenho
      V. Lote 5 – Gestão da Continuidade
      VI. Lote 6 – Conformidade
   b) Categoria II – , Gestão de ameaças de segurança
      I. Lote 7 – Definição do plano de implementação de um centro de operação de segurança (SOC)
      II. Lote 8 – Implementação de um centro de operação de segurança (SOC)
      III. Lote 9 – Definição do modelo de monitorização de um centro de operação de segurança (SOC)
      IV. Lote 10 – Operação de um centro de operação de segurança (SOC)
      V. Lote 11 – Identificação e avaliação de ameaças de segurança
      VI. Lote 12 – Definição da gestão\ de respostas a incidentes
      VII. Lote 13 – Serviço de respostas a incidentes
   c) Categoria III – Engenharia de segurança
      I. Lote 14 – Segurança física
      II. Lote 15 – Desenho de arquiteturas de redes e comunicações seguras

III. Lote 16 – Implementação e administração de arquiteturas de redes e comunicações seguras

IV. Lote 17 – Segurança no ciclo de desenvolvimento de *software*

d) Categoria IV – Gestão de identidades e acessos

I. Lote 18 – Elaboração de políticas de acesso

II. Lote 19 – Gestão de entidades e controlo de acesso lógico

III. Lote 20 – Implementação do processo de gestão de identidades e acessos

IV. Lote 21 – Infraestruturas de chaves públicas

V. Lote 22 – Implementação de infraestruturas de chaves públicas

e) Categoria V – Proteção de dados pessoais e privacidade

I. Lote 23 – Estratégia e governo para proteção de dados pessoais

II. Lote 24 – Classificação e gestão da informação

III. Lote 25 – Proteção contra perda de informação

Cláusula 4.ª Descrição dos serviços

1. Os serviços contratualizados ao abrigo do acordo quadro objeto do presente procedimento, devem estar em estreito alinhamento estratégico com as orientações emanadas pelo Ministério da Saúde ou por qualquer outro normativo legal aplicável (nomeadamente referem-se os despachos n.ºs 1348/2017, de 8 de fevereiro e 3156/2017, de 13 de abril, ambos do Ministério da Saúde, bem como a Resolução de Conselho de Ministros nº 62/2016, de 17 de outubro).
2. Acresce ao referido no número anterior do presente artigo que os serviços contratualizados ao abrigo do acordo quadro objeto do presente procedimento, devem ainda estar alinhados com as **Boas Práticas de Gestão, Controlo e Operação do Risco e Segurança da Informação na SPMS**, designadamente:

   A framework de referência para o Risco e Segurança alinhada com a *framework* de governança, gestão e operação do sistema de informação do eSIS.

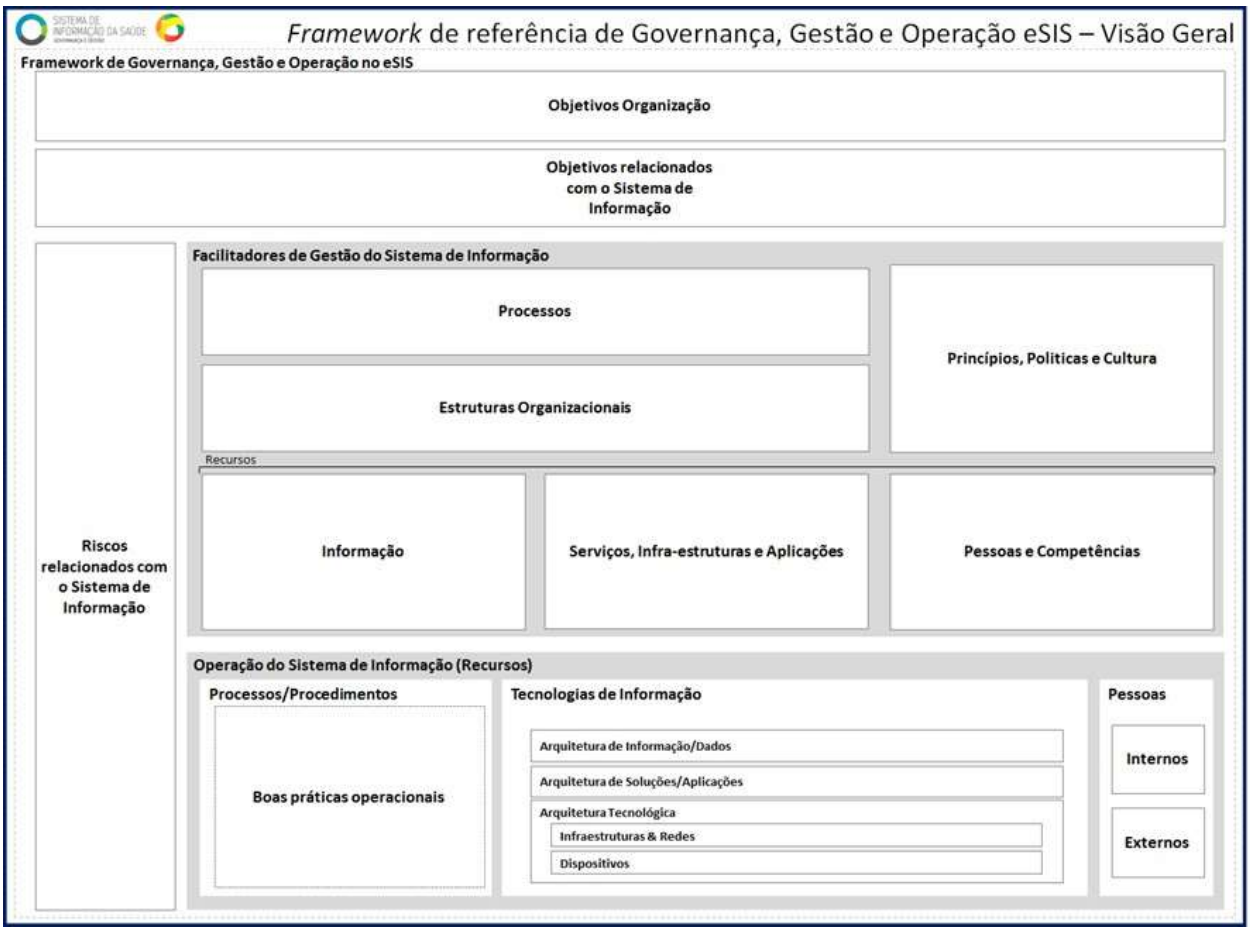

Figura 1 - Framework de governança, gestão e operação do sistema de informação do eSIS

As diferentes componentes da *framework* de referência do Risco e Segurança no eSIS representam os elementos fundamentais para os quais foram identificados o estado atual (*as-is*) e o estado futuro (*to-be*), permitindo desta forma conhecer o *gap* e desenvolver os planos de ação que no próximo ciclo estratégico deverão ser implementados. Destacam-se as seguintes principais dimensões:

- Objetivos do Sistema de Informação da Organização relacionados com o Risco e Segurança;
- Riscos do Sistema de Informação relacionados com o Risco e Segurança;
- Facilitadores de Gestão do Risco e Segurança do Sistema de Informação;
- Operação do Risco e Segurança do Sistema de Informação.

A *framework* pretende funcionar como um guia para a governança, gestão e operação do Risco e Segurança no eSIS, permitindo às diferentes entidades uma melhor coordenação e partilha de boas práticas.

3. Relativamente às componentes do presente procedimento, são elas:

Categoria I – Governo da segurança e gestão do risco (lotes 1 a 6)

Estratégia e plano de ação de segurança	Análise de risco	Políticas e normas de segurança	Avaliação de desempenho	Gestão da continuidade	Conformidade

Características do serviço	
Descrição	• Pretende-se a definição da estratégia de segurança e respetivo plano de ação. • Esta definição deve contemplar as soluções, os seus componentes e os respetivos processos e procedimentos que suportam a sua orientação. Desta forma é preponderante garantir que, as necessidades do negócio do ponto de vista da segurança da informação são suprimidas. • É necessário garantir pelo menos um modelo de governo, a normalização e recolha de métricas. • O plano de ação de segurança deve contemplar todas as vertentes da estratégia de segurança previamente definida. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação), nomeadamente os objetivos relacionados com o sistema de informação onde se enquadram os relacionados com a segurança da informação. • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas ou outros métodos de recolha de informação que o concorrente defina na metodologia apresentada.
Resultado pretendido com este serviço	• Desenho, implementação ou apoio à operacionalização da estratégia de segurança • Plano de ação da estratégia de segurança
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *Certified in the Governance of Enterprise IT (CGEIT)* • *Cobit 5 foundation*

Estratégia e plano de ação de segurança	Análise de risco	Políticas e normas de segurança	Avaliação de desempenho	Gestão da Continuidade	Conformidade

Características do serviço	
Descrição	• Pretende-se com a análise de risco a representação de um processo de identificação de vulnerabilidades e ameaças, assim como o impacto e probabilidade de ocorrência das mesmas, tendo em conta o contexto organizacional. • Para esta análise de risco pretende-se incluir uma ou mais das seguintes categorias: Danos físicos, interação humana, falhas de equipamentos ou sistemas, má utilização da informação e/ou dados, fuga de informação e erros aplicacionais.

	• O relatório final deve apresentar a análise de risco, os critérios e falhas identificadas, assim como recomendações para o respetivo tratamento. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação), nomeadamente em relação ao catálogo de riscos de gestão e operação. • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas, outros métodos de recolha de informação e ferramentas tecnológicas de suporte que o concorrente defina na metodologia apresentada.
Resultado pretendido com este serviço	• Acompanhamento da operação dos modelos de gestão de riscos implementados • Relatório com os riscos identificados, possíveis impactos, probabilidades de ocorrência e recomendações para tratamento dos mesmos
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *Certified in Risk and Information Systems Control (CRISC)*

Estratégia e plano de ação de segurança | Análise de risco | **Políticas e normas de segurança** | Avaliação de desempenho | Gestão da Continuidade | Conformidade

Características do serviço	

Descrição	• Pretende-se a definição de políticas e normas de segurança.
	• Os resultados da definição das políticas e normas de segurança devem estar de acordo com as necessidades organizacionais, requisitos e objetivos de negócio, bem como as leis e regulamentos em vigor, nomeadamente:
	  ◦ Com os *standards* do mercado na área da segurança da informação como os da série ISO/IEC 27000
	  ◦ Com o regulamento (UE) 2016/679 do parlamento europeu e do conselho, de 27 de abril de 2016
	• As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação), nomeadamente em relação ao catálogo de riscos de gestão e operação.
	• As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.

Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas ou outros métodos de recolha de informação que o concorrente defina na metodologia apresentada.
Resultado pretendido com este serviço	• Desenho, implementação ou apoio à operação da *framework* de políticas de segurança da informação • Desenho, implementação ou apoio à operação das políticas, normas e procedimentos de segurança
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *ISO 27001 Lead Implementer* • *ISO 27001 Lead Auditor*

Estratégia e plano de ação de segurança	Análise de risco	Políticas e normas de segurança	Avaliação de desempenho	Gestão da Continuidade	Conformidade

Características do serviço	
Descrição	• Pretende-se a análise e definição de medidas de avaliação de desempenho e a execução da avaliação de desempenho com base nas métricas definidas e *benchmark* de gestão, bem como nos controlos de segurança em uso pela organização. • É necessário que seja apresentado, de forma concreta, o grau de maturidade de segurança presente na organização, com base na avaliação previamente efetuada, assim como recomendações para a melhoria do mesmo.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas ou outros métodos de recolha de informação que o concorrente defina na metodologia apresentada.
Resultado pretendido com este serviço	• Relatório de análise da maturidade dos sistemas de segurança da informação e da organização • Definição de métricas de desempenho • Desenho, implementação ou apoio à operação dos processos e metodologias de avaliação de desempenho • Desenho, implementação ou apoio à avaliação de desempenho dos controlos de segurança
Certificações aplicáveis	• *Certified Information Systems Auditor (CISA)* • *ISO 27001 Lead Auditor*

Estratégia e plano de ação de segurança	Análise de risco	Políticas e normas de segurança	Avaliação de desempenho	Gestão da Continuidade	Conformidade

Características do serviço	
Descrição	• Pretende-se o desenho, implementação ou apoio à operação da estratégia de continuidade de negócio da organização tendo em consideração uma abordagem por cenários de risco. • Pretende-se o desenho, implementação ou apoio à operacionalização dos processos de gestão da continuidade que contemplem as medidas necessárias para garantir que os recursos, as pessoas e os processos de negócio podem retomar a normal atividade em tempo útil, de forma a minimizar os efeitos da disrupção. • Os processos de gestão da continuidade deverão especificar os procedimentos a seguir, antes, durante e depois de um desastre, seja ele natural, técnico ou de origem humana. Este plano de recuperação deverá contemplar, mas não se limitar aos sistemas informáticos. • Pretende-se também a definição de processos de continuidade de negócio, elencando procedimentos necessários para que o negócio continue de forma sustentável enquanto sujeito a disrupções superiores aos critérios definidos. Os processos de continuidade de negócio deverão garantir os requisitos de disponibilidade, integridade e confidencialidade dos componentes e da informação relevante, durante e depois o processo de recuperação. As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação

	da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas, outros métodos de recolha de informação, ferramentas tecnológicas e simulacros.
Resultado pretendido com este serviço	• Plano de recuperação de negócio • Plano de continuidade de negócio • Cenários de risco de continuidade • Desenho, implementação ou apoio à operação dos processos, procedimentos e planos de suporte à continuidade nas dimensões de pessoas, processos e tecnologias
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *ISO 22301 Lead Implementer/Auditor*

Estratégia e plano de ação de segurança	Análise de risco	Políticas e normas de segurança	Avaliação de desempenho	Gestão da continuidade	Conformidade

Características do serviço	
Descrição	• Pretende-se a verificação da conformidade de todos os controlos de segurança relativos a leis, regulamentos e normas em vigor, implementadas ou em processo de implementação na organização. Tal não se limita ao entendimento das leis e regulamentos existentes e/ou relevantes na prática da segurança da informação mas também a outras normas aplicáveis à organização na execução do negocio. • Pretende-se que exista um alinhamento com o regulamento (UE) 2016/679 do parlamento europeu e do conselho, de 27 de abril de 2016. • Os controlos verificados, assim como todas as não-conformidades deverão ser apresentados de forma assertiva e detalhada nos relatórios a entregar. • Caso sejam detetadas não-conformidades, é necessário elencar o plano de ação para a correção das mesmas. • As atividades deverão ser alinhadas com a framework de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas, outros métodos de recolha de informação e ferramentas tecnológicas de suporte.
Resultado pretendido com este serviço	• Relatório de análise da conformidade • Plano de ação • Desenho, implementação ou apoio à operação dos processos de conformidade
Certificações aplicáveis	• *Certified Information Systems Auditor (CISA)* • *Certified Information Security Manager (CISM)*

4. Categoria II – Gestão de ameaças de segurança (lotes 7 a 13)

Definição do plano de implementação de um centro de operação de segurança (SOC)	Implementação de um centro de operação de segurança (SOC)	Definição do modelo de monitorização de um centro de operação de segurança (SOC)	Operação de um centro de operação de segurança (SOC)	Identificação e avaliação de ameaças de segurança	Definição da gestão de respostas a incidentes	Serviço de respostas a incidentes

Características do serviço	
Descrição	• Pretende-se a definição do plano de implementação do centro de operação de segurança em todas as suas vertentes, onde o mesmo deverá cumprir na totalidade os requisitos de deteção e reação a incidentes de segurança. Os requisitos incluem, mas não se limitam, à correlação dos dados gerados, à integridade dos mesmos, à disponibilidade 24 horas por dia, 7 dias por semana da plataforma e à confidencialidade da informação e dos seus canais de transmissão. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Plano de implementação onde deverá estar contemplada a arquitetura física, lógica e respetiva tecnologia utilizada
Certificações aplicáveis	• Certificação relevante do fabricante da tecnologia SIEM • *Certified Information Systems Security Professional* (CISSP) • *Systems Security Certified Practitioner* (SSCP)

Definição do plano de implementação de um centro de operação de segurança (SOC)	**Implementação de um centro de operação de segurança (SOC)**	Definição do modelo de monitorização de um centro de operação de segurança (SOC)	Operação de um centro de operação de segurança (SOC)	Identificação e avaliação de ameaças de segurança	Definição da gestão de respostas a incidentes	Serviço de respostas a incidentes

Características do serviço	
Descrição	• Pretende-se a implementação do centro de operação de segurança com base num plano de definição de um centro de operação de segurança (SOC), caso este já exista. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a algumas soluções

	tecnológicas.
Resultado pretendido com este serviço	• A infraestrutura física do centro de operação de segurança
Certificações aplicáveis	• Certificação relevante do fabricante da tecnologia SIEM • *Certified Information Systems Security Professional* (CISSP) • *Systems Security Certified Practitioner* (SSCP)

Definição do plano de implementação de um centro de operação de segurança (SOC) | Implementação de um centro de operação de segurança (SOC) | **Definição do modelo de monitorização de um centro de operação de segurança (SOC)** | Operação de um centro de operação de segurança (SOC) | Identificação e avaliação de ameaças de segurança | Definição da gestão de respostas a incidentes | Serviço de respostas a incidentes

Características do serviço	
Descrição	• Pretende-se que sejam definidas métricas e/ou procedimentos para a monitorização de todos os aspetos relativos a segurança da organização, que deverá incluir, mas não se limitar, à vertente técnica e operacional. Deverão ser identificados todos sistemas e processos cuja monitorização poderá gerar alarmística relevante para a identificação, e subsequentemente correção de incidentes de segurança. • A monitorização dos aspetos de segurança da organização deverá ser feita de forma continua, o que inclui a implementação de processos cujo objetivo deverá ser a criação e apresentação do estado da segurança, num determinado instante. • O concorrente deverá definir de forma concreta, nos relatórios finais, quais os ativos mais relevantes para uma monitorização eficaz da infraestrutura organizacional, assim como todos os tipos de alarmística que tal gere. Deverão, também, ser identificados e definidos os casos de uso que poderão vir a ser relevantes para a implementação do centro de operação de segurança. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a soluções tecnológicas.
Resultado pretendido com este serviço	• Procedimento de monitorização de acordo com a política de resposta a incidentes • Definição dos níveis de serviço • Definição de casos de uso
Certificações aplicáveis	• *GIAC Continuous Monitoring Certification* (GMON)

Definição do plano de implementação de um centro de operação de segurança (SOC)	Implementação de um centro de operação de segurança (SOC)	Definição do modelo de monitorização de um centro de operação de segurança (SOC)	Operação de um centro de operação de segurança (SOC)	Identificação e avaliação de ameaças de segurança	Definição da gestão de respostas a incidentes	Serviço de respostas a incidentes

Características do serviço	
Descrição	• Pretende-se a prestação de serviços por parte do concorrente por forma a garantir os serviços necessários para o correto funcionamento do centro de operação de segurança (SOC), que poderá incluir, mas não se limitar, ao serviço de manutenção e monitorização. Este serviço poderá, consoante as necessidades da organização, requisitar a operação e disponibilidade 24 horas por dias, 7 dias por semana da equipa responsável. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Equipa capaz de prestar os serviços necessários para a gestão e monitorização do centro de operações de segurança (SOC)
Certificações obrigatórias	• Certificação relevante do fabricante da tecnologia SIEM

Definição do plano de implementação de um centro de operação de segurança (SOC)	Implementação de um centro de operação de segurança (SOC)	Definição do modelo de monitorização de um centro de operação de segurança (SOC)	Operação de um centro de operação de segurança (SOC)	Identificação e avaliação de ameaças de segurança	Definição da gestão de respostas a incidentes	Serviço de respostas a incidentes

Características do serviço	
Descrição	• Pretende-se a execução de serviços relativos a identificação e/ou a análise de ameaças de segurança. Este processo incluí serviços de testes de vulnerabilidades e intrusão com base em metodologias disponíveis no mercado ou metodologias próprias do concorrente. • Os relatórios finais deverão incluir, por além dos detalhes técnicos das ameaças identificadas, informação e recomendações para remediar e/ou minimizar o impacto das mesmas. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas

	consideramos que este serviço pode ser realizado recorrendo a soluções tecnológicas.
Resultado pretendido com este serviço	• Relatório dos resultados da auditoria/testes de segurança • Plano de ação para mitigar as possíveis ameaças identificadas
Certificações obrigatórias	Uma destas certificações é obrigatória: • *Certified Ethical Hacker* (CHE) • *Offensive Security Certified Professional* (OSCP)

Características do serviço	
Descrição	• Pretende-se a definição de uma metodologia detalhada de gestão e resposta a incidentes de *cybersegurança* que deverá incluir, mas não se limitar, à elaboração da norma de resposta a incidentes, definição de equipa de peritos para investigação de incidentes de segurança e respetivos acessos, fontes de informação relativa a ameaças e definição de metodologia e ferramentas de investigação. Tal deverá ser suportado por um processo de identificação, resposta, recuperação e revisão dos incidentes de segurança. • A metodologia deve ainda considerar os níveis de criticidade dos incidentes, lista de responsáveis e respetivos níveis de *Escalation and Reporting*. • Para a definição da metodologia de resposta a incidentes devem ser considerados os processos de monitorização de segurança, assim como a tecnologia e o plano de implementação do centro de operação de segurança (SOC), caso exista. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Norma e procedimento de resposta a incidentes, níveis de criticidade, responsáveis e respetivas funções • Definição dos níveis de serviço • Definição de casos de uso
Certificações aplicáveis	• *EC-Council Certified Incident Handler (ECIH)* • *GIAC Certified Incident Handler (GCIH)*

Definição do plano de implementação de um centro de operação de segurança (SOC)	Implementação de um centro de operação de segurança (SOC)	Definição do modelo de monitorização de um centro de operação de segurança (SOC)	Operação de um centro de operação de segurança (SOC)	Identificação e avaliação de ameaças de segurança	Definição da gestão de respostas a incidentes	Serviço de respostas a incidentes

Características do serviço	
Descrição	• No âmbito do modelo de resposta a incidentes de *cybersegurança*, é necessário operacionalizar a metodologia definida para o efeito. • Desta forma, pretende-se a apresentação de um plano de serviços para implementação e operação do modelo de resposta a incidentes, no qual deverá estar claro os elementos que compõe a equipa de resposta a incidentes e as respetivas funções, respeitando as pré-definidas na norma de resposta a incidentes. Adicionalmente, pretende-se um exemplo do modelo de relatório de serviço e os SLA's, caso estes sejam diferentes dos estabelecidos pela norma. • O concorrente poderá ainda apresentar sugestões de melhoria ao modelo atualmente definido assim como novas ferramentas para a operacionalização do mesmo. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar estão definidas na norma de resposta a incidentes, caso exista, no entanto consideramos que este serviço pode ser realizado recorrendo a outras ferramentas apresentadas pelo proponente.
Resultado pretendido com este serviço	• Relatórios de serviço • Níveis de serviço a prestar • Lista de elementos da equipa e respetivas funções
Certificações aplicáveis	• *EC-Council Certified Incident Handler (ECIH)* • *GIAC Certified Incident Handler (GCIH)*

Categoria III – Engenharia de segurança (lotes 14 a 17)

Segurança física	Desenho de arquiteturas de redes e comunicações seguras	Implementação e administração de arquiteturas de redes e comunicações seguras	Segurança no ciclo de desenvolvimento de *software*

Características do serviço	
Descrição	• A segurança física representa um conjunto de ameaças, vulnerabilidades e riscos diferentes de outros tipos de segurança, quer seja dos equipamentos ou da informação. Este tipo de ameaça de segurança contempla temas como a destruição física, intrusão de indivíduos na infraestrutura, problemas ambientais, roubo ou vandalismo. • Pretende-se desta forma a elaboração de uma norma de segurança física, na qual deverão estar definidos as zonas e respetivos níveis de criticidade, assim como os controlos de

	acesso a implementar para cada uma e as funções dos responsáveis autorizados. • A norma deve contemplar a definição do plano de ação em caso de emergências, formação, deteção de intrusões, proteção contra incêndios e falhas energéticas, plano de simulacros e respetivo planeamento. • O concorrente deverá ainda apresentar uma proposta do plano de implementação dos controlos definidos na norma e um conjunto de casos de uso representativos. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Norma de segurança física • Plano de implementação dos controlos aplicáveis • Definição de casos de uso
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Information Systems Security Engineering Profession (ISSEP)* • *Systems Security Certified Practitioner (SSCP)*

Características do serviço	
Descrição	• Redes de computadores e comunicação usam diversos mecanismos, dispositivos, *software* e protocolos que estão interrelacionados e integrados. • A segurança de redes é um pilar fundamental para segurança da informação, dado o conjunto de diferentes tecnologias tradicionalmente presentes numa arquitetura e, a sua constante evolução em termos de funcionalidades e requisitos. • Pretende-se a elaboração de um estudo e respetivo desenho de uma arquitetura de redes e comunicações seguras. O desenho deve ser preponderante quer para construção de novas soluções, assim como para a reestruturação de soluções existentes. • Deve contemplar um modelo físico e lógico da arquitetura futura, normas reguladoras, definição de casos de uso, *software* e *hardware* de suporte, as políticas e normas de segurança em vigor, estabelecendo como a solução deverá cumprir os objetivos desenhados, nomeadamente, requisitos de funcionalidade, compatibilidade, extensibilidade, segurança, usabilidade e manutenção. Este desenho deve ter em consideração as necessidades para as quais a arquitetura se aplica, garantindo robustez, resiliência a falhas, escalabilidade e a evolução a longo prazo. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Desenho de arquitetura, fluxos de comunicação, diagramas físicos e lógicos, casos de uso, identificação do *hardware* e *software* de suporte • Planos de implementação da arquitetura/solução

Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Information Systems Security Engineering Profession (ISSEP)*

Segurança física	Desenho de arquiteturas de redes e comunicações seguras	Implementação e administração de arquiteturas de redes comunicações seguras	Segurança no ciclo de desenvolvimento de *software*

Características do serviço	
Descrição	• Redes de computadores e comunicação usam diversos mecanismos, dispositivos, softwares e protocolos que estão interrelacionados e integrados. • A segurança de redes é um pilar fundamental para segurança da informação, dado o conjunto de diferentes tecnologias, tradicionalmente presentes numa arquitetura, e a sua, constante, evolução em termos de funcionalidades e requisitos. • A implementação de uma arquitetura de redes e comunicações seguras depreende a configuração e instalação dos componentes de rede e segurança constituintes da arquitetura, configuração dos casos de uso previamente definidos e criação de novos. • O processo de administração de redes de segurança deve contemplar manutenção de *hardware* e *software* especializados, análise e identificação de novas necessidades, suporte a inclusão de novos e mais robustos sistemas. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Relatórios de serviço • Sugestões de evolução e melhoria
Certificações aplicáveis	• *Systems Security Certified Practitioner (SSCP)* • *Certified Information Systems Security Professional (CISSP)* • *Information Systems Security Engineering Profession (ISSEP)*
Certificações obrigatórias	• Certificação relevante de um fabricante de tecnologia de redes (*networking*)

Segurança física	Desenho de arquiteturas de redes e comunicações seguras	Implementação e administração de arquiteturas de redes comunicações seguras	Segurança no ciclo de desenvolvimento de *software*

Características do serviço	
Descrição	• O desenvolvimento de *software* é um dos aspetos mais negligenciados no que respeita às preocupações de segurança, e como tal é um vetor de ataque muito apetecível. Por forma a reduzir eventuais impactos provenientes das aplicações é extremamente importante garantir o desenvolvimento de código seguro, as comunicações e as interações entre todos os componentes aplicacionais. • Nos ciclos de desenvolvimento de software, o concorrente deverá ter a capacidade de integrar o processo de planeamento e gestão de projeto a componente de segurança desde

	o ciclo inicial até ao momento do "*go live*", garantindo que todos os requisitos de segurança estão em conformidade com as políticas da corporação, normas de segurança da informação existentes e em última análise pelas boas práticas do mercado. • Deve, também, garantir o envolvimento e respetivo nível de segurança da aplicação, no caso de necessidade de alterações nos planos inicialmente definidos. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• *Framework* de acompanhamento de projetos na componente de segurança • Relatório das necessidades/esclarecimentos dos requisitos de segurança em cada fase do desenvolvimento da aplicação
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)*

Categoria IV – Gestão de identidades e acessos (lotes 18 a 22)

Elaboração de políticas de acesso	Gestão de entidades e controlo de acesso lógico	Implementação do processo de gestão de identidades e acessos	Infraestruturas de chaves públicas	Implementação de infraestruturas de chaves públicas

Características do serviço	
Descrição	• Os acessos são um dos aspetos mais explorados da segurança uma vez que representam uma porta direta para conteúdos críticos. • Os controlos de acesso são mecanismos de segurança que controlam e registam como os utilizadores e sistemas comunicam e interagem com outros sistemas ou recursos. Estes controlos necessitam de ser aplicados através de um método de defesa por camadas em profundidade. • É extremamente importante que exista um conhecimento alargado sobre os mecanismos de exploração dos controlos de forma a garantir a definição de uma norma de acesso que garanta os requisitos de segurança definidos pela entidade. • Pretende-se a definição de uma norma que deve contemplar os controlos a implementar para cada uma das funções dos responsáveis autorizados de acordo com níveis de criticidade dos ativos e respetivos níveis de privilégios por função. • A norma deve ainda definir uma cadeia de aprovação por tipo de acesso ou ativo a aceder, planos de ação em caso de emergências, formação, deteção de intrusões, proteção contra incêndios e falhas energéticas, plano de simulacros e respetivo planeamento. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.

Resultado pretendido com este serviço	• Desenho, implementação ou apoio à operação das políticas, normas e procedimentos de segurança relacionados com o controlo de acessos
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *Certified Identity and Access Manager (CIAM)*

Elaboração de políticas de acesso	Gestão de entidades e controlo de acesso lógico	Implementação do processo de gestão de identidades e acessos	Infraestruturas de chaves públicas	Implementação de infraestruturas de chaves públicas

Características do serviço	
Descrição	• Pretende-se a definição do processo de gestão identidades, pessoas e ativos, garantindo os requisitos de identificação, autenticação, autorização e responsabilização. • Para identificação, deve garantir que um sujeito (utilizador, processo ou programa) é a entidade que diz ser. Esta identificação deve ser realizada a partir do fornecimento de um elemento unívoco (nome de utilizador ou ID). • De forma a ser autenticado, o sujeito deve providenciar uma segunda parte de credenciais, quer seja uma palavra-passe, chave criptográfica, PIN ou um *token*. Estas duas partes devem ser validadas em conjunto. Assim que o sujeito se identifica deste modo, o concorrente deve garantir que os acessos do mesmo são os estritamente permitidos, garantindo autorização na base do princípio de privilégio mínimo. • Os controlos de acesso lógicos deverão impor mecanismos de controlo de acesso sobre os sistemas, processos e a informação relevante. Tais poderão ser embebidos ou não em sistemas operativos, aplicações, bases de dados ou outros sistemas relevantes. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Processo de gestão de identidades, controlos de acesso e procedimentos de autenticação
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *Certified Identity and Access Manager (CIAM)*

Elaboração de políticas de acesso	Gestão de entidades e controlo de acesso lógico	Implementação do processo de gestão de identidades e acessos	Infraestruturas de chaves públicas	Implementação de infraestruturas de chaves públicas

Características do serviço	
Descrição	• Pretende-se que o concorrente implemente o processo de gestão de identidades e acessos de acordo com o processo já definido. • O concorrente deverá recorrer a ferramentas de *software* ou *hardware* para a implementação do mesmo, apresentando assim a sua proposta de tecnologia a utilizar e os respetivos controlos que a mesma garante. • Este ponto contempla ainda a configuração de toda a solução e implementação dos casos de uso definidos, assim como todas configurações ou alterações necessárias para a interoperabilidade com outros sistemas já existentes como sistemas operativos, aplicações, bases de dados ou outros sistemas relevantes. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço deve ser realizado recorrendo a software e hardware especializado.
Resultado pretendido com este serviço	• Implementação da solução de gestão de identidades
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *Certified Identity and Access Manager (CIAM)*

Elaboração de políticas de acesso	Gestão de entidades e controlo de acesso lógico	Implementação do processo de gestão de identidades e acessos	Infraestruturas de chaves públicas	Implementação de infraestruturas de chaves públicas

Características do serviço	
Descrição	• Pretende-se a definição, de acordo com a legislação europeia e nacional em vigor, dos serviços e processos, bem como o plano de implementação de uma infraestrutura de chaves públicas para a gestão do ciclo de vida de certificados digitais, nomeadamente, para o registo, emissão e revogação dos diversos certificados e chaves. • Toda a definição deverá obedecer aos requisitos descritos no regulamento Nº 910/2014 do Parlamento Europeu e do Conselho.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.

Resultado pretendido com este serviço	• Plano de implementação, contemplando a arquitetura física e lógica dos serviços e processos.
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *ANS: Security Auditor, PKI Auditor*

Elaboração de políticas de acesso	Gestão de entidades e controlo de acesso lógico	Implementação do processo de gestão de identidades e acessos	Infraestruturas de chaves públicas	Implementação de infraestruturas de chaves públicas

Características do serviço	
Descrição	• O concorrente deverá implementar uma infraestrutura de chaves públicas de acordo com a legislação europeia e nacional em vigor. A implementação da infraestrutura de chaves pública, deve respeitar o plano já definido e aplica-lo de acordo com a tecnologia escolhida pelo proponente. • A infraestrutura deverá ser sujeite a auditorias efetuadas por empresas credenciadas pela Autoridade Credenciadora, para a verificação da conformidade com o regulamento Nº 910/2014 do Parlamento Europeu e do Conselho.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a soluções tecnológicas.
Resultado pretendido com este serviço	• Implementação da infraestrutura de chaves públicas
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *Certified Identity and Access Manager (CIAM)* • *ANS: Security Auditor, PKI Auditor*

Categoria V – Proteção de dados pessoais e privacidade (lotes 23 a 25)

Estratégia e governo para proteção de dados pessoais	Classificação e gestão da informação	Proteção contra perda de informação

Características do serviço	
Descrição	• Pretende-se a definição da estratégia e normas relativas à proteção dos dados pessoais conforme o quadro legislativo atualmente em vigor. • Salienta-se a necessidade de conformidade com a Lei n.º 67/98 da Proteção de Dados Pessoais que transpõe para a ordem jurídica portuguesa a diretiva 95/46/EC do Parlamento europeu e o subsequente regulamento GDPR (*General Data Protection Regulation*) 2016/679 em vigor a partir de Maio/2018. • A estratégia e normas devem ser aplicáveis de forma transversal a toda a organização.

	• As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo proponente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Relatório detalhado da estratégia relativa a proteção de dados pessoais • Desenho, implementação ou apoio à operação dos processos de gestão da privacidade a serem aplicados na organização • Normas de privacidade a serem aplicadas na organização
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)* • *ISO 27001 (Information Security): Lead Auditor, Implementer* • *Data Privacy Officer Certified*

Estratégia e governo para proteção de dados pessoais | Classificação e gestão da informação | Proteção contra perda de informação

Características do serviço	
Descrição	• A classificação da informação é o passo inicial para garantir um controlo efetivo sobre o ativo mais importante das organizações, a sua informação. A classificação da informação suporta a implementação dos controlos adequados à proteção informação. • Pretende-se a definição da estratégia e das metodologias para a classificação da informação interna com base na análise da criticidade da mesma, com o objetivo de garantir que a informação é tratada de acordo com o risco que ela representa dentro da organização. • Deverão ser detalhados e classificados todos os tipos de informação identificada na análise, por forma a determinar os métodos e os recursos que poderão aceder e/ou manipular tal informação, assim como os requisitos de cifra, armazenamento e meios de transmissão. Deverá ser tida em conta o estado da informação a cada momento, “Em Uso”, “ Em Repouso” e “Em Trânsito”. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo proponente, mas consideramos que este serviço pode ser realizado recorrendo a entrevistas.
Resultado pretendido com este serviço	• Apoio à implementação da política de classificação da informação tendo em conta a sua criticidade e os requisitos de cifra, armazenamento e meios de transmissão.
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP);* • *Certified Information Security Manager (CISM)* • *Data Privacy Officer Certified*

Estratégia e governo para proteção de dados pessoais | Classificação e gestão da informação | Proteção contra perda de informação

Características do serviço	
Descrição	• Pretende-se a implementação de mecanismos de proteção contra perda de informação, por forma a efetivar os controlos definidos de acordo com as politicas e normas internas, legislação europeia e nacional em vigor. • A implementação dos mecanismos de proteção deve respeitar a estratégia e as metodologias para a classificação da informação interna assim como os seus níveis de criticidade garantindo que a informação é tratada de acordo com o risco que ela representa dentro da organização. • As atividades deverão ser alinhadas com a *framework* de risco e segurança da informação da entidade (nas dimensões de gestão e operação). • As atividades deverão garantir o alinhamento da segurança da informação com os restantes domínios do sistema de informação.
Ferramentas	• As ferramentas a utilizar dependem da abordagem proposta pelo concorrente, mas consideramos que este serviço pode ser realizado recorrendo a soluções tecnológicas.
Resultado pretendido com este serviço	• Desenho, implementação ou apoio à operação dos mecanismos de proteção contra a perda de informação
Certificações aplicáveis	• *Certified Information Systems Security Professional (CISSP)* • *Certified Information Security Manager (CISM)*

Cláusula 5.ª Prazo de vigência

1. O acordo quadro tem a duração de 2 (dois) anos, a contar da data da sua entrada em vigor, e considera-se automaticamente renovado por períodos de 1 (um) ano se nenhuma das partes o denunciar, mediante notificação à outra parte por carta registada com aviso de receção, com a antecedência mínima de 60 (sessenta) dias em relação ao seu termo.
2. Após a renovação a que se refere o número anterior, a denúncia do acordo quadro pode ser efetuada a qualquer momento, desde que seja precedida de notificação à outra parte, por carta registada com aviso de receção, com uma antecedência mínima de 90 (noventa) dias em relação à data do termo pretendida.
3. O prazo máximo de vigência do acordo quadro, incluindo renovações, é de 4 (quatro) anos.

Cláusula 6.ª Forma e documentos contratuais

1. Os contratos de prestação celebrados ao abrigo do presente Acordo Quadro, são reduzidos a escrito.
2. Fazem parte integrante do acordo quadro os seguintes documentos:

a) Os suprimentos dos erros e das omissões do presente caderno de encargos identificados pelos concorrentes, desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar, ou pelo órgão a quem esta competência tenha sido delegada;
b) Os esclarecimentos e as retificações relativos ao presente caderno de encargos;
c) O presente caderno de encargos;
d) As propostas adjudicadas;
e) Os esclarecimentos prestados pelos adjudicatários sobre as propostas adjudicadas.

3. Em caso de divergência entre os documentos referidos no número anterior, a prevalência é determinada pela ordem pela qual são indicados nesse número.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seus anexos, prevalecem os primeiros, salvo quanto aos ajustamentos propostos de acordo com o disposto no artigo 99.º do Código dos Contratos Públicos (CCP) e aceites pelo adjudicatário nos termos do disposto no artigo 101.º desse mesmo diploma.
5. Além dos documentos indicados no n.º 2, o adjudicatário obriga-se também a respeitar, no que lhe seja aplicável, as normas europeias e portuguesas, as especificações e homologações de organismos oficiais e fabricantes ou entidades detentoras de patentes.
6. Em caso de divergência entre as obrigações a que se refere o número anterior, a prevalência é determinada pela ordem na qual são indicadas.

Secção II

Obrigações das Partes

Cláusula 7.ª Obrigações dos cocontratantes

1. Para além das previstas no CCP, constituem obrigações dos cocontratantes:
   a) O prestador terá de informar a SPMS, sempre que exista algum facto ou ação em tribunal que possa dar origem à sua insolvência ou a processo de recuperação;
   b) Apresentar proposta a todos os convites no âmbito do acordo quadro;
   c) Prestar os serviços às entidades adquirentes conforme as normas legais vigentes aplicáveis ao exercício da atividade, e nos termos e condições definidos no presente caderno de encargos;
   d) Comunicar à SPMS, EPE e às entidades adquirentes, logo que deles tenham conhecimento, os factos que tornem total ou parcialmente impossível o cumprimento de qualquer das suas obrigações, designadamente:

i. Impossibilidade temporária de prestação do serviço;

ii. Impossibilidade legal de prestação do serviço.

e) Não alterar as condições de prestação dos serviços, fora dos casos previstos no caderno de encargos;

f) Não ceder, sem prévia autorização da SPMS, EPE, a sua posição contratual nos contratos celebrados com as entidades adquirentes;

g) Prestar de forma correta e fidedigna as informações referentes às condições em que são prestados os serviços, bem como prestar todos os esclarecimentos que se justifiquem, de acordo com as circunstâncias;

h) Comunicar à SPMS, EPE qualquer facto que ocorra durante a execução do acordo quadro e dos contratos celebrados ao seu abrigo e que altere, designadamente, a sua denominação e sede social, os seus representantes legais, a sua situação jurídica ou a sua situação comercial, bem como as alterações aos contactos e moradas indicados no contrato para a gestão do acordo quadro;

i) Produzir relatórios de faturação e enviar estes relatórios à SPMS, EPE, com uma periodicidade trimestral, designadamente para efeitos estatísticos, autorizando expressamente a SPMS, EPE ao tratamento dos dados fornecidos;

j) Retificar os relatórios de faturação apresentados nos termos da alínea anterior, sempre que sejam detetadas irregularidades nos valores;

k) Sempre que solicitado pela SPMS, EPE, disponibilizar declaração emitida por um Revisor Oficial de Contas ou pela entidade fiscalizadora das contas da empresa, na qual se certifiquem os valores comunicados nos relatórios de faturação entregues, relativos aos procedimentos realizados ao abrigo do acordo quadro;

l) Comunicar à SPMS, EPE e às entidades adquirentes a nomeação do gestor de contrato responsável pela gestão do acordo quadro e dos contratos celebrados ao abrigo do mesmo, bem como quaisquer alterações relativamente à sua nomeação;

m) Disponibilizar a informação relevante para a gestão dos contratos à SPMS, EPE e às entidades adquirentes;

n) Respeitar os termos e condições dos acordos celebrados com o Estado que se encontrem em vigor;

o) Para efeitos de habilitação nos procedimentos de aquisição ao abrigo do acordo quadro, manter permanentemente atualizados os documentos de habilitação, bem como os documentos que atestem o poder de representação do cocontratante;

p) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do acordo quadro, e não utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos.

Cláusula 8.ª Obrigações das entidades adquirentes na gestão do acordo quadro

1. Constituem obrigações das entidades adquirentes, no âmbito e nos limites fixados:
   a) Reportar toda a informação relativa aos contratos celebrados ao abrigo do acordo quadro até 10 (dez) dias úteis após a adjudicação;
   b) Efetuar os procedimentos aquisitivos segundo as regras definidas no acordo quadro;
   c) Nomear um gestor responsável pela gestão dos contratos celebrados ao abrigo do acordo quadro, bem como comunicar quaisquer alterações a essa nomeação aos cocontratantes com quem tenham celebrado contrato;
   d) Monitorizar o cumprimento contratual no que respeita às respetivas condições e aplicar as devidas sanções em caso de incumprimento;
   e) Reportar os resultados da monitorização referida na alínea anterior e comunicar, em tempo útil à SPMS, EPE, os aspetos relevantes que tenham impacto no cumprimento do acordo quadro ou dos contratos celebrados ao seu abrigo.
2. A informação referida na alínea a) do número anterior deve ser enviada através de relatórios de contratação, elaborados em conformidade com o modelo a disponibilizar pela SPMS, EPE.

Cláusula 9.ª Obrigações da SPMS, EPE

1. Constituem obrigações da SPMS, EPE, no âmbito e nos limites fixados pelo Decreto-Lei n.º 19/2010, de 22 de março, na redação dada pelo Decreto-Lei n.º 108/2011, de 17 de novembro, na Portaria n.º 227/2014, de 6 de novembro, e sem prejuízo de outras que estejam previstas no presente caderno de encargos:
   a) Fiscalizar o cumprimento do acordo quadro e dos contratos de fornecimento celebrados ao abrigo do mesmo, designadamente para apuramento do cumprimento das obrigações contratuais por parte dos cocontratantes e das entidades adquirentes;

b) Monitorizar a qualidade da prestação de serviços, designadamente realizando auditorias e tratando a informação recebida ao abrigo do disposto nas cláusulas anteriores e, quando justificado, aplicar sanções em caso de incumprimento, incluindo a suspensão temporária ou a exclusão de algum cocontratante do acordo quadro, designadamente em caso de:

i. Reiterado reporte de falta de qualidade e/ou de falhas inesperadas na utilização dos produtos fornecidos por parte dos serviços utilizadores das entidades adquirentes e/ou incumprimento reiterado dos prazos de entrega da prestação dos serviços;

ii. Deteção dos casos reiterados referidos na subalínea i) anterior, em ações de monitorização pela SPMS, EPE;

iii. O cocontratante não apresentar proposta a procedimento lançado ao abrigo do acordo quadro.

c) Promover a atualização do acordo quadro, mantendo o tipo de prestação e os objetivos das especificações fixadas no acordo quadro, e desde que tal se justifique em função da ocorrência de inovações tecnológicas, conquanto os preços unitários não sejam superiores.

Cláusula 10.ª Auditoria à prestação de serviços

A qualquer momento a SPMS, EPE e as entidades adquirentes ou outras entidades mandatadas para o efeito, podem solicitar informação ou realizar auditorias com vista à monitorização da qualidade da execução dos contratos de prestação de serviços e o cumprimento das obrigações legais e, quando justificado, aplicar as devidas sanções.

Secção III

Das relações entre as partes no acordo quadro

Cláusula 11.ª Sigilo e confidencialidade

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa aos destinatários, de que possa ter conhecimento ao abrigo ou em relação com a execução do presente contrato.
2. O dever de sigilo previsto no número anterior abrange, designadamente, documentos escritos, dados pessoais, desenhos, planos, aplicações e programas informáticos no formato

de código fonte ou código objeto, especificações, segredos comerciais, métodos e fórmulas, contratos de financiamento e situações internas, de natureza laboral ou outra.

3. A informação coberta pelo dever de sigilo não pode ser transmitida a terceiros, nem objeto de licenciamento ou qualquer outro uso ou modo de aproveitamento económico, salvo se tal for autorizado expressamente, por escrito, pela entidade adjudicante.
4. O adjudicatário só pode transmitir informação confidencial aos seus colaboradores e, em qualquer caso, apenas se ocorrerem, cumulativamente, as seguintes circunstâncias:
    a) Os colaboradores em causa necessitarem de conhecer essa informação, tendo em vista o cumprimento das suas tarefas ao abrigo do contrato;
    b) Os colaboradores estiverem informados sobre a natureza confidencial da informação;
    c) Os colaboradores se obrigarem a cumprir o dever de sigilo emergente desta cláusula.
5. O adjudicatário é responsável pelo cumprimento do dever de sigilo por parte dos seus colaboradores, qualquer que seja a natureza jurídica do vínculo, inclusivamente após a cessação deste, independentemente da causa da cessação.
6. O adjudicatário é ainda responsável perante a entidade adjudicante, em caso de violação do dever de sigilo pelos terceiros por si subcontratados, bem como por quaisquer colaboradores desses terceiros.
7. O adjudicatário assume, igualmente, o compromisso de remover e destruir, no final do contrato, todo e qualquer tipo de registo (digital ou em papel) relacionado com os dados analisados e que o adjudicante considere acesso privilegiado.
8. Exclui-se do dever de sigilo previsto na presente cláusula a informação que fosse comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário, bem como a informação que o mesmo seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 12.ª Direitos de propriedade intelectual e industrial

1. O adjudicatário garante que respeita as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registadas, relacionadas com o hardware, software e documentação técnica que utilizam no desenvolvimento da sua atividade.

2. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização de marcas registadas, patentes registadas ou licenças.
3. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o adjudicatário terá de a indemnizar de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar.
4. Sempre que legalmente admissível e na máxima extensão admitida na lei, o resultado da prestação dos serviços será registado a favor da entidade adjudicante, em sede de direito de propriedade industrial e/ou de propriedade intelectual, conforme o caso, ainda que se verifique a cessação do contrato por qualquer motivo.
5. O adjudicatário obriga-se a colaborar e a prestar assistência à entidade adjudicante, relativamente aos procedimentos e às formalidades necessárias para a realização dos referidos registos.

Cláusula 13.ª Patentes, licenças e marcas registadas

1. São da responsabilidade dos cocontratantes quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
2. Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o adjudicatário terá de a indemnizar de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar.

Cláusula 14.ª Dados pessoais

A atividade desenvolvida pelo adjudicatário e respetivos trabalhadores ou colaboradores, no âmbito do presente procedimento, independentemente do vínculo contratual que possuam com o mesmo, encontra-se sujeita à aplicação da Lei n.º 67/98 de 26 de Outubro (Lei da Proteção de Dados Pessoais).

Cláusula 15.ª Utilização dos sistemas de informação

Caso a execução do presente contrato implique o acesso às instalações e a utilização dos sistemas de informação da entidade adjudicante por colaboradores ou subcontratados do adjudicatário, os mesmos obrigam-se ao cumprimento integral das regras de utilização dos sistemas de informação em vigor na entidade adjudicante.

Cláusula 16.ª Casos fortuitos ou de força maior

1. Nenhuma das partes incorrerá em responsabilidade se, por caso fortuito ou de força maior, for impedida de cumprir as obrigações assumidas no acordo quadro.
2. Entende-se por caso fortuito ou de força maior qualquer situação ou acontecimento imprevisível e excecional, independente da vontade das partes, e que não derive de falta ou negligência de qualquer delas.
3. A parte que invocar casos fortuitos ou de força maior deverá comunicar e justificar tais situações à outra parte, bem como informar o prazo previsível para restabelecer a situação.

Cláusula 17.ª Suspensão do acordo quadro

1. Sem prejuízo do direito de resolução do acordo quadro, a SPMS, EPE pode, em qualquer altura, por motivos de interesse público, nomeadamente quando estiverem em causa razões de segurança pública, suspender total ou parcialmente a execução do acordo quadro.
2. A suspensão produz os seus efeitos a contar do dia seguinte ao da notificação dos cocontratantes no acordo quadro, salvo se da referida notificação constar data posterior.
3. A SPMS, EPE pode, a qualquer momento, levantar a suspensão da execução do acordo quadro.
4. Os prestadores de serviços selecionados como cocontratantes no acordo quadro não podem reclamar ou exigir qualquer compensação ou indemnização com base na suspensão total ou parcial do acordo quadro.
5. Caso o cocontratante selecionado no acordo quadro não disponibilize os recursos suficientes para a realização do serviço contratualizado, a SPMS, EPE reserva-se o direito de, com justa causa, e sem prejuízo de resolução nos termos do número seguinte, o suspender do acordo quadro, sem prejuízo de resolução nos termos do número seguinte.

Cláusula 18.ª Resolução sancionatória por incumprimento contratual

1. O incumprimento, por qualquer dos cocontratantes selecionados, das obrigações que sobre si recaem nos termos do acordo quadro, dos contratos celebrados ao seu abrigo ou dos demais documentos contratuais aplicáveis, confere à SPMS, EPE o direito à resolução do acordo quadro relativamente àquele, podendo a SPMS, EPE solicitar o correspondente ressarcimento de todos os prejuízos causados.

2. O incumprimento dos requisitos mínimos de serviço deve ser reportado pelas entidades adquirentes à SPMS, EPE.
3. Para efeitos da presente cláusula, e sem prejuízo de outras disposições legais e contratuais aplicáveis, considera-se consubstanciar incumprimento a verificação de qualquer das seguintes situações, em relação a cada um dos prestadores de serviços:
   a) Incumprimento das suas obrigações relativas aos pagamentos das contribuições à Administração Fiscal ou à Segurança Social, nos termos das disposições legais aplicáveis;
   b) Prestação de falsas declarações;
   c) Não apresentação dos relatórios previstos na cláusula 31.ª do presente caderno de encargos;
   d) Recusa do serviço a uma entidade adquirente;
   e) Não apresentação de proposta ou apresentação de proposta não válida, nos termos da cláusula 27.ª do presente caderno de encargos;
   f) Incumprimento dos requisitos mínimos previstos nas cláusulas 4.ª do presente caderno de encargos;
   g) Prestação de serviços que não constem do acordo quadro;
   h) Incumprimento da obrigação de sigilo e confidencialidade prevista na cláusula 11.ª do presente caderno de encargos.
4. Para efeitos do disposto nas alíneas f), g) e h) do número anterior, considera-se haver incumprimento definitivo quando, após advertência e aplicação de sanção, o cocontratante continue a incorrer em incumprimento.
5. A resolução é notificada ao cocontratante em causa, por carta registada com aviso de receção, da qual conste a indicação da situação de incumprimento e respetivos fundamentos.
6. A resolução do acordo quadro relativamente a um cocontratante não prejudica a aplicação de qualquer das sanções previstas na cláusula seguinte do presente caderno de encargos.

Cláusula 19.ª Sanções

1. O incumprimento das obrigações do cocontratante determina a aplicação de sanções pecuniárias nos termos a definir em cada procedimento.
2. O valor das sanções constantes do número anterior é descontado na fatura relativa ao período em que se deu o facto que originou a sua aplicação.

3. Pelo incumprimento do disposto na cláusula 4.ª do presente documento, a SPMS, EPE poderá após a ocorrência da 5.ª infração aplicar uma penalização de suspensão ou eliminação do prestador de serviços incumpridor do acordo quadro, no lote em causa.

Cláusula 20.ª Cessão da posição contratual e subcontratação

1. Os cocontratantes só podem ceder a sua posição no acordo quadro, ou subcontratar total ou parcialmente a prestação de serviços objeto do acordo quadro, mediante autorização prévia e por escrito da SPMS, EPE.

2. Para efeitos da autorização da cessão por parte da SPMS, EPE, o cocontratante, cedente, deve apresentar uma proposta fundamentada e instruída com os documentos de habilitação relativos ao potencial cessionário que lhe foram exigidos na fase de formação do acordo quadro.

3. O prestador não poderá recorrer a terceiras entidades que tratem dados pessoais sem o consentimento prévio da entidade adjudicante.

4. Para efeitos da autorização da subcontratação por parte da SPMS, EPE, o cocontratante, subcontratante, deve apresentar uma proposta fundamentada e instruída com os documentos de habilitação e adesão ao catálogo através do formulário constante no sítio da internet, relativos ao potencial subcontratado, que lhe foram exigidos na fase de formação do acordo quadro.

5. A SPMS, EPE deve pronunciar-se sobre a proposta do cocontratante no prazo de 30 dias a contar da respetiva apresentação, desde que regularmente instruída.

6. Nos casos em que a SPMS, EPE venha a autorizar a subcontratação, o cocontratante permanece integralmente responsável perante a SPMS, EPE pelo exato e pontual cumprimento de todas as obrigações contratuais.

PARTE II - Dos procedimentos de contratação celebrados ao abrigo do acordo quadro

Secção I

Obrigações das entidades adquirentes no âmbito dos contratos celebrados ao abrigo do acordo quadro

Cláusula 21.ª Contratação ao abrigo do acordo quadro

1. A contratação ao abrigo do acordo quadro é efetuada através de convite a todos os cocontratantes do lote do acordo quadro ao abrigo do qual será lançado o procedimento, nos termos do artigo 259.º do CCP.
2. Os procedimentos lançados ao abrigo do acordo quadro devem ser efetuados através da plataforma eletrónica disponível em www.comprasnasaude.pt, nos termos do disposto na Portaria n.º 227/2014, de 6 de novembro, alterado pela portaria n.º 21/2015, de 4 de fevereiro.
3. Deve ser dirigido um convite às entidades selecionadas no acordo quadro, não podendo ser fixado um prazo para apresentação das propostas inferior a 5 (cinco) dias.
4. A entidade adquirente responsável pelo convite pode recorrer ao leilão eletrónico, nos termos previstos no CCP, para melhorar as condições propostas pelos concorrentes.
5. Os preços unitários devem ser indicados com duas casas decimais, em algarismos e por extenso, e devem incluir todas as taxas, impostos e restantes condições, não sendo admitidos portes ou outras taxas adicionais em qualquer circunstância.
6. As entidades adquirentes devem identificar no momento da compra ao abrigo do presente acordo quadro, a totalidade do objeto sob o qual pretendem que incida o serviço a adquirir devendo para o efeito identificar a categoria e o lote, conforme modelo indicado no **Anexo A**.

Cláusula 22.ª Definição das prestações a contratualizar

1. As entidades adquirentes devem em cada procedimento:
   a) Definir as condições específicas que se aplicam à contratualização dos serviços em causa, as quais podem ser da seguinte natureza:
      i. Prazos de entrega;
      ii. Termos de aceitação;
      iii. Definir os níveis de serviço exigíveis;
      iv. Modelo de monitorização e controlo dos níveis de serviço definidos.

b) Realizar inquéritos de satisfação a cada prestador após o término de um contrato, de modo a poder avaliar os prestadores de serviços e aferir a qualidade dos serviços prestados, devendo ser definido um nível de serviço mínimo para esse questionário (exemplo consta em Anexo B ao presente documento).

c) Definir, para cada nível de serviço ou prazos de entrega, as penalizações pecuniárias a aplicar, em caso de incumprimento.

Cláusula 23.ª Critérios de adjudicação nos procedimentos ao abrigo do Acordo Quadro

1. Nos procedimentos ao abrigo do acordo quadro a adjudicação é feita por lote.
2. O critério de adjudicação nos procedimentos desenvolvidos ao abrigo do presente acordo quadro poderá ser o do mais baixo preço, ou o da proposta economicamente mais vantajosa.

Cláusula 24.ª Documentos da proposta nos procedimentos desenvolvidos ao abrigo do acordo quadro

Devem fazer parte dos documentos que integram as propostas apresentadas os procedimentos desenvolvidos ao abrigo do presente acordo-quadro:

a) Apresentação de preço de proposta;

b) Documento descritivo do serviço a prestar;

c) Identificação do gestor de contrato inerente à prestação de serviços a contratar.

Cláusula 25.ª Forma e Prazo de Vigência dos contratos celebrados ao abrigo do acordo-quadro

1. Os contratos de prestação de serviços celebrados ao abrigo do acordo quadro serão reduzidos a escrito e terão uma duração máxima de 1 (um) ano a contar da data da sua assinatura, prorrogável por mais 1 (um) ano até ao limite máximo de 2 (dois) anos, não podendo a sua duração total ser superior a 3 (três) anos.
2. Os contratos que sejam celebrados ao abrigo do acordo-quadro podem produzir efeitos para além da vigência do acordo-quadro, desde que não ultrapassem as durações previstas no número anterior.
3. A celebração de novo acordo quadro com o mesmo objeto impossibilita qualquer renovação, por parte das entidades adquirentes, dos contratos celebrados ao abrigo do acordo quadro objeto do presente caderno de encargos.

Cláusula 26.ª Condições e prazo de pagamento

1. As entidades adquirentes são exclusivamente responsáveis pelo pagamento do preço dos serviços que lhe sejam prestados, não podendo, em caso algum, o cocontratante emitir faturas à SPMS, EPE, na qualidade da entidade que celebrou o acordo-quadro objeto do presente procedimento.
2. O preço da prestação de serviços às entidades adquirentes é o que resultar do disposto neste caderno de encargos e da proposta adjudicada no procedimento celebrado ao abrigo do acordo quadro, não podendo, em caso algum, ser superior ao preço máximo de referência estabelecido neste acordo quadro.
3. O prazo de pagamento é o que for praticado por cada entidade adquirente, nos termos da lei.
4. O atraso no pagamento confere ao prestador de serviços o direito aos juros de mora calculados nos termos da lei.
5. Não podem ser realizados quaisquer pagamentos no âmbito da prestação de serviços sem que se mostrem pagos os emolumentos devidos por fiscalização prévia do contrato respetivo por parte do Tribunal de Contas.

Secção II

Obrigações dos cocontratantes no âmbito dos contratos celebrados ao abrigo do acordo quadro

Cláusula 27.ª Obrigações

1) Para além das previstas no CCP, constituem obrigações dos cocontratantes:
   a) Obrigatoriedade de resposta aos procedimentos / call offs despoletados ao abrigo do acordo quadro objeto do presente procedimento, ou seja, todos os prestadores de serviços qualificados em cada lote são obrigados a responder, no prazo determinado, a todos os procedimentos / *call offs* lançados, para o respetivo lote;
   b) Cumprimento do prazo de disponibilização de recursos, num prazo máximo de 15 (quinze) dias para a disponibilização dos recursos para a execução dos serviços, desde a data da assinatura do contrato. O prazo para disponibilização dos recursos pode ser estendido, mediante um acordo entre ambas as partes;

c) Garantir que o pessoal operacional possui os conhecimentos e credenciação necessários para o desempenho das suas funções;

d) Prestar o serviço em perfeita conformidade com as condições estabelecidas nos documentos contratuais, podendo a entidade adquirente exercer, por si ou através de consultores especializados, a fiscalização e acompanhamento da execução do contrato;

e) Prestar de forma correta e fidedigna as informações referentes às condições em que são prestados os serviços, bem como prestar todos os esclarecimentos que se justifiquem, de acordo com as circunstâncias;

f) Recorrer a todos os meios humanos, materiais e tecnológicos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo;

g) Informar a entidade adquirente sobre as alterações verificadas durante a execução do contrato;

h) Comunicar à entidade adquirente, com uma antecedência mínima de 30 dias, os factos que tornem total ou parcialmente impossível a prestação dos serviços definida no caderno de encargos e demais documentos contratuais;

i) Enviar com uma periodicidade trimestral, a informação sobre as ocorrências na execução do contrato, destinada ao acompanhamento da execução do contrato;

j) Elaborar, no final da execução do contrato, um relatório final, com informação detalhada sobre as situações ocorridas e os prazos assumidos para a resolução/indemnização dos mesmos.

Cláusula 28.ª Revisão de Preços

A revisão de preços só pode ocorrer após 12 (doze) meses contados do dia seguinte à entrada em vigor do acordo quadro e em casos devidamente justificados.

Cláusula 29.ª Aditamentos

1. Quaisquer alterações de ordem financeira e técnica relativamente aos serviços selecionados, que ocorram durante o prazo de vigência dos acordos quadro, devem ser obrigatoriamente comunicadas à SPMS, EPE.

2. Para formalização dos aditamentos, deverão os cocontratantes proceder ao seu preenchimento e submissão *on-line* e envio via fax ou *email* para a SPMS, EPE, com vista à sua autorização.
3. Para efeitos do n.º 1, consideram-se aditamentos os decorrentes das seguintes situações:
   a) Aumento de Preços;
   b) Redução de Preços;
   c) Inserção de Descontos;
   d) Interrupção Temporária de prestação do serviço;
   e) Alteração de outros elementos.
4. Os aditamentos tipificados no número anterior deverão ser utilizados da forma e com base nos documentos necessários à comprovação dos requisitos que a seguir se indicam:
   a) Aumento de Preços: este aditamento deverá ser utilizado para formalização dos pedidos de aumento de preço, o qual só pode ser praticado após autorização da SPMS, EPE;
   b) Redução de Preço: este aditamento deverá ser utilizado quando o cocontratante determina a redução de preço, diretamente junto da SPMS, EPE;
   c) Inserção de Descontos: este aditamento deverá ser utilizado sempre que o cocontratante pretenda efetuar descontos no preço em função das quantidades ou de prazos de pagamento ou da localização da instituição. Não são aceites aditamentos que introduzam escalões de desconto menos favoráveis que os que constam do catálogo;
   d) Interrupção Temporária de prestação de serviços: este aditamento deve ser utilizado sempre que haja uma interrupção de prestação de serviços nos termos do n.º 2 da cláusula 30.ª;

Cláusula 30.ª Impossibilidade temporária de prestação de serviços

1. Sempre que o cocontratante se encontre em situação de impossibilidade temporária de prestação de serviços, deverá comunicar fundamentadamente tal facto à SPMS, EPE.
2. Para efeitos do disposto no número anterior, considera-se impossibilidade temporária de prestação de serviços uma interrupção por período não superior a 90 (noventa) dias contínuos.

3. Findo o prazo previsto no número anterior sem que a situação se regularize, deverá o cocontratante solicitar a prorrogação do prazo, reservando-se a SPMS, EPE, todavia, o direito de resolver o contrato.
4. Não é admissível a impossibilidade temporária de prestação de serviços nos primeiros 8 (oito) meses de vigência do acordo quadro, que será considerada incumprimento dos prazos de execução.

PARTE III– Reporte

Cláusula 31.ª Reporte e monitorização

1. É obrigação dos cocontratantes produzir e enviar os seguintes relatórios de gestão do acordo quadro:
   a) Relatórios de faturação;
   b) Relatórios de níveis de serviço.
2. Os cocontratantes devem enviar os relatórios de faturação às entidades adquirentes com uma periodicidade trimestral e à SPMS, EPE com uma periodicidade semestral.
3. O não envio dos relatórios referidos no n.º 1 da presente cláusula, ou a existência de erros nos mesmos que não permitam a monitorização da faturação, tem um efeito suspensivo no pagamento das faturas em dívida até à regularização da situação em causa.
4. Para efeitos do disposto no número anterior, a entidade adquirente deverá notificar previamente o cocontratante para, num prazo não superior a 5 (cinco) dias, emitir o relatório em falta ou corrigir a informação em falta no relatório enviado.
5. Os relatórios são emitidos tendo em conta a existência de 2 (dois) perfis diferenciados:
   a) SPMS, EPE – recebe a informação respeitante aos contratos resultantes de procedimentos conduzidos de forma individual pelas entidades adquirentes e a informação agregada ao nível das entidades adquirentes e das entidades adquirentes que as integram, caso os contratos resultem de procedimentos conduzidos por entidades adquirentes;
   b) Entidade adquirente – recebe a informação individualizada da realidade que representa.
6. Os relatórios de faturação devem conter, com a agregação de informação indicada no número anterior, os seguintes elementos:

a) Identificação da entidade adquirente;
b) Número de contrato;
c) Duração prevista do contrato;
d) Datas de início e de fim do contrato;
e) Descrição quantitativa do serviço e respetivos preços unitários;
f) Identificação dos lotes;
g) Valor de contrato;
h) Número, data e valor das faturas.

7. Os relatórios de níveis de serviço podem ser solicitados pelas entidades adquirentes com uma periodicidade mensal e devem conter, com a agregação de informação indicada no número anterior da presente cláusula, os seguintes elementos relativos a requisitos definidos na cláusula 4.ª do presente caderno de encargos, bem como eventuais sanções aplicadas pelas entidades adquirentes:
   a) Identificação da entidade adquirente;
   b) Número de contrato;
   c) Duração prevista do contrato;
   d) Datas de início e de fim do contrato;
   e) Quantidades de serviços encomendados e entregues;
   f) Número de dias decorridos entre a data da encomenda e a data de entrega da aceitação do serviço;
   g) Tipo e quantidade de serviços prestados sem a qualidade requerida;
   h) Justificação para eventuais incumprimentos nos serviços;
   i) Sanções aplicadas e respetiva justificação.
8. Os relatórios definidos nos números anteriores devem ser enviados à SPMS, EPE e entidades adquirentes, até ao dia 20 (vinte) do mês subsequente ao final do semestre, trimestre ou mês do ano civil a que digam respeito, conforme periodicidades previstas no n.º 2 e 7 da presente cláusula, em formato eletrónico a definir pela SPMS, EPE.

PARTE IV - Disposições finais

Cláusula 32.ª Comunicações e notificações

1. Quaisquer comunicações ou notificações entre a SPMS, EPE e os cocontratantes relativas ao acordo quadro, devem ser efetuadas através de correio eletrónico com aviso de entrega, carta registada com aviso de receção ou fax.
2. Qualquer comunicação ou notificação feita por carta registada é considerada recebida na data em que for assinado o aviso de receção ou, na falta dessa assinatura, na data indicada pelos serviços postais.
3. Qualquer comunicação ou notificação feita por correio eletrónico é considerada recebida na data constante na respetiva comunicação de receção transmitida pelo recetor para o emissor.
4. As notificações e as comunicações que tenham como destinatário a SPMS, EPE, entidades adquirentes e que sejam efetuadas através de correio eletrónico, fax ou outro meio de transmissão escrita e eletrónica de dados, feitas após as 17 (dezassete) horas do local de receção ou em dia não útil nesse mesmo local, presumem-se feitas às 10 (dez) horas do dia útil seguinte.

Cláusula 33.ª Foro competente

Para resolução de todos os litígios decorrentes do contrato, fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

Cláusula 34.ª Contagem dos prazos na fase de execução do acordo quadro e dos contratos celebrados ao seu abrigo

À contagem de prazos na fase de execução do acordo quadro e dos contratos celebrados ao seu abrigo, são aplicáveis as seguintes regras:

a) Não se inclui na contagem do prazo o dia em que ocorrer o evento a partir do qual o mesmo começa a correr;

b) Os prazos são contínuos, não se suspendendo nos sábados, domingos e feriados;

c) O prazo fixado em semanas, meses ou anos, a contar de certa data, termina às 24 (vinte e quatro) horas do dia que corresponda, dentro da última semana, mês ou ano, a essa data; se no último mês não existir dia correspondente, o prazo finda no último dia desse mês;

d) O prazo que termine em sábado, domingo, feriado ou em dia em que o serviço, perante o qual deva ser praticado o ato, não esteja aberto ao público, ou não funcione durante o período normal, transfere-se para o 1.º dia útil seguinte.

Cláusula 35.ª Interpretação e validade

1. O acordo quadro e demais documentos contratuais regem-se pela lei portuguesa, sendo interpretados de acordo com as suas regras.
2. As partes no acordo quadro que tenham dúvidas acerca do significado de quaisquer documentos contratuais, devem colocá-las à parte contrária a quem o significado dessa disposição diga diretamente respeito.
3. Se qualquer disposição do acordo quadro ou de quaisquer documentos contratuais for anulada ou declarada nula, as restantes disposições não serão prejudicadas por esse facto, mantendo-se em vigor.

Cláusula 36.ª Direito aplicável

1. O acordo quadro tem natureza administrativa.
2. A tudo o que não esteja especialmente previsto no presente caderno de encargos aplica-se a legislação portuguesa e, em especial, o regime constante do Código da Contratação Pública, aprovado pelo D.L. nº 18/2008, de 29 de janeiro, com as alterações vigentes o qual prevalece sobre as disposições que lhe sejam desconformes.

ANEXOS:

Anexo A – Categoria do Serviço

Anexo B – Exemplo de Inquérito de satisfação

ANEXO A – CATEGORIA DO SERVIÇO
(EXEMPLO)

Categoria	Lote	Serviço
Categoria 1 – Governo da segurança e gestão do risco	Lote 1 – Estratégia e plano de ação de segurança	Características funcionais, características técnicas, (…)
(…)	(…)	(…)

ANEXO B – EXEMPLO NÃO VINCULATIVO DE QUESTIONÁRIO DE INQUERITO DE SATISFAÇÂO APOS TERMINUS DE CONTRATO

Exemplo de Questionário de Satisfação

Questão	Avaliação	Comentários
Como classificaria o desempenho geral do fornecedor?	Escala da avaliação	
Qual o nível de cumprimento dos níveis de serviço impostos no contrato?	Escala da avaliação	
Qual o grau de satisfação para com o trabalho realizado?	Escala da avaliação	
Qual o grau de criação de valor do fornecedor?	Escala da avaliação	
Voltaria a trabalhar com o mesmo fornecedor?	Sim / Não	
Recomendaria o fornecedor a outras entidades clientes?	Sim / Não	

Escala de Avaliação:

5 – Muito Bom

1 – Muito Mau