



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Consulta Prévia n.º

001/ASI/ 2021

CADERNO DE ENCARGOS

**Aquisição de serviços de outsourcing de apoio
à Administração de Segurança da Informação (ASI)**



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1	INTRODUÇÃO	1
2	Objeto.....	1
3	DESCRIÇÃO DOS SERVIÇOS A PRESTAR	2
3.1	Preparação	2
3.2	Avaliação e Tratamento do Risco.....	3
3.3	Operação do SGSI.....	3
3.4	Gestão e Controlo	3
3.5	Cronograma.....	4
4	PERFIL DE COMPETÊNCIAS	4
5	REQUISITOS DO FORNECEDOR.....	4
6	REQUISITOS DE QUALIFICAÇÕES PROFISSIONAIS	5
7	LOCAL DE PRESTAÇÃO DE SERVIÇOS	5
8	PRAZO DE EXECUÇÃO	5
9	PREÇO, CONDIÇÕES DE PAGAMENTO E FATURAÇÃO	5
10	CRITÉRIO DE ADJUDICAÇÃO	Erro! Marcador não definido.
11	SIGILO	6
12	REQUISITOS DE PROTEÇÃO DE DADOS	7
13	REQUISITOS DE SEGURANÇA DA INFORMAÇÃO	8
14	PENALIDADES	9
15	GESTOR DO CONTRATO.....	11
16	CASOS FORTUITOS OU DE FORÇA MAIOR.....	11
17	PATENTES, LICENÇAS E MARCAS.....	11
18	CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO	12
19	RESOLUÇÃO DO CONTRATO.....	12
20	GARANTIA.....	12
21	LEGISLAÇÃO APLICÁVEL.....	12



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

1 INTRODUÇÃO

O processo de implementação do Sistema de Gestão da Segurança da Informação da Assembleia da República (SGSI-AR) compreende o desenvolvimento das seguintes atividades: Diagnóstico; Planeamento; Implementação e Operação; Monitorização e Avaliação; e Melhoria Contínua.

Implementação do SGSI-AR

A implementação do SGSI-AR, iniciada no segundo semestre de 2019, tem como objetivo estabelecer a sistematização de controlos de segurança da informação baseada na norma ISO/IEC 27001: 2013 e está a ser desenvolvida em duas fases:

1ª FASE - concluída em junho de 2020

- **DIAGNÓSTICO DA SITUAÇÃO ATUAL:** consistiu na compreensão do negócio, na determinação do *gap* entre os requisitos standard e as práticas atuais;
- **PLANEAMENTO DO SISTEMA:** o Planeamento do SGSI-AR compreendeu o desenvolvimento das seguintes atividades:
 - ✓ Desenhar o modelo de administração de segurança da informação
 - ✓ Elaborar a política geral de segurança da informação
 - ✓ Documentar as políticas operacionais, processos e procedimentos do SGSI
 - ✓ Elaborar o roadmap estratégico de implementação do SGSI

2ª FASE – iniciada em julho de 2020

- **IMPLEMENTAÇÃO E OPERAÇÃO:** consiste em implementar e operacionalizar a política de segurança da informação através de controlos e medidas de segurança da informação, de processos e de procedimentos;
- **MONITORIZAÇÃO E AVALIAÇÃO:** inclui a realização de controlos e práticas necessárias para avaliar a eficiência e a eficácia do SGSI-AR, com o objetivo de melhorar o desempenho do sistema;
- **MANUTENÇÃO E MELHORIA:** compreende a execução de ações corretivas e preventivas com base nos resultados da avaliação, com o objetivo de assegurar a melhoria contínua do SGSI-AR.

2 OBJETO

Após a conclusão da 1ª Fase do processo de implementação do SGSI-AR (Diagnóstico da Situação Atual e Planeamento do Sistema), foi elaborado o respetivo Relatório de Avaliação onde são apresentadas as principais conclusões do diagnóstico, com resultados do *gap analysis* e recomendações de ações a desenvolver em função de observações e de evidências das práticas de segurança de informação na AR, face aos requisitos da norma ISO 27001:2013.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

O presente Caderno de Encargos tem por objeto a aquisição de serviços de apoio em regime de *outsourcing* para a gestão do sistema de Segurança da Informação da Assembleia da República, que compreende a implementação e operacionalização das recomendações do Relatório de Diagnóstico do SGSI-AR, que a seguir se descrevem.

3 DESCRIÇÃO DOS SERVIÇOS A PRESTAR

De acordo com o cronograma do plano de implementação dos sistemas em questão, a fase subsequente do processo é a Implementação e Operação, ou seja, implementar as políticas operacionais, procedimentos, modelos e processos definidos na fase de planeamento.

Para melhorar a eficácia e a eficiência na gestão da Administração de Segurança da Informação foi adquirida uma plataforma de software que permite a gestão de forma estruturada da **Documentação** (manuais, planos e políticas operacionais, procedimentos, processos, modelos, relatórios e a declaração de aplicabilidade); de **Incidentes** de Segurança da Informação; de **Auditorias** ISO 27001; do **Risco**; de **Inquéritos**, de **Questionários**, de **Awareness** e **E-learning**, que estão a ser desenvolvidos no âmbito da implementação do SGSI-AR.

Tendo em consideração o facto de a área de Administração de Segurança da Informação dispor atualmente de um único funcionário, a implementação em tempo útil das recomendações apresentadas no Relatório de Diagnóstico só será exequível através de recurso a serviços de apoio para a Administração de Segurança de Informação, em regime de *outsourcing*.

No desenvolvimento das atividades descritas nesta prestação de serviços, os entregáveis abaixo discriminados deverão ser disponibilizados na plataforma de SGSI-AR.

3.1 Preparação

Atividades	Entregáveis	Duração
Acompanhamento das aprovações e comunicação/partilha dos elementos do SGSI desenhados no SGSI. Coordenar na Formação/Consciencialização do SGSI desenhado na organização para todas as partes interessadas. Acompanhar no estabelecimento e nomeação dos perfis, responsabilidades e autoridades do SGSI. Acompanhar na identificação das competências ou necessidades de competências para os perfis e responsabilidades do SGSI.	Acompanhamento pela Equipa CISOaaS da execução das iniciativas e atividades do SGSI Ações de formação/consciencialização (conteúdos e aulas)	2 meses

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

3.2 Avaliação e Tratamento do Risco

Atividades	Entregáveis	Duração
Coordenar o levantamento e inventário da informação Coordenar a avaliação de risco de segurança da informação de acordo com a metodologia definida na AR. Acompanhar a execução do plano de tratamento de risco de Segurança da Informação.	Base de dados do Inventário Registo e relatório de avaliação de risco Plano de tratamento de risco	4 meses

3.3 Operação do SGSI

Atividades	Entregáveis	Duração
Acompanhamento das atividades do Roadmap estratégico – Planos de ação SGSI. Planeamento e acompanhamento da comunicação dos Objetivos de SI a toda a organização. Rever e Documentar todas as Políticas, Procedimentos, SoA e Processos Operacionais de SI exigidas pela norma e identificadas na avaliação de risco. Planeamento e acompanhamento da revisão pela Gestão. Planeamento e acompanhamento das Revisões de Acessos (lógico e físicos), Auditorias técnicas e Internas do SGSI. Coordenar o levantamento de necessidades de formação, planeamento e acolhimento do funcionário. Acompanhamento na monitorização de métricas do SGSI e eventos de SI. Apoio na determinação de oportunidades de melhoria (OMs) e ações corretivas (ACs) oriundas de auditorias internas.	Acompanhamento pela Equipa CISOaaS da execução das iniciativas e atividades do SGSI Verificação pela Equipa CISOaaS da aferição das métricas e objetivos do SGSI Documentos do SGSI Relatório da revisão pela Gestão. Plano de formações de Segurança da Informação Relatórios das Revisões e auditorias (técnicas e internas) Registo de OMs e ACs	8 meses

3.4 Gestão e Controlo

Atividades	Entregáveis	Duração
Pontos de situação trimestrais – atualização do plano de atividades, identificação do progresso, níveis do serviço, gestão de riscos do serviço e eventuais constrangimentos identificados.	Relatório de gestão de serviço CISOaaS	12 meses

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

3.5 Cronograma

ATIVIDADES	MÊS 1	MÊS 2	MÊS 3	MÊS 4	MÊS 5	MÊS 6	MÊS 7	MÊS 8	MÊS 9	MÊS 10	MÊS 11	MÊS 12
Preparação												
Avaliação e Tratamento do Risco												
Operação do SGSI												
Gestão e Controlo												

4 PERFIL DE COMPETÊNCIAS

A equipa deverá ser constituída, pelo menos, pelos seguintes perfis multidisciplinares de competências de conhecimentos teóricos e práticos, nas áreas de cibersegurança e segurança da informação, evidenciando as suas qualificações, através da inclusão da cópia das certificações profissionais requeridas:

i. Gestor de Segurança da Informação

Perfil sénior de *advisor* estratégico de segurança da informação com pelo menos **10 anos** de experiência em Segurança da Informação e em projetos de avaliação, implementação, manutenção e melhoria de Sistemas de Gestão de Segurança da Informação baseados na norma ISO/IEC 27001.

ii. Especialista de Gestão de Segurança da Informação

Perfil sénior de gestor de cibersegurança e segurança da informação, para a gestão, acompanhamento e controlo das políticas operacionais e processos de gestão de segurança da informação, com pelo menos **5 anos** de experiência em Segurança da Informação e em projetos de avaliação, implementação, manutenção e melhoria de Sistemas de Gestão de Segurança da Informação baseados na norma ISO/IEC 27001.

iii. Consultor de Gestão de Segurança da Informação

Perfil de consultor de cibersegurança e segurança da informação, com pelo menos **3 anos** de experiência em Segurança da Informação e em projetos de avaliação, implementação, manutenção e melhoria de Sistemas de Gestão de Segurança da Informação baseados na norma ISO/IEC 27001.

5 REQUISITOS DO FORNECEDOR

O fornecedor deverá satisfazer os seguintes requisitos:

- Estar certificado na norma ISO/IEC 27001 por entidade acreditada, num âmbito adequado a este projeto, isto é, consultoria em cibersegurança ou em sistemas de segurança de informação;
- Experiência comprovada através de declaração, de já ter prestado serviços de **Administração de Segurança da Informação as a Service (ASlaaS)**, a pelo menos 5 (cinco) empresas ou instituições em Portugal, nos últimos 3 (três) anos;

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- Dispor de uma linha dedicada de apoio e suporte à prestação de serviços de cibersegurança e segurança da informação, em situações de emergência.

6 REQUISITOS DE QUALIFICAÇÕES PROFISSIONAIS

A equipa deverá ser constituída, pelo menos, pelos seguintes perfis multidisciplinares de competências de conhecimentos teóricos e práticos, nas áreas de cibersegurança e segurança da informação, evidenciando as suas qualificações, através da inclusão de cópia das seguintes certificações profissionais:

- Pelo menos 1 consultor certificado com ISO/IEC 27001 *Lead Auditor*;
- Pelo menos 2 consultores certificados com ISO/IEC 27001 *Lead Implementer*;
- Pelo menos 1 consultor certificado com ISO/IEC 27005 *Risk Lead Manager*;
- Pelo menos 1 consultor certificado com *CISM – Certified Information Security Manager*.

7 LOCAL DE PRESTAÇÃO DE SERVIÇOS

Os serviços serão executados com 30% de ocupação presencial nas instalações da Assembleia da República, na Avenida D. Carlos I, 128, 1200-650, Lisboa e com 70% através de videoconferência, em sessões de trabalho remoto, à exceção de casos de força maior, devidamente justificados e acordados entre as partes.

8 PRAZO DE EXECUÇÃO

Os serviços serão prestados pelo período de 1 (um) ano, com início da data de assinatura do contrato e término após 12 meses.

9 PREÇO, CONDIÇÕES DE PAGAMENTO E FATURAÇÃO

- a) Para a prestação dos serviços de **Administração de Segurança da Informação as a Service (ASlaaS)**, a Assembleia da República pagará o preço total constante da proposta que não deverá exceder os **60.000,00 € (sessenta mil euros)**, acrescido de IVA à taxa legal em vigor.
- b) Considera-se incluído no valor do serviço todos os custos inerentes ao cumprimento integral dos requisitos descritos no caderno de encargos, bem como eventuais elementos adicionais incluídos na proposta do concorrente.
- c) O valor acima referido será pago pela Assembleia da República ao adjudicatário, em 12 (doze) prestações mensais e sucessivas, no prazo máximo de 30 (trinta) dias a contar da data da receção da fatura correspondente, desde que apresentada nos termos adequados à sua liquidação.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- d) A Assembleia da República poderá formular reservas à faturação apresentada, aceitando-a total ou parcialmente, notificando desse facto o adjudicatário, no prazo de 5 (cinco) dias após o conhecimento daquela e do relatório referente à intervenção, solicitando-lhe que este proceda à respetiva retificação da mesma.
- e) O adjudicatário poderá, se assim o desejar, formular reservas à aceitação parcial, apresentando, nos 5 (cinco) dias subsequentes ao conhecimento daquela, reclamação em que se especifique a natureza dos vícios, erros ou faltas e os correspondentes valores a que se ache com direito.
- f) Findo o prazo fixado no número anterior sem que o adjudicatário tenha apresentado reclamação, a Assembleia da República assumirá o silêncio como consentimento, entendendo-se que o(a) adjudicatário(a) aceitará a redução efetuada e exigirá, num prazo de 8 (oito) dias, a substituição da fatura ou o crédito a que houver lugar.
- g) Em caso de desacordo sobre o montante indicado nas faturas, a Assembleia da República efetuará o pagamento relativo ao montante que entende aceitar, sem prejuízo de acerto posterior.
- h) Qualquer atraso no pagamento de faturas não autoriza o(a) adjudicatário(a) a invocar exceção de não cumprimento de qualquer das obrigações que lhe incumbam, salvo nos casos previstos no Código dos Contratos Públicos (CCP).

10 SIGILO E CONFIDENCIALIDADE

- a) O adjudicatário obriga-se a observar o mais estrito sigilo sobre toda a informação e documentação, técnica e não técnica, relacionada com a atividade da AR ou qualquer outra entidade envolvida na execução do contrato.
- b) A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
- c) O adjudicatário compromete-se a respeitar a confidencialidade sobre todos os dados ou informações disponibilizadas pelo adjudicante, bem como pelas informações de carácter pessoal, funcional ou processual dos Sistemas de Informação da Assembleia da República, não os disponibilizando a quaisquer outras entidades, salvo autorização expressa do adjudicante.
- d) 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 de acesso privilegiado.
- e) O adjudicatário garante que terceiros que envolva na execução dos serviços, respeitam as obrigações de sigilo e confidencialidade constantes nos números anteriores.
- f) Caso o adjudicatário ou os seus representantes a quem tenha sido transmitida, no todo ou em parte, informação confidencial fiquem legalmente obrigados a revelar algum elemento constante da mesma,

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

por força da lei, de processo judicial ou a pedido de entidade de regulação ou de fiscalização, compromete-se - e fará com que os seus representantes também se comprometam - a avisar de imediato a entidade adjudicante, previamente à divulgação da informação reservada, de modo a que sejam conjuntamente asseguradas quaisquer providências necessárias para manter, dentro do legalmente permitido, a confidencialidade da informação reservada.

- g) Nenhum aviso, comunicado à imprensa, relatório ou aviso público destinado a fins publicitários ou de referência ao objeto do contrato pode ser realizado pelo prestador de serviços sem aprovação escrita prévia da Assembleia da República.
- h) Para além das ações penais, civis e processos disciplinares que ao caso couber, o adjudicatário pagará à entidade adjudicante uma compensação pela divulgação, seja por que meio for, de factos relativos à Assembleia da República, aos Deputados, funcionários ou outros agentes vinculados à entidade pública contratante, num montante calculado pela seguinte fórmula: $C = RMMG \times 50$, em que: C – Montante da compensação (em euros) e; RMMG – remuneração mínima mensal garantida em vigor.
- i) O disposto no número anterior não é aplicável em caso de imposição legal ou judicial de comunicação de factos sigilosos, desde que sejam cumpridos os estritos termos e objetivos inerentes à obrigação de comunicação.

11 REQUISITOS DE PROTEÇÃO DE DADOS

- a) Será celebrado um contrato de proteção de dados entre a Assembleia da República e adjudicatário que deverá conter as normas constantes das cláusulas seguintes.
- b) No caso de o Adjudicatário necessitar de aceder a dados pessoais, fá-lo-á exclusivamente na medida do estritamente necessário para integral e adequada prossecução dos fins constantes neste caderno de encargos, e por conta e de acordo com as instruções da Assembleia da República, nos termos da legislação aplicável à proteção de dados pessoais.
- c) O Adjudicatário não pode proceder à reprodução, gravação, cópia ou divulgação dos dados pessoais para outros fins que não constem do contrato, comprometendo-se ainda ao seguinte:
 - i. Respeitar integralmente o disposto na legislação nacional e internacional em vigor relativa à proteção de dados pessoais, e em qualquer outra legislação que a substitua ou venha a ser aplicável a esta matéria, nomeadamente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD), e a Lei n.º 58/2019, de 8 de agosto.
 - ii. Cumprir rigorosamente as instruções da Assembleia da República no que diz respeito ao acesso, registo, transmissão ou qualquer outra operação de tratamento de dados pessoais.
 - iii. Tratar os dados pessoais de forma lícita, utilizando-os exclusivamente para as finalidades a que se reporta o Contrato, não podendo ser posteriormente acedidos nem tratados de forma incompatível com tais finalidades.

ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- iv. Implementar as medidas técnicas e organizativas para proteger os dados contra destruição acidental ou ilícita, perda acidental, alterações, difusão ou acesso não autorizados, e contra qualquer outra forma de tratamento ilícito dos mesmos dados pessoais.
 - v. Comunicar de imediato à Assembleia da República quaisquer reclamações ou questões colocadas pelos titulares dos dados pessoais.
 - vi. Apagar e destruir os dados pessoais tratados quando os mesmos deixarem de ser necessários para a execução do contrato, e sempre em prazo não superior a um ano após a cessação do contrato que esteve na base da licitude do seu tratamento.
 - vii. Sem prejuízo do disposto na alínea seguinte, o Adjudicatário obriga-se a manter os dados pessoais estritamente confidenciais, sendo responsável pela confidencialidade e utilização dos mesmos por parte dos respetivos trabalhadores, outros colaboradores ou subcontratados.
 - viii. Se quaisquer dados se perderem ou forem danificados no âmbito da execução do contrato, por causas imputáveis ao Adjudicatário, este compromete-se a adotar as medidas que forem necessárias com vista à recuperação dos dados, sem quaisquer custos adicionais para a Assembleia da República.
- d) O Adjudicatário obriga-se a ressarcir a Assembleia da República por todos os prejuízos em que este venha a incorrer em virtude da utilização ilegal e/ou ilícita dos dados referidos, nomeadamente por indemnizações e despesas em que tenha incorrido na sequência de reclamações ou processos propostos pelos titulares dos dados, bem como por taxas, coimas e multas que tenha de pagar.

12 REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

No âmbito desta prestação de serviços, o adjudicatário obriga-se a cumprir os seguintes requisitos de segurança da informação:

- a) A descrição da informação a ser fornecida/acedida e os métodos para fornecer/aceder a informação;
- b) A classificação da informação fornecida/acedida tem de ser efetuada de acordo com os critérios de classificação de informação estabelecidos na AR;
- c) Os requisitos legais e regulamentares aplicáveis, incluindo a proteção de dados, os direitos de propriedade intelectual, os direitos de autor (copyright) e uma descrição de como vai ser garantido o seu cumprimento;
- d) A obrigação de cada parte contratual de implementar os controlos acordados, incluindo controlos de acesso, avaliação do desempenho, monitorização, gestão de incidentes, e realização de auditorias;
- e) A lista de funcionários do fornecedor autorizados para aceder ou receber informação da AR ou, em alternativa, os procedimentos/condições estabelecidos para autorizar e remover os privilégios de acesso ou receção de informação da AR;
- f) As políticas operacionais de segurança da informação relevantes para o contrato em causa;



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

- g) Os requisitos do Processo de Gestão de Incidentes e Pedidos de Serviço da AR e do Processo de Gestão de Incidentes de Segurança da Informação, com destaque para as responsabilidades de notificação e colaboração durante a resolução de incidentes;
- h) Os requisitos de formação e sensibilização necessários para determinados procedimentos e requisitos de segurança da informação (por exemplo, resposta a incidentes ou procedimentos de autorização);
- i) Os regulamentos relevantes para a subcontratação, incluindo os controlos necessários a implementar;
- j) Os acordos com parceiros relevantes, incluindo a pessoa de contacto para questões relacionadas com segurança da informação;
- k) Os requisitos de rastreio, quando considerado necessário, dos funcionários dos fornecedores, tais como a verificação da sua identidade, a informação pessoal e o registo criminal. Estes requisitos incluem ainda as responsabilidades para conduzir os procedimentos de rastreio e notificação, no caso de o rastreio não ser concluído ou se os resultados levantarem dúvidas ou preocupações;
- l) O direito de auditar os processos e controlos do fornecedor;
- m) Os processos a seguir em caso de disputas contratuais;
- n) A obrigação do fornecedor em providenciar informação sobre incidentes de segurança da informação para revisão da AR;
- o) A obrigação do fornecedor em assegurar a monitorização e revisão dos aspetos de segurança da informação relativos às relações com os seus próprios fornecedores (quando aplicável);
- p) A obrigação do fornecedor em assegurar a continuidade de serviço adequada, através de planos de recuperação de desastres que assegurem os níveis de continuidade dos serviços acordados com a AR, no caso de ocorrência de falhas ou desastres;
- q) A obrigação do fornecedor em apresentar periodicamente relatórios sobre a eficiência dos controlos e as medidas estabelecidas para a correção atempada de questões relevantes suscitadas no relatório;
- r) A obrigação do fornecedor em cumprir com os requisitos de segurança da informação da AR (e.g. proteção contra software malicioso; salvaguarda de dados; procedimentos de recuperação de desastres; controlos criptográficos; gestão de vulnerabilidade; gestão de incidentes de segurança da informação; recolha, manutenção e proteção de evidências, incluindo logs e audit trails; autenticação e controlo de acessos).

13 PENALIDADES

- a) No caso de mora ou cumprimento defeituoso das prestações do contrato por parte do adjudicatário, poderá a Assembleia da República interpelar o adjudicatário para cumprir pontualmente as tarefas



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

contratadas, quando tal ainda for possível e se mantenha o interesse na prestação, devendo nesse caso o adjudicatário dar-lhes cumprimento imediato, bem como suportar todos os danos que a Assembleia da República sofra na sequência de tais factos.

- b) Sem prejuízo do disposto no número anterior, e da obrigação de indemnizar por parte do adjudicatário, poderá a Assembleia, aplicar-lhe as seguintes penalidades:
- Pelo atraso no cumprimento do prazo previsto na proposta para efeitos de prestação da totalidade dos serviços objeto do presente procedimento – 5% (por cem) do preço contratual por cada 10 dias de atraso;
 - No caso de incumprimento pelo adjudicatário de outras obrigações decorrentes do presente CE, serão aplicadas as seguintes penalidades diárias por cada prestação em falta de acordo com a seguinte fórmula:

$$“P= V \times A/500 ”$$

em que “P” corresponde à penalidade, “V” ao preço total do contrato e “A” o número de dias em atraso no cumprimento integral e satisfatório da prestação.

- c) A aplicação de penalidades pela entidade adjudicante nos termos previstos nos números anteriores, deverá ser precedida de comunicação endereçada ao adjudicatário, onde será feita menção à intenção de aplicação de penalidades, o seu valor, o respetivo fundamento e a indicação de que o mesmo dispõe de um prazo de 10 (dez) dias úteis para efeitos de exercício do seu direito de audiência prévia. 5. Decorrido o prazo de audiência prévia, deverá a entidade adjudicante comunicar ao adjudicatário se mantém, ou não, a aplicação das penalidades, e em caso afirmativo, conceder-lhe um prazo não inferior a 5 (cinco) dias úteis para levar a cabo o respetivo pagamento.
- d) A aplicação das sanções acima referidas será efetivada a critério da entidade adjudicante, designadamente por desconto no pagamento ou pagamentos subsequentes à verificação do facto que tenha dado origem à penalidade.
- e) As penalidades previstas na presente cláusula não afastam o direito da entidade adjudicante de ser indemnizada, nos termos gerais, quando se verificarem os fundamentos de facto e de direito para o efeito.
- f) O não cumprimento de cláusulas do contrato, quando a sua gravidade o justifique pelos prejuízos acusados à Assembleia da República, poderá constituir fundamento para resolução imediata do contrato, nos termos legalmente aplicáveis.
- g) Na determinação da gravidade do incumprimento a Assembleia da República tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do Adjudicatário e as consequências do incumprimento.
- h) O valor acumulado das sanções pecuniárias não pode exceder 20% do preço contratual, nos termos do nº 2 do artigo 329º, do C.C.P.

14 GESTOR DO CONTRATO

O contraente público nos termos do artigo 290º-A do CCP designará um gestor do contrato, com a função de acompanhar permanentemente a execução deste.

15 CASOS FORTUITOS OU DE FORÇA MAIOR

- a) Nenhuma das partes pode ser responsável pelo incumprimento ou pelo cumprimento defeituoso das obrigações emergentes do contrato, na estrita medida em que se verifiquem em casos de força maior, sendo considerados casos de força maior as circunstâncias que impossibilitam o cumprimento das obrigações emergentes do contrato, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar, como seja, a título de exemplo, a emergência de um surto epidemiológico.
- b) 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.
- c) Quando uma das partes não aceite por escrito que certa ocorrência invocada pela outra constitua força maior, cabe a esta fazer prova do mesmo.
- d) A verificação de uma situação de força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas, pelo período de tempo comprovadamente correspondente ao impedimento resultante de força maior.
- e) Caso a impossibilidade de execução do contrato, em resultado de força maior, se prolongue por um período contínuo superior a um mês, qualquer das partes pode proceder à respetiva resolução, mediante comunicação enviada à outra parte, com pelo menos 5 (cinco) dias de antecedência.

16 PATENTES, LICENÇAS E MARCAS

- a) São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, na prestação de serviços, de marcas registadas, patentes registadas ou licenças.
- b) Caso a entidade adjudicante venha a ser demandada por ter infringido, na execução do contrato, qualquer dos direitos mencionados no ponto anterior, o adjudicatário indemniza-a de todas as despesas que, em consequência haja lugar e de todas as quantias que tenha que pagar, seja a que título for.



ADMINISTRAÇÃO DE SEGURANÇA DA INFORMAÇÃO

17 CESSÃO DA POSIÇÃO CONTRATUAL E SUBCONTRATAÇÃO

- a) O adjudicatário não pode ceder a terceiros, total ou parcialmente, a sua posição contratual, ou qualquer dos direitos e obrigações decorrentes do contrato, nomeadamente subcontratar, sem autorização prévia da entidade adjudicante.
- b) Para efeitos de obtenção da *suprarreferida* autorização, deverá o adjudicatário observar o previsto sobre esta matéria no artigo 318.º do Código dos Contratos Públicos.

18 RESOLUÇÃO DO CONTRATO

- a) A entidade adjudicante reserva-se ao direito de resolver o contrato em caso de incumprimento definitivo pelo adjudicatário das suas obrigações contratuais, nos termos do disposto na parte final do n.º 1 do artigo 325.º e ainda do disposto nos artigos 334.º, 335.º e 448.º do Código dos Contratos Públicos.
- b) Em tais circunstâncias a entidade adjudicante comunicará por escrito ao adjudicatário as deficiências do serviço, fixando um prazo para a sua regularização, findo o qual, se as anomalias não tiverem sido totalmente corrigidas, terá lugar a resolução do contrato que será comunicada ao adjudicatário mediante carta registada com aviso de receção, na qual serão indicadas as razões que a entidade adjudicante considera justificativas da resolução.
- c) Sem prejuízo da resolução do contrato nos termos previstos nos pontos anteriores, a entidade adjudicante mantém o direito ao pagamento das indemnizações e penalidades aplicáveis nos termos do presente caderno de encargos ou de qualquer disposição legal vigente.

19 GARANTIA

O adjudicatário garantirá, sem qualquer encargo para a entidade adjudicante, os serviços prestados, contra quaisquer defeitos ou discrepâncias com as exigências legais e com as características, especificações e requisitos técnicos definidos no presente Caderno de Encargos.

20 LEGISLAÇÃO APLICÁVEL

Em tudo o que o presente caderno de encargos for omissivo observar-se-á o disposto no C.C.P., aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro, com a redação decorrente da entrada em vigor do Decreto-Lei n.º 111-B/2017, de 31 de agosto e na sua redação atual, demais legislação aplicável e, em qualquer caso, sempre a Lei portuguesa.