

CONCURSO PÚBLICO

AQUISIÇÃO DE SERVIÇOS SOC - SECURITY OPERATIONS CENTER

Processo nº (22/2023)

CADERNO DE ENCARGOS

PARTE I
CLÁUSULAS JURÍDICAS

CAPÍTULO I

DISPOSIÇÕES GERAIS

Cláusula 1ª

Definições e acrónimos

1. Para efeitos do presente Caderno de Encargos e respetivos anexos, os termos referidos nas alíneas seguintes têm o sentido que aí lhes é atribuído:
 - a) **ADJUDICATÁRIO**: concorrente ao qual é adjudicada a proposta; utilizado neste Caderno de Encargos no mesmo sentido, de **COCONTRATANTE**.
 - b) **ARRANQUE DO PROJETO** – Momento em que o **COCONTRATANTE** inicia a prestação do Serviço, nomeadamente, a etapa de “Preparação”;
 - c) **ATIVIDADE**: Unidade mínima necessária para a execução de uma tarefa definida no *workflow*;
 - d) **CADERNO DE ENCARGOS**: O presente documento;
 - e) **COCONTRATANTE**: O operador económico com o qual seja celebrado o contrato ao abrigo do presente concurso; utilizado, no presente documento, com o mesmo sentido de **ADJUDICATÁRIO**;
 - f) **CONTRAENTE PÚBLICO** ou **AGÊNCIA, I.P.** - A Agência para o Desenvolvimento e Coesão, I.P., entidade com a qual será celebrado o **CONTRATO** para a prestação dos serviços no âmbito do presente procedimento;
 - g) **CONTRATO**: O contrato de aquisição dos serviços a celebrar de acordo com as cláusulas jurídicas e técnicas constantes do **CADERNO DE ENCARGOS** e das demais peças do procedimento;
 - h) **DOCUMENTO**: O documento corresponde ao registo, qualquer que seja a sua data, forma ou suporte material, que contém uma informação e é produzido ou recebido por uma entidade pública ou privada no exercício da sua atividade;
 - i) **EVENTO OU EVENTO DE SEGURANÇA**: Corresponde a uma alteração no funcionamento da rede ou do sistema de informação indicando que uma política de segurança pode ter sido violada ou que ocorreu uma falha nos mecanismos de proteção;
 - j) **GESTOR DE CONTRATO**: Elemento da **ENTIDADE ADJUDICANTE** nomeado para

desempenhar as funções previstas no Artigo 290.º -A do CCP;

- k) *INCIDENTE DE SEGURANÇA*: Corresponde a um *EVENTO DE SEGURANÇA* que constitui uma ameaça e que compromete a segurança ou privacidade dos seus constituintes;
 - l) *NÍVEIS DE SERVIÇO* – Conjunto de metas a cumprir na prestação do SERVIÇO, face a vários parâmetros / indicadores estabelecidos no CADERNO DE ENCARGOS; o mesmo que SLA;
 - m) *PROCESSO*: Sequência de atividades ou fluxos de trabalho (*workflows*) interligados que transformam um conjunto de entradas em resultados. Os processos são normalmente transversais no sentido em que atravessam várias áreas da organização. Os processos podem ser considerados como sendo de negócio – focados na atividade central da organização – ou de suporte – focados em atividades que apoiam a execução da atividade central da organização;
 - n) *PROPOSTA*: A proposta adjudicada;
 - o) *SERVIÇO* – Designação genérica do conjunto de serviços a prestar pelo COCONTRATANTE expressamente identificados no CADERNO DE ENCARGOS ou necessários para o cumprimento das suas obrigações ao abrigo do CONTRATO;
2. Para efeitos do presente documento e respetivos Anexos, os acrónimos referidos na lista seguinte têm o sentido que aí lhes é atribuído:
- a) API – Application Programming Interface, conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma baseado na Web;
 - b) CCP – Código dos Contratos Públicos, aprovado pelo Decreto-Lei nº 18/2008, de 29 de janeiro, com a redação resultante do Anexo iii ao Decreto-Lei nº 111-B/2017, de 31 de agosto e as alterações introduzidas pelas Retificações nº 36-A/2017, de 31 de outubro e 42/2017, de 30 de novembro, pelos Decretos-Lei nºs 33/2018, de 15 de maio, 170/2019, de 04 de dezembro, pela Resolução da AR nº 16/2020, de 19 de março, pela Lei nº 30/2021, de 21 de maio e pela Retificação nº 25/2021, de 21 de julho;
 - c) CSIRT – Computer Security Incident Response Team (Equipa de Resposta a *INCIDENTES DE SEGURANÇA* de Computadores), é uma equipa especializada em segurança informática que tem como objetivo tratar de uma forma eficiente todas as situações perigosas que ocorrem em sistemas de computadores; FEEI - Fundos Europeus Estruturais e de Investimento, instrumentos de financiamento aprovados por legislação da União Europeia que suportam ações europeias, nacionais, regionais, locais e até internacionais, para atingir objetivos de desenvolvimento;
 - d) IOC - *Indicators of Compromise*, indicadores que permitem relacionar qualquer atividade suspeita com indicadores recentes;
 - e) ITIL – *Information Technology Infrastructure Library*, modelo para gestão de serviço que documenta as melhores práticas para o suporte, operação e entrega de serviços TIC;

- f) KPI – *Key Performance Indicators* ou indicadores fundamentais para avaliação e análise do desempenho e da qualidade dos serviços prestados;
- g) MS – Microsoft;
- h) PC – *Personal Computer* ou computador pessoal;
- i) SI/TI – Sistemas de Informação e Tecnologias de Informação;
- j) SIEM – *Security Information and Event Management*, resulta da combinação do SEM (Security Event Manager - Gestão de *EVENTOS DE SEGURANÇA*) e SIM (Security Information Management - Gestão de Informações de Segurança) permitindo analisar em tempo real alertas de segurança, gerir logs, obter uma visão ampla das atividades no ambiente de IT, etc.;
- k) SLA – *Service Level Agreement*, o mesmo que Níveis de Serviço.
- l) SOAR – *Security Orchestration, Automation and, Response*, conjunto de soluções de softwares compatíveis que permitem que uma organização recolha dados sobre ameaças de segurança de várias fontes, de forma a responder a ocorrências que condicionem a segurança, melhorando a eficiência das operações digitais;
- m) SOC – *Security Operations Center*, Centro de Operações de Segurança centralizado para monitorização da segurança da informação de uma organização.

Cláusula 2ª

Objeto

O presente caderno de encargos compreende as cláusulas a inserir no contrato a celebrar na sequência do procedimento pré-contratual, ao abrigo da alínea b) do n.º 1 do artigo 20.º do CCP, que tem por objeto a aquisição de serviços SOC – Security Operations Center para a Agência, I.P., de acordo com as especificações técnicas descritas na parte II do presente Caderno de Encargos e a que corresponde o Processo n.º 22/2023.

Cláusula 3ª

Prevalência

1. O presente caderno de encargos contempla as cláusulas a incluir no contrato que se pretende celebrar.
2. O contrato integra os seguintes elementos:
 - a) Os suprimentos dos erros e das omissões do caderno de encargos identificados pelos concorrentes e expressamente aceites pelo órgão competente para a decisão de contratar, nos termos do disposto no artigo 50.º do Código dos Contratos Públicos;

- b) Os esclarecimentos e as retificações relativos ao caderno de encargos;
 - c) O presente caderno de encargos e os seus anexos;
 - d) A proposta;
 - e) Os esclarecimentos sobre a proposta prestados pelo COCONTRATANTE;
 - f) O clausulado contratual.
2. Sem prejuízo do disposto no número seguinte, em caso de divergência entre os vários documentos que integram o contrato, a prevalência é determinada pela ordem por que vêm enunciados no número anterior.
3. Os ajustamentos propostos pelo CONTRAENTE PÚBLICO nos termos previstos no artigo 99.º do Código dos Contratos Públicos e aceites pelo COCONTRATANTE nos termos previstos no artigo 101.º do mesmo Código prevalecem sobre todos os documentos previstos no n.º 1 da presente cláusula.

Cláusula 4ª

Poder de conformação da prestação pelo Contraente Público

1. Sem prejuízo da autonomia do Cocontratante, dentro dos limites e termos do CE, e da Proposta adjudicada, o Cocontratante aceita expressamente os poderes do Contraente Público, nos termos dos artigos 302.º e seguintes do CCP e demais legislação em vigor, de definição e conformação dos serviços a prestar, com vista a atingir os objetivos globais do projeto a implementar.
2. O poder de conformação a que se refere o número anterior não prejudica nem diminui os deveres do Cocontratante de afetação dos recursos e desenvolvimento dos serviços desenvolvendo todos os esforços para atingir os objetivos do Contrato.

Cláusula 5ª

Vigência

O contrato terá início na data da sua assinatura, que previsivelmente ocorrerá em março de 2023, e terá a duração de 30 meses, sem prejuízo das obrigações acessórias, que perduram para além da cessação do contrato.

Cláusula 6ª

Local de prestação dos serviços

A prestação dos serviços tem lugar nas instalações do COCONTRATANTE ou da Agência, I.P., conforme se mostre mais adequado para o desenvolvimento, em cada momento, dos serviços a prestar, a acordar na fase de preparação da execução do contrato.

CAPÍTULO II

OBRIGAÇÕES DAS PARTES

SECÇÃO I

OBRIGAÇÕES DO COCONTRATANTE

Cláusula 7.ª

Obrigações do Cocontratante

1. Sem prejuízo de outras obrigações previstas na legislação aplicável e no presente Caderno de Encargos e respetivos anexos, constituem obrigações principais do Cocontratante as seguintes:
 - a) Preparar, planear e coordenar a execução de todos os serviços necessários e adequados à melhor execução do contrato, em conformidade com as Especificações Técnicas previstas no presente Caderno de Encargos, e de acordo com a respetiva proposta e em articulação com a Agência, I.P., bem como de todas as obrigações daí decorrentes;
 - b) Participar nas reuniões de preparação, de acompanhamento ou esclarecimento convocadas para o efeito pela Agência, I.P., com a presença obrigatória do gestor de projeto afeto à prestação de serviços;
 - c) Prestar os serviços nos termos por si propostos e em cumprimento integral, adequado e atempado de acordo com o previsto no presente caderno de encargos;
 - d) Cumprir as normas legais em vigor, designadamente no que diz respeito às obrigações no domínio laboral;
 - e) Comunicar, de imediato, ao CONTRAENTE PÚBLICO quaisquer factos que tornem total ou parcialmente impossível a prestação dos serviços contratada, ou o cumprimento de qualquer outra das suas obrigações.;

- f) Não alterar as condições de prestação dos serviços fora dos casos previstos no presente CE;
 - g) Desenvolver todas as diligências a praticar todos os atos junto do CONTRAENTE PÚBLICO, de forma a garantir a correta e adequada implementação dos serviços contratados;
 - h) Prestar de forma correta e fidedigna todas as informações referentes às condições em que é efetuada a prestação dos serviços, bem como prestar todos os esclarecimentos que se revelem necessários ou sejam solicitados pelo CONTRAENTE PÚBLICO;
 - i) Comunicar ao CONTRAENTE PÚBLICO qualquer alteração da denominação social, dos representantes legais, dos estatutos, dos gerentes, ou outras com relevância para a prestação dos serviços, designadamente, mas não de modo exclusivo, a apresentação à insolvência.
 - j) Cumprir com o disposto no artigo 419.º-A do CCP, por força da norma constante do n.º 13 do artigo 42.º do CCP, na redação concedida pelo Decreto-Lei n.º 78/2022, de 7 de novembro, se aplicável.
2. O Cocontratante fica ainda obrigado a recorrer a todos os meios humanos, materiais e informáticos 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.

Cláusula 8ª

Número e perfil dos colaboradores do Cocontratante

1. A prestação dos serviços deve ser executada por uma equipa, a definir pelo COCONTRATANTE tendo em vista a adequação à melhor execução do contrato, de acordo com a definição do número de elementos e dos perfis mínimos obrigatórios e respetivas características descritas na Parte II do CE.
2. Sem prejuízo do disposto na Parte II do CE relativamente aos requisitos da equipa, compete ao Cocontratante a alocação dos diferentes membros da equipa proposta para a adequada e tempestiva execução da prestação dos serviços, que constituem uma obrigação de resultado.
3. Compete ao COCONTRATANTE alocar os recursos humanos necessários para garantir a prestação dos serviços contratados e assegurar a máxima adequação das competências de cada um deles à realização das ações compreendidas nas áreas de conhecimento

identificadas no presente caderno de encargos, sem prejuízo do cumprimento do adicionalmente exigido nas especificações técnicas do caderno de encargos.

Cláusula 9ª

Substituição dos colaboradores que integram a proposta adjudicada

1. O Cocontratante poderá substituir qualquer colaborador afeto à prestação dos serviços contratados por colaborador com *curriculum* idêntico, ou superior, desde que o solicite ao Contraente Público com a antecedência mínima de 5 dias úteis, devendo, para o efeito, juntar os documentos necessários para comprovação dos requisitos de equivalência ao colaborador a substituir, e garantir, salvo situações excecionais, que a saída do colaborador substituído só ocorre após o novo colaborador estar em condições de assegurar a continuidade das atividades que o colaborador substituído se encontrava a desenvolver.
2. Nos casos previstos nos números anteriores é da responsabilidade e encargo exclusivos do Cocontratante a prévia transmissão de conhecimento necessária para que o novo colaborador possa dar continuidade às atividades que o colaborador substituído estava a desenvolver.
3. O Cocontratante não poderá substituir mais do que um elemento da equipa por mês.
4. Ao CONTRAENTE PÚBLICO assiste o direito de exigir do COCONTRATANTE a substituição de quaisquer colaboradores deste, caso se verifique que a respetiva prestação não é satisfatória.
5. O COCONTRATANTE deverá assegurar a substituição dos colaboradores referidos no número anterior no prazo máximo de 5 dias após a notificação do CONTRAENTE PÚBLICO para esse efeito, devendo juntar igualmente os documentos necessários para comprovação dos requisitos de experiência idênticos ou superiores ao do colaborador substituído.
6. O direito a que se refere o nº 4 não preclude nenhum dos deveres previstos no presente CE para o Cocontratante.

Cláusula 10.ª

Transferência da propriedade e direitos de propriedade intelectual

1. Os produtos que resultem da execução do objeto do contrato, designadamente o resultado dos serviços de desenvolvimento aplicacional, bem como todos os resultados dos serviços prestados ao abrigo da bolsa de horas, serão considerados como obra de encomenda, nos

- termos do disposto do Código do Direito de Autor e dos Direitos Conexos, pertencendo à Agência, I.P. a titularidade dos mesmos, bem como a propriedade dos respetivos suportes.
2. A Agência, I.P. poderá, para seu uso exclusivo, proceder à reprodução de todos os produtos referidos no número anterior, bem como manuais e qualquer documentação elaborada e fornecida ao abrigo do presente contrato.
 3. O Cocontratante não pode utilizar a favor de outras entidades, ainda que públicas, nem divulgar quaisquer elementos elaborados ao abrigo do presente contrato, salvo autorização prévia expressa por escrito da Agência, I.P..
 4. A titularidade dos direitos de propriedade intelectual sobre quaisquer obras e materiais desenvolvidos, criados, modificados ou personalizados pelo Cocontratante para o Contraente Público ou pelo Contraente Público ao abrigo do Contrato, incluindo nomeadamente, escritos, relatórios, esquemas, desenhos, imagens, fotografias, especificações, parametrizações, dados em formato eletrónico e tabulações, inquéritos e questionários, invenções, inovações técnicas, know-how, processos, técnicas, métodos de investigação, documentos ou quaisquer outras criações, de qualquer natureza ou meio, (em conjunto “obras”) pertence ao Contraente Público, ao abrigo do regime da obra por encomenda e como tal cabendo exclusivamente a este todos os direitos de propriedade intelectual a elas inerentes, considerando-se contrapartida suficiente para tal a remuneração adjudicada.
 5. O Cocontratante garante que todos os seus colaboradores afetos à prestação de serviços, independentemente do vínculo jurídico que possuam com o Cocontratante, foram atempadamente informados e aceitaram que os direitos de propriedade intelectual sobre as obras acima indicadas pertencem exclusivamente ao Contraente Público.
 6. O Cocontratante é responsável pela infração de quaisquer direitos de patente, de conceção, de licenças, de projetos, de marcas, de nomes, ou de quaisquer outros direitos de propriedade intelectual, industrial ou afins, respeitantes aos bens e aos serviços objeto do Contrato, nomeadamente, projetos, estudos, programas informáticos, equipamento, materiais, documentação ou trabalhos realizados.
 7. O Cocontratante é responsável por qualquer reclamação formulada perante o Contraente Público, resultante de violação dos direitos referidos nos números anteriores, adotando o Contraente Público o procedimento que se revele mais adequado para a intervenção plena do Cocontratante na discussão e no esclarecimento, perante terceiros reclamantes ou quaisquer autoridades, das dúvidas que, neste âmbito, se coloquem.

8. No caso de o Contraente Público ser demandado por violação de direitos constantes dos números anteriores, o Cocontratante indeniza-o por todas as despesas que, em consequência, deva suportar e por todas as quantias que tenha de pagar, seja a que título for.
9. Com a aceitação dos serviços objeto do presente CONTRATO, ocorre a transferência da propriedade dos mesmos para o CONTRAENTE PÚBLICO, bem como de todos os documentos elaborados pelo COCONTRATANTE previstos neste CE, podendo o CONTRAENTE PÚBLICO utilizá-los, reproduzi-los, alterá-los e cedê-los livremente, sem quaisquer restrições e sem necessidade de autorização do COCONTRATANTE.

Cláusula 11.ª

Patentes, licenças e marcas registadas

1. São da responsabilidade do Cocontratante quaisquer encargos decorrentes da utilização de marcas registadas, patentes registadas ou licenças.
2. Caso a Agência, I.P. venha a ser demandada por ter infringido, na execução do contrato a celebrar, qualquer dos direitos mencionados no número anterior, o Cocontratante indeniza-a de todas as despesas que, em consequência, haja de fazer e de todas as quantias que tenha de pagar seja a que título for.

Cláusula 12.ª

Dever de sigilo

1. O Cocontratante obriga-se a não divulgar quaisquer informações e documentação, técnica e não técnica, comercial ou outra, relativa à Agência, I.P., de que venha a ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. Nenhum documento ou dado a que o COCONTRATANTE tenha acesso, direto ou indiretamente, no âmbito do contrato poderá ser reproduzido sem autorização expressa escrita do CONTRAENTE PÚBLICO.
3. O Cocontratante obriga-se também a não utilizar as informações obtidas para fins alheios à execução do contrato.
4. O Cocontratante obriga-se a remover e destruir no termo final do prazo contratual todo e qualquer registo, em papel ou eletrónico, que contenha dados ou informações referentes ou obtidas na execução do contrato.

5. O COCONTRATANTE garantirá o sigilo absoluto quanto a todas as informações de que, no âmbito do contrato, os seus colaboradores, independentemente do título a que prestem serviços, venham a ter conhecimento, relativo a todo o tipo de funções, atividades, processos, documentos, regras e procedimentos internos designadamente, os dados relativos a processos e outro expediente, seja qual for a sua natureza, e toda a informação constante das bases de dados ou ficheiros a que tenham que aceder para cumprimento dos serviços a prestar.
6. O dever de sigilo mantém-se em vigor após a extinção das obrigações decorrentes do contrato, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

Cláusula 13.^a

Proteção de dados pessoais

1. A atividade desenvolvida pelo COCONTRATANTE e respetivos colaboradores, independentemente da natureza da relação contratual que com eles possua, encontra-se sujeita ao disposto no Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, (Regulamento Geral sobre a Proteção de Dados), bem como na Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do referido Regulamento.
2. O COCONTRATANTE assume a qualidade de subcontratante no que diz respeito ao tratamento dos dados pessoais objeto do contrato, em que o CONTRAENTE PÚBLICO assuma a qualidade de entidade responsável pelo tratamento.
3. O COCONTRATANTE obriga-se a executar o objeto do contrato de acordo com o princípio do *Privacy by Design* e do *Privacy by Default* (se aplicável), fazendo constar esta obrigação e a metodologia e processos definidos nos Relatórios técnicos dos serviços prestados, previstos no presente caderno de encargos.
4. O COCONTRATANTE obriga-se, ainda, enquanto subcontratante, ao cumprimento de todos os deveres e obrigações que impendem sobre o CONTRAENTE PÚBLICO, enquanto entidade responsável pelo tratamento de dados pessoais objeto do contrato a celebrar, comprometendo-se designadamente a:

- a) Utilizar os dados pessoais a que tenha acesso ou que lhe tenham sido transmitidos pelo Contraente Público, única e exclusivamente para efeitos da prestação de serviços objeto do contrato a celebrar.
 - b) Não copiar, reproduzir, adaptar, modificar, alterar, apagar, destruir, difundir, transmitir, divulgar ou por qualquer outra forma colocar à disposição de terceiros os dados pessoais a que tenha acesso, ou que lhe sejam transmitidos pelo Contraente Público, sem que, tenha sido por esta, expressamente instruído por escrito.
 - c) Comunicar de imediato qualquer situação que possa afetar o tratamento dos dados em causa, ou que de algum modo possa dar origem ao incumprimento das disposições legais em matéria de proteção de dados pessoais;
 - d) Assegurar que os trabalhadores temporários e os seus colaboradores (incluindo representantes legais, trabalhadores, prestadores de serviços, procuradores e consultores, independentemente da natureza e validade do vínculo jurídico estabelecido com o cocontratante e o referido colaborador) cumprem todas as obrigações previstas na presente cláusula;
 - e) Assegurar a confidencialidade dos dados pessoais recolhidos, sem prejuízo de respeito com obrigações legais, nomeadamente a entidades policiais, judiciais, fiscais e reguladoras.
 - f) Colaborar com o DPO (*Data Protection Officer* – Encarregado de Proteção de Dados) do CONTRAENTE PÚBLICO, facultando todas as informações e esclarecimentos que este vier a solicitar no âmbito das suas funções.
5. As partes ficam desde já autorizadas a comunicar o conteúdo do contrato a celebrar, bem como os elementos com eles relacionados, à Comissão Nacional de Proteção de Dados.
6. Em observância pelo Regulamento Geral sobre a Proteção de Dados, os *curricula* e/ou outros documentos nos quais constem dados pessoais, deverão vir acompanhados do consentimento expresso dos seus titulares, para que o Contraente Público, no âmbito exclusivo do procedimento de contratação pública em apreço, fique habilitada para o tratamento desses dados.
7. Uma vez atingida a finalidade prevista do número anterior, incluindo monitorização do contrato a celebrar e auditorias decorrentes do procedimento, os dados pessoais serão eliminados, no respeito pelo Regulamento Geral sobre a Proteção de Dados.
8. O encarregado da proteção dos dados da Agência, I.P. é a colaboradora Ana Paula Duarte, com o e-mail: protecao.dados@adcoesao.pt, para o qual deverão ser remetidas quaisquer

questões, sem prejuízo do direito de as apresentar também à entidade reguladora, a Comissão Nacional de Proteção de Dados.

9. O incumprimento de algum dos deveres constantes na presente cláusula, bem como a verificação da inexistência de garantias de *compliance*, constitui fundamento de resolução do contrato por incumprimento, sem prejuízo do dever de indemnização ao responsável pelo tratamento a que possa haver lugar, por danos sofridos ou eventuais violações que lhe sejam imputadas.

Cláusula 14.^a

Conflito de interesses

Em caso de conflito de interesses, superveniente, durante a execução dos serviços contratados, o Cocontratante deverá informar, no prazo de 48 (quarenta e oito) horas, da ocorrência do facto e dos procedimentos que adotará para a resolução do conflito, sujeitos à aprovação da Agência, I.P.

SECÇÃO II

OBRIGAÇÕES DA AGÊNCIA. I.P.

Cláusula 15.^a

Preço base e preço contratual

1. O preço base fixado para o presente procedimento, que constitui o encargo máximo a pagar pela execução da prestação de serviços que constitui objeto do contrato a celebrar, é de **€ 212.490,00 € (duzentos e doze mil quatrocentos e noventa euros)**, a que acresce o IVA à taxa legal em vigor, se este for legalmente devido.
2. O preço a pagar pela prestação dos serviços, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, abrange todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente cometida à Agência, I.P., incluindo despesas de alojamento, alimentação, deslocação de meios humanos, despesas de transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças que, para execução do contrato, sejam da responsabilidade do Cocontratante.
3. Não há lugar a revisão de preços durante o prazo de vigência do contrato.

4. Nos termos do disposto no n.º 3 do artigo 47.º do CCP, o preço base foi fixado tendo em consideração uma consulta informal ao mercado nos termos e para os efeitos do artigo 35.º-A do CCP.

okCláusula 16.ª

Condições de pagamento

1. O COCONTRATANTE obriga-se a apresentar uma fatura, mensalmente, em função dos serviços prestados e objeto de aceitação provisória, relativamente às unidades de entrega no âmbito da contratação de capacidade, e de acordo com o aprovado pela Agência, I.P., acompanhada do correspondente Relatório de Serviços prestados, identificando o número de horas utilizadas, por perfil, sob pena de devolução.
2. No âmbito do desenvolvimento aplicacional, serão feitos os seguintes pagamentos:
 - a) Com a aceitação do *setup* do serviço – 6% do valor do contrato;
 - b) Pelos 3 serviços de *External Security Assessment* com *Penetration Testing* - 24% do valor do contrato. O pagamento é efetuado pela realização de cada serviço;
 - c) Os restantes 70% do valor do contrato serão pagos mensalmente, na sequência da aceitação dos entregáveis definidos no CE.
3. As percentagens a que se refere o número anterior são apuradas por referência ao valor global definido na proposta adjudicada.
4. A faturação deve respeitar o regime estabelecido na Parte II do CE relativamente aos abatimentos a que haja lugar, por incumprimento dos Níveis de Serviço.
5. Em caso algum poderão ser pagos adiantamentos.
6. As quantias devidas pela Agência, I.P. devem ser pagas no prazo de 30 (trinta) dias após a receção das respetivas faturas, as quais só podem ser emitidas após o vencimento da obrigação respetiva.
7. Consideram-se vencidas as obrigações com a aceitação dos serviços prestados a que as mesmas correspondem.
8. A emissão das faturas pelo Cocontratante deve observar o disposto no artigo 9.º Decreto-Lei nº 111-B/2017, de 31 de agosto, com a redação conferida pelo artigo 3º do Decreto-Lei nº 104/2021, de 27 de novembro.
9. As faturas têm de conter obrigatoriamente a indicação do número de compromisso, para efeitos de cumprimento da Lei sobre os Compromissos e Pagamentos em Atraso, sob pena de devolução.
10. Em caso de discordância por parte da Agência, I.P. quanto aos valores indicados nas faturas,

deve este comunicar, por escrito, ao Cocontratante, os respetivos fundamentos, ficando o Cocontratante obrigado a prestar os esclarecimentos necessários ou a proceder à emissão de nova fatura corrigida.

11. Desde que devidamente emitidas, as faturas são pagas através de transferência bancária para a instituição de crédito indicada pelo Cocontratante e da qual este deve ser titular.
12. O atraso no pagamento das faturas apresentadas fará a Agência, I.P. incorrer em mora com a correspondente aplicação do artigo 1.º da Lei nº 3/2010, de 27 de abril, sobre o montante em dívida, à taxa legalmente fixada para o efeito, desde o respetivo vencimento até integral e efetivo pagamento.
13. O atraso no pagamento de quaisquer faturas regularmente emitidas não autoriza o COCONTRATANTE a invocar a exceção de não cumprimento de qualquer das obrigações que lhe incumbem por força do contrato, salvo nos casos previstos no artigo 327.º do Código dos Contratos Públicos.

SECÇÃO III

ACOMPANHAMENTO E FISCALIZAÇÃO DA EXECUÇÃO DO CONTRATO

Cláusula 17.ª

Acompanhamento e fiscalização do modo de execução do contrato

1. Sem prejuízo das competências exercidas pelos demais membros da equipa da Agência, I.P., a execução do contrato é acompanhada pelo gestor do contrato, António Miguéns, da Unidade de Sistemas de Informação, designado pela Agência, I.P. nos termos e para os efeitos previstos no artigo 290.º-A do CCP.
2. O desempenho das funções de acompanhamento e fiscalização do modo de execução do contrato não exime o Cocontratante de responsabilidade por qualquer incumprimento ou cumprimento defeituoso das suas obrigações.

CAPÍTULO III

MODIFICAÇÃO, INCUMPRIMENTO E EXTINÇÃO DO CONTRATO

Cláusula 18.^a

Cessão da posição contratual e subcontratação

1. Sem prejuízo do disposto na alínea a) do n.º 1 do artigo 318.º do Código dos Contratos Públicos, o COCONTRATANTE pode ceder a sua posição contratual, na fase de execução do contrato, mediante autorização do Contraente Público.
2. Para efeitos da autorização prevista no número anterior, o COCONTRATANTE deve apresentar uma proposta fundamentada e instruída com os documentos previstos no n.º 2 do artigo 318.º do Código dos Contratos Públicos.
3. O CONTRAENTE PÚBLICO deve pronunciar-se sobre a proposta do COCONTRATANTE no prazo de 5 (cinco) dias a contar da respetiva apresentação, desde que regularmente instruída, considerando-se o referido pedido rejeitado se, no termo desse prazo, o mesmo não se pronunciar expressamente.
4. Em caso de incumprimento pelo COCONTRATANTE que reúna os pressupostos para a resolução do contrato, este cederá a sua posição contratual ao concorrente do procedimento pré-contratual que antecedeu a celebração do contrato que venha a ser indicado pelo CONTRAENTE PÚBLICO, de acordo com o estabelecido no artigo 318.º-A do Código dos Contratos Públicos.
5. A cessão da posição contratual a que se refere o número anterior opera por mero efeito do ato do CONTRAENTE PÚBLICO, sendo eficaz a partir da data por este indicada.
6. Aplica-se à subcontratação o regime constante do Código dos Contratos Públicos, nos termos do disposto nos artigos 316.º e seguintes, não podendo ser objeto de subcontratação mais do que 20% (vinte por cento) do contrato.

Cláusula 19.^a

Penalidades

1. Sem prejuízo da aplicação de outras sanções previstas no presente Caderno de Encargos, pelo incumprimento de obrigações emergentes do contrato, a Agência, I.P. pode aplicar ao Cocontratante as seguintes penalidades:
 - a) No valor de €1.000,00 (mil euros) pela falta, sem justificação atempada e por motivo ponderoso, do gestor do projeto a qualquer reunião agendada para a qual deva estar

presente;

- b) 2% (dois por cento) do preço contratual por cada incumprimento de uma das tarefas de monitorização contínua de eventos, tal como previstas no nº 2.1.3.1 da Parte II do presente Caderno de Encargos.
- c) 1% (um por cento) do preço contratual por cada substituição de elementos da equipa em violação do disposto no Caderno de Encargos;
- d) 1% (um por cento) do preço contratual por cada violação das atividades de gestão e administração das plataformas tecnológicas identificadas no nº 2.1.3.2 da Parte II do Caderno de Encargos;
- e) 5% (cinco por cento) do preço contratual pela não realização, atempada e nos termos previstos no nº 2.2 da Parte II do Caderno de Encargos, de qualquer dos *External Security Assessment com penetration teststing*;
- f) 1 % (um por cento) do preço contratual, por cada não entrega atempada e completa de qualquer dos entregáveis referidos no nº 2.1.2 da Parte II do Caderno de Encargos.
- g) Pelo incumprimento das datas e prazos de entrega dos serviços e documentação solicitados, será aplicada uma penalidade diária calculada nos seguintes termos:

$$P = V \times A/Y$$

Em que:

P = Penalidade; V = preço contratual; A = dias de atraso, incluindo sábados, domingos e feriados; Y = número total de dias no contrato.

- h) 1% do preço contratual pelo incumprimento de qualquer obrigação constante do presente caderno de encargos, que não se subsuma nas alíneas anteriores, por cada dia de atraso e até ao pontual cumprimento;
2. O valor acumulado das penalidades a aplicar não poderá exceder o limite máximo de 20% do preço contratual.
 3. Nos casos em que seja atingido o limite máximo previsto no número anterior, e a Agência, I.P. decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 % (trinta por cento).
 4. Em caso de resolução do contrato por incumprimento definitivo, nos termos do artigo 333.º do Código dos Contratos Públicos, a Agência, I.P. pode aplicar uma pena pecuniária até ao limite indicado no número anterior.
 5. A Agência, I.P. pode compensar os pagamentos devidos ao abrigo do contrato com as sanções de natureza pecuniária devidas nos termos da presente cláusula, obrigando-se o Cocontratante a emitir os necessários documentos contabilísticos para o efeito.

6. As sanções de natureza pecuniária previstas na presente cláusula não obstam a que a Agência, I.P. exija uma indemnização pelo dano excedente nos termos das disposições relativas à obrigação de indemnização por mora e incumprimento definitivo previstas na lei.
7. A aplicação de abatimentos, nos termos previstos na Parte II do CE, relativa aos Níveis de Serviço, não impede ou preclui a aplicação de penalidades.
8. Na determinação da gravidade do incumprimento, a Agência, I.P. tem ainda em consideração a duração da infração, a sua eventual reiteração, o grau de culpa do prestador de serviços e consequências do incumprimento.

Cláusula 20.^a

Força maior

1. Não podem ser impostas penalidades ao Cocontratante, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior.
2. Para efeitos do contrato, só são consideradas de força maior as circunstâncias que, cumulativamente e em relação à parte que as invoca:
 - a) Impossibilitem o cumprimento das obrigações emergentes do contrato;
 - b) Sejam alheias à sua vontade;
 - c) Não fossem por ela conhecidas ou previsíveis à data da celebração do contrato; e
 - d) Não lhe seja razoavelmente exigível contornar ou evitar os efeitos produzidos por aquelas circunstâncias.
3. Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do Cocontratante, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do Cocontratante ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c) Determinações governamentais, administrativas ou judiciais de natureza sancionatória, ou de outra forma resultantes do incumprimento pelo Cocontratante de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo Cocontratante de normas legais;

- e) Incêndios ou inundações com origem nas instalações do Cocontratante cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f) Avarias nos sistemas informáticos ou mecânicos do Cocontratante não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros;
 - h) Declaração de estado de emergência ou de calamidade, nem obrigações legais ou administrativas de teletrabalho, em situações de pandemia declarada pela Organização Mundial de Saúde.
4. A parte que invocar caso de força maior deve comunicar e justificar tal situação à outra parte, logo após a sua ocorrência, bem como informar o prazo previsível para restabelecer o cumprimento das obrigações contratuais.

Cláusula 21.ª

Resolução do contrato por parte da Agência, I.P.

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a Agência, I.P. pode resolver o contrato, a título sancionatório, no caso de o Cocontratante violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.
2. Constitui, entre outros, fundamento de resolução sancionatória, o incumprimento das Especificações Técnicas do CE de forma que impeça a execução do contrato ou que determine que a respetiva execução coloque em causa a credibilidade da Agência, I.P. ou limite gravemente os objetivos a atingir.
3. O direito de resolução referido no número 1 exerce-se mediante declaração enviada ao Cocontratante e não implica a repetição das prestações já realizadas pelo mesmo nos termos previstos no presente CE.

Cláusula 22.ª

Resolução do contrato por parte do Cocontratante

1. O Cocontratante pode resolver o contrato com os fundamentos previstos no artigo 332º do CCP.
2. Salvo na situação prevista na alínea c) do n.º 1 do artigo 332º do CCP, o direito de resolução é exercido por via judicial.
3. A resolução do contrato não determina a repetição das prestações já realizadas pelo

Cocontratante, cessando, porém, todas as obrigações deste ao abrigo do contrato, com exceção daquelas a que se refere o artigo 444º do CCP.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Cláusula 23.ª

Deveres de informação

1. Cada uma das partes deve informar sem demora a outra de quaisquer circunstâncias que cheguem ao seu conhecimento e possam afetar os respetivos interesses na execução do contrato, de acordo com a boa-fé.
2. Em especial, cada uma das partes deve avisar de imediato a outra de quaisquer circunstâncias, constituam ou não força maior, que previsivelmente impeçam o cumprimento ou o cumprimento tempestivo de qualquer uma das suas obrigações.
3. No dia seguinte ao da verificação ou conhecimento do impedimento, a parte deverá informar a outra do tempo ou da medida em que previsivelmente será afetada a execução do contrato.

Cláusula 24.ª

Comunicações

1. Todas as comunicações entre a Agência, I.P. e o Cocontratante devem ser efetuadas através de carta registada com aviso de receção ou correio eletrónico, de acordo com as informações que, para o efeito, constarem no contrato.
2. Qualquer comunicação 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 feita por correio eletrónico é considerada efetuada na data da respetiva expedição e recebida no dia útil seguinte.

Cláusula 25.ª

Regra de informação e publicidade

No cumprimento das disposições legais europeias e nacionais, todos os produtos a entregar

no âmbito do contrato devem obedecer às regras de informação e publicitação do cofinanciamento dos fundos europeus do Portugal 2020.

Cláusula 26.ª

Despesas e encargos

1. Todas as despesas e encargos decorrentes ou necessários para a celebração do contrato são da responsabilidade do Cocontratante.
2. O Cocontratante fica sujeito ao cumprimento das disposições legais e regulamentares, em vigor, designadamente sobre acidentes de trabalho e medicina no trabalho, relativamente aos elementos da sua equipa, na execução dos trabalhos, correndo por sua conta os encargos que daí resultem.
3. Não será exigida a prestação de caução, nos termos do disposto na alínea a) do n.º 2 do artigo 88.º do CCP, sendo que a Agência, I.P. pode, se o considerar conveniente, proceder à retenção de até 10 dos valores dos pagamentos a efetuar, em conformidade com o n.º 3 do mesmo artigo.

Cláusula 27.ª

Foro competente

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

Cláusula 28.ª

Direito aplicável

1. O contrato é regulado pela lei portuguesa, com expressa renúncia a qualquer outra.
2. O contrato tem natureza administrativa e rege-se pelo Código dos Contratos Públicos, aprovado pelo Decreto-Lei nº 18/2008, de 29 de janeiro, com a redação conferida pela Lei nº 30/2021, de 21.05, pela Retificação nº 25/2021, de 21.07 e pelo Decreto-Lei n.º 78/2022, de 7 de novembro.

Cláusula 29.ª

Contagem dos prazos

Os prazos previstos no presente caderno de encargos são contínuos, correndo em sábados, domingos e dias feriados.

PARTE II – CADERNO DE ENCARGOS

ESPECIFICAÇÕES TÉCNICAS

Security Operations Center

Âmbito e Objetivos do Documento

A Agência, I.P. pretende elevar o seu atual nível de segurança informática recorrendo a estratégias de cibersegurança, nomeadamente a monitorização dos *EVENTOS DE SEGURANÇA*. Como tal, pretende adquirir uma solução de monitorização de segurança a fornecer remotamente a partir do centro de operações de segurança (SOC – Security Operations Center) do COCONTRATANTE. Este tipo de serviços permitem obter uma visão geral dos sistemas da organização.

Pretende-se com este serviço avaliar e monitorizar continuamente o estado global da segurança informática que deverá obedecer aos requisitos mínimos, descritos nos capítulos seguintes do presente documento.

O serviço a adjudicar deverá ter em conta as últimas tendências do mercado, nomeadamente um “modern SOC” que deverá ter a capacidades de SIEM e SOAR, permitindo a criação de workbooks e automação.

A proposta de implementação engloba os seguintes serviços:

1. **SOC as a Service** que assegura a recolha de logs, dos activos de rede e segurança, sob vigilância 24/7 dos analistas do Security Operation Center a partir de fora do perímetro da Agência, I.P.;

2. **External Security Assessment c/ Penetration Testing**, serve também como diagnóstico inicial e funciona como um teste efetivo, ainda a partir da infraestrutura pública de Internet, às vulnerabilidades encontradas, analisando a sua exequibilidade de exploração.
3. **Análise Contínua de Vulnerabilidades**, para avaliar se existem vulnerabilidades de segurança internas e externas nos servidores e sites que servem a Agência, I.P.
4. **Serviços de simulação de phishing e sensibilização de cibersegurança**, que tem como objetivo promover a sensibilização dos colaboradores da Agência, I.P. no âmbito da segurança da informação, através da utilização de uma plataforma integrada de sensibilização e formação em cibersegurança.

Este conjunto de serviços apresentados irá permitir habilitar e reforçar as componentes de identificação, proteção, deteção, resposta e recuperação de ameaças e *INCIDENTES DE SEGURANÇA* que possam afetar os sistemas da Agência, I.P. O processo de *INCIDENTES DE SEGURANÇA* não se encontra atualmente documentado.

Para garantir a integração nativa, isto é, maximizar as funcionalidades da tecnologia, pretende-se que todas as tecnologias referidas sejam do mesmo COCONTRATANTE.

SERVIÇOS A PRESTAR

A Agência, I.P. pretende renovar a sua infraestrutura de segurança, passando a considerar um conjunto de soluções. Como tal, as soluções a contratar que serão objeto do presente Caderno de Encargos compreendem a implementação de um Centro de Operações de Segurança, que deverá ser composto pelas seguintes soluções:

1. SOC as a Service
2. External Security Assessment c/ Penetration Testing
3. Análise Contínua de Vulnerabilidades
4. Serviços de simulação de phishing e sensibilização de cibersegurança

SOC as a Service

R. SRV 1. Requisito introdutório: A Agência, I.P. pretende gerir e monitorizar ambientes de segurança a potenciais ameaças aos seus sistemas de informação. Para tal, pretende-se a implementação de um serviço de monitorização de segurança a

fornecer remotamente a partir do centro de operações de segurança do COCONTRATANTE (Centro de Operações de Segurança - SOC).

R. SRV 2. O Security Operations Center (SOC) deverá ser composto por uma equipa de profissionais de segurança, suportados por uma infraestrutura de monitorização, logging e correlação de *EVENTOS* capaz de suportar todos os componentes de infraestrutura de segurança. Desta forma a Agência, I.P. será apoiada na vertente de segurança na deteção e remediação de problemas de segurança.

R. SRV 3. **Pretende-se que o serviço a prestar pelo COCONTRATANTE inclua as seguintes componentes:**

- a. O COCONTRATANTE deverá possuir um Centro de Operações de Segurança (SOC) com Operação 24 horas por dia, todos os dias da semana;
- b. O atendimento do SOC deverá ser realizado em língua portuguesa durante todo o período de cobertura de 24 horas por dias, todos os dias da semana;
- c. Integração com as equipas técnicas da Agência, I.P.;
- d. IOC (Indicators of Compromise) que permitem relacionar qualquer atividade suspeita com indicadores recentes;
- e. Equipa de analistas com múltiplas certificações e experiência em tecnologias distintas;
- f. Disponibilização de informação para análise forense;
- g. Apoio na adaptação do processo de gestão e *INCIDENTES* da Agência, I.P.;
- h. O serviço estará assente num modelo de gestão da plataforma Azure Sentinel, no Tenant da Agência, I.P., em que a operação é feita com base na gestão desta plataforma pela Agência, I.P. O Azure Sentinel ainda não se encontra disponível na Agência, I.P.
- i. O serviço deverá estar preparado para uma eventual alteração para um modelo de SIEM tradicional, com a instalação de um coletor nas instalações da Agência, I.P., responsável pela recolha, normalização, compressão e envio de logs para o SOC.

Características do Serviço

R. SRV 4. **As principais características do serviço a prestar serão:**

- a. Monitorização de segurança 24x7 – análise de *EVENTOS DE SEGURANÇA* 24 horas por dias, 7 dias por semana;
- b. Reporting de Segurança – report mensal completo, incluindo tracking e follow-up;
- c. Tracking de problemas – seguimento de problemas, desde a sua criação até à resolução;

- d. Resposta a *INCIDENTES* (Shutdown) – informação e apoio para desligar dispositivos comprometidos;
- e. Resposta a *INCIDENTES* (Isolation) – informação e apoio para remoção do dispositivo da rede para sanitização;
- f. Resposta a *INCIDENTES* (Incident Mitigation) – informação e apoio para aplicação de workarounds para mitigação do problema;
- g. Resposta a *INCIDENTE* (Emergency Patching) – informação e apoio para aplicação de patches de emergência;
- h. Correlação de Logs – correlação de logs entre sistemas do cliente e IOC;
- i. Tracking de Versões de aplicações – inventário de sistemas, plataformas e aplicações;
- j. O serviço a fornecer deverá ainda ser suportado numa plataforma *Multi-tenant* de forma que os logs permaneçam isolados de quaisquer outros que possam existir;
- k. Antes da entrada em serviço, deverá ser realizada uma auditoria de vulnerabilidades (vulnerability assessment) a todos os ativos que irão ser monitorizados pelo SOC;
- l. A plataforma SIEM deverá ter a capacidade de retenção de logs pelo período que a Agência, I.P. considerar adequado, que se prevê que seja no mínimo de 3 meses, tendo em conta aspetos da legislação, sendo obrigatoriamente comunicado nas reuniões de serviço;
- m. As atividades deverão estar alinhadas com as *frameworks* de referência de risco e segurança da informação, nomeadamente NIST e ISO27001.

Entregáveis

- R. SRV 5. Os entregáveis do serviço a prestar pelo COCONTRATANTE são:
- a. Relatório com Alertas de monitorização – relatório com os alertas de deteção de *INCIDENTES* de segurança através de notificações 24x7x365 enviadas para a Agência, I.P.;
 - b. Avaliação de vulnerabilidades – antes da entrada em produção do serviço de SOC, todos os ativos são alvo de uma análise e é emitido um relatório com as vulnerabilidades encontradas, detalhes técnicos analisados e recomendações para correções;
 - c. Relatório de Serviço – mede o desempenho do SOC utilizando diversos indicadores, e é entregue mensalmente à Agência, I.P. Deve incluir as seguintes métricas:

1. Histórico de evolução das ameaças com indicador de ameaças ao longo do ano;
2. Indicador do nível de ameaça corrente;
3. Resumo das atividades ao longo do mês
4. Recomendações para melhorar o nível de segurança.
5. Exemplo de outros indicadores, a serem definidos em fase de execução:

Tabela 1 – Indicadores de desempenho

Indicadores	Descrição
Tempo médio de Resolução	Tempo médio decorrido na resolução de um <i>INCIDENTE</i>
Tempo médio de Resposta	Tempo médio na resposta a um <i>INCIDENTE</i>
Nível de Cumprimento de Serviço	Percentagem de <i>INCIDENTES</i> resolvidos de acordo com o nível de serviço
Resolução de Primeira Chamada	Percentagem de <i>INCIDENTES</i> resolvidos na primeira chamada
Número de <i>INCIDENTES</i> Repetidos	Número de <i>INCIDENTES</i> idênticos registados num período temporal específico
Rácio de Reabertura	Percentagem de <i>INCIDENTES</i> resolvidos que são reabertos
<i>INCIDENTES</i> Pendentes	Número de <i>INCIDENTES</i> idênticos em fila de resolução
Percentagem de <i>INCIDENTES</i> Graves	Relação do número de <i>INCIDENTES</i> graves vs total de <i>INCIDENTES</i>
Índices de Satisfação do Utilizador	Número de utilizadores satisfeitos com a prestação do serviço

- d. Reuniões de Serviço – para analisar a qualidade do serviço e apresentar o relatório mensal;
- e. Incluir e integrar pelo menos os seguintes componentes:
 1. Detecção de credenciais expostas;
 2. Detecção de domínios semelhantes;
 3. Operação e Manutenção de 5 honey pots (solução técnica para deteção antecipada de possíveis intrusões).
- f. Incluir e integrar a análise contínua de vulnerabilidades para **500 ativos** (internos ou externos) acompanhado com reporting e recomendações;

- g. Incluir, numa fase inicial, um assessment de segurança externa com penetration testing, seguido de retest após introdução e correções por parte do adjudicatário;
- h. A resposta a *INCIDENTES* deverá ser ilimitada desde as fases de identificação até à resolução do *INCIDENTES*.

Metodologia da operação SOC

2.1.3.1 Monitorização contínua de *EVENTOS*

- R. SRV 6. **Requisito introdutório:** A atividade associada à monitorização contínua de *EVENTOS* a prestar pelo COCONTRATANTE através do SOC deverá contemplar as tarefas apresentadas nos requisitos seguintes:
- R. SRV 7. **Recolha de informação:**
1. Recolha de informações de várias fontes de informação;
 2. Identificação da necessidade de integração de novas fontes de informação;
 3. Recolha de indicators of compromise (IOCs);
 4. Recolha de Informação sobre Vulnerabilidades;
 5. Recolha de Informação de contexto organizacional em OSINT.
- R. SRV 8. **Validação da informação:**
1. Monitorizar e recolher logs e pacotes de tráfego de várias fontes;
 2. Validar o processo de padronização;
 3. Certificar que nenhuma Informação é recolhida para além do estritamente necessário.
- R. SRV 9. **Categorização da informação:**
1. Tipo de fonte de informação;
 2. Tipo de log recolhido;
 3. Ação identificada no log: sucesso ou falha.
- R. SRV 10. **Armazenamento da informação na infraestrutura da Agência, I.P.:**
1. Identificar e assegurar o armazenamento correto da informação online;
 2. Identificar e assegurar o armazenamento correto da informação offline;
 3. Identificar e assegurar o armazenamento correto dos backups;

4. Identificar e assegurar o respetivo tempo de retenção, que se prevê que seja no mínimo de 3 meses;
5. Identificar e assegurar que a informação armazenada não está comprometida;
6. Criar mecanismos que assegurem que a Informação pode ser acedida quando necessário, assegurando, por exemplo, mecanismos RBAC (Role-Based Access Control).

R. SRV 11. **Sanitização da informação e disposição:**

1. Identificação dos stakeholders que podem aceder à informação;
2. Sanitização da Informação para que possa ser disponibilizada a vários stakeholders;
3. Criar mecanismos que garantam a informação (relatórios, consolas, gráficos, etc.).

R. SRV 12. **Critérios de prioridade, definindo fórmulas de prioridade para *INCIDENTES DE SEGURANÇA* que deverão conter:**

1. Recursos necessários para gerir o *INCIDENTE*;
2. Impacto no funcionamento do SOC e na organização;
3. Tipos de *INCIDENTES*;
4. Origem e/ou destino do ataque.

R. SRV 13. **Critérios de escalamento:**

1. Identificação dos vários níveis de escalamento por tipo de *INCIDENTE*;
2. Identificar responsáveis por cada nível de escalamento;
3. Identificar SLAs associados a cada nível de escalamento;
4. Definir contactos por cada nível de escalamento.

R. SRV 14. **Divulgação de informações:**

1. Parceiros ou Beneficiários;
2. Equipas de Gestão da Agência, I.P.;
3. Organizações Governamentais;
4. Outros SOC's ou CSIRTS.

2.1.3.2 Atividades de gestão e administração das plataformas tecnológicas

- R. SRV 15. Para além das atividades relacionadas com a monitorização contínua de *EVENTOS*, existem também atividades de gestão e administração das plataformas tecnológicas pertencentes ao SOC, como a solução SIEM, recolha de logs, captura de tráfego, etc. a executar:
- a. Manutenção e evolução das plataformas, incluindo upgrades necessários;
 - b. Operação e configuração da plataforma;
 - c. Integração de novos log sources e pacotes de tráfego;
 - d. Desenvolvimento de novos *use cases*, dashboards, relatórios e regras de correlação
 - e. Análise de performance e capacidade da plataforma;
 - f. Análise e necessidade de alterações à plataforma;
 - g. Análise de mudanças de arquitetura ou renovação tecnológica alinhada com o Roadmap dos fornecedores;
 - h. Análise e Otimização do SIEM em termos de parametrização e capacidade;
 - i. Atualização e parametrização de componente de acordo com recomendações do fabricante;
 - j. Health check da plataforma de SIEM e ativos que reportam *EVENTOS* ;
 - k. Ajustar e otimizar as políticas de correlação e monitorização existentes;
 - l. Suporte na otimização do sistema de alarme SIEM e eliminação de falsos positivos.

Infraestrutura a Monitorizar

- R. SRV 16. Espera-se que a monitorização dos ativos referidos acima, venha a gerar a ingestão de cerca de **32 GB de logs diários**.

External Security Assessment c/ Penetration Testing

- R. SRV 17. Requisito introdutório: Este serviço funciona como um teste efetivo, ainda a partir da infraestrutura pública de Internet, às vulnerabilidades encontradas, analisando a sua exequibilidade de exploração.

- R. SRV 18. Este serviço terá de ser realizado, pelo menos, 3 (três) vezes, uma vez em cada ano civil durante o período em que decorre o contrato.
- R. SRV 19. A Agência, I.P. acordará com o Cocontratante a execução deste teste, nos seguintes termos:
- i. No primeiro ano, a data de execução será acordada até um mês após a assinatura do contrato;
 - ii. Nos anos seguintes, a data de execução do teste será acordada até dia 31 de janeiro.
- R. SRV 20. Atividades de exploração às vulnerabilidades encontradas, de forma a chegar à efetiva exploração, levando a situações de: níveis de privilégio/acesso inesperados, degradação da resposta de serviço ou indisponibilização de serviço, entre outras situações anómalas.
- R. SRV 21. Deve incluir até 13 dias de pentesting e reporting à infraestrutura e rede externa, 4 dias de pentesting de até duas aplicações e 3 dias para retesting.
- R. SRV 22. O modelo de execução será sobre grey-box, time boxed.
- R. SRV 23. Os entregáveis a apresentar à Agência, I.P. com a implementação desta solução são:
- a. Relatório com:
 1. Lista das vulnerabilidades exploradas;
 2. Documentação com o detalhe da exploração das vulnerabilidades encontradas e seus resultados;
 3. Lista de recomendações e correção e/ou de mitigação do impacto das vulnerabilidades em estudo.
- R. SRV 24. Os entregáveis terão que ser entregues à Agência, I.P. até 15 dias após a realização deste serviço.

Análise Contínua de Vulnerabilidades

- R. SRV 25. Requisito introdutório: Para que Agência, I.P. consiga assegurar uma deteção e proteção contínua dos seus ativos, pretende-se a implementação de um serviço em modelo *Cloud* que proporcione visibilidade global sobre as vulnerabilidades

dos sistemas, independentemente da sua localização. A Agência, I.P. possui atualmente licenciamento Microsoft que cobre *workstations* e servidores.

R. SRV 26. Os entregáveis a apresentar à Agência, I.P. com a implementação desta solução são:

- a. Detecção de vulnerabilidades em tempo real;
- b. Identificação da sua localização;
- c. Priorização da sua resolução com base no risco e contexto de negócio;
- d. Redução da exposição ao risco de ataque da organização;
- e. Integração com o serviço de SOC;
- f. Acesso à plataforma de gestão de vulnerabilidades;

R. SRV 27. Disponibilização de dashboard para acompanhamento em tempo real das vulnerabilidades encontradas, classificadas de acordo com a sua criticidade e risco, e recomendações de mitigação.

Serviços de simulação de phishing e sensibilização de cibersegurança

R. SRV 28. Requisito introdutório: Para que Agência, I.P. consiga melhorar a sensibilização dos seus colaboradores no âmbito da segurança da informação, pretende-se a aquisição de um serviço para 220 colaboradores que utilize uma plataforma integrada de sensibilização e formação em cibersegurança, incluindo capacidade de execução de simulações de phishing e formação para 220 colaboradores.

R. SRV 29. Esta plataforma deverá fornecer os conteúdos em língua portuguesa que irão ser adequados aos níveis obtidos pelos colaboradores através dos exercícios de simulações de phishing.

R. SRV 30. A plataforma deverá cumprir os seguintes requisitos:

- a. Integração com Active Directory;
- b. Criação de grupos dinâmicos de utilizadores, como por exemplo criação de grupos de utilizadores por departamento de forma a endereçar campanhas de phishing, automatização dos fluxos de trabalho e agrupar os mesmos com base no nível de risco;
- c. Funcionalidade/capacidade de efetuar campanhas de engenharia social através de phishing por voz através da plataforma de sensibilização;
- d. Possibilidade de, através da consola de gestão da plataforma, assignar utilizadores ou grupos de utilizadores atribuindo permissões de acesso a funcionalidades da

plataforma. Exemplo: acesso à componente de relatórios (individuais e/ou por grupo) para análise da evolução das campanhas de phishing e respetiva evolução das formações atribuídas aos utilizadores;

- e. Capacidade de aproveitar a simulação de phishing para, de uma forma dinâmica e com o objetivo de criar uma sensibilização maior ao utilizador, evidenciar as red flags que o utilizador falhou de forma a reforçar a componente de formação e aumentar a capacidade de análise/sensibilização do utilizador;
- f. Capacidade de efetuar atividades de engenharia social recorrendo a dispositivos de armazenamento USB (pen-drives) “descaracterizadas” e dispersas nas instalações da organização;
- g. Deverá ser permitido o acesso a todos os conteúdos disponíveis pela plataforma, independentemente da língua;
- h. A plataforma deverá ter a capacidade de inteligência artificial (IA) para que, de forma automática, seja possível atribuir o melhor modelo para a simulação de phishing e formação para cada utilizador com base no seu histórico, dando aos utilizadores uma melhor experiência adaptada e personalizada ao seu nível de conhecimento;
- i. Funcionalidade que permita aferir, o grau de sensibilização da organização para uma melhor definição da estratégia global da organização;
- j. Acesso a mais de 100 conteúdos em Português PT;
- k. Suporte de equipa especializada na definição da metodologia de trabalho, por exemplo, configuração dos mailservers, personalização da consola, execução de campanha inicial para definição de baseline, criação customizada de campanhas de phishing, definição dos programas de formação, delinear uma cultura de segurança da organização, produção periódica de relatórios para avaliação do programa de sensibilização e formação;
- l. A plataforma deverá ter capacidade/acesso a relatórios granulares, como por exemplo, com identificação do tipo de browser utilizado no acesso à simulação de phishing.

Fases do Projeto

Para definição do plano de implementação do projeto foram definidas três etapas distintas:

- a) A etapa de Preparação permitindo preparar as condições para o arranque do projeto e para a fase de Implementação;
- b) A etapa de Implementação, que ocorre durante os restantes meses e que prevê a prestação dos serviços conforme os requisitos indicados neste CADERNO DE ENCARGOS;
- c) A etapa de Encerramento.

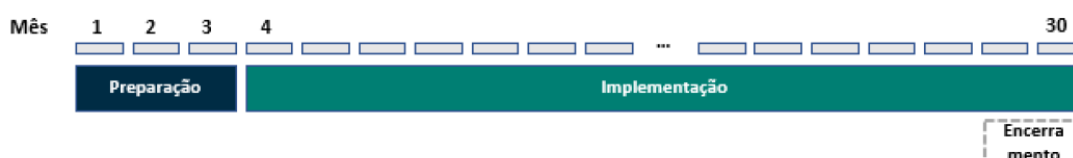


Figura 1 – Fases do Projeto

Preparação

- R. SRV 31. Neste período de Preparação, deve ser assegurado o planeamento, com identificação clara dos pontos críticos para o sucesso da implementação do serviço, com o detalhe exigido pelos vários sistemas de informação no âmbito deste contrato, indicando também as tarefas e momentos na dependência da Agência, I.P. para cumprimento do plano.
- R. SRV 32. O Cocontratante deverá planear, sempre que aplicável, a gestão de transferência de conhecimento, assegurando o sucesso do projeto.
- R. SRV 33. Deverá ser conjuntamente articulado:
- A. Validação do ponto de partida e cronograma dos serviços;
 - B. Preparação das equipas;
 - C. Preparação de meios (comunicações, segurança, acessos);
 - D. Revisão do âmbito;
 - E. Recolha de informação de contexto de negócio e operação;
 - F. Criação e revisão das regras de correlação e outros conteúdos;

- R. SRV 34. Deverá ser fornecido o plano de execução dos trabalhos de implementação do projeto, a submeter a validação prévia da Agência, I.P., nos 5 dias subsequentes à assinatura do contrato.
- R. SRV 35. O período para execução das tarefas da fase de preparação do projeto deverá ser inferior a 90 dias, sendo que os SLA só entram em vigor após esta fase.

Implementação

- R. SRV 36. Esta fase inicia-se imediatamente após a fase de Preparação e consideram-se aqui todas as atividades necessárias para a implementação de um centro de operação de segurança em todas as suas vertentes descritas no capítulo 2, tais como:
- A. Recolha de *EVENTOS* e engenharia da plataforma de SIEM;
 - B. Monitorização e triagem de *EVENTOS*;
 - C. Respostas a *INCIDENTES*;
 - D. Elaboração de relatórios.

Encerramento

- R. SRV 37. A fase de Encerramento, que tem a duração prevista de dois meses, pretende assegurar a passagem necessária de conhecimento à Agência, I.P., ou a quem esta designar. Deve ser efetuada até à data de conclusão do serviço. O Plano de Atividades a concretizar nesta fase deve ser apresentado pelo Cocontratante 15 dias antes do início da mesma para validação e aprovação da Agência, I.P.

Gestão do Contrato

- R. GC 1. Requisito introdutório: O modelo e requisitos para a Gestão do Contrato, abarcam a organização, as práticas, os procedimentos e mecanismos a adotar entre as partes no sentido de gerir e controlar o relacionamento, o cumprimento dos objetivos do contrato e a respetiva gestão financeira.

Relacionamento e Funções

São objetivos genéricos do relacionamento e funções:

- a. Assegurar a comunicação eficaz, eficiente e coordenação entre as partes;
 - b. Assegurar uma prestação de serviço de acordo com o contratado, através da documentação de todas as atividades e controlo de execução;
 - c. Prever e dimensionar serviços contratados em função da evolução das necessidades da Agência, I.P.;
 - d. Definir e implementar processos que otimizem a eficácia e eficiência da prestação de serviço;
 - e. Analisar a qualidade de serviço para identificar oportunidades de melhoria;
- R. GC 2. O modelo deve garantir uma rápida e eficaz tomada de decisão e a resolução célere e expedita de divergências e litígios.

Equipas

- R. GC 3. Requisito introdutório: O COCONTRATANTE deve assegurar a gestão integral de todos os assuntos respeitantes aos colaboradores que utiliza na prestação do serviço.

Instalações

- R. GC 4. Os custos relativos às instalações no COCONTRATANTE ou à criação de condições de qualquer tipo para permitir a prestação remota do Serviço, serão suportados por este.

Modelo de gestão de acompanhamento dos trabalhos

- R. GC 5. Requisito introdutório: A coordenação dos trabalhos irá ser feita com base em metodologias ágeis. A gestão macro do projeto assenta em reuniões para controlo, acompanhamento e garantia da qualidade dos serviços prestados.

R. GC 6. O COCONTRATANTE é responsável pela preparação de documentos de suporte às reuniões com a Agência, I.P.:

Tabela 2 – Reuniões e Reporting de Controlo

Reunião	Periodicidade	Intervenientes	Assuntos	Documentos	Envio documento
Reunião Semanal	Semanal	COCONTRATANTE e Agência, I.P.	Realização de pontos de situação e acompanhamento da performance e evolução do serviço prestado <ul style="list-style-type: none"> Levantamento de necessidades e de oportunidades de melhoria, e alinhamento dos próximos passos 	Documento de Suporte: Ponto de situação da atividade semanal; Pontos críticos	A enviar pelo COCONTRATANTE, 1 dia antes da reunião
Reunião de Serviço	Mensal	COCONTRATANTE e Agência, I.P.	Análise global da qualidade dos serviços prestados, apresentação do relatório mensal e definição de ações estratégicas de melhoria	Relatório de Serviço: Ponto de situação sobre a prestação do serviço ao longo do período decorrido; Apresentação dos indicadores de desempenho; Análise de consumos do contrato no sentido de assegurar a melhor gestão das capacidades contratadas; Cumprimento dos níveis de serviço; Apresentação de lista de melhorias / evoluções propostas pelo COCONTRATANTE visando o	A enviar pelo COCONTRATANTE, 1 dia antes da reunião

Reunião	Periodicidade	Intervenientes	Assuntos	Documentos	Envio documento
				<p>incremento da qualidade e da eficiência do serviço prestado, conforme previsto na Gestão de Serviço</p> <p>Pontos para decisão</p>	

- R. GC 7. Poderão ser ainda realizadas reuniões periódicas de ponto de situação sempre que necessário no sentido de efetuar avaliação dos trabalhos realizados, discutir o plano de trabalho, respetivos riscos, problemas / questões a avaliar, identificação de ações de melhoria do serviço, etc.
- R. GC 8. Relativamente a ferramentas de acompanhamento do progresso, existirão 2 ferramentas principais, sendo que sempre que necessário adaptar-se-ão às necessidades específicas do projeto:
- i. **Monday.com ou equivalente** – acompanhamento de atividades;
 - ii. **Equipa no Teams** - contacto assíncrono entre membros da equipa, partilha de ficheiros e cerimónias não presenciais
- R. GC 9. Todas as reuniões efetuadas no âmbito do relacionamento e funções serão suportadas por uma ata que incluirá:
- i. Lista de participantes nas reuniões;
 - ii. Agenda da reunião;
 - iii. Temas debatidos e conclusões;
 - iv. Ações decorrentes, prazos e responsáveis.
- R. GC 10. A elaboração da ata é da responsabilidade do COCONTRATANTE e deverá ser sempre validada pela Agência, I.P. previamente à sua distribuição para assinatura.

Mecanismo de controlo de níveis de serviço

Níveis de Serviço

- R. NS 1 Requisito introdutório: Este capítulo apresenta os Níveis de Serviço a assegurar pelo COCONTRATANTE numa lógica de obrigação de resultados com penalizações a aplicar perante o incumprimento dos níveis de serviço contratualizados.
- R. NS 2 Os níveis de serviço entram em vigor, na medida do aplicável à fase do projeto logo após o período inicial de Preparação.
- R. NS 3 A prestação de serviços tem de cumprir os objetivos estabelecidos através de Níveis de Serviço definidos.
- R. NS 4 Estão definidos Níveis de Serviço para *INCIDENTES* e para a Monitorização SOC.
- R. NS 5 Os Níveis de Serviço para *INCIDENTES* encontram-se na tabela seguinte:

Tabela 3 – Níveis de Serviço para *INCIDENTES*

#	Prioridade do <i>INCIDENTE</i>	Tempo Máximo de Resposta	Target de Cumprimento
1	P1 – Prioridade Extrema	30 minutos	90%
2	P2 – Prioridade Alta	2 horas	90%
3	P3 – Prioridade Média	8 horas	90%
4	P4 – Prioridade Baixa	24 horas	90%

- R. NS 6 As Prioridades dos *INCIDENTES* dividem-se em:
1. P1 – Os *INCIDENTES* com Prioridade Extrema são aqueles que poderão afetar severamente a qualidade do serviço prestado ou que têm grande impacto para o desenvolvimento do negócio;
 2. P2 – Os *INCIDENTES* com Prioridade Alta são aqueles que em regra causam degradação do serviço;
 3. P3 – Os *INCIDENTES* com Prioridade Média são aqueles que não afetarão de forma significativa o serviço prestado e não terão em regra um impacto significativo para o desenvolvimento do negócio;

4. P4 – Os *INCIDENTES* com Prioridade Baixa são aqueles que não afetarão o serviço prestado e não terão um impacto significativo para o desenvolvimento do negócio.

R. NS 7 A indisponibilidade do serviço será contabilizada a partir da primeira abertura do *INCIDENTE*. O tempo de resposta será a data de início de intervenção a partir do momento em que é feita a triagem do *INCIDENTE*.

R. NS 8 Os Níveis de Serviço para *INCIDENTES* e para a Monitorização SOC são calculados por base mensal, e analisados durante a reunião de serviço mensal com o gestor de serviço.

R. NS 9 Os Níveis de Serviço para a Monitorização SOC encontram-se na tabela seguinte:

Tabela 4 – Níveis de Serviço de Monitorização SOC

#	Indicador	Tempo máximo de resposta	Target de Cumprimento
1	SLA Triagem na receção de incidentes – 60 minutos	60 minutos	90%
2	Disponibilidade do serviço de SOC	-	99,9%
3	Entrega do relatório mensal de SOC até o dia 8 do mês seguinte ao serviço	Até dia 8 do mês N+1	-
4	Reunião de serviço até dia 15 do mês seguinte ao serviço	Até dia 15 do mês N+1	-
5	Entrega do relatório de análise forense até 15 dias após <i>INCIDENTE</i>	Até 15 dias	-
6	Falsos positivos dos serviços de deteção	-	<=10%

Incumprimentos associadas aos Níveis de Serviço

R. NS 10 Requisito introdutório: Este capítulo apresenta o método de quantificação das falhas associadas aos Níveis de Serviço, em caso de não concretização dos objetivos de cumprimento definidos no capítulo anterior por parte do COCONTRATANTE.

R. NS 11 Para a aplicação das Penalizações referentes aos Níveis de Serviço deve ser utilizado o custo total da mensalidade do contrato.

R. NS 12 As Penalizações associadas a cada Nível de Serviço podem ser de três tipos:

A. Penalização A:

Tabela 5 – Penalizações do tipo A

Desvio face ao Objetivo	Penalização
Desvio superior a 2%	1,50%
Desvio superior a 4%	3%
Desvio superior a 6%	5%
Desvio superior a 8%	7,50%
Desvio superior a 10%	10%

B. Penalização B:

Tabela 6 – Penalizações do tipo B

Desvio face ao Objetivo	Penalização
Desvio entre 1 e 3 dias	1,50%
Desvio entre 4 e 5 dias	3%
Desvio superior a 6 dias	10%

C. Penalização C:

Tabela 7 – Penalizações do tipo C

Desvio face ao Objetivo	Penalização
Desvio superior a 0,1%	1,50%
Desvio superior a 0,5%	3%
Desvio superior a 1%	5%
Desvio superior a 2%	7,50%
Desvio superior a 10%	10%

R. NS 13 Apresentam-se na tabela abaixo os tipos de Penalizações associadas aos Níveis de Serviço para *INCIDENTES*:

Tabela 8 – Penalizações dos Níveis de Serviço para *INCIDENTES*

#	Prioridade do <i>INCIDENTE</i>	Penalização
1	P1 – Prioridade Extrema	A

2	P2 – Prioridade Alta	A
3	P3 – Prioridade Média	A
4	P4 – Prioridade Baixa	A

R. NS 14 Apresentam-se na tabela abaixo os tipos de Penalizações associadas aos Níveis de Serviço para Monitorização SOC:

Tabela 9 - Penalizações dos Níveis de Serviço para a Monitorização SOC

#	Indicador	Penalização
1	SLA Triagem na receção de incidentes - 60 minutos	A
2	Disponibilidade do serviço de SOC	C
3	Entrega do relatório mensal de SOC até o dia 8 do mês seguinte ao serviço	B
4	Reunião de serviço até dia 15 do mês seguinte ao serviço	B
5	Entrega do relatório de análise forense até 15 dias após INCIDENTE	B
6	Falsos positivos dos serviços de deteção	A

R. NS 15 Para o cálculo do Abatimento total na faturação, deverão ser somadas todas as Penalizações identificadas.

R. NS 16 Os Abatimentos, aplicáveis mensalmente, não podem ultrapassar 10% de penalização da faturação referente ao mês em que ocorreram as respetivas falhas no cumprimento dos Níveis de Serviço.

R. NS 17 Os Abatimentos não constituem nem prejudicam a aplicação das penalizações por incumprimentos contratuais, nos termos fixados na Parte I do CE.

R. NS 18 A Agência, I.P. pode decidir proceder à resolução do contrato caso se verifiquem, em três meses consecutivos os seguintes incumprimentos:

1. 3 (três) desvios superiores a 8% face ao objetivo, ou 2 (dois) ou mais desvios superiores a 10% face ao objetivo, para penalizações do tipo A;
2. 2 (dois) ou mais desvios superiores a 10% face ao objetivo, para penalizações do tipo C.

Apêndice I – Competências específicas da equipa

Certificações

O COCONTRATANTE deve apresentar na proposta uma equipa que, na sua totalidade, apresente as certificações indicadas abaixo:

- i. ISO 27001 Lead Auditor
- ii. ISO 27001 Lead Implementor
- i. ITIL
- ii. PMP
- i. Microsoft Security AZ-500
- ii. Microsoft Security MS-500
- iii. Microsoft Security SC-900
- iv. Microsoft Security SC-200

Cada um dos elementos da equipa apresentada deve ter, pelo menos, uma das certificações apresentadas acima.

Podem ser apresentadas outras certificações que sejam equivalentes ou superiores às indicadas, cabendo ao adjudicatário comprovar essa circunstância.

Competências Gerais

O COCONTRATANTE deverá apresentar uma equipa na qual, pelo menos, um elemento colabore na rede nacional de CSIRT há mais de 6 meses, contados da data da entrega da proposta, sendo obrigatório que, ao longo de todo o período de vigência do CONTRATO, integre a equipa um elemento com estas características.;

A equipa global terá de ser composta por uma equipa de gestão do projeto e uma equipa de implementação que apresente perfis/elementos com a experiência profissional identificada de seguida:

- a. Equipa de Gestão do Projeto – Na equipa proposta o Concorrente pode apresentar um ou mais elementos. Na equipa terá que existir a seguinte experiência:
 - i. Experiência profissional mínima de 3 (três) anos em gestão de projeto, na área de IT Governance;
 - ii. Experiência profissional mínima de 3 (três) anos em gestão de projeto, na área de Information Security.

Caso a equipa apresentada seja composta por 2 (dois) ou mais elementos, devem indicar o Gestor de Projeto principal para a área de IT Governance e para a área de Information Security, sendo que um mesmo elemento pode ser o Gestor de Projeto principal de ambas as áreas.

- b. Equipa de Implementação e Operação SOC – Na equipa proposta o Concorrente terá de apresentar perfis de Implementação e perfis de Operação SOC.
 - 1. Para os perfis de Implementação todos os elementos têm de possuir a seguinte experiência mínima:
 - i. Experiência profissional mínima de 1 (um) ano em projetos de implementação de soluções Azure Sentinel;
 - ii. Experiência profissional mínima de 2 (dois) projetos em que tenha desempenhado funções na implementação de Azure Sentinel.
 - 2. Para os perfis de Operação SOC (Equipa 24x7) – O Concorrente terá de apresentar no mínimo 4 elementos com este perfil. Na equipa terá que existir a seguinte experiência:
 - i. Experiência profissional mínima de 1 (um) ano em funções de Operação SOC.
- Para a equipa de Implementação e Operação SOC, podem existir elementos que se enquadrem nos dois tipos de perfis.