



**CONCURSO PÚBLICO COM PUBLICIDADE
INTERNACIONAL**

**Renovação e modernização da Solução de
Comunicações Unificadas, serviços de NOC (Network
Operations Center) e SOC (Security Operations
Center)**

Caderno de Encargos

Procedimento n.º 220/2021

Setembro de 2021

Parte I - CLÁUSULAS JURÍDICAS

Cláusula 1ª

Objecto do contrato

O presente procedimento tem por objecto a *Renovação e modernização da Solução de Comunicações Unificadas, serviços de NOC (Network Operations Center) e SOC (Security Operations Center)*, em conformidade com as Cláusulas Técnicas do presente Caderno de Encargos.

Cláusula 2ª

Contrato

1. O contrato resultante do presente procedimento será reduzido a escrito, nos termos do artigo 94.º do Código dos Contratos Públicos.
2. Fazem ainda parte do Contrato os elementos dispostos no n.º 2 do artigo 96.º do Código dos Contratos Públicos.
3. Em caso de divergência entre os documentos referidos no número anterior, a ordem de prevalência é a que se dispõe na legislação.

Cláusula 3ª

Vigência do Contrato

1. Os serviços objecto do procedimento deverão ser prestados durante o prazo de 36 (trinta e seis meses). O prazo de fornecimento e instalação dos serviços é de 30 (trinta dias), após a adjudicação.

Cláusula 4ª

Obrigações do Adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas Cláusulas Contratuais, decorre para o prestador de serviços a obrigação de prestar os serviços descritos no objecto do presente Caderno de Encargos.

2. O adjudicatário obriga-se a executar o objeto do contrato de forma profissional e competente, utilizando os conhecimentos técnicos, o know-how, a diligência, o zelo e a pontualidade próprios das melhores práticas.
3. Constituem ainda obrigações do adjudicatário:
 - a) Apresentar os documentos de habilitação;
 - b) Prestar os serviços à entidade adjudicante, conforme as características técnicas, requisitos mínimos e com as especificações constantes do presente caderno de encargos;
 - c) Recorrer a todos os meios humanos e materiais que sejam necessários e adequados à execução do contrato;
 - d) Comunicar antecipadamente, logo que tenha conhecimento, à entidade adjudicante, o facto que torne total ou parcialmente impossível a prestação dos serviços objeto do procedimento, ou o cumprimento de qualquer outra das suas obrigações nos termos do contrato celebrado com a entidade adjudicante;
 - e) Não alterar as condições do fornecimento da prestação dos serviços fora das especificações do presente caderno de encargos;
 - f) Não subcontratar, no todo ou em parte, a execução do objeto do contrato, sem prévia autorização da entidade adjudicante;
 - g) Comunicar qualquer facto que ocorra durante a execução do contrato e que altere, designadamente, a sua denominação social, os seus representantes legais, a sua situação jurídica e a sua situação comercial;
 - h) Manter sigilo e garantir a confidencialidade, não divulgando quaisquer informações que obtenham no âmbito da formação e da execução do contrato, nem utilizar as mesmas para fins alheios àquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos;
 - i) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.

Cláusula 5ª

Objecto do Dever de Sigilo

1. O prestador de serviços deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao adjudicatário, de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objecto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. O Adjudicatário garantirá sigilo quanto às informações que os seus colaboradores venham a ter conhecimento, relacionadas com a actividade da Adjudicante mesmo após a conclusão dos trabalhos.
4. O dever de sigilo previsto no número anterior impõe-se, de igual modo, às entidades que assegurem a realização dos trabalhos objecto de subcontratação parcial.
5. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo prestador de serviços ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.
6. O dever de sigilo mantém-se em vigor até ao termo do prazo de 5 (cinco) anos a contar do cumprimento ou cessação, por qualquer causa, 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 6ª

Proteção de dados pessoais

1. O prestador de serviços e a entidade adjudicante obrigam-se, durante a vigência do contrato e, sempre que exigível, após a sua cessação, a dar rigoroso cumprimento ao disposto na respectiva legislação aplicável, nomeadamente ao Regulamento (EU) 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril.

Cláusula 7ª

Preço base

O preço máximo que a entidade adjudicante se dispõe a pagar pelo objecto do contrato é de 165.600,00€ (cento e sessenta e cinco mil e seiscentos euros), acrescido de IVA à taxa legal em vigor.

Este valor corresponde a um total máximo mensal de 4.600,00€ (quatro mil e seiscentos euros), acrescido de IVA à taxa legal em vigor.

Cláusula 8ª

Preço contratual

1. Pela prestação dos serviços objecto do contrato, bem como pelo cumprimento das demais obrigações dele decorrentes, a Ordem dos Enfermeiros deve pagar ao prestador de serviços o preço constante da proposta adjudicada.
2. O preço referido nos números anteriores inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante.
3. Na factura, e consequente pagamento, serão tomados em conta o custo total da adjudicação e dedução relativa à penalização por eventuais atrasos na realização dos trabalhos ou outras deduções previstas no Caderno de Encargos.
4. O preço contratual constituirá um valor máximo, não sendo devidas prestações pelo valor remanescente de serviços que não sejam comprovadamente prestados.

Cláusula 9ª

Condições de Pagamento

1. As quantias devidas pela entidade adjudicante, nos termos da cláusula anterior, serão pagas no prazo de 30 dias após recepção das respectivas facturas.
2. Em caso de discordância por parte da entidade adjudicante, quanto aos valores indicados na factura, deve esta comunicar ao prestador de serviços, por escrito, os respetivos fundamentos, ficando o prestador de serviços obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova factura corrigida.
3. Desde que devidamente emitidas e observado o disposto no n.º 1, as facturas serão pagas através de transferência bancária.

Cláusula 10ª

Sanções

1. Sem prejuízo das responsabilidades do Cocontratante perante Terceiros e da aplicação de penalidades por outras entidades com competência para tal, a Ordem dos Enfermeiros poderá aplicar ao Cocontratante sanções pecuniárias, de acordo com o disposto nas Cláusulas expressamente previstas neste Caderno de Encargos e/ou no Contrato e, desde que o incumprimento do Cocontratante decorra de atos ou omissões que lhe sejam imputáveis.
2. Pelo incumprimento de obrigações emergentes do contrato, a entidade adjudicante pode exigir do adjudicatário o pagamento de uma sanção pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - A. Pelo incumprimento dos serviços contratualizados, será aplicada uma sanção correspondente a 10% do preço contratual.
 - B. Pelo incumprimento dos prazos de entrega do fornecimento e instalação dos serviços, até 20% do preço contratual.
 - C. Pelo incumprimento dos níveis definidos nas especificações técnicas do caderno de encargos ou daqueles a que o Cocontratante se haja obrigado na sua proposta, será aplicada uma sanção correspondente da 20% do preço contratual referente à instalação/serviço onde ocorre o incumprimento, pelo período em que o mesmo se mantenha.
3. As sanções aplicadas nos termos do número anterior poderão ser contabilizadas ou convertidas em horas de serviço ou em valor monetário, por aplicação dos preços contratualizados aplicáveis.
4. Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.
5. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.
6. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.

7. Nos casos em que seja atingido o limite previsto no número anterior e a Entidade Adjudicante decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 %.
8. As sanções pecuniárias previstas na presente cláusula não obstam a que a entidade adjudicante exija uma indemnização pelos danos decorrentes da mora no cumprimento, cumprimento defeituoso e incumprimento definitivo.
9. Caso o segundo outorgante não cumpra as condições contratuais, poderá ainda ser rescindido o contrato.

Cláusula 11ª

Força Maior

1. Não podem ser impostas penalidades ao prestador de serviços, 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, entendendo-se como tal as circunstâncias que impossibilitem a respectiva realização, alheias à vontade da parte afectada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Pode constituir força maior, se verificados os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, actos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
 - a) Circunstâncias que não constituam força maior para os subcontratados do prestador de serviços, na parte em que intervenham;
 - b) Greves ou conflitos laborais limitados às sociedades do prestador de serviços 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 prestador de serviços de deveres ou ónus que sobre ele recaiam;
 - d) Manifestações populares devidas ao incumprimento pelo prestador de serviços de normas legais;

- e) Incêndios ou inundações com origem nas instalações do prestador de serviços 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 prestador de serviços não devidas a sabotagem;
 - g) Eventos que estejam ou devam estar cobertos por seguros.
 - h) A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
4. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

Cláusula 12ª

Resolução por Parte da Ordem dos Enfermeiros

1. Sem prejuízo de outros fundamentos de resolução previstos na lei, a Ordem dos Enfermeiros pode resolver o contrato, a título sancionatório, no caso de o prestador de serviços violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.
2. O direito de resolução exerce-se mediante declaração enviada ao prestador de serviços.

Cláusula 13ª

Resolução por parte do Prestador de Serviços

Sem prejuízo de outros fundamentos de resolução previstos na lei, o prestador de serviços pode resolver o contrato nos casos previstos no artigo 332.º do CCP.

Cláusula 14ª

Boa-fé

As partes obrigam-se a atuar de boa-fé na execução do contrato e a não exercer os direitos nele previstos, ou na lei, de forma abusiva.

Cláusula 15ª

Uso de Sinais Distintivos

Nenhuma das partes pode utilizar a denominação, marcas, nomes comerciais, logótipos e outros sinais distintivos do comércio que pertençam à outra sem o seu prévio consentimento escrito.

Cláusula 16ª

Subcontratação e Cessão da Posição Contratual

1. A subcontratação pelo prestador de serviços e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do CCP.
2. Em caso de incumprimento pelo adjudicatário das suas obrigações, nos termos do art.º 318.º-A do CCP, o mesmo cede a sua posição contratual ao concorrente do procedimento pré-contratual na sequência do qual foi celebrado o contrato, mediante a ordem sequencial de classificação no procedimento, a fim de concluir um novo contrato para a adjudicação da conclusão dos trabalhos.

Cláusula 17ª

Comunicações e Notificações

1. Em sede de execução contratual, todas as comunicações da entidade adjudicante dirigidas ao adjudicatário são efetuadas por escrito e enviadas através de correio registado, fax ou correio eletrónico, de acordo com os elementos a indicar pelo adjudicatário.
2. Em sede de execução contratual, todas as comunicações do adjudicatário dirigidas à entidade adjudicante são efetuadas por escrito e enviadas através de correio registado, fax ou correio eletrónico.
3. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 18ª

Gestor de Contrato

Tal como estipulado no Artigo 290-A do CCP, a Ordem dos Enfermeiros designará um gestor do contrato, com a função de acompanhar permanentemente a execução do mesmo.

Cláusula 19ª

Legislação aplicável

Em tudo o que não se encontrar especialmente regulado, aplicam-se as disposições constantes da legislação portuguesa.

Cláusula 20ª

Foro Competente

Para todas as questões emergentes do contrato será competente o Tribunal Administrativo de Círculo de Lisboa, com expressa renúncia a qualquer outro.

Parte II - CLÁUSULAS TÉCNICAS

Cláusula 21ª **Âmbito do Contrato**

O presente procedimento visa a renovação e modernização da Solução de Comunicações Unificadas, adquirir serviços de NOC (Network Operations Center), Break and Fix e SOC (Security Operations Center).

Cláusula 22ª **Especificação Técnica**

1. Certificações

O Adjudicatário deverá apresentar as certificações de fabricante que atestam as suas competências na vertente de desenho da solução (conceção), implementação e suporte pós-venda das soluções que preconizam implementar.

É condição obrigatória o Adjudicatário fazer prova de:

- a) Ser parceiro certificado do fabricante no território nacional;
- b) Apresentar por escrito a garantia da existência de parcerias válidas com os fabricantes dos equipamentos e serviços a que deve dar suporte no âmbito do presente procedimento, permitindo-lhe ter acesso a serviços de *back-to-back* com o fabricante;
- c) apresentar comprovativo das certificações ISO 9001, ISO 20000-1 e ISO 27001.
- d) O concorrente deverá comprovar a existência de quadros técnicos certificados para prestar assistência aos equipamentos e serviços da entidade adjudicante, devendo estes ter, certificação válida em:
 - Cisco - CCIE de colaboração, CCNP Security;
 - CompTIA - CompTIA Infrastructure Security Expert, CompTIA CySA+, CompTIA Security+, CompTIA PenTest+, CompTIA Security Analytics Expert;
 - EC Council - Certified Ethical Hacker;
 - ISACA - CISSP - Certified Information Systems Security Professional, CISM - Certified Information Security Manager;
 - Certificação técnica nos equipamentos a fornecer.

2. Substituição das equipas

- a) A qualquer alteração à composição da equipa indicada em sede de formação do contrato deve ser previamente comunicada à Entidade Adjudicante e só será aceite caso reúna os requisitos mínimos exigidos no caderno de encargos, podendo, para o efeito, ser solicitada informação e documentação adicional para confirmação dos elementos curriculares apresentados.

- b) A substituição referida no número anterior deverá ocorrer da seguinte forma:
- O Adjudicatário deverá, em 5 dias úteis, identificar o seu melhor recurso considerando os requisitos mínimos exigidos e obter a aceitação pela Entidade Adjudicante;
 - O Adjudicatário deverá assegurar que nos 5 dias úteis após a aceitação o recurso inicia a prestação do serviço.
- c) Sempre que se constate a inadequação de algum elemento da equipa encarregue da execução dos serviços contratados, tendo em conta os requisitos exigidos e o comportamento comumente expectável, poderá a Entidade Adjudicante exigir a sua substituição, aplicando-se, com as devidas adaptações, o disposto nos números anteriores.

3. Serviços de NOC (Network Operations Center), Break and Fix e SOC (Security Operations Center)

A Entidade Adjudicante pretende contratar um serviço de suporte, gestão e operação, implementação de melhorias nas plataforma, monitorização e correção de ocorrência, análise de eventos de segurança com capacidade de resposta operacional, em regime 24x7x365 e pelo período de 36 meses. Estes serviços têm como objetivo identificar e corrigir de forma atempada qualquer incidente de performance, disponibilidade e ataques ou ameaças externas dirigidas aos seus serviços e sistemas que possam de alguma forma comprometer o funcionamento e bom nome da organização.

O serviço a propor deve incluir todos os suportes, materiais, equipamentos, ferramentas, infraestrutura e pessoal qualificado para a prestação dos serviços aqui identificados e respeitando os sistemas de confidencialidade, e regras de proteção de dados.

O Adjudicatário tem obrigatoriamente de contemplar a notificação dos alertas críticos por email, telefone e SMS.

4.1. Âmbito do serviço a ser prestado

- a) Serviço de suporte em regime 24x7, com SLA de tempo de resposta de 4 horas;
- b) Serviço de monitorização de performance e disponibilidade em regime de 24x7;
- c) Serviço de monitorização de eventos de segurança em regime de 24x7;
- d) Serviço de correção de eventos de segurança em regime de 24x7;
- e) Serviço de Operação e Gestão de infraestrutura;
- f) Avaliar, no âmbito da segurança, a infraestrutura tecnológica implementada;
- g) Aplicar configurações rede, switching e firewall no sentido de adequar a infraestrutura às melhores praticas de segurança em vigor, com o objetivo de prevenção a incidentes e de responder eficazmente a ataques neste âmbito;

- h) Gestor de serviço dedicado;
- i) Trimestralmente executar um *Healthcheck appointment* a todos os sistemas e equipamento no âmbito do contrato;
- j) Apresentar um relatório com os resultados, 5 dias úteis após a execução do *Healthcheck appointment*;
- k) Correção de incidentes de segurança será sobre os equipamentos, sistemas e aplicações geridas no âmbito do contrato. A intervenção sobre outros sistemas será intermediada pela equipa de IT da Ordem.

4.2. Componentes a considerar:

- a) NOC (*Network Operations Center*) ;
- b) SOC (*Security Operations Center*);
- c) *Break and Fix*

4.3. Requisitos Genéricos

- a) Possibilidade de abertura de pedidos por:
 - E-mail;
 - Telefone;
 - Portal Web.
- b) Serviço de apoio ao cliente: 24 x 7
- c) Diagnóstico remoto;
- d) Escalonamento de incidentes;
- e) Acesso a novas versões de software;
- f) Substituição/reparação de hardware;
- g) Deslocações on-site;
- h) Manutenção preventiva: 24 x 7 x 4;
- i) Manutenção corretiva: 24 x 7 x 4
- j) Manutenção evolutiva: 24 x 7 x 4

4.4. Serviços de monitorização de eventos de performance e disponibilidade:

4.4.1. Equipamentos

- Equipamentos de Switching Core e Acesso;
- Firewalls Cisco Firepower;
- Telefonia IP (Call Manager e CCX);
- Firewall Cooperativa Palo Alto (Máquina Virtual);
- Cluster Hyper-V;
- Deve estar previsto a inclusão de novas fontes de informação durante o período de prestação do serviço.

4.4.2. Requisitos Genéricos

Requisitos técnicos do Serviço de monitorização de eventos de performance e disponibilidade:

- Monitorização contínua dos indicadores de desempenho;

- Verificação contínua da disponibilidade e performance;
- Monitorização da disponibilidade e capacidade;
- Estado do equipamento, processamento, Memória, Temperatura, Largura de banda, Latência;
- Monitorização dos alertas operacionais dos assets; Alerta quando os limites mínimos ou máximos predefinidos são violados;
- Identificação do parque abrangido pelo serviço (Hardware, Versões de software).

4.5. Requisitos Funcionais

4.5.1. Serviços mínimo de parâmetros a serem monitorizados:

- Utilização da interface, erros, bytes enviados e recebidos
- CPU
- Memória
- Disco
- Utilização do processo

4.6. Níveis de Serviço

Devem ser definidos os níveis de serviço associados ao serviço de monitorização de eventos de performance e disponibilidade:

Métrica	Valor
Disponibilidade mensal da solução SIEM	99,5%
Notificação de alertas identificados	4 horas

4.7. Serviços de monitorização de eventos de segurança

4.7.1. Equipamentos

- Equipamentos de Switching Core e Acesso;
- Rede Wifi;
- Rede Privada e VPN;
- Firewalls Cisco Firepower;
- Solução Cisco ESA;
- Solução Cisco AMP;
- Servidores Físicos e Virtuais;
- Desktops, Laptops e dispositivos moveis conectados na rede de dados da Entidade Adjudicante;
- Domain Controllers e Microsoft Active Directory;
- Firewall Cooperativa Palo Alto (Máquina Virtual);
- Deve estar previsto a inclusão de novas fontes de informação durante o período de prestação do serviço.

4.7.2. Requisitos Genéricos do Serviço

Este serviço deverá considerar a execução das seguintes tarefas:

- Identificação e revisão de todos os eventos classificados como suspeitos de serem ameaças à segurança da rede corporativa;
- Identificação e comunicação de incidentes de segurança de acordo com o processo acordado entre as partes;
- Validação dos incidentes identificados e gerados pelos mecanismos de correlação e alarmística;
- Acompanhamento da resolução do incidente de segurança;
- Elaboração de recomendações;
- Definição, configuração e realização de relatórios customizados e geração de alarmística;
- Elaboração mensal de relatório de incidentes de segurança;
- Elaboração mensal de um plano para correção de incidentes de segurança;
- Retenção de logs;
- Definição de roadmap com ações que visem melhorar o serviço e a consequente postura de segurança da organização;
- Apoio à definição e ou melhoria dos indicadores de segurança;
- Correções e implementação de melhorias dos indicadores de segurança;
- Monitorização em tempo real dos eventos importantes provenientes das várias plataformas;
- Correções e implementação de melhorias importantes provenientes das várias plataformas;
- Desenhar e implementar Dashboards para o serviço, com a identificação de métricas e indicadores (KPIs) adequados;
- Relatório mensal com as atividades, eventos e tarefas executadas;
- Entrega de documentação técnica das parametrizações, desenvolvimentos e implementações executadas.

4.8. Tratamento e análise

Deve ser contemplada a receção e tratamento dos eventos provenientes dos equipamentos de segurança como:

- Normalização, agregação e correlação de eventos;
- Classificação e priorização atendendo à sua criticidade;
- Integração com threat intelligence feeds como:
 - Blacklists de endereços IP;
 - Comunicações com Botnets;
 - Malware;
 - Entre outros.
- Recolha de Indicadores de compromisso;
- Gestão de incidentes de segurança de informação;
- Correção de Incidentes;
- Implementação de melhorias;
- Produção de relatórios com recomendações.

4.9. Gestão de incidentes de segurança

A Entidade Adjudicante pretende que o adjudicatário efetue uma monitorização 24/7 e atue de imediato a qualquer incidente que ocorra na infraestrutura ao abrigo do presente caderno de encargos.

A metodologia de respostas de incidentes adotada deve permitir responder de forma rápida e eficiente aos incidentes de segurança. O Adjudicatário deve adotar medidas preventivas para evitar sempre que possível ocorrência de incidentes.

A metodologia deve ter em conta os processos de:

- Identificação, classificação, investigação;
- Resposta, remediação, contenção, recuperação;
- Comunicação e escalonamento;
- Alterações e plano de ação;
- Lições aprendidas.

4.10. Métricas

Durante a fase de setup do serviço devem ser definidas as métricas /KPI que serão utilizadas para medir o estado da segurança, como por exemplo:

- Nº de Incidentes de segurança abertos por gravidade;
- Nº de incidentes recorrentes;
- Tempo médio de resolução do incidente;
- Tempo de resposta a incidentes por gravidade;
- % de Intrusões Detetados e bloqueados vs Detetados e não bloqueados.

4.11. Relatórios e Dashboards

Devem ser produzidos relatórios mensais sobre os incidentes registados, análise efetuada e recomendações de mitigação de eventuais vulnerabilidades.

Deve ser contemplada o desenho e implementação de Dashboards que permitam identificar métricas e indicadores (KPIs) adequados.

4.12. Proteção e retenção de Logs

- a) Os eventos de segurança devem ser protegidos adequadamente (perda, alteração e confidencialidade) através da utilização de encriptação, controlo de acessos e backups;
- b) Os eventos de segurança devem ser guardados para permitir a sua análise forense;
- c) Os eventos e alertas devem ser transmitidos utilizando protocolos seguros sempre que os equipamentos o suportarem;
- d) Os log's devem ser retidos no mínimo por um período superior a 90 dias;
- e) Em caso de uma solicitação urgente por parte de Entidade Adjudicante deve o Adjudicatário garantir o acesso aos logs num prazo inferior a 24 horas.

4.13. Níveis de Serviço

Devem ser definidos os níveis de serviço associados ao serviço de monitorização de segurança:

Métrica	Valor
Disponibilidade mensal da solução SIEM	99,5%
Notificação de alertas identificados	4 horas

4.14. Serviços de Gestão & Operação:

Equipamentos

- Equipamentos de Switching Core e Acesso;
- Firewalls Cisco Firepower;
- Telefonia IP (Call Manager e CCX);
- Solução Cisco ESA;
- Solução Cisco AMP;
- Cluster Hyper-V ;
- Servidores Físicos e Virtuais;
- Firewall Cooperativa Palo Alto (Máquina Virtual).

4.14.1. Requisitos Genéricos do serviço

Este serviço deverá ser realizado por equipas especializadas que têm competências nas mais diversas áreas tecnológicas e que garantem as atividades de gestão diária dos equipamentos em âmbito, nomeadamente:

A execução dos pedidos de serviço;

- A operação e gestão diária das diferentes componentes da infraestrutura em âmbito, garantido assim o correto funcionamento da mesma e a sua adaptação às necessidades do negócio. Sendo que os processos de gestão de alterações são baseados nas melhores práticas de mercado;
- Este serviço deverá contemplar a atividade de upgrade de versões dos equipamentos em âmbito;
- Correção e implementação de alterações e melhorias à infraestrutura em âmbito de forma proativa e corretiva, sempre que se justificar.

4.15. Plataforma de Monitorização

Não é âmbito deste procedimento a Entidade Adjudicante adquirir qualquer equipamento ou Software para este serviço. O Adjudicatário deverá possuir uma ferramenta de monitorização própria (ex: SIEM).

Serão valorizados os serviços que possuam soluções que permitam de forma fácil fazer evoluir o serviço de monitorização de segurança para um serviço mais abrangente que comtemple também a monitorização, gestão e operação dos equipamentos (rede e segurança) e serviços assegurados pelos mesmos (ex: largura de banda dos links Internet).

Para o efeito o sistema de monitorização de suporte ao serviço deve suportar os seguintes requisitos funcionais:

- Todos os componentes, daqui em diante referidos como coletores, são fornecidos como um dispositivo virtual;
- Os coletores encaminham os dados do evento para a camada de armazenamento e correlação;
- Os coletores podem armazenar dados em cache caso a camada de armazenamento e correlação fique indisponível. O coletor deve manter os logs em cache até ao seu limite de capacidade de armazenamento;
- Os coletores devem poder limitar a largura de banda utilizada para o upload do evento;
- Os coletores devem poder compactar os dados antes de os enviar para a camada de armazenamento e correlação.
- Os coletores comunicam com a camada de armazenamento e correlação por HTTPS. A direção da comunicação é dos coletores para a camada de armazenamento e correlação;
- Se um coletor falhar, um de substituição poderá ser implementado simplesmente registando novamente um novo dispositivo "Collector" na camada de armazenamento e correlação. Os coletores deverão ser configurados e geridos centralmente bastando a informação de endereço IP necessárias para reimplementar um coletor;
- Os coletores devem ser capazes de processar > 10K EPS;
- Os coletores devem executar o processo de descoberta e coletar dados de desempenho usando protocolos diferentes, como SNMP, WMI, SSH;
- Os coletores devem poder processar as informações do NetFlow;
- Os coletores também devem atualizar automaticamente novos analisadores (parsers) se os mesmos, forem atualizados no sistema de gestão central do SIEM;
- Quando implementado num ambiente de "multitenant", um coletor deve poder manipular logs de vários "tenants" em simultâneo;
- As atualizações de firmware dos coletores devem ser geridas na consola de web do SIEM, evitando a necessidade de conectar-se a cada coletor e executar a atualização individualmente;
- Interface de gestão acessível via web (https);
- Dashboards configuráveis;
- Gestão de inventário baseado numa CMDB, e deve armazenar:
 - Versão / Firmware / SO instalado no dispositivo
 - Número de série do dispositivo
 - Interfaces configuradas no dispositivo junto com
 - Nome da interface
 - IP e sub-rede
 - Status da interface (ativado, desativado)
 - Quaisquer níveis de segurança configurados no dispositivo
 - A velocidade da interface
 - A velocidade e o nome da interface devem ser editáveis
 - Valores personalizados, conforme necessário.
 - Processos em execução no dispositivo ou sistema operativo

- Alertar quando houver uma alteração no status do processo, monitorizando ativamente através de protocolos, conforme descrito nos protocolos:
 - SNMP
 - WMI
 - VM SDK
 - OPSEC
 - JDBC
 - Telnet
 - SSH
 - JMX
 - Por exemplo, alerta quando um processo ou serviço é interrompido.
- Todos os componentes de recolha (sonda), devem possuir uma versão em uma appliance por forma a serem instalados na infraestrutura Vmware ou Hyper-V;
- Integração com Active Directory e Domain Controllers em Windows, recolha, análise de logs e eventos;
- Os métodos de autenticação externa devem ser suportados e incluir:
 - Active Directory;
 - RADIUS.
- Integração feeds de Threat Intelligence (TI);
- Monitorização e produção de relatórios de segurança, com os eventos relevantes (eventos de segurança, logs, vulnerabilidades, spam, phishing, IPs ou URLs, vírus, malware, etc);
- Acesso baseado em perfis de utilização, permitindo que diferentes perfis tenham acesso a diferentes níveis de visualização;
- Correlação de eventos, permitindo relacionar os eventos de várias localizações em tempo real;
- Possibilidade de efetuar análise personalizada de log utilizando scripts, ou equivalente;
- Compatibilidade com equipamentos e sistemas, tais como:
 - Devices de rede (inclui-se nestes devices: Switches, Routers, Wireless Lan);
 - Devices de segurança (inclui-se nestes devices: Firewalls, Network IPS);
 - Servidores com sistemas operativos Windows e Linux;
 - Servidores web (Apache, IIS);
 - Base dados Oracle e Microsoft;
 - Equipamentos de Storage;
 - Infraestrutura de Virtualização nomeadamente VmWare e Microsoft Hyper.
- Gestão de versões de configurações do equipamento;
- Capacidade de recolher a configuração do dispositivo de rede, identificar mudanças e fornecer comparação lado-a-lado;
- Recolha das versões de software instaladas;
- Serviços de deteção de mudanças de configuração nos equipamentos;
- Serviço de alarmística, incluindo arquivo de falhas e serviços de notificação (capacidade de forwarding de eventos e alarmes para um sistema de gestão de falhas a um nível superior ou outro, sob a forma de email);
- Possibilidade de remediação automática baseada em scripts;

- Monitorização e produção de relatórios de performance e utilização dos equipamentos (ao nível da porta e VLAN);
- Monitorização dos níveis ambientais dos equipamentos (Temperatura, humidade, fan's);
- Os dispositivos podem ser monitorizados através de Agentes, Windows Log Forward, PowerShell, SSH;
- Capacidade de coletar eventos do Windows via WMI e agente.

A plataforma de monitorização deverá contemplar pelo menos 1000 EPS (Eventos por Segundo), das fontes padrão identificadas como necessárias e fundamentais pela Entidade Adjudicante, até ao total de 50 fontes de informação.

5. Renovação e modernização da Solução de Comunicações Unificadas

A Entidade Adjudicante pretende renovar a atual plataforma de comunicações de voz, introduzindo novas funcionalidades em linha com as atuais tendências de mercado que incorporem comunicações unificadas (voz, IM, Presence, Video One-2-One e Salas Vídeo Conferência) e solução de reuniões on-line.

De forma a manter o suporte e permitir a continua evolução da plataforma, assim como a adoção de uma estratégia de gestão de equipamentos, utilizadores e funcionalidades mais flexível e otimizada, substituindo o modelo de licenciamento atualmente em produção, para um modelo de licenciamento / suporte subscricional.

Este modelo tem como objetivo manter a solução de comunicações sempre atualizada e ter uma maior previsibilidade de custos de suporte e manutenção.

É também o objetivo na adoção do modelo de subscrição, a possibilidade de em cada final de ciclo de renovação, ser possível efetuar uma atualização quanto ao número de subscrições e o seu nível funcional, no sentido de otimizar a solução implementada tornando-a mais eficiente e flexível.

A solução deverá basear-se no modelo de subscrição para as componentes core, nomeadamente para as plataformas de Call Control, Contact Center sendo a sua instalação mantida nos datacenters da Entidade Adjudicante e que são alvo de upgrade no âmbito desta consulta.

5.1. Vídeo

#	REQUISITO
a)	A solução apresentada deverá permitir uma total integração de terminais de vídeo
b)	Deverá ser similar a utilização de um terminal de voz e/ou de vídeo, registando-se os dois na mesma solução
c)	Deverá ser SIP com suporte de BFCP para partilha de documentos/desktop
d)	Deverá suportar H.264 AVC

#	REQUISITO
e)	A solução deverá suportar chamadas de vídeo para sistemas externos à rede da OE, através da Internet (B2B/B2C)
f)	Deverá suportar a interligação de terminais de videoconferência SIP ou H.323;
g)	Deverá ter a capacidade de Network Address Translation (NAT) traversal, permitindo as comunicações externas à firewall do OE de forma segura
h)	Deverá disponibilizar serviços de discovery e relay STUN (Session Traversal Utilities for NAT);
i)	Deverá ser compatível com o protocolo STUN
j)	Deverá disponibilizar uma interface simples
k)	Deverá ter escalabilidade para várias chamadas em simultâneo
l)	Deverá suportar marcação por URI - Uniform Resource Identifier
m)	Deverá permitir a gestão de largura de banda dedicada às comunicações de vídeo
n)	Deverá existir a possibilidade dos clientes móveis deverão poder aceder ao OE via rede GSM/4G, sem necessidade de estabelecer VPN.

5.2. Aplicações – Comunicações Unificadas – Desktop

#	REQUISITO
a)	A solução proposta deverá permitir a utilização de um cliente de colaboração unificado com as funcionalidades de voz, vídeo, Instant Messaging/Chat, Presença e Partilha de Conteúdos
b)	O cliente para desktop deverá ser um cliente rico de comunicações unificadas integrando Presença, Mensagens Instantâneas, Voz, Vídeo, Correio de Voz e Conferências Web
c)	O cliente unificado deverá suportar standards de voz G. 711, G. 729a, G. 722, iLBC
d)	O cliente unificado deverá suportar o codec de vídeo H.264 A VC
e)	O cliente deverá suportar diferentes formatos de vídeo: QCIF, CIF, VGA, e 720p até 30 frames por segundo
f)	O cliente proposto deverá ser XMPP para IM e Presença e SIP para Voz e Vídeo
g)	O cliente unificado deverá suportar alta disponibilidade
h)	O cliente unificado deverá ter a capacidade de marcação de pacotes para QOS de voz e de vídeo
i)	O cliente unificado deverá implementar Call Admission Control, de forma integrada com o sistema de comunicações
j)	O cliente unificado deverá operar em dois modos para voz e vídeo, definidos pelo utilizador: • softphone, o media é terminado diretamente no cliente de desktop; deskphone control, o media é terminado no telefone de secretaria, permitindo ao utilizador o controlo do telefone de secretária a partir do cliente unificado
k)	O cliente unificado deverá permitir a ligação de vídeo HD para terminais de videoconferências
l)	O cliente unificado deverá estar disponível para a plataforma Windows e Mac
m)	O cliente unificado deverá permitir a funcionalidade de chat, mantendo um histórico das conversações
n)	O cliente unificado deverá ainda permitir a criação de group chats na mesma interface
o)	O cliente unificado deverá disponibilizar o histórico de todas as comunicações, incluindo chamadas perdidas e recebidas e correio de voz
p)	A interface do cliente unificado deverá ser simples e intuitiva

#	REQUISITO
q)	O cliente unificado deverá integrar a presença telefónica e de calendário
r)	Deverá ser possível a integração com ferramentas Microsoft Office e principais browsers (como por exemplo: Internet Explorer e Firefox)
s)	O cliente unificado deverá ter uma interface completa de funcionalidades de voz e vídeo, nomeadamente, a colocação de chamada em espera, realização de conferências, colocação da chamada em mute e transferência de chamada

5.3. Aplicações – Clientes de comunicações para equipamentos móveis (Cliente de Mobilidade)

#	REQUISITO
a)	O cliente de mobilidade deverá permitir a utilização do equipamento móvel como um terminal de comunicações IP integrado na solução proposta
b)	O cliente de mobilidade deverá permitir ao utilizador efetuar, receber e gerir as chamadas da sua extensão corporativa, a partir do equipamento móvel
c)	O cliente de mobilidade deverá estar disponível automaticamente para utilização através de conectividade Wi-Fi ou VPN à rede corporativa
d)	O cliente de mobilidade deverá ser gerido e registado na plataforma central de comunicações proposta, do ponto de vista de administração deverá comportar-se como qualquer outro terminal da solução
e)	O cliente de mobilidade deverá integrar com o deskphone permitindo de forma transparente passar a chamada de um terminal para o outro
f)	O cliente deverá ter a capacidade de fazer conferências de voz, colocação de chamada em espera e transferência de chamada
g)	O cliente de mobilidade deverá integrar com a lista telefónica do terminal móvel. Deverá ser possível pesquisar um contacto e fazer uma chamada diretamente através do cliente de mobilidade
h)	O cliente de mobilidade deverá integrar com o diretório corporativo (Active Directory ou LDAP)
i)	Durante uma chamada deverá ser possível fazer o handover para a rede GSM sem Interrupção da chamada, caso o utilizador saia da cobertura Wi-Fi
j)	Deverá ser possível aceder ao correio de voz através do cliente de mobilidade
k)	A solução a propor deverá incluir a possibilidade de efetuar e/ou receber chamadas a partir da internet através do cliente de mobilidade sem recurso a VPN corporativas.

5.4. Serviço de Vídeo Conferência On-line (Cloud)

#	REQUISITO
a)	O serviço de vídeo conferência on-line (Cloud), tem de ser do mesmo fabricante que a solução de comunicações unificadas.
	A solução deverá ser gerida na mesma plataforma da solução de eventos on-line em produção (cisco Control Hub)
b)	Serviço de conferências de voz, vídeo e conteúdos online, acessível por subscrição de utilizadores nomeados, identificados por um endereço de mail.
c)	Licenciado por utilizadores nomeados com acesso as seguintes plataformas (ou equivalentes) Webex Meetings Suite, Subscrição para 5 user inclui o acesso a: • Webex Meetings (1000 participantes) • Webex Trainings (1000 participantes) • Webex Events (1000 participantes) • Webex Support (5 participantes)

#	REQUISITO
e)	Gravação do áudio, vídeo e os conteúdos das reuniões (sessões) a pedido do utilizador
f)	60GB de armazenamento disponível na Cloud para sessões gravadas
g)	Agendamento de reuniões, pelo Organizador, no Outlook ou no portal (site)
h)	Registo de <i>endpoints video</i> das salas no serviço online
i)	Estar Integrado com a solução de comunicações unificadas On-Premises
j)	Organizador e convidados entram na reunião por, Web Browser no PC, aplicação nos dispositivos móveis Android e Apple e sala de videoconferência
g)	Partilha de conteúdos: qualquer participante pode partilhar documentos, apresentações e aplicações
h)	Cada organizador tem uma sala pessoal acessível por: • Por Web-Browser • Por videoconferência
k)	Anotações: durante a partilha de conteúdos, podem fazer-se anotações, que ficam visíveis para todos os participantes

5.5. Segurança

#	REQUISITO
a)	A solução deverá implementar funções de segurança em todos os componentes tais como os terminais, central, gateways, aplicações, entre outros
b)	A solução deverá efetuar a separação do tráfego de voz, vídeo e dados, garantido a qualidade da voz e vídeo sobre os dados;
c)	A solução proposta deverá permitir que apenas terminais autorizados se possam registar;
d)	A segurança da configuração do telefone deverá ser garantida para que não possa ser copiada;
e)	Como alguns telefones irão estar em zonas de acesso público (corredores, salas de reunião, etc.), a solução deverá implementar funcionalidades de segurança que limitam a utilização desses terminais;
f)	A solução deverá implementar mecanismos que previnam que os telefones possam receber um upgrade de firmware malicioso;
g)	A solução deverá implementar mecanismos de encriptação (em todos os seus elementos).

5.6. Dimensionamento da solução de comunicações unificadas e reuniões on line

O Adjudicatário deverá fornecer as seguintes soluções em modelo de subscrição contemplando todo o software e equipamentos necessários ao correto funcionamento da solução de comunicações unificadas de acordo com o seguinte quadro:

Subscrição A-FLEX-3 - 36 Meses.		
Callmanager, Collaboration Flex Plan 3.0		
A-FLEX-3	Collaboration Flex Plan 3.0	1
Initial Term - 36.00 Months		
SVS-FLEX-SUPT-BAS	Basic Support for Flex Plan	1
A-FLEX-FILESTG-ENT	File Storage Entitlement	2960
A-FLEX-PROPACK-ENT	Pro Pack for Cisco Control Hub Entitlement	149
A-FLEX-NUPL-P	NU On-Premises Calling Professional	144
A-FLEX-NUPL-A	NU On-Premises Calling Access	14
A-FLEX-STD-CUBE	CUBE Standard Trunk Session License	45
A-FLEX-SRST-E	SRST Endpoints (1)	300
A-FLEX-P-PRO	Unified Communications Manager Smart License - Pro (1)	143
A-FLEX-P-ACC	Access Smart License (1)	14
A-FLEX-P-UCXN	Unity Connection Smart License (1)	144
A-FLEX-P-ER	Emergency Responder Smart License (1)	443
A-FLEX-SW-12.5-K9	On-Premises & Partner Hosted Calling SW Bundle v12.5 (1)	1
A-FLEX-MSG-NU-ENT	Messaging Named User Entitlement (1)	148
Flex Contact Center		
A-FLEX-CC	Flex Contact Center	1
SVS-FLEX-SUPT-BAS	Basic Support for Flex Plan	1
A-FLEX-PJXPC	Flex CC On-Premises UCCX Premium Concurrent Agent	9
A-FLEX-J-AGT-RTU	On-Premises PCCE & UCCE, Hosted CCE & CCX Agent RTU	1
A-FLEX-05-12.5-K9	On-Premises UCCX Standard & Premium Media Kit v12.5	1
A-FLEX-PJX-SVR12.5	On-Premises UCCX Standard & Premium Server v12.5 (incl 12.6)	1
A-FLEX-PJXPAGT12.5	On-Premises UCCX Premium Agent License v12.5	9
Webex Meetings Suite		
A-FLEX-NUM-EE	NU Webex Meetings - Meetings Suite	5
A-AUD-VOIP	Included VoIP (1)	1
A-AUD-EDGEAUD-USER	Webex Edge Audio (1)	5
A-AUD-TOLLDIALIN	Meetings Toll Dial-In Audio (1)	5
A-FLEX-NBR-STG	Webex Cloud Recording Storage Entitlement	5
A-FLEX-MSTE-NU-ENT	Meeting Suite Named User Entitlement (1)	5

REQUISITOS	QUANTIDADE
Solução de Aplicação de Colaboração em equipa - mensagens individuais e em grupo e partilha de arquivos em salas virtuais com conteúdo e contexto persistentes para melhores interações da equipa	144

REQUISITOS	QUANTIDADE
Utilizadores Avançados, este utilizador terá instalado no seu posto de trabalho um telefone físico também deverá ter acesso à utilização de um cliente de colaboração unificado com as funcionalidades de voz, vídeo, Instant Messaging/Chat, Presença e Partilha de Conteúdos. Estes utilizadores poderão ter associados até 10 dispositivos	144
Licenciamento basico, este perfil não terá utilizador associado, destina-se a terminais analógicos ou para instalação em zonas comuns. Licenciamento com acesso a funcionalidades básicas de telefonia.	14
Utilizadores licenciandos com acesso a VoiceMail	144

REQUISITOS	QUANTIDADE
Serviço de Vídeo Conferência On-line (Cloud)	
Organizador das reuniões (Utilizador nomeado) Acesso a: • Webex Meetings (1000 participantes) • Webex Trainings (1000 participantes) • Webex Events (1000 participantes) Webex Support (5 participantes)	5

As quantidades e funcionalidades acima descritas são adicionais as funcionalidades em produção, não será admitido qualquer downgrade das funcionalidades da solução em produção.

5.7. Serviços de profissionais

Deveram estar contemplados no mínimo os seguintes serviços de upgrade da solução de comunicações:

Descrição dos Serviços

UPG Unified Communications Manager 14

INICIAR

Reunião de kickoff

DEFINIR

Levantamento de requisitos

Levantamento de requisitos para a instalação da solução (entrar nos equipamentos actuais e tirar inventario e configs)

Fazer levantamento das licenças existentes (LCU) e Invocar PUT/MCE (download SWs necessários para migração) +

UCSS/SWSS + Smart License

Verificar compatibilidades hw/sw (versões actuais/futuras , firmwares telefones , modelos telefons , versões vmware,...)

Elaborar e Enviar pré-requisitos para a implementação

Levantamento/Backup das base de dados (a partir desta altura a base de dados fica "congelada" para alterações)

CONSTRUIR

Solução de Colaboração - UC

Fazer o upgrade do CUCM PUB e SUB (a definir com ou sem PCD ou Direct Refresh Upgrade) + Upg HD ova 160G

Upgrade de CIMC e Esxi

Upgrade de memória dos servidores

Instalação e configuração dos Expressways para MRA

Re-hosting das licenças CUCM + Integração/Migração Smart License + Inst.Servidor Satellite

Configuração Webex App em UC mode

Configuração Devices Webex App (Jabber) no CUCM

Instalação e configuração de Conector de calendário Híbrido(Expressway C)

Upgrade de Easylynq + Conector novo

Upgrade de UCCX + Licenciamento + Testes e ensaios

ENTREGAR

Colocação em Serviço

Preparar os certificados dos telefones para migração de cluster.

Update do Firmware dos telefones

Migração do CUCM + Switch de versão

Testes e Ensaios

Acompanhamento em produção da nova solução (Next Business Day + Tuning da rede)

Formacao (Preparacao + 1 sessão a power users de 1h)

FECHAR

Actualização da Documentação de projeto

GESTÃO

Gestão de Projeto

5.8. Formação

A proposta deverá incluir formação a ministrar às pessoas que irão trabalhar regularmente com a solução e que devem mandaticamente incidir nas seguintes soluções/áreas:

- a) Solução de Comunicações Unificadas;
- b) Solução de Contact Center;
- c) Serviço de Vídeo Conferência Online
- d) adequados à complexidade e à dimensão da implementação. A formação deverá prever uma parte "on-job", ou seja, ministrada no local de trabalho e com a presença dos formadores da empresa a quem for adjudicada esta prestação de serviços;
- e) A formação a propor deverá contemplar dois níveis de utilizador:
 - o Utilizadores finais em termos de utilização (ex: Utilizador final, telefonistas, agentes e supervisores do Contact Center);
 - o Elementos da área das tecnologias de informação e comunicação no âmbito da administração e gestão do sistema (ex: Administrador IT).
 - o No mínimo deverá ser assegurado 40 Horas dedicadas à formação dos colaboradores da Entidade Adjudicante.

5.9. Dimensionamento do suporte solução de comunicações unificadas *On-Premises*

O Adjudicatário deverá considerar serviços de Manutenção, Configuração, Suporte, Reparação, Substituição de equipamentos com avaria, atualização e instalação de firmwares, novas versões dos produtos/Sistemas operativos e instalação de Major Releases nas versões mais recentes.

Sede (Lisboa, nº 75)	Código Produto	Designação	Qtd
CORE	WS-C3850-24XS-S	Cisco Catalyst 3850 24 Port 10G Fiber Switch IP Base	2
	S3850UK9-163	UNIVERSAL	2
	PWR-C1-350WAC/2	350W AC Config 1 SecondaryPower Supply	2
	CAB-TA-EU	Europe AC Type A Power Cable	4
	STACK-T1-50CM	50CM Type 1 Stacking Cable	2
	CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	2
Interfaces para ligação ao Sup7L-E do Catalyst 4500 existente	GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	27
	SFP-H10GB-CU5M=	10GBASE-CU SFP+ Cable 5 Meter	14
ACESSO	WS-C4506E-S7L+96V+	4506-E Chassis, two WS-X4648-RJ45V+E, Sup7L-E, LAN Base	1
	CAB-CON-C4K-RJ45	Console Cable 6ft with RJ-45-to-RJ-45	1

	WS-X4648-RJ45-E	Catalyst 4500 E-Series 48-Port 10/100/1000 (RJ45)	1
	C4500E-S7L-DEFAULT	Default WS-X45-SUP7L-E with WS-X4648-RJ45V+E Bundle	1
	S45EUK9-33-1511SG	CAT4500e SUP7-E/SUP7L-E Universal Crypto Image	1
	PWR-C45-2800ACV	Catalyst 4500 2800W AC Power Supply (Data and PoE)	1
	CAB-AC-2800W-EU	Europe Power Cord	2
	PWR-C45-2800ACV/2	Catalyst 4500 2800W AC Power Supply (Data and PoE)	1
	WS-X45-SUP7L-E	Catalyst 4500 E-Series Supervisor LE, 520Gbps	1
	WS-X4648-RJ45V+E	Catalyst 4500 E-Series 48-Port PoE+ Ready 10/100/1000(RJ45)	2
	C4500E-LB	License for Lan Base	1

Sede (Lisboa, nº 68)	Código Produto	Designação	Qtd
ACESSO	WS-C3560X-24P-S	Catalyst 3560X 24 Port PoE IP Base	1
	WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	1

DR (Coimbra)	Código Produto	Designação	Qtd
CORE	WS-C3850-24XS-S	Cisco Catalyst 3850 24 Port 10G Fiber Switch IP Base	1
	S3850UK9-163	UNIVERSAL	1
	PWR-C1-350WAC/2	350W AC Config 1 SecondaryPower Supply	1
	CAB-TA-EU	Europe AC Type A Power Cable	2
	STACK-T1-50CM	50CM Type 1 Stacking Cable	1
	CAB-SPWR-30CM	Catalyst 3750X and 3850 Stack Power Cable 30 CM	1
Interfaces para ligações a Servidores			
	GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	18
	SFP-H10GB-CU5M=	10GBASE-CU SFP+ Cable 5 Meter	6

Secções Regionais	Código Produto	Designação	Qtd
ACESSO	SG500X-24P-K9-G5	24-Port Gig POE with 4-Port 10-Gig Stackable Managed Switch	6
	WS-C2960X-24PS-L	Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base	5
	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	5

Firewalls	Código Produto	Designação	Qtd
Sede (Lisboa, nº 75)	ASA5516-FPWR-K9	ASA 5516-X with FirePOWER services, 8GE, AC, 3DES/AES	1
	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
DR (Coimbra)	ASA5516-FPWR-K9	ASA 5516-X with FirePOWER services, 8GE, AC, 3DES/AES	1

	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
Cisco Firepower Management Center for 2 devices	FS-VMW-2-SW-K9	Cisco Firepower Management Center,(VMWare) for 2 devices	1

Sede (Lisboa, nº 75)			
Telefonia IP	Código Produto	Designação	Qtd
SERVIDOR	BE6M-M4-K9=	Cisco Business Edition 6000M Svr (M4), Export Restricted SW	1
	UCSC-PSU1-770W=	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	1
	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	1
	CAB-9K10A-EU=	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	1
Gateway CUBE - 30 Canais	CISCO2901-V/K9	Cisco 2901 Voice Bundle, PVD3-16, UC License PAK, FL-CUBE10	1
	S29UK9-15204M	Cisco 2901-2921 IOS UNIVERSAL	1
	FL-CUBEE-5	Unified Border Element Enterprise License - 5 sessions	1
	FL-CUBEE-25	Unified Border Element Enterprise License - 25 sessions	1
	PWR-2901-AC	Cisco 2901 AC Power Supply	1
	CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
	SL-29-IPB-K9	IP Base License for Cisco 2901-2951	1
	SL-29-UC-K9	Unified Communication License for Cisco 2901-2951	1
	ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	1
	MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)	1
	MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR	1
	PVD3-16	16-channel high-density voice DSP module	1

DR (Coimbra)			
Telefonia IP	Código Produto	Designação	Qtd
SERVIDOR	BE6M-M4-K9=	Cisco Business Edition 6000M Svr (M4), Export Restricted SW	1
	UCSC-PSU1-770W=	770W AC Hot-Plug Power Supply for 1U C-Series Rack Server	1
	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	1
	CAB-9K10A-EU=	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	1
Gateway CUBE - 15 Canais	ISR4321-V/K9	Cisco ISR 4321 Bundle, w/UC License, CUBE-10	1
	CAB-AC-C5-EUR	AC Power Cord, Type C5, Europe	1
	FL-CUBEE-5	Unified Border Element Enterprise License - 5 sessions	1

ENDPOINTS	Código Produto	Designação	Qtd
Gateways Analógicas de 2 portas			
	VG202	Cisco VG202 Analog Voice Gateway	7

CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	7
SVGXIPV-15001M	Cisco Voice Gateway 20x Series IP VOICE W/O CRYPTO	7
CAB-ETH-S-RJ45	Yellow Cable for Ethernet, Straight-through, RJ-45, 6 feet	7
PS-SWITCH-AC-3P	3 Prong C13/C14 On-Off AC Power Supply Switch	7
PWR-30W-AC	Power Supply 30 Watt AC	7

Telefones IP	Código Produto	Designação	Qtd
	CP-7962G=	Cisco UC Phone 7962, spare	9
	CP-7915=	7915 UC Phone Grayscale Expansion Module	9
	CP-SINGLFOOTSTAND=	Footstand kit for single 7914, 7915, or 7916	9
	CP-7942G=	Cisco UC Phone 7942, spare	9
	CP-6921-C-K9=	Cisco UC Phone 6921, Charcoal, Standard Handset	103
	CP-7841-K9=	Cisco UC Phone 7841	5
	CP-7821 K9=	Cisco UC Phone 7821	6

Telefones IP Wireless	Código Produto	Designação	Qtd
	CP-7925G-E-K9=	Cisco 7925G ETSI; Battery/Power Supply Not Included	11
	CP-7925G-SW-K9-E	Cisco 7925G Software, ETSI	11
	CP-BATT-7925G-STD=	Cisco 7925G Battery, Standard	11
	CP-DSKCH-7925G-BUN	Cisco 7925G Desk Top Charger, Power Supply, AC Power Cord	11
	CP-DSKCH-7925G	Cisco 7925G Desk Top Charger	11
	CP-PWR-DC7925G-CE	Cisco 7925G Desk Top Charger Power Supply For Europe	11
	CP-8821	Cisco 7925G ETSI; Battery/Power Supply	1

Software de Taxação	Código Produto	Designação	Qtd
	ELQS0000150	EasyLynq Server, 150 Extensões	1
	ELSAG020200	Agente PBX para CUCM x	1
	ELSPA000001	Migração do agente CallManager x	1
		Migração do EasyLynq Server em 2008 R2 para Windows server 2012 R2 ou superior	1

PARTNER SUPPORT SERVICE	Código Produto	Designação
Sede (Lisboa, nº 75)		
CORE	CON-PSRT-WSCX3852	WS-C3850-24XS-S - PRTNR SS 24x7x4 Cisco Catalyst 3850 24 Port 10G Fiber Sw
ACESSO	CON-PSRT-C4506S7L	WS-C4506E-S7L+96V+ - PRTNR SS 24x7x4 4506-E Chassis,two WS-X4648-RJ45V+E,Sup7

Sede (Lisboa, nº 68)		
ACESSO	CON-PSRT-3560X2PS	WS-C3560X-24P-S - PRTNR SS 24x7x4 Catalyst 3560X 24 Port PoE IP Base
	CON-PSRT-WSC224SL	WS-C2960X-24PS-L
DR (Coimbra)		
CORE	CON-PSRT-WSCX3852	WS-C3850-24XS-S - PRTNR SS 24x7x4 Cisco Catalyst 3850 24 Port 10G Fiber Sw
Secções Regionais		
ACESSO	CON-PSRT-SG5039G5	SG500X-24P-K9-G5 - PRTNR SS 24x7x4 24-Port Gig POE with 4-Port 10-Gig Stackabl
	CON-PSRT-WSC224SL	WS-C2960X-24PS-L

PARTNER SUPPORT SERVICE	Código Produto	Designação
Firewalls		
Sede (Lisboa, nº 75)	CON-PSRT-ASA556F9	ASA5516-FPWR-K9 - PRTNR SS 24x7x4 ASA 5516-X with FirePOWER services, 8GE ASA with FirePOWER Services Advanced Malware Protection
DR (Coimbra)	CON-PSRT-ASA556F9	ASA5516-FPWR-K9 - PRTNR SS 24x7x4 ASA 5516-X with FirePOWER services, 8GE ASA with FirePOWER Services Advanced Malware Protection
Cisco Firepower Management Center for 2 devices	CON-PSUU-VMW2	FS-VMW-2-SW-K9

Telefonia IP

PARTNER SUPPORT SERVICE	Código Produto	Designação
Sede (Lisboa, nº 75)		
SERVIDOR	CON-PSRT-BE6M4M4K	BE6M-M4-K9= - PRTNR SS 24x7x4 Cisco Business Edition 6000M Svr (M4), E
Gateway CUBE - 30 Canais	CON-PSRT-2901V	CISCO2901-V/K9 - PRTNR SS 24x7x4 Cisco 2901 Voice Bun

Telefonia IP

PARTNER SUPPORT SERVICE	Código Produto	Designação
DR (Coimbra)		
SERVIDOR	CON-PSRT-BE6M4M4K	BE6M-M4-K9= - PRTNR SS 24x7x4 Cisco Business Edition 6000M Svr (M4), E
Gateway CUBE - 15 Canais	CON-PSRT-ISR4321V	ISR4321-V/K9 - PRTNR SS 24x7x4 Cisco ISR 4321 UC Bundle, PVD4-32, UC L

Telefonia IP		
PARTNER SUPPORT SERVICE	Código Produto	Designação
ENDPOINTS		
Gateways Analógicas de 2 portas	CON-PSRT-VG202	VG202 - PRTNR SS 24x7x4 Cisco VG202 Analog Voice Gateway
Telefones IP	CON-PSRT-CP7962	CP-7962G= - PRTNR SS 24x7x4 Cisco Unified IP Phone 7962
	CON-PSRT-CP7915	CP-7915= - PRTNR SS 24x7x4 7915 IP Phone Grayscale Expansion Module
	CON-PSRT-CP7942	CP-7942G= - PRTNR SS 24x7x4 Cisco Unified IP Phone 7942
	CON-PSRT-21CK	CP-6921-C-K9= - PRTNR SS 24x7x4 Cisco Unified IP Phone 6921, Char, STD
	CON-PSRT-CP7841K9	CP-7841-K9= - PRTNR SS 24x7x4 Cisco UP Phone 7841
	CON-PSRT-CP7821K9	CP-7821-K9= - PRTNR SS 24x7x4 Cisco UP Phone 7821
Telefones IP Wireless	CON-PSRT-8821	CP-8821-E-K9= - PRTNR SS 24x7x4 Cisco 8821 FCC; CM/CME UL Req'd; Battery
	CON-PSRT-7925G1K	CP-7925G-E-K9= - PRTNR SS 24x7x4 Cisco 7925G FCC; CM/CME UL Req'd; Battery
	CON-PSRT-CP-DSKCH	CP-DSKCH-7925G-BUN - PRTNR SS 24x7x4 Cisco 7925G Desk Top

PARTNER SUPPORT SERVICE	Código Produto
Serviços Eurofluxo	Easylynq Server

5.9.1 Upgrade memória ram em dois servidor Cisco Business Edition 6000M Svr (M4)

Atualmente cada servidor tem instalado 32 GB de memoria ram, pretende-se instalar mais 64GB em cada servidor para que cada servidor fique com um total de 96GB de memoria ram. Requisitos mínimos para o upgrade de memoria:

Sede (Lisboa, nº 75)		
Código Produto	Designação	Qtd
UCS-MR-1X162PRUA-RF	16GB DDR4 - 2133MHZ DIMM/PC4-17000 dual Rank 4/1,2c	4

DR (Coimbra)		
Código Produto	Designação	Qtd
UCS-MR-1X162PRUA-RF	16GB DDR4 - 2133MHZ DIMM/PC4-17000 dual Rank 4/1,2c	4

Os Dimm de memoria ram devem ser iguais ou superiores a 16GB por unidade.

5.9.2. Requisitos mínimos para o Servidor de Comunicações Voz

- a) A solução de telefonia é composta por dois Servidores, Cisco Unified Communications, instalados numa plataforma de hardware virtualizada que assegura todo o processamento de chamadas da rede de comunicações IP em redundância. Estes servidores encontram-se implementados na Sede da Ordem dos Enfermeiros e na Secção Regional de Coimbra e são responsáveis por todas as comunicações de voz que são originadas ou têm como destino terminais IP, independentemente da localização do terminal.
- b) Interface Web-based que permite uma configuração quer do próprio sistema quer dos dispositivos terminais, quer estejam locais ou remotos.
- c) Disponibilizar, sem necessidade de hardware específico para processamento de voz, todas as funcionalidades de comutação e serviços telefónicos para dispositivos de telefonia IP, tais como: telefones, gateways e aplicações multimédia.
- d) Outros serviços de dados, voz e vídeo como Unified Messaging e Interactive Response System (IVR) devem interagir com a Unified Communications Manager através da disponibilização a parceiros de APIs (application programming interfaces).
- e) Disponibilização os utilizadores que vejam a informação de texto apresentada nos telefones na sua língua nativa, bem como recebam os tons de sinalização igual aos utilizados na rede pública do seu país.
- f) Possibilidade de o administrador do sistema disponibilizar um serviço conhecido por mobilidade de extensão. Este serviço deverá permitir associar o telefone e o perfil de utilizador a qualquer telefone da mesma gama. Utilizar o número de identificação pessoal (PIN) da mobilidade de extensão para iniciar sessão num equipamento telefónico, o número de telefone que lhe foi atribuído, bem como as definições que estabeleceu a partir das páginas Web de opções do utilizador que estão associadas a esse telefone.

5.9.3. Funcionalidades mínimas que o Cisco Unified Communications deverá garantir:

- Funcionalidades de Utilizador - Callback entre telefones IP (modelos 69xx, 79xx, 89xx e 99xx) em caso de ocupado e não atendimento.
- Aplicação IPMA, implementando a função Diretor / Secretária:
- Funções de Diretor (redireccionamento ou transferência imediata, não incomodar, redireccionamento de todas as chamadas, interceção de chamadas, filtragem de chamadas com base no número chamador)
- Funções de Secretária (Intercom, redireccionamento ou transferência imediata, redireccionamento de todas as chamadas, gestão das chamadas do Diretor através de consola)
- Auto Atendant com funcionalidade de queueing
- Web Dialer (aplicação Pc click-to-dial)
- Video (suporte SCCP, H.323 e SIP)
- Funcionalidades de Sistema

- Q.SIG ISO basic call com general functional procedures
- Encriptação das chamadas
- Alternate Automatic Routing – AAR
- Esta funcionalidade permite a remarcação automática de um número de destino com manipulação de dígitos (possivelmente apresentando o DDI de acesso ao destino via rede pública) em caso de não ser possível a marcação pela rede privada devido a limitações de largura de banda em Locations.
- Funcionalidades de Administração
- Multilevel Administration Access (MLA) – permite definir o acesso à plataforma Cisco Unified Communications Manager com vários níveis, de modo a criar contas de utilizadores com perfis diferentes.
- HTTPS – Administração da plataforma via Web mas de uma forma segura.

5.9.4. Requisitos mínimos de Gateways de Voz

- Na Manutenção/Suporte de uma rede multiserviços com integração de voz e dados é necessário dispor de equipamentos que efetuem a interface entre a infraestrutura de comunicações baseada na comutação de pacotes (IP) e o mundo da voz convencional (redes públicas de Operadores de Telecomunicações e/ou centrais telefónicas convencionais privadas). Os equipamentos que asseguram estas funcionalidades são os Gateways de voz.
- Como gateway de voz entre a solução de telefonia IP e a PSTN deverá ser configurado um router da Cisco não inferior à série. O equipamento considerado da Cisco deverá ser dotado de licenciamento CUBE para ligação à rede pública através de um SIP trunk. Este equipamento deverá possuir ainda, DSPs disponíveis para garantir os mecanismos de transcoding necessários para assegurar o correto funcionamento da solução;
- Serviços mínimos de Mobilidade;
- No contexto da mobilidade na Ordem dos Enfermeiros, as Comunicações Unificadas representam uma plataforma avançada de gestão das comunicações dos trabalhadores móveis. Reencaminhamento de chamadas, mensagens unificadas, controlo e bloqueio de chamadas, gestão de presenças, cumprimento de normas da organização, são algumas das funcionalidades que deverão estar garantidas no sentido de aumentar a eficiência e a produtividade dos utilizadores, ao ser adotada uma plataforma unificada;
- A utilização de uma central telefónica IP única (centralizada ou distribuída) deverá ser implementar a funcionalidade de “Extension Mobility”. Com a utilização desta funcionalidade deverá ser possível que qualquer colaborador tenha acesso à sua extensão telefónica independentemente do local em que se encontra. Por exemplo, um colaborador que tenha a necessidade de se deslocar de Lisboa para os Açores poderá efetuar o login num telefone existente nesse local, e importar o seu perfil de utilizador para esse telefone. A partir dessa altura, aquele telefone passa a ter permissões para realização de chamadas de acordo com o perfil do utilizador, independentemente do tipo de permissões que o telefone tinha originalmente. Adicionalmente, qualquer chamada proveniente do exterior ou de outra extensão interna com destino

- ao DDI desse colaborador será entregue no telefone em que o mesmo se encontra;
- A utilização de uma solução de Comunicações Unificadas, para além das funcionalidades standard de processamento de chamadas, deverá disponibilizar funcionalidades de mobilidade tais como o “single number reach” que possibilita que a aplicação efetue de uma forma inteligente a gestão de filtros e de rotas, para além de permitir que de uma forma totalmente automática as chamadas com destino ao DDI de um determinado colaborador possam ser encaminhada para um terminal alternativo, como por exemplo, o telemóvel do mesmo. Assim, mesmo que o colaborador se encontre ausente, poderá continuar a estar contactável através do seu DDI. Esta funcionalidade pode ser ativada e desativada a partir do próprio telefone;
 - Associada a esta funcionalidade, deverá contemplar a funcionalidade de “Dial via Office”. A utilização do mecanismo “Dial via Office” deverá possibilitar que os colaboradores que habitualmente se encontram fora dos escritórios da Ordem dos Enfermeiros possam utilizar os telemóveis para realização de chamadas através dos recursos disponibilizados pela central telefonia IP existente no Escritório;

5.9.5. Requisitos mínimos Solução de IVR

- O Adjudicatário deverá garantir a atualização, manutenção e suporte da solução IVR, incluído a manutenção do atual fluxo, criação de novos fluxos e criação de Inquéritos de satisfação baseados na aplicação de IVR .

5.9.6. O Cisco Unified Contact Center Express Enhanced deverá considerar a solução de Contact Center.

A plataforma Cisco UCCX Enhanced deverá ser uma solução versátil e repleta de funcionalidades. Entre as diversas funcionalidades do Cisco Unified Contact Center Express deverá garantir:

- Registos da atividade do funcionamento do Contact Center através da geração de CCDRs (Contact Call Detail Records), guardadas numa base de dados relacional para posterior processamento;
- Capacidades de geração de Relatórios Históricos;
- Acesso completo à base de dados através de schemas publicados;
- Agente para o Cisco IP Phone 797x, 796x, 794x e IP Communicator;
- Suporte de Screen Pop Ups simples para recolha e disponibilização de informação;
- Sessões IVR Prompt e Collect incluídas;
- Tratamento de chamadas em queue incluído;
- Linear (hunt group);
- Circular (Grupo de distribuição);
- Agente disponível há mais tempo;
- Número chamador (ANI/DNIS);
- Hora, dia da semana, estatísticas real-time e condições em queue;
- Detecção de Overflow;
- Tratamento em queue customizável, incluindo música em espera e mensagens parametrizáveis;

- Enhanced Supervisor inclui Silent Monitoring, Call Barge-in e Call Intercept;
- As funcionalidades de Screen Pop Up incluem a integração com qualquer aplicação Windows, incluindo aplicações CRM;
- Suporte de gravação de chamadas a pedido, permitindo ainda a posterior escolha e reprodução de chamadas gravadas;
- Pop Up no ecrã para permitir que qualquer informação introduzida pelo cliente ou por informação interna seja visualizada no posto de trabalho do agente;
- Agente com o maior número médio de chamadas atendidas;
- Agente com o menor tempo de atendimento médio;
- Roteamento condicional de chamadas;
- Por perfil – Possibilidade de definição de até 150 perfis, cada um com até 10 níveis de competência. Cada agente pode estar associado até um máximo de 50 perfis de competência distintos;
- Por prioridades – em cada momento cada chamada pode ser reprioritizada, existindo 10 níveis possíveis de prioridade;

5.9.7. Requisitos mínimos para o Módulo de Relatórios

Requisitos mínimos para Funcionalidade / Tipo de Relatório
Viewing Reports. View reports for the entire contact center using the Historical Reports client.
Custom Reports. Generate custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures.
Integrated Self-Service Historical Reporting with Cisco Unified Contact Center Express Seat License
Application Performance Analysis report
Call-by-Call Contact Call Detail Record (CCDR) report
Traffic Analysis report
Integrated ACD Historical Reporting with Cisco Unified Contact Center Express Seat License
Agent Call Summary report
Agent Detail report
Agent Login Logout Activity report
Agent Not Ready Reason Code Summary report
Agent State Detail report
Agent State Summary report (by agent)
Agent State Summary report (by interval)
Agent Wrap-up Data Summary report
Agent Wrap-up Data Summary Detail report
Application Summary report
Call Custom Variables report
Called Number Summary Activity report
Common Skill Contact Service Queue Activity report
Contact Service Queue Activity report (by CSQ)

Contact Service Queue Activity report (by interval)
Contact Service Queue Activity report
Contact Service Queue Call Distribution Summary report
Contact Service Queue Priority Summary report
Contact Service Queue Service Level report
CSQ Agent Summary report
Detailed Call, CSQ, Agent report
Priority Summary Activity report

6. Governo do Serviço

Deverá ser apresentado o modelo de governo preconizado que deverá prever reuniões periódicas, criando assim uma estrutura hierárquica de serviço que envolve os níveis adequados de gestão.

Neste serviço deverão existir pelo menos os seguintes perfis, funções e experiência.

7. Gestor de Transição

- Planear as atividades de setup da transição do serviço;
- Definição de Milestone do projeto de setup;
- Organização e participação em reuniões de steering.

8. Certificações e experiência de Gestor Serviço

O Gestor de Transição deverá ser certificado em PMP (Project Management Professional), e deverá ter mais de 5 anos de experiência em projetos.

9. Gestor de Serviço

- Reunião de avaliação de realização dos objetivos do serviço;
- Define os objetivos do serviço e toma as decisões de alto nível para orientar a sua execução;
- Aprovação da introdução e/ou remoção de equipamentos no âmbito do Contrato.
- As reuniões da Gestão Contratual, deverão ser realizadas com uma periodicidade mínima trimestral e deverão conter os elementos de análise associados ao seu âmbito de atuação nomeadamente o desempenho do serviço. A sua estrutura definitiva será revista e acordada durante a fase de transição do serviço.

10. Gestão Operacional

- Realiza o seguimento diário da atividade do serviço;
- Garante a aplicação das normas, processos e metodologias definidas;
- Analisa potenciais riscos no serviço e define ações corretivas;
- Garante a participação dos elementos necessários ao desenrolar do serviço;
- Garante a disponibilidade dos meios;
- Revisão mensal da atividade do período em causa. Esta revisão deverá ter enfoque nos seguintes aspetos:
 - Avaliação e análise dos níveis de serviço – SLA's;

- Análise dos problemas do serviço;
- Definição de eventuais ações corretivas;
- Validação do planejamento para o próximo período;
- Concordância em relação a melhoria contínua de serviços;
- Gere e toma decisões sobre problemas não resolvidos durante o período regular do serviço.
- As reuniões da Gestão Operacional do Serviço, deverão ser realizadas com uma periodicidade mínima mensal e deverão conter os elementos de análise associados ao seu âmbito de atuação, com especial enfoque na análise e avaliação de:
- Revisão operacional do desempenho e segurança da rede e infraestrutura de maior relevância do período em causa. De forma ilustrativa e não exaustiva pretende-se rever a:
 - Caracterização dos incidentes corretivos e plano de ações;
 - Revisão do conjunto de ações necessárias e propostas para melhoria do serviço;
 - Revisão de incidentes recorrentes e propor o plano de ações para evitar futuras recorrências.

11. Modelo de Transição e Equipa de Gestão do Serviço

Os concorrentes têm de apresentar o planeamento de como pretendem implementar este serviço, tendo em consideração a metodologia ITIL.

12. Níveis de serviço (24/7)

Os níveis de serviço devem estar de acordo com as prioridades abaixo indicadas. Os níveis de serviço são aplicáveis e medidos numa base mensal:

Prioridade	Definição	Tempos de resposta/Intervenção remoto	Tempos de resposta/Intervenção local
Prioridade 1 (Severa)	Produtos com avaria, provocando falha grave nas aplicações, ou serviço em baixo, não estando disponíveis backups ou redundâncias e causando um impacto crítico na atividade da Entidade Adjudicante. Eventos de segurança, ataques ou ameaças externas dirigidas aos seus serviços e sistemas que possam de alguma forma comprometer o funcionamento e bom nome da organização. Exemplo: ataques de Ransomware	15 minutos	4 horas
Prioridade 2 (Alta)	Produtos com avaria, as aplicações estão seriamente degradadas, causando um impacto significativo na atividade do cliente. (Exemplo:	2 horas	8 horas

	Diminuição de performance da rede; velocidade; QoS; acesso exterior condicionado; etc.).		
Prioridade 3 (Normal)	A performance da rede ou aplicações estão degradadas, a sua funcionalidade encontra-se afetada, embora sem impacto significativo na atividade do cliente.	4 horas	Dia útil seguinte
Prioridade 4 (Baixa)	Pedidos de informação e esclarecimento. O cliente requer um pedido de informação, os pedidos nesta prioridade são prestados de forma remota.	8 horas	Dia útil seguinte
Prioridade 5 (Baixa)	Updates de major release, implementações/configurações de equipamentos, aplicações e sistemas a fornecer no contrato.	3 dias úteis após pedido	5 dias úteis após pedido
Prioridade 6 (Baixa)	Aplicar correções e melhorias resultantes do <i>Healthcheck appointment</i> , realizado aos equipamentos, sistemas e aplicações	5 dias uteis após a apresentação do relatório	5 dias uteis após a apresentação do relatório

Cláusula 23ª

Local de implementação

A implementação da solução será realizada na área geográfica constituída pelos seguintes locais:

1. Sede - Avenida Almirante Gago Coutinho, 75 - 1700-028 Lisboa;
2. Sede - Avenida Almirante Gago Coutinho, 68 - 1700-031 Lisboa;
3. Secção Regional do Sul- Rua Castilho, 59 – 1250-068 Lisboa;
4. Secção Regional do Norte – Rua Latino Coelho, 352 – 4000-314 Porto;
5. Secção Regional do Centro – Av. Bissaya Barreto, 185 – 3000-076 Coimbra;
6. Secção Regional da Região Autónoma dos Açores – R. Dr. Armando Narciso, 2 – 9500-185 Ponta Delgada;
7. Secção Regional da Região Autónoma da Madeira – R. Visconde Cancong, 35 (Santa Maria Maior) – 9060-036 Funchal.
8. Datatcenter 1 - situa-se na Sede- Avenida Almirante Gago Coutinho, 75 - 1700-028 Lisboa

Datatcenter 2 - situa-se na Secção Regional do Centro – Av. Bissaya Barreto, 185 – 3000-076 Coimbra