INSTITUTO DA MOBILIDADE E DOS TRANSPORTES, I.P.

Caderno de encargos

Tipo de procedimento:	**Concurso Publico**
Data de aprovação:	***07/12/2022***
Serviço requerente:	**DSSI**
Objeto:	**Aquisição de solução de software de segurança de endpoint**
CPV:	48730000-4 - Pacote de software de segurança
Procedimento n.º:	***2022/75245***

Índice

Parte I 5
Cláusulas jurídicas 5
Capítulo I 5
Disposições gerais do contrato 5
Cláusula 1.ª 5
Objeto e âmbito 5
Cláusula 2.ª 5
Contrato 5
Cláusula 3.ª 6
Gestor do contrato 6
Cláusula 4.ª 6
Prazo de execução 6
Cláusula 5.ª 7
Preço e condições de pagamento 7
Capítulo II 8
Obrigações contratuais 8
Cláusula 6.ª 8
Obrigações do adjudicatário 8
Cláusula 7.ª 9
Entrega e instalação de licenças, upgrades e updates 9
Cláusula 8.ª 10
Sigilo 10
Cláusula 9.ª 10
Patentes, licenças e marcas registadas 10
Cláusula 10.ª 11
Proteção de dados 11
Cláusula 11.ª 11
Obrigações da entidade adjudicante 11
Capítulo III 12
Vicissitudes contratuais 12

Cláusula 12.ª 12
Responsabilidade do adjudicatário 12
Cláusula 13.ª 12
Resolução do Contrato 12
Cláusula 14.ª 13
Sanções contratuais 13
Cláusula 15.ª 13
Força Maior 13
Capítulo IV 15
Disposições finais 15
Cláusula 16.ª 15
Cessão da posição contratual e subcontratação 15
Cláusula 17.ª 15
Despesas 15
Cláusula 18.ª 16
Interpretação do Contrato 16
Cláusula 19.ª 16
Publicidade 16
Cláusula 20.ª 16
Comunicações e notificações 16
Cláusula 21.ª 17
Contagem dos prazos 17
Cláusula 22.ª 17
Foro Competente 17
Cláusula 23.ª 17
Lei Aplicável 17
PARTE II 17
Especificações técnicas 17
Cláusula 1.ª 17
Enquadramento 17
Requisitos gerais 18
Cláusula 3.ª 18

Cláusula 4.ª 23
Solução de controlo de acesso à rede 23
Cláusula 5.ª Solução de proteção do posto de trabalho e Acesso remoto 27
Cláusula 6.ª 30
Proteção avançada do posto de trabalho 30
Cláusula 8.ª 36
Declarações, Certificações e Acreditações 36
Cláusula 9.ª 36
Formação 36

Parte I

Cláusulas jurídicas

Capítulo I

Disposições gerais do contrato

Cláusula 1.ª

Objeto e âmbito

1. O presente caderno de encargos é composto pelo clausulado jurídico e técnico, que rege o presente procedimento e visa integrar o contrato a celebrar entre o IMT, I.P., enquanto entidade adjudicante, e o adjudicatário.
2. O procedimento contratual de concurso público tem por objeto a aquisição de solução de software de segurança de endpoint e a que corresponde o 48730000-4 - Pacote de software de segurança.
3. Em tudo o que não se encontre previsto e/ou especificado nas peças do procedimento, a saber: anúncios, programa de concurso e caderno de encargos, nos quais são indicados os termos e as condições que serão incluídos no contrato a celebrar, subsidiariamente, as disposições constantes no Código dos Contratos Públicos (CCP), bem como outras disposições legais e regulamentares.

Cláusula 2.ª

Contrato

1. O contrato a celebrar na sequência do presente procedimento contratual será composto pelo respetivo clausulado contratual e seu(s) anexo(s), integrando e respeitando as disposições legais e regulamentares aplicáveis.
2. O contrato a celebrar integra ainda, e é composto, pelos seguintes elementos:
   a) Os suprimentos dos erros e das omissões do caderno de encargos identificadas pelo(s) concorrente(s), desde que esses erros e omissões tenham sido expressamente aceites pelo órgão competente para a decisão de contratar;
   b) Demais esclarecimentos e retificações relativos ao caderno de encargos;
   c) O presente caderno de encargos;
   d) A proposta adjudicada;
   e) Os esclarecimentos sobre a proposta adjudicada prestados pelo adjudicatário.

3. Em caso de divergência entre os documentos referidos no número anterior, a respetiva prevalência é determinada pela ordem pela qual são indicados.
4. Em caso de divergência entre os documentos referidos no n.º 2 e o clausulado do contrato e seu(s) anexo(s), se existentes, prevalecem os primeiros, salvo quanto aos ajustamentos propostos ao abrigo do disposto no artigo 99.º do CCP e aceites pelo adjudicatário nos termos do disposto no artigo 101.º do referido Código.

Cláusula 3.ª
Gestor do contrato

1. Nos termos e para efeitos do definido no artigo 290.º-A do CCP, será designado, no momento da assinatura do contrato, um gestor do contrato do IMT, I.P., com a função de acompanhar permanentemente a execução deste.
2. Caso o gestor detete desvios, defeitos ou outras anomalias na execução do contrato, deve comunicá-los de imediato ao órgão competente para a decisão de contratar, propondo em relatório fundamentado as medidas corretivas que, em cada caso, se revelem adequadas.

Cláusula 4.ª
Prazo de execução

1. A execução da presente aquisição tem data de início prevista com a assinatura do contrato ou comunicação do compromisso, caso o mesmo não venha a ser reduzido a escrito, e deverá o licenciamento ser disponibilizado num prazo máximo de 20 dias calendário, a contar daquela data e com limite de 31/12/2022, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato, incluindo as de confidencialidade, suporte e de garantia, quando aplicáveis.
2. As partes obrigam-se a cumprir fiel e imperativamente os prazos contratuais definidos, devendo proceder à comunicação imediata, assim que do mesmo tenham conhecimento, de qualquer impedimento ou circunstância modificativa do prazo de execução.

Cláusula 5.ª

Preço e condições de pagamento

1. O preço base[1] global definido para a presente aquisição é de € 211.000,00 (duzentos e onze mil euros), sendo este o montante máximo que esta entidade se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato, incluindo eventuais prorrogações do mesmo.
2. Pela execução da(s) prestação/prestações objeto do contrato, a entidade adjudicante obriga-se ao pagamento ao adjudicatário do(s) valor(es) constante(s) da(s) fatura(s) por este enviada(s), as quais deverão referir obrigatoriamente o número do contrato, a designação do objeto contratual e o número de compromisso respetivo, obtido nos termos do n.º 3 do artigo 5.º da Lei n.º 8/2012 de 21 de fevereiro.
3. A(s) fatura(s) referida(s) no número anterior, apenas pode(m) ser emitida(s) após a boa verificação do cumprimento/vencimento da obrigação respetiva, a qual deverá respeitar e acompanhar o(s) prazo(s) e a(s) fase(s) de execução contratuais definidos para o efeito nas especificações técnicas (Parte II) deste caderno de encargos.
4. Com efeito, e sempre que tal seja disposto pelo serviço requerente, as faturas deverão ser acompanhadas dos entregáveis respetivos, designadamente relatórios de execução.
5. Desde que devidamente verificados os pressupostos identificados e definidos *supra*, a(s) fatura(s) será/serão validada(s) pelo gestor de contrato, no prazo internamente definido para o efeito.
6. O prazo de validação interna da(s) fatura(s) por parte da entidade adjudicante não poderá ser superior a 30 (trinta) dias a contar da data da sua receção.
7. Uma vez cumprido o disposto nos números anteriores, o IMT, I.P. procederá ao pagamento da(s) fatura(s), através de transferência bancária, no prazo de 30 (trinta) dias contados da data da sua validação.
8. O processo interno de pagamento da entidade adjudicante, não deve exceder, em qualquer caso, 60 (sessenta) dias.
9. Em caso de atraso por parte do IMT, I.P. no cumprimento de obrigações pecuniárias, tem o adjudicatário direito a juros de mora sobre o montante em dívida, à taxa legalmente fixada para o efeito, pelo período correspondente à mora.

[1] Preço base = montante máximo, sem IVA, que esta entidade se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato.

Capítulo II
Obrigações contratuais

Cláusula 6.ª
Obrigações do adjudicatário

1. Sem prejuízo das obrigações previstas em demais legislação aplicável, da celebração do contrato decorrerem para o adjudicatário as seguintes obrigações principais:
   a) Fornecer os bens, conforme as características técnicas e requisitos mínimos constantes das especificações do presente caderno de encargos;
   b) Preparação, planeamento e prestação de todos os requisitos inerentes à(s) prestação/prestações objeto do contrato;
   c) Reunião e manutenção das condições e premissas técnicas previstas e descritas no presente caderno de encargos, salvo se forem negociadas condições mais vantajosas para a entidade adjudicante;
   d) Prestação, de forma correta, fidedigna, rápida e eficaz, das informações referentes às condições em que será/é executado o objeto do contrato, durante o período de vigência do mesmo, sem prejuízo das demais obrigações acessórias que perdurem para além de tal prazo ou da prestação de outros esclarecimentos adequados, que se justifiquem, de acordo com os circunstancialismos inerentes;
   e) Recurso a todos os meios humanos, materiais e técnicos que sejam necessários e adequados à execução do contrato;
   f) Designação e indicação à entidade adjudicante do responsável do contrato, por parte do adjudicatário, para efeitos de comunicações e demais situações necessárias, o qual deverá estar definido no momento da assinatura do mesmo, bem como quaisquer alterações relativas à sua nomeação;
   g) Comunicação à entidade adjudicante, logo que dele(s) tenha(m) conhecimento, do(s) facto(s) que tornem total ou parcialmente impossível a prestação do objeto contratual, bem como o cumprimento de qualquer outra das suas obrigações;
   h) Não alteração das condições de prestação de serviços fora dos casos previstos no caderno de encargos e/ou contrato a celebrar, sem orientação expressa da entidade adjudicante;

i) Não cedência da posição contratual sem prévia autorização da entidade adjudicante, para o efeito;

j) Comunicação junto da entidade adjudicante de qualquer facto que ocorra, durante a execução do contrato a celebrar, que o altere, designadamente, o seu responsável do contrato, a sua denominação e sede social, os seus representantes legais, a sua situação jurídica e a sua situação comercial;

k) Não divulgação, por qualquer forma, sem prévia autorização escrita da entidade adjudicante, dos elementos entregues por esta, no âmbito do presente procedimento, bem como das informações que o adjudicatário vier a ter conhecimento, na fase de execução do contrato, relacionadas com a atividade da entidade adjudicante, restringindo-se a sua utilização ao prosseguimento do fim a que se destinam.

2. Constituem ainda obrigações do adjudicatário:

a) Apresentar os documentos de habilitação a que estão obrigados, nos termos do artigo 81.º do Código dos Contratos Públicos (CCP);

b) 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 aquela execução, abrangendo esta obrigação todos os seus agentes, funcionários, colaboradores ou terceiros que nelas se encontrem envolvidos;

c) Possuir todas as autorizações, consentimentos, aprovações, registos e licenças necessários para o pontual cumprimento das obrigações assumidas no contrato.

Cláusula 7.ª

Entrega e instalação de licenças, upgrades e updates

1. A entrega das licenças adquiridas e dos upgrades e updates a que se refere a alínea a) n.º 1 da cláusula 6.ª são disponibilizados no prazo máximo de 5 (cinco) dias a partir do respetivo lançamento por parte da empresa proprietária.
2. A disponibilização das licenças dos upgrades e updates referida no número anterior é efetuado através de download.
3. A instalação e a parametrização de software e dos upgrades e updates são feitas pela entidade adjudicante ou por quem esta indicar.

4. O adjudicatário obriga-se, sempre que solicitado, a assistir a entidade adjudicante na realização instalação e a parametrização de software.
5. A entidade adjudicante comunica ao adjudicatário a existência de quaisquer irregularidades no software ou dos upgrades e updates.
6. O adjudicatário dispõe do prazo de 5 (cinco) dias a contar da data da comunicação referida no número anterior para proceder a todas as reparações e retificações necessárias à regular utilização do software cujas licenças são adquiridas, assim como do software objeto de upgrades e updates.

Cláusula 8.ª
Sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa ao IMT, I.P., de que possa ter conhecimento ao abrigo do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não poderão ser transmitidas a terceiros, nem poderão ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever de sigilo previsto, a informação e a documentação que sejam comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário 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.
4. O dever de sigilo mantém-se durante e após a vigência do contrato, relativamente a todos os dados e informação provenientes da execução do mesmo.

Cláusula 9.ª
Patentes, licenças e marcas registadas

1. São da responsabilidade do adjudicatário quaisquer encargos decorrentes da utilização, no âmbito do contrato, de marcas registadas, patentes registadas ou licenças.
2. Caso a entidade adjudicante venha a ser demandada por alegadamente ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, a segunda contraente indemniza-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 10.ª
Proteção de dados

1. No âmbito do contrato a celebrar, os contraentes obrigam-se ao integral cumprimento da legislação aplicável relativa à proteção de dados pessoais, designadamente quanto ao disposto no Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.
2. Em conformidade com o definido no número anterior os contraentes ficam obrigados, e garantirão, por todo o tempo, o cumprimento do quadro normativo presente no citado Regulamento, bem como, todas as normas que lhe sejam aplicáveis em matéria de proteção de dados.

Cláusula 11.ª
Obrigações da entidade adjudicante

1. Constitui obrigação da entidade adjudicante pagar o preço contratual adjudicado, mediante verificação do bom cumprimento da prestação e execução contratual por parte do adjudicatário, em respeito das condições de pagamento estabelecidas na cláusula 5.ª do presente caderno de encargos.
2. Sem prejuízo do preço contratual constante da proposta adjudicada, a entidade adjudicante só se obriga a pagar ao adjudicatário a(s) prestação/prestações que efetivamente venha(m) a ser executada(s).
3. Constitui ainda obrigação da entidade adjudicante o acompanhamento da prestação e execução, resultante do contrato a celebrar, pelo gestor designado para o efeito, nos termos do artigo 290-A.º do CCP.
4. A entidade adjudicante comunicará ao adjudicatário, logo que dele(s) tenha(m) conhecimento, do(s) facto(s) que tornem total ou parcialmente impossível a prestação do objeto contratual, bem como o cumprimento de qualquer outra prestação contratual, dentro dos termos e condições definidos para o efeito.
5. Com efeito, procederá igualmente à comunicação ao adjudicatário da alteração do gestor de contrato designado, bem como respetivos elementos de contacto, caso a mesma ocorra durante o período de vigência do mesmo.

Capítulo III
Vicissitudes contratuais

Cláusula 12.ª
Responsabilidade do adjudicatário

1. O adjudicatário responde pelos danos que causar à entidade adjudicante em razão do incumprimento culposo das obrigações que sobre ele impendam.
2. O adjudicatário responde ainda perante a entidade adjudicante pelos danos causados pelos atos e omissões de terceiros, por si empregues na execução de obrigações emergentes do contrato, como se tais atos ou omissões fossem praticados por aquele.

Cláusula 13.ª
Resolução do Contrato

1. Caso se verifique que o adjudicatário não coloca à disposição da entidade adjudicante, os meios e/ou recursos necessários, identificados no presente caderno de encargos e na proposta adjudicada, necessários à boa execução do contrato, e/ou uma vez verificado o não cumprimento do(s) prazo(s) definidos para o efeito, sem que para tal haja fundamento ou impedimento justificativo, a entidade adjudicante poderá resolver o contrato, não havendo lugar ao pagamento de qualquer indemnização ao adjudicatário.
2. Sem prejuízo do disposto no número anterior, a entidade adjudicante poderá resolver o contrato em caso de incumprimento definitivo por facto imputável ao adjudicatário, das respetivas prestações contratuais, bem como nos demais termos previstos e dispostos no CCP (cfr. artigo 325.º e ss.).
3. Para efeitos do disposto na presente cláusula, considera-se incumprimento definitivo quando houver atraso na prestação, por facto imputável ao adjudicatário, por um período superior a 30 (trinta) dias úteis.
4. Completados 30 (trinta) dias úteis de atraso o contrato poderá ser resolvido unilateralmente pelo IMT, I.P., enquanto entidade adjudicante.
5. O exercício pela entidade adjudicante do direito de resolução previsto nos números anteriores não preclude o direito de a mesma vir a ser ressarcida pelos prejuízos que lhe advierem da conduta do adjudicatário, nos termos gerais do direito.

6. O disposto no presente artigo não se aplica se o atraso se verificar por razões não imputáveis ao adjudicatário, caso em que este poderá propor, por via de carta registada, com uma antecedência mínima de 90 (noventa) dias, a resolução do contrato.

Cláusula 14.ª
Sanções contratuais

1. Em caso de incumprimento dos prazos constantes da proposta do concorrente ou no caderno de encargos, por causa imputável ao adjudicatário, o IMT, I.P., enquanto entidade adjudicante, poderá aplicar uma sanção diária, de acordo com a seguinte formula:

   P = V * A/365

   Sendo:

   P = montante da sanção;

   V = valor do contrato;

   A = número de dias de atraso.

2. O valor da sanção pecuniária a aplicar será creditado a favor da entidade adjudicante, ou deduzido ao preço contratualizado a que haja lugar pagar, nos termos referidos na cláusula 5.ª do presente Caderno de Encargos.

Cláusula 15.ª
Força Maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havido 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 respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fossem razoavelmente exigíveis contornar ou evitar.
2. Podem constituir força maior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos

de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.

3. Não constituem força maior, nomeadamente:

   a) Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
   b) Greves ou conflitos laborais limitados às sociedades do adjudicatário 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 resultante do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;
   d) Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
   e) Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou incumprimento de normas de segurança;
   f) Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;
   g) Eventos que estejam ou devam estar cobertos por seguros.

4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente consubstanciada à outra parte.
5. 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.

Capítulo IV
Disposições finais

Cláusula 16.ª
Cessão da posição contratual e subcontratação

1. O adjudicatário não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato, sem autorização expressa da entidade adjudicante para o efeito.
2. Mediante a autorização contemplada no número anterior, deverá ser apresentada pelo cessionário ou subcontratado toda a documentação exigida ao adjudicatário no presente procedimento.
3. A entidade adjudicante aprecia, designadamente, se o cessionário ou subcontratante não se encontra em nenhuma das situações previstas no artigo 55.º do CCP.

Cláusula 17.ª
Despesas

São da responsabilidade e correm por conta do adjudicatário, designadamente as seguintes despesas:

a) Todos os encargos derivados da apresentação da proposta, assinatura do contrato, prestação de garantias e seguros;
b) O pagamento de quaisquer impostos, taxas, direitos de qualquer natureza ou outros encargos exigidos palas autoridades competentes, relativos à execução do contrato no território do país ou países do(s) fornecedor(s);
c) A obtenção de quaisquer autorizações e o pagamento de quaisquer emolumentos exigidos pelas autoridades competentes relativamente ao cumprimento das obrigações que impendem sobre a prestação contratual;
d) Quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças;
e) Correm igualmente por conta do adjudicatário todas e quaisquer despesas, nomeadamente despesas de transporte, armazenamento e manutenção de materiais, e/ou alojamento e alimentação de meios humanos, bem como de instalação e/ou configuração de equipamentos, formação e/ou apoio técnico;

f) Encargos com telecomunicações, reprodução/impressão de documentos, equipamento informático, consumíveis de escritório e demais despesas gerais com material de economato, bem como com correios e/ou tradução/obtenção de documentos (oficiais e não oficiais);

g) Todas as despesas inerentes à celebração do contrato.

Cláusula 18.ª
Interpretação do Contrato

1. Em caso de dúvida sobre a interpretação das regras aplicáveis à execução do contrato, o adjudicatário deve solicitar, por escrito, um esclarecimento à entidade adjudicante, através do endereço indicado no contrato, pertencente ao gestor do contrato designado.
2. O adjudicatário obriga-se a ter em conta, na execução dos serviços, as orientações que lhe forem transmitidas pela entidade adjudicante, designadamente pelo gestor do contrato, na medida em que as mesmas não colidam com as regras aplicáveis à execução do contrato.

Cláusula 19.ª
Publicidade

O adjudicatário não poderá fazer ou consentir qualquer espécie de publicidade relacionada com o contrato a celebrar na sequência do presente procedimento, sem a prévia autorização do IMT, I.P., enquanto entidade adjudicante.

Cláusula 20.ª
Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, nos termos do CCP, para o domicílio ou sede contratual de cada uma, identificados no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.
3. À data das notificações e comunicações é aplicável o artigo 469.º do CCP.

Cláusula 21.ª
Contagem dos prazos

1. A contagem de prazos na fase de formação dos contratos rege-se pelo disposto no artigo 470.º do CCP e acompanha o disposto no Código do Procedimento Administrativo, por remissão da disposição aplicável.
2. A contagem de prazos na fase de execução dos contratos é realizada nos termos do artigo 471.º do CCP, sem prejuízo dos prazos para o cumprimento das obrigações assumidas pelas partes no âmbito do contrato.

Cláusula 22.ª
Foro Competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo de Círculo de Lisboa.

Cláusula 23.ª
Lei Aplicável

O contrato rege-se pela Lei portuguesa.

PARTE II
Especificações técnicas

Cláusula 1.ª
Enquadramento

A presente aquisição tem por objeto atualizar a infraestrutura de segurança, beneficiando das mais recentes tecnologias que o mercado oferece e simultaneamente, mitigando os riscos emergentes nas diversas componentes de operação.

Neste sentido pretende adquirir as seguintes soluções de segurança:

- Solução de proteção de Email
- Solução de controlo de acesso à rede
- Solução de proteção avançada do posto de trabalho

- Solução de proteção do posto de trabalho e acesso remoto

Cláusula 2.ª
Requisitos gerais

Com o objetivo de simplificar a gestão da infraestrutura, permitindo uma maior flexibilidade e gestão de recursos, a solução a apresentar deverá integrar naturalmente e a 100% com a firewall existente (Fortinet), possibilitando desta forma que exista uma maior integração e correlação das soluções a implementar.

A solução a apresentar deverá prever o suporte e subscrição de todos os serviços de segurança enunciados no presente documento, por parte do fabricante por um período mínimo de 1 ano e em regime 24x7.

Cláusula 3.ª

Solução de proteção de Email

Pretende-se a implementação uma solução de proteção de email, totalmente baseada na Cloud para 1300 caixas de correio, devendo a solução possuir um conjunto de especificações e de tecnologias enumeradas de seguida:

1. <u>Sistema</u>

As seguintes funcionalidades deverão ser suportadas:

- Serviço com gestão na Cloud
- Inspeção de inbound e outbound
- Suporte para múltiplos domínios
- Suporte para endereços de IPV4 e IPV6
- Virtual hosting com Pools de endereço de Origem e/ou Destino
- Autenticação SMTP suportada em LDAP, RADIUS, POP3 e IMAP
- Routing de email baseado em LDAP
- Inspeção por utilizador baseado em atributos LDAP
- Políticas baseadas em localização geográfica

- Interface gráfica para Webmail e/ou gestão de Quarentenas
- Gestão de filas de correio
- Suporte para vários idiomas de Webmail e interface de administração em conformidade com o RFC SMTP
- Interface gráfica em HTML5
- Compatibilidade com serviços na Cloud (Microsoft 365, Google Workspace, Amazon AWS e Microsoft Azure)

2. Proteção Antisspam

As seguintes funcionalidades deverão ser suportadas:

- Reputação de domínio e de remetente
- Spam e assinaturas em anexo
- Regras heurísticas dinâmicas
- Proteção em tempo real contra campanhas de ataque
- Categorização de URL incluindo spam, malware e phishing, pornografia, domínios registados recentemente
- Greylisting para endereços IPv4, IPv6 e contas de email
- Reputação do remetente local (baseado em IPv4, IPv6 e End Point ID)
- Análise comportamental
- Integração externa de URI de Spam e listas negras em tempo real (SURBL/RBL)
- Deteção de newsletter suspeita
- Análise de imagem e PDF
- Listas seguras e negras a nível global, por domínio e por utilizador
- Suporte para padrões de identidade do remetente nomeadamente:
    - Sender Policy Framework (SPF)
    - Domain Keys Identified Mail (DKIM)
    - Domain-Based Message Authentication (DMARC)
- Perfis de notificação
- Serviços de Quarentena de sistema com self-service para utilizadores

3. Proteção contra ataques direcionados

As seguintes funcionalidades deverão ser suportadas:

- Desativação e reconstrução de conteúdo:
  - Neutralização de documentos Office e PDF (remoção de conteúdos perigosos)
  - Neutralização de conteúdo HTML de email
  - Remoção de hiperligações (URL)
  - Reescrita de URLs
- Business Email Compromise (BEC):
  - Proteção anti-spoof multinível
  - Análise de falsificação de identidade - deteção manual e automática de falsificação de identidade
  - Detecção de domínios semelhantes (cousin domains)
- URL Click Protect com rescrita de URL e revalidação em momento de acesso
- Integração com plataforma de Browser Isolation para neutralização de ameaças baseadas em vulnerabilidades de browser

4. API de Integração

As seguintes funcionalidades deverão ser incluídas:

- Integração Microsoft 365:
  - Recuperação de ameaça pós-entrega
  - Agendamento de Verificação
  - Verificação em tempo real
  - Verificação de correio interno

5. Deteção de conteúdos

As seguintes funcionalidades deverão ser suportadas:

- Deteção de Antivírus:
    - Verificação de assinatura CPRL
    - Deteção comportamental baseada em heurística
    - Deteção de Greyware
- Proteção contra campanhas de malware
- Deteção de conteúdos ativos (PDF e documentos Office)
- Verificação das ameaças na remoção da quarentena
- Verificação de hash de ficheiros personalizadas
- Deteção de MIME e tipo de ficheiros
- Prevenção contra perda de dados com deteção de impressões digitais e deteção de dados confidenciais
- Desencriptação automática de ficheiros, PDF e documentos Office
- Verificação de PDF e análise de imagem
- Serviço dinâmico de conteúdos para adultos

6. Encriptação

As seguintes funcionalidades deverão ser suportadas:

- Serviço dinâmico de conteúdos para adultos
- Encriptação TLS "Server to Server" com controlo granular do cyphersuite a aplicar
- Suporte S / MIME
- Encriptação sem cliente para o desktop do destinatário utilizando Encriptação com base na Identidade (Identity Based Encryption - IBE)

7. Gestão, Logs e Reporting

As seguintes funcionalidades deverão ser suportadas:

- Modos de gestão básico / avançado

- Contas de administração baseadas em funções por domínio,
- Atividade, alteração de configurações, logs e relatório de incidentes
- Módulo de relatório integrado
- Rastreio detalhado de mensagens
- Quarentena centralizada para implantações em grande escala
- Suporte SNMP com recurso a MIBs (standards e privadas) com traps baseadas em thresholds
- Open REST API para configuração e gestão

8. Avançadas

As seguintes funcionalidades deverão ser suportadas:

- Arquivo de e-mails baseados em políticas com opções para armazenamento remoto
- Recursos de servidor de e-mail avançado
    - Interface de webmail
    - Acesso IMAP e POP3
    - Funções de calendário
    - "Undo" de mail enviado
- Integração de SAML 2.0 SSO e ADFS para acesso webmail e ao portal das quarentenas

9. Serviços de Implementação

Os serviços de implementação devem incluir as seguintes atividades macro:

- Workshop de definição de âmbito e pré-requisitos;
- Instalação e Configuração da solução de proteção de email proposta
- Configuração da política de segurança
- Testes de aceitação
- Entrega da documentação
- Formação on job

Cláusula 4.ª

Solução de controlo de acesso à rede

Pretende-se a implementação uma solução de controlo de acesso à rede para 1300 dispositivos, suportado em um cluster de máquinas virtuais, devendo a solução possuir um conjunto de especificações e de tecnologias enumeradas de seguida:

1. Descrição geral

- Suporte para mínimo de 1300 dispositivos terminais concorrentes (Wired, Wireless e VPN);
- Suporte para switch dos fabricantes Cisco (família catalyst), HPE/Aruba e Fortinet;
- Integração com repositórios de autenticação Microsoft AD, LDAP e repositório local;
- Validação de postura de clientes (mínimo por existência de antivírus e sistema operativo atualizados);
- Segmentação e/ou política de rede por tipo de equipamentos (desktop, portátil, telemóvel, tablet, etc);
- Suporte para gestão de 3 ou mais locais físicos distintos, com políticas e equipamentos distintos;
- Funcionalidades de relatórios e alarmísticas com correlação de eventos;
- Possibilidade para implementar futuramente automação para resposta a incidentes;
- Funcionalidade de RADIUS Proxy
- Integração com os seguintes fabricantes de soluções MDM: AirWatch; MaaS360; Mobile Iron, Google GSuite, XenMobile e Microsfot InTune;
- Verificação do estado dos terminais (posture validation):
    - Patchs do sistema operativo
    - Antivirus
    - Verificação do serviço
    - Verificação de aplicações instaladas
    - Entradas no registry
- Disponibilização de REST API
- Disponibilizar integração outbound de enventos de segurança

2. Administração

As seguintes funcionalidades deverão ser suportadas:

- Acesso de gestão gráfica e texto: HTTPS com recurso a web browser
- Acesso de gestão em modo de texto: SSH, Telnet ou consola
- Sem necessidade de utilização de software cliente proprietário para gestão gráfica
- Suporte para gestão local e gestão centralizada em simultâneo
- Suporte para gestão centralizada com integração em plataforma específica para o efeito

3. Visualização:

As seguintes funcionalidades deverão ser suportadas:

- Deteção de dispositivos na Rede
    - Activa
    - DHCP Fingerprinting
    - FortiGate sessions
    - HTTP/HTTPS
    - Range de IPs
    - Localização
    - Trafico de rede
    - ONVIF
    - Agente Passivo
    - Agente Persistente
    - Pedido de Radius
    - Scripting
    - SNMP
    - SSH

  - TCP
  - Telnet
  - UDP
  - Vendor OUI
  - WinRM
  - Windows Profile
- Identificação de dispositivos rogue
- Classificação e perfilagem de dispositivos
- Deteção de anomalias
- Scan de rede para deteção e classificação de dispositivos através de agente (Persistente, Passivo, Dissolvable)
- Captive portal

4. **Automação e controlo:**

As seguintes funcionalidades deverão ser suportadas:

- Segmentação de firewall
- Políticas de acesso á rede
- IoT onboarding com sponsor
- Deteção e restrição de dispositivos rogue
- Suporte de autenticação e bypass feitos por MAC Address
- Radius EAP
- Capacidade de onboarding BYOD (Bring your own device)
- Verificar a conformidade do Endpoint
- Sistema de Single Sign-on de utilizadores Web e Firewall
- Gestão de contas guest

5. **Relatórios:**

As seguintes funcionalidades deverão ser suportadas:

- Gerar Relatórios personalizáveis

6. **Alta Disponibilidade**

As seguintes funcionalidades deverão ser suportadas:

- Alta disponibilidade (Modo ativo-passivo)

7. **Serviços do fabricante**

- A implementação deverá ser acompanhada de um pacote de serviços prestado pelo fabricante para coordenação inicial do projeto, validação de pré-requisitos e definição de arquiteturas e casos de uso a implementar.
- Instalação, registo e licenciamento inicial da plataforma e apoio no Go-live da solução.

8. **Serviços de Implementação**

Os serviços de implementação devem incluir as seguintes atividades macro:

- Workshop para definição do âmbito de implementação e pré-requisitos
- Instalação e configuração do cluster da solução de NAC
- Registo das Licenças
- Instalação dos certificados, Email, LDAP e integração com um Syslog
- Pesquisa e deteção de "devices" nas diversas subnets
- Classificação do tipo de "devices" (máximo de 20 tipos)
- Definição de VLANs produtivas e quarentena;
- Definição e configuração das políticas de acesso à rede;
- Preparação do "Persistent Agent"
- Aplicação das políticas definidas
- Definição e configuração do Portal de Guest/BOYD
- Piloto - ativação da solução NAC num local em ambiente controlado e limitado (a definir no workshop)
- Testes de aceitação do Piloto
- Implementação global da solução NAC nos restantes sites a definir
- Testes de aceitação finais
- Entrega da documentação
- Formação On Job

Cláusula 5.ª
Solução de proteção do posto de trabalho e Acesso remoto

Pretende-se a implementação de uma solução de proteção e acesso remotos para 1300 endpoints, devendo esta possuir um conjunto de especificações e de tecnologias que enumeramos de seguida:

1. <u>Requisitos de sistema:</u>

As seguintes funcionalidades deverão ser suportadas:

- Suporte para instalação em Windows server 2012 R2 ou mais recente;
- Suporte para gestão de clientes Windows, Mac, Linux, Chromebooks, IOS e Android;
- O agente a propor deve ser compatível com a solução NGFW existente (Fortigate 501E)

- O Agente instalado deve ser também o agente cliente de ligação VPN.

2. <u>Aprovisionamento:</u>

As seguintes funcionalidades deverão ser suportadas:

- Inventário de software instalado nas máquinas cliente;
- Integração com Windows AD;
- Informação do endpoint em tempo real;
- Painel de vulnerabilidades;
- Aprovisionamento e distribuição centralizada de software;
- Atribuição automática de grupos;
- Definições de sandboxing sincronizadas automaticamente;
- Telemetria em tempo real do endpoint;
- Controlo de acesso dinâmico para imposição da conformidade, criando grupos que podem ser utilizados por uma NGFW para controlos de acesso dinâmicos;
- Quarentena do endpoint que se encontre comprometido;
- Resposta automatizada sem intervenção manual;
- Split Tunnel baseado em aplicações
- Filtros Web com pesquisa por palavra-chave/ filtros de YouTube

3. <u>Controlo remoto:</u>

As seguintes funcionalidades deverão ser suportadas:

- Análise de antivírus por solicitação;
- Análise de vulnerabilidades por solicitação;
- Quarentena do cliente;

4. <u>Telemetria e monitorização:</u>

As seguintes funcionalidades deverão ser suportadas:

- Informação do cliente (versão do cliente, Sistema Operativo, IP, MAC address, perfil assignado, avatar do utilizador);
- Envio de relatório de estado para plataforma externa;

5. <u>Segurança do cliente e componente VPN:</u>

As seguintes funcionalidades deverão ser suportadas:

- Dispor de uma solução de Anti-virus;
- Deteção de ameaças baseada na cloud;
- Dispor de uma solução de Anti-Exploit;
- Funcionalidade de filtragem web;
- Funcionalidade de Firewall aplicacional;
- Suportar IPsec VPN;
- Suportar SSL VPN;
- Controlo de equipamentos USB;
- Possibilidade de ligar à VPN antes do login no Windows;
- Sistemas operativos a suportar:
    - Windows 7 (32 bits e 64 bits);
    - Windows 8 e 8.1 (32 bits e 64 bits);
    - Windows 10 (32 bits e 64 bits);
    - Windows server 2008 ou mais recente;
    - Mac OS X 10.14, 10.15, 11+;
    - iOS 9.0 ou posterior.
    - Android 5.0 ou posterior
    - Ubuntu 16.04 ou mais recente;
    - Red Hat 7.4 ou mais recente;
    - CentOS 7.4 ou mais recente com KDE ou GNOME.

6. Serviços de Implementação:

Os serviços de implementação devem incluir as seguintes atividades macro:

- Workshop de definição de âmbito e pré-requisitos;
- Instalação e parametrização da consola de gestão centralizada;
- Criação até 12 perfis de acesso.
- Configuração até 12 políticas simples com parametrizações padrões;
- Instalação até 12 endpoints para testes VPN, até 3 sistemas operativos diferentes.
- Testes de aceitação
- Entrega da documentação

- Formação On Job

Cláusula 6.ª
Proteção avançada do posto de trabalho

É necessária uma solução avançada de nova geração para proteção de endpoints, que analise em tempo real e automaticamente a postura do utilizador e dos servidores, através de uma abordagem não baseada em assinaturas, mas na análise de comportamentos, que permita bloquear malware e exploits tanto conhecido como desconhecido. Deve incorporar tanto a deteção como a resposta automática a ameaças, constituindo uma solução de Deteção e Resposta de Endpoints (conhecida pelo seu acrónimo EDR). A solução deve contemplar um total de 1300 licenças para postos de trabalho e servidores.

1. **Características mínimas:**

- Capacidade de detetar em tempo real atividades potencialmente maliciosas, mesmo quando o computador não está ligado à rede, incluindo monitorização de processos em execução, arranque e término dos processos, bem como interações entre processos, alterações maliciosas no sistema, ligações de rede e eventos suspeitos associados a ficheiros DLL.
- Capacidades de prevenção de ameaças (pré-execução) e desativação (pós-execução), impedindo a execução de ficheiros, DLLs e aplicações maliciosas, e impedindo o estabelecimento de conexões maliciosas. Deve permitir a definição de listas personalizadas para autorização e bloqueio destas proteções (por hash, nome e/ou caminho de arquivo, ou por aplicação, incluindo dados de versão e fabricante), bem como facilmente marcar, tanto manualmente como automaticamente, determinada atividade como falso positivo, impedindo também a ocorrência de deteções semelhantes. Além disso, deve ser possível definir "whitelists" de aplicações, processos e ficheiros considerados seguros, para que não desencadeiem eventos de segurança.
- Capacidade automatizada de resposta a incidentes em tempo real, baseada em conjuntos de ações orquestradas, para permitir no mínimo: interromper processos,

eliminar ficheiros, restaurar as definições de base (tais como registos de sistema modificados) e isolar completamente os processos individuais ou o dispositivo da rede.

- As capacidades de resposta devem incluir a possibilidade de definir scripts personalizados para interação com qualquer elemento (via API, por exemplo), independentemente do seu fabricante. Estes scripts de resposta devem ser selecionáveis com base na gravidade do evento de segurança detetado, a partir da mesma secção da consola onde as restantes respostas automatizadas são configuradas.
- Deve ser capaz de se integrar de forma nativa com a solução de segurança do perímetro do mesmo fabricante, bloqueando nas firewalls os IPs relacionados com eventos maliciosos a nível global para toda a organização, bem como com a solução de controlo de acesso à rede, permitindo isolar os hospedeiros infetados/suspeitos na camada de acesso.
- Deve ser dada uma resposta eficaz na prevenção de explorações e malware, mesmo em condições de falta de conectividade com servidores de gestão e/ou recursos baseados na nuvem.

- Avaliação de vulnerabilidade e patching virtual, com a capacidade de descobrir aplicações vulneráveis analisando as suas comunicações, incluindo a sua classificação de reputação e o detalhe dos códigos CVE aplicáveis, e patching virtual, desativando o acesso ou comunicação com o exterior de aplicações vulneráveis.

2. **<u>Proteção dos seguintes cenários de ataque:</u>**

- Escalada de privilégios, como por exemplo, substituir programas legítimos do sistema operativo, escalar privilégios de kernel (impedindo um intruso de usar informações de outro processo com privilégios mais elevados para executar um processo malicioso com permissões do sistema), ou tentativas de incluir utilizadores em grupos de administradores do Sistema Operativo.
- Malware conhecido (através de executáveis ou abertura de documentos maliciosos, mesmo sem conhecimento prévio dos mesmos ou deteções anteriores) e desconhecido,

bem como tentativas de explorar vulnerabilidades de 0 dias, detetadas através do seu comportamento, o que permite a aplicação imediata de medidas de reparação.

- Ransomware: devem ser aplicadas de imediato medidas de remediação, e bloqueadas os processos, assim que forem detetados comportamentos do tipo ransomware, tais como processos que leem ou escrevem demasiados ficheiros num curto espaço de tempo, e/ou que modificam valores dos mesmos (através da sua compressão ou encriptação, por exemplo).
- Dispositivos USB: deve ser capaz de permitir dispositivos fiáveis (registando a sua atividade), bem como configurar políticas de ação (como a prevenção imediata da interação) com outros maliciosos ou desconhecidos.
- Scripts: Scripts maliciosos (pelo menos PowerShell, Cscripts, Office macros) devem ser detetados e impedidos de funcionar, bem como impedir que um processo inicie um processo legítimo que possa ser usado para fins maliciosos (como motores de script).
- Roubo de palavra-passe, proteção de processos onde o intruso pode usar ferramentas para despejar credenciais.

3. **Investigação de incidentes:**

- Fornecer análises forenses detalhadas sobre ameaças e ataques detetados em dispositivos, recolhendo informações como ficheiros e URIs acedidos, módulos carregados, processos executados, etc.
- Mapeamento de comportamentos maliciosos detetados de acordo com a matriz MITRE ATT&CK, com possibilidade de realizar pesquisas avançadas com base nestes comportamentos, além de outros parâmetros como ficheiros, processos, etc.
- Período mínimo de retenção de 6 meses para eventos de segurança em implantações em nuvem.
- Possibilidade de recolher toda a telemetria do endpoint, quer esteja ou não relacionada com eventos de segurança, incluindo atividades relacionadas com processos, ficheiros, chaves de registo e a rede.
- Possibilidade de envio de logs via Syslog para integração com um SIEM ou SOAR.

- Deve permitir a integração nativa com a plataforma SIEM do fabricante, de modo que os eventos da plataforma EDR possam ser incorporados na investigação de eventos de segurança da organização e na avaliação global de ameaças.
- Capacidade de obter snapshots instantâneos da memória, por exemplo, para o estudo de malware do tipo file-less, bem como a recuperação no endpoint, de ficheiros relacionados com eventos de segurança.

4. <u>Arquitetura de Serviço:</u>

- A solução EDR deve ser capaz de ser implementada tanto em formato on-prem como na nuvem, com a opção de implementação mista sendo favoravelmente valorizada para uma melhor proteção de dispositivos tanto dentro da rede corporativa como fora dela.
- Suporte do Agente para os seguintes sistemas e ambientes operativos:
    - Windows: XP SP2/SP3, 7, 8, 8.1, 10 e 11.
    - Windows Server: 2003 SP2, R2 SP2, 2008 SP2, 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 e 2022.
    - MacOS: El Captain (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11.x) e Monterey (12.x).
    - Linux: Redhat Enterprise Linux e CentOS 6.x, 7.x e 8.x, Ubuntu LTS 16.04.x, 18.04.x e 20.04.x servidor, en 64-bit, Oracle Linux 7.7+ e 8.2+, Amazon Linux AMI 2 e SUSE SLES 15.1
    - Ambientes VDI: VMware Horizons 6 e 7 e Citrix XenDesktop 7
    - Todos os sistemas operativos suportados no Google Cloud Marketplace

5. <u>Requisitos de implementação, manutenção e agente:</u>

- Os agentes deverão ser atualizados sem a intervenção do utilizador, e sem necessidade de interromper a estação de trabalho ou a atividade do servidor, e deverão ter uma pegada ou impacto muito baixo no desempenho do computador, com uma carga de CPU inferior a 2%, consumindo menos de 120MB de RAM e 100MB de espaço em disco, e

com um consumo de tráfego de rede não superior a 20 kbps. O agente deve incorporar proteção anti-adulteração, para evitar desativações tanto do utilizador como de qualquer software malicioso.

6. **Serviços do fabricante:**

- A implementação deverá ser acompanhada de um pacote de serviços prestado pelo fabricante, incluindo no mínimo a instalação da infraestrutura, o ajuste inicial dos alertas, a assistência na produção de medidas de proteção e uma formação on-job da solução para os administradores.
- O fabricante deverá ter a capacidade de prestar serviços de consultoria, formação e assistência na investigação de incidentes de segurança, caso seja solicitado para tal.
- Da mesma forma, o fabricante deverá ter a capacidade de fornecer um serviço 24x7 de monitorização contínua de ameaças, análise e classificação de alertas, e gestão de incidentes pelos seus analistas.

7. **Gestão de plataformas:**

- A gestão da solução deve poder ser realizada na sua totalidade através de um navegador web, sem ser necessário em qualquer caso a instalação de software adicional.
- Deve fornecer dashboards que mostrem o estado de segurança e as ameaças, bem como a "saúde" dos diferentes elementos da plataforma.
- Deve permitir a configuração granular de perfis de acesso com diferentes privilégios, bem como a atribuição de utilizadores a estes perfis.
- A solução deve suportar de base o acesso e funcionamento em formato multi-tenant (RBAC/Controlo de Acesso Baseado em Funções).
- Suporte da API RestFull para desenvolver integrações adicionais necessárias.

8. **Outros requisitos:**

- A solução EDR deve poder coexistir, temporariamente, com a atual solução AV no momento da sua implementação.

- Deve ser capaz de complementar a segurança global da solução com a execução de ficheiros suspeitos/maliciosos numa sandbox para garantir a exatidão da sua análise e fornecer um veredicto adicional.
- O modelo de licenciamento deve ser por computadores protegidos e não por outros parâmetros, como o número de utilizadores, CPUs, etc.
- A solução deve ser compliance com as normas de segurança HIPAA e PCI-DSS.

9. Serviços de Implementação:

Os serviços de implementação devem incluir as seguintes atividades macro:

- Gestão de projecto global
- Kickoff de planeamento e pré-requisitos
- Instalação da infraestrutura, registo e licenciamento
- Suporte na instalação de certificados, Email, LDAP e integração Syslog
- Suporte na catalogação de ativos
- Suporte no desenvolvimento de políticas para um máximo de 3 cenários definidos
- Assistência na preparação de Agentes Persistentes para distribuição pela rede
- Validação das Políticas e Enforcement
- Suporte ao Go Live para 1 localização onde os utilizadores estão ligados (até 200 utilizadores)
- Testes finais e fecho do projecto
- Documentação Final

10. Serviços de Gestão:

- A solução deverá incluir monitorização, operação e gestão do EDR pelo período de 12 meses.
- Deverá ter monitorização 24x7x365 com triagem de alertas e tratamento de incidentes por analistas experientes na resposta na plataforma EDR
- A solução deverá ter acompanhamento de gestor de serviço para acompanhamento e reporting mensal

- Deverá ser enviada alarmística da plataforma de EDR por e-mail

Cláusula 8.ª
Declarações, Certificações e Acreditações

1. A equipa de gestão e operação da solução EDR deverá contar com certificação Certified Ethical Hacker e EC-Council Certified Incident Handler.
2. A equipa de gestão de projeto deverá possuir as certificações BS25599 Lead Auditor e ISO27001 Lead Implementor.
3. A empresa concorrente deverá ser membro da rede nacional CSIRT.

Cláusula 9.ª
Formação

Deve ser proporcionada formação on-job em todas as valências (implementação, operação, gestão e administração) da solução proposta para 3/4 técnicos do IMT, I.P.