AT autoridade tributária e aduaneira

DIREÇÃO DE SERVIÇOS DE CONTRATAÇÃO PÚBLICA E LOGÍSTICA

Divisão de Contratação

CONCURSO PÚBLICO

N.º **78/CP/AT/2024**

CADERNO DE ENCARGOS

Autoridade Tributária e Aduaneira

Aquisição de uma solução para salvaguarda de ciberataques

ÍNDICE

CAPITULO - I

DISPOSIÇÕES INICIAIS

Cláusula 1.ª - Objeto e conteúdo funcional

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar pelo Estado Português, através da Autoridade Tributária e Aduaneira, doravante designada apenas por AT, na sequência do Concurso Público, que tem por **objeto** a aquisição de uma solução para salvaguarda de ciberataques.

2. **Descrição da solução pretendida**

A aquisição pretendida é uma solução de proteção contra ciberataques/incidentes, integrada ao nível do software, hardware, com análise de vetores de ataque, que permita endereçar as seguintes necessidades, cumprindo ainda todos os requisitos técnicos identificados:

2.1. Solução de Recuperação contra ciberataques:

a) De forma a tirar partido da solução de proteção de dados existente na AT, a solução a propor deverá permitir a total integração com a atual solução Dell Avamar e Data Domain, permitindo assim um mecanismo de replicação nativo entre a solução existente e a solução a propor;
b) O controlo e gestão da solução de ciberproteção deverão ser feitos a partir do cofre, mantendo o isolamento lógico da rede de produção, pelo que a replicação deverá ser feita através de mecanismos nativos entre o Data Domain do Datacenter Central e o repositório do cofre, sem qualquer orientação ou conhecimento do software de proteção de dados, do lado da produção;
c) A solução a propor deve combinar os benefícios do isolamento e da continuidade de negócio, minimizando o impacto de um ciberataque ou incidente disruptivo, garantindo assim uma maior probabilidade de sucesso na recuperação dos sistemas críticos, alinhado com as práticas descritas pelo *National Institute of Standards and Technology* (NIST);
d) A solução de retenção de dados deve ter por base um repositório, que ao nível da gestão e retenção eletrónica de dados, cumpra com os seguintes normativos:
    i. Sarbanes-Oxley;
    ii. SEC 17a-4;
    iii. CFTC Rule 1.31b;
    iv. HIPAA;
    v. ISO Standard 15489-1;
    vi. MoREQ 2 EU.
e) Deve garantir a automação e fluxo de trabalho para um mínimo de 14 cópias “Gold” dos dados mais críticos, para um segundo repositório, o qual tem de replicar nativamente com a solução de proteção de dados em produção no Datacenter, para que os processos de negócios possam ser retomados após um ataque destrutivo;

f) Os processos de deteção deverão incidir sobre os vetores de ataque mais utilizados, como o malware, ransomware e criptoware, sem necessidade de recurso exclusivo a deteção de assinatura maliciosa, que obrigue a uma atualização constante da solução para manter o sucesso dos índices de deteção de código malicioso.

2.2. A solução de proteção contra ciberataques/incidentes deve combinar as seguintes premissas de proteção e recuperação:

a) Planeamento e *design*, por avaliação dos sistemas e aplicações críticas para o negócio, infraestrutura atual, tempo de recuperação contra ciberataques/incidentes e objetivos de recuperação, para adequar a implementação da solução. Devem ser incluídos os mapeamentos de dependências com a infraestrutura associada, metadados, etc.;

b) Isolamento e replicação, com base nos resultados da fase de planeamento e design, de forma a implementar as condições necessárias para um cofre de recuperação contra ciberataques/incidentes;

c) Procedimentos de analítica, por forma a salvaguardar o bom funcionamento e asseverar a eficácia das ferramentas de segurança, sendo requisito a capacidade análise de vetores de ataque, que permitam detetar possíveis comprometimentos da informação protegida;

d) Capacidade de restauro e recuperação, seguindo os padrões que a solução disponibiliza, acrescido das considerações complementares a aplicar conforme os cenários desenhados a montante, no plano de resposta a ciberataques/incidentes, incluindo-se o auxílio na avaliação forense e do dano sofrido nos dados, preparação da recuperação a partir das imagens “Gold” das aplicações e binários de sistemas operativos, culminando na reposição do ambiente de produção no mais curto espaço de tempo possível.

2.3. Em termos de características técnicas mínimas, a solução a propor deve assegurar:

2.3.1. Capacidade de proteção de dados mais críticos, em estado imutável, para a proteção do seguinte volume de dados:

a) 15TB de dados do tipo VMware;
b) 5TB de dados do tipo bases de dados;
c) 31TB de dados do tipo Fileshare.

2.3.2. Capacidade de desempenho e escalabilidade:

a) Capacidade de escrita correspondente a até pelo menos 26TB/hora;
b) Capacidade de expansão, sem recursos a troca de controladores, até pelo menos 160TB úteis, excluindo efeitos de deduplicação e/ou compressão;
c) Suporte para protocolos NFS/CIFS e OpenStorage (e em simultâneo, se necessário).

2.3.3. O repositório de proteção de dados deve permitir a realização das diversas operações de *backup*, recuperação e replicação, sem necessidade de interrupção ou janela de tempo dedicada para as tarefas de manutenção do repositório.

2.3.4. A solução a fornecer deve incluir todo o software necessário ao bom funcionamento da mesma, incluindo-se a replicação, encriptação (sem recurso a discos especiais e/ou dedicados para o efeito) e mecanismo de retenção imutável.

2.3.5. A solução deve ser fornecida sem limites de clientes e/ou agentes aplicacionais, mas devidamente licenciada para a quantidade de front-end a analisar.

2.3.6. Visando o garante da máxima integridade dos dados armazenados, a solução deverá contemplar, ao nível do repositório de dados, os seguintes níveis mínimos de redundância e validação:

a) Fontes de alimentação redundantes;
b) Proteção de disco de dupla paridade (RAID 6);
c) Mecanismos de verificação de integridade dos dados durante a escrita.

2.3.7. A solução deve ainda ser fornecida em formato PBBA (Purpose-Built Backup Appliance), isto é, deve ter um conjunto de características diferenciadoras dos restantes dispositivos appliances e storage arrays tradicionais, onde se destaca:

a) Ser capaz de armazenar especificamente dados de backup no formato do software de backup, sendo inviável o uso dos dados para outros propósitos;
b) Implementação de elevadas taxas de deduplicação (tipicamente 10:1 ou mais), sendo inviável o uso dos dados para outras tarefas que não recuperações;
c) Permitir a replicação dos dados com elevada eficiência (maioritariamente devido à deduplicação dos dados), de forma a facilitar a realização de backups rápidos a partir de localizações remotas;
d) Fornecer a tradução de protocolo (por exemplo, S3, OpenStack) para transferência de dados para repositórios de cloud (“cloud tiering”), se necessário.

2.4. Pretende-se ainda que a tecnologia de cibersegurança a implementar suporte os seguintes conceitos, na sua implementação, operacionalidade e gestão:

2.4.1 Deve proteger um mínimo de 14 cópias da informação protegida no Datacenter, em que pelo menos 50% serão “Gold”, saudáveis, para recuperação, na eventualidade de um ciberataque/incidente;

2.4.2 Por forma a reduzir a margem de ataque, a solução deverá recorrer a um isolamento lógico (do tipo air-gap) do cofre, desligado da rede de produção, gerido a partir do próprio cofre, e com acesso restrito apenas a utilizadores com as devidas credenciais de acesso ao cofre;

2.4.3 A transferência de dados deve ser protegida por handshake digital, com encriptação do link de replicação e dos dados a sincronizar;

2.4.4 Deve proteger as cópias sincronizadas através de um mecanismo de retenção certificado, que garanta a imutabilidade dos dados protegidos no cofre;

2.4.5 Deve ter processos de analítica integrada, que permita a análise periódica dos dados contidos no formato nativo de backup, sem necessidade de proceder a recuperações e efetuar a procura de indicadores de comprometimento da informação;

2.4.6 Os processos de analítica devem efetuar uma análise dos dados com recurso a indexação total de conteúdos, dentro do cofre, sem qualquer recurso ou ligação ao exterior;

2.4.7 A gestão deve ser baseada em políticas e automatização dos workflows de proteção;

2.4.8 A solução a propor deve incluir toda a infraestrutura necessária ao bom e regular funcionamento do cofre, incluindo, mas não se limitando, a: computação, armazenamento, ativos de rede e de segurança, todo o software e licenciamento necessário à análise dos dados a proteger no cofre, cabos, fibras óticas e racks;

2.4.9 A solução deverá integrar-se nativamente com a plataforma de backups atualmente implementada na AT, a saber, Dell/EMC Avamar e Dell/EMC Data Domain.

2.4.10 A solução deve ainda contemplar todos os serviços de implementação da solução de cibersegurança, bem como a realização de testes que permitam aferir o sucesso de implementação da mesma, de acordo com os requisitos a definir entre a AT e o proponente da solução.

2.4.11 Os serviços deverão ser assegurados por técnicos certificados do fabricante, sem recurso a subcontratação.

3. O adjudicatário deve assegurar o suporte e manutenção de toda a solução fornecida, devendo o mesmo ser assegurado diretamente e por um único fabricante, com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção e suporte pretendidos são:

a) Garantia mínima de 3 anos;
b) O tempo de resposta (nível de serviço) é de 4 horas, 24x7, 365 dias por ano, incluindo peças e mão-de-obra;
c) Prestação de assistência contínua até à resolução da avaria;
d) O suporte deverá ser dado diretamente pelo fabricante localmente (preferencialmente em língua portuguesa), sem recorrer a qualquer parceiro para esse efeito

4. O adjudicatário deverá ainda incluir todos os serviços necessários à instalação e configuração inicial do repositório de proteção de dados, bem como os serviços de interligação com a infraestrutura Dell/EMC Avamar e Data Domain existente na AT.

5. Devem ainda ser realizados testes de backup e de recuperação, após a integração, a definir em conjunto com as equipas da AT.

6. **Enquadramento da aquisição na AT**

6.1. Em sede das cópias de segurança/backups, a solução existente na AT é baseada em infraestrutura Dell/EMC Avamar e Data Domain, suportando os sistemas centrais, bem como os principais Serviços distribuídos geograficamente, tais como as maiores Direções de Finanças e Serviços Centrais.

6.2. Esta infraestrutura de backups salvaguarda atualmente serviços e plataformas como:

- DNS, WINS e DHCP;
- Acesso das Lojas do Cidadão;
- Sistemas de assinaturas digitais;
- Gestão de utilizadores;
- Sistemas de backup das Direções e Serviços de Finanças, Alfândegas e Serviços Centrais;
- Profiling;
- IDS;
- Antivírus;
- Microsoft SCCM;
- E-Learning;
- Servidores de gestão das impressoras das Direções e Serviços de Finanças, Alfândegas e Serviços Centrais;
- Servidor de suporte à Liscont;
- Servidor de Base de Dados de Conhecimento do Helpdesk;
- Ferramenta de suporte ao Helpdesk;
- Servidores de suporte ao polos distribuídos;
- Portais;
- SGA, SCOI, SGPC;
- Entre muitos outros serviços.

6.3. Esta solução, todavia, não garante a salvaguarda a ciberataques dirigidos, como por exemplo, ransomwares. Assim, para assegurar a salvaguarda deste tipo de ataques, importa adquirir uma solução complementar de proteção contra ciberataques e/ou incidentes passíveis de corromper a informação armazenada, integrada tanto ao nível do software, como do hardware e que faça ainda a análise de vetores de ataque, enquanto ao mesmo tempo endereça os objetivos de RTO e RPO estabelecidos.

7. A descrição do objeto obedece à classificação CPV (Common Procurement Vocabulary) 30200000-1 Equipamento e material informático, de acordo com o Regulamento (CE) n.º 213/2008 da Comissão, de 28 de novembro de 2007, que alterou o Regulamento (CE) n.º 2195/2002 do Parlamento Europeu e do Conselho.

Cláusula 2.ª - Preço-Base

1. O preço máximo que a entidade adjudicante se dispõe a pagar pela execução de todas as prestações que constituem o objeto do contrato é de €338.980,49 (trezentos e trinta e oito mil, novecentos e oitenta euros e quarenta e nove cêntimos), S/IVA, incluído.
2. O preço base foi fixado com base nos preços atualizados do mercado obtidos através de consulta informal ao mercado, realizada nos termos previstos no artigo 35.º A do CCP, conforme **Anexo I** do presente caderno de encargo.

Cláusula 3.ª - Local de entrega dos bens/Prestação dos serviços

O local da entrega dos bens e da prestação dos serviços objeto do contrato será em Lisboa, na Av. Engenheiro Duarte Pacheco, n.º 28.

CAPITULO - II

OBRIGAÇÕES CONTRATUAIS

Cláusula 4.ª - Obrigações principais do fornecedor

Sem prejuízo de outras obrigações previstas na legislação aplicável, no Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorre para o fornecedor como obrigação principal a entrega dos bens/prestação dos serviços identificados na sua proposta, em conformidade com o presente Caderno de Encargos.

Cláusula 5.ª - Prazo de entrega/Instalação e configuração

1. O adjudicatário obriga-se à entrega/Instalação e configuração dos bens, objeto do contrato com todos os elementos referidos no presente Caderno de Encargos, até à data limite de 15 (quinze) dias, contados após a produção de efeitos do contrato.

Cláusula 6.ª - Prazo de execução

O adjudicatário obriga-se à execução do contrato com todos os elementos referidos no presente Caderno de Encargos, contado a partir da produção de efeitos do contrato até 31 de dezembro de 2024.

Cláusula 7.ª - Preço contratual e formas de pagamento

1. Pelo fornecimento dos bens/prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a AT deve pagar ao fornecedor o preço constante da proposta adjudicada, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.

2. O preço referido no n.º 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao contraente público, incluindo as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças da responsabilidade do adjudicatário.
3. O preço a que se refere o n.º 1 será pago numa única prestação, após a entrega, instalação e configuração dos bens.

Cláusula 8.ª - Condições de pagamento

1. A quantia devida pela AT, nos termos da cláusula anterior, deve ser paga no prazo de 60 (sessenta) dias após a receção das respetivas faturas, as quais só poderão ser emitidas após o vencimento da obrigação correspondente.
2. Para os efeitos do número um, e atento o artigo 36.º do código do IVA, a prestação vence-se 30 (trinta) dias após a entrega, instalação e configuração dos bens, objeto do contrato.
3. Em caso de discordância por parte AT, quanto aos valores indicados na fatura, deve este comunicar ao fornecedor, por escrito, os respetivos fundamentos, ficando o fornecedor obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Desde que devidamente emitidas e observado o disposto no n.º 1, as faturas serão pagas através de transferência bancária.
5. O atraso no pagamento das faturas devidas pela AT confere ao adjudicatário o direito de exigir juros de mora, nos termos previstos no artigo 326.º do CCP.

Cláusula 9.ª - Patentes, licenças e marcas registadas

1. Os contraentes garantem que respeitam as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registadas, relacionadas com o hardware, Software e documentação técnica que utilizam no desenvolvimento da sua atividade.

2. A AT não assume qualquer responsabilidade por infrações cometidas pelo adjudicatário no âmbito da execução do contrato, relativamente a direitos de propriedade intelectual e industrial relacionados com o hardware, *Software* e documentação técnica por este utilizado, cujos direitos e autorizações legais para o efeito devam por ele ser assegurados.

Cláusula 10.ª - Sigilo

1. Os Contraentes obrigam-se a garantir o sigilo quanto a informação diretamente relacionada com o objeto do contrato, bem como tomar todas as medidas necessárias para que os seus funcionários e agentes se vinculem a igual obrigação, quanto aos conhecimentos que venham a ter no âmbito dos trabalhos em que estão envolvidos.
2. Os Contraentes tratarão como confidencial toda a informação por eles devidamente identificada como tal, ou que pela natureza das circunstâncias que rodeiam a sua divulgação deva, em boa fé, ser considerada como confidencial.
3. Para efeitos do disposto no número anterior, considera-se como confidencial, independentemente da sua identificação como tal, toda a informação a que o fornecedor tenha acesso relacionada com sistemas de segurança para proteção de informação, sistemas informáticos, sistemas de informação, instalações, métodos de trabalhos e *core business* da AT.
4. Carece de consentimento prévio, através da AT:
   a) A divulgação pelo adjudicatário de qualquer informação, sob qualquer forma, relacionada com o presente projeto ou com qualquer outro de que venha a ter conhecimento;
   b) A utilização do logótipo da AT para efeitos de publicidade, assim como a referência à sua qualidade de fornecedor.
5. Encontra-se excluída da presente obrigação de confidencialidade a informação que:
   a) Tenha sido prévia e legitimamente divulgada por terceiros a qualquer um dos contraentes;
   b) Se encontre disponível para o público em geral;
   c) Os contraentes tenham sido legal ou judicialmente obrigados a revelar, desde que observados os procedimentos estabelecidos para o efeito;
   d) Seja conhecida do contraente que a revelou em momento anterior à celebração do contrato;
   e) Tenha sido transmitida ao contraente por uma terceira entidade sem que lhe tenha sido imposta qualquer obrigação de confidencialidade;
   f) Os contraentes acordem, por escrito, na possibilidade da sua divulgação.

Cláusula 11.ª - Propriedade

Com a entrega e pagamento dos bens objeto do contrato ocorre a transferência da posse e da propriedade daqueles para o contraente público, sem prejuízo das obrigações de garantia que impendem sobre o fornecedor.

Cláusula 12.ª - - Procedimentos ambientais e de gestão de resíduos

1. É da inteira responsabilidade do fornecedor o destino a dar aos resíduos produzidos ou recolhidos no decurso da sua atividade, sem prejuízo de poder utilizar as estruturas da Entidade Adjudicante destinada à recolha de resíduos, caso exista, e mediante previa autorização.
2. O fornecedor deverá desenvolver as atividades objeto do presente procedimento, garantindo o cumprimento das normas ambientais aplicáveis.

Cláusula 13.ª - Nomeação de gestor

1. A Entidade Adjudicante nomeia como gestor responsável pelo contrato a celebrar……, para efeitos do disposto no artigo 290º-A do CCP.
2. O Adjudicatário obriga-se, até à data de início do contrato, a comunicar à AT, a nomeação do gestor de contrato responsável pelo contrato celebrado, bem quaisquer alterações relativamente à sua nomeação, no prazo de 5 dias. O gestor deve disponibilizar à respetiva entidade adjudicante, contatos telefónicos de e-mail de contato direto.

CAPITULO - III

PENALIDADES

Cláusula 14.ª - Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a AT pode exigir do fornecedor o pagamento de uma pena pecuniária, calculada de acordo com a fórmula: P = V x A/n.º dias do contrato, em que P corresponde ao montante da penalização, V ao valor do contrato e A ao número de dias de atraso.
2. Na determinação da gravidade do incumprimento, a AT tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do fornecedor e as consequências do incumprimento.
3. O direito à aplicação de penalidades deverá ser exercido pela AT dentro do prazo máximo de 60 (sessenta) dias sobre a data da ocorrência que lhe deu origem.
4. A importância que for devida pelo fornecedor correspondente às penalidades será deduzida, sem demais formalidades, na fatura a pagamento à data da aplicação da penalidade.
5. As penas pecuniárias previstas na presente cláusula ficam limitadas a 20% ou 30% do valor do contrato, nos termos previstos, respetivamente, nos números 2 e 3 do art.º 329.º do Código dos Contratos Públicos, consoante o caso que se aplicar.

Cláusula 15.ª - Força maior

1. Não podem ser impostas penalidades ao fornecedor dos produtos, 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 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 fosse razoavelmente exigível contornar ou evitar.
2. Constituem motivos de 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. 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 16.ª - Resolução do contrato

1. O contrato pode ser resolvido por qualquer das partes em caso de incumprimento definitivo, grave ou reiterado, e culposo por uma das Partes das obrigações por si assumidas no contrato, nos termos gerais de Direito, sem prejuízo das correspondentes indemnizações legais a que houver lugar.
2. Para efeitos do disposto no número anterior, a Parte não culposa comunicará por escrito a ocorrência da situação de incumprimento suscetível de gerar resolução contratual, concedendo à contraparte um prazo não inferior a 30 dias para que aquela reponha a situação de incumprimento, sem o que, o incumprimento se tornará definitivo e determinará a resolução contratual, nos demais termos gerais de direito.
3. O contrato pode também ser resolvido através da AT caso se verifique alguma das seguintes situações, as quais são desde já entendidas como situações de incumprimento grave e culposo por parte do fornecedor:
   a) Quando se verificar reiterada inobservância das disposições do contrato ou má fé do fornecedor;
   b) Prestação de falsas declarações;
   c) Estado de falência ou insolvência;
   d) Cessação da atividade;
   e) Condenação, por sentença transitada em julgado, por infração que afete a idoneidade profissional do fornecedor e desde que não tenha ocorrido reabilitação judicial.
4. O direito de resolução referido no número anterior exerce-se mediante declaração escrita enviada ao fornecedor.

Cláusula 17.ª - Foro competente

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

CAPITULO - IV

DISPOSIÇÕES FINAIS

Cláusula 18.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(s) deve ser comunicada à outra parte.

Cláusula 19.ª - Encargos

Correm por conta do adjudicatário todas as despesas em que este haja de incorrer em virtude das obrigações emergentes do contrato.

Cláusula 20.ª - Produção de efeitos

O contrato produz todos os seus efeitos a partir da sua assinatura.

Cláusula 21.ª - Contagem dos prazos

Na fase de execução do contrato, e para efeitos do presente caderno de encargos, todos os prazos são contínuos, correndo em sábados, domingos e dias feriados.

Cláusula 22.ª - Legislação aplicável

O contrato será regulado pela legislação portuguesa, com expressa renúncia a qualquer outra.

Anexos:

I. Consulta preliminar ao mercado (8 páginas)

XXXXX

From: XXXXX@warpcom.com>
Sent: 13 de julho de 2022 11:37
To: XXXXX
Subject: RE: Pedido de orçamento para uma solução de cibersegurança

Esta mensagem é de um remetente externo

Esta mensagem veio de fora da sua organização. Por favor evite clicar em links ou descarregar anexos se o remetente ou o teor da mensagem forem desconhecidos ou suspeitos.

Viva XXXXX,

Conforme solicitado, confirmo a disponibilidade e viabilidade de uma solução de cibersegurança de acordo com as especificações indicadas na sua consulta.

O valor de investimento s/ IVA para esta solução e serviços pretendidos, é de 338.980,49€.

Qualquer questão, pf não hesite em nos contactar.

Com os sinceros agradecimentos,

XXXXX
Sales Director
T. +351 XXXXX | M. +351 XXXXX

From: XXXXX@at.gov.pt> **Sent:** 4 de julho de 2022 19:53
To: XXXXX@warpcom.com>
Subject: Pedido de orçamento para uma solução de cibersegurança

CAUTION: This email originated from a source outside Warpcom.

Ex.mo XXXXX,
Boa tarde,

Agradeço a vossa informação com relação à disponibilidade de uma solução de cibersegurança com as características que abaixo se descriminam, donde, confirmando-se a viabilidade, agradeço ainda a indicação do valor para uma possível aquisição, **não devendo contudo serem feitas referências a marcas comerciais e modelos**.

Todos os valores a apresentar devem ser sem IVA.

- A solução de cibersegurança deve:

1. Integrar nativamente com a solução Dell Avamar e Data Domain existente na AT;
2. Toda a gestão e administração da solução de cibersegurança deverá ser feita a partir do cofre;
3. A solução de retenção de dados deve ter por base um repositório, que ao nível da gestão e retenção eletrónica de dados, cumpra com os seguintes normativos:
    i. Sarbanes-Oxley;
    ii. SEC 17a-4;
    iii. CFTC Rule 1.31b;
    iv. HIPAA;
    v. ISO Standard 15489-1;
    vi. MoREQ 2 EU.
4. Deve garantir a automação e fluxo de trabalho para um mínimo de 14 cópias "Gold" dos dados mais críticos, para um segundo repositório;
5. Deve ter processos de deteção que incidirão sobre os vetores de ataque mais utilizados, como o malware, ransomware e criptoware, sem necessidade de recurso exclusivo a deteção de assinatura maliciosa, que obrigue a uma atualização constante da solução para manter o sucesso dos índices de deteção de código malicioso.

- Deve ainda assegurar as seguintes premissas de proteção e recuperação:
    1. Planeamento e design, por avaliação dos sistemas e aplicações críticas para o negócio, infraestrutura atual, tempo de recuperação contra ciberataques/incidentes e objetivos de recuperação, para adequar a implementação da solução;
    2. Isolamento e replicação, com base nos resultados da fase de planeamento e design, de forma a implementar as condições necessárias para um cofre de recuperação contra ciberataques/incidentes;
    3. Procedimentos de analítica, por forma a salvaguardar o bom funcionamento e asseverar a eficácia das ferramentas de segurança, sendo requisito a capacidade análise de vetores de ataque, que permitam detetar possíveis comprometimentos da informação protegida;
    4. Capacidade de restauro e recuperação, a partir das imagens "Gold" das aplicações e binários de sistemas operativos, culminando na reposição do ambiente de produção no mais curto espaço de tempo possível.

- Em termos de características técnicas mínimas, a solução deve assegurar:
    1. Volume de dados:
        a. 15TB de dados do tipo VMware;
        b. 5TB de dados do tipo bases de dados;
        c. 31TB de dados do tipo Fileshare.
    2. Capacidade de desempenho e escalabilidade:
        a. Capacidade de escrita correspondente a até pelo menos 26TB/hora;

b. Capacidade de expansão, sem recursos a troca de controladores, até pelo menos 160TB úteis, excluindo efeitos de deduplicação e/ou compressão;
c. Suporte para protocolos NFS/CIFS e OpenStorage (e em simultâneo, se necessário).

3. O repositório de proteção de dados deve permitir a realização das diversas operações de backup, recuperação e replicação, sem necessidade de interrupção ou janela de tempo dedicada para as tarefas de manutenção do repositório.
4. A solução a fornecer deve incluir todo o software necessário ao bom funcionamento da mesma, incluindo-se a replicação, encriptação (sem recurso a discos especiais e/ou dedicados para o efeito) e mecanismo de retenção imutável.
5. A solução deve ser fornecida sem limites de clientes e/ou agentes aplicacionais, mas devidamente licenciada para a quantidade de front-end a analisar.
6. Visando o garante da máxima integridade dos dados armazenados, a solução deverá contemplar, ao nível do repositório de dados, os seguintes níveis mínimos de redundância e validação:
    a. Fontes de alimentação redundantes;
    b. Proteção de disco de dupla paridade (RAID 6);
    c. Mecanismos de verificação de integridade dos dados durante a escrita.
7. A solução deve ainda ser fornecida em formato PBBA (Purpose-Built Backup Appliance), isto é, deve ter um conjunto de características diferenciadoras dos restantes dispositivos appliances e storage arrays tradicionais, onde se destaca:
    a. Ser capaz de armazenar especificamente dados de backup no formato do software de backup, sendo inviável o uso dos dados para outros propósitos;
    b. Implementação de elevadas taxas de deduplicação (tipicamente 10:1 ou mais), sendo inviável o uso dos dados para outras tarefas que não recuperações;
    c. Permitir a replicação dos dados com elevada eficiência (maioritariamente devido à deduplicação dos dados), de forma a facilitar a realização de backups rápidos a partir de localizações remotas;
    d. Fornecer a tradução de protocolo (por exemplo, S3, OpenStack) para transferência de dados para repositórios de cloud (“cloud tiering”), se necessário.

- Deve ainda garantir:
    1. A proteção para um mínimo de 14 cópias da informação;
    2. A solução deverá recorrer a um isolamento lógico (do tipo *air-gap*) do cofre, desligado da rede de produção, gerido a partir do próprio cofre, e com acesso restrito apenas a utilizadores com as devidas credenciais de acesso ao cofre;
    3. A transferência de dados deve ser protegida por *handshake* digital, com encriptação do *link* de replicação e dos dados a sincronizar;
    4. Deve proteger as cópias sincronizadas através de um mecanismo de retenção certificado, que garanta a imutabilidade dos dados protegidos no cofre;

5. Deve ter processos de analítica integrada, que permita a análise periódica dos dados contidos no formato nativo de backup, sem necessidade de proceder a recuperações e efetuar a procura de indicadores de comprometimento da informação;
6. Os processos de analítica devem efetuar uma análise dos dados com recurso a indexação total de conteúdos, dentro do cofre, sem qualquer recurso ou ligação ao exterior;
7. A gestão deve ser baseada em políticas e automatização dos workflows de proteção;
8. A solução a propor deve incluir toda a infraestrutura necessária ao bom e regular funcionamento do cofre, incluindo, mas não se limitando, a: computação, armazenamento, ativos de rede e de segurança, todo o software e licenciamento necessário à análise dos dados a proteger no cofre, cabos, fibras óticas e racks.

Por último, devem ainda ser considerados os serviços de instalação, suporte e manutenção:

1. O suporte e manutenção de toda a solução fornecida deve ser assegurado diretamente e por um único fabricante, com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção e suporte pretendidos são:
   a) Garantia mínima de 2 anos;
   b) O tempo de resposta (nível de serviço) é de 4 horas, 24x7, 365 dias por ano, incluindo peças e mão-de-obra.
   c) Prestação de assistência contínua até à resolução da avaria.

Devem ainda ser incluídos todos os serviços necessários à instalação e configuração inicial do repositório de proteção de dados, bem como os serviços de interligação com a infraestrutura Dell/EMC Avamar e Data Domain existente na AT.

Antecipadamente agradecido,

Com os melhores cumprimentos,
XXXXX

.....

AT autoridade tributária e aduaneira

Sistemas de Informação
Área de Gestão de Operações e Comunicações
Núcleo de Gestão de Operações e Serviços

.....

Av. Eng. Duarte Pacheco, n.º 28 Geral: +351 XXXXX
1099 – 013 Lisboa Telef.: +351 XXXXX
Edifício Satélite Fax: +351 XXXXX

XXXXX

From: XXXXX@milestone.pt>
Sent: 13 de julho de 2022 17:06
To: XXXXX
Subject: RE: Pedido de orçamento para uma solução de cibersegurança

Boa tarde XXXXX,

No seguimento do seu pedido, informamos que existe disponibilidade de uma solução que cumpre todos os requisitos e serviços solicitados e que a mesma tem um valor de aquisição de 346.847,13€ s/ IVA.

Esta inclui igualmente todos os serviços necessários à instalação e configuração inicial do repositório de proteção de dados, bem como os serviços de interligação com a infraestrutura Dell/EMC Avamar e Data Domain existente na AT.

Ao dispor para qualquer esclarecimento necessário.

XXXXX

Manager

TM. +351 XXXXX
E.XXXXX @milestone.pt

www.milestone.pt

Estrada de Alfragide, 107
Ed.2
2610-008 Lisboa

De: XXXXX@at.gov.pt> **Enviada:** 4 de julho de 2022 19:54
Para: XXXXX@milestone.pt>
Assunto: Pedido de orçamento para uma solução de cibersegurança

Ex.mo XXXXX, Boa tarde,

Agradeço a vossa informação com relação à disponibilidade de uma solução de cibersegurança com as características que abaixo se descriminam, donde, confirmando-se a viabilidade, agradeço ainda a indicação do valor para uma possível aquisição, **não devendo contudo serem feitas referências a marcas comerciais e modelos**.

Todos os valores a apresentar devem ser sem IVA.

- A solução de cibersegurança deve:
    1. Integrar nativamente com a solução Dell Avamar e Data Domain existente na AT;
    2. Toda a gestão e administração da solução de cibersegurança deverá ser feita a partir do cofre;
    3. A solução de retenção de dados deve ter por base um repositório, que ao nível da gestão e retenção eletrónica de dados, cumpra com os seguintes normativos:
        i. Sarbanes-Oxley;
        ii. SEC 17a-4;
        iii. CFTC Rule 1.31b;
        iv. HIPAA;
        v. ISO Standard 15489-1;
        vi. MoREQ 2 EU.
    4. Deve garantir a automação e fluxo de trabalho para um mínimo de 14 cópias "Gold" dos dados mais críticos, para um segundo repositório;
    5. Deve ter processos de deteção que incidirão sobre os vetores de ataque mais utilizados, como o malware, ransomware e criptoware, sem necessidade de recurso exclusivo a deteção de assinatura maliciosa, que obrigue a uma atualização constante da solução para manter o sucesso dos índices de deteção de código malicioso.

- Deve ainda assegurar as seguintes premissas de proteção e recuperação:
    1. Planeamento e design, por avaliação dos sistemas e aplicações críticas para o negócio, infraestrutura atual, tempo de recuperação contra ciberataques/incidentes e objetivos de recuperação, para adequar a implementação da solução;
    2. Isolamento e replicação, com base nos resultados da fase de planeamento e design, de forma a implementar as condições necessárias para um cofre de recuperação contra ciberataques/incidentes;
    3. Procedimentos de analítica, por forma a salvaguardar o bom funcionamento e asseverar a eficácia das ferramentas de segurança, sendo requisito a capacidade análise de vetores de ataque, que permitam detetar possíveis comprometimentos da informação protegida;
    4. Capacidade de restauro e recuperação, a partir das imagens "Gold" das aplicações e binários de sistemas operativos, culminando na reposição do ambiente de produção no mais curto espaço de tempo possível.

- Em termos de características técnicas mínimas, a solução deve assegurar:
    1. Volume de dados:
        a. 15TB de dados do tipo VMware;

b. 5TB de dados do tipo bases de dados;
c. 31TB de dados do tipo Fileshare.

2. Capacidade de desempenho e escalabilidade:
   a. Capacidade de escrita correspondente a até pelo menos 26TB/hora;
   b. Capacidade de expansão, sem recursos a troca de controladores, até pelo menos 160TB úteis, excluindo efeitos de deduplicação e/ou compressão;
   c. Suporte para protocolos NFS/CIFS e OpenStorage (e em simultâneo, se necessário).
3. O repositório de proteção de dados deve permitir a realização das diversas operações de backup, recuperação e replicação, sem necessidade de interrupção ou janela de tempo dedicada para as tarefas de manutenção do repositório.
4. A solução a fornecer deve incluir todo o software necessário ao bom funcionamento da mesma, incluindo-se a replicação, encriptação (sem recurso a discos especiais e/ou dedicados para o efeito) e mecanismo de retenção imutável.
5. A solução deve ser fornecida sem limites de clientes e/ou agentes aplicacionais, mas devidamente licenciada para a quantidade de front-end a analisar.
6. Visando o garante da máxima integridade dos dados armazenados, a solução deverá contemplar, ao nível do repositório de dados, os seguintes níveis mínimos de redundância e validação:
   a. Fontes de alimentação redundantes;
   b. Proteção de disco de dupla paridade (RAID 6);
   c. Mecanismos de verificação de integridade dos dados durante a escrita.
7. A solução deve ainda ser fornecida em formato PBBA (Purpose-Built Backup Appliance), isto é, deve ter um conjunto de características diferenciadoras dos restantes dispositivos appliances e storage arrays tradicionais, onde se destaca:
   a. Ser capaz de armazenar especificamente dados de backup no formato do software de backup, sendo inviável o uso dos dados para outros propósitos;
   b. Implementação de elevadas taxas de deduplicação (tipicamente 10:1 ou mais), sendo inviável o uso dos dados para outras tarefas que não recuperações;
   c. Permitir a replicação dos dados com elevada eficiência (maioritariamente devido à deduplicação dos dados), de forma a facilitar a realização de backups rápidos a partir de localizações remotas;
   d. Fornecer a tradução de protocolo (por exemplo, S3, OpenStack) para transferência de dados para repositórios de cloud (“cloud tiering”), se necessário.

- Deve ainda garantir:
  1. A proteção para um mínimo de 14 cópias da informação;
  2. A solução deverá recorrer a um isolamento lógico (do tipo *air-gap*) do cofre, desligado da rede de produção, gerido a partir do próprio cofre, e com acesso restrito apenas a utilizadores com as devidas credenciais de acesso ao cofre;

3. A transferência de dados deve ser protegida por *handshake* digital, com encriptação do *link* de replicação e dos dados a sincronizar;
4. Deve proteger as cópias sincronizadas através de um mecanismo de retenção certificado, que garanta a imutabilidade dos dados protegidos no cofre;
5. Deve ter processos de analítica integrada, que permita a análise periódica dos dados contidos no formato nativo de backup, sem necessidade de proceder a recuperações e efetuar a procura de indicadores de comprometimento da informação;
6. Os processos de analítica devem efetuar uma análise dos dados com recurso a indexação total de conteúdos, dentro do cofre, sem qualquer recurso ou ligação ao exterior;
7. A gestão deve ser baseada em políticas e automatização dos workflows de proteção;
8. A solução a propor deve incluir toda a infraestrutura necessária ao bom e regular funcionamento do cofre, incluindo, mas não se limitando, a: computação, armazenamento, ativos de rede e de segurança, todo o software e licenciamento necessário à análise dos dados a proteger no cofre, cabos, fibras óticas e racks.

Por último, devem ainda ser considerados os serviços de instalação, suporte e manutenção:

1. O suporte e manutenção de toda a solução fornecida deve ser assegurado diretamente e por um único fabricante, com suporte ao nível local e preferencialmente em língua portuguesa. A manutenção e suporte pretendidos são:
   a) Garantia mínima de 2 anos;
   b) O tempo de resposta (nível de serviço) é de 4 horas, 24x7, 365 dias por ano, incluindo peças e mão-de-obra.
   c) Prestação de assistência contínua até à resolução da avaria.

Devem ainda ser incluídos todos os serviços necessários à instalação e configuração inicial do repositório de proteção de dados, bem como os serviços de interligação com a infraestrutura Dell/EMC Avamar e Data Domain existente na AT.

Antecipadamente agradecido,

Com os melhores cumprimentos,
XXXXX

.....

AT autoridade tributária e aduaneira

Sistemas de Informação
Área de Gestão de Operações e Comunicações
Núcleo de Gestão de Operações e Serviços

.....

Av. Eng. Duarte Pacheco, n.º 28 Geral: +351 XXXXX
1099 – 013 Lisboa Telef.: +351 XXXXX
Edifício Satélite Fax: +351 XXXXX