# CONTRATO

**Aquisição de uma solução para salvaguarda de ciberataques**

**Processo N.º 78/CP/AT/2024**

Celebram o presente contrato a contar da data da aposição das assinaturas eletrónicas por cada um dos outorgantes,

Como Primeiro Outorgante, o Estado Português, através da AUTORIDADE TRIBUTÁRIA E ADUANEIRA (AT), pessoal coletiva, 600084779, com sede na Rua da Prata n.º 20 e 22, 1149-027 – Lisboa, representado no ato pelo Sr. Subdiretor-geral da Área de Recursos Financeiros e Patrimoniais da AT, Dr. Nelson Roda Inácio, no uso de competência subdelegada, conforme despacho n.º 10249/2024 de 26/08/2024, publicado no D.R., 2.ª Série, n.º 168, de 30/08/2024.

Como Segundo Outorgante, o Adjudicatário, Warpcom Services, S.A., pessoa coletiva nº 505134195, com sede na Estrada de Alfragide, 67, Alfrapark, Edifício F, Piso 3, 2610-008 Lisboa, representado no presente ato por Bruno Manuel Silva Ho, com o cartão de cidadão n.º 10633039 0 ZX9, válido até 03/08/2031, na qualidade de representante legal, com poderes para outorgar o presente contrato, conforme documentos juntos ao processo, nos termos das seguintes cláusulas:

## Cláusula 1.ª
## Objeto e conteúdo funcional

1. O objeto do presente contrato é 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. <u>Solução de Recuperação contra ciberataques:</u>

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**

**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.

**Cláusula 3.ª**

**Prazo de entrega/Instalação e configuração**

O Segundo Outorgante obriga-se à entrega/Instalação e configuração dos bens, objeto do presente contrato com todos os elementos referidos no Caderno de Encargos, até à data limite de 15 (quinze) dias, contados a partir da data da outorga do contrato.

**Cláusula 4.ª**

**Prazo de execução**

O Segundo Outorgante obriga-se à execução do contado a partir da data da outorga do contrato até 31 de dezembro de 2024.

**Cláusula 5.ª**

**Preço contratual**

1. O preço contratual é de €338.980,00 (trezentos e trinta e oito mil, novecentos e oitenta euros), S/IVA, de forma a incluir todas as prestações objeto do presente contrato.

2. O preço referido no número anterior inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída ao Primeiro Outorgante, 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 Segundo Outorgante.
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 6.ª**

**Condições de pagamento**

1. A quantia devida pelo Primeiro Outorgante, nos termos da cláusula anterior, deve ser paga no prazo de 60 (sessenta) dias após a receção da respetiva fatura, devendo constar o número do procedimento/contrato e enviada de acordo com o artigo 299.º-B do CCP, a qual só poderá ser emitida após o vencimento da obrigação correspondente.
2. Para efeitos do disposto no número anterior, a obrigação considera-se vencida com a entrega, instalação e configuração dos bens, objeto do contrato
3. Em caso de discordância por parte do Primeiro Outorgante, quanto aos valores indicados na fatura, deve este comunicar ao Segundo Outorgante, por escrito, os respetivos fundamentos, ficando o Segundo Outorgante obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. Desde que devidamente emitidas e observado o disposto no número um, as faturas serão pagas através de transferência bancária.
5. O atraso no pagamento das faturas devidas pelo Primeiro Outorgante confere ao Segundo Outorgante o direito de exigir juros de mora, nos termos previstos no artigo 326.º do CCP.

**Cláusula 7.ª**

**Caução**

Não há lugar a prestação de caução, nos termos do n.º 2 do art.88º do CCP.

**Cláusula 8.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 9.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 10.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 11.ª**

**Nomeação de Gestor**

1. O Primeiro Outorgante nomeia como gestor responsável pelo contrato a celebrar o Eng.º Luis Lopes Encarnação, Chefe de Equipa Multidisciplinar de 2.º Nível da Área de Gestão de Operações e Comunicações da AT, para efeitos do disposto no artigo 290º-A do CCP.
2. O Segundo Outorgante designa como gestor do contrato o Sr. João Santos, com os seguintes contatos: Email joao.santos@warpcom.com e Tel: 927113803.

**Cláusula 12.ª**

**Despesas**

Correm por conta do Segundo Outorgante todas as despesas em que este haja de incorrer em virtude de obrigações emergentes do contrato a celebrar.

**Cláusula 13.ª**

**Legislação aplicável**

O contrato é regulado pelo disposto no Código dos Contratos Públicos, aprovado pelo Decreto-Lei n.º 18/2008, de 29 de janeiro na sua atual redação e respetiva legislação regulamentar.

**Cláusula 14.ª**

**Disposições Finais**

1. Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.
2. Os pagamentos ao abrigo do presente contrato serão efetuados após a verificação dos formalismos legais em vigor para o processamento das despesas públicas.

3. A decisão de contratar relativa ao presente contrato foi autorizada pelo despacho de 14-10-2024, do Sr. Subdiretor-geral da Área de Recursos Financeiros e Patrimoniais da AT, exarado no processo registado em GPS através do número 691020246912007101, contendo apensa a informação n.º 2412/DC/AT/2024, datada de 2024-10-11, no uso de competência subdelegada.
4. Por despacho de 08-11-2024, do Sr. Subdiretor-geral da Área de Recursos Financeiros e Patrimoniais da AT, exarado no processo registado em GPS através do número 691020246912007203 contendo apensa a informação n.º 2506/DC/AT/2024, datada de 2024-11-04, no uso de competência subdelegada, foi adjudicado o fornecimento objeto do presente contrato, bem como aprovada a minuta relativa ao presente contrato.
5. O encargo total resultante do presente contrato, será suportado por conta de verbas inscritas no orçamento de funcionamento da AT de 2024, sob a rubrica com a classificação económica da despesa 02.02.05.B0.00 – Locação Material Informático, a que corresponde o compromisso n.º 6952425933.

Pelo Segundo Outorgante foi declarado que aceita o presente contrato com todas as suas condições de que tem inteiro e perfeito conhecimento e a cujo cumprimento se obriga.

**Primeiro Outorgante**

Nelson Roda Inácio
Assinado de forma digital por Nelson Roda Inácio
Dados: 2024.11.15 19:41:24 Z

Nélson Roda Inácio
(Autoridade Tributária e Aduaneira)

**Segundo Outorgante**

BRUNO MANUEL SILVA HO
Digitally signed by BRUNO MANUEL SILVA HO
Date: 2024.11.15 10:02:41 Z

Bruno Manuel Silva Ho
(Warpcom Services, S.A..)

| AUTORIDADE TRIBUTÁRIA E ADUANEIRA (AT) | | |
|---|---|---|
| DIRECÇÃO DE SERVIÇOS GESTÃO DE RECURSOS FINANCEIROS | | |
| REGISTO Nº | X | 24IN31300293 |
| ANOTAÇÃO Nº | | |
| 18/11/2024 | Fátima Nunes | |

Fátima Nunes
Assistente Técnico