CONCURSO PÚBLICO PARA AQUISIÇÃO DE HARDWARE E SOFTWARE, INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE, COM VISTA À MELHORIA DA INFRAESTRUTURA TECNOLÓGICA DE DATA CENTER, BACKUP E SITE DE RECUPERAÇÃO

CADERNO DE ENCARGOS

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

PARTE I

Cláusulas jurídicas

Cláusula 1.ª

Objeto

O objeto do contrato consiste na aquisição de software e hardware, incluindo serviços de instalação, configuração e suporte, com vista à melhoria da infraestrutura tecnológica de data center, backup e site de recuperação, de acordo com as cláusulas técnicas descritas na Parte II deste caderno de encargos.

Cláusula 2.ª

Preço base

O preço base (preço máximo) do contrato a celebrar é de **167.342,31€**, valor ao qual acresce o IVA à taxa legal em vigor.

Cláusula 3.ª

Consulta preliminar ao mercado

Nos termos do disposto nos artigos 47.º, n.º 3 e 35.º - A, ambos do Código dos Contratos Públicos (CCP), previamente ao presente procedimento foi efetuada consulta preliminar ao mercado, tendo sido o preço base estabelecido com base na média dos orçamentos obtidos na sequência de consulta preliminar ao mercado.

Cláusula 4.ª

Local de entrega e instalação

Os bens objeto do presente contrato serão entregues e instalados no edifício da sede da Câmara Municipal da Amadora (CMA), localizado na Av. do Movimento das Forças Armadas 1, 2700-595 Amadora.

Cláusula 5.ª

Prazo de entrega e implementação da solução

O prazo máximo de entrega e de implementação é de 60 dias a contar da celebração do contrato.

Cláusula 6.ª

Gestor do contrato

Nos termos do disposto no artigo 290.º-A, conjugado com o artigo 96.º, n. º 1 alínea i), ambos do Código dos Contratos Públicos, as funções de gestor do contrato serão desempenhadas pelo técnico especialista de Sistemas e Tecnologias de Informação João Pinto.

Cláusula 7.ª

Condições de pagamento

1. Os pagamentos só serão efetuados depois de comprovado o cumprimento do contrato, no prazo de 30 dias após apresentação de fatura, em conformidade com o definido na presente cláusula.
2. O cocontratante, depois de concluída a execução integral do contrato, deverá no prazo de 10 dias, enviar ao gestor do contrato prova do cumprimento, nomeadamente, auto com os fornecimentos e serviços prestados, documentação produzida ou trocada, registos fotográficos, ou outro, para efeitos de validação.
3. O gestor do contrato poderá, no decurso da execução, emanar diretivas genéricas sobre a forma mais adequada de o cocontratante prestar prova do cumprimento, para efeitos do disposto nos dois números anteriores.
4. O gestor do contrato dispõe de 10 dias para validar a prova de execução enviada pelo cocontratante. Em caso de discordância, rejeita a validação do cumprimento de forma devidamente fundamentada ou solicita documentação e prova adicional do cumprimento, dispondo o cocontratante, neste último caso, de 5 dias para remeter a documentação adicional necessária.
5. Depois de obtida a validação da prova de execução por parte do gestor do contrato, pode o cocontratante emitir fatura, devendo o pagamento ocorrer no prazo de 30 dias a contar da data de envio da fatura.
6. Nos pagamentos a efetuar ao cocontratante, serão deduzidos os descontos e as penalidades que lhe tenham sido aplicados.
7. Não são permitidos adiantamentos.
8. Nos termos do n.º 4, do artigo 299.º, do CCP, o prazo de pagamento não deverá exceder em qualquer caso, os 60 dias.

Cláusula 8.ª

Sigilo

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

1. O cocontratante deve guardar sigilo sobre toda a informação e documentação relativa ao contraente público de que possa ter conhecimento no âmbito da execução do contrato.
2. A informação e a documentação, cobertas pelo dever de sigilo, não pode em caso algum ser transmitida a terceiros, nem 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 documentação que seja comprovadamente do domínio público à data da respetiva obtenção pelo cocontratante ou que este esteja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

Cláusula 9.ª - Patentes, licenças e marcas registadas

1. São da responsabilidade do cocontratante quaisquer encargos decorrentes da utilização, na pr\estação de serviços, de marcas registadas, patentes registadas ou licenças.
2. Caso o contraente público venha a ser demandado por ter infringido, na execução do contrato, qualquer dos direitos mencionados no número anterior, o cocontratante indemniza-o 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 - Seguros

É da responsabilidade do cocontratante a cobertura, através de contratos de seguro de responsabilidade civil, de acidentes pessoais/de trabalho, conforme aplicável, bem como, o seguro de todo o material e demais equipamento que sejam sua propriedade ou que estejam a qualquer título em seu poder e que sejam utilizados na preparação e execução do contrato, se aplicável, nos termos da legislação em vigor à data da celebração do contrato.

Cláusula 11.ª

Cessão da posição contratual

O cocontratante não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato.

Cláusula 12.ª

Incumprimento e penalidades

1. Por cada dia de incumprimento do prazo de entrega indicado na proposta, o cocontratante ficará sujeito ao pagamento de multa de até 1% do preço contratual, a graduar em função da gravidade

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

do incumprimento.

2. Por cada dia de incumprimento das demais obrigações contratuais, o cocontratante ficará sujeito ao pagamento de multa de até 0,5% do preço contratual, a graduar em função da gravidade do incumprimento.
3. O gestor do contrato, em caso de incumprimento, poderá elaborar o enquadramento dos factos, enquadramento contratual e valor previsível da penalidade, e notificar o cocontratante para o exercício de audiência prévia por um período de 10 dias. Findo esse prazo e depois de ponderada a pronúncia eventualmente apresentada, o gestor do contrato pode propor ao órgão competente do contraente público a aplicação de penalidades.
4. As penalidades aplicadas descontam nos pagamentos subsequentes do contrato.

Cláusula 13.ª – Cessão da posição contratual por incumprimento

Em caso de incumprimento, pelo cocontratante, das suas obrigações, que reúna os pressupostos para a resolução do contrato, o cocontratante pode vir a ceder a sua posição contratual, nos termos do disposto no artigo 318.º-A do CCP.

Cláusula 14.ª

Resolução do contrato pelo contraente público

Sem prejuízo das causas de resolução previstas no artigo 333.º do CCP, o contraente público pode resolver o contrato a título sancionatório caso, decorram mais de 30 dias desde o termo do prazo para entrega e implementação da solução, sem que o cocontratante tenha apresentado justificação que evidencie que o atraso não lhe é imputável.

Cláusula 15.ª

Tratamento de dados pessoais

1. Nos termos e para os efeitos previstos no Regulamento Geral de Proteção de Dados (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, os eventuais dados pessoais que venham a ser transmitidos no presente procedimento serão tratados com a finalidade de gestão e conclusão daquele, ou para outras finalidades que decorram de obrigações legais a que o contraente público esteja adstrito.

2. Todos os dados pessoais que vierem a figurar no contrato a celebrar serão tratados com a finalidade de formação e execução da relação contratual, ou para outras finalidades que decorram de obrigações legais a que o contraente público esteja adstrito.

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

Cláusula 16.ª

Foro competente

O foro competente para dirimir quaisquer conflitos decorrentes do presente contrato é o do tribunal administrativo que tenha jurisdição sobre o Município da Amadora.

PARTE II

Cláusulas técnicas

1- Enquadramento

O dimensionamento da infraestrutura de Data Center (DC), a melhoria do sistema de backups, a evolução do site secundário para um site de recuperação de desastres (DR), são fundamentais para garantir a continuidade dos negócios, a segurança da informação e a conformidade legal (obrigações legais, regulamentares e outras).

Esta renovação tecnológica da infraestrutura que, atualmente, suporta os serviços core, é um investimento necessário e que tem em conta os seguintes princípios: performance, alta disponibilidade e escalabilidade.

Adicionalmente, e potenciando os recursos tecnológicos já existentes, pretende-se implementar uma solução de Disaster Recovery que permita a recuperação rápida dos serviços no site secundário (Atual DC BFPS ou possível nova localização nos Estaleiros Municipais). Para um grupo mais restrito de workloads, pretende-se dotar de mais uma linha de defesa adicional contra malware, replicando os sistemas mais críticos em tempo real, com capacidade de imutabilidade e CDP (Continuous Data Protection), o que permitirá recuperar os sistemas protegidos para um qualquer ponto de restauro de forma rápida e eficaz, com reduções drásticas de RPO (Recovery Point Objective) e RTO (Recovery Time Objective).

2- Requisitos técnicos

2.1 Servidores de virtualização

Deverão ser propostos três (3) servidores de virtualização com as seguintes características mínimas:

1. Formato rackmountable com dimensão não superior a 1U;

2. Inclusão de kit de rack com braço de gestão de cablagem traseiro;
3. Dois (2) processadores do tipo Intel Xeon-Gold 6426Y com 16 Cores e 2.5Ghz de clock, ou equivalente;
4. 512 GB de memória RAM, com recurso a DIMMs Dual Rank x4 DDR5-4800 de capacidade não inferior a 64 GB;
5. Capacidade máxima suportada até 8 Terabytes de memória RAM DDR5-4800 através de 32 slots (16 por processador);
6. Dispositivo de boot dedicado para instalação de sistema operativo, com dois (2) discos de 480GB NVMe M.2 SSDs hot-plug, com capacidade de criação automática de RAID1 por hardware;
7. Suporte até pelo menos dez (10) discos internos no mesmo chassi;
8. Módulo de gestão, com consola remota e porta 1Gb Ethernet dedicada, com capacidade de federação, capacidade de controlo energético, atualizações de firmware, configurações na BIOS e Virtual Media Unificado;
9. Suporte para sistema de gestão remota do equipamento em regime de power-off;
10. Sistema de instalação e gestão de sistema operativo e firmware remotamente;
11. Uma (1) placa de rede dual-port 10Gb BASE-T (cobre);
12. Uma (1) placa Host Bus Adapter Fibre Channel dual-port de 32Gbps;
13. Deverá incluir todos os cabos de fibra necessários;
14. Fontes de alimentação Titanium com certificação de eficiência 80 PLUS até 96%, hot-plug, redundantes, com capacidade mínima de 1.000W;
15. Suporte para Windows Server 2019 e 2022; VMware ESXi 7.0 U3, 8.0, 8.0 U1, 8.0 U2 e 8.0 U3; Red Hat Enterprise Linux (RHEL) 8.6 e 9.0; SUSE Linux Enterprise Server (SLES) 15 SP4; Ubuntu 20.04.5 LTS; Oracle Linux 9;
16. Deverá ser proposto, juntamente com os servidores, software de gestão que permita as seguintes funcionalidades:
    a. Compatibilidade com instalação em servidor(es) virtual(is), sem a necessidade de licenciamento adicional de sistema operativo ou base de dados de suporte à aplicação;
    b. Interface gráfico web baseado em HTML 5 e compatível com web browsers de dispositivos móveis;
    c. Monitorização e alarmística para servidores, switches de rede, equipamentos de armazenamento de dados e PDU's monitorizáveis;
    d. Monitorização de consumos energéticos e temperaturas para servidores

e. Funcionalidades avançadas de pesquisa e filtragem em todo o ambiente, com resultados em modo gráfico da localização do item pesquisado;
f. Vista gráfica de datacenter e dos respetivos equipamentos e localização em bastidor, incluindo mapa térmico;
g. Gestão de arrays de armazenamento, com criação automática de volumes de dados;
h. Instalação automatizada (unattended) de sistema operativo via rede, compatível Microsoft Windows Server, VMware ESXi, RedHat Enterprise Linux, SUSE Linux;
i. Gestão centralizada de firmwares e drivers, incluindo instalação de firmware de firmware online;
j. Consola remota com Virtual KVM Web-Based e capacidade para 6 users concorrentes, Virtual Power, Virtual Media (DVD, PEN USB ou pasta de ficheiros), acesso seguro SSL/AES/RC4, Consola SSH;
k. Suporte dado pelo fabricante da solução onde será instalado o software de gestão (Servidores, Storage);

17. Capacidade de assegurar que o servidor não executa código de firmware que possa estar comprometido, com validação em runtime, bem como capacidade para fazer rollback para o firmware de fábrica;
18. Compatibilidade nativa com sistema Security Protection Data Model (SPDM) que permite a verificação e a autenticação dos componentes compatíveis com esta tecnologia;
19. O servidor deverá incluir sistema de monitorização em cloud, sem custos, que inclua tecnologia de inteligência artificial para análise e tratamento de eventos relacionados com suporte preditivo e mitigação de risco. Todo o licenciamento e infraestrutura, caso exista, devem estar incluídos para a totalidade da solução.

    Este sistema deverá disponibilizar, pelo menos, a seguinte informação:

    a. Inventário global de servidores em todos os Datacenters;
    b. Dashboard com o estado dos servidores;
    c. Dashboard operacional global;
    d. Capacidade de aprendizagem global com deteção preditiva de eventuais problemas;
    e. Relatório global de garantia e suporte dos servidores;
    f. Inventário detalhado do servidor (hardware, opções, firmware, drivers e software) com relatórios;
    g. Coleta automática de dados de telemetria e sensores sem a utilização de recursos do host para o efeito;
    h. Análise preditiva de falha de peças dos servidores;

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

i. Análise de problemas de firmware, driver, SO / hypervisor e software do sistema;
j. Notificação por e-mail de alertas.

2.2 Array de Armazenamento

Deverá ser proposto um (1) Array de armazenamento de alto débito. O Array deve garantir as seguintes especificações mínimas:

1. Tecnologia All-NVMe End-to-end;
2. Duas controladoras em arquitetura simétrica "full-mesh" com coerência de cache em que os volumes são acedidos simultaneamente por todas as controladoras;
3. Capacidade de escalar linearmente até quatro (4) controladoras em arquitetura simétrica full-mesh;
4. Deve ser do tipo mission-critical, com uma disponibilidade de 100% comprovada em site público do fabricante;
5. O sistema operativo do Array deverá ser baseado em serviços (service-centric) em que cada serviço possa ser implementado, atualizado e reiniciado de forma independente;
6. Tem de apresentar, no mínimo, 256 GB de memória por controladora, sem recurso a discos SSD/NVMe para o efeito;
7. Deverá ser fornecido com uma capacidade de 31.3 TB úteis (antes de deduplicação/compressão ou qualquer outra tecnologia de otimização de espaço em disco) em discos do tipo NVMe SSD não superiores a 3.84 TB, com implementação de RAID 6;
8. Deverá permitir capacidade de expansão para, no mínimo, um total de 384 discos;
9. O chassi base do Array em conjunto com eventuais gavetas de expansão a propor não deverão ultrapassar os 2U’s em bastidor;
10. Deverá disponibilizar um total de 8 portas Fibre Channel a 32 Gb (4 por cada controladora) para conetividade a hosts (front-end)
11. O Array deve suportar até, pelo menos, um total de 32 portas para conetividade a hosts (front-end);
12. O Array deverá suportar de forma nativa os seguintes protocolos: Fibre Channel, iSCSI, NVMe-oF;
13. A conetividade back-end a eventuais futuras gavetas de expansão do Array deverá ser feita através de ligações a 100 GbE;
14. Os volumes devem ser distribuídos por todos os discos (wide-striping) de forma a tirar partido total da performance do Array;

15. Deverá incluir funcionalidades nativas de otimização de dados entre as quais: Thin Provisioning, Zero Detection, Compressão e Deduplicação (in-line);
16. Deverá incluir funcionalidades nativas de proteção de dados entre as quais: Virtual Volumes, Snapshots e Virtual Clones;
17. Deverá incluir uma ferramenta de backup nativa para realização de backups diretos (sem recurso a softwares de backup);
18. Deverá suportar e incluir capacidade de replicação remota de dados nativa;
19. Deverá permitir encriptação FIPS total por hardware;
20. O Array deve ter capacidade multi-tenant com gestão individualizada, possibilidade de definição de utilizadores dedicados, níveis de serviços diferenciados, e garantia de desempenho máximo e mínimo por Array lógico;
21. O software deve incluir funcionalidades de QoS (Quality of Service) com possibilidade de definição de níveis de SLA por volume;
22. Todas as funcionalidades do Array devem vir incluídas de base sem necessidade de licenciamento adicional;
23. Deverá suportar, no mínimo, os seguintes Sistemas Operativos: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi;
24. Deverá suportar mecanismo nativos de migração a partir do Array de armazenamento existente (HPE 3PAR 8200).

2.3. Repositório de backups para disco

Deverão ser propostos dois sistemas X86, com capacidade de armazenamento, para ser utilizado como repositório de backup para disco. Os sistemas deverão garantir as seguintes especificações mínimas:

1. Formato rack-mountable com dimensões não superiores a 2U em bastidor;
2. Inclusão de kit de montagem em bastidor;
3. Um processador Intel Xeon-Silver 4410Y com 12 Cores e 2.0Ghz de clock, ou equivalente;
4. Capacidade para suportar até dois processadores;
5. 128 GB de memória RAM, utilizando DIMMs Dual Rank x4 DDR5-4800 não inferiores a 64 GB;
6. Capacidade para suportar até 12 slots DIMM, por processador;
7. Suporte mínimo de 4 Terabytes de RAM DDR 4800 MT/s;
8. Controladora de discos interna, com 8GB de cache FBWC dedicada, suportada por condensador híbrido, e capacidade para suportar RAID 0, 1, 5, 6, 10, 50, 60, e RAID 1 e 10 com

tripla paridade; capacidade de expansão online do array e da capacidade lógica e migração online de tipo de RAID;

9. Dois discos de M.2 NVMe Solid-State Drive (SSDs) de 480GB, em RAID 1 por Hardware, para instalação de Sistema Operativo;
10. Oito (8) discos de 12TB SATA 7.2K LFF HDD, para dados, com capacidade de serem retirados "a quente", com luz indicadora de utilização (para evitar perca de dados ou downtime, devido a remoção indevida de discos);
11. Uma (1) placa de rede dual-port 10Gb BASE-T (cobre);
12. Módulo de gestão com porta 1Gb Ethernet dedicada;
13. Capacidade de gestão remota com capacidade de federação, controlo energético, atualizações de firmware, configurações na BIOS e Virtual Media Unificado;
14. Suporte para sistema de gestão remota do equipamento em regime de power-off;
15. Sistema de instalação e gestão de sistema operativo e firmware remotamente;
16. Suporte de UEFI**;**
17. Suporte para RESTful API;
18. Capacidade de assegurar que o servidor não executa código de firmware que possa estar comprometido, com validação em runtime, bem como capacidade para fazer rollback para o firmware de fábrica;
19. Fontes de alimentação com certificação de eficiência 80 PLUS Platinum até 94%, hot-plug, redundantes, com capacidade mínima de 1.600W;
20. Suporte para Windows Server 2019 e 2022; VMware ESXi 7.0 U3, 8.0, 8.0 U1, 8.0 U2 e 8.0 U3; Red Hat Enterprise Linux (RHEL) 8.6 e 9.0; SUSE Linux Enterprise Server (SLES) 15 SP4; Ubuntu 22.04 LTS e 24.04 LTS;
21. Capacidade de integração nativa com o software de Backup atualmente em uso na CM Amadora (Veeam Backup & Replication) para maior performance de escrita e leitura;
22. Deverá ser proposto, juntamente com os servidores, software de gestão que permita as seguintes funcionalidades:
    a. Compatibilidade com instalação em servidor(es) virtual(is), sem a necessidade de licenciamento adicional de sistema operativo ou base dedados de suporte à aplicação;
    b. Interface gráfico web baseado em HTML 5 e compatível com web browsers de dispositivos móveis;
    c. c. Monitorização e alarmística para servidores, switches de rede, equipamentos de armazenamento de dados e PDU's monitorizáveis;
    d. Monitorização de consumos energéticos e temperaturas para servidores;

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

e. Funcionalidades avançadas de pesquisa e filtragem em todo o ambiente, com resultados em modo gráfico da localização do item pesquisado;
f. Vista gráfica de datacenter e dos respetivos equipamentos e localização em bastidor, incluindo mapa térmico;
g. Gestão de arrays de armazenamento, com criação automática de volumes de dados;
h. Instalação automatizada (unattended) de sistema operativo via rede, compatível Microsoft Windows Server, VMware ESXi, RedHat Enterprise Linux, SUSE Linux;
i. Gestão centralizada de firmwares e drivers, incluindo instalação de firmware de firmware online;
j. Consola remota com Virtual KVM Web-Based e capacidade para 6 users concorrentes, Virtual Power, Virtual Media (DVD, PEN USB ou pasta de ficheiros), acesso seguro SSL/AES/RC4, Consola SSH;
k. Suporte dado pelo fabricante da solução onde será instalado o software de gestão (Servidores, Storage);

23. Capacidade de assegurar que o servidor não executa código de firmware que possa estar comprometido, com validação em runtime, bem como capacidade para fazer rollback para o firmware de fábrica.
24. Apenas para o equipamento do repositório de backup que ficará localizado no ambiente Produtivo, deve ser contemplado um HBA (Host Bus Adapter) dual-port Fibre Channel 16Gb, de forma interligar uma biblioteca de tapes HPE MSL4048 existente, com duas drives LTO-6.

2.4 Conectividade

Pretende-se interligar os vários componentes da solução com algum nível de redundância, com os seguintes requisitos mínimos:

1. Ligar os servidores de virtualização ao array de armazenamento através de FC (fibra) a 32Gbps ligando cada uma das portas a uma controladora do array diferente;
2. Ligar os servidores de virtualização à rede da CMA em ethernet (cobre) a 10Gbps ligando cada uma das portas a um switch diferente;
3. Ligar o array de armazenamento à rede da CMA em ethernet (cobre) a 10Gbps ligando cada uma das portas a um switch diferente;
4. Ligar os repositórios de backup para disco à rede CMA em ethernet (cobre) a 10Gbps ligando cada uma das portas a um switch diferente;
5. Ligar o repositório de backup para disco que ficará no DC Sede através de FC (fibra) a 16Gbps à HPE MSL4048 usando as duas portas.

As ligações FC (fibra) poderão ser efectuadas de forma directa (Direct attach) ou através de switchs FC a incluir na proposta visto que a CMA já tem os switchs necessários para suportar as conexões ethernet (cobre).

2.5 Software de Disaster Recovery e Replicação

Deverá ser proposto licenciamento para software de Disaster Recovery e Replicação entre dois sites com as seguintes funcionalidades mínimas:

6. Licenciamento do software de Disaster Recovery e Replicação para um mínimo de 10 VMs;
7. Consola web-based com gestão gráfica simplificada;
8. Capacidade de suportar Continuous Data Protection (CDP) com replicação near sync e sem impacto na performance;
9. O software de Disaster Recovery e replicação deverá utilizar réplicas de I/O nas máquinas virtuais sem recurso a agentes ou snapshots;
10. Capacidade de configurar políticas de CDP (Continuous Data Protection) que garantam por defeito o menor intervalo possível com possibilidade de ter RPOs de segundos;
11. A replicação near sync deverá utilizar réplicas de I/O das máquinas virtuais entre os sites A e B;
12. A replicação deverá ter por base um sistema de journaling com milhares de checkpoints que permitam recuar no tempo de forma granular e recuperar os dados de uma máquina virtual até 30 dias;
13. Suporte para capacidade de orquestração, automação e analítica avançada para a simplificação do processo de failover;
14. Capacidade de analisar e detetar padrões anómalos de escritas de I/O e/ou encriptação de dados de forma a mitigar ataques de ransomware;
15. O software deverá criar automaticamente tags no jornal da replicação sempre que detetar padrões anómalos de escrita ou atividade suspeita de ransomware;
16. Capacidade de integração via API com ferramentas existentes de segurança como SIEM ou SOAR;
17. Deverá ter a capacidade de replicar dados entre sites assim como infraestruturas em cloud pública (AWS, Google Cloud, Azure);
18. A replicação deverá ter funcionalidades de um-para-muitos, permitindo uma VM replica simultaneamente para várias plataformas como VMware vSphere, Microsoft Hyper-V, Azure, AWS enquanto replica localmente ou para um site secundário;

19. Possibilidade de recuperação de componentes individuais num grupo de proteção como VMs, ficheiros ou pastas;
20. Capacidade de implementação de MFA (multi-factor authentication) para vários utilizadores;
21. Suporte para execução de uma ou mais VMs diretamente de um backup num ambiente isolado (Sandbox), com a capacidade de solucionar problemas, testar numa cópia do ambiente de produção, sem interferir nas operações;
22. Deverá permitir a configuração de grupos de proteção por tipologias de VM com capacidade de recuperação consistente de diversas aplicações;
23. Recuperação automatizada e rápida das aplicações através da pré-configuração de ordem de boot, rede e endereços de IP.

2.6 Suporte (Especificações da assistência técnica):

1. Para todos os equipamentos descritos nos pontos anteriores deverão ser considerados serviços de suporte com a duração de três (3) anos com tempo de resposta de quatro (4) horas, on-site, 24/7 prestado pelo fabricante do equipamento;
2. O suporte deve ser disponibilizado sempre em português de Portugal durante todo o horário de cobertura (24x7) e através de um único ponto de contacto para todo o tipo de incidentes de Hardware e Software. O tempo de resposta (Call-Back), a contar partir da abertura da chamada de verá ser de:
    a. até 15 minutos para incidentes críticos (sistemas parados)
    b. até 1 hora para incidentes não críticos;
3. No caso dos servidores, o suporte dado pelo fabricante deve incluir suporte colaborativo para Sistemas Operativos que incluem: Microsoft Windows Server e Red Hat, SUSE;
4. Deverá ser implementada uma solução de suporte que permita a abertura automática de chamadas, no caso de incidentes de falha ou pré-falha de algum componente de hardware;
5. Os serviços de reparação deverão ser realizados apenas por técnicos de equipas residentes em Portugal e devidamente credenciados pelo fabricante do equipamento;
6. A reparação de hardware deverá apenas ser realizada com peças genuínas do fabricante dos equipamentos;
7. Deverá ser disponibilizado um portal/ferramenta que permita uma visão global e em tempo real do estado de suporte de todos os equipamentos registados. Deverá também permitir a abertura de chamadas de suporte e o acompanhamento de todos os casos abertos.

2.7 Serviços de Instalação e configuração

Deverão ser incluídos os serviços necessários para a instalação e start-up dos equipamentos propostos, bem como a configuração da solução na sua totalidade:

1. Reunião de kick-off com a equipa de projeto da CM Amadora;
2. Levantamento de pré-requisitos para definição de configurações técnicas;
3. Desenho detalhado e definição de configurações necessárias à sua operacionalização;
4. Instalação física em bastidores existentes dos equipamentos propostos e interligação à LAN/SAN;
5. Configuração inicial dos equipamentos propostos e da sua rede de gestão com validação de acessos;
6. Atualizações e upgrades de firmware de acordo com as recomendações do fabricante;
7. Ligação dos servidores de virtualização ao Array de armazenamento proposto

a. garantindo redundância de caminhos;

8. Configuração de cluster de virtualização de três (3) Nós, baseado em Microsoft Hyper-V, com alta disponibilidade;
9. Migração dos workloads existente na atual infraestrutura;
10. Configuração da solução de Backup recorrendo ao software de Backup existente (Veeam Backup & Replication) e integração de todos os repositórios incluídos na solução;
11. Implementação das políticas de backup a definir em conjunto com a CM Amadora;
12. Implementação de um ambiente de DR em site secundário recorrendo a equipamento existente na CM Amadora e configuração e parametrização das políticas de replicação entre o ambiente Produtivo e o DR, recorrendo ao software de Backup atualmente em uso (Veeam Backup & Replication);
13. Instalação e parametrização do software de disaster recovery e replicação com políticas de Continuous Data Protection e proteção anti-ransomware entre sites;
14. Testes funcionais para validação da solução implementada e do seu bom funcionamento;
15. Participação com as equipas internas da CM Amadora em testes de compatibilidade, recuperação, failover e funcionais;
16. Documentação com descrição detalhada da solução implementada.

3. Declarações:

Av. Movimento das Forças Armadas, n.º 1, 2700-595 Amadora | Portugal
T [+351] 214 369 000 | geral@cm-amadora.pt | www.cm-amadora.pt

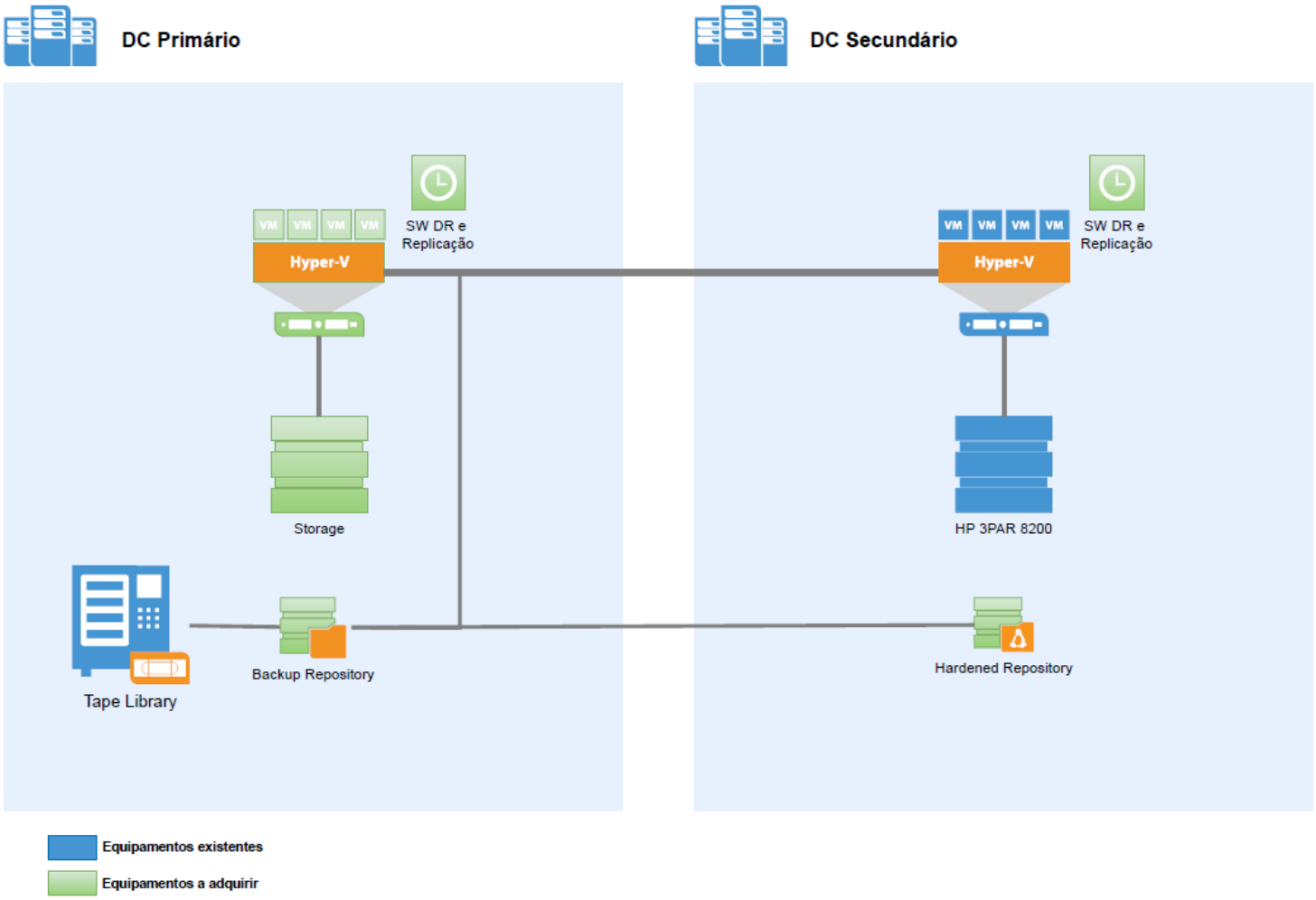
O proponente deverá apresentar a seguinte informação relativamente aos produtos propostos:

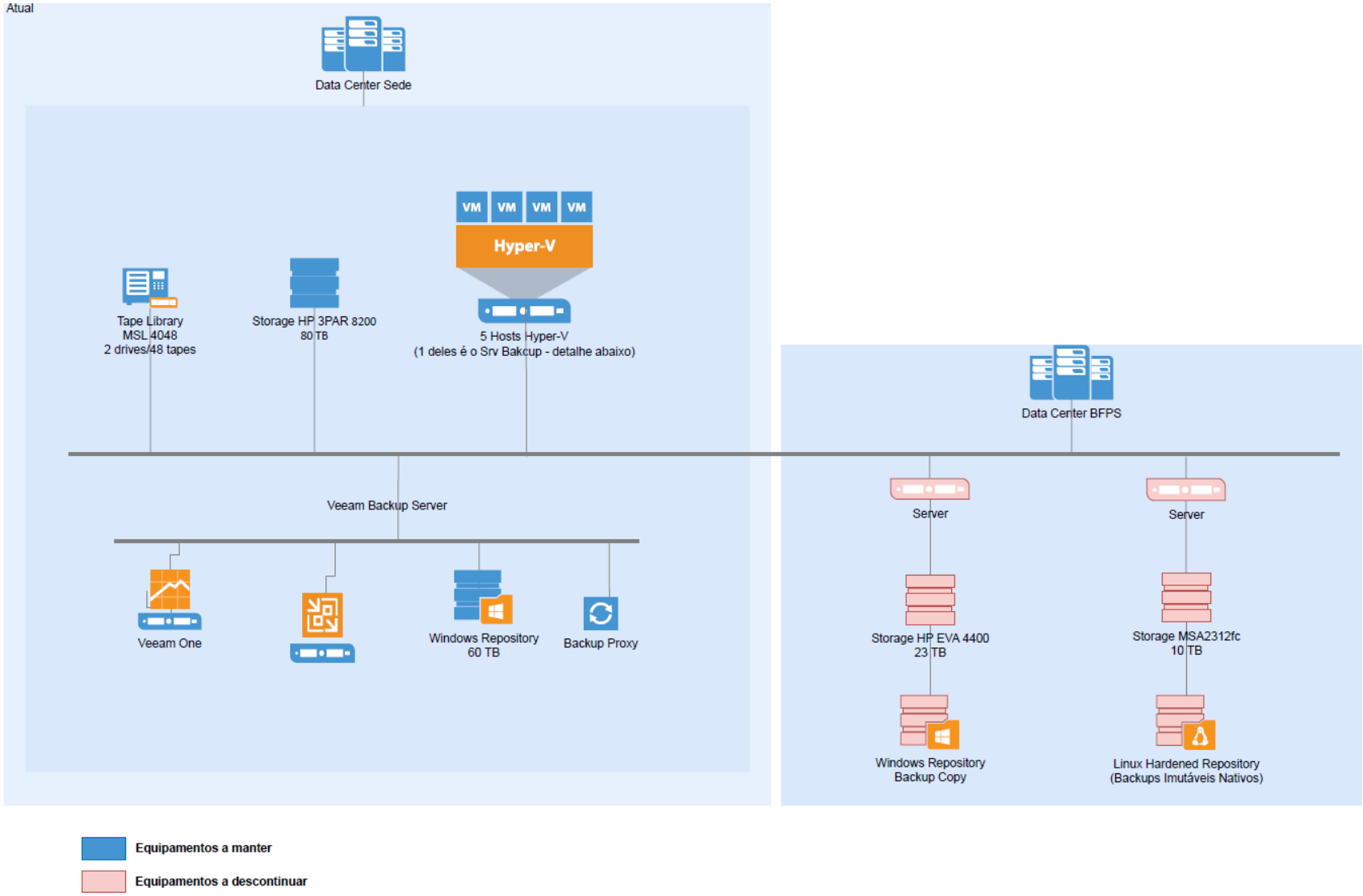
1. Declaração do fabricante onde conste o conhecimento técnico da infraestrutura e responsabilidade pela solução apresentada na proposta;
2. Declaração que ateste que o integrador detém o nível de parceria máximo com o fabricante do hardware e software solicitado no presente caderno de encargos;
3. Declaração do fabricante que ateste a sua capacidade em instalar e configurar os equipamentos que irão fazer parte da solução da CM Amadora.

PRESIDENTE

VITOR FERREIRA

Dimensionamento Infraestrura DC - Hypervisor - Storage - Backups - DR




Atual
Data Center Sede
VM
VM
VM
VM
Hyper-V
Tape Library
MSL 4048
2 drives/48 tapes
Storage HP 3PAR 8200
80 TB
5 Hosts Hyper-V
(1 deles é o Srv Bakcup - detalhe abaixo)
Veeam Backup Server
Veeam One
Windows Repository
60 TB
Backup Proxy
Data Center BFPS
Server
Server
Storage HP EVA 4400
23 TB
Storage MSA2312fc
10 TB
Windows Repository
Backup Copy
Linux Hardened Repository
(Backups Imutáveis Nativos)
Equipamentos a manter
Equipamentos a descontinuar