tourcenter

Rua Barros de Alfredo, Matosinhos, 4450-203
21 380 3511
support@tourcenter.com

Data:
Maio 16, 2024

Planeamento e Projeto de Infraestrutura de Rede

Índice

Visão Geral da Proposta

A TourCenter tem o prazer de submeter à PowerWind – Wind Electric Power Generation, S.A. a presente proposta técnica para o desenvolvimento e modernização da infraestrutura de rede da empresa. Esta proposta foi preparada com base num estudo detalhado das necessidades e requisitos específicos identificados nas instalações da PowerWind, com o objetivo de otimizar e expandir a capacidade da rede existente, garantindo assim uma maior eficiência e segurança nas operações diárias e futuras.

A presente proposta delineia um plano que inicia com um levantamento técnico detalhado para avaliar a infraestrutura atual da PowerWind, identificando áreas que necessitam de melhorias ou de maior integração. Segue-se uma análise minuciosa dos requisitos, durante a qual determinamos as necessidades específicas de *hardware*, *software* e conectividade que se alinhem com as finalidades operacionais e de segurança da PowerWind. Com base nesta análise, propomos um projeto de arquitetura de rede robusto, escalável e adaptável às necessidades futuras da empresa. Este projeto focará em soluções de LAN e WAN, integrando as melhores práticas de segurança e eficiência operacional, garantindo assim que a infraestrutura IT da PowerWind esteja preparada para suportar tanto as operações atuais quanto os desafios futuros no setor de energia eólica *offshore*.

Levantamento de Existências, Necessidades e Condicionantes

Estado Atual

A infraestrutura IT da PowerWind, situada predominantemente na sua sede no distrito de Viana do Castelo, atualmente consiste num conjunto de sistemas que foram estabelecidos para suportar as operações iniciais e agora necessitam de avaliação para futura expansão e modernização. A empresa dispõe de uma variedade de *hardware*, incluindo servidores dedicados para a gestão administrativa, projetos, desenvolvimento e manutenção, além de múltiplos PCs *desktop* que, conforme relatado pelos utilizadores, estão a tornar-se obsoletos e lentos, o que afeta a eficiência operacional. Em termos de *software*, a PowerWind utiliza uma gama de aplicações específicas para a gestão de projetos de energia eólica, além de *software* administrativo padrão para funções de contabilidade, recursos humanos e comunicação interna. No entanto, os sistemas operativos e as aplicações estão em diversas versões, o que pode representar um risco em termos de segurança e compatibilidade.

A rede de dados existente é baseada numa infraestrutura de cablagem que não foi totalmente atualizada para acompanhar o crescimento recente da empresa, resultando em desafios de conectividade e gestão de tráfego de rede. Além disso, a segurança da rede é uma preocupação crescente, especialmente considerando a necessidade de conexões seguras para comunicação entre a sede, a nave industrial, e entidades externas, incluindo subcontratados e fornecedores.

Necessidade identificadas

Na PowerWind, a modernização da infraestrutura de rede é crucial para sustentar o crescimento e a diversificação das operações. Os computadores e servidores atuais tornaram-se obsoletos e lutam para suportar as exigências diárias, tornando imperativa a sua substituição por equipamentos mais modernos e eficientes, capazes de lidar com o aumento do volume de trabalho e de dados. Além disso, com os departamentos espalhados por diferentes pisos e uma nave industrial separada, existe uma necessidade premente de fortalecer e fiabilizar a rede. Isto inclui a melhoria do sistema de cablagem existente, a instalação de Wi-Fi de alta eficiência e a garantia de conexões seguras entre todas as localizações da empresa.

A segurança da rede é uma preocupação primordial, especialmente devido à necessidade de comunicação segura com fornecedores e parceiros externos. Portanto, é essencial implementar soluções de segurança de rede atualizadas, como *firewalls*, sistemas de deteção e prevenção de intrusões (IDS e IPS) e redes privadas virtuais (VPN). Além disso, considerando que a gestão de toda a infraestrutura atualmente recai sobre um único técnico, é crítico reforçar a equipa de IT. Para além disso, é também importante fornecer ferramentas avançadas que facilitem a gestão e manutenção da rede que ajudará a otimizar os recursos e melhorar a resposta a eventuais problemas.

No que diz respeito à impressão, especialmente a de grandes formatos que é frequente em projetos da PowerWind, é vital que as soluções de impressão não só sejam económicas, mas também totalmente integradas à rede da empresa para assegurar eficiência e facilidade de acesso.

Finalmente, qualquer nova infraestrutura deve ser desenhada para ser tanto flexível quanto escalável. Isso garante que futuras expansões ou modificações possam ser implementadas facilmente, sem a necessidade de revisões completas do sistema existente.

Condicionantes

Alguns desafios específicos são derivados da localização e das características físicas das instalações da empresa, isto é, a proximidade ao mar pode acelerar a corrosão e causar outros danos aos equipamentos, o que requer medidas especiais para proteção contra a humidade e a salinidade. Para além disso, a presença de maquinaria pesada na nave industrial pode causar interferências eletromagnéticas, afetando a performance da rede, o que necessitará de soluções específicas como *shielding* para mitigar essas interferências. Por fim, a instalação da infraestrutura de rede deverá ser planeada e executada em consonância com as obras de adaptação do edifício, para assegurar a integração eficiente da infraestrutura de rede com as instalações físicas, evitando refazer trabalhos na infraestrutura e garantindo uma implementação sem falhas.

Análise de Requisitos

Hardware

1. **Servidores**

- **Servidor de Projeto e Desenvolvimento:** Devido à necessidade de processar grandes volumes de dados, é recomendado um servidor com processadores de alto desempenho, no mínimo 128 GB de RAM e SSDs em configuração RAID para melhor desempenho e redundância.
- **Servidor Administrativo:** Deverá suportar as operações administrativas diárias, incluindo contabilidade e recursos humanos. Recomenda-se um servidor com pelo menos 64 GB de RAM e capacidade de armazenamento adequada para documentos e *backups* diários.
- **Servidor de Gestão:** Para gerir toda a infraestrutura, um servidor dedicado com ferramentas avançadas de monitorização e gestão de rede é essencial. Este servidor deve também estar equipado com *software* de segurança atualizado e capacidades de *backup*.

2. ***Workstations***

- **Departamentos de Engenharia e Desenvolvimento:** PCs de alto desempenho com processadores rápidos, no mínimo 32 GB de RAM e placas gráficas dedicadas para suportar *software* de *design* e simulação.

- **Departamento Administrativo e Comercial:** PCs com requisitos moderados, sugerindo processadores de médio alcance, 16 GB de RAM e com gráficas integradas que são suficientes para tarefas administrativas e de gestão.
- **Receção e Áreas Comuns:** Estações de trabalho mais básicas para tarefas gerais de escritório, *internet* e acesso a sistemas internos.

3. **Equipamentos de Rede**

- ***Switches* e *Routers*:** Deverão suportar altas taxas de transferência de dados e incluir funcionalidades avançadas de segurança para dividir o tráfego de rede entre departamentos e proteger dados sensíveis.
- **Soluções de Wi-Fi:** *Access points* de alta capacidade para cobrir completamente os espaços de escritório e a nave industrial, garantindo conectividade estável e segura para todos os dispositivos.

4. **Armazenamento e *Backup***

- **Soluções de Armazenamento em Rede (NAS/SAN):** Para armazenamento de dados centralizado e *backups*, recomendam-se dispositivos NAS/SAN com capacidades de encriptação e suporte para RAID, facilitando a gestão de dados e a recuperação em caso de falhas.
- **Soluções de *Backup Offsite*:** Contratar serviços de *backup* na *cloud* para garantir redundância de dados e proteção contra perda de dados em caso de desastres naturais ou falhas técnicas.

5. **Dispositivos Periféricos**

- **Impressoras e *Plotters*:** Para o departamento de projetos, manter *plotters* de alta capacidade para impressão de grandes formatos é essencial. Impressoras multifuncionais devem ser distribuídas estrategicamente pelos outros departamentos para eficiência e facilidade de acesso.

6. **Software de Gestão de Rede**

- **Ferramentas de Monitorização e Gestão:** Adotar soluções que permitam monitorizar o desempenho da rede em tempo real, gerir configurações de segurança e identificar rapidamente quaisquer problemas ou vulnerabilidades.

Cablagem

1. **Cablagem para Áreas Administrativas e de Escritório**

- **Tipo de Cabo:** Cat6A
- **Descrição:** O cabo de categoria 6A suporta frequências até 500 MHz e é adequado para 10GBASE-T (*Ethernet* de 10 Gbps). É mais do que suficiente para as necessidades administrativas e de escritório, proporcionando uma margem para futuras atualizações de rede.
- **Utilização:** Deve ser usado nas conexões de *desktops*, impressoras e outros dispositivos de rede nos escritórios, incluindo o departamento de direção, *marketing* e áreas comerciais.

2. **Cablagem para Áreas de Engenharia e Desenvolvimento**

- **Tipo de Cabo:** Cat6A ou superior
- **Descrição:** Dada a necessidade de grandes transferências de dados e o uso intensivo de aplicações como CAD e *software* de simulação, o Cat6A é o mínimo recomendado.
- **Utilização:** Em todas as estações de trabalho de engenharia e desenvolvimento, além de servidores dedicados a essas funções.

3. **Cablagem para a Nave Industrial**

- **Tipo de Cabo:** Cabo blindado Cat6A ou Fibra Ótica
- **Descrição:** A nave industrial pode ter problemas com interferências eletromagnéticas devido à operação de maquinaria pesada. O uso de cabo blindado (STP - *Shielded Twisted Pair*) ou fibra ótica é essencial para garantir a integridade e segurança da transmissão de dados.
- **Utilização:** Conexões entre o *hardware* de rede (*switches*, *routers*) e os PCs industriais, além de sistemas de monitorização e controlo de máquinas.

4. **Conexões entre Edifícios**

- **Tipo de Cabo:** Fibra Ótica
- **Descrição:** Para interligar o edifício principal com a nave industrial e outros edifícios, a fibra ótica é a melhor escolha devido à sua imunidade a interferências eletromagnéticas e capacidade de suportar distâncias maiores sem perda de sinal.
- **Utilização:** Conexões de *backbone* que ligam os diferentes edifícios da PowerWind, garantindo uma comunicação de alta velocidade e confiável entre todas as localizações.

Desempenho

1. **Capacidade de Banda Larga**

A PowerWind requer uma infraestrutura de rede que suporte uma largura de banda substancial para acomodar o volume e a complexidade das suas operações. Com a intensificação do uso de aplicações para projetos de engenharia eólica e a necessidade de comunicações constantes entre a sede, a nave industrial e parceiros externos, é crucial que a largura de banda seja suficiente para evitar congestionamentos e atrasos. A empresa deverá ter uma ligação à internet com capacidade de no mínimo 1 Gbps simétricos, com opções de escalabilidade conforme o crescimento das necessidades. Este requisito é essencial para suportar a transferência de dados intensiva, não apenas internamente, mas também com clientes e fornecedores internacionais, garantindo agilidade e eficácia nas operações.

2. **Velocidade de Processamento**

Os servidores da PowerWind devem ser equipados para lidar com aplicações de alta exigência e outras ferramentas de engenharia usadas no *design* de componentes de turbinas eólicas. Estes servidores precisam de processadores de alto desempenho, idealmente com múltiplos núcleos para facilitar o processamento paralelo e maximizar a eficiência. A capacidade de processamento deve ser complementada com uma

quantidade robusta de RAM — sugerimos no mínimo 64 GB por servidor — para suportar múltiplas operações simultâneas sem degradação do desempenho.

3. **Taxas de Transmissão de Dados**

As velocidades de *upload* e *download* dentro da rede interna e para o exterior devem ser suficientemente rápidas para manter a eficiência operacional, reduzindo o tempo de resposta para todas as atividades empresariais. É recomendado que a rede interna opere a no mínimo 10 Gbps nos *switches* principais para facilitar um tráfego fluido de dados, especialmente para aplicações que exigem grandes transferências de dados, como *backups* de servidores ou transferências de ficheiros de grandes dimensões. Para a internet, além da largura de banda básica mencionada, deve-se garantir que as taxas de *upload* não sejam significativamente inferiores às de *download*, pois a comunicação bidirecional eficaz é crucial para colaborações remotas e serviços *cloud based*.

Conectividade

1. **Interconexão entre Sede e Nave Industrial**

A eficiência na comunicação entre a sede da PowerWind e a nave industrial é crucial devido à integração necessária das operações de engenharia e produção. Para garantir uma conectividade robusta e segura, recomendamos a implementação de um link de fibra ótica dedicado entre os dois locais. Este link não só proporcionará uma largura de banda elevada, capaz de suportar todas as transmissões de dados em tempo real, como também minimizará as latências. A fibra ótica é resistente a interferências eletromagnéticas, o que é particularmente importante dada a presença de maquinaria pesada na nave industrial que pode gerar tais perturbações.

2. **Conexões Remotas**

Com a crescente necessidade de flexibilidade no trabalho, incluindo a possibilidade de colaboração remota com fornecedores e subcontratados, a PowerWind necessitará de uma infraestrutura de rede privada virtual (VPN) robusta e segura. A VPN permitirá que os trabalhadores remotos, incluindo os engenheiros em campo ou em outras localizações geográficas, acedam à rede corporativa de maneira segura e eficaz. Deverão ser implementadas políticas de segurança restritas, incluindo autenticação multifator e encriptação, para proteger os dados sensíveis da empresa contra acessos não autorizados.

3. **Redundância na Conexão**

Para assegurar a alta disponibilidade da rede e minimizar o tempo de inatividade, a PowerWind deve considerar a implementação de uma estratégia de redundância nas suas conexões de rede. Isto inclui ter múltiplas linhas de internet de diferentes fornecedores e, idealmente, rotas de fibra ótica que entram no edifício por caminhos físicos distintos. Esta abordagem não só protegerá a empresa contra falhas de um único fornecedor, como também garantirá uma continuidade operacional em caso de danos físicos a uma das rotas. Adicionalmente, recomenda-se o uso de *switches* e *routers* com suporte para *failover* automático, o que garante uma troca rápida para uma conexão de backup sem intervenção manual e sem perda percetível de serviço.

Segurança

1. Proteções contra Ameaças Externas e Internas

Para assegurar a integridade e a confidencialidade dos dados da PowerWind, é fundamental implementar uma camada robusta de proteção contra ameaças tanto externas como internas. Recomenda-se a instalação de *firewalls* nos pontos de entrada da rede, que ofereçam prevenção contra intrusões e filtragem de tráfego *web*. Estes dispositivos deverão ser configurados para atualizações automáticas a fim de garantir proteção contra as ameaças mais recentes.

Além disso, todos os *endpoints* da rede, incluindo PC's *desktop* e portáteis, devem estar protegidos com *software* antivírus e que seja capaz de detetar e neutralizar *software* malicioso em tempo real. A configuração de acesso a redes baseada em princípios de menor privilégio e a segmentação de rede são também essenciais para minimizar o risco de movimentos laterais de ameaças dentro da organização.

2. Políticas de Segurança de Dados

É crucial desenvolver e implementar políticas de segurança de dados rigorosas, que regulamentem o acesso, o compartilhamento e o armazenamento de informações sensíveis. Estas políticas devem incluir:

- **Controlo de Acesso:** Definir claramente quem tem acesso a quais dados e em que circunstâncias. Utilizar autenticação multifatorial para acessos a sistemas críticos.
- **Encriptação de Dados:** Encriptar todos os dados sensíveis em repouso e em trânsito, utilizando algoritmos fortes e comprovados para garantir a sua integridade e confidencialidade.
- **Auditorias de Segurança:** Realizar auditorias regulares para garantir a conformidade com as políticas estabelecidas e identificar quaisquer práticas inseguras ou vulnerabilidades.

3. Monitorização e Gestão de Segurança

A implementação de ferramentas e práticas para a monitorização contínua da rede e a resposta rápida a incidentes de segurança é um pilar fundamental para a proteção da infraestrutura IT. Deverá ser estabelecido um sistema de gestão de eventos e informações de segurança (SIEM) que registe e analise *logs* de todos os dispositivos e aplicações em tempo real. Este sistema ajudará a identificar padrões anormais ou atividades suspeitas que possam indicar uma tentativa de ataque ou uma falha de segurança.

Para além disso, é importante desenvolver e testar um plano de resposta a incidentes que inclua procedimentos claros para a contenção, erradicação e recuperação de ataques. Este plano deve ser acompanhado de formação regular para a equipa de IT e simulações de incidentes para garantir uma resposta eficaz e coordenada sob condições de stress.

Escalabilidade

1. Flexibilidade da Rede

A capacidade de adaptar e expandir a infraestrutura de rede é fundamental para acompanhar o crescimento contínuo da PowerWind. A rede deve ser projetada com uma arquitetura modular, permitindo a fácil inclusão de mais utilizadores, dispositivos e serviços sem necessidade de reconfigurações significativas ou interrupções operacionais. Utilizar tecnologias como *switches* e *routers* escaláveis e implementar topologias de rede que suportem expansão, como redes definidas por *software* (SDN), são passos essenciais para garantir esta flexibilidade.

A segmentação de rede através de VLANs (*Virtual Local Area Networks*) e a implementação de políticas de acesso dinâmico permitirão que novos grupos de utilizadores e dispositivos sejam integrados com segurança e eficiência, garantindo ao mesmo tempo que os recursos de rede são alocados de forma otimizada. Este planeamento cuidadoso assegura que a rede não só atenda às necessidades atuais, mas também esteja preparada para o crescimento futuro sem requerer investimentos desproporcionais.

2. Atualizações de Equipamentos

Manter a infraestrutura IT atualizada é crucial para a sustentabilidade e eficácia operacional a longo prazo. A política de atualização de *hardware* e *software* da PowerWind deve ser proativa e alinhada com as melhores práticas da indústria. Deverá incluir a avaliação regular do desempenho e da capacidade dos equipamentos existentes, bem como um plano de substituição escalonado que minimize interrupções e maximize o retorno sobre o investimento.

Para o *hardware*, recomenda-se estabelecer ciclos de vida útil claros para cada tipo de dispositivo, com atualizações planeadas antes que os equipamentos atinjam o fim da sua eficiência operacional. Para o *software*, é essencial garantir que todos os sistemas operativos, aplicações e ferramentas de gestão estejam sempre atualizados com as últimas versões disponíveis, beneficiando assim das melhorias de segurança e desempenho mais recentes.

Adicionalmente, a adoção de soluções baseadas em *cloud* para certas aplicações e dados pode oferecer escalabilidade e flexibilidade adicional, permitindo à PowerWind ajustar rapidamente os recursos de acordo com as necessidades operacionais e de mercado, sem a necessidade de investimentos significativos em infraestrutura física.

Fiabilidade

1. Soluções de Backup e Recuperação

Para garantir a estabilidade e a segurança dos dados críticos da PowerWind, é essencial implementar sistemas de *backup* robustos e estratégias de recuperação de desastres bem definidas. Os backups devem ser realizados de forma regular e automática, utilizando uma combinação de soluções locais e na *cloud* para maximizar a proteção e a disponibilidade dos dados.

Recomenda-se a configuração de *backups* incrementais diários e *backups* completos semanais, armazenados em locais geograficamente dispersos para proteger contra perdas de dados causadas por desastres naturais ou falhas técnicas no local principal. Além disso, é crucial testar regularmente os procedimentos de recuperação para assegurar que são eficazes e que permitem um rápido restauro dos sistemas em caso de falha.

A implementação de um plano de recuperação de desastres detalhado é também uma medida indispensável. Este plano deve incluir instruções claras sobre como proceder em diferentes cenários de falhas, designação de responsabilidades específicas para a equipa de IT e informações de contacto essenciais. O objetivo é minimizar o tempo de inatividade e garantir a continuidade das operações empresariais sob qualquer circunstância.

2. **Manutenção e Suporte Técnico**

A manutenção regular da infraestrutura e o suporte técnico adequado são fundamentais para a estabilidade da rede e para prevenir problemas antes que eles causem impactos operacionais significativos. A PowerWind deve estabelecer *Service Level Agreement* (SLAs) com fornecedores de serviços que detalhem claramente as expectativas de tempo de resposta e de resolução de problemas.

Estes SLAs devem incluir suporte técnico disponível 24/7, especialmente para incidentes críticos que possam afetar as operações principais da empresa. Além disso, a manutenção preventiva da rede deve ser realizada periodicamente para verificar a saúde dos servidores, *switches*, *routers* e outras componentes críticas, e para atualizar *firmware* e *software* conforme necessário.

A inclusão de monitorização proativa da rede também é recomendada, utilizando ferramentas que possam alertar a equipa de IT sobre questões potenciais antes que elas evoluam para falhas sérias. Isto inclui a monitorização do desempenho da rede, a utilização de recursos e a deteção de padrões anormais que possam indicar problemas emergentes.

Acessibilidade

1. **Formação e Documentação**

Para maximizar a eficácia da nova infraestrutura é fundamental disponibilizar formação adequada aos colaboradores. Esta formação deve ser abrangente, abordando todos os aspetos técnicos e práticos do uso das novas ferramentas e sistemas. Deve-se considerar a realização de sessões de formação presenciais ou virtuais, *workshops* interativos e seminários regulares como parte de um programa de formação contínua que ajude os colaboradores a manterem-se atualizados com as últimas tecnologias e práticas.

Além da formação, é essencial fornecer documentação detalhada para todas as novas ferramentas e sistemas. Esta documentação deve incluir manuais do utilizador, FAQs (perguntas frequentes), tutoriais em vídeo e guias de resolução de problemas que possam ajudar os colaboradores a resolver autonomamente questões menores sem necessidade de assistência técnica direta. A documentação deve ser facilmente acessível, idealmente armazenada numa localização centralizada como um portal interno ou uma

base de conhecimento online, onde os colaboradores possam procurar e encontrar informações rapidamente.

Ambientais e *Compliance*

1. **Conformidade com Normas**

A empresa deve aderir às normas nacionais e internacionais que regulam a proteção de dados, cibersegurança e a operação de infraestruturas críticas. Isto inclui, por exemplo, a conformidade com o Regulamento Geral de Proteção de Dados (RGPD) para a proteção de dados pessoais dentro da União Europeia, bem como normas como ISO/IEC 27001 para a gestão da segurança da informação.

A implementação de um sistema de gestão de *compliance* que monitorize continuamente a conformidade com estas normas é crucial. Devem ser realizadas auditorias regulares, tanto internas como externas, para garantir que todos os sistemas e processos estão em conformidade e para corrigir quaisquer desvios ou vulnerabilidades identificadas.

2. **Considerações Ambientais**

Recomenda-se a utilização de equipamentos eletrónicos com proteção contra a humidade, que possam ser selados contra a entrada de ar salino. Além disso, as instalações que abrigam a infraestrutura, como *data centers*, devem ser desenhadas com sistemas de climatização e de ventilação apropriados para controlar a umidade e reduzir a exposição a contaminantes corrosivos. O uso de desumidificadores e sistemas de filtração de ar pode ser necessário para manter as condições ambientais dentro dos parâmetros seguros para o equipamento eletrónico.

Características de cada um dos locais

A nova infraestrutura da empresa é constituída por dois edifícios. Um edifício principal com 3 pisos onde se encontram vários departamentos e uma Nave Industrial onde se realiza a produção de componentes para parques eólicos.

O edifício principal tem 3 pisos sendo tendo esse as seguintes características:

- **Piso 0:**
  - Receção – 2 utilizadores
  - Área de exposição.

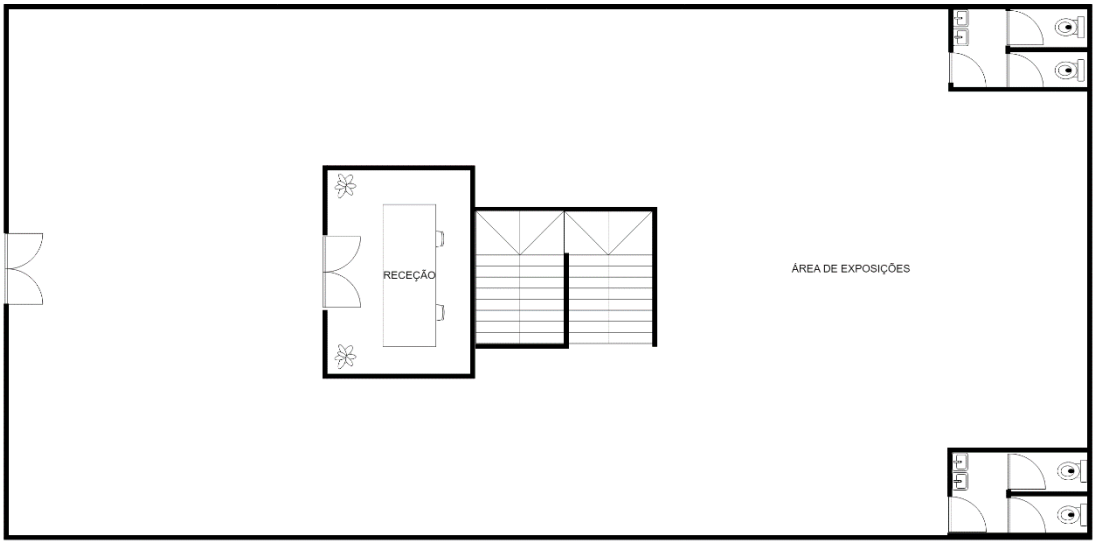


Figura 1 - Piso 0

- **Piso 1:**
  - Departamento de Projetos - 8 utilizadores
  - Departamento de Desenvolvimento e Manutenção - 12 utilizadores

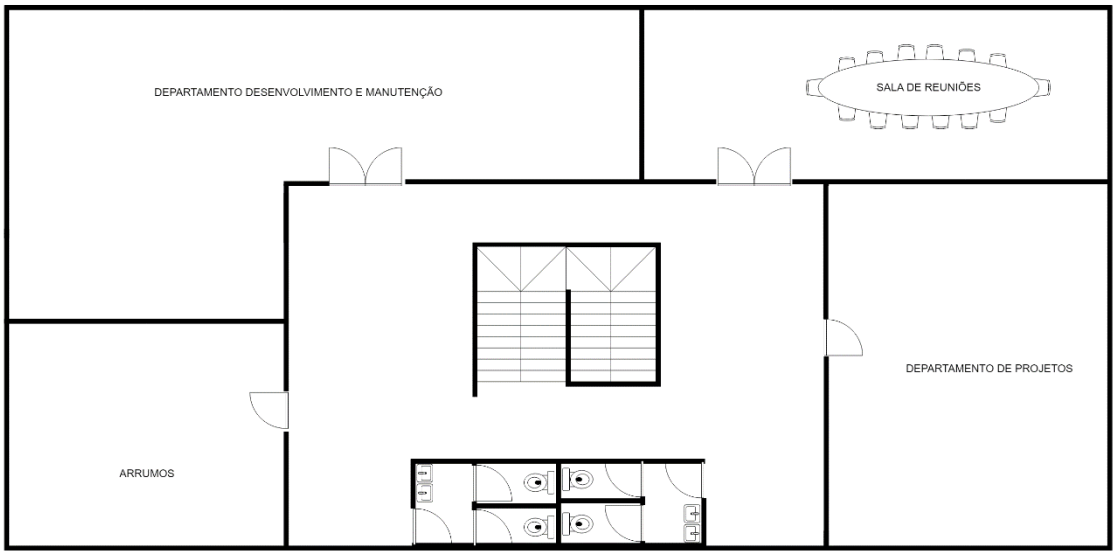


Figura 2 - Piso 1

- **Piso 2:**
  - Direção - 3 utilizadores
  - Serviços Administrativos - 3 utilizadores
  - Departamento de *Marketing* - 8 utilizadores
  - Departamento Comercial - 7 utilizadores
  - Sala de Informática - 2 utilizadores

- Diretor do Departamento Comercial - 1 utilizador

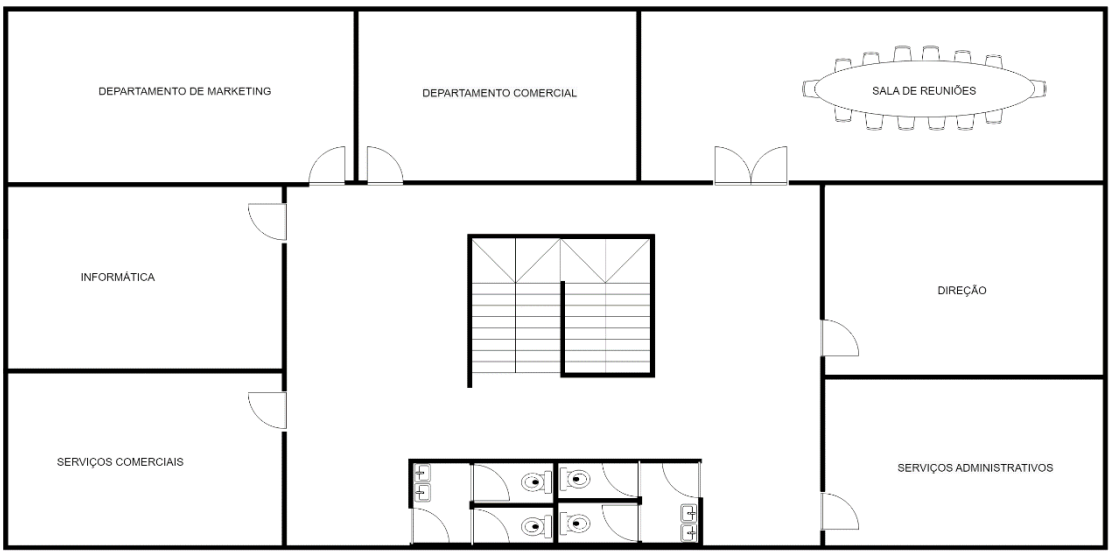


Figura 3 - Piso 2

- **Nave Industrial:**
  - Zona de Produção – 12 utilizadores
  - Auditório/Sala de Formação
  - Zona de Testes

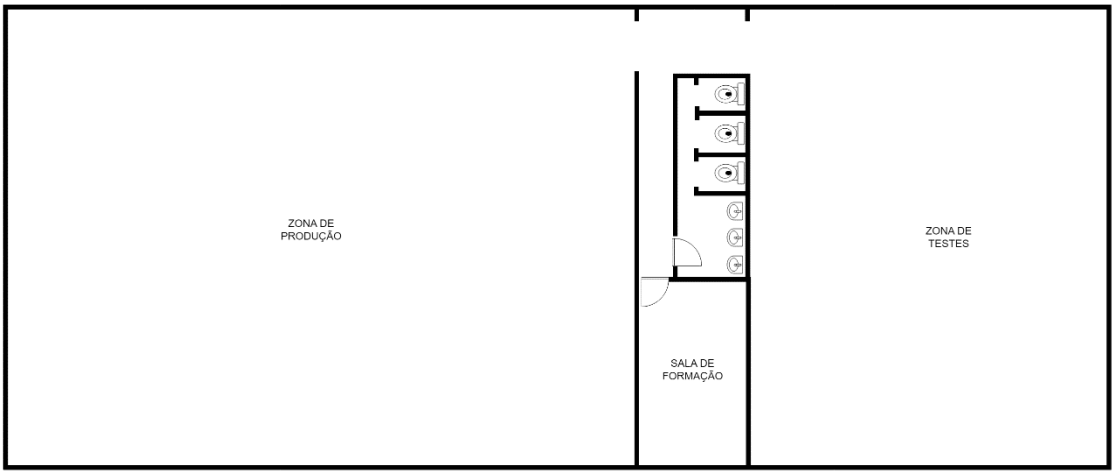


Figura 4 - Nave industrial

Sistema de Cablagem

Esta secção detalha o sistema de cablagem estruturada projetado para a **PowerWind**. A implementação segue as normas TIA/EIA-568-C, utilizando cablagem Categoria 6a (Cat6a) para suportar velocidades de até 10 Gbps, e uma topologia em estrela hierárquica. Este projeto visa garantir uma infraestrutura de rede robusta, escalável e segura, adequada para as necessidades atuais e futuras da empresa.

Premissas e Normas:

- **Normas Utilizadas**: TIA/EIA-568-C (Telecommunications Cabling Standards)
- **Tipo de Cablagem**: Categoria 6a (Cat6a) para suportar até 10 Gbps
- **Topologia**: Estrela Hierárquica
- **Distância Máxima**: 100 metros por segmento de cablagem horizontal
- **Segurança e Separação de Redes**: Uso de VLANs para segmentação de tráfego por departamento

Subsistemas de Cablagem:

1. **Subsistema de Backbone de Campus**
   O distribuidor de campus (CD) será instalado na sede da PowerWind, conectando todos os edifícios do campus, incluindo a nave industrial, com fibra óptica monomodo para alta taxa de transferência e resistência a interferências.
   O CD será equipado com conectores LC para facilitar a conexão com outros distribuidores.

2. **Subsistema de Backbone de Edifício**
   Cada edifício terá um distribuidor de edifício (BD) localizado no piso térreo para interligar os distribuidores de piso (FD) em cada andar. Será utilizado cabo de fibra óptica multimodo OM4 para garantir uma conexão rápida e confiável entre os andares.

3. **Subsistema de Piso (Cablagem Horizontal**
   Em cada andar de cada edifício, serão instalados distribuidores de piso (FD) para interligar as tomadas de telecomunicações (TO) às estações de trabalho. Será utilizado cabo UTP Cat6A para garantir uma conexão Ethernet de alta velocidade e baixa latência.
   Os FDs serão equipados com patch panels e tomadas RJ-45 para facilitar a conexão dos dispositivos finais.

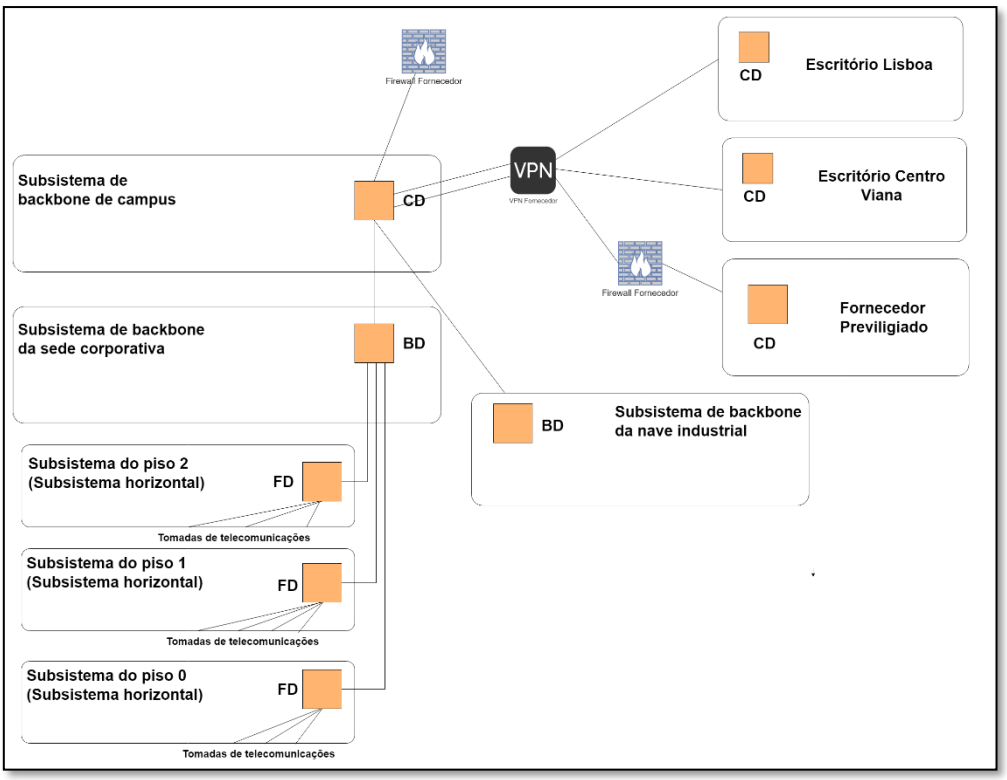
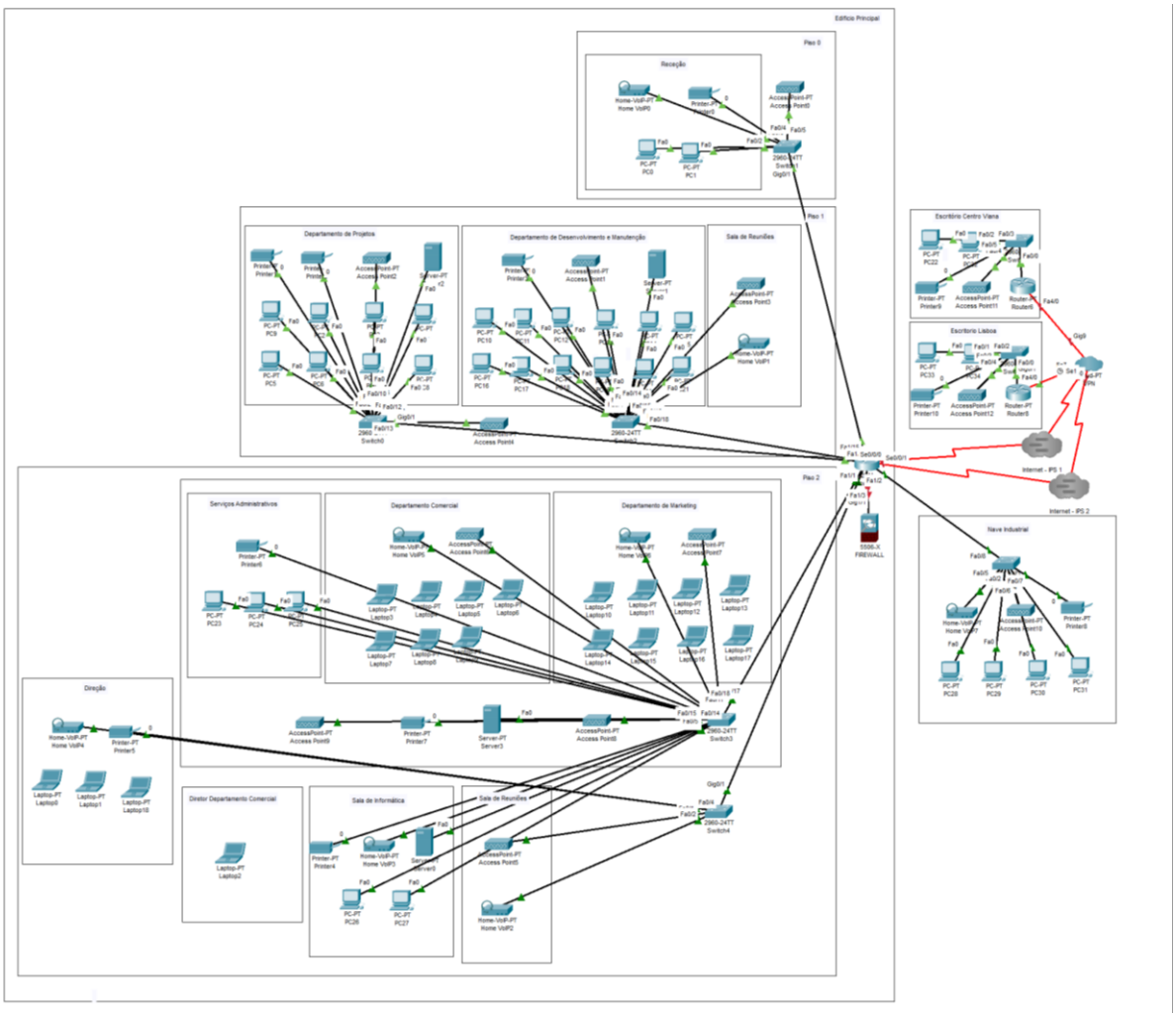


Figura 5 Sistema de Cablagem

Proposta de Arquitetura Lógica

Apresentamos por fim o esquema da arquitetura lógica proposta para a PowerWind, concebida para suportar todas as operações e garantir a eficácia e segurança da infraestrutura de conforme as necessidades detalhadas anteriormente.



Especificação de componentes

Equipamentos

1. **Servidor de Projeto e Desenvolvimento (2 unidades)**
    - **Modelo:** HP DL380P G8
    - **Especificações:** 128GB RAM, 3 SSDs
2. **Servidor Administrativo (1 unidade)**
    - **Modelo:** Dell PowerEdge R650xs
    - **Especificações:** 64GB RAM, 2TB HDD

3. **Servidor de Gestão (1 unidade)**
    - **Modelo:** HPE ProLiant DL380 Gen10
    - **Especificações:** 64GB RAM, 1TB HDD
4. **All-in-One PCs HP ENVY 32 GB RAM**
    - **Modelo:** All-in-One HP ENVY 34-c1005ns i7-12700, 32 GB RAM
    - **Especificações:** Tela de 34", Intel Core i7-12700, 32 GB RAM, 1 TB SSD, NVIDIA
5. **All-in-One PCs ACER 16 GB RAM**
    - **Modelo:** All-in-One ACER C27-1800
    - **Especificações:** Tela de 27", Intel Core i5-12450H, 16 GB RAM, 1024 GB SSD
6. **Portáteis para ASUS Vivobook M1502YA**
    - **Modelo:** Portátil ASUS Vivobook M1502YA R7 (16 GB RAM)
    - **Especificações:** Tela de 15.6", AMD Ryzen 7 7700U, 16 GB RAM, 512 GB SSD, AMD Radeon Graphics
7. **Serviço NAS para backups**
    - **Modelo:** Synology DiskStation DS920+
    - **Especificações:** 4GB RAM, 4 baias para HDD/SSD
8. **Impressoras e Plotters (10 unidades)**
    - **Modelo:** HP LaserJet Pro MFP M428fdw
9. **Routers 10Gbps com suporte para failover (1 unidade)**
    - **Modelo:** Cisco RV345
10. **Switches 10Gbps com suporte para failover (8 unidades)**
    - **Modelo:** Netgear XS708T
11. **Home VoIP**
    - **Modelo:** Cisco SPA112
12. **Access Points (12 unidades)**
    - **Modelo:** Ubiquiti UniFi AP-AC

Cablagem

1. **Cat6A 500 MHz**
    - **Preço por metro:** €1.80
    - **Total 500m**
2. **Fibra Ótica**
    - **Preço por metro:** €1.97
    - **Total 500m**
3. **Tomadas RJ-45**
    - **Preço:** €9.19
    - **Total**: 100 Unidades

Software e Serviços

1. **VPN**
    - **Modelo:** NordVPN Teams
    - **Preço Anual:** €576
2. **ISP 1**
    - **Provedor:** NOS Empresas
    - **Preço Anual:** €580
3. **ISP 2**
    - **Provedor:** Vodafone Pro empresas
    - **Preço Anual:** €500
4. **Firewall**
    - Fortinet FortiGate 100E
    - **Preço Anual:** €1,200
5. **SIEM**
    - Splunk Enterprise
    - **Preço Anual:** €2,000
6. **Software para Monitorização e Gestão**
    - SolarWinds Network Performance Monitor
    - **Preço Anual:** €1,500
7. **Serviço de Backup Cloud**
    - AWS Backup

- **Preço Anual:** €1,200

Estimativa de Orçamento

Equipamento	Localização	Quantidade	Preço/Unidade	SubTotal
Access Point - Ubiquiti UniFi AP-AC	Nave Industrial	4	120.00 €	480.00 €
Access Point - Ubiquiti UniFi AP-AC	Sede - Piso 0	1	120.00 €	120.00 €
Access Point - Ubiquiti UniFi AP-AC	Sede - Piso 1	4	120.00 €	480.00 €
Access Point - Ubiquiti UniFi AP-AC	Sede - Piso 2	5	120.00 €	600.00 €
Access Point - Ubiquiti UniFi AP-AC	Esc V.C.	1	120.00 €	120.00 €
Access Point - Ubiquiti UniFi AP-AC	Esc Lisboa	1	120.00 €	120.00 €
Netgear XS708T - Switch	Nave Industrial	1	1,000.00 €	1,000.00 €
Netgear XS708T - Switch	Sede - Piso 0	1	1,000.00 €	1,000.00 €
Netgear XS708T - Switch	Sede - Piso 1	2	1,000.00 €	2,000.00 €
Netgear XS708T - Switch	Sede - Piso 2	2	1,000.00 €	2,000.00 €
Netgear XS708T - Switch	Esc V.C.	1	1,000.00 €	1,000.00 €
Netgear XS708T - Switch	Esc Lisboa	1	1,000.00 €	1,000.00 €
Servidor D. Engenharia - HP DL380P G8	Sede - Piso 1	2	3,500.00 €	7,000.00 €
Servidor Administrtivo - Dell PowerEdge R650xs	Sede - Piso 2	1	4,495.00 €	4,495.00 €
Servidor Gestão - HPE ProLiant DL380 Gen10	Sede - Piso 2	1	5,438.95 €	5,438.95 €
Home VoIP - Cisco SPA112	Sede - Piso 0	1	50.00 €	50.00 €
Home VoIP - Cisco SPA112	Sede - Piso 1	1	50.00 €	50.00 €
Home VoIP - Cisco SPA112	Sede - Piso 2	5	50.00 €	250.00 €
Home VoIP - Cisco SPA112	Nave Industrial	1	50.00 €	50.00 €
Home VoIP - Cisco SPA112	Esc Lisboa	1	50.00 €	50.00 €
Home VoIP - Cisco SPA112	Esc V.C.	1	50.00 €	50.00 €
Impressora - HP LaserJet Pro MFP M428fdw	Sede - Piso 0	1	400.00 €	400.00 €
Impressora - HP LaserJet Pro MFP M428fdw	Sede - Piso 1	3	400.00 €	1,200.00 €
Impressora - HP LaserJet Pro MFP M428fdw	Sede - Piso 2	3	400.00 €	1,200.00 €
Impressora - HP LaserJet Pro MFP M428fdw	Nave Industrial	1	400.00 €	400.00 €
Impressora - HP LaserJet Pro MFP M428fdw	Esc V.C.	1	400.00 €	400.00 €
Impressora - HP LaserJet Pro MFP M428fdw	Esc Lisboa	1	400.00 €	400.00 €
NAS - Synology DiskStation DS920+	Sede	1	550.00 €	550.00 €
Pc HP 22-DG0000NP J4025 (8 GB RAM)	Escritório (viana)	2	529.99	1,059.98 €
Pc HP 22-DG0000NP J4025 (8 GB RAM)	Escritório (Lisboa)	2	529.99	1,059.98 €
Pc HP 22-DG0000NP J4025 (8 GB RAM)	Piso 0 (Receção)	2	529.99	1,059.98 €
PC HP ENVY 34-c1005ns (i7-12700, 32 GB RAM)	Piso 1 (D. Desen.)	10	2780.5	27,805.00 €
PC ASUS A3402WBAK-WA577W (i7-1255U - 16 GB RAM)	Piso 1 (D. Projecto)	10	972.45	9,724.50 €
PC ASUS A3402WBAK-WA577W (i7-1255U - 16 GB RAM)	Piso 2 (S. Informatica)	2	972.45	1,944.90 €
PC ACER C27-1800 (i5-12450H - 16 GB RAM)	Piso 2 (S. Admin.)	3	729.9	2,189.70 €
PC ACER C27-1800 (i5-12450H - 16 GB RAM)	Nave Industrial	4	729.9	2,919.60 €
Portátil ASUS Vivobook M1502YA R7 (16 GB RAM)	Piso 1 (D. Projecto)	5	649.99 €	3,249.95 €
Portátil ASUS Vivobook M1502YA R7 (16 GB RAM)	Piso 1 (D. Projecto)	19	649.99 €	12,349.81 €
Cabo Fibra Óptica 8 Fibras 50/125 OM3	Vários Locais	500	1.97 €	985.00 €
Cabo blindado RJ45 CAT6a 1m	Vários Locais	3000	1.09 €	3,270.00 €
Tomada de rede RJ45 FORIX	Vários Locais	100	9.19 €	919.00 €
			Total:	92,521.35 €

Serviço/Sotware	Custo Anual
VPN - NordVPN Teams	500.00 €
ISP1 - NOS Empresas	576.00 €
ISP2 - Vodafone Pro Empresas	580.00 €
Firewall - Fortinet	1,200.00 €
SIEM - Splunk	2,000.00 €
SMG - SolarWinds	1,500.00 €
Backup Cloud - AWS	1,200.00 €
Total	7,556.00 €

O orçamento total é 100 077 euros.