UNIVERSIDADE NOVE DE JULHO
DIRETORIA DOS CURSOS DE INFORMÁTICA

CAROLINA DE ANDRADE FRANZOLIN
GABRIEL MATOS ALENCAR
GEOVANNA VIEIRA DOS SANTOS
GUILHERME VITALA FORTUNATO
LUCAS OLIVEIRA CAMPOS
LUIS EDUARDO PEDRO
OLIVER CHRISTIAN SOUZA
SHEILA LUIZA SOARES CABRAL
YAGO RAIOL DA SILVA

PROJETO EM INFRAESTRUTURA COMPUTACIONAL: DATA CENTER

SÃO PAULO
2024

CAROLINA DE ANDRADE FRANZOLIN
GABRIEL MATOS ALENCAR
GEOVANNA VIEIRA DOS SANTOS
GUILHERME VITALA FORTUNATO
LUCAS OLIVEIRA CAMPOS
LUIS EDUARDO PEDRO
OLIVER CHRISTIAN SOUZA
SHEILA LUIZA SOARES CABRAL
YAGO RAIOL DA SILVA

PROJETO EM INFRAESTRUTURA COMPUTACIONAL: DATA CENTER

Trabalho apresentado à Universidade Nove de Julho, UNINOVE, em cumprimento parcial às exigências da disciplina de Projeto em Infraestrutura Computacional, sob orientação do Prof. **Fábio de Jesus Souza.**

SÃO PAULO
2024

“Na escola, a tecnologia é como um livro, se não se abrir, ler e pensar, de nada adianta.”

(William Antonio Zacariotto)

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

AES - Advanced Encryption Standard

CD - Compact Disc

CPF - Cadastro de Pessoas Físicas

CPU - Central Processing Unit

DHCP - Protocolo de Configuração Dinâmica de Host

DNS - Sistema de Nomes de Domínio

DVD - Disco Versátil Digital

EDR - Detecção e Resposta de Endpoints

FTP - Protocolo de Transferência de Arquivos

GB - Gigabyte

Gbps - Gigabits por segundo

GHz - Gigahertz

ISP - Provedor de Serviços de Internet

HD - Disco Rígido

IP - Endereços de Protocolo de Internet

KVA - Quilovolt-ampère

MB - Megabyte

RG - Registro Geral

SMS - Serviço de Mensagens Curtas

SFP - Plugável de Formato Pequeno

SFP+ - Plugável de Formato Pequeno a Mais

SSD - Unidade de Estado Sólido

TB - Terabyte

TI - Tecnologia da Informação

VPN - Rede Virtual Privada

VLAN’s - Virtual Local Area Network

RJ45 - Registered Jack-45

F/UTP - Par trançado de blindagem coletiva com folha de alumínio.,

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1. RESUMO

Segundo Lakatos e Marconi (2008 p.220) "a especificação do objetivo de uma pesquisa responde às questões para quê? e para quem?". Os objetivos determinam

os resultados que a equipe pretende alcançar no desenvolvimento do projeto deste módulo.

No semestre anterior, a equipe desenvolveu um projeto focado na criação de um banco de dados eficiente para a escola. O objetivo desse projeto era garantir que todas as informações acadêmicas e administrativas estivessem organizadas de forma sistemática, facilitando o acesso, a manipulação e a manutenção dos dados. Esse banco de dados foi projetado para atender às necessidades específicas da escola, incluindo o gerenciamento de matrículas, controle de notas, registros de frequência, informações de funcionários e outras operações.

A criação do banco de dados foi uma etapa fundamental que proporcionou uma base sólida para a gestão da informação na escola, por isso o projeto referido desenvolvido no semestre anterior será um dos componentes principais a ser integrado e gerenciado no data center.

Diante disso, a proposta do projeto é manter a segurança, integridade e agilidade para com os dados de uma escola. Portanto o projeto visa a construção de um data center de pequeno porte abrangendo os seguintes tópicos: Análise de Requisitos, Projeto de Infraestrutura Física, Aquisição de Equipamentos, Rede e Conectividade, Sistemas de Energia e Resfriamento, Segurança e Monitoramento, Backup e Recuperação de Desastres, Testes e Validação.

Em um primeiro momento, as informações a serem contempladas serão as plantas, questões de segurança física e digital (backups), a rede e conectividade da escola e posteriormente a aquisição de equipamentos.

1.1. *ABSTRACT*

According to Lakatos and Marconi (2008 p.220), "the specification of the objective of a research answers the questions why? and for whom?". The objectives determine the results that the team aims to achieve in the development of this module project.

In the previous semester, the team developed a project focused on creating an efficient database for the school. This project aimed to ensure that all academic and administrative information was organized systematically, facilitating access, manipulation, and maintenance of the data. This database was designed to meet the specific needs of the school, including enrollment management, grade control, attendance records, employee information, and other operations.

The creation of the database was a fundamental step that provided a solid foundation for information management in the school, so the aforementioned project developed in the previous semester will be one of the main components to be integrated and managed in the data center.

Therefore, the project proposal is to maintain security, integrity, and agility towards the data of a school. Therefore, the project aims to build a small-scale data center covering the following topics: Requirements Analysis, Physical Infrastructure Design, Equipment Acquisition, Network and Connectivity, Power and Cooling Systems, Security and Monitoring, Backup and Disaster Recovery, Testing, and Validation.

Initially, the information to be addressed will be the plans, physical and digital security issues (backups), the school's network and connectivity, and subsequently the acquisition of equipment.

2. DESCRIÇÃO DA ESCOLA

O Colégio Jorgina, fundado em 1990, é uma instituição de ensino dedicada ao público infantojuvenil. Ao longo dos anos, tem se destacado por oferecer uma educação de qualidade, focada no desenvolvimento integral dos alunos.

Com uma abordagem pedagógica moderna e inovadora, o colégio busca não apenas transmitir conhecimento, mas também estimular habilidades criativas, sociais e emocionais. Suas instalações acolhedoras e equipe de educadores comprometidos criam um ambiente propício para o aprendizado e o crescimento pessoal dos estudantes.

O Colégio Jorgina é reconhecido por sua dedicação à formação educacional das gerações mais jovens, preparando-os para os desafios do futuro.

3. MISSÃO, VISÃO E VALORES DA ESCOLA

3.1. MISSÃO

Nossa missão no Colégio Jorgina é proporcionar uma educação de excelência, centrada no desenvolvimento integral de cada aluno. Buscamos cultivar habilidades acadêmicas, criativas e sociais, preparando os estudantes para enfrentar os desafios do mundo contemporâneo com confiança e ética.

3.2. VISÃO

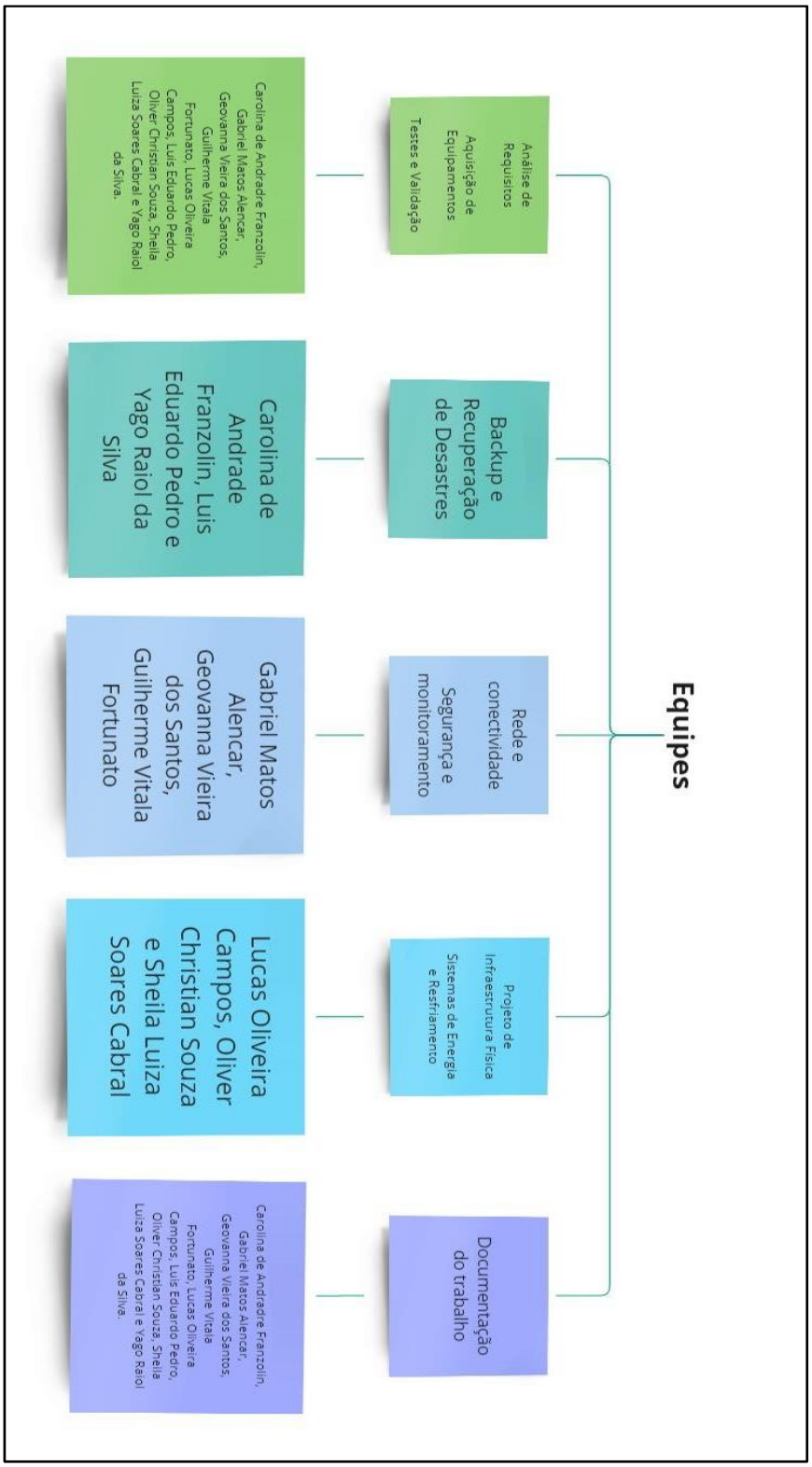
Nossa visão é sermos reconhecidos como uma referência em educação infanto-juvenil, conhecidos por nosso compromisso com a qualidade educacional e a formação de cidadãos responsáveis e bem preparados. Almejamos oferecer um ambiente de aprendizado inspirador, onde cada aluno possa explorar seu potencial ao máximo.

3.3. VALORES

- Excelência Educacional: Buscamos a excelência em tudo o que fazemos, desde a entrega de conteúdo até a interação com os alunos, pais e colegas.
- Desenvolvimento Integral: Acreditamos em uma educação que vai além do acadêmico, valorizando o crescimento pessoal, emocional e social de cada aluno.
- Respeito e Inclusão: Cultivamos um ambiente onde o respeito mútuo e a inclusão são fundamentais, acolhendo a diversidade de origens, ideias e perspectivas.
- Inovação Pedagógica: Estamos comprometidos em adotar abordagens pedagógicas inovadoras, incorporando tecnologia e métodos modernos para enriquecer a experiência de aprendizado.
- Parceria com a Comunidade: Valorizamos a colaboração entre alunos, pais, educadores e a comunidade em geral, reconhecendo que a educação é uma jornada compartilhada.
- Responsabilidade Social: Promovemos a consciência sobre o impacto social e ambiental, incentivando os alunos a se tornarem cidadãos responsáveis e preocupados com o bem-estar coletivo.

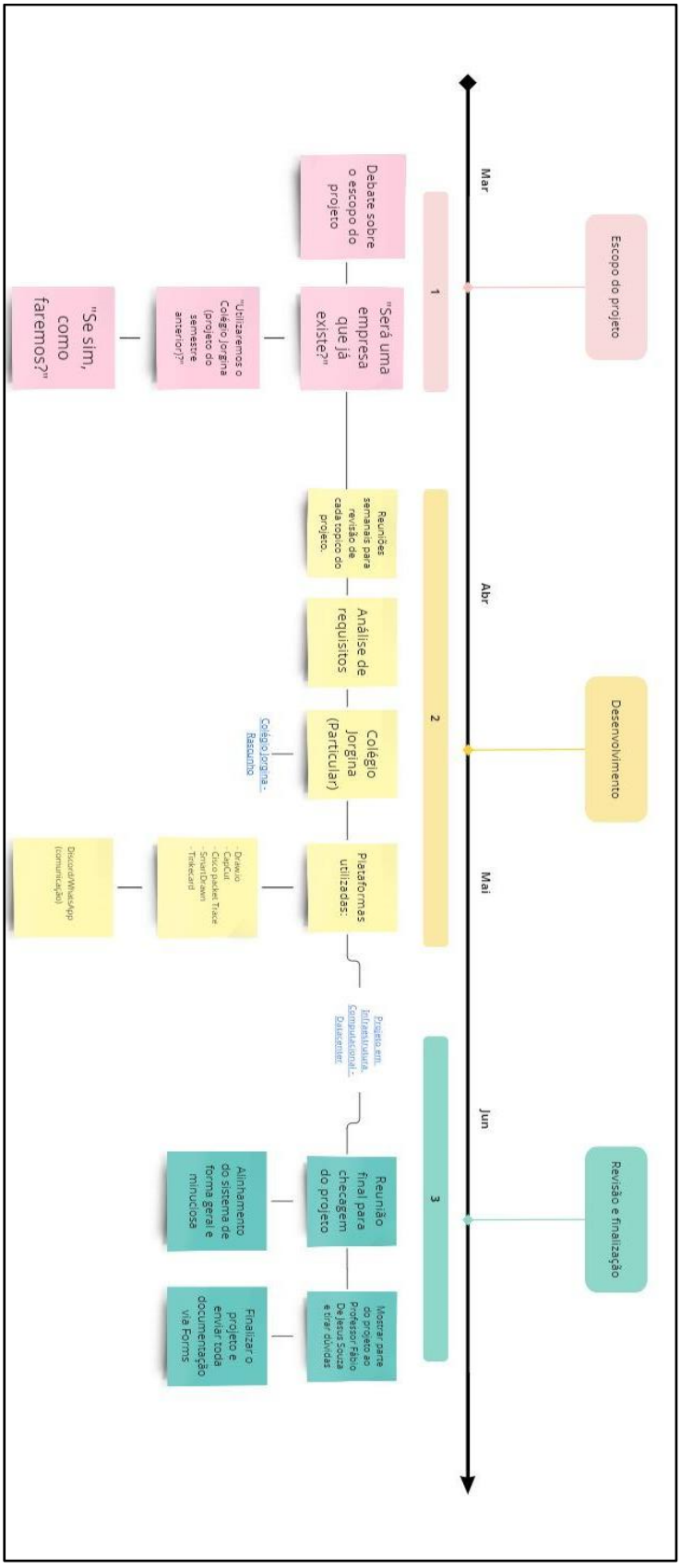
4. DEFINIÇÃO DA EQUIPE, DIVISÃO DE PAPÉIS E TAREFAS, CRONOGRAMA DE DESENVOLVIMENTO

Figura 1 - Divisão de Equipes



Fonte: Autor (2024).

Figura 2 - Linha do tempo do desenvolvimento do projeto

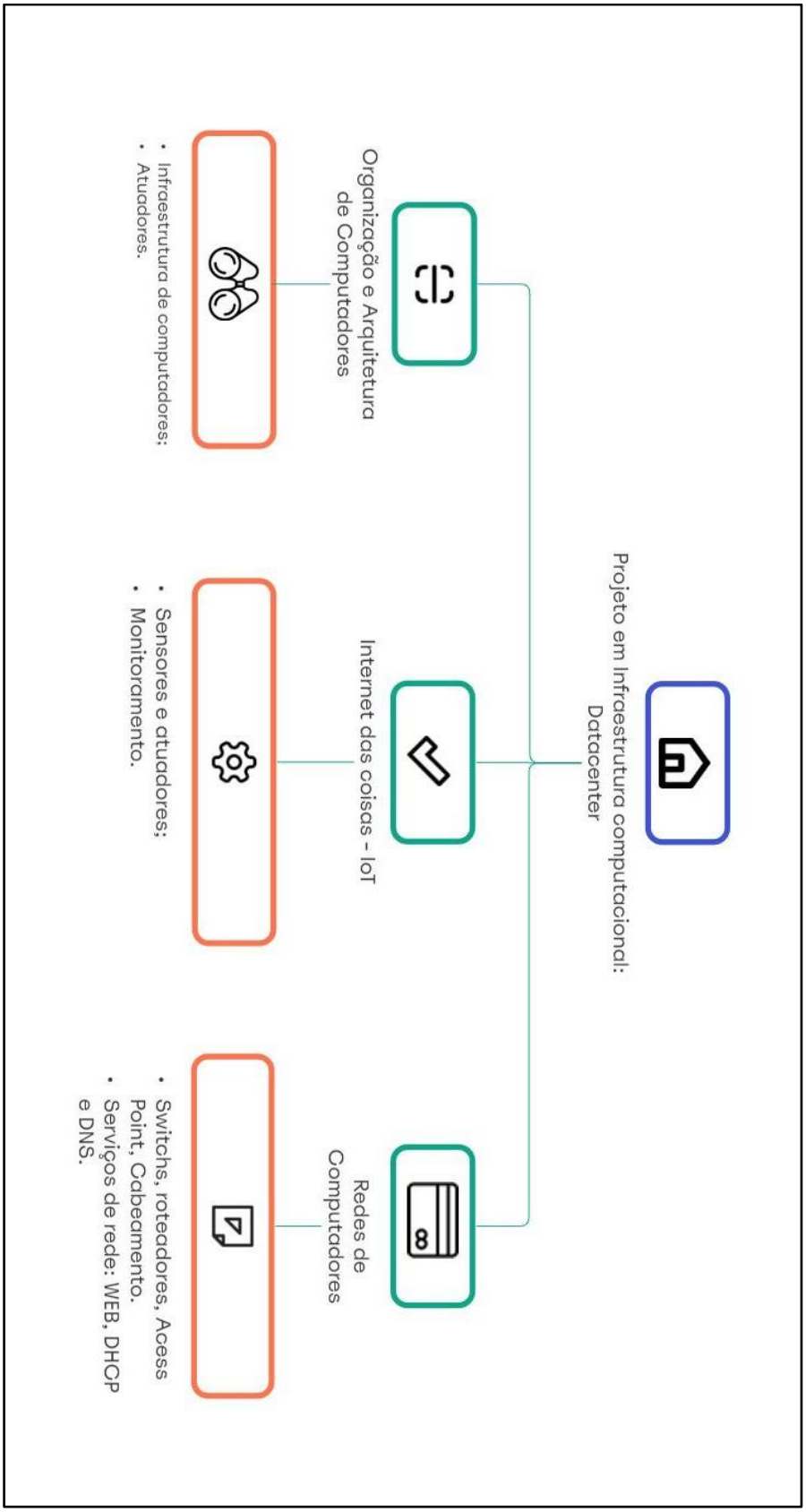


Fonte: Autor (2024).

5. PARTICIPAÇÃO DAS DISCIPLINAS DO SEMESTRE

- Organização e Arquitetura de Computadores : Infraestrutura de computadores, *HDs* e fitas de *backups*.
- Internet das Coisas: Desenvolver sensores, atuadores, sistemas de monitoramento, dispositivos inteligentes e aplicativos através da programação em linguagem C++.
- Redes de Computadores: Criação de servidores, cabeamento, serviços de rede como *WEB*, *DHCP* e *DNS*, manutenção de *IPs* e sub-redes.

Figura 3 - Matérias contempladas



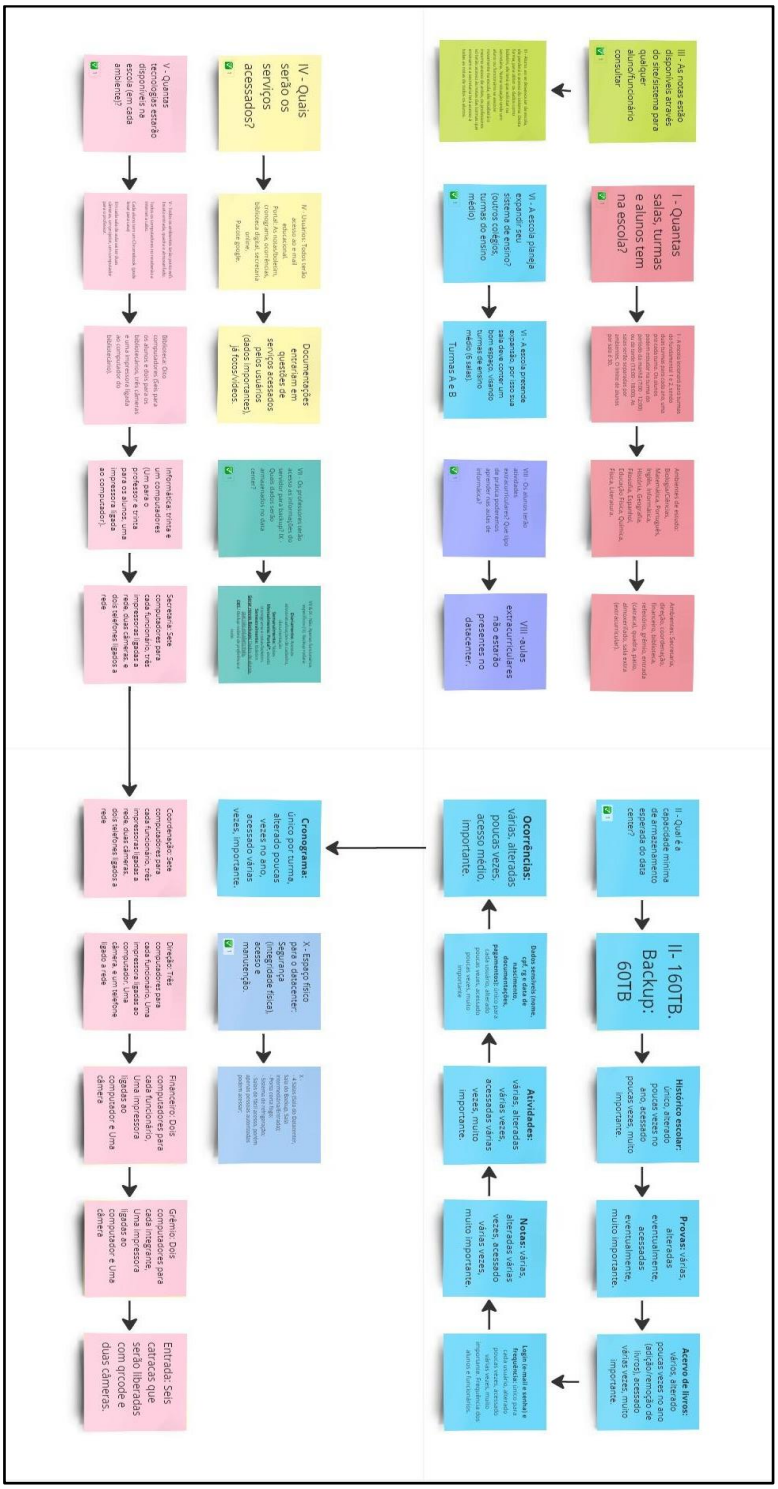
Fonte: Autor (2024).

- Projeto em Infraestrutura Computacional: Data center.
- Organização e Arquitetura de Computadores: Infraestrutura de computadores; Atuadores.
- Internet das Coisas - *IOT*: Sensores e atuadores; Monitoramento.
- Redes de Computadores: *Switches*, roteadores, *access point*, cabeamento; Serviços de rede: *WEB, DHCP,* e *DNS*.

6. ANÁLISE DE REQUISITOS

A seguir haverá a análise de requisitos feita nas primeiras semanas de reunião sobre o projeto, sendo uma base para a construção do que o projeto necessitava e como seria colocada em prática. Algumas ideias, posteriormente, foram desconsideradas.

Figura 4 - Análise de requisitos



Fonte: Autor (2024).

I. Quantidade de Salas, Turmas e Alunos

A escola lecionará para turmas do Fundamental 1 e 2, sendo duas turmas para cada ano e uma para cada turno. Os alunos podem estudar na turma do período da manhã (7:00 - 12:00) ou da tarde (13:00 - 18:00).

As salas serão separadas por ambientes e o limite de alunos por turma é 30. Além disso, a escola conterá os seguintes ambientes de estudo: Biologia/Ciências, Matemática, Português, Inglês, Informática, História, Geografia, Filosofia, Espanhol, Educação Física, Química, Física e Literatura.

Outras instalações incluem: Secretaria, direção, coordenação, financeiro, biblioteca, refeitório, grêmio, entrada (catraca), quadra, pátio, almoxarifado, sala extra (extra curricular).

II. Capacidade Mínima de Armazenamento Esperada do Data Center

A capacidade mínima esperada do data center é de 160 TB. Sendo o *backup* de 60 TB, dividido em:

- Histórico escolar: único, alterado poucas vezes no ano, acessado poucas vezes, muito importante.
- Provas: várias, alteradas eventualmente, acessadas eventualmente, muito importante.
- Acervo de livros: vários, alterado poucas vezes no ano (adição/remoção de livros), acessado várias vezes, muito importante.
- *Login* (*e-mail* e senha) e frequência: único para cada usuário, alterado poucas vezes, acessado várias vezes, muito importante.
- Notas: várias, alteradas várias vezes, acessadas várias vezes, muito importante.
- Atividades: várias, alteradas várias vezes, acessadas várias vezes, muito importante.
- Dados sensíveis (nome, CPF, RG, data de nascimento, documentações, pagamentos): único para cada usuário, alterado poucas vezes, acessado poucas vezes, muito importante.
- Ocorrências: várias, alteradas poucas vezes, acesso médio, importante.

- Cronograma: único por turma, alterado poucas vezes no ano, acessado várias vezes, importante.

III. Acesso às Notas pelo Site/Sistema

Os professores só terão acesso às notas das turmas que ensinam e a secretaria terá acesso a todas as notas de todos os alunos. Caso o aluno se desassocie da escola, ele perderá o acesso ao sistema. Desta forma, para obter os dados como boletim, ele terá que solicitar na secretaria.

IV. Serviços Acessados

Para usuários: todos terão acesso ao *e-mail* educacional. Portal da escola: notas/boletim, cronograma, ocorrências, biblioteca digital, secretaria *online*. Pacote *Google* presente para todos. Documentações entram em questões de serviços acessados pelos usuários (dados importantes), enquanto fotos/vídeos são documentos de pouca relevância que não entram em serviços acessados.

V. Tecnologias Disponíveis na Escola

Todos os ambientes terão ponto *Wi-Fi*, exceto entrada, quadra e almoxarifado. Todos os computadores receberão internet a cabo. Cada aluno terá um *Chromebook* (pode levar para casa).

Disposição das tecnologias em cada ambiente:

- Em cada sala de aula haverá duas câmeras, um projetor e um computador para o professor.
- Na biblioteca haverá oito computadores (seis para os alunos e dois para os bibliotecários), três câmeras e uma impressora ligada ao computador do bibliotecário.
- Na sala de informática haverá trinta e um computadores (um para o professor e trinta para os alunos) e uma impressora ligada ao computador.
- Na secretaria haverá sete computadores para cada funcionário, três impressoras ligadas à rede, duas câmeras e dois telefones ligados à rede.
- Na sala de coordenação haverá sete computadores para cada funcionário, três impressoras ligadas à rede, duas câmeras e dois telefones ligados à rede.
- Na direção haverá três computadores para cada funcionário, uma impressora ligada ao computador, uma câmera e um telefone ligado à rede.

- Na sala do financeiro haverá dois computadores para cada funcionário, uma impressora ligada ao computador e uma câmera.
- No grêmio haverá dois computadores para cada integrante, uma impressora ligada ao computador e uma câmera.
- Na entrada haverá seis catracas liberadas com *QR code* e duas câmeras.

VI. Expansão do Sistema de Ensino

A escola pretende expandir, por isso suas salas devem conter um bom espaço, visando turmas de ensino médio (6 salas, turmas A e B).

VII. Acesso dos Professores às Informações do Servidor para *Backup* e Dados Armazenados no *Data Center*.

Os professores não terão acesso às informações do servidor para *backup*; apenas funcionários específicos (TI) terão esse acesso.

O *backup* será realizado da seguinte forma:

- Diariamente: acessos ativos/atualizações de cadastro, documentação.
- Semanalmente: notas.
- Mensalmente: portal, exceto cronograma e notas/boletim.
- Semestralmente: boletim.
- Geração de novos *backups*: dados de alunos que não estudam mais.
- Observação: o *backup* será realizado preferencialmente à noite.

VIII. Atividades Extracurriculares e Práticas nas Aulas de Informática

As aulas extracurriculares não estarão presentes no *data center*.

IX. Espaço Físico para o *Data center*: Segurança (Integridade Física), Acesso e Manutenção

O espaço físico contará com quatro salas (sala do data center, sala do *backup*, sala intermediária/entrada), porta corta-fogo, sistema de refrigeração e salas de fácil acesso, porém apenas pessoas autorizadas poderão acessar.

7. PROJETO DE INFRAESTRUTURA FÍSICA

Neste segmento, após explorar a importância fundamental das plantas para o funcionamento eficiente e seguro de um ambiente crítico de TI, é essencial adentrarmos nas medidas específicas de cada cômodo. Afinal, essas dimensões não são apenas números estáticos, mas representam a infraestrutura física na qual as operações de TI se baseiam.

A sala do *data center* possui dimensões de 7 x 2.83 metros e localizada estrategicamente no penúltimo andar da escola. Esta localização permite um fácil acesso para manutenção e atualizações, ao mesmo tempo que oferece segurança contra inundações e outros riscos no térreo.

Em seguida, encontra-se a sala dos *backups*, com suas medidas de 1.86 x 2.85 metros. Este cômodo, apesar de menor, é crucial para a redundância e recuperação de dados em caso de falhas. Sua proximidade com a sala do *data center* permite uma rápida transferência de dados, mantendo a integridade e a segurança das informações armazenadas.

O *hall* de entrada, medindo 1.36 x 4.85 metros, funciona como um espaço intermediário que controla o acesso ao data center e à sala de *backups*. Este *hall* garante que apenas pessoas autorizadas possam entrar nessas áreas críticas, sendo equipado com sistemas de segurança como portas corta-fogo e sistemas de controle de acesso.

Ao compreender essas medidas, pode-se visualizar melhor a complexidade e a sofisticação por trás da infraestrutura crítica de um *data center* moderno. Cada metro quadrado é planejado com precisão para assegurar que todos os componentes operem em sinergia, garantindo a máxima eficiência e segurança das operações de TI.

7.1. A RELEVÂNCIA CRÍTICA DAS PLANTAS

Antes de adentrar nas plantas específicas, é essencial compreender por que elas desempenham um papel tão vital. As plantas do *data center* não são apenas diagramas estáticos; são representações dinâmicas da infraestrutura física e lógica que sustentam as operações de TI. Ao entender suas nuances e interconexões, os profissionais de TI e engenheiros de infraestrutura podem otimizar o desempenho, mitigar riscos e garantir a confiabilidade operacional.

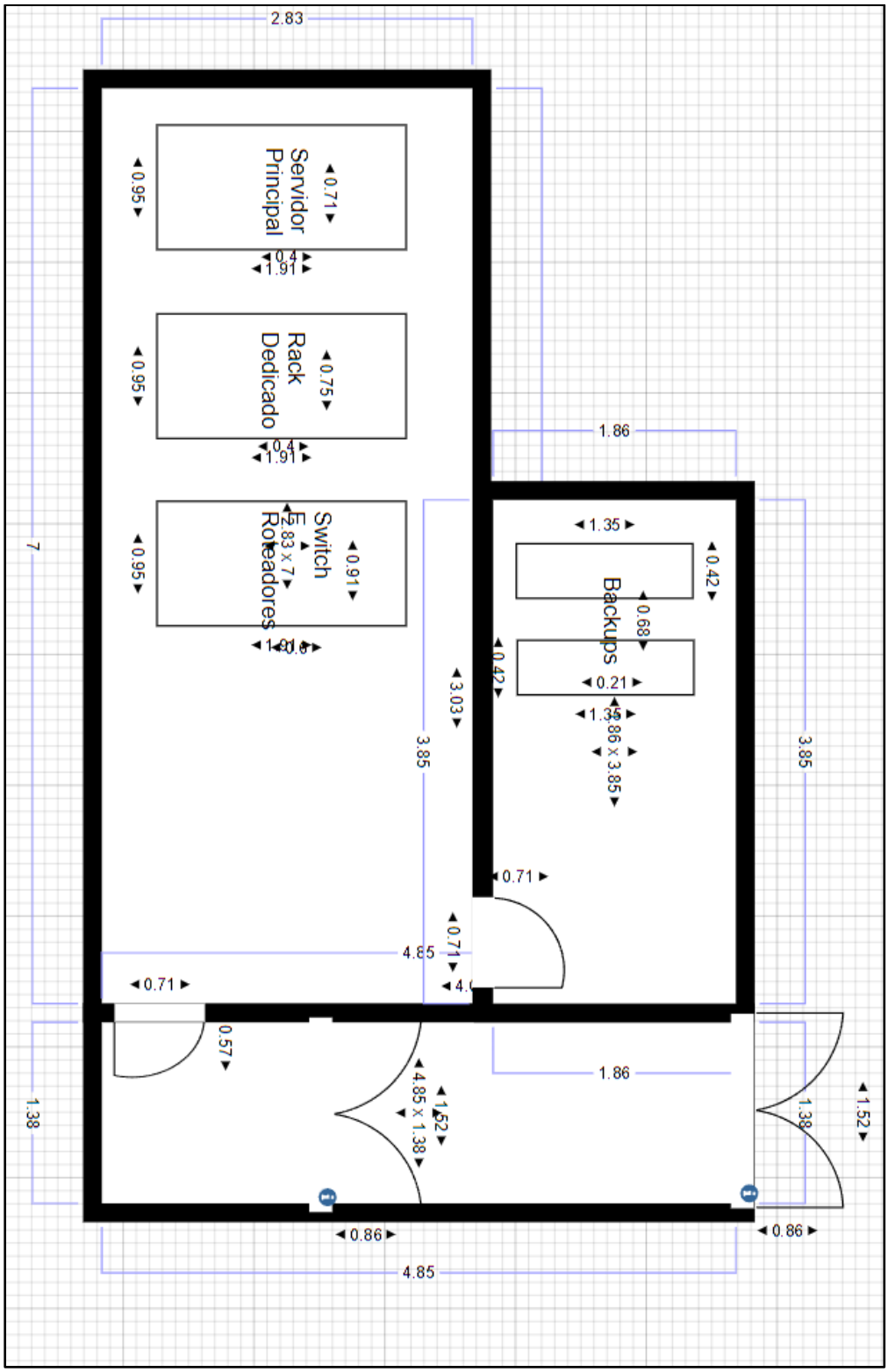
7.1.2. UM OLHAR HOLÍSTICO NAS PLANTAS DO DATA CENTER

A partir deste ponto, será realizado um exame detalhado de cada planta do *data center*, explorando suas características distintas e sua função dentro do ambiente mais amplo. Por meio desta análise, será destacada como cada planta é adaptada para atender a necessidades específicas, ilustrando a complexidade e a sofisticação por trás da infraestrutura crítica de um *data center* moderno.

Nesta seção será apresentada a planta limpa do *data center*, destacando as dimensões de cada sala e a disposição estratégica dos racks e suportes mecânicos para os *backups*. Essa representação visual oferece uma visão clara e detalhada da infraestrutura física do *data center*, ressaltando a organização precisa dos componentes essenciais para o processamento e armazenamento de dados de forma segura e eficiente.

7.1.3. Planta limpa do *data center*

Figura 5 - Planta limpa do *Data Center*



Fonte: Autor (2024).

A planta limpa oferece uma visão detalhada e abrangente dos principais componentes do *data center*, fundamentais para o processamento e armazenamento de dados de forma segura e eficiente. A disposição estratégica dos *racks* de servidores, *switches* e *backups* é meticulosamente planejada para garantir a máxima eficácia operacional.

O *rack* do servidor principal é o núcleo do *data center*, onde reside o poder de processamento e armazenamento dos dados críticos da empresa. O servidor é equipado com a mais recente tecnologia para garantir desempenho e confiabilidade inigualáveis. Além disso, há um *switch* nesse *rack* do servidor, permitindo uma eficiente gestão de rede. Sua disposição organizada facilita as operações de manutenção e atualização, minimizando o tempo de inatividade.

No rack dedicado à redundância de servidor, *switch* e roteador, a prevenção contra falhas é prioridade. Aqui, servidores, *switches* e roteadores redundantes aguardam prontos para entrar em ação instantaneamente, garantindo a continuidade das operações mesmo diante de falhas inesperadas. Essa configuração estratégica proporciona uma camada adicional de segurança e tranquilidade para as operações do *data center*.

O terceiro *rack* abriga *switches* e roteadores adicionais, responsáveis por fornecer conectividade essencial para diversos setores do *data center*. Sua distribuição cuidadosamente planejada assegura uma cobertura abrangente e uma rede robusta, essencial para garantir a comunicação eficaz entre os diversos componentes do *data center* e seus usuários.

Além disso, há um segundo cômodo onde estão localizados dois suportes mecânicos para guardar os discos rígidos de *backup*, complementando a infraestrutura principal do *data center*.

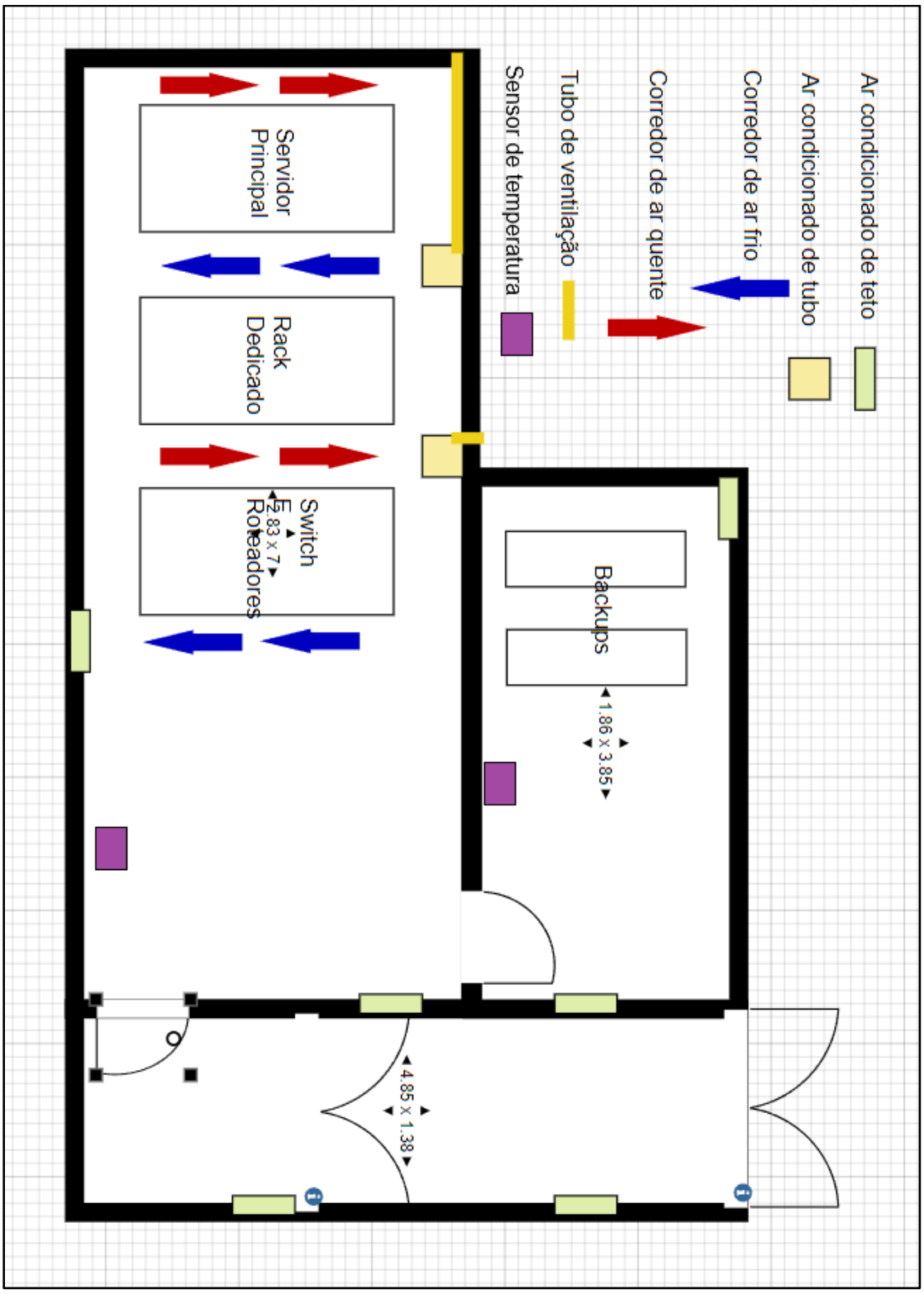
Em resumo, a planta oferece uma representação clara e detalhada da infraestrutura crítica do *data center*, destacando sua organização e disposição estratégica para garantir o funcionamento eficiente e seguro das operações de TI, mesmo nas situações mais desafiadoras.

Após explorar a infraestrutura física do *data center*, com suas salas estrategicamente planejadas e equipadas para garantir o processamento e

armazenamento eficiente dos dados, é fundamental agora mergulhar em outro aspecto crucial para o funcionamento operacional: o controle de temperatura.

7.1.4. Planta de refrigeração do *data center*

Figura 6 - Planta de Refrigeração do *Data Center*



Fonte: Autor (2024).

Uma sala de resfriamento de *data center* é um espaço projetado para controlar a temperatura e a umidade, garantindo que os equipamentos de computação funcionem de maneira eficiente. Essa é uma medida essencial, pois os equipamentos de computação geram calor significativo durante a operação, e o superaquecimento pode danificar esses dispositivos, levando a falhas e perda de dados. Além disso, temperaturas muito altas podem reduzir a vida útil dos componentes eletrônicos e aumentar o consumo de energia.

A prática comum de separação em corredores de ar quente e ar frio é adotada em *data centers* para otimizar a eficiência do resfriamento. No corredor de ar frio, os equipamentos de TI são alimentados com ar frio, mantendo-os em uma temperatura adequada para a operação ideal. Por sua vez, o ar quente gerado pelos equipamentos é direcionado para o corredor de ar quente, evitando sua mistura com o ar frio e sua recirculação nos sistemas de resfriamento.

Essa circulação de ar é assegurada pelos dois tubos de ventilação do data center, estrategicamente posicionados para garantir a circulação adequada do ar dentro do ambiente. Esses tubos desempenham um papel crucial na remoção do ar quente gerado pelos equipamentos de computação e na introdução de ar frio para resfriar esses dispositivos. O fluxo de ar controlado proporcionado pelo sistema de ventilação é essencial para manter uma temperatura padrão em todo o *data center*, evitando a formação de pontos quentes que poderiam levar ao superaquecimento dos equipamentos.

Além disso, cada sala do *data center* é equipada com dois sistemas de ar-condicionado de teto, posicionados estrategicamente para criar o corredor de ar quente e ar frio. Esses sistemas de ar-condicionado garantem um resfriamento eficiente e direcionado, controlando a temperatura de forma precisa e garantindo que todos os equipamentos recebam resfriamento adequado. Sua configuração flexível e intensidade de resfriamento adaptável tornam esses sistemas essenciais para garantir um resfriamento eficiente em todas as condições operacionais do *data center*.

Cinco sensores de temperatura estão sendo utilizados no sistema.

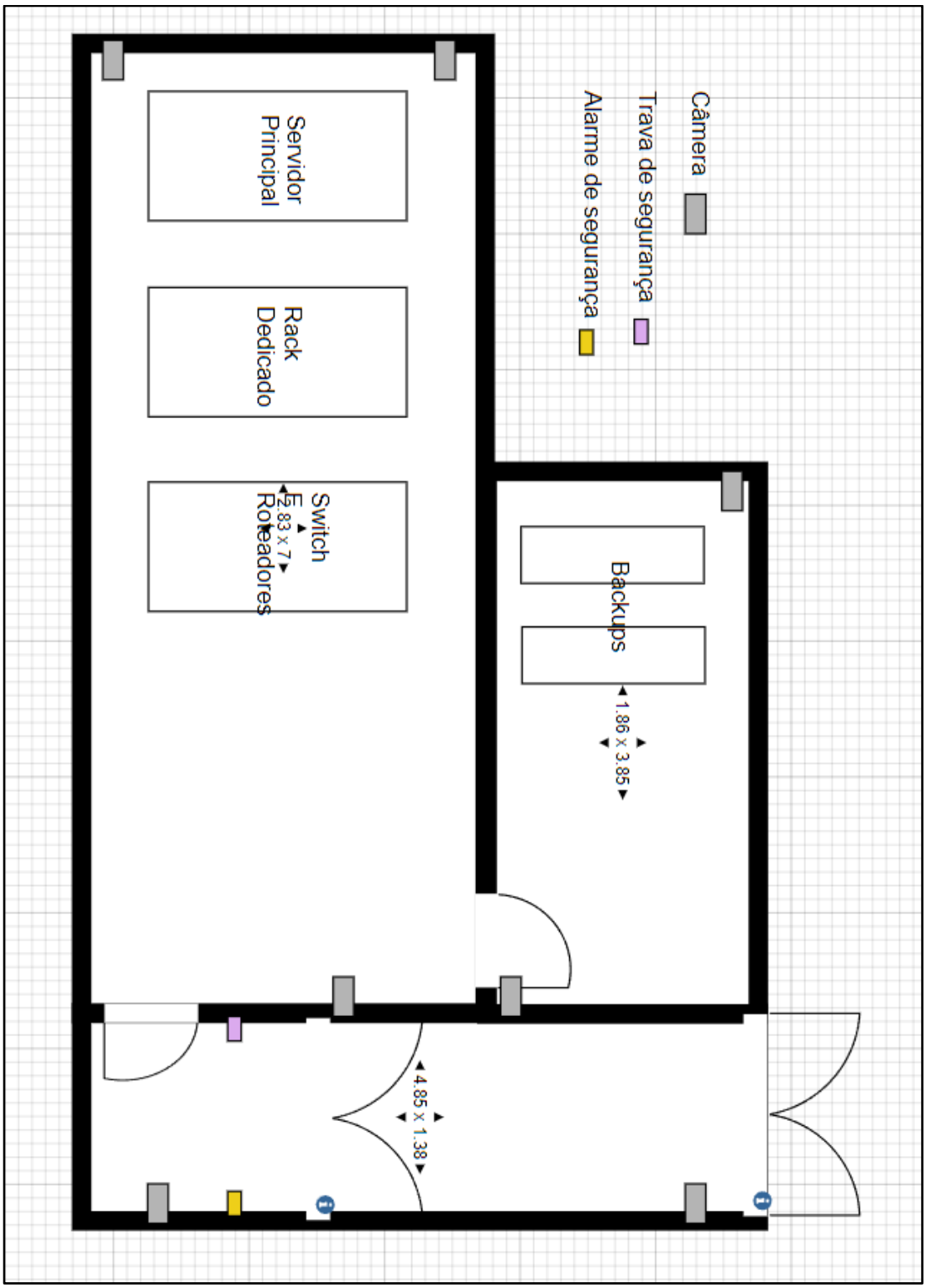
- Um sensor instalado na entrada principal do *data center* para monitorar as condições ambientais externas.

- Dois sensores posicionados dentro dos *racks* que abrigam os servidores, para monitorar as condições térmicas nesses locais críticos.
- Outro sensor colocado na sala dos *racks*, o ambiente principal onde os servidores estão localizados, assegurando uma cobertura abrangente da temperatura e umidade nesse espaço crítico.
- Um sensor alocado na sala de *backup*, monitorando continuamente as condições nesse ambiente de contingência.

Após discorrer sobre a importância do controle de temperatura e resfriamento eficiente no *data center*, torna-se vital abordar outro aspecto crucial: a segurança física. Essa é uma medida essencial para garantir a integridade e confidencialidade dos equipamentos e dados armazenados, além de proteger contra acesso não autorizado e atividades suspeitas dentro do ambiente do *data center*.

7.1.5. Planta de segurança física do *data center*

Figura 7 - Planta de Segurança Física



Fonte: Autor (2024).

A sala do *data center* é protegida por medidas de segurança física rigorosas para garantir a integridade e a confidencialidade dos equipamentos e dados armazenados.

As medidas implementadas visam controlar o acesso e monitorar as atividades dentro da sala do *data center*, garantindo a segurança dos ativos críticos e dos dados sensíveis armazenados. São elas:

- Controle de Acesso na Entrada: Na entrada da sala do *data center*, uma trava de segurança foi instalada, oferecendo duas opções de autenticação: biometria e crachá de identificação. Essa medida assegura que apenas pessoal autorizado tenha acesso ao ambiente.

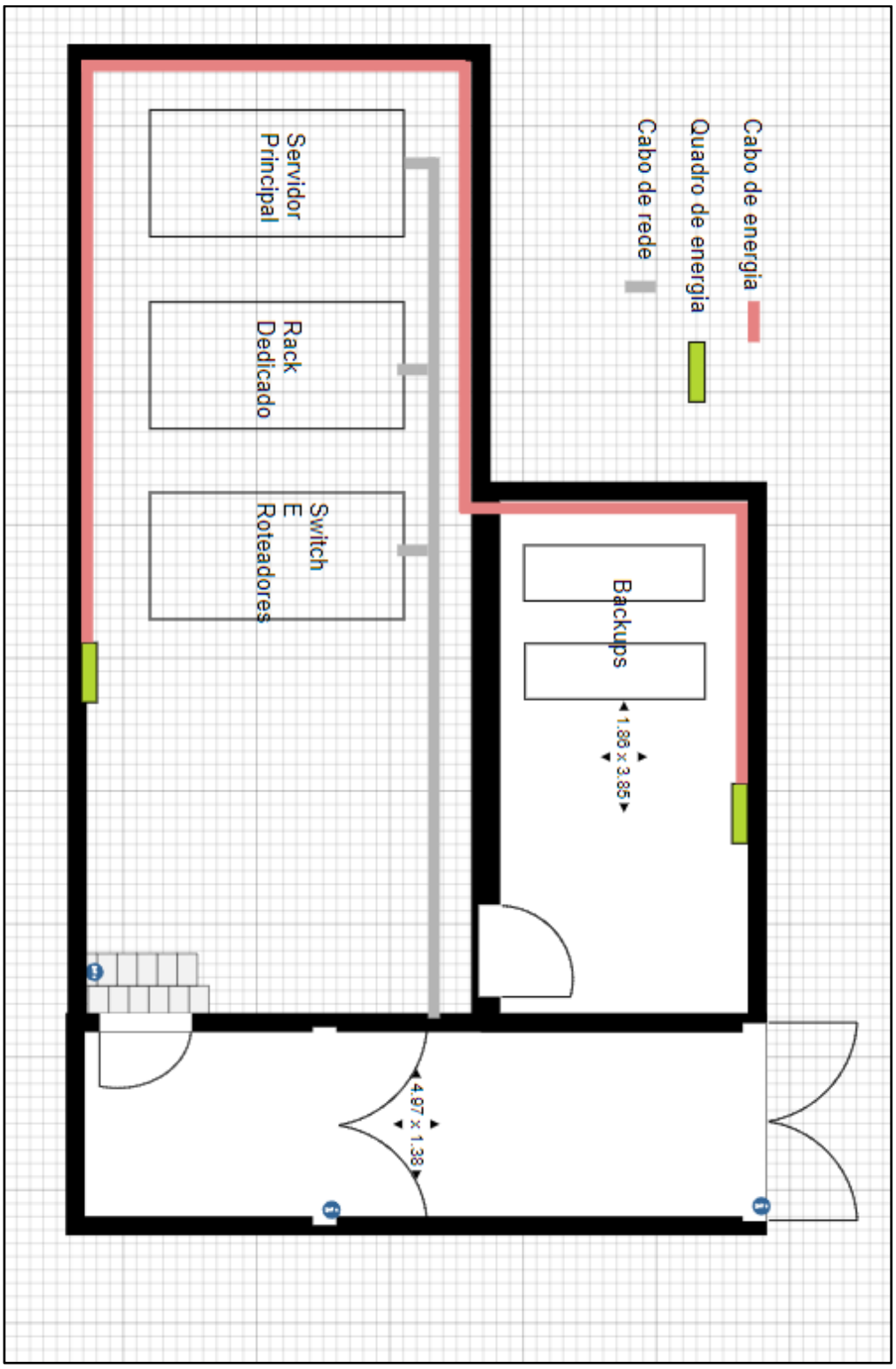
- Monitoramento por Câmeras na Sala dos *Racks*: Três câmeras de vigilância foram estrategicamente posicionadas dentro da sala dos *racks* para fornecer cobertura abrangente e monitorar continuamente as atividades. Essas câmeras são essenciais para detectar e registrar qualquer atividade suspeita ou acesso não autorizado aos equipamentos de TI e servidores.
- Monitoramento na Sala de *Backups*: Duas câmeras de vigilância foram instaladas na sala de *backups*, onde os *backups* estão localizados nos suportes mecânicos. Essas câmeras garantem que qualquer acesso ou manipulação dos *backups* seja registrado e possa ser auditado posteriormente, garantindo a segurança e a integridade dos dados de *backup*.
- Sistema de Alarme no *Hall* de Entrada: No *hall* de entrada, um sistema de alarme foi instalado para detectar qualquer tentativa de intrusão. Alarmes externos também foram instalados nas proximidades para serem acionados caso necessário, aumentando a segurança do perímetro do *data center*.

Essas medidas de segurança física são fundamentais para garantir que apenas pessoal autorizado tenha acesso à sala do *data center* e que todas as atividades dentro do ambiente sejam monitoradas de forma contínua, protegendo os ativos críticos e os dados sensíveis armazenados.

Após a garantia da segurança física do *data center*, é importante explorar sua infraestrutura interna para compreender como ela contribui para a eficiência operacional e a manutenção adequada dos equipamentos, sendo uma parte fundamental dessa infraestrutura o piso elevado.

7.1.6. Planta do piso elevado do *data center*

Figura 8 - Planta do Piso Elevado



Fonte: Autor (2024).

O piso elevado desempenha um papel crucial na organização e na funcionalidade do ambiente do *data center*. Com uma altura de 30 centímetros, esse tipo de piso oferece espaço suficiente para a passagem eficiente dos cabos de rede, além de facilitar a manutenção dos equipamentos. Ao adentrar na sala, degraus conduzem ao piso elevado, garantindo acesso facilitado e segurança aos usuários.

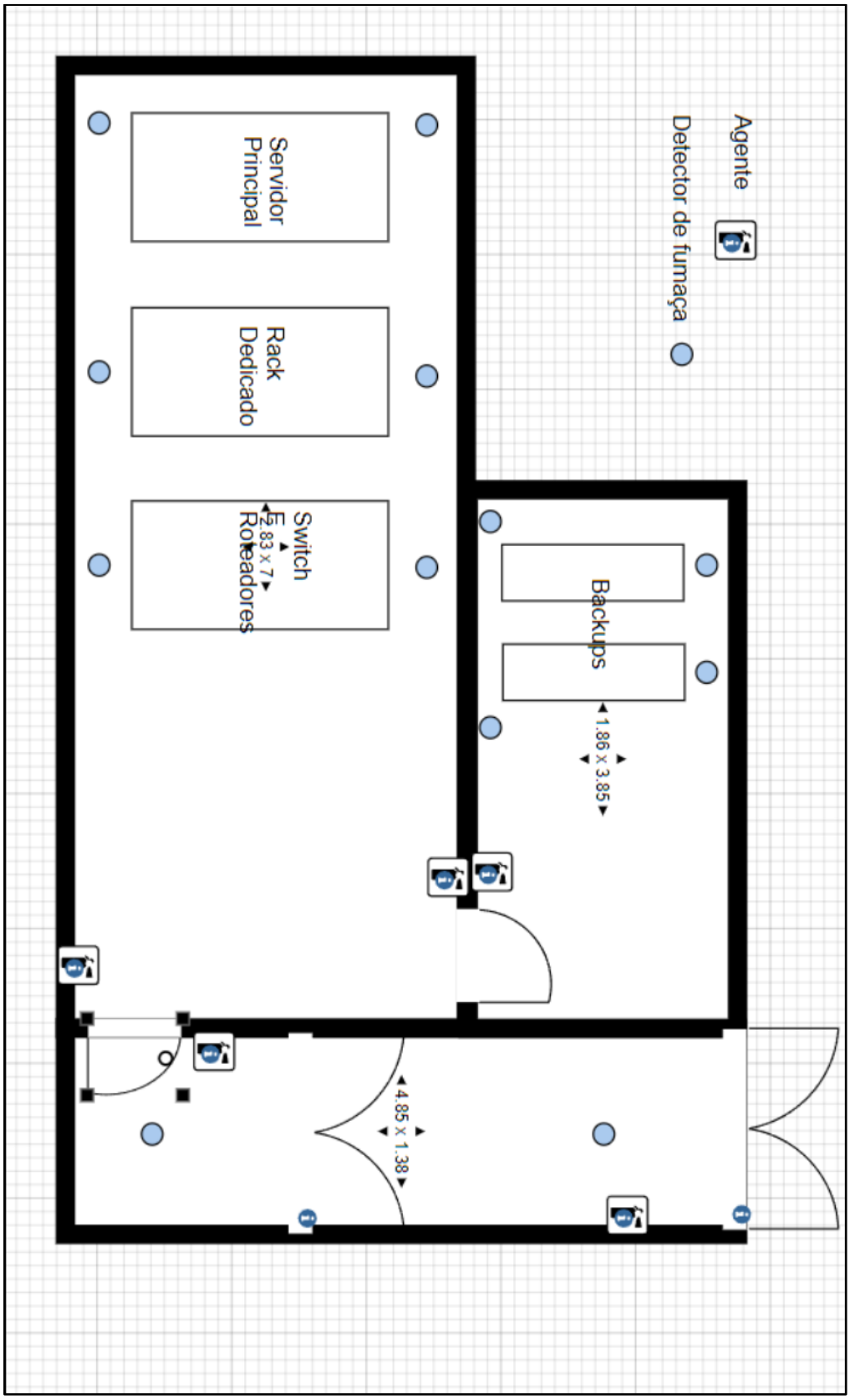
Suas principais funções incluem facilitar a manutenção e instalação dos equipamentos, permitir a circulação de ar para refrigeração eficiente e proporcionar flexibilidade para reconfigurações futuras. Os painéis removíveis permitem acesso fácil às instalações abaixo, o que é essencial para a realização de manutenções e modificações na infraestrutura.

Além disso, destaca-se que os cabos de energia são distribuídos pelas quinas por debaixo do piso elevado, mantendo uma distância segura dos cabos de rede. Essa disposição estratégica dos cabos garante não apenas uma maior segurança, mas também facilita o acesso para manutenção e reparos quando necessário.

Os dois quadros de energia nessa localização elevada, um localizado na sala de *backups* e outro na sala dos *racks*, facilitam a distribuição dos cabos de alimentação, evitando emaranhados e simplificando futuras manutenções.

7.1.7. Planta anti-incêndio do *data center*

Figura 9 - Planta de Anti Incêndio do *Data Center*



Fonte: Autor (2024).

Na planta de prevenção contra incêndios, são identificados os componentes responsáveis por auxiliar em casos de emergência.

No *hall* de entrada, duas portas corta-fogo são posicionadas estrategicamente para garantir a segurança e o controle de incêndios. Essas portas são projetadas para resistir ao fogo por um período determinado, impedindo sua propagação para outras áreas do *data center* e permitindo a evacuação segura em situações de emergência.

O sistema de detecção de fumaça é composto por 12 detectores distribuídos de maneira estratégica. Na sala dos *racks*, seis detectores estão localizados na parte superior, divididos igualmente entre o lado direito e o lado esquerdo. Na sala dos *backups*, quatro detectores estão posicionados também na parte superior, seguindo a mesma distribuição. Além disso, no corredor principal que dá acesso às salas dos *racks* e *backups*, dois detectores estão instalados, um na porta de entrada e outro na porta das salas, ambos na parte superior.

O sistema anti-incêndio também inclui extintores de incêndio, todos contendo gás carbônico (CO2) e indicados para incêndios das classes B e C. Esses extintores atuam por abafamento e resfriamento, sendo eficazes contra materiais combustíveis, líquidos inflamáveis e fogo proveniente de equipamentos elétricos. Ao todo, são cinco extintores distribuídos da seguinte forma: o primeiro está localizado no corredor de acesso às salas dos *racks* e *backups*, o segundo está na porta de acesso da sala dos *racks*, um ao lado de fora e outro na parte de dentro. O terceiro extintor está na porta de acesso à sala dos *backups*, e o quarto extintor está posicionado na porta interna da sala dos *backups*.

8. SERVIDOR

8.1. SERVIDOR RS H2483XU-RP QNAP

O primeiro servidor do *data center* é o Servidor TS h2483XU-RP *Qnap*, cujo

o valor é igual a R$ 211.000,00. Esse servidor é essencial para o funcionamento do ambiente e oferece alta capacidade de processamento e armazenamento.

8.1.2. Servidor TS-1273AU-RP Qnap (Servidor dedicado)

O segundo servidor é o Servidor TS-1273AU-RP *Qnap*, com um valor unitário de R$58.500,00. Esse servidor é dedicado a tarefas específicas e possui recursos otimizados para atender às demandas críticas do *data center*.

8.2. RACKS

8.2.1. Rack Apc 19” Netshelter Sx 42u Ar3300 (Rack normal)

Para acomodar os servidores e demais equipamentos, foram escolhidos dois *racks* do modelo *APC 19” Netshelter Sx 42u Ar3300*. Cada *rack* tem um valor unitário de R$ 12.967,92, totalizando R$ 25.935,84. Estes *racks* são ideais para otimizar o espaço e garantir a organização dos componentes.

8.2.2. Rack APC para Servidor 19 Netshelter SX 42U - AR3100 (Rack servidor)

Além dos *racks* normais, também foi adquirido um *Rack* APC para Servidor 19 *Netshelter SX 42U - AR3100*, com valor unitário de R$ 11.200,00. Esse *rack* é especialmente projetado para acomodar servidores, *switches* e outros dispositivos de rede de forma eficiente.

8.3. *FAILOVER* ATIVO-PASSIVO

No cenário escolar, opta-se pelo *failover* de tipo ativo-passivo, em que o servidor primário (ativo) é o único responsável pela execução das operações normais, enquanto o servidor secundário (passivo) permanece em estado de espera, monitorando o primário. Em caso de falha, o secundário assume o papel de ativo e passa a operar, garantindo a continuidade dos serviços. Essa abordagem é comumente adotada para assegurar alta disponibilidade dos sistemas críticos, como os utilizados para gerenciamento escolar e plataformas digitais (portal escolar).

9. *BACKUP* E RECUPERAÇÃO DE DESASTRES

9.1. CLASSIFICAÇÃO DE DADOS

- *Tier* 2: Arquivos de alunos desassociados e semestralmente; cópias *offline* por fita magnética, *HDs* ou *SSDs*.
- *Tier* 4: Arquivos diários, semanais e mensais; *online*.

9.1.1. Rotina de *backup*

- *Backup* noturno: das 20 horas até às 5 horas da manhã.

9.1.2. Programas de backup utilizados

- *Cobian Backup* (físico): Este software gratuito facilita a realização de *backups* de arquivos em pendrives, *HDs* externos e outros computadores da rede. Ele suporta *backups* completos, diferenciais e incrementais, oferece criptografia e permite a automação dos *backups* através de agendamento.

- *Backup Center* (digital): Este programa gratuito fornece todas as funcionalidades necessárias para criar cópias de segurança de arquivos em *HDs* internos e externos, *CD*/*DVD*, computadores da rede, servidores *FTP* e outros dispositivos. Ele permite a realização de *backups* completos e incrementais, agendamento automático e criptografia de dados.

9.1.3. Rotina de testes

- Testes automatizados: Dos *backups* antigos e recentes, realizados *online* pelo *Azure* e fisicamente pela rotina de teste da funcionalidade do sistema. Este sistema verifica se os *backups* estão iniciando corretamente, interage com o usuário e avalia a eficácia dos recursos de automação.
- Teste de *restore*: Simulação de cenários de restauração de dados, verificando se as informações podem ser recuperadas adequadamente. Fitas magnéticas são verificadas para 6.656 usos e vida útil de 30 anos.

9.1.4. Empresa de backup

Empresa contratada: *HelpITech*, responsável por *backups* na nuvem e físicos.

9.1.5. *Backup online* e físico

- *Backup online*: Realizado diariamente, semanalmente e mensalmente. Mensalmente, é feito o *backup* físico de todos esses dados, armazenados em local contratado e mantidos à vácuo.

- Cópias *online*: 1 dia de ontem e 1 dia de hoje. Utilização do *Azure (Microsoft)*, custando R$6.125,00 por cópia, totalizando R$12.250,00 para duas cópias, com criptografia *AES-256 bits*.
- Cópia física: *InetWeb*, ao custo de R$11.228,80, utilizando fita magnética *HP LT0-8 Ultrium Q2078A* com criptografia *AES-256*.

9.1.6. *Criptografia*

A criptografia *AES-256* é uma forma de manter dados seguros, convertendo-os em texto cifrado que só pode ser decifrado com a chave correta. Utiliza uma chave de 256 *bits*, garantindo alta segurança para os dados armazenados.

9.1.7. Sistema de armazenamento à vácuo

Para proteção de *HDs*, *SSDs* e fitas magnéticas, será utilizado um sistema à vácuo.

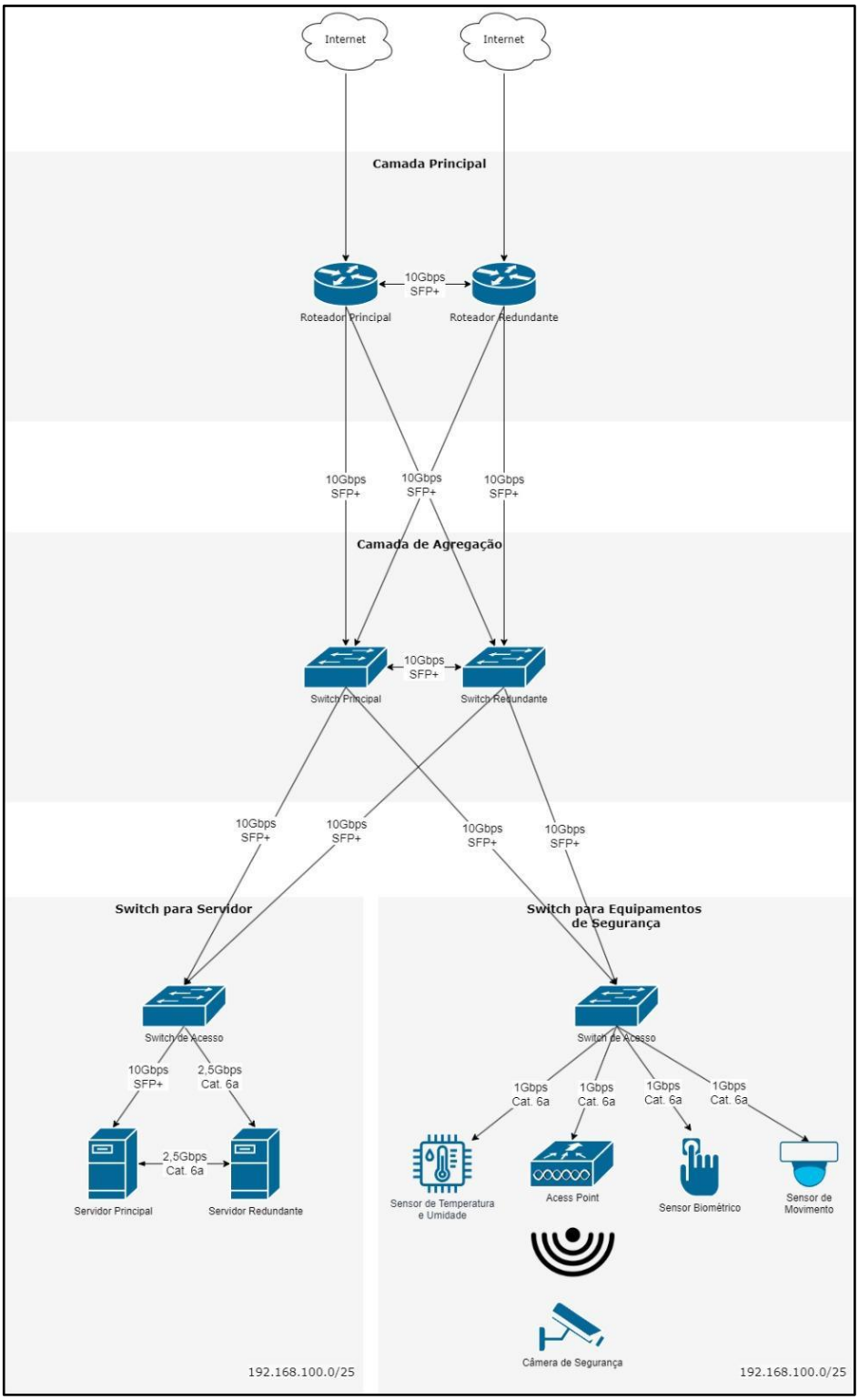
9.1.8. Técnicas de *backup*

- *Backup* diferencial e incremental: Técnica que permite atualizar *backups* existentes com novas informações, mantendo um histórico das alterações.

10. REDE E CONECTIVIDADE

10.1. CAMADAS, EQUIPAMENTOS E LINKS DE CONEXÃO

Figura 10 - Diagrama de Rede



Fonte: Autor (2024).

O projeto da rede do data center é estruturado em diferentes camadas, cada uma desempenhando um papel específico na interconexão e na operação dos equipamentos. A seguir, são fornecidas explicações detalhadas das camadas do diagrama de redes, os equipamentos que se conectam, as redundâncias e os serviços de rede oferecidos.

10.1.1. Camada principal

A camada principal do data center é responsável por gerenciar e controlar o tráfego de dados entre a rede interna e a internet, garantindo uma conexão estável e segura. Esta camada é essencial para a comunicação eficiente de todos os sistemas e para a aplicação de políticas de segurança de rede. No data center da escola, a camada principal é composta por dois roteadores: um operante e um redundante, que asseguram a continuidade dos serviços em caso de falha de um dos dispositivos.

Os roteadores utilizados na camada principal são do modelo Mikrotik Cloud Core Router CCR2004-1G-12S+2XS. Este equipamento possui um processador quad-core ARM de 64 bits com 1,7 GHz, 4 GB de RAM e 128 MB de armazenamento NAND. Ele é equipado com 12 portas SFP+ para conexões de 10 Gbps e 2 portas SFP28 para conexões de 25 Gbps, além de uma porta Gigabit Ethernet. O roteador suporta diversas funcionalidades avançadas, incluindo roteamento dinâmico, firewall, gerenciamento de largura de banda e VPN.

A redundância na camada principal é assegurada através de dois roteadores que permitem realizar uma operação contínua. Em condições normais, o roteador operante gerencia todo o tráfego de rede. No entanto, se o roteador operante falhar, o roteador redundante assume automaticamente as funções do roteador principal sem interrupção perceptível no serviço. Este processo é viabilizado pelo protocolo VRRP (Virtual Router Redundancy Protocol), que monitora o estado dos roteadores e realiza a transição de controle em caso de falha. Ambos os roteadores estão configurados para usar um IP virtual compartilhado, 192.168.100.1. Este IP virtual é o endereço que os dispositivos na rede utilizam como gateway padrão, enquanto cada roteador possui um IP real distinto para fins de administração e monitoramento, como 192.168.100.2 para o roteador operante e 192.168.100.3 para o roteador redundante. Esta configuração assegura que, em caso de falha do roteador principal, o roteador

redundante pode assumir o IP virtual e continuar a fornecer serviços de rede sem interrupção.

Para garantir uma comunicação de alta velocidade e baixa latência entre os roteadores da camada principal e os switches da camada subsequente, o cabeamento utilizado será de links de 10 Gbps através de módulos SFP+ (Small Form-factor Pluggable Plus). Este tipo de cabeamento é ideal para transmissões de dados em alta velocidade, proporcionando uma conexão estável e de alta performance com mínima interferência.

10.1.2. Camada de Agregação

Na camada de agregação, 2 switches conectam os roteadores da camada principal aos switches da camada de acesso. A camada de agregação desempenha um papel crucial no data center, concentrando e interligando o tráfego da rede e dispositivos antes de enviá-lo para a camada de acesso ou para a saída da rede. Além disso, ela é importante para escalabilidade da rede do data center, pois seus switches comportam a conexão de diversos switches da camada de acesso, conforme necessário para atender às demandas de expansão e crescimento do data center.

Os switches utilizados na camada de agregação são do modelo Switch Cloud Mikrotik CRS317-1G-16S+RM. Cada um desses equipamentos é caracterizado por 16 portas SFP+ de 10 Gbps e uma porta Gigabit Ethernet, oferecendo alta capacidade de transmissão de dados. Além disso, os switches possuem um sistema de refrigeração redundante, com dois coolers independentes em cada dispositivo, garantindo uma dissipação eficiente do calor e aumentando a confiabilidade operacional em ambientes de alta demanda.

A redundância na camada de agregação é garantida pela configuração de ambos os switches em paralelo. Ambos os dispositivos operam simultaneamente, distribuindo o tráfego de forma equilibrada entre si. Em caso de falha de um dos switches, o outro assume automaticamente a carga de trabalho, garantindo a continuidade dos serviços sem interrupções.

O cabeamento utilizado na camada de agregação é a mesma da camada principal, ou seja, links de 10 Gbps através de módulos SFP+ (Small Form-factor Pluggable Plus). Esta escolha garante uma comunicação de alta velocidade e baixa latência entre os switches da camada de agregação e a camada de acesso.

10.1.3. Camada de acesso

A camada de acesso é a interface entre os dispositivos finais dos usuários e o restante da infraestrutura de rede do data center. Ela é responsável por fornecer conectividade local aos dispositivos, garantindo acesso eficiente aos recursos da rede interna e externa. Diferente das outras camadas, esta não possui redundância de equipamentos, então apenas um switch será disposto para conectar certo equipamento à rede do data center.

A divisão dos switches de acesso é feita com base na função dos equipamentos. Desta forma, um switch será responsável por conectar os servidores, tanto o principal quanto o redundante, enquanto outro switch conectará os equipamentos de segurança, como controlador de acesso, kit de alarmes com sensor de biometria, e sensores de temperatura e umidade, além de um access point para conectar as câmeras de segurança via Wi-Fi.

Os switches utilizados na camada de acesso são do modelo Switch Cisco Business 220 CBS220-24T-4X-NA. Esse equipamento possui 24 portas Gigabit Ethernet e 4 portas SFP+ de 10 Gbps, oferecendo uma ampla capacidade de conexão para os dispositivos finais. Além disso, ele possui recursos avançados de gerenciamento de rede, como VLANs, QoS e segurança integrada, proporcionando uma solução completa para as necessidades de conectividade do data center.

No switch reservado para os servidores, o principal receberá uma conexão SFP+ de 10 Gbps, enquanto o servidor redundante é limitado à um link de 2.5 Gbps pela porta RJ45, recebendo então uma conexão F/UTP de categoria 6a tanto do servidor principal quanto do switch. No switch responsável por conectar os equipamentos de segurança, todos os dispositivos possuem portas Gigabit, então também será feita uma conexão F/UTP de categoria 6a.

10.2. SERVIÇOS DE REDE E SEGURANÇA

Os serviços de rede e segurança do data center incluem:

- Antivírus *Kaspersky Next EDR Foundations*, responsável por proteger os servidores contra ameaças cibernéticas.
- Sistema Operacional *Windows Server* 2022 16 *Core* (*Data center Edition*), que permite a configuração de serviços de rede, como *DHCP, DNS e Firewall, e*

serviços de segurança para os servidores, como Failover (Ativo-Passivo). Esses serviços são essenciais para garantir o funcionamento e a segurança da rede, fornecendo recursos como atribuição dinâmica de endereços *IP*, resolução de nomes de domínio, proteção contra intrusões e recuperação de falhas.

Essa estrutura de rede foi projetada para fornecer uma conectividade confiável, segura e eficiente para os usuários e aplicativos da instituição, garantindo alta disponibilidade, desempenho otimizado e proteção contra ameaças cibernéticas.

10.3. ENDEREÇO DE REDE

O endereço de rede atribuído é 192.168.100.0/25, com uma máscara de subrede de 255.255.255.128. Isso permite a alocação de até 126 *hosts* na rede, com o primeiro *host* sendo 192.168.100.1, o último *host* 192.168.100.126 e o endereço de *broadcast* 192.168.100.127.

10.3.1. Equipamentos da rede

Os equipamentos de rede incluem:

- *Gateway* Padrão: 192.168.100.1
- Roteador Principal: 192.168.100.2
- Roteador Secundário: 192.168.100.3
- Servidor Principal: 192.168.100.20
- Servidor Redundante: 192.168.100.21
- *IP* Virtual para Serviço (servidores): 192.168.100.22
- *Access Point*: 192.168.100.40

10.3.2. Configuração DHCP do servidor

A configuração DHCP do servidor é a seguinte:

- Gateway padrão: 192.168.100.1
- IP inicial: 192.168.100.90
- Máscara de Subrede: 255.255.255.128
- Número Máximo de Usuários: 37

10.3.3. Equipamentos com *IP* dinâmico

Os equipamentos com *IP* dinâmico incluem:

- Controlador de Acesso
- Alarme
- Monitores de Temperatura
- Câmeras de Segurança

10.4. LARGURA DE BANDA

O pico estimado para utilização da largura de banda da rede foi:

- Pico de *Backup*: *2TB* em 9 horas, alcançando 517,81 *Mbps*;
- Pico de Acesso: 800 Usuários, exigindo 53,3 *Mbps*;
- Total estipulado: 571,11 *Mbps*.

10.5. *ISP'S* (PROVEDORES DE SERVIÇOS DE INTERNET)

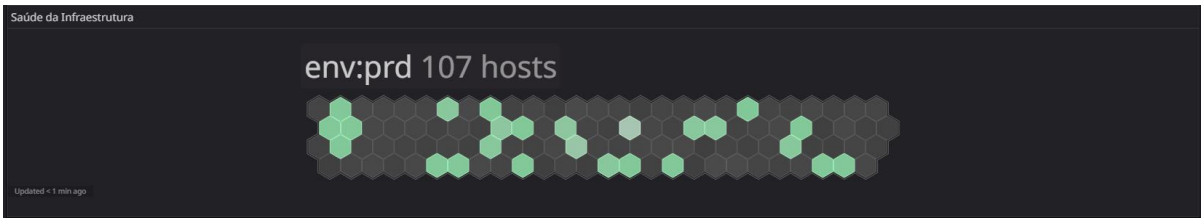
As opções de provedores de *internet* incluem:

- Claro: 1*GB* por R$199,90/Mensal;
- Vivo: 1GB por R$500,00/Mensal.

11. SEGURANÇA E MONITORAMENTO

11.1. *DATADOG*

Figura 11 - Exemplo meramente ilustrativo de *Dashboard* no *Datadog*, Saúde da Infraestrutura.



Fonte: Autor (2024)

O monitoramento de infraestrutura é uma prática essencial para garantir a estabilidade, segurança e eficiência dos sistemas de uma organização. Nesse contexto, o *Datadog*, um *software* de monitoramento como serviço (*SaaS*), desempenha um papel crucial ao fornecer uma plataforma abrangente para monitorar e analisar diversos aspectos da infraestrutura de TI.

O *Datadog* oferece uma ampla gama de recursos e funcionalidades para monitorar diferentes componentes de uma infraestrutura, desde servidores e bancos de dados até serviços de rede e aplicativos. Através da instalação de um agente nos servidores, o *Datadog* é capaz de coletar dados de desempenho em tempo real, incluindo métricas de *CPU*, memória, disco, rede e outros indicadores-chave. Além disso, o *Datadog* pode monitorar *logs* de sistema e eventos, permitindo a detecção precoce de problemas e a análise de tendências.

No contexto do projeto apresentado, o *Datadog* seria utilizado para monitorar os servidores do *data center*, incluindo o banco de dados, *backups* e métricas dos sensores de temperatura e umidade. O plano pro do *Datadog*, estimado em cerca de $15 por *host* por mês, oferece uma solução acessível para monitorar até 10 *hosts*, tornando-o uma opção viável para pequenos *data centers*, como contempla o projeto apresentado.

Além disso, o *Datadog* oferece integrações com uma variedade de serviços e ferramentas, permitindo uma visão holística da infraestrutura de TI. Isso inclui a capacidade de monitorar serviços de rede, como *switches*, roteadores e *firewalls*. Essa integração permite uma visão unificada do ambiente de TI, facilitando a detecção e resolução de problemas.

11.1.1 Descrição dos equipamentos de segurança e monitoramento

Este capítulo apresenta a descrição dos equipamentos de segurança e monitoramento de um *data center*, detalhando suas especificações e capacidades de integração. Os itens incluem câmeras de segurança, controlador de acesso, alarme/sensor de entrada, sensores de temperatura/umidade e detectores de fumaça.

11.1.2. Câmeras de segurança

As câmeras de segurança são da marca Tapo e totalizam sete unidades, distribuídas conforme especificado abaixo:
Localizações:

- Duas câmeras no corredor principal (entrada);
- Três câmeras na sala do servidor;
- Duas câmeras na sala de *backup*.

As câmeras possuem conexão *Wi-Fi* e utilizam cartões *MicroSD SanDisk* de 512 *GB* para armazenamento. Cada câmera é equipada com um cartão *MicroSD*, totalizando sete cartões.

O *software* utilizado para as câmeras é o Tapo App, disponível gratuitamente na *App Store*, portanto, essas câmeras não podem ser integradas com o *Datadog*.

11.1.3. Controlador de acesso

O controlador de acesso disponível é de um modelo não especificado e utiliza métodos de autenticação por biometria e/ou crachá. Este equipamento possui conexão *Ethernet*.

O software utilizado é o *Idflex* Admin, que é gratuito. Além disso, este controlador de acesso possui capacidade de integração com o *Datadog*.

11.1.4. Alarme/Sensor de entrada

O alarme/sensor de entrada está localizado na entrada do *Data Center* e possui conexão *Ethernet*.

O *software* associado a este dispositivo é o Intelbras AMT *Mobile* V3, disponível gratuitamente na *App Store*. Este alarme pode ser integrado com o *Datadog*.

11.1.5. Sensores de temperatura/umidade

Os sensores de temperatura/umidade são do modelo *Kit Term-2S*, e há um total de cinco unidades instaladas nas seguintes localizações:

- Um sensor na entrada do *Data Center*;
- Um sensor na sala do servidor, próximo à circulação de ar do piso elevado;
- Dois sensores dentro dos *racks* dos servidores;
- Um sensor na sala de *backup*.

Esses sensores possuem conexão *Ethernet* e utilizam um *software* próprio. Com um *software* de gerenciamento pode gerar relatórios, gráficos e com sistema de alertas por *e-mail*, *SMS* (opcional) ou discador telefônico (opcional) ou módulo remoto (opcional). Além disso, eles podem ser integrados com o *Datadog*.

11.1.6. Detectores de fumaça

O *Data Center* conta com doze detectores de fumaça, distribuídos da seguinte forma:

- Dois detectores na entrada;
- Seis detectores na sala dos servidores;
- Dois detectores na sala de *backup*.

Não necessitam de *software* próprios e nem integrações com o *datadog*.

Os equipamentos descritos neste capítulo são essenciais para a segurança e monitoramento do *Data Center*, proporcionando proteção abrangente contra diversas ameaças. A capacidade de integração com o *Datadog* foi considerada para os dispositivos aplicáveis, garantindo uma gestão centralizada e eficiente.

12. SISTEMA DE ENERGIA E RESFRIAMENTO

12.1. CORREDORES DE AR QUENTE E AR FRIO

O sistema de refrigeração do *data center* é essencial para garantir o funcionamento eficiente dos equipamentos de computação. Para controlar a

temperatura e umidade, o *data center* adota a prática de separação em corredores de ar quente e ar frio. No corredor de ar frio, os equipamentos de TI recebem ar frio para manter uma temperatura adequada para a operação ideal.

Os tubos de ventilação estrategicamente posicionados garantem a circulação adequada do ar frio dentro do ambiente. Eles removem o ar quente gerado pelos equipamentos e introduzem ar frio para resfriá-los. Esse fluxo de ar controlado evita a formação de pontos quentes que poderiam levar ao superaquecimento dos equipamentos.

12.1.1. Monitoramento de temperatura

O *data center* implementa um monitoramento de temperatura para garantir condições operacionais ideais para o equipamentos de computação. Cinco sensores de temperatura foram estrategicamente instalados em diferentes áreas:

Um sensor na entrada principal do *data center* monitora as condições ambientais externas, fornecendo informações sobre variações de temperatura e umidade.

Nos *racks* que abrigam os servidores, um sensor é posicionado para monitorar as condições térmicas desses locais críticos, garantindo que os equipamentos permaneçam dentro de limites seguros de temperatura.

Outro sensor é colocado na sala dos *racks* para oferecer uma visão abrangente da temperatura e umidade nesse espaço central, permitindo a detecção precoce de problemas de calor.

Na sala de *backups*, um sensor monitora continuamente as condições, garantindo a proteção dos equipamentos críticos mesmo em situações de falha ou emergência.

Os sensores estão configurados cada um para enviar uma mensagem de alerta via *SMS* ou *e-mail* caso a temperatura detectada ultrapasse 25 graus Celsius na área que monitoram. Essa funcionalidade integrada proporciona uma camada extra de segurança, permitindo uma resposta rápida a situações de superaquecimento e garantindo a proteção contínua dos equipamentos de computação.

Esses sensores desempenham um papel crucial no monitoramento contínuo das condições de temperatura em todo o *data center*,proporcionando um ambiente operacional seguro e estável para os equipamentos de computação.

12.1.2. Distribuição de energia elétrica

O *data center* conta com 2 quadros de distribuição de energia 380V (volts) que fornecem energia para o resto dos componentes do *data center*. Esses quadros desempenham um papel crucial na distribuição eficiente da energia elétrica em todo o ambiente do *data center*, garantindo alimentação adequada para servidores, sistemas de resfriamento, redes e outros equipamentos críticos.

12.1.3. Cabeamento de energia elétrica

Todo o cabeamento elétrico é cuidadosamente planejado e executado para garantir uma conexão segura e confiável entre os quadros de distribuição de energia e os equipamentos do *data center*. O cabeamento é passado por debaixo do piso elevado e pelas quinas de cada sala, seguindo um trajeto otimizado que minimiza o risco de danos físicos e garante uma organização eficiente.

Essa abordagem de instalação permite uma distribuição uniforme e ordenada dos cabos, facilitando a manutenção e evitando interferências desnecessárias no ambiente do *data center*. Além disso, contribui para a segurança, reduzindo o risco de tropeções ou danos acidentais aos cabos.

O cabeamento é de alta qualidade e segue padrões rigorosos de instalação para garantir a integridade do sistema elétrico do data center e minimizar possíveis problemas de desempenho ou falhas.

12.1.4. Redundância

Além da presença de dois quadros de distribuição de energia, o *data center* é projetado com redundância elétrica para garantir máxima disponibilidade e confiabilidade. Isso inclui sistemas de alimentação redundantes, como um *nobreak* de 10 *KVA (Quilovolt-ampere)* que opera continuamente para fornecer energia principal, o *nobreak* mantém os sistemas operacionais até que o gerador de energia a diesel, com potência máxima de 72 *KVA (Quilovolt-ampere)* e equipado com um quadro de transferência automática (ATS), entre em funcionamento. Essas medidas, juntamente com caminhos de distribuição de energia redundantes, garantem que o *data center*

permaneça operacional mesmo em caso de falhas de energia, proporcionando continuidade aos serviços críticos.

13. AQUISIÇÃO DE EQUIPAMENTOS

Tabela 1 - Aquisição de Equipamentos: materiais.

Descrição	Unidade	Valor Unitário	Valor Total
Servidor *TS h2483XU- RP*	1	R$ 211.000,00	R$ 211.000,00

Qnap.			
Servidor *TS-1273AU-RP Qnap*	1	R$ 58.500,00	R$ 58.500,00
Rack Apc 19” *Netshelter Sx 42u Ar3300*	2	R$ 12.967,92	R$ 25.935,84
Rack APC para Servidor 19 *Netshelter SX 42U - AR3100*	1	R$ 11.200,00	R$ 11.200,00
Suporte mecânico de disco rígido	2	R$ 75,00	R$ 150,00
Split Duto *Carrier Built-in Versatile 60000*	2	R$ 12.169,85	R$ 24.339,70
Split Teto Inverter *Carrier X Power Connect*	6	R$ 9.099,00	R$ 54.594,00
Duto de ar condicionado	40	R$ 260,00	R$ 10.400,00
Agentes - *HFC-227*	5	R$ 6.500,00	R$ 32.500,00
Detector de fumaça endereçável 2951J	12	R$ 1.500,00	R$ 18.000,00

Kit de Alarme Intelbras AMT 2018 E com 13 Sensores	1	R$ 1.470,00	R$ 1.470,00
Câmera de Segurança	7	R$ 400,00	R$ 2.800,00
Controlador de Acesso Bio/Prox *iDFlex - Control iD*	1	R$ 1.154,25	R$ 1.154,25
Nobreak *10KVA* - Senoidal	1	R$ 16.500,00	R$ 16.500,00
Gerador de Energia- *ND72100ES3QTA* - Nagano	1	R$ 16.000,00	R$ 45.000,00
Quadro Distribuidor De Energia	2	R$ 16.000,00	R$ 32.000,00
Kit Term-2S	5	R$ 3.606,00	R$ 18.030,00
Cartão *MicroSD SanDisk* 512*GB*	7	R$ 332,00	R$ 2.324,00
Fita Magnética *HP LT0-8 Ultrium Q2078A*	4	R$ 800,00	R$ 3.200,00

Fonte: Autor (2024).

Tabela 2 - Aquisição de Equipamentos: serviços.

Descrição	Unidade	Valor Unitário	Valor Total
Link 1 *GB* (Claro)	1	R$ 199,90	R$ 199,90
Link 1 *GB* (Vivo)	1	R$ 500,00	R$ 500,00
Azure Backup	2	R$ 6.125,00	R$ 12.250,00
Antivírus *Kaspersky Next EDR Foundations*	1	R$ 663,00	R$ 663,00
Sistema Operacional *Windows Server* 2022 16 *Core*	1	R$ 9.265,00	R$ 9.265,00
Datadog	2	R$ 78,40	R$ 156,80

Fonte: Autor (2024).

Tabela 3 - Aquisição de Equipamentos: cabeamento.

Descrição	Unidade	Valor Unitário	Valor Total
Dell Networking Cabo, *SFP*+ até 10 m	4	R$ 1.681,00	R$ 6.724,00
Dell Networking Cabo, *SFP*+ até 20 m	7	R$ 2.615,00	R$ 18.305,00
305 metros de cabo *Cat*. 6a	1	R$ 4.299,00	R$ 4.299,00

Fonte: Autor (2024).

Tabela 4 - Aquisição de Equipamentos: equipamento de rede.

Descrição	Unidade	Valor Unitário	Valor Total
Mikrotik Cloud Core Router CCR2004	2	R$ 4.271,05	R$ 8.542,10
Switch Cloud Roteador *Mikrotik*	2	R$ 5.099,15	R$ 10.198,30
Switch Cisco Business 220	2	R$ 3.099,00	R$ 6.198,00
Access Point HPE	1	R$ 2.189,00	R$ 2.189,00

Fonte: Autor (2024).

Tabela 5 - Aquisição de Equipamentos: total de gastos.

Descrição	Valor Total
Materiais	R$ 543.161,95
Serviços	R$ 23.034,70
Cabeamento	R$ 29.328,00
Equipamentos de rede	R$ 27.127,40
TOTAL:	**R$ 622.652,05**

Fonte: Autor (2024).

14. TESTES E VALIDAÇÃO

Com o objetivo de alcançar um desempenho de alta eficiência no data center, a equipe projetou uma rotina robusta de testes e validação. Essa iniciativa, implementada de forma periódica e estratégica, visa garantir a manutenção preventiva, a qualidade superior dos serviços e equipamentos e, consequentemente, a operacionalidade impecável da infraestrutura.

Para cada tópico, foi identificado possíveis cenários de risco e projetado soluções preventivas e abordagens robustas para garantir a segurança e a confiabilidade.

14.1. TESTES NA INFRAESTRUTURA FÍSICA

- Cenário de Desastre Natural e Crescimento da Demanda.

Foi pensado em possíveis desastres naturais como um terremoto, inundações ou outro evento que possa afetar o *data center*, onde foi avaliado a resiliência de sua infraestrutura física. Esta avaliação abrangeu não apenas a robustez da estrutura do prédio, os sistemas de proteção contra incêndio e os sistemas de energia de reserva, mas também aproveitou as vantagens de sua localização estratégica. Por estar situado no penúltimo andar, o *data center* desfruta de uma proteção adicional contra inundações, proporcionando uma camada extra de proteção em face de potenciais desafios ambientais.

Outro ponto levantado foi o aumento significativo na demanda por serviços (novas turmas, novos produtos), e assim foi avaliado a capacidade da infraestrutura física de suportar o crescimento da demanda, incluindo o espaço disponível, a capacidade de refrigeração e a infraestrutura de rede.

14.1.1. Aquisição de Equipamentos

- Falha de Equipamentos e Compatibilidade e Integração:

Foi simulado a falha de um componente crítico do *data center*, como um servidor, um *switch* de rede ou um sistema de armazenamento e a integração de novos equipamentos no *data center*, incluindo servidores, dispositivos de rede e sistemas de armazenamento.

Posteriormente, foi avaliado o impacto da falha no desempenho do *data center* e na disponibilidade dos serviços, bem como a capacidade dos sistemas de

redundância de garantir a continuidade das operações, além da compatibilidade dos novos equipamentos com os sistemas existentes e garantir que a integração seja realizada de forma suave e sem interrupções nos serviços.

14.1.2. Rede e Conectividade

- Ataque Cibernético e Congestionamento da Rede:

Um ataque cibernético à rede do data center foi simulado, como um ataque DDoS ou um *malware* para verificar a efetividade das medidas de segurança da rede, incluindo *firewalls*, sistemas de detecção de intrusão e soluções de proteção contra *malware*.

Nessa simulação, foi feito um pico alto no tráfego na rede do *data center*, como o lançamento de um novo produto ou serviço, e nesse teste, teve como objetivo avaliar a capacidade da rede de lidar com o pico de tráfego sem comprometer o desempenho dos serviços e a experiência do usuário.

14.1.3. Sistemas de Energia e Resfriamento

- Falha de Energia e Falha de Resfriamento:

Foi simulado uma falha no fornecimento de energia para o *data center*, como uma queda de energia ou um problema no gerador de *backup* e assim, foi analisado a capacidade dos sistemas de energia de reserva de garantir a continuidade das operações do *data center* em caso de falha no fornecimento de energia.

Foi colocado em pauta a hipótese de uma falha no sistema de refrigeração do data center, como uma falha no sistema de ar condicionado ou um vazamento de água,e assim avaliado a capacidade dos sistemas de refrigeração de manter a temperatura adequada no *data center* e evitar o superaquecimento dos equipamentos.

14.1.4. Segurança e Monitoramento

- Falha no sistema de monitoramento

Foi hipotetizada uma falha no sistema de monitoramento do *data center* (desativação intencional dos sistemas IDS/IPS principais e o monitoramento da resposta dos sistemas redundantes e da equipe de TI à falha), como uma falha nos sistemas de detecção de intrusões ou nos sistemas de monitoramento de

desempenho para avaliar a capacidade dos sistemas redundantes de monitoramento em assumir as funções críticas em caso de falha e testar a eficácia dos procedimentos de detecção e resposta a falhas nos sistemas de monitoramento.

A eficiência dos sistemas de monitoramento foi testada, assegurando que o desempenho e a segurança do *data center* sejam mantidos mesmo durante falhas nos sistemas de monitoramento principais.

A parte de segurança contempla tudo anteriormente citado nos demais tópicos, desde a segurança física à digital.

15. CONCLUSÃO

Ao concluírem a árdua jornada de desenvolvimento do projeto de *data center*, a equipe composta por Carolina de Andrade Franzolin, Gabriel Matos Alencar, Geovanna Vieira Dos Santos, Guilherme Vitala Fortunato, Lucas Oliveira Campos, Luis Eduardo Pedro, Oliver Christian Souza, Sheila Luiza Soares Cabral e Yago Raiol da Silva celebra com imensa satisfação os significativos avanços alcançados. A construção deste *data center*, desde a concepção inicial até a implementação final, exigiu um esforço conjunto monumental, marcado por dedicação, maturidade e expertise multidisciplinar.

Ao chegarem à etapa final deste trabalho, torna-se fundamental recapitular os resultados obtidos. O *data center*, idealizado para o Colégio Jorgina, instituição de ensino dedicada ao público infantojuvenil, encontrou na construção deste *data center* a solução para otimizar o controle de informações e o desempenho dos servidores da escola. Através dessa iniciativa, a gestão de dados cruciais para alunos, pais, professores e funcionários será aprimorada, garantindo maior eficiência e transparência no ambiente educacional.

Além dos resultados tangíveis, a equipe vivenciou uma jornada rica em aprendizados. A complexidade do projeto desafiou as habilidades técnicas e, mais importante ainda, fortaleceu a capacidade de trabalho em equipe e resolução de problemas. As nuances de colaboração multidisciplinar e a necessidade de adaptabilidade foram lições valiosas que certamente levarão consigo para futuros desafios.

16. REFERÊNCIAS

MOTTA, Sérgio. 10 programas gratuitos de backup para Windows. **SOFTDOWNLOAD**, 2023. Disponível em: https://www.softdownload.com.br/10-programas-gratuitos-backup-arquivos-windows.html. Acesso em: 16 maio 2024.

AHLGREN, Matt. O QUE É CRIPTOGRAFIA AES-256 E COMO FUNCIONA?. **WSR,** 2024. Disponível em: https://www.websiterating.com/pt/blog/cloud-storage/what-is-aes-256-encryption/. Acesso em: 16 maio 2024.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 6. ed. São Paulo: Atlas, 2008.

SISTEMA DE BIBLIOTECAS PROF. JOSÉ STORÓPOLI. Universidade Nove de Julho. **Manual para Elaboração de Trabalhos Acadêmicos de acordo com ABNT**. Disponível em: <http://docs.uninove.br/arte/pdfs/Manual-Elaboracao-de-Trabahos-ABNT.pdf>. Acesso em 30 de setembro de 2016.