UNIVERSIDADE SÃO JUDAS TADEU

BRUNO MARQUES MARTINS
ENZO GABRIEL GONÇALVES DE ABREU
IGOR SALDANHA DE ARAÚJO GARCIA NAVARRO
KAIQUE DIAS GONÇALVES DA SILVA
KAIQUE OLIVEIRA COSTA
LUIZ FELIPE SILVA ROBERTO
MURILO ANTÔNIO AMORIM SILVA

TUPÃ STUDIOS

SÃO PAULO

2025

BRUNO MARQUES MARTINS

ENZO GABRIEL GONÇALVES DE ABREU

IGOR SALDANHA DE ARAÚJO GARCIA NAVARRO

KAIQUE DIAS GONÇALVES DA SILVA

KAIQUE OLIVEIRA COSTA

LUIZ FELIPE SILVA ROBERTO

MURILO ANTÔNIO AMORIM SILVA

TUPÃ STUDIOS

Trabalho acadêmico apresentado como parte da avaliação da disciplina de Sistemas Computacionais e Segurança e Ambientes Computacionais e Conectividade, com foco no desenvolvimento do projeto empresarial Tupã Studios.

Orientadores:

Prof. Danilo De Souza Miguel

Prof. Carlos Enrique Lopez Noriega

Prof. Nelson Augusto Oliveira De Aguiar

São Paulo

2025

RESUMO

Este trabalho apresenta o projeto de uma infraestrutura computacional e de segurança para a empresa fictícia Tupã Studios, um estúdio brasileiro de desenvolvimento de jogos que cresceu muito durante a pandemia de covid-19, saindo de 7 para 210 funcionários distribuídos em quatro unidades. Diante dos desafios de proteger a propriedade intelectual e garantir a conectividade em um ambiente multi-escritório, foi realizada uma análise de vulnerabilidades que norteou o desenvolvimento da solução. O projeto detalha uma arquitetura de rede centralizada no modelo *Hub-and-Spoke*, com segmentação por *VLANs* para maior segurança. São especificadas as configurações de *hardware* para servidores e *desktops* de cada setor, com foco em custo-benefício, além de um plano de segurança da informação que estabelece políticas preventivas e de resposta a incidentes. A solução se completa com a integração de dispositivos *IoT* para monitoramento e a adoção de serviços de nuvem para a hospedagem dos servidores de jogos. O resultado é uma infraestrutura de TI robusta, segura e escalável, que serve como base para o crescimento e sucesso da Tupã Studios no mercado de entretenimento digital.

Palavras-chave: Segurança da Informação; Infraestrutura de Redes; Estúdio de Jogos; Arquitetura de TI; Plano de Segurança.

ABSTRACT

This document presents the design of a comprehensive IT and security infrastructure for the fictional company Tupã Studios, a Brazilian game development studio that boomed during the covid-19 pandemic, going from 7 to 210 employees distributed across four locations. Faced with the challenges of protecting intellectual property and ensuring connectivity in a multi-office environment, a vulnerability assessment was conducted to guide the solution's development. The project details a centralized Hub-and-Spoke network architecture with VLAN segmentation for enhanced security. Hardware configurations for servers and desktops in each department are specified with a focus on cost-effectiveness, alongside an information security plan that establishes preventive and incident response policies. The solution is complemented by the integration of IoT devices for monitoring and the adoption of cloud services for hosting game servers. The result is a robust, secure, and scalable IT infrastructure that serves as a foundation for the growth and success of Tupã Studios in the digital entertainment market.

Keywords: Information Security; Network Infrastructure; Game Studio; IT Architecture; Security Plan.

LISTA DE FIGURAS

Figura 4.1 - Planta baixa da Matriz em São Paulo 10
Figura 4.2 - Estrutura de Rede da Matriz em São Paulo 11
Figura 4.3 - Planta baixa da filial em São Paulo 12
Figura 4.4 - Estrutura de Rede da filial em São Paulo 13
Figura 4.5 - Planta baixa da filial no Rio de Janeiro 14
Figura 4.6 - Estrutura de Rede da filial no Rio de Janeiro 15
Figura 4.7 - Planta baixa da filial em Recife 16
Figura 4.8 - Estrutura de Rede da filial em Recife 17
Figura 7.1 - Distribuição do nível de risco 33
Figura 7.2 - Vulnerabilidades e níveis por setor 33

LISTA DE TABELAS

Tabela 3.1 - Setores e funcionários por unidade 9
Tabela 5.1 - IPs por setor na matriz 21
Tabela 5.2 - IPs por setor na Filial de São Paulo 22
Tabela 5.3 - IPs por setor na Filial do Rio de Janeiro 23
Tabela 5.4 - IPs por setor na Filial de Recife 24
Tabela 5.5 - IPs por filial 24
Tabela 9.1 - Preços para cada serviço AWS 47
Tabela 9.2 - Preços para cada serviço GCP 51
Tabela 9.3 - Comparativo de preços AWS x GCP 52
Tabela 11.1 - Valores totais de investimento em hardware 62

LISTA DE QUADROS

Quadro 6.1 - Softwares por setor 26
Quadro 7.1 - Análise de vulnerabilidades por setor 30
Quadro 10.1 - Detalhamento dos servidores On-premises 53
Quadro 11.1 - Detalhes técnicos de Hardware em inovação 54
Quadro 11.2 - Detalhes técnicos de Hardware em segurança 55
Quadro 11.3 - Detalhes técnicos de Hardware em desenvolvimento PC1 56
Quadro 11.4 - Detalhes técnicos de Hardware em desenvolvimento PC2 57
Quadro 11.5 - Detalhes técnicos de Hardware em atendimento ao cliente 58
Quadro 11.6 - Detalhes técnicos de Hardware em administração 59
Quadro 11.7 - Detalhes técnicos de Hardware em marketing 60
Quadro 11.8 - Detalhes técnicos de Hardware em limpeza e manutenção 61

SUMÁRIO

1 INTRODUÇÃO 5

2 MERCADO DE JOGOS 6

3 INFORMAÇÕES SOBRE A EMPRESA 7

3.1 Informações das unidades 9

4 PLANTAS BAIXAS 10

4.1 Sede São Paulo 10

4.1.1 Estrutura de Rede 11

4.2 Filial São Paulo 12

4.2.1 Estrutura de Rede 13

4.3 Filial Rio de Janeiro 14

4.3.1 Estrutura de Rede 15

4.4 Filial Recife 16

4.4.1 Estrutura de Rede 17

5 EXPLICAÇÃO DA INFRAESTRUTURA DE REDES DA EMPRESA 18

5.1 Arquitetura De Rede Local (*LAN*) 18
5.2 Servidores e Gerenciamento Centralizado 18
5.3 Conectividade entre Unidades (*WAN*) e Uso da Nuvem 19
5.4 Plano de Endereçamento *IP* e Segmentação de Rede 19
5.4.1 Estratégia de Endereçamento Global 20
5.4.2 Segmentação com *VLANs* (Virtual *LANs*) 20
5.4.3 Atribuição de Endereços 20
6 DESCRITIVO DE *SOFTWARES* E SISTEMAS OPERACIONAIS 25
7 PLANO DE SEGURANÇA 28
7.1 Análise de vulnerabilidades 28
7.2 Boas Práticas dos Funcionários 34
7.2.1 Senhas e Autenticação(2FA) 34
7.2.2 Uso de Dispositivos e Computadores 34
7.2.3 Proteção de Dados e Informações 34
7.2.4 Redes e Conectividade 35
7.2.5 *Backups* e Continuidade 35
7.2.6 Responsabilidades 35
7.2.7 Conscientização em Segurança Digital 35
7.2.8 Proteção de Dados e Informações 36
7.2.9 Boas Práticas em Redes Sociais e Comunicação 36
7.2.10 Gestão Física e Ambiental. 37
7.2.11 Responsabilidade no Trabalho Remoto 37
7.2.12 Cultura de Segurança 37
7.3 Plano de Contingência 37
7.3.1 Objetivo 38
7.3.2 Procedimentos de Contingência por Tipo de Incidente 38

7.3.3 Responsáveis 39
8 SERVIÇOS DE NUVEM NECESSÁRIOS 40
9 COMPARAÇÃO DE SERVIÇOS DE NUVEM 41
9.1 Preços AWS 42
9.1.1 Computação (Máquinas Virtuais) 42
9.1.2 Banco de Dados Gerenciado 42
9.1.3 Armazenamento 43
9.1.4 Balanceamento de Carga 43
9.1.5 Segurança 44
9.1.6 Monitoramento e Logs 44
9.1.7 Entrega de Conteúdo (CDN) 45
9.1.8 CI/CD e Ferramenta de Desenvolvimento 45
9.2 Tabela Preços AWS 47
9.3 Preços GCP 47
9.3.1 Máquinas virtuais 48
9.3.2 Banco de Dados Gerenciado 48
9.3.3 Armazenamento 48
9.3.4 Balanceamento de Carga 48
9.3.5 Segurança 49
9.3.6 Monitoramento e Logs 49
9.3.7 Entrega de Conteúdo 50
9.3.8 CI/CD e Ferramenta de Desenvolvimento 51
9.4 Tabela Preços GCP 51
9.5 Tabela Comparação AWS x GCP 52
10 DESCRITIVO DOS SERVIDORES 53
11 DESCRITIVO DOS HARDWARES POR SETOR 54

11.1 Setor de Inovação 54
11.2 Setor de Segurança 55
11.3 Setor de Desenvolvimento 56
11.4 Setor de Atendimento ao Cliente 58
11.5 Setor Administração 59
11.6 Setor de Marketing 60
11.7 Setor de Limpeza e Manutenção 61
11.8 Valores Totais 62
12 IMPLEMENTAÇÃO DE DISPOSITIVOS *IOT* **63**
12.1 Segurança Física e Monitoramento de Ativos Críticos 63
12.2 Gestão de Energia e Continuidade Operacional 64
12.3 Otimização do Ambiente de Trabalho (Smart Office) 64
13 CONCLUSÃO **65**
REFERÊNCIAS **66**
GLOSSÁRIO **69**

1 INTRODUÇÃO

O setor de entretenimento digital, especialmente o de desenvolvimento de jogos, representa um mercado global dinâmico e altamente competitivo. Para empresas brasileiras como a Tupã Studios, um estúdio com 210 funcionários distribuídos em quatro escritórios, estabelecer uma base tecnológica sólida não é apenas uma necessidade operacional, mas um pilar estratégico para a inovação e o sucesso. A natureza do negócio, que envolve a criação e o gerenciamento de propriedade intelectual de alto valor, como o código-fonte de jogos, exige uma infraestrutura computacional que seja, ao mesmo tempo, resiliente, segura e escalável.

O principal desafio abordado neste trabalho é a concepção de uma infraestrutura de *TI* que responda às complexidades operacionais da Tupã Studios. Isso inclui a necessidade de proteger seus ativos digitais contra ameaças internas e externas, garantir a comunicação eficiente entre suas equipes geograficamente dispersas e prover uma plataforma estável para o ciclo de desenvolvimento e para a entrega de jogos online aos seus clientes. A análise de vulnerabilidades revelou riscos que vão desde o acesso físico inadequado a servidores até a exposição de dados em redes não segmentadas, demandando uma solução integrada.

O objetivo deste trabalho é projetar e documentar uma infraestrutura computacional e de segurança completa para a empresa Tupã Studios. Para atingir este objetivo, o projeto abrange desde a definição da arquitetura física e lógica da rede, incluindo um plano de endereçamento *IP* detalhado, até a especificação do *hardware* para servidores e estações de trabalho de cada setor. Adicionalmente, é apresentado um plano de segurança formal, a implementação de dispositivos *IoT* para monitoramento e uma estratégia para o uso de serviços em nuvem, garantindo uma abordagem holística para a tecnologia da informação na empresa.

2 MERCADO DE JOGOS

O mercado de jogos eletrônicos é uma das indústrias de entretenimento que mais cresce no mundo, superando setores como cinema e música em faturamento. Em 2024, a receita global da indústria ultrapassou US$250 bilhões, com mais de 3 bilhões de jogadores em diversas plataformas, incluindo dispositivos móveis, consoles e PCs.

No Brasil, o setor também apresenta expansão significativa, movimentando cerca de R$5 bilhões em 2023, segundo a Abragames. Os jogos online, *multiplayer* e *free-to-play* se destacam, atraindo públicos variados e aumentando a presença nacional no mercado internacional.

Além do crescimento econômico, a indústria de games é marcada por avanços tecnológicos constantes, como realidade virtual, inteligência artificial aplicada a *gameplay* e análise de dados de jogadores para personalização da experiência. Tais tendências reforçam a importância de uma infraestrutura de *TI* robusta e segura, capaz de suportar operações internas, proteger a propriedade intelectual e oferecer escalabilidade em um mercado altamente competitivo.

3 INFORMAÇÕES SOBRE A EMPRESA

Tupã Studios é um estúdio brasileiro de desenvolvimento de jogos online multiplataforma (consoles e PC). A empresa possui um total de 210 funcionários distribuídos em três filiais, sendo a matriz localizada em São Paulo com 70 funcionários, e três unidades regionais situadas no Rio de Janeiro, Recife, cada uma com 40 funcionários e São Paulo II com 60 funcionários. A área de atuação da Tupã Studios está inserida no setor de tecnologia e entretenimento digital, especificamente no desenvolvimento e publicação de jogos eletrônicos. O objetivo da organização é criar experiências digitais divertidas e acessíveis, consolidando-se como referência no mercado nacional.

Dentro do estúdio existem diferentes setores de atuação, cada um com funções específicas e necessárias para o funcionamento pleno da empresa. O setor de desenvolvimento de jogos é formado por 80 funcionários e tem como responsabilidade principal a criação e implementação de novos jogos. Essa área abrange atividades como design de jogos, programação, arte e animação, áudio, gerenciamento de projetos e testes de qualidade. Para o desempenho dessas atividades, utilizam-se *softwares* como *Unreal Engine*, *Blender*, *Photoshop*, *FL Studio* e *Jira*. Esses *softwares* são fundamentais para implementação da lógica de jogo e prototipagem, criação visual, mixagem de áudio e gestão de tarefas, respectivamente.

O setor de marketing e vendas, formado por 25 colaboradores, tem como principal função promover os jogos da empresa e ampliar sua presença no mercado. Entre suas atividades estão a criação de campanhas publicitárias, a gestão de redes sociais e a definição de estratégias de distribuição em plataformas digitais, como *Steam* e consoles (Playstation e Xbox), além de lojas físicas. Para isso, utiliza ferramentas como *Adobe Illustrator* e *Adobe Premiere*, voltadas à produção de materiais visuais e audiovisuais, *Meta Business Suite*, para gerenciamento de mídias sociais, e *Google Analytics*, que auxilia na análise de resultados e no entendimento do comportamento do público.

O setor de inovação, formado por 15 colaboradores, é encarregado da pesquisa, desenvolvimento e aplicação de novas tecnologias, como inteligência

artificial, visando ao aprimoramento do produto e à melhoria da experiência do usuário. Para o desenvolvimento dessas atividades, utilizam-se ferramentas como *Python*, que auxilia na experimentação e criação de novos protótipos e sistemas de inteligência artificial.

A área de Administração e Recursos Humanos da Tupã Studios, composta por 30 funcionários, é responsável pela gestão financeira, contábil e de pessoas. Suas principais funções incluem o controle orçamentário, processos de recrutamento e seleção, além de programas de treinamento e desenvolvimento profissional. Para otimizar suas atividades, a equipe utiliza *softwares* como *SAP*, *Microsoft Excel* e *Trello*, visando garantir um ambiente de trabalho eficiente e produtivo.

O setor de limpeza e manutenção é composto por 20 colaboradores, sendo responsável pela higienização dos ambientes de trabalho e pela conservação predial, realizando reparos elétricos, hidráulicos e estruturais sempre que necessário. Para auxiliar no gerenciamento dessas atividades, são utilizados *softwares* de gestão predial, como o *Maximo Asset Management*.

O setor de atendimento ao cliente conta com 20 colaboradores e tem como objetivo responder dúvidas e solucionar problemas técnicos nesta área, são utilizados *softwares* de CRM como *Zendesk*, possibilitando maior proximidade com os usuários e um suporte mais ágil e eficaz.

O setor de segurança digital, composto por 10 colaboradores, é responsável pela aplicação de boas práticas e pelo gerenciamento da integridade de dados de usuários, funcionários, fornecedores e parceiros. Para apoiar essas atividades, são utilizados *Fortinet FortiGate*, *Bitdefender GravityZone*, *Wireshark* e *Splunk*, ferramentas que permitem monitoramento de rede, detecção de ameaças e implementação de políticas de proteção.

A área jurídica e de aspectos legais, conta com 10 colaboradores, atua no gerenciamento de direitos autorais, contratos e regulamentações específicas da indústria de jogos. A equipe utiliza *softwares* como *Microsoft Office* e *DocuSign*, que garantem a elaboração adequada e a assinatura segura de documentos e contratos.

Os produtos da Tupã Studios são os jogos eletrônicos multiplataforma, desenvolvidos para diferentes públicos e dispositivos. Entre as principais informações estratégicas gerenciadas pela empresa destacam-se o código-fonte dos jogos, os dados dos usuários e os contratos estabelecidos com parceiros. Já as

principais tarefas desempenhadas abrangem o desenvolvimento de novos títulos, a publicação e divulgação em diferentes canais, o suporte ao cliente e a pesquisa de novas tecnologias que garantam a competitividade da empresa em um mercado global altamente dinâmico.

3.1 Informações das unidades

A Tabela 3.1 a seguir detalha a distribuição dos setores e o respectivo número de funcionários por unidade da empresa.

Tabela 3.1 - Setores e funcionários por unidade

São Paulo - Matriz	**São Paulo II**	**Rio de Janeiro**	**Recife**
Dev - 40	Dev - 40	Administração - 15	Atendimento - 20
Marketing - 15	Inovação - 15	Jurídico - 10	Administração - 15
Limpeza/Manutenção - 5	Limpeza/Manutenção - 5	Limpeza/Manutenção - 5	Limpeza/Manutenção - 5
Segurança - 10	N/A	Marketing - 10	N/A
Total = 70	Total = 60	Total = 40	Total = 40

Fonte: Autores do projeto (2025)

Nota: Total de Funcionários = 210

4 PLANTAS BAIXAS

4.1 Sede São Paulo

Figura 4.1 - Planta baixa da Matriz em São Paulo

Fonte: Autores do projeto (2025)

4.1.1 Estrutura de Rede

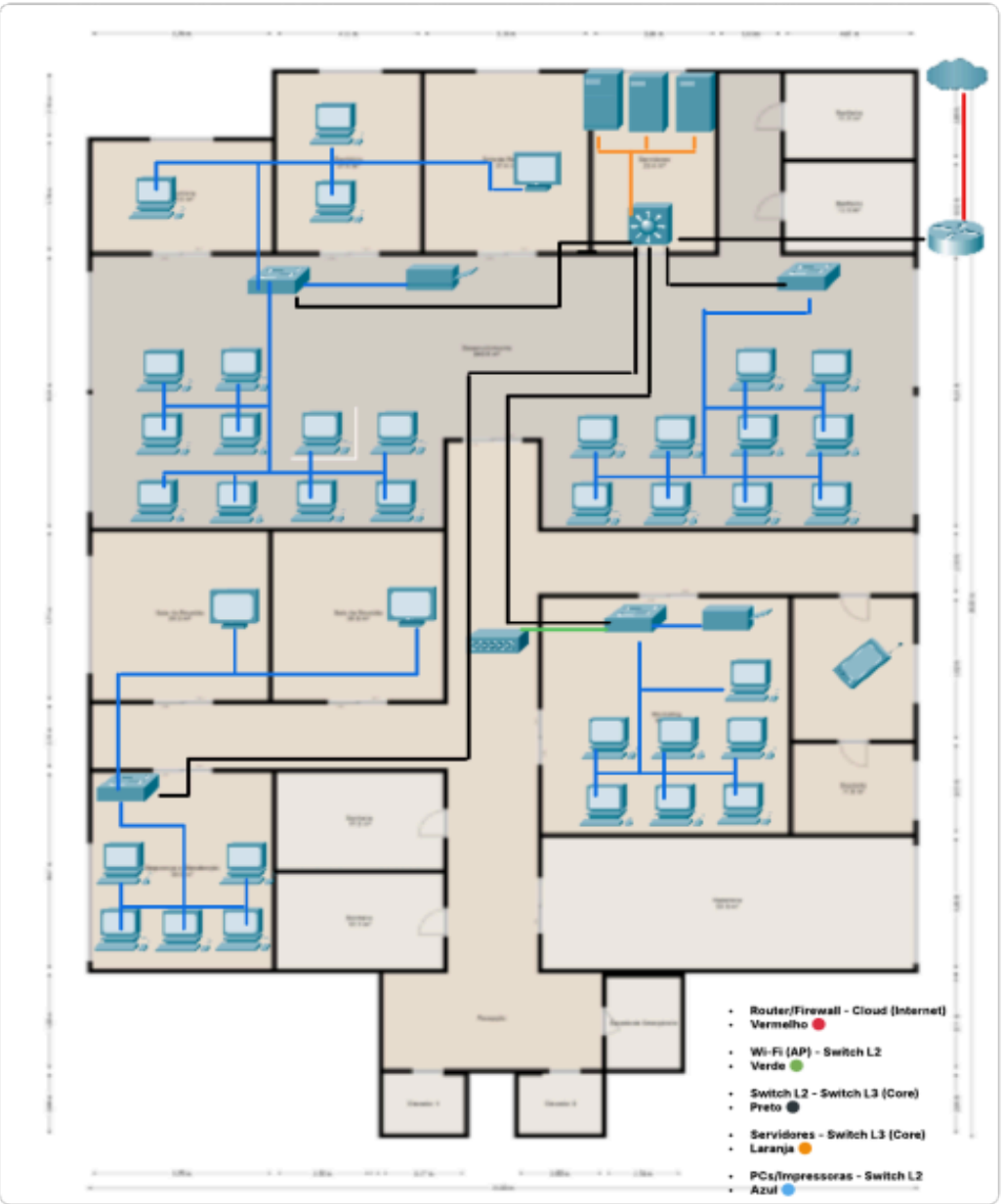

Figura 4.2 - Estrutura de Rede da Matriz em São Paulo

Fonte: Autores do projeto (2025)

4.2 Filial São Paulo

Figura 4.3 - Planta baixa da filial em São Paulo

Fonte: Autores do projeto (2025)

4.2.1 Estrutura de Rede

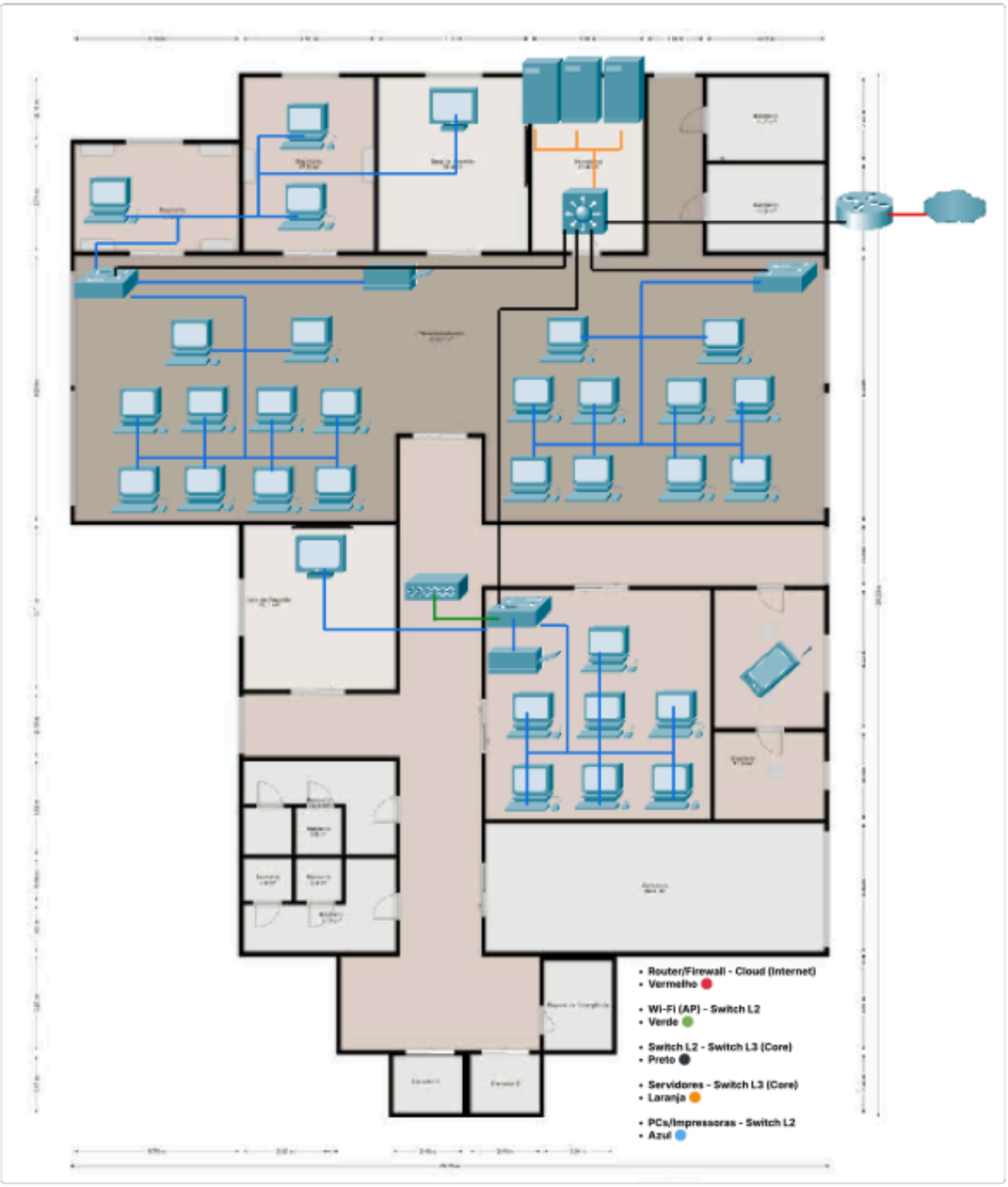

Figura 4.4 - Estrutura de Rede da filial em São Paulo

Fonte: Autores do projeto (2025)

4.3 Filial Rio de Janeiro

Figura 4.5 - Planta baixa da filial no Rio de Janeiro

Fonte: Autores do projeto (2025)

4.3.1 Estrutura de Rede

Figura 4.6 - Estrutura de Rede da filial no Rio de Janeiro

Fonte: Autores do projeto (2025)

4.4 Filial Recife

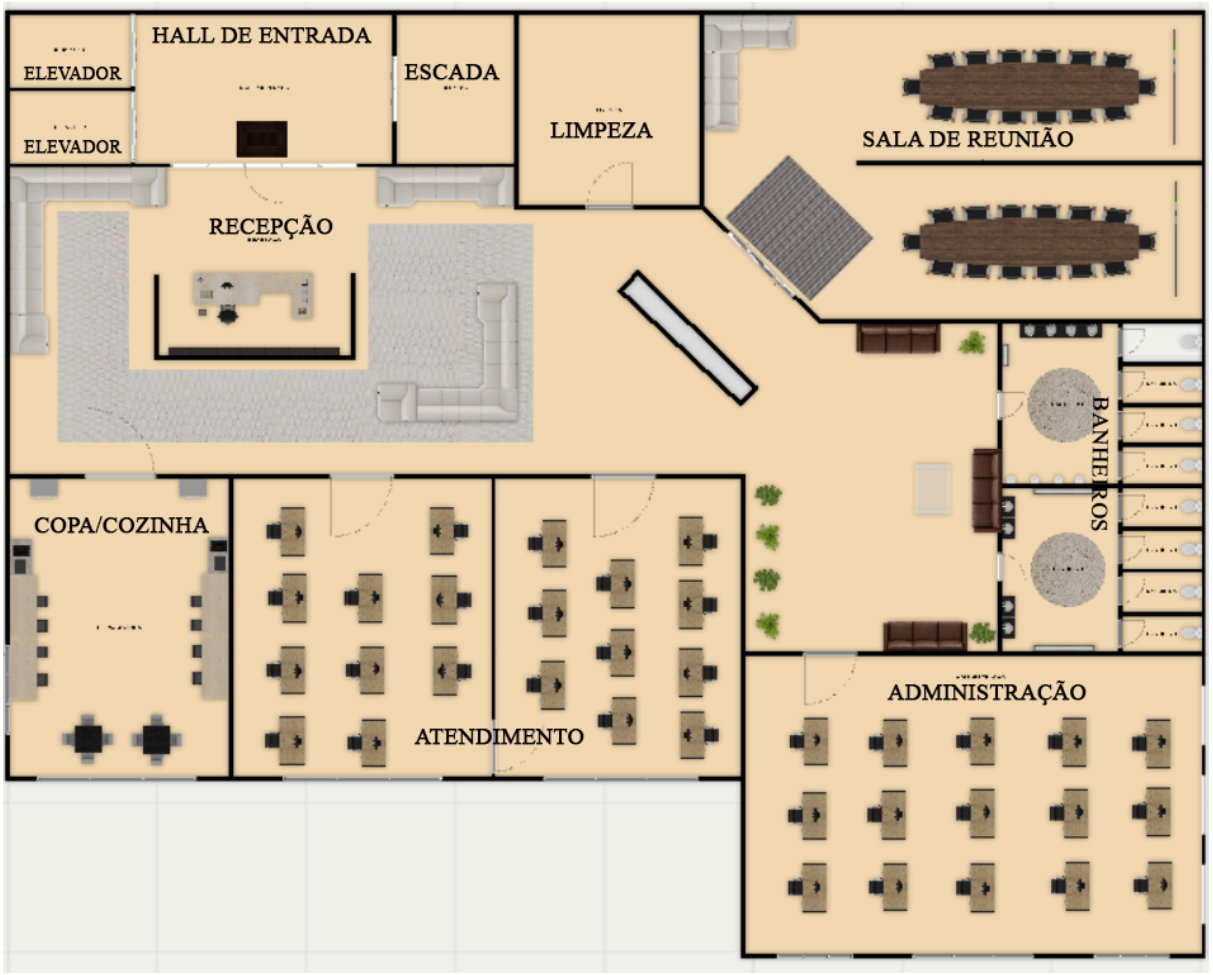

Figura 4.7 - Planta baixa da filial em Recife

Fonte: Autores do projeto (2025)

4.4.1 Estrutura de Rede

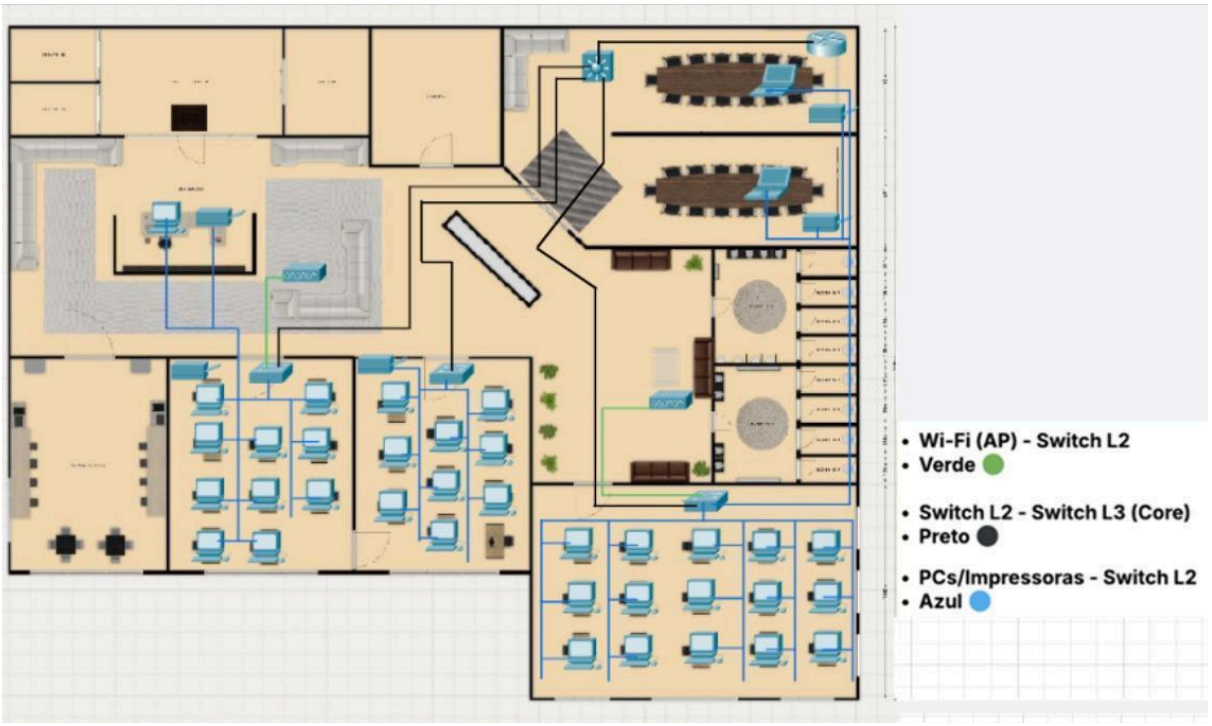

Figura 4.8 - Estrutura de Rede da filial em Recife

Fonte: Autores do projeto (2025)

5 EXPLICAÇÃO DA INFRAESTRUTURA DE REDES DA EMPRESA

A infraestrutura de redes da Tupã Studios foi projetada com base em um modelo de gerenciamento centralizado, visando máxima segurança, escalabilidade e resiliência. A arquitetura combina recursos locais com uma infraestrutura de nuvem dedicada, garantindo alta performance tanto para as operações corporativas quanto para os servidores de jogos. A Matriz em São Paulo funciona como o núcleo de toda a rede, com a filial de São Paulo II servindo como um *site* de redundância estratégica.

5.1 Arquitetura De Rede Local (*LAN*)

Para garantir um tráfego interno rápido e organizado, as unidades da empresa utilizam uma arquitetura hierárquica robusta, com componentes específicos para cada função.

Roteador de Borda *(Router/Firewall)*: Presente nas unidades de São Paulo, Rio de Janeiro e Recife, este equipamento funciona como um portão seguro para a rede. Ele integra um *firewall* que inspeciona todo o tráfego, protegendo os ativos internos contra ameaças e aplicando as políticas de segurança da empresa.

Camada de *Core (Switch L3)*: O coração da rede local é um *Switch Layer* 3. Ele atua como o *backbone* de alta velocidade, interconectando os servidores e os diferentes segmentos da rede (*VLANs*). Sua capacidade de roteamento interno alivia a carga do roteador de borda, otimizando drasticamente a performance e permitindo que a rede cresça sem gargalos.

Camada de Acesso *(Switch L2)*: Distribuídos pelos setores, os *Switches Layer 2* são responsáveis por conectar diretamente os dispositivos dos colaboradores, como computadores, impressoras e pontos de acesso *Wi-Fi*.

Conectividade Sem Fio (*Wi-Fi)*: Pontos de acesso (*APs*) são instalados para fornecer uma rede *Wi-Fi* corporativa segura, garantindo mobilidade e conectividade para dispositivos móveis, inclusive para equipes de manutenção e limpeza poderem abrir chamados de serviço.

5.2 Servidores e Gerenciamento Centralizado

O poder de processamento e gerenciamento é centralizado estrategicamente nas unidades de São Paulo para maior controle e segurança.

Matriz São Paulo (*Hub* Primário): Esta unidade abriga os servidores críticos que gerenciam toda a rede da empresa. A infraestrutura inclui um servidor de rede (para serviços como *DNS, DHCP e Active Directory*), um servidor de código-fonte (protegendo o principal ativo intelectual da Tupã) e um servidor de *backups* para os dados dos setores administrativo, jurídico e de RH.

Filial São Paulo II (*Hub* de Redundância): Atuando como um "*backup*" da Matriz, esta unidade garante a continuidade dos negócios. Seus servidores incluem um servidor de rede de contingência, um *backup* do código-fonte e um servidor de *build* de testes (*QA*) / Pesquisa e Desenvolvimento (*P&D*), fundamental para o processo de desenvolvimento e validação dos jogos e *updates*.

5.3 Conectividade entre Unidades (*WAN*) e Uso da Nuvem

A comunicação entre as filiais é feita de forma segura e centralizada, com um propósito bem definido para a nuvem.

Modelo *Hub-and-Spoke:* As filiais do Rio de Janeiro e Recife não possuem uma conexão direta com a internet. Elas se conectam como "*spokes*" à Matriz em São Paulo ("*hub*") através de túneis *VPN* seguros. Todo o tráfego dessas unidades é roteado para o *firewall* central da Matriz, garantindo que as mesmas políticas de segurança sejam aplicadas uniformemente em toda a organização.

Infraestrutura de Nuvem (*Cloud*): A utilização de serviços de nuvem **(*Google Cloud*)** é exclusivamente dedicada a hospedar os servidores de jogos *multiplayer*. Essa estratégia separa o tráfego massivo dos jogadores da rede corporativa interna, garantindo baixa latência para os usuários e protegendo as operações da empresa.

5.4 Plano de Endereçamento *IP* e Segmentação de Rede

O plano de endereçamento *IP* foi projetado para estabelecer uma arquitetura de rede que garanta segurança, organização e escalabilidade. A estratégia adotada, fundamentada em um esquema de endereçamento hierárquico e na segmentação

por meio de *VLANs (Virtual LANs*), visa suportar o crescimento contínuo e as operações distribuídas da empresa.

5.4.1 Estratégia de Endereçamento Global

Para toda a corporação, foi alocada a faixa de rede privada ***10.0.0.0/8***. A escolha por esta faixa se deve à sua vasta capacidade de endereços, que permite uma expansão futura sem a necessidade de reestruturar a rede.

A estrutura de endereçamento segue um padrão hierárquico e intuitivo: *10.[site].[vlan].[dispositivo].*

[site]: O segundo octeto identifica a localidade física (ex: 10 para a Matriz SP, 20 para a Filial SP II), permitindo que a equipe de TI identifique a origem de um dispositivo instantaneamente.

[vlan]: O terceiro octeto representa a rede virtual (*VLAN*) à qual o dispositivo pertence, agrupando-os por função ou setor (ex: 10 para Servidores, 20 para Desenvolvimento).

5.4.2 Segmentação com *VLANs* (Virtual *LANs*)

A rede de cada unidade é segmentada em *VLANs* para isolar o tráfego e aumentar a segurança. Os benefícios dessa abordagem são:

Segurança: Isola os ativos críticos. A *VLAN* de Servidores (*ID* 10) fica separada da *VLAN* Corporativa (*ID* 30) e completamente inacessível pela *VLAN* de *Wi-Fi* para Visitantes (*ID* 50). Isso impede que um incidente em uma área da rede se espalhe para as outras.

Performance: Reduz o tráfego de *broadcast* desnecessário na rede, melhorando a eficiência e a velocidade para todos os usuários.

Organização: Agrupa os dispositivos por função, facilitando a aplicação de políticas de acesso e a administração da rede. O roteamento entre as diferentes *VLANs* é controlado pelo *Switch Core* (*Layer 3*).

5.4.3 Atribuição de Endereços

A atribuição de *IPs* é gerenciada de forma híbrida:

Endereços Estáticos: Equipamentos de infraestrutura crítica como servidores, impressoras e os próprios dispositivos de rede (*switches*, roteadores) recebem *IPs* fixos. Isso garante que eles sejam sempre acessíveis no mesmo endereço.

Endereços Dinâmicos (*DHCP*): As estações de trabalho dos funcionários e os dispositivos móveis recebem seus endereços *IP* automaticamente do servidor de rede. Isso simplifica a gestão e a manutenção da rede, eliminando a necessidade de configurar cada máquina individualmente.

5.4.3.1 Endereçamento *IP* – Matriz São Paulo (*Hub* Primário)

O bloco de rede principal definido para a Matriz é o *10.10.0.0/16*. A partir dele, a rede foi segmentada por setores (*VLANs*), conforme detalhado na Tabela 5.1 a seguir.

Tabela 5.1 - *IPs* por setor na matriz

Nome da *VLAN*	*ID*	Rede (*Subnet*)	*Gateway*	Faixa de *IPs* (DHCP)	Observações
Servidores	10	10.10.10.0/24	10.10.10.1	N/A	*IPs* fixos e manuais.
Desenvolvimento	20	10.10.20.0/24	10.10.20.1	10.10.20.50 - .254	Rede para os desenvolvedores.
Corporativo	30	10.10.30.0/24	10.10.30.1	10.10.30.50 - .254	Para Marketing, ADM, RH e Jurídico.
Segurança	40	10.10.40.0/24	10.10.40.1	10.10.40.50 - .254	Rede isolada para a equipe do SOC.
Wi-Fi Visitantes	50	10.10.50.0/24	10.10.50.1	10.10.50.1 - .254	Acesso apenas à *internet*.
Gerenciamento	99	10.10.99.0/24	10.10.99.1	N/A	Acesso restrito para a equipe de *TI*.

Fonte: Autores do projeto (2025)

5.4.3.2 Endereçamento *IP* – Filial São Paulo II (*Hub* de Redundância)

Para o endereçamento *IP* da filial de São Paulo foi definida uma alocação do bloco de rede 10.20.0.0/16. A Tabela 5.2 demonstra a distribuição das redes e seus respectivos *gateways* para cada *VLAN*.

Tabela 5.2 - *IPs* por setor na Filial de São Paulo

Nome da *VLAN*	*ID*	Rede (*Subnet*)	*Gateway*	Faixa de *IPs* (*DHCP*)	Observações
Servidores	10	10.20.10.0 /24	10.20.10.1	N/A	*IPs* fixos para os servidores de redundância e *HPC*.
Desenvolvimento	20	10.20.20.0 /24	10.20.20.1	10.20.20.50 - .254	Rede para a equipe de desenvolvimento.
Inovação	25	10.20.25.0 /24	10.20.25.1	10.20.25.50 - .254	Rede separada para a equipe de *P&D*.
Wi-Fi Visitantes	50	10.20.50.0 /24	10.20.50.1	10.20.50.1 - .254	Acesso apenas à *internet*.
Gerenciamento	99	10.20.99.0 /24	10.20.99.1	N/A	Acesso restrito para a equipe de *TI*.

Fonte: Autores do projeto (2025)

5.4.3.3 Endereçamento *IP* – Filial Rio de Janeiro (*Spoke*)

A estrutura de rede da filial do Rio de Janeiro utiliza o bloco *10.30.0.0/16* para organizar os setores. A tabela 5.3 a seguir detalha as faixas de *IP, gateways* e sub-redes designadas para cada departamento.

Tabela 5.3 - *IPs* por setor na Filial do Rio de Janeiro

Nome da *VLAN*	ID	Rede (*Subnet*)	*Gateway*	Faixa de *IPs* (*DHCP*)	Observações
Corporativo	30	10.30.30.0 /24	10.30.30.1	10.30.30.50 - .254	Rede única para todos os funcionários (ADM, Jurídico, Marketing).
Wi-Fi Visitantes	50	10.30.50.0 /24	10.30.50.1	10.30.50.1 - .254	Acesso apenas à *internet*.
Gerenciamento	99	10.30.99.0 /24	10.30.99.1	N/A	Acesso restrito para a equipe de *TI*.

Fonte: Autores do projeto (2025)

5.4.3.4 Endereçamento *IP* – Filial Recife (*Spoke*)

O bloco de rede definido para a filial de Recife é o *10.40.0.0/16*. A partir dele, a alocação de endereços *IP* foi segmentada por setor, conforme detalhado na Tabela 5.4.

Tabela 5.4 - *IPs* por setor na Filial de Recife

Nome da *VLAN*	*ID*	Rede (*Subnet*)	*Gateway*	Faixa de *IPs* (*DHCP*)	Observações
Corporativo	30	10.40.30.0 /24	10.40.30.1	10.40.30.50 - .254	Rede para a equipe de Administração.
Atendimento	60	10.40.60.0 /24	10.40.60.1	10.40.60.50 - .254	Rede para a equipe de Atendimento ao Cliente.
Wi-Fi Visitantes	50	10.40.50.0 /24	10.40.50.1	10.40.50.1 - .254	Acesso apenas à *internet*.
Gerenciamento	99	10.40.99.0 /24	10.40.99.1	N/A	Acesso restrito para a equipe de *TI*.

Fonte: Autores do projeto (2025)

5.4.3.5 Endereçamento das *WANs*

Para realizar o endereçamento das conexões *WAN*, foi definido o bloco de sub-redes principal *10.254.0.0/24*. A Tabela 5.5 a seguir detalha como esses *IPs* foram distribuídos na conexão ponto-a-ponto por filial.

Tabela 5.5 - *IPs* por filial

Conexão	Sub-rede / 30	*IP* de um lado	IP do outro lado
Hub SP I <-> *Hub* SP II	*10.254.0.0 /30*	*10.254.0.1* (SP I)	*10.254.0.2* (SP II)
Hub SP I <-> *Spoke* RJ	*10.254.0.4 /30*	*10.254.0.5* (SP I)	*10.254.0.6* (RJ)
Hub SP I <-> *Spoke* Recife	*10.254.0.8 /30*	*10.254.0.9* (SP I)	*10.254.0.10* (Recife)
Hub SP II <-> *Spoke* RJ	*10.254.0.12 /30*	*10.254.0.13* (SP II)	*10.254.0.14* (RJ)
Hub SP II <-> *Spoke* Recife	*10.254.0.16 /30*	*10.254.0.17* (SP II)	*10.254.0.18* (Recife)

Fonte: Autores do projeto (2025)

6 DESCRITIVO DE *SOFTWARES* E SISTEMAS OPERACIONAIS

A Tupã Studios adota uma estratégia híbrida no uso de sistemas operacionais, buscando equilibrar desempenho, compatibilidade e custo-benefício. O *Windows* 10/11 *Pro* é utilizado em setores que dependem de *softwares* proprietários, como design gráfico, edição de áudio, atendimento, marketing e jurídico. Já o *Linux* (*Ubuntu*) é adotado em desenvolvimento, inovação, manutenção e segurança, por oferecer maior estabilidade, segurança e redução de custos de licenciamento. Nos servidores, a empresa utiliza exclusivamente o *Linux Server*, responsável por serviços de rede, repositórios de código, integração contínua, segurança digital e servidores de jogos. Essa padronização garante que cada setor opere em um ambiente adequado às suas demandas, preservando a eficiência operacional e a segurança da informação.

No setor de Desenvolvimento de Jogos, utilizam-se ferramentas como *Unreal Engine, Blender, Photoshop, FL Studio e Jira*. Enquanto o *Windows* é destinado às atividades de design e áudio, o *Ubuntu* é utilizado em programação e servidores de integração contínua.

O setor de Marketing e Vendas emprega *softwares* como *Adobe Illustrator, Adobe Premiere, Meta Business Suite* e *Google Analytics*. Por depender do pacote *Adobe*, opera exclusivamente em *Windows*.

No setor de Inovação, voltado para pesquisa e prototipagem, o *Python* é a principal ferramenta de cálculo e simulação, sendo executado em ambiente *Ubuntu*.

Em Administração e Recursos Humanos, os *softwares* utilizados são *SAP*, *Microsoft Excel* e *Trello*. Neste setor, todas as máquinas utilizam *Windows.*

O setor de Limpeza e Manutenção faz uso do *Maximo Asset Management*, acessado por meio do aplicativo em dispositivos móveis *Samsung Galaxy A05s*, garantindo mobilidade, praticidade e maior eficiência na gestão das atividades.

No Atendimento ao Cliente, o sistema *Zendesk* e *discord* são executados em ambiente *Windows*, garantindo praticidade e facilidade no suporte aos usuários.

No setor de Segurança Digital, ferramentas como *Fortinet FortiGate, Bitdefender GravityZone, Wireshark* e *Splunk* são utilizadas em servidores e estações baseadas em *Ubuntu*, assegurando monitoramento e proteção.

A área Jurídica e de aspectos legais utiliza o *Microsoft Office* e o *DocuSign*, que exigem ambiente *Windows* para garantir compatibilidade plena.

Por fim, a infraestrutura de Servidores é centralizada em *Linux Server*, que dá suporte ao *GitLab*, *Jenkins*, serviços de rede, segurança digital e servidores de jogos, permitindo maior escalabilidade e confiabilidade operacional.

Cada equipe possui requisitos específicos de software para desempenhar suas funções, desde ferramentas de desenvolvimento e design até sistemas administrativos. O Quadro 6.1 consolida essas necessidades, listando os sistemas operacionais e os principais softwares utilizados em cada área da organização.

Quadro 6.1 - *Softwares* por setor

	S.O	***Software Windows***	***Software Linux***
Desenvolvimento	*Windows* e *Linux*	*Photoshop* e *FL Studio*	*Unreal Engine, Blender* e *Jira*
Marketing e Vendas	*Windows*	*Adobe Illustrator, Adobe Premiere, Meta Business Suite* e *Google Analytic*	**N/A**
Inovação	*Linux*	**N/A**	*Python*
ADM e RH	*Windows*	*Windows Excel SAP* e *Trello*	**N/A**
Limpeza e Manutenção	*Android*	**N/A**	*Maximo Asset Management (APP)*
Atendimento ao Cliente	Windows	*Zendesk* e *Discord*	**N/A**
Segurança	*Linux*	**N/A**	*Fortinet FortiGate, Bitdefender GravityZone, Wireshark* e *Splunk*
Jurídico	*Windows*	*Microsoft Office* e *DocuSign*	**N/A**
Servidores	*Linux Server*	**N/A**	*GitLab, Jenkins*

Fonte: Autores do projeto (2025)

7 PLANO DE SEGURANÇA

O Plano de Segurança da Informação (PSI) é o documento norteador que estabelece as diretrizes, responsabilidades e procedimentos para proteger os ativos de informação da Tupã Studios. Esta seção detalha as políticas de boas práticas (7.2), o plano de contingência (7.3) e a gestão de riscos que compõem este plano.

7.1 Análise de vulnerabilidades

No setor de desenvolvimento um dos grandes problemas está associado ao armazenamento inadequado e à falta de segurança nos dados, podendo resultar em vazamentos de informações confidenciais e roubo intelectual. Mas se faz necessário ressaltar sobre as dependências em *Frameworks* e a ausência de testes e revisões nos códigos, fatores que aumentam o risco de falhas no jogo e a presença de *exploits*.

No Marketing e Vendas, a dependência de ferramentas em nuvem, como *Meta Business Suite* e *Google Analytics*, eleva a chance de ataques por meio de credenciais vazadas ou acessos não autorizados, podendo resultar em roubo de dados e comprometimento de contas oficiais. Além disso, o uso intenso de *Adobe Illustrator* e *Premiere* mantém as estações sujeitas a vulnerabilidades comuns em ambientes *Windows*.

No setor de Inovação, a utilização do *Python* em ambiente *Linux* exige atenção à compatibilidade e às atualizações de bibliotecas. Embora o *Linux* ofereça maior robustez, falhas em configuração podem comprometer resultados e expor o ambiente de testes.

Na Administração e Recursos Humanos, o uso do *SAP*, do *Trello* e do *Excel* envolve dados financeiros e de colaboradores, o que os torna alvos de grande valor. O principal risco está no uso de planilhas sem criptografia e no acesso remoto sem autenticação reforçada. Além disso, a falta de *backups* seguros e a ocorrência de falhas de *hardware* aumentam o risco de perda de históricos e dados críticos.

O setor de Limpeza e Manutenção, apesar de não lidar diretamente com dados estratégicos, pode ser alvo de ataques indiretos por engenharia social ou acessos a sistemas de gestão predial sem controles adequados de autenticação. A falta de treinamento em segurança da informação e a ausência de protocolos claros aumentam o risco de acesso não autorizado a áreas restritas.

No Atendimento ao Cliente, a utilização do *Zendesk* concentra dados sensíveis de usuários. A principal vulnerabilidade está no risco de vazamento de informações de clientes por falhas de autenticação ou por incidentes envolvendo credenciais expostas. Porém, a dependência de um *software* terceirizado faz com que o risco de paralisação no atendimento possa acontecer por ataques *DDoS* direto.

Na área de Segurança Digital, ainda que já existam ferramentas como *FortiGate*, *Splunk* e *Bitdefender*, a vulnerabilidade está na dependência de configuração adequada e na necessidade de monitoramento constante. Uma falha de ajuste pode comprometer toda a rede corporativa.

No setor Jurídico, o uso do *Microsoft Office* e do *DocuSign* envolve documentos legais e contratos, tornando-os alvos de ataques de *phishing* e adulteração de arquivos digitais. Além disso, a falta de revisão de cláusulas pode resultar em multas, sanções regulatórias e custos adicionais, prejudicando financeiramente e legalmente.

Não menos importante, a infraestrutura é essencial para o funcionamento da empresa. A exposição de *switches* e roteadores, junto à falta de *no-breaks* e geradores aumentam o risco de interrupções da rede, falhas de *hardwares* e perda de dados.

Por fim, nos Servidores, a padronização no uso de *Linux Server* traz vantagens em termos de segurança e custo, mas exige atenção redobrada em práticas de *hardening*, permissões de acesso e monitoramento de serviços críticos.

Para aprofundar a análise de risco, o quadro 7.1 identifica as possíveis vulnerabilidades específicas de cada setor. O detalhamento inclui a ameaça principal, a probabilidade, o impacto potencial e o nível de risco calculado.

Quadro 7.1 - Análise de vulnerabilidades por setor

Setor	Vulnerabilidade	Ameaça Principal	Probabilidade	Impacto Potencial	Nível	Nível de Risco
Desenvolvimento	Código-fonte exposto	*Phishing* / ataque interno	Média	Perda intelectual, atraso de projetos	Alta	Alto
	Vulnerabilidades de *Framework*	Ataque as vulnerabilidades conhecidas	Baixa	Falhas de jogabilidade e segurança	Média	Baixo
	Falta de controle de acesso em ambientes testes	Invasão e roubo de *scripts*	Média	Vazamento de atualizações	Média	Médio
	Falta de *code test / Review*	*Exploits* dentro do jogo	Média	Perda da reputação com a comunidade	Alta	Alto
Marketing	Senhas fracas e Falta de Verificação em dois fatores	Roubo de credenciais	Alta	Vazamento de informações dos produtos	Alta	Alto
	Materiais de campanhas sem criptografia	Interceptação e roubo de informações promocionais	Média	Perda de impacto e *hype* fora do momento	Média	Médio
	Falta de controle de acesso	Acesso indevido por ex funcionários	Média	Vazamentos de dados de *leads*	Alta	Alto

	Utilização de E-mails sem autenticação	*Phishing* usando o nome da empresa	Média	Golpes em jogadores e dano a credibilidade	Alta	Alto

(Continuação)

Setor	**Vulnerabilidade**	**Ameaça Principal**	**Probabilidade**	**Impacto Potencial**	**Nível**	**Nível de Risco**
Inovação	Exposição de ambientes de testes	Roubo de tecnologias e projetos	Média	Desvantagens competitivas	Alta	Alto
Administração	Planilhas sem criptografia	Vazamento por acesso remoto	Baixa	Infração da LGPD, prejuízo financeiro	Alta	Médio
	Falta de *backups* de documentos	Falhas de *Hardware*	Baixa	Perda de dados e históricos	Alta	Médio
	Falta de controle de acesso	Acesso indevido	Média	Fraudes e manipulação de registros	Alta	Alto
	Uso de softwares desatualizados	Exploração de brechas de segurança	Média	Corrupção de dados	Alta	Alto
Limpeza e Manutenção	Falta de treinamento	Engenharia Social	Baixa	Acesso físico não autorizado	Média	Baixo
	Descartes de documentos inadequados	Informação em lixo corporativo	Baixa	Vazamento de contratos	Média	Baixo
	Falta de monitoramento em salas de servidores	Uso de dispositivos maliciosos	Média	Espionagem	Alta	Alto

Atendimento ao Cliente	Ataques *DDoS*	Falha no atendimento	Baixa	Paralisação dos processos	Média	Baixo
	Falta de autenticação multifator em contas de suporte	Invasão de sistema de atendimento	Baixa	Acesso à informações dos jogadores	Alta	Médio

(Continuação)

Setor	**Vulnerabilidade**	**Ameaça Principal**	**Probabilidade**	**Impacto Potencial**	**Nível**	**Nível de Risco**
Segurança Digital	Má configuração de *firewall* / *SIEM*	Exploração remota	Média	Comprometimento da rede inteira	Alta	Alto
	Ausência de testes de penetração	Exploração de falhas não identificadas	Média	Invasão da rede	Alta	Alto
	Falta de proteção contra *cheats*	Exploração de falhas *anticheat*	Média	Perda de confiança da comunidade	Alta	Alto
Jurídico	Contratos digitais não verificados	*Phishing* e adulteração de *docs*	Média	Fraudes contratuais e processos	Alta	Alto
	Falta de revisão de cláusulas	Multas e processos	Baixa	Sanções financeiras	Alta	Médio
Infraestrutura	*Switch* exposto no corredor	Derramamento de líquidos	Baixa	Interrupção da rede	Média	Baixo
	Cabeamento sem organização	Curto circuito e perda de conexão	Baixa	Lentidão ou falta de internet	Média	Baixo
	Falta de equipamentos (*No*	Quedas de energia	Média	Paralisação de processos	Média	Médio

	breaks e geradores)					

Fonte: Autores do projeto (2025)

A análise de risco identificou o panorama geral de exposição da empresa. A Figura 7.1 ilustra a distribuição percentual consolidada do nível de risco. Na sequência, a Figura 7.2 detalha o mapeamento das vulnerabilidades e seus respectivos níveis por setor.

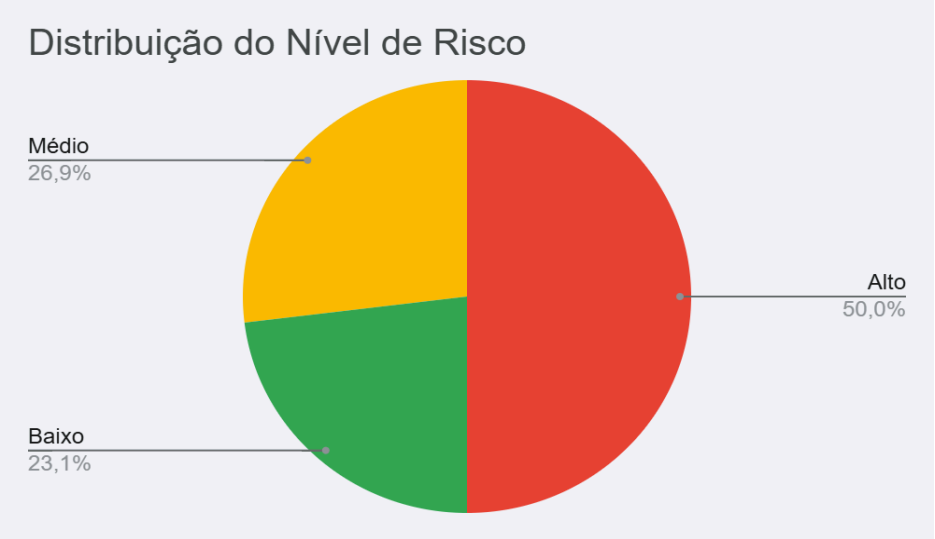

Figura 7.1 - Distribuição do nível de risco

Fonte: Autores do projeto (2025)

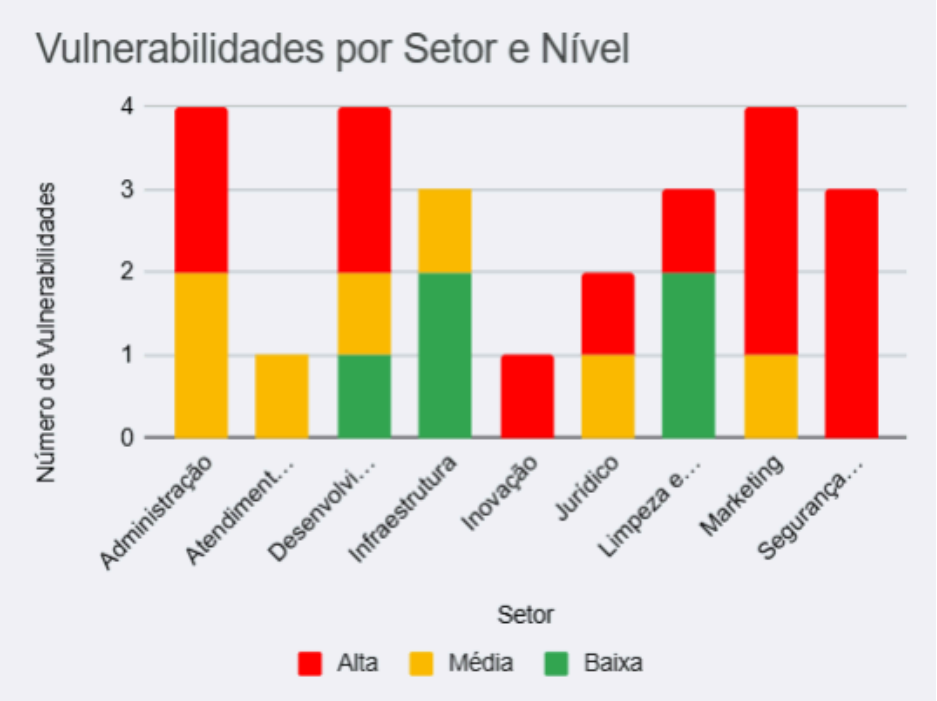

Figura 7.2 - Vulnerabilidades e níveis por setor

Fonte: Autores do projeto (2025)

7.2 Boas Práticas dos Funcionários

A segurança da informação é uma responsabilidade compartilhada por todos os colaboradores. Esta seção define as boas práticas mandatórias que visam reduzir os riscos de origem humana, protegendo as credenciais de acesso, os dispositivos e o ambiente de trabalho.

7.2.1 Senhas e Autenticação(2FA)

a) Todos os colaboradores devem utilizar senhas fortes e exclusivas para acesso a sistemas corporativos, com mínimo de 10 caracteres, incluindo letras maiúsculas, números e caracteres especiais.

b) É obrigatório ativar a autenticação multifator (MFA) em todos os sistemas e plataformas corporativas.

c) Está terminantemente proibido o compartilhamento de credenciais entre funcionários ou pessoas externas à organização.

7.2.2 Uso de Dispositivos e Computadores

a) Os dispositivos corporativos devem ser bloqueados imediatamente quando o usuário se afastar de sua estação de trabalho, utilizando os comandos apropriados:

- ***Windows***: *Windows* + L

- ***Linux***: Ctrl + Alt + L

b) É terminantemente proibido realizar atividades de ordem pessoal nos computadores e sistemas da organização.

c) O uso de *softwares* e aplicativos não autorizados é estritamente proibido.

d) O uso de dispositivos externos, como pen-drives, é proibido dentro da organização.

7.2.3 Proteção de Dados e Informações

a) Todas as informações corporativas, incluindo dados de clientes, projetos, código-fonte e documentos financeiros, devem ser armazenados de forma segura e criptografada, conforme as diretrizes da organização.

b) É proibido o envio de documentos ou informações sensíveis por canais inseguros (e-mail pessoal e serviços não autorizados).

c) O descarte de documentos físicos e mídias digitais deve seguir as normas de destruição segura da organização.

7.2.4 Redes e Conectividade

a) O uso de redes corporativas deve ser restrito a atividades profissionais, evitando conexões inseguras ou públicas e de ordem pessoal.

b) É proibido conectar dispositivos externos à rede sem autorização prévia da equipe de Segurança Digital (SOC).

c) Qualquer incidente ou suspeita de ataque cibernético deve ser imediatamente reportado à equipe responsável.

7.2.5 *Backups* e Continuidade

a) Todos os dados críticos devem ser incluídos em rotinas de *backup* seguro

b) Manter *backups* redundantes em nuvem e em unidades distintas

c) Realizar testes periódicos de restauração de dados.

d) Utilizar servidores espelhados para garantir alta disponibilidade.

7.2.6 Responsabilidades

a) Todos os colaboradores são responsáveis por cumprir as políticas e diretrizes, garantindo a segurança das informações e sistemas da organização.

b) Violações às políticas podem resultar em medidas disciplinares, incluindo advertências, suspensão ou até rescisão de contrato, além de responsabilidades legais quando aplicável.

7.2.7 Conscientização em Segurança Digital

a) Treinamento Contínuo: Participar ativamente dos treinamentos periódicos obrigatórios sobre engenharia social e *phishing* promovidos pela empresa.

b) Análise de E-mails: Sempre verificar a autenticidade dos remetentes antes de responder a solicitações, especialmente aquelas que envolvem dados sensíveis ou transações financeiras.

c) Cuidado com *Links* e Anexos: Evitar clicar em *links* ou baixar anexos de e-mails suspeitos ou não solicitados. Na dúvida, encaminhe a mensagem para a equipe de Segurança Digital (SOC) para análise.

d) Reporte Imediato: Qualquer e-mail ou comunicação suspeita deve ser imediatamente reportada, mesmo que pareça inofensiva.

7.2.8 Proteção de Dados e Informações

a) Armazenamento seguro: Arquivos de trabalho, especialmente dados críticos como código-fonte e informações de clientes, devem ser armazenados exclusivamente nos locais autorizados (*GitLab*, *SharePoint*, servidor interno). É proibido salvar documentos críticos no *desktop* ou em dispositivos pessoais.

b) Princípio do Menor Privilégio: Cada colaborador deve acessar apenas os dados e sistemas estritamente necessários para a execução de suas funções.

d) Envio Seguro de Dados: O uso de criptografia é mandatório para o envio de dados sensíveis. É proibido o envio de informações corporativas por canais inseguros, como e-mail pessoal ou serviços de mensagem não autorizados.

c) Descarte Consciente: Documentos físicos e mídias digitais que contêm informações sensíveis devem seguir as normas de destruição segura da organização.

7.2.9 Boas Práticas em Redes Sociais e Comunicação

a) Separação de Contas: Mantenha perfis pessoais e corporativos estritamente separados para evitar a associação indevida de opiniões pessoais à marca.

b) Confidencialidade: Nunca divulgue informações internas, confidenciais ou sobre projetos em andamento em redes sociais ou fóruns públicos.

c) Verificação de Fontes: Antes de compartilhar qualquer conteúdo nos perfis institucionais da empresa, confirme a veracidade e a credibilidade da fonte.

d) Acesso Seguro: Utilize as contas corporativas apenas em dispositivos autorizados e gerenciados pela empresa para evitar o roubo de credenciais.

7.2.10 Gestão Física e Ambiental.

a) Controle de Acesso: Não permita a entrada de pessoas não autorizadas em áreas restritas, como salas de servidores e *racks* de rede. Mantenha o crachá sempre visível e nunca o empreste a terceiros.

b) Prevenção de Acidentes: Relate imediatamente à equipe de manutenção qualquer incidente como derramamento de líquidos, falhas elétricas ou sobreaquecimento de equipamentos para prevenir danos e interrupções.

7.2.11 Responsabilidade no Trabalho Remoto

a) Conexão Segura: Conecte-se sempre à rede da empresa utilizando a *VPN* corporativa para garantir que a comunicação seja criptografada e segura.

b) Equipamentos Autorizados: Utilize apenas os equipamentos fornecidos e autorizados pela Tupã Studios para acessar os sistemas e dados corporativos.

c) Ambiente Controlado: Evite compartilhar o computador de trabalho com familiares ou terceiros para prevenir acessos indevidos e infecções por *malware*.

7.2.12 Cultura de Segurança

a) Vigilância e Reporte: Reporte imediatamente qualquer atividade suspeita, por menor que pareça, à equipe de Segurança Digital.

b) Colaboração Ativa: Colabore com as auditorias internas de segurança e participe ativamente das simulações de incidentes e testes de resposta.

c) Integridade dos Dados: Respeite e siga as políticas de *backup* e versionamento de código para garantir a integridade e a recuperabilidade dos nossos projetos.

7.3 Plano de Contingência

O Plano de Contingência define ações imediatas e responsáveis para situações críticas que possam comprometer a operação, segurança e integridade dos dados da Tupã Studios.

7.3.1 Objetivo

Garantir que todos os incidentes críticos, como falhas de sistemas, invasões, vazamentos de dados ou indisponibilidade de serviços, sejam tratados de forma organizada, minimizando impactos operacionais, legais e financeiros.

7.3.2 Procedimentos de Contingência por Tipo de Incidente

Esta seção descreve as ações de resposta específicas que devem ser tomadas para cada tipo de incidente. O cumprimento destes procedimentos é mandatório para mitigar os impactos.

7.3.2.1 Comprometimento de credenciais

a) Bloqueio imediato da conta afetada.
b) Redefinição de senha e ativação obrigatória de MFA.
c) Auditoria dos acessos anteriores.

d) Comunicação ao setor de Segurança Digital e aos gestores.

7.3.2.2 Vazamento ou perda de dados

a) Isolamento imediato do sistema ou servidor afetado.
b) Acionamento do *backup* mais recente.
c) Investigação da origem do incidente pelo SOC.
d) Comunicação transparente aos clientes e parceiros afetados.
e) Revisão e reforço das políticas de proteção de dados.

7.3.2.3 Falha de *hardware* ou interrupção de serviços

a) Acionamento de servidores espelhados e *backup* redundante.
b) Redirecionamento de operações críticas para sistemas secundários.
c) Substituição ou reparo imediato do equipamento afetado.
d) Registro detalhado do incidente, tempo de resposta e ações corretivas.

7.3.2.4 Invasão ou ataque à rede

a) Isolamento do segmento comprometido.
b) Bloqueio de *IPs* suspeitos.
c) Análise forense detalhada do ataque.
d) Aplicação de patches e correções de vulnerabilidade.
e) Testes de restauração e monitoramento contínuo pós-incidente.

7.3.2.5 Incidente físico ou ambiental

a) Acionamento imediato da equipe de segurança predial.
b) Bloqueio do acesso a áreas críticas.
c) Avaliação de danos e continuidade da operação por rotas alternativas.
d) Revisão das permissões de acesso e reforço de controles.

7.3.3 Responsáveis

SOC: Monitoramento, investigação e coordenação das ações digitais.

***TI* / Infraestrutura**: Restauração de sistemas, manutenção de equipamentos e suporte técnico.

RH / Administração: Comunicação interna e controle de acesso a pessoas.

Jurídico: Orientação sobre impacto legal e comunicação externa.

8 SERVIÇOS DE NUVEM NECESSÁRIOS

A Tupã Studios pretende oferecer servidores *online*, com esse objetivo, precisa de uma infraestrutura em nuvem que seja capaz de suportar baixa latência, escalabilidade em tempo real e segurança. Para isso, os serviços essenciais incluem máquinas virtuais para hospedar os servidores de jogo, bancos de dados de alta performance para gerenciar contas, *rankings* e inventários, além de serviços de rede que garantam distribuição de tráfego e proteção contra ataques (*DDoS* por exemplo).

Outro ponto importante é a análise de dados dos jogadores, utilizada para equilibrar partidas, identificar fraudes e melhorar a experiência de jogo. Serviços de armazenamento escalável também são fundamentais, pois permitem lidar com atualizações constantes, *patches* e conteúdo adicional.

a) **Computação (Máquinas Virtuais):**

Para hospedar os servidores do jogo (*lobby*, *matchmaking*, salas de jogo, *APIs* de *backend*);

b) Banco de Dados Gerenciado:

Para armazenar contas de jogadores, *rankings*, progressão e inventários;

c) Armazenamento Escalável:

Para atualizações do jogo, arquivos de mídia, *patches*, conteúdo adicional;

d) Rede e Balanceamento de Carga:

Distribuir conexões entre múltiplos servidores, garantindo que nenhum fique sobrecarregado;

e) Segurança e Autenticação:

Controle de acessos e proteção contra ataques comuns em jogos (ex.: *DDoS*);

f) Monitoramento e Logs:

Para acompanhar o desempenho dos servidores e detectar falhas ou trapaças;

g) Entrega de Conteúdo (CDN):

Acelerar *downloads* de patches, *DLCs* e conteúdos para jogadores em diferentes regiões;

h) Ferramentas de Desenvolvimento e Integração Contínua (CI/CD):

Automatizar atualizações e testes de servidores/jogos.

9 COMPARAÇÃO DE SERVIÇOS DE NUVEM

Tanto a *Amazon Web Services* (*AWS*) quanto o *Google Cloud Platform* (*GCP*) oferecem soluções robustas, mas apresentam pontos fortes distintos que atendem a diferentes perfis de empresas e necessidades operacionais. Essa diferenciação se manifesta não apenas na variedade de serviços disponibilizados, mas também no modelo de precificação, na maturidade das soluções e no foco tecnológico de cada provedor. Dessa forma, ao analisar a adoção de uma plataforma de nuvem para suportar servidores *online*, torna-se relevante compreender de forma detalhada as particularidades de cada ambiente. A seguir, apresenta-se uma comparação detalhada dos principais serviços utilizados na infraestrutura da Tupã Studios,

considerando tanto a *Amazon Web Services* (AWS) quanto o *Google Cloud Platform* (GCP), ambas na região São Paulo (*southamerica-east1*)

A **AWS** é a nuvem mais consolidada do mercado, com uma ampla gama de serviços voltados para diferentes necessidades. No setor de jogos, destaca-se pelo *Amazon GameLift*, um serviço dedicado à hospedagem e gerenciamento automático de servidores *multiplayer*, que facilita o escalonamento conforme a quantidade de jogadores aumenta ou diminui. Além disso, a AWS possui uma rede global extremamente abrangente, o que ajuda a reduzir a latência ao aproximar os servidores dos usuários finais. Por outro lado, a complexidade de gerenciamento e o modelo de preços, que pode se tornar difícil de prever, são fatores que exigem atenção.

No entanto, o ***Google Cloud***, apesar de ter um portfólio de serviços um pouco mais enxuto, se destaca em áreas ligadas a *big data*, inteligência artificial e *machine learning*, o que pode ser muito vantajoso para jogos que utilizam personalização, análise comportamental e sistemas avançados de *matchmaking*. Outro diferencial do *GCP* é sua rede global de altíssima performance, a mesma usada em serviços como *YouTube* e *Gmail*, que garante baixa latência em diferentes regiões do mundo. A plataforma também oferece um modelo de custos mais simples e competitivo, com descontos automáticos de uso contínuo, o que pode ser atrativo para estúdios menores ou que buscam previsibilidade financeira. Por outro lado, o GCP ainda não possui um serviço tão especializado para jogos quanto o *GameLift* da AWS, exigindo maior customização por parte da equipe de desenvolvimento.

9.1 Preços AWS

Para a estimativa de custos, foi utilizado o *AWS Pricing Calculator* (https://calculator.aws/). As configurações foram baseadas em uma estimativa de 100.000 jogadores ativos, utilizando a região América do Sul (São Paulo). Os preços detalhados para cada serviço são apresentados a seguir.

9.1.1 Computação (Máquinas Virtuais)

Amazon EC2 (*Elastic Compute Cloud*) para rodar os servidores do jogo. É um serviço da AWS que permite criar e gerenciar instâncias de servidores na nuvem.

São apresentadas diferentes opções de pagamento para a instância **c3** (*computer optimized, Linux*).

a) 32 *vCPUs* e 20 GiB *RAM*: US$ 2,86/h
Custo total: US$ 4.730,40/mês

9.1.2 Banco de Dados Gerenciado

DynamoDB para armazenar contas, *rankings* e progresso do jogo. O *Amazon DynamoDB* é um banco de dados de documentos e chave-valor que oferece desempenho inferior a 10 milissegundos em qualquer escala. É um banco de dados gerenciado, multirregional, multimestre e durável com segurança incorporada, *backup* e restauração, além de armazenamento em cache na memória para aplicativos na escala da Internet.

a) Custo mensal de gravação: US$35,15/mês
b) Custo mensal de leitura: US$4,17/mês
c) Custo das instâncias *DAX* do *DynamoDB*: US$1,116.90/mês
d) Custo da gravação adiantada (Pagamento adiantado):US$ 225,00
e) Custo de leitura adiantada (Pagamento adiantado): US$45,00
Custo total: US$1,156.22/mês

9.1.3 Armazenamento

Amazon Simple Storage Service para *patches*, arquivos e mídias. O *Amazon Simple Storage Service* (*Amazon S3*) é um armazenamento para a *Internet*. Você pode usar o *Amazon S3* para armazenar e recuperar qualquer volume de dados, a qualquer momento, de qualquer lugar na *Web*. Essa classe é utilizada para armazenar *builds* e *patches* ativos do jogo, arquivos de mídia que precisam ser baixados rapidamente pelos jogadores e conteúdos que são acessados constantemente pelo *launcher* ou cliente.

a) S3 *Standard*: US$23,75/mês

Custo mensal total = US$23,75/mês

9.1.4 Balanceamento de Carga

***Elastic Load Balancer* (*ELB*)** voltado para distribuir conexões entre os servidores. O *Elastic Load Balancing* distribui automaticamente o tráfego de entrada do aplicativo em vários destinos, como instâncias do *Amazon EC2*, contêineres, endereços IP e funções do *Lambda*.

a) *Application Load Balancer*: US$ 24,82/mês
b) Balanceamento de Carga (NLB): US$ 1.650,00/mês
c) Servidores de Jogo (EC2): US$ 3.500,00/mês
d) Transferência de Dados (Out): US$ 19.500,00/mês
e) Uso de LCU para o *Application Load Balancer*: US$1.606/mês
Custo total = US$ 26.280,82/mês

9.1.5 Segurança

AWS Shield voltado para a parte de segurança e autenticação. O *AWS Shield* Avançado é um serviço pago que oferece proteções adicionais para aplicativos voltados para a Internet executados no *Amazon Elastic Compute Cloud* (*EC2*), *Elastic Load Balancing* (*ELB*), *Amazon CloudFront*, *AWS Global Accelerator* e *Amazon Route 53.*

a) Cloudfront: US$128/mês
b) Elastic Load Balancing (ELB): US$184,32/mês
c) Elastic IP: US$5,12/mês
d) Global Accelerator: US$25,60/mês
e) Shield Avançado: US$3.000,00/mês
Custo total = US$3.343,04/mês

9.1.6 Monitoramento e Logs

Amazon CloudWatch para acompanhar desempenho e checar falhas/trapaças. O *Amazon CloudWatch* é um serviço de gerenciamento e monitoramento que fornece dados e *insights* acionáveis para recursos de infraestrutura e aplicações da *AWS*, híbridos e locais.

a) Métricas

- 1.500 – 5.000 / Métricas mês
- US$ 0,30 / por métrica
- Total mensal: US$ 450 - 1.500 / Mês
- Total médio mensal: US$ 975 / Mês

b) Logs

- 1 - 5 TB logs/mês
- *CloudWatc*h (Ingestão de *logs*): US$ 0,90/GB (padrão) + US$ 0,45 (acesso infrequente)
- Total mensal: US$ 1.350 - 6.750 / Mês
- Total médio mensal: US$ 4.050 / Mês

c) Alarmes

- 50 - 100 alarme (1 métrica cada)
- Alta resolução: US$ 0,405 / métrica de alarme / Mês
- Total mensal: U$20,25 - US$40,50 / Mês
- Total médio mensal: US$ 30,375 / Mês
- Total Mensal: US$ 5.055,375

9.1.7 Entrega de Conteúdo (CDN)

Amazon CloudFront para *downloads* rápidos de *patches*.

O *Amazon CloudFront* é o serviço de *Content Delivery Network* (*CDN*) da *AWS*. Ele é utilizado para distribuir conteúdos do jogo (como atualizações, patches, *DLCs* e mídias) com baixa latência e alta velocidade, garantindo que os jogadores em diferentes regiões tenham o mesmo desempenho de *download*. O *CloudFront* funciona em conjunto com o *Amazon S3*, armazenando cópias temporárias (cache) dos arquivos em servidores de borda distribuídos globalmente. Assim, quando um jogador baixa um *patch* ou conteúdo adicional, o arquivo é entregue pelo servidor mais próximo geograficamente, reduzindo o tempo de espera e a carga sobre os servidores principais.

a) Transferência de Dados - Primeiros 10 TB/mês: 10.000 GB x 0,085: US$850,00

b) Solicitações HTTPS (GET/PUT): 50 milhões x US$0,000001 : US$50,00

Custo Total = US$900,00/mês

9.1.8 CI/CD e Ferramenta de Desenvolvimento

Atualização de *deploys* e testes são vitais para lançar atualizações, novos recursos e correções de *bugs* rapidamente e com segurança. Para isso podem ser utilizados o *AWS CodePipeline*, *AWS CodeBuild*, *AWS CodeDeploy* e *AWS CodeCommit*.

O *AWS CodePipeline* é um serviço gerenciado de entrega contínua que ajuda a automatizar *pipelines* de liberação para oferecer atualizações rápidas e confiáveis de aplicativos e infraestruturas.

a) 12 *pipelines* ativos → 1 gratuito, restam 11 pagos

b) US$ 1,00 = US$ 11,00

c) 2.360 minutos executados → 100 gratuitos, restam 2.260 faturáveis.

d) 2.260 × US$ 0,002 = US$ 4,52

Total mensal = US$ 11,00 + US$ 4,52 = US$ 15,52/mês

O *AWS CodeBuild* é um serviço de integração contínua totalmente gerenciado que compila o código-fonte, executa testes e produz pacotes de *software* prontos para implantação.

e) 100 compilações por mês x 10 minutos : 1.000,00 minutos cobrados (mensal)
f) 1.000,00 minutos x US$0,12: US$120,00
Custo total = US$120,00/mês

O *AWS CodeDeploy* é um serviço de implantação totalmente gerenciado que automatiza implantações de *software* para vários serviços de computação, como *Amazon EC2*, *AWS Fargate*, *AWS Lambda* e seus servidores *on-premises*.

g) 20 instâncias
h) 300 implantações
i) 2 x 300 x US$0,02: US$120,00
Custo total = US$120,00/mês

O *AWS CodeCommit* é um serviço seguro, altamente escalável e totalmente gerenciado para controle de fontes que hospeda repositórios *Git* privados.

j) Número de usuários ativos: 80
- Qualquer usuário ativo recebe:
- 1.000 repositórios por conta; até 25.000 mediante solicitação.
- 50 GB armazenamento/mês
- 10.000 solicitações Git/mês
Custo mensal total: US$75.00/mês

9.2 Tabela Preços AWS

A Tabela 9.1 consolida os custos mensais de todos os serviços de nuvem detalhados anteriormente.

Tabela 9.1 - Preços para cada serviço AWS

Serviço de Cloud	Preço
Computação	US$ 4.730,40
Banco de Dados	US$ 1.156,22

Armazenamento	US$ 23,75
Rede e Balanceamento de carga	US$ 26.280,82
Segurança e Autenticação	US$ 3.343,04
Monitoramento de Logs	US$ 5.055,375
Entrega de Conteúdo	US$ 900,00
CI/CD	US$ 330,52

Fonte: Autores do projeto (2025)

Nota: Total mensal US$ 41.820,125

9.3 Preços GCP

Para a estimativa de custos dos serviços *Google Cloud Platform* (GCP), foi utilizada a ferramenta oficial *GCP Pricing Calculator*, disponível em: https://cloud.google.com/products/pricing-calculator. As configurações foram baseadas em uma estimativa de 100.000 jogadores ativos, utilizando a região América do Sul (São Paulo) (*southamerica-east1*)

Os planos escolhidos foram pensados para que haja o menor custo final total. Sendo assim, a maior assinatura disponível pelo GCP é a de 3 anos.

9.3.1 Máquinas virtuais

São a base da hospedagem dos servidores de jogo, responsáveis por rodar o *lobby*, *matchmaking*, salas de jogo e *APIs* de *backend*:

a) vCPUs - 8

b) Memória - 32 GB

Total mensal - US$ 2.115,99/ Mês

9.3.2 Banco de Dados Gerenciado

Essencial para armazenar contas de jogadores, *rankings*, progressão e inventários o ***Cloud SQL*** fornece bancos prontos para uso, com *backup* automático e a opção de alta disponibilidade, garantindo consistência e resiliência.

a) vCPUs HA - US$ 43,41456 / Mês (* 12)

b) Memória HA - US$ 36,792 / 5 *gibibyte* Mês (* 32)

Total mensal - US$ 1.698,31872 / Mês

9.3.3 Armazenamento

O **armazenamento escalável** é um componente fundamental para a operação de jogos online, permitindo que a Tupã Studios gerencie atualizações do jogo, *patches*, arquivos de mídia e conteúdos adicionais de forma eficiente. Armazenamento Padrão - US$ 0,035 / GB Mês (* 1.500)

a) *Nearline Storage* - US$ 0,020 / GB Mês (* 500)

b) *Coldline Storage* - US$ 0,007 / GB Mês (* 50)

Total Mensal - US$ 62,55 / Mês

9.3.4 Balanceamento de Carga

A **Rede e Balanceamento de Carga** são cruciais para garantir uma experiência de jogo *online* fluida e sem interrupções. Eles permitem que o tráfego seja distribuído de forma inteligente entre os servidores, prevenindo sobrecargas e mantendo a baixa latência, essencial para a jogabilidade em tempo real. Cálculos considerando jogabilidade de 8h/dia:

a) Regras de encaminhamento - US$ 18,25 / Mês (primeiras 5 regras)

b) Tratamento de dados de entrada - US$ 0,012 / 1 gibibyte (* 150.000)

c) Tratamento de dados de saída + *Network Egress* - (US$ 0,012 + US$ 0,085) = US$ 0,097 / 1 gibibyte (* 150.000)

Total Mensal - US$ 16.368,25 /Mês

9.3.5 Segurança

A **Segurança e Autenticação** são a primeira linha de defesa da Tupã Studios, protegendo tanto a infraestrutura quanto os jogadores de ameaças cibernéticas. O uso de serviços gerenciados garante que a validação de identidade

seja rápida e robusta, prevenindo acessos não autorizados e ataques de negação de serviço (*DDoS*).

a) Usuários Ativos Mensais - US$ 0,0 / 0 a 49.999 *MAU*

b) Usuários Ativos Mensais - US$ 0,0055 / 50.000 a 99.999 *MAU* (* 50.000)

c) Usuários Ativos Mensais - US$ 0,0046 / 100.000 a 999.999 MAU (* 1)

d) SMS de *MFA* - US$ 0,02 (* 7.500)

e) *Google Cloud Armor Standard* - US$ 0,75 / por Milhão de solicitações (* 1.000)

Total Mensal - US$ 1.175,00 / Mês

9.3.6 Monitoramento e Logs

Os serviços de **Monitoramento e Logs** são essenciais para a Tupã Studio ao manter a qualidade, a estabilidade e a justiça nos servidores de jogos *online*, impedindo que trapaças e falhas ocorram, ou seja, elementos vitais para a satisfação e retenção da comunidade.

a) *Cloud Logging*

- Armazenamento de *logs*
  - US$ 0,50/gigabyte - 50 GiB (grátis)
- Retenção de registros
  - US$ 0,01/gigabyte
- Total = US$ 9,00 /Mês

b) *Cloud Monitoring*

- Dados exclusivos do *Google Prometheus*
  - US$ 0,060/milhão amostra + US$ 0,048 /milhão de amostra (média de 5 bilhão de amostra por mês)
- Total = US$ 540,00 /Mês

c) *Cloud Tracer*

- Rastreamento de requisições
  - US$ 0,20/milhão de períodos
- Total = US$ 259,50

Total = US$ 808,50/Mês

9.3.7 Entrega de Conteúdo

A **Entrega de Conteúdo (*CDN - Content Delivery Network*)** é um serviço indispensável para a Tupã Studios garantir que jogadores recebam atualizações e *patches* com a máxima velocidade e eficiência.

Considerando um volume de 50.000 GiB mensal:

d) Transferência de dados de saída do cache - US$ 0,09 / < 10 TiB (* 10.000)
e) Transferência de dados de saída do cache - US$ 0,06 / 10 a 150 TiB (* 40.000)
f) Preenchimento de cache - US$ 0,02 / GiB (* 50.000)
g) Solicitações de pesquisa no cache HTTP/HTTPS - US$ 0,0075 / por 10.000 solicitações (* 120.000)

Total mensal - US$ 5.200 /Mês

9.3.8 CI/CD e Ferramenta de Desenvolvimento

As **Ferramentas de Desenvolvimento e Integração Contínua (CI/CD)** são vitais para lançar atualizações, novos recursos e correções de bugs rapidamente e com segurança.

a) *Cloud Build e2-standard-2* - US$ 0,0 / primeiros 2.500 min (* 2.200)
b) *Cloud Build e2-standard-2* - US$ 0,006 / por min adicional (* 0)
c) Armazenamento *Artifact Registry* - US$ 0,10 / GB (* 100)
d) Transferência de dados - US$ 0,08 / GB (* 50)
e) *GitLab Cloud Build Triggers* - US$ 0,00

Total Mensal - US$ 14,00

9.4 Tabela Preços GCP

A Tabela 9.2 a seguir apresenta o detalhamento dos custos mensais para a infraestrutura no Google Cloud Platform (GCP), com base nos cálculos de 100.000 usuários.

Tabela 9.2 - Preços para cada serviço GCP

Serviço de Cloud	Preço
Computação	US$ 2.115,99
Banco de Dados	US$ 1.698,31
Armazenamento	US$ 62,55
Rede e Balanceamento de carga	US$ 16.368,25
Segurança e Autenticação	US$ 1.175,00
Monitoramento de Logs	US$ 808,50
Entrega de Conteúdo	US$ 5.200
CI/CD	US$ 14,00

Fonte: Autores do projeto (2025)

Nota: Total mensal US$ 27.442,60

9.5 Tabela Comparação AWS x GCP

Para consolidar a análise de custos, a tabela a seguir apresenta um comparativo direto dos preços da AWS e do GCP. Os valores são baseados na estimativa de 100.000 jogadores e detalham o custo por serviço, bem como o investimento mensal total em cada provedor.

Tabela 9.3 - Comparativo de preços AWS x GCP

Serviços de Cloud	Preço AWS	Preço GCP
Computação	US$ 4.730,40	US$ 2.115,99
Banco de Dados	US$ 1.156,22	US$ 1.698,31
Armazenamento	US$ 23,75	US$ 62,55
Rede e Balanceamento de carga	US$ 26.280,82	US$ 16.368,25

Segurança e Autenticação	US$ 3.343,04	US$ 1.175,00
Monitoramento de Logs	US$ 5.055,375	US$ 808,50
Entrega de Conteúdo	US$ 900,00	US$ 5.200
CI/CD	US$ 330,52	US$ 14,00
Total Mensal	US$ 41.820,125	US$ 27.442,60

Fonte: Autores do projeto (2025)

Diante dessa análise detalhada dos custos e da complexidade de otimização, a empresa optou pelo *Google Cloud Platform* (*GCP*) como seu provedor de nuvem principal.

A decisão foi baseada na avaliação de que a infraestrutura de rede global do GCP, de forma notória, sua fibra de alta capacidade e as menores taxas de latência de conexão, se alinha perfeitamente às exigências de baixa latência e alta disponibilidade de um jogo online. Além disso, a arquitetura de rede do GCP é projetada para mitigar o pico de custos de saída (*Data Transfer Out*), oferecendo um modelo de preços mais previsível e acessível em comparação com a AWS.

10 DESCRITIVO DOS SERVIDORES

O Quadro 8.1 a seguir detalha as especificações técnicas de hardware, software e o custo estimado para os servidores que compõem a infraestrutura da Tupã.

Quadro 10.1 - Detalhamento dos servidores *On-premises*

Função do Servidor	Hardware	Sistema Operacional	Softwares Principais	Custo Estimado (Hardware)
Matriz São Paulo (Hub Primário)				
SP1-NET-SRV01 (Rede)	CPU: 16-Core (Intel Xeon E5 v4), RAM: 128GB, Armazenamento: 2TB SSD RAID 1	*Linux Server*	DNS, DHCP, Active Directory (Samba)	R$ 7.000 - R$ 12.000
Função do Servidor	**Hardware**	**Sistema Operacional**	**Softwares Principais**	**Custo Estimado (Hardware)**
SP1-CODE-SRV01 (Código)	CPU: 16-Core (Intel Xeon E5 v4), RAM: 128GB,	*Linux Server*	*GitLab*	R$ 9.000 - R$ 15.000

	Armazenamento: 4TB NVMe RAID 10			
SP1-BCK-SRV01 (Backup)	CPU: 8-Core (Intel Xeon E5 v4), RAM: 64GB, Armazenamento: 50 TB HDD RAID 6	*Linux Server*	*Bacula ou Veeam for Linux*	R$ 12.000 - R$ 20.000
Filial SP II (Hub de Redundância)				
SP2-NET-SRV02 (Rede)	CPU: 16-Core (Intel Xeon E5 v4), RAM: 128GB, Armazenamento: 2TB SSD RAID 1	*Linux Server*	*DNS, DHCP*, etc. (Replicação/*Fail over*)	R$ 7.000 - R$ 12.000
SP2-CODE-BCK01 (Código)	Configuração idêntica ao SP1-CODE-SRV01	*Linux Server*	*GitLab* (Replicação)	R$ 9.000 - R$ 15.000
Infraestrutura de Alta Performance				
SP2-HPC-SRV01 (Build & Inovação)	CPU: 32-Core (AMD Threadripper/EPYC), GPU: NVIDIA RTX 3090 24GB, RAM: 256GB, Armazenamento: 4TB NVMe	*Linux Server (Ubuntu)*	*Jenkins, Unreal Engine Tools, MATLAB, Python (TensorFlow), Docker*	R$ 30.000 - R$ 45.000
Custo Total Estimado				R$ 74.000 - R$ 119.000

Fonte: Autores do projeto (2025)

11 DESCRITIVO DOS HARDWARES POR SETOR

Para atender às necessidades específicas de cada departamento, os hardwares são distribuídos de acordo com a função e a demanda operacional. Os Quadros a seguir detalham as especificações dos equipamentos por setor.

11.1 Setor de Inovação

O Setor de Inovação é focado em pesquisa e desenvolvimento (P&D), o que exige equipamentos de alta capacidade para prototipagem, análise de dados e testes de novos conceitos. O Quadro 11.1 a seguir detalha o *hardware* específico alocado para esta equipe.

Quadro 11.1 - Detalhes técnicos de Hardware em inovação

Componente	Especificação	Justificativa

Processador (CPU)	AMD Ryzen 7 ou Intel Core i7	Oferece um excelente número de núcleos para a maioria das simulações, representando o ponto ideal entre performance e preço.
Placa-Mãe	Chipset Intermediário (Ex: AMD B650 ou Intel B760)	Fornece todos os recursos necessários (suporte a NVMe, RAM DDR5) com grande estabilidade e um custo significativamente menor que os modelos de topo.
Placa de Vídeo (GPU)	NVIDIA GeForce RTX 3060 (12 GB)	Os 12 GB de VRAM são um grande diferencial para treinar modelos de *IA*, tornando-a a melhor escolha de custo-benefício.
Memória RAM	32 GB DDR5	É uma quantidade robusta para a maioria dos projetos de IA e simulação, com a vantagem de ser uma melhoria fácil e mais barata no futuro, caso necessário.
Armazenamento	1 TB SSD NVMe + 2 TB HDD	Mantém a agilidade do *SSD* para o sistema e softwares, com um *HDD* de bom tamanho para armazenamento de dados, otimizando o custo.

(Continuação)

Sistema Operacional	Linux (Ubuntu LTS)	Padrão da empresa, sem custo de licença.
Softwares Pré-instalados	*Python (Anaconda, TensorFlow, PyTorch, NumPy),* VS *Code, Docker, Bitdefender*	Ambiente completo e seguro para a equipe de pesquisa e desenvolvimento.
Custo Estimado	R$ 7.000 - R$ 9.000 por unidade	Custo total para os 15 *desktops*: R$ 105.000 - R$ 135.000

Fonte: Autores do projeto (2025)

11.2 Setor de Segurança

O Quadro 11.2 apresenta o descritivo de *hardware* utilizado pelo Setor de Segurança para monitoramento e resposta a incidentes.

Quadro 11.2 - Detalhes técnicos de *Hardware* em segurança

Componente	Especificação	Justificativa
Processador (CPU)	Intel Core i5-10400F	Processador mais núcleos é essencial para rodar múltiplas ferramentas de análise, máquinas virtuais e compilar dados de segurança sem travamentos.
Placa-Mãe	Gigabyte B460M DS3H	Oferece estabilidade e todos os conectores necessários, incluindo múltiplas saídas de vídeo e suporte para os componentes de média-alta velocidade.
Placa de Vídeo (GPU)	Modelo com suporte a múltiplos monitores (Ex:AMD RX 580)	O foco aqui não é a potência 3D, mas a capacidade de conectar 3 ou 4 monitores simultaneamente, fundamental para um analista de segurança.
Memória RAM	16 GB DDR4	Permite analisar grandes arquivos de *log*, rodar máquinas virtuais para análise de malware e manter diversas ferramentas de monitoramento abertas ao mesmo tempo.

(Continuação)

Armazenamento	500 GB SSD NVMe	A alta velocidade de leitura e escrita do *SSD NVMe* é crucial para acelerar a busca e a análise em grandes volumes de dados de segurança.
Sistema Operacional	Linux (Ubuntu LTS)	Conforme o padrão da empresa, oferece acesso a uma vasta gama de ferramentas de segurança *open-source* e maior controle sobre o sistema.
Softwares Pré-instalados	Wireshark, Splunk (agente), Docker, suíte de segurança e ferramentas de análise forense.	Ambiente pronto para monitoramento de rede, análise de *logs*, virtualização e resposta a incidentes.

Custo Estimado	R$ 3.800 - R$ 4.500 por unidade	Custo total para os 10 *desktops*: R$ 38.000 - R$ 45.000.

Fonte: Autores do projeto (2025)

11.3 Setor de Desenvolvimento

Os Quadros apresentam o descritivo de hardware padrão utilizado pelas equipes do Setor de Desenvolvimento.

Quadro 11.3 - Detalhes técnicos de *Hardware* em desenvolvimento PC1

Componente	Especificação	Justificativa
Placa-mãe	Asus TUF Gaming B550M-Plus	Custo-benefício com ótima performance.
Processador (CPU):	AMD Ryzen 5 5500	Processador de alto desempenho compatível com a Placa-Mãe utilizada e com ótima *single treading* para processos como photoshop e FL studio.
Placa de Vídeo (GPU)	RX 580	Utilizada para a aceleração de hardware promovendo uma maior eficiência e praticidade no processo de criação de imagens e áudio.
Memória RAM	2 de 8GB (DDR4)	Compatibilidade com *dual-channel* da placa-mãe

(Continuação)

Armazenamento	NVMe M.2 (500GB) e SSD (1 TB)	*NVMe* com capacidade considerável de espaço para S.O e aplicativos utilizados
Sistema Operacional	Windows 10/11	Sistema Operacional compatível com os *softwares* utilizados
Softwares utilizados	Photoshop e FL Studio, Jira	*Softwares* utilizados para a edição de imagem, criação de som e organização do time, respectivamente.
Custo estimado	R$4.000 - R$5.500	Custo total para 40 *desktops*: R$160.000 - R$220.000

Fonte: Autores do projeto (2025)

Quadro 11.4 - Detalhes técnicos de *Hardware* em desenvolvimento PC2

Componente	Especificação	Justificativa
Placa-mãe	Chipset alto padrão (AM5 e B650)	Ótima performance.
Processador (CPU):	AMD Ryzen 9 7900X	Processador de alto desempenho compatível com a placa-mãe. Possui 12 núcleos, utilizados para processos pesados como *Unreal Engine*.
Placa de Vídeo (GPU)	Nvidia Geforce RTX 4080 (12 GB)	Placa de vídeo robusta para a criação de cenários e objetos que necessitam de grande carga de vídeo.
Memória RAM	4 de 8GB (DDR5)	Compatibilidade com *four-channel* da placa-mãe
Armazenamento	NVMe M.2 (1 TB) e SSD (1 TB)	NVMe com grande capacidade de espaço para S.O e aplicativos utilizados e *SSD* com capacidade para arquivos grandes.
Sistema Operacional	Linux	Sistema Operacional compatível com *softwares* utilizados e sem a necessidade de uma licença paga
Softwares utilizados	Blender e Unreal Engine	*Softwares* utilizados para a criação de modelos 3D, mecânicas e algoritmos do jogo
Custo estimado	R$8.000 - R$10.500	Custo total para 40 *desktops*: R$320.000 - R$405.000

Fonte: Autores do projeto (2025)

11.4 Setor de Atendimento ao Cliente

O Setor de Atendimento ao Cliente é a linha de frente da comunicação, necessitando de equipamentos confiáveis para gerenciar as plataformas de comunicação. O Quadro 11.5 detalha o hardware padrão utilizado por esta equipe.

Componente	Especificação	Justificativa

Placa-mãe	Chipset intermediário (LGA 1151 ou AM4)	Equilibra custo baixo, facilidade de manutenção e confiabilidade, pontos fundamentais para máquinas usadas diariamente por longas horas.
Processador (CPU):	Intel i5 ou AMD Ryzen 5	Equilibram potência e custo, oferecendo múltiplos núcleos suficientes para lidar com multitarefas do dia a dia
Placa de Vídeo (GPU)	Integrada	Não se faz necessário o uso de *GPU* dedicada
Memória RAM	8 GB DDR4	Permite que os atendentes trabalhem com diversas aplicações abertas ao mesmo tempo, evitando lentidão.
Armazenamento	SSD 480 GB	Garante inicialização rápida do *Windows*, abertura veloz de programas e carregamento de páginas e históricos de atendimento. Traz mais confiabilidade e agilidade do que *HDDs* tradicionais.
Sistema Operacional	Windows	A adoção do *Windows* como sistema operacional para o setor de atendimento ao cliente foi definida com base em critérios de segurança, desempenho e compatibilidade com as ferramentas utilizadas.
Softwares utilizados	Zendesk e Discord	São executados em ambiente Windows para garantir praticidade e segurança no suporte aos usuários
Custo estimado	R$ 1.490 - 2.170	Custo total para 20 *desktops*: R$ 29.800 - 43.400

Quadro 11.5 - Detalhes técnicos de Hardware em atendimento ao cliente

Fonte: Autores do projeto (2025)

11.5 Setor Administração

Esta subseção descreve os hardwares padrão fornecidos aos setores de Administração, RH e Jurídico. O Quadro 11.6 lista as especificações das estações de trabalho utilizadas nas rotinas administrativas.

Quadro 11.6 - Detalhes técnicos de *Hardware* em administração

Componente	Especificação	Justificativa
Placa-mãe	Chipset AMD A520 ou B550	AMD A520 - Oferece compatibilidade com processadores Ryzen série 4000/5000, garantindo bom desempenho e baixo custo B550 - Indicado para maior durabilidade e flexibilidade ao longo do prazo.
Processador (CPU):	AMD Ryzen 3 4000 ou 5000 Series	Processadores suficientes para as demandas administrativas. Inclui placa de vídeo integrada necessária, evitando gastos com um componente extra.
Placa de Vídeo (GPU)	Integrada ao processador	Suporta todas as tarefas do escritório sem necessidade de placa delicada. Reduz custo e consumo de energia
Memória RAM	8GB ou 16GB	8 GB é suficiente para atividades administrativas do dia a dia,como planilhas e navegação
Armazenamento	SSD de 256GB	O *SSD* proporciona maior velocidade na inicialização do sistema e na abertura de programas, além de oferecer espaço adequado para documentos e arquivos administrativos, garantindo eficiência no trabalho
Sistema Operacional	Windows 10/11	O sistema garante compatibilidade com *softwares* de escritório, segurança e estabilidade para uso administrativo.

(Continuação)

Componente	Especificação	Justificativa

Softwares utilizados	Windows Excel, SAP e Trello	São essenciais para a gestão administrativa: O Excel para planilhas e relatórios, o *SAP* para o controle e integração de processos empresariais e o *Trello* para organização de tarefas e produtividade
Custo estimado	R$ 3.500 - R$ 4.000	R$105.000 a R$120.000

Fonte: Autores do projeto (2025)

11.6 Setor de Marketing

Esta seção descreve os hardwares designados para a equipe de Marketing. O Quadro 11.7 lista as especificações das estações de trabalho, que são otimizadas para as demandas de produção de mídia digital e gerenciamento de campanhas.

Quadro 11.7 - Detalhes técnicos de *Hardware* em marketing

Componente	Especificação	Justificativa
Placa-mãe	Chipset LGA 1200 ou AM4	LGA 1200 - Pois suporta somente os processadores de 10ª Geração da *Intel*. AM4 - Isso por conta da compatibilidade eletrônica e física do *hardware*.
Processador (CPU):	AMD Ryzen 5500/ Intel core i5 10th	Possuem alto desempenho em multitarefas, garantindo que os *softwares* que o setor de marketing utiliza rodem de forma fluida.
Placa de Vídeo (GPU)	RTX 3050	Propõe a aceleração de *GPU* para os *softwares* de edição, modelagem e renderização sem esforço.
Memória RAM	16GB	Garanta múltiplos programas pesados que rodam simultaneamente sem travamentos, aumentando a produtividade do setor.

(Continuação)

Componente	Especificação Sugerida (Custo Otimizado)	Justificativa

Armazenamento	SSD NVMe 1TB	*NVMe*/*SSD Sata* para velocidade de leitura e escrita, melhor resposta no sistema e a necessidade prática, pois aumenta a produtividade.
Sistema Operacional	Windows 10/11	*Windows* 11, pois tem um suporte atualizado e por conta do *firewall* ser mais seguro.
Softwares utilizados	Adobe Illustrator, Adobe Premiere, Meta Business Suite e Google Analytic	Esses *softwares* são necessários porque garantem que o setor permita criar conteúdos profissionais.
Custo estimado	R$3,300 - R$4,500	Custo total para 25 *desktops*: R$ 82.500 - 112.500

Fonte: Autores do projeto (2025)

11.7 Setor de Limpeza e Manutenção

O Quadro 11.8 apresenta o descritivo de hardware padrão utilizado pela equipe de Limpeza e Manutenção.

Quadro 11.8 - Detalhes técnicos de *Hardware* em limpeza e manutenção

Componente	Especificação	Justificativa
Memória RAM	6 GB	Garante fluidez mesmo em tarefas mais pesadas ou multitarefas, como sincronizar grandes volumes de dados.
Armazenamento	128 GB	Permite que o dispositivo armazene o *Maximo Asset Management Mobile App*, relatórios e documentos sem precisar de gerenciamento constante de espaço.
Processador	Octa-Core	Permite que o dispositivo execute várias tarefas simultaneamente sem travamentos e maior fluidez.
Custo estimado	R$ 709,99	Custo Total: R$ 7.100

Fonte: Autores do projeto (2025)

11.8 Valores Totais

Esta seção consolida todos os custos estimados no projeto, incluindo o investimento em *hardware on-premise*. A tabela 11.1 a seguir apresenta o valor total necessário para a implementação e operação.

Tabela 11.1 - Valores totais de investimento em *hardware*

Setor	Preço dos Setores
Servidores	R$ 74.000 - R$ 119.000
Inovação	R$ 105.000 - R$ 135.000
Segurança	R$ 38.000 - R$ 45.000
Desenvolvimento I	R$ 160.000 - R$ 220.000
Desenvolvimento II	R$ 320.000 - R$ 405.000
Atendimento ao Cliente	R$ 29.800 - R$ 43.400
Administração	R$ 105.000 - R$ 112.500
Marketing	R$ 82.500 - R$ 150.000
Limpeza e Manutenção	R$ 7.100
Preço Total	R$ 921.400 - R$ 1.237.100

Fonte: Autores do projeto (2025)

12 IMPLEMENTAÇÃO DE DISPOSITIVOS *IOT*

A adoção estratégica de dispositivos IoT na Tupã Studios visa fortalecer a segurança física, otimizar a gestão de infraestrutura e mitigar riscos operacionais identificados na análise de vulnerabilidades. A implementação será focada em três áreas principais: segurança de ativos críticos, continuidade operacional e otimização do ambiente de trabalho.

12.1 Segurança Física e Monitoramento de Ativos Críticos

Esta é a área de maior prioridade, focada em proteger a infraestrutura de servidores e, consequentemente, a propriedade intelectual da empresa.

a) Controle de Acesso Inteligente (*Smart Locks*):

- Aplicação: Substituir as fechaduras tradicionais das salas de servidores e outras áreas restritas por um sistema de controle de acesso baseado em cartões NFC/RFID, integrados aos crachás dos funcionários.
- Benefícios: Esta medida mitiga diretamente o risco de acesso físico não autorizado. O sistema gera um *log* detalhado de todas as entradas, permitindo auditorias precisas. Além disso, o acesso de um crachá perdido ou de um ex-colaborador pode ser revogado instantaneamente, aumentando a segurança.

b) Sensores Ambientais para Salas de Servidores:

- Aplicação: Instalar sensores de temperatura, umidade e detecção de líquidos dentro das salas de servidores na Matriz e na Filial SP II.
- Benefícios: Os sensores monitoram o ambiente 24/7 e enviam alertas automáticos para a equipe de Segurança e Manutenção caso a temperatura exceda um limite seguro ou se um vazamento for detectado. Isso previne falhas de *hardware* por superaquecimento e mitiga o risco de derramamento de líquidos e danos aos equipamentos.

12.2 Gestão de Energia e Continuidade Operacional

a) Fontes de Alimentação Ininterrupta Inteligentes:

- Aplicação: Equipar os *racks* de servidores com sistemas de UPS que possuam conectividade IoT.

- Benefícios: Em caso de falha de energia, a UPS não apenas mantém os servidores ligados, mas também envia um alerta para a equipe de TI, informando o estado da bateria. Se a energia não retornar, a UPS pode ser programada para iniciar um desligamento seguro e automatizado dos servidores, prevenindo a corrupção de dados e mitigando o risco de paralisação de processos por quedas de energia.

12.3 Otimização do Ambiente de Trabalho (Smart Office)

a) Gestão Inteligente de Iluminação e Climatização:

- Aplicação: Implementar sensores de presença e luminosidade nas áreas comuns e salas de reunião para controlar a iluminação e o ar-condicionado de forma automática.

- Benefícios: Redução significativa nos custos de energia, pois as luzes e o ar-condicionado são desligados automaticamente em ambientes desocupados. Além disso, melhora o conforto dos colaboradores, contribuindo para um ambiente de trabalho mais produtivo.

13 CONCLUSÃO

Este trabalho teve como objetivo a concepção de uma infraestrutura computacional e de segurança para a Tupã Studios, respondendo diretamente aos desafios operacionais de um estúdio de jogos moderno. A metodologia, que partiu de uma análise de vulnerabilidades, permitiu a criação de um ecossistema tecnológico onde cada decisão, da escolha do hardware à topologia de rede, foi justificada por uma necessidade real de negócio.

A arquitetura resultante se destaca pela sua resiliência e segurança. A implementação de uma rede *Hub-and-Spoke* com segmentação por *VLANs* garante o controle centralizado e o isolamento de tráfego, enquanto o plano de segurança da informação formaliza as políticas e os procedimentos de resposta a incidentes. Um pilar fundamental desta arquitetura é a estratégia de servidores, que concentra os serviços críticos na matriz e utiliza a filial de São Paulo II como um site de redundância. Este modelo de *failover*, com replicação de dados e serviços de rede, assegura a continuidade dos negócios e protege a propriedade intelectual da empresa contra falhas catastróficas.

Conclui-se que a infraestrutura proposta é mais do que uma solução técnica; é um ativo estratégico que habilita a Tupã Studios a operar com eficiência e segurança. Ela fornece as ferramentas necessárias para o desenvolvimento de jogos e a resiliência para proteger suas criações, estabelecendo uma base sólida para o crescimento sustentável da empresa no competitivo mercado de entretenimento digital.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 14724**: informação e documentação: trabalhos acadêmicos: apresentação. Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023**: informação e documentação: referências: elaboração. Rio de Janeiro, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6024**: informação e documentação: numeração progressiva das seções de um documento: apresentação. Rio de Janeiro, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6027**: informação e documentação: sumário: apresentação. Rio de Janeiro, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6028**: informação e documentação: resumo, resenha e recensão: apresentação. Rio de Janeiro, 2021
.
A DIFERENÇA entre endereços IP estáticos e dinâmicos. In: **AVG ANTIVIRUS**. Disponível em: https://www.avg.com/pt/signal/static-vs-dynamic-ip-addresses. Acesso em: 14 set. 2025.

AMAZON WEB SERVICES (AWS). **AWS Pricing Calculator**. Disponível em: https://calculator.aws/#/addService. Acesso em: 22 set. 2025.

AMAZON WEB SERVICES. **Amazon GameLift**: Hospedagem de servidores dedicados para jogos. Disponível em: https://aws.amazon.com/pt/gamelift/servers/?nc2=h_prod_gt_gls. Acesso em: 22 set. 2025.

AMAZON WEB SERVICES. **O que é a AWS?**. Disponível em: https://aws.amazon.com/pt/what-is-aws/. Acesso em: 22 set. 2025.

BENEFÍCIOS das VLANs. In: **GTA UFRJ**. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2012_2/vlan/beneficios.html. Acesso em: 14 set. 2025.

ENDEREÇO IP estático vs. dinâmico: Semelhanças e diferenças. In: **FORTINET**. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/static-vs-dynamic-ip. Acesso em: 14 set. 2025.

EXPLORING Hub-and-Spoke Network Topology: A Simplified Model for Scalable Connections. In: **EXAM-LABS**. Disponível em: https://www.exam-labs.com/blog/exploring-hub-and-spoke-network-topology-a-si. Acesso em: [Data de acesso?].

GOMES, Bruna. **Cibersegurança, segurança da informação e segurança digital**: qual a diferença desses termos? Contacta, 24 set. 2024. Disponível em:

https://www.contacta.com.br/blog/ciberseguranca-seguranca-da-informacao-e-seguranca-digital-qual-a-diferenca-desses-termos. Acesso em: 03 set. 2025.

GOMES, Bruna. **O que é e como fazer um plano de segurança da informação**. Disponível em: https://www.contacta.com.br/blog/plano-de-seguranca-da-informacao. Acesso em: 03 set. 2025.

GOOGLE. **Cloud SQL Pricing**. Disponível em: https://cloud.google.com/sql/pricing?hl=pt_br. Acesso em: 22 set. 2025.

GOOGLE CLOUD. **Casos de uso comuns dos desenvolvedores**. Disponível em: https://cloud.google.com/developers/use-cases?hl=pt-br. Acesso em: 22 set. 2025.

GOOGLE CLOUD. **Cloud Build pricing**. Disponível em: https://cloud.google.com/build/pricing?hl=pt_br. Acesso em: 7 out. 2025.

GOOGLE CLOUD. **Família de máquinas de uso geral para o Compute Engine**. In: Documentação do Compute Engine. 2025. Disponível em: https://cloud.google.com/compute/docs/general-purpose-machines?hl=pt-br#c3-highcpu. Acesso em: 22 set. 2025.
GOOGLE CLOUD. **Preço | Artifact Registry**. Disponível em: https://cloud.google.com/artifact-registry/pricing?hl=pt-br. Acesso em: 7 out. 2025.

GOOGLE CLOUD. **Preço | Cloud CDN**. Disponível em: https://cloud.google.com/cdn/pricing?hl=pt-br. Acesso em: 7 out. 2025.

GOOGLE CLOUD. **Preço | Identity Platform**. Disponível em: https://cloud.google.com/identity-platform/pricing?hl=pt-br. Acesso em: 7 out. 2025.

GOOGLE CLOUD. **Preços do Cloud Load Balancing**. Disponível em: https://cloud.google.com/load-balancing/pricing?hl=pt_br. Acesso em: 7 out. 2025.

GOOGLE CLOUD. **Preços do Cloud Storage**. Disponível em: https://cloud.google.com/storage/pricing?hl=pt-br#south-america. Acesso em: 22 set. 2025.

GOOGLE CLOUD. **Preços | Google Cloud Armor**. Disponível em: https://cloud.google.com/armor/pricing?hl=pt-br. Acesso em: 7 out. 2025.

GOOGLE CLOUD. **Visão geral do Google Cloud**. Disponível em: https://cloud.google.com/docs/overview?hl=pt-br. Acesso em: 22 set. 2025.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Normas de apresentação tabular**. 3. ed. Rio de Janeiro: IBGE, 1993. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv23907.pdf. Acesso em: 01 nov. 2025.

INTERNET of Things (IoT). In: **UPS SYSTEMS**. Disponível em: https://www.upssystems.co.uk/internet-of-things-iot. Acesso em: 25 set. 2025.

O QUE é o Gerenciamento de Vulnerabilidades? In: **MICROSOFT SECURITY**. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-vulnerability-management. Acesso em: 11 set. 2025.

O QUE é o servidor DHCP (Dynamic Host Configuration Protocol) no Windows Server? In: **MICROSOFT LEARN**. Disponível em: https://learn.microsoft.com/pt-br/windows-server/networking/technologies/dhcp/dhcp-top. Acesso em: 14 set. 2025.

O QUE é VLAN? Será que eu deveria usar na minha rede? In: **YOUTUBE**. Disponível em: https://www.youtube.com/watch?v=4CEBW06CJGM. Acesso em: 14 set. 2025.

O QUE é: Roteador de borda de um provedor? In: **INTERNET GOIÂNIA**. Disponível em: https://internetgoiania.com.br/blog/glossario/roteador-borda-provedor-fibra-optica-goiania/. Acesso em: 05 set. 2025.

PASSMARK SOFTWARE. **CPU Comparison**. Disponível em: https://www.cpubenchmark.net/singleCompare.php. Acesso em: 25 set. 2025.

PUGET SYSTEMS. **Hardware Recommendations for Unreal Engine**. Puget Systems, 2024. Disponível em: https://www.pugetsystems.com/solutions/real-time-3d-rendering-virtual-production/unreal-engine/hardware-recommendations/. Acesso em: 24 set. 2025.
SECURITY Software & Solutions. In: **SPLUNK**. Disponível em: https://www.splunk.com/en_us/products/cyber-security.html. Acesso em: 28 set. 2025.

SENAI. Departamento Nacional. **Arquitetura de redes**. [Brasília, DF]: SENAI Departamento Nacional, 2012. Disponível em: https://professorleonardomello.wordpress.com/wp-content/uploads/2013/03/arquit_redes.pdf. Acesso em: 12 set. 2025.

SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL (SENAC). **Normas administrativas**. São Paulo: Senac, 2024. Disponível em: https://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf. Acesso em: 27 ago. 2025.

SMART lock. In: **WIKIPEDIA**. Disponível em: https://en.wikipedia.org/wiki/Smart_lock. Acesso em: 25 set. 2025.

SOUSA, Gustavo Fernandes de. **Implementação de um dispositivo IoT para monitoramento de produção de uma lixadeira de cabos**. Instituto Federal de Rondônia, 2023. Disponível em: https://repositorio.ifro.edu.br/items/50b1154f-f45d-4255-9fdf-ef8590392a94. Acesso em: 26 set. 2025.

VERSUS. **Comparação de placas-mãe**. Disponível em: https://versus.com/br/motherboard. Acesso em: 25 set. 2025.
WHAT'S the difference between a Layer 2 & Layer 3 switch. In: **SERVER FAULT**. Disponível em: https://serverfault.com/questions/123726/whats-the-difference-between-a-layer-2-layer-3-switch. Acesso em: 05 set. 2025.

WHY Zero Trust Network Access (ZTNA) Prevents Cyberattacks in Microsoft 365. In: **SEDONATEK**. Disponível em: https://pages.sedonatek.com/insights/why-zero-trust-network-access-ztna-prevents-cyberattacks-in-microsoft-365. Acesso em: 15 set. 2025.

GLOSSÁRIO

Active directory – autenticação e gerenciamento de acesso (centraliza o gerenciamento, controle dos usuários, computadores e permissões da rede).

APs – ponto de acesso para conexão wifi.

Backbone – o núcleo de alta velocidade de uma rede *(Switch L3).*

Backend – a lógica de uma aplicação.

Camada de *core* – responsável pela transmissão de dados em alta velocidade e troca de tráfego.

Data Transfer Out – taxa de transferência de dados de saída.

DDoS – ataque distribuído de negação de serviço. Uma tentativa de sobrecarregar um servidor com uma inundação de tráfego de múltiplas fontes.

DHCP – protocolo que atribui endereços IP automaticamente aos dispositivos em uma rede.

DNS – o sistema que traduz nomes de domínio em endereços IP.

Dual-channel – tecnologia para o acesso de dois módulos de memória RAM ao mesmo tempo, melhorando a passagem de informações.

Exploit – um código ou técnica que se aproveita de uma vulnerabilidade em um software ou sistema.

Firewall – dispositivo de segurança que monitora e filtra o tráfego de rede, decidindo o que bloquear ou permitir.

Hardening – o processo de configurar o sistema da forma mais segura possível, removendo serviços desnecessários e aplicando patches.

HPC – computação de alta performance.

Hub-and-Spoke – modelo de estrutura de rede centralizada.
Intellectual Property – propriedade intelectual pertencente a organização.
IoT – internet das coisas, ou seja, dispositivos que possam conectar-se com a internet.
LAN – rede de área local
Latência – o tempo de atraso na comunicação de dados.
Logs – registros de atividades.
Malware – software malicioso, termo genérico para vírus.
Matchmaking – o processo em jogos online que junta jogadores na mesma partida.
Open-source – modelo de código aberto.
Patches – correções e atualizações feitas em aplicativos.
Phishing – tentativa de fraude que rouba credenciais do usuário, fingindo ser uma entidade confiável.
Quality Assurance – garantia do padrão de qualidade.
S.O – sistema operacional.
Servidores *on-premise* – hardware e software dos servidores localizados fisicamente nas instalações físicas da organização.
Single threading – refere-se à capacidade de um processador (CPU) de executar apenas uma tarefa por vez em um único núcleo.
SOC – centro de operações de segurança
Testes de penetração – simulação de ataque cibernético autorizada para identificar vulnerabilidades em sistemas, redes ou aplicações.
TI – tecnologia da informação.
UPS – fonte de alimentação ininterrupta.
VLAN - rede local virtual
VPN - rede privada virtual que cria um "túnel" seguro e criptografado sobre uma rede pública, usado para conectar as filiais ao Hub.
WAN - rede de longa distância que conecta redes locais geograficamente separadas.