

INSTITUTO FEDERAL DO PARANÁ

RODRIGO CASSIANO GÜNTHER

INSTALAÇÃO E IMPLEMENTAÇÃO DE UM SERVIDOR DE REDES BASEADO EM
LINUX, PARA A EMPRESA FORCETECH JR SOLUÇÕES, DO INSTITUTO
FEDERAL DO PARANÁ, CAMPUS UNIÃO DA VITÓRIA

UNIÃO DA VITÓRIA

2022

RODRIGO CASSIANO GÜNTHER

INSTALAÇÃO E IMPLEMENTAÇÃO DE UM SERVIDOR DE REDES BASEADO EM
LINUX, PARA A EMPRESA FORCETECH JR SOLUÇÕES, DO INSTITUTO
FEDERAL DO PARANÁ, CAMPUS UNIÃO DA VITÓRIA

Trabalho de Conclusão de Curso apresentado ao
Curso Tecnólogo em Análise e Desenvolvimento de
Sistemas, do Instituto Federal do Paraná – Campus
União da Vitória, como requisito parcial de
avaliação da disciplina TCC II.

Orientador: Prof. Celso Canteri

UNIÃO DA VITÓRIA

2022

Ficha catalográfica automática da biblioteca do IFPR
DADOS FORNECIDOS PELO(A) AUTOR(A)

G977i Günther, Rodrigo Cassiano
INSTALAÇÃO E IMPLEMENTAÇÃO DE UM
SERVIDOR DE REDES BASEADO EM LINUX, PARA
A EMPRESA FORCETECH JR SOLUÇÕES, DO
INSTITUTO FEDERAL DO PARANÁ, CAMPUS
UNIÃO DA VITÓRIA / Rodrigo Cassiano Günther;
orientador(a) Celso Canteri. -- União da Vitória, 2022.
76 f.


Trabalho de Conclusão de Curso (Graduação -
Graduação em Tecnólogo em Análise e Desenvolvimento
de Sistemas) -- Instituto Federal do Paraná, Campus União
da Vitória, 2022.

1. Servidor de Rede. 2. Linux. 3. Internet. 4.
Empresa Júnior. . I. Canteri, Celso, orient. II. Título.


TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal do Paraná – Campus União da Vitória, foram convocados para realizar a arguição do trabalho de conclusão de curso de Rodrigo Cassiano Günther, intitulado: **INSTALAÇÃO E IMPLEMENTAÇÃO DE UM SERVIDOR DE REDES BASEADO EM LINUX, PARA A EMPRESA FORCETECH JR SOLUÇÕES, DO INSTITUTO FEDERAL DO PARANÁ, CAMPUS UNIÃO DA VITÓRIA**, sob orientação do Professor Esp. Celso Canteri, que após terem inquirido o aluno e realizada a avaliação do trabalho são de parecer pela sua aprovação no rito da defesa. A outorga do título de Tecnólogo em Análise e Desenvolvimento de Sistemas está sujeita a homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Colegiado do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas.


UNIÃO DA VITÓRIA, 10 de maio de 2022.

Documento assinado digitalmente
 CELSO CANTERI
Data: 13/05/2022 14:16:52-0300
Verifique em <https://verificador.iti.br>


Celso Canteri
Presidente da banca examinadora
Instituto Federal do Paraná

Documento assinado digitalmente
 ALEX MATEUS PORN
Data: 12/05/2022 11:30:59-0300
Verifique em <https://verificador.iti.br>

Alex Mateus Porn
Avaliador Interno – Instituto Federal do Paraná

Documento assinado digitalmente
 GERALDO RANTHUM
Data: 26/05/2022 18:04:06-0300
Verifique em <https://verificador.iti.br>

Geraldo Ranthum
Avaliador Externo – Universidade Tecnológica Federal do Paraná

Documento assinado digitalmente
 RAFAEL DOS PASSOS CANTERI
Data: 25/05/2022 01:06:18-0300
Verifique em <https://verificador.iti.br>

Rafael dos Passos Canteri
Avaliador Externo – Universidade Federal do Mato Grosso do Sul

AGRADECIMENTOS

A minha esposa Ana Paula Weiller Günther e a minha filha Nathália Weiller Günther pela paciência, pelo apoio incondicional, e por serem compreensivas durante meus períodos de ausência.

A meu pai Dieter Renato Günther (in memoriam), que sempre me apoiou e incentivou incondicionalmente em minha vida, me ensinou como ser uma pessoa honesta e dedicada, como amar a família, como respeitar o próximo.

Ao Professor Celso Canteri, orientador deste TCC, pelos ensinamentos, pelas inúmeras horas de orientação, por sua dedicação como professor e amigo.

Aos amigos Thiago Schmidt e Lucas Ruan Alebrante, por sua amizade e apoio nos três anos decorridos do curso.

RESUMO

Ao final do ano de 2019, implantou-se no Instituto Federal do Paraná (IFPR), campus União da Vitória, o projeto Empresa Júnior (EJ). Este projeto tem como finalidade trazer a experiência aos alunos de uma empresa real, com todas as suas funcionalidades e objetivos. Com os benefícios de aprender o seu funcionamento, seus trâmites legais, processos de implantação, desenvolvimento de produto/serviço, relacionamento com clientes, ações de marketing, venda e entrega do produto. Foi obtido um valor para financiar a infraestrutura da EJ através de um Projeto de Extensão do IFPR. Esta verba foi revertida em equipamentos, os quais incluíam um servidor de rede, dois roteadores, um computador *desktop*, e um *rack* para acomodação do servidor e roteadores. Observou-se a necessidade de implantação de um Sistema Operacional (SO), com todas suas funcionalidades no servidor da EJ. Foi optado pelo SO Linux por tratar-se de *software* gratuito de código aberto, amplamente utilizado em servidores pelo mundo. Portanto, este trabalho tem como objetivo principal a implantação, montagem, instalação e configuração de um servidor de rede/servidor *web*, para suprir a demanda de funcionalidades necessárias à EJ. Para tal, a metodologia aplicada foi identificar qual a distribuição Linux necessária que englobe todos os requisitos acima relacionados, bem como todos os *softwares* secundários necessários para o funcionamento da empresa. As escolhas das tecnologias e *softwares*, baseiam-se em pesquisa técnica bibliográfica com objetivo de adequar ao *hardware* previamente adquirido, e a infraestrutura de rede existente do IFPR.

Palavras-chave: Servidor de Rede. Linux. Internet. Empresa Júnior.

ABSTRACT

At the end of 2019, the Junior Enterprise (JE) project was implemented at the Instituto Federal do Paraná (IFPR), União da Vitória campus. This project aims to bring the experience to students of a real company, with all its features and objectives. With the benefits of learning how it works, its legal procedures, implementation processes, product/service development, customer relationships, marketing actions, sales and product delivery. An amount was obtained to finance the JE infrastructure through an IFPR Extension Project. This amount was invested in equipment, which included a Network Server, two routers, a Desktop computer, and a Rack to accommodate the Server and routers. It was observed the need to implement an Operating System (OS), with all its features on the JE server. The Linux OS was chosen because it is free open source software, widely used on servers around the world. Therefore, this work has as main objective the implantation, assembly, installation and configuration of a network server/web server, to supply the demand of necessary functionalities to the JE. To this end, the methodology applied was to identify which Linux distribution is needed that encompasses all the requirements listed above, as well as all the secondary software necessary for the company to function. The choices of technologies and software are based on technical bibliographic research in order to adapt to the previously acquired hardware and the existing IFPR network infrastructure.

Keywords: Network Server. Linux. Internet. Junior Enterprise.

LISTA DE ILUSTRAÇÕES

Figura 1 – página de download do Ubuntu versão servidor.....	34
Figura 2 – tela do <i>software</i> Rufus.....	35
Figura 3 – tela de seleção de idioma da instalação do Ubuntu.....	36
Figura 4 – tela de opção de atualização da instalação do Ubuntu.....	36
Figura 5 – tela de seleção de layout de teclado da instalação do Ubuntu	37
Figura 6 – tela de configuração de rede da instalação do Ubuntu	38
Figura 7 – tela de seleção de disco rígido da instalação do Ubuntu	38
Figura 8 – tela de configuração de usuário/senha/nome do anfitrião da instalação do Ubuntu	39
Figura 9 – tela de opção de instalação do ssh da instalação do Ubuntu	39
Figura 10 – tela inicial da instalação do WordPress	44
Figura 11 – tela de configuração do banco de dados, usuário e senha do WordPress	45
Figura 12 – tela final da configuração da instalação do WordPress	45
Figura 13 – tela da instalação do WordPress com a configuração de usuário e senha administrativos	46
Figura 14 – tela de sucesso na instalação do WordPress	46
Figura 15 – tela inicial da instalação do Postfix, seleção do tipo de instalação	47
Figura 16 – seleção do nome do servidor Postfix.....	47
Figura 17 – tela da instalação do Postfix, seleção de aliases para o root.....	48
Figura 18 – seleção de nomes de anfitrião para o servidor Postfix	48
Figura 19 – configuração de endereçamento de rede do servidor Postfix	48
Figura 20 – tela de opção por atualização síncrona da instalação do Postfix.....	49
Figura 21 – tela de configuração do tamanho da caixa de correio da instalação do Postfix.....	49
Figura 22 – tela de seleção dos protocolos tcp da instalação do Postfix	49
Figura 23 – tela resultante do comando “#sudo ss -lnpt grep dovecot.....	53
Figura 24 – configuração do Squirrelmail para o Apache	54
Figura 25 – tela inicial da página oficial do Registro.br.....	55
Figura 26 – tela do formulário de cadastro de conta de acesso no Registro.br	55
Figura 27 – configurações do domínio forcetechjr.com.br	56
Figura 28 – resultado do comando “#sudo systemctl status certbot.timer”	57

Figura 29 – tela de configuração do certificado de criptografia do Webmin.....	59
Figura 30 – tela de configuração de Cifra SSL do Webmin	59
Figura 31 – terminal de texto do Linux Ubuntu	62
Figura 32 – terminal de texto do Microsoft Windows10, acesso ao servidor via ssh.	62
Figura 33 – tela inicial do Webmin	63
Figura 34 – página de índice padrão do servidor Apache	63
Figura 35 – tela de informações do PHP	64
Figura 36 – tela de resposta do servidor MariaDB ao comando “#sudo service mysql status”	64
Figura 37 – tela do painel de administração do phpMyAdmin	65
Figura 38 – tela inicial do painel de administração do WordPress.....	65
Figura 39 – cliente de e-mail Thunderbird, composição de e-mail.....	66
Figura 40 – tela de leitura do cliente de e-mail Thunderbird	66
Figura 41 – tela de composição de e-mail do Squirrelmail	67
Figura 42 – tela da caixa de entrada do Squirrelmail	67
Figura 43 – informações de certificado de criptografia do navegador para o endereço https://forcetechjr.com.br/	68
Figura 44 – informações do registro de domínio forcetechjr.com.br	68
Figura 45 – página institucional da empresa Forcetech JR Soluções.....	69

LISTA DE QUADROS

Quadro 1 - Distribuições Linux	20
Quadro 2 – Distribuições Linux – complemento do Quadro 1 - página 20	21

LISTA DE SIGLAS

ABNT	– Associação Brasileira de Normas Técnicas
AWS	– <i>Amazon Web Services</i> (Serviços de Internet da empresa Amazon)
BSD	– <i>Berkeley Software Distribution</i> (Distribuição de Software Berkeley)
CGI	– <i>Common Gateway Interface</i> (Interface Comum de Saída)
CNPJ	– Cadastro Nacional de Pessoa Jurídica
CPF	– Cadastro Nacional de Pessoa Física
DNS	– <i>Domain Name System</i> (Sistema de Nomes de Domínio)
EJ	– Empresa Júnior
FTP	– <i>File Transfer Protocol</i> (Protocolo de Transferência de Arquivos)
GB	– Gigabytes
GNOME	– <i>GNU Network Object Model Environment</i> (Ambiente de Modelo de Objeto de Rede da GNU)
GNU	– <i>GNU's Not Unix</i> (GNU Não é Unix)
GPL	– <i>General Public Licence</i> (Licença Pública Geral)
HP	– Hewlett Packard
HTML	– <i>Hyper Text Markup Language</i> (Linguagem de Marcação de Hipertexto)
HTTP	– <i>Hyper Text Transfer Protocol</i> (Protocolo de Transferência de Hipertexto)
HTTPS	– <i>Secure Hyper Text Transfer Protocol</i> (Protocolo de Transferência de Hipertexto Seguro)
IBM	– <i>International Business Machines Corporation</i> (Corporação Internacional de Máquinas de Negócios)
ICMP	– <i>Internet Control Message Protocol</i> (Protocolo de Controle de Mensagens de Internet)
IFPR	– Instituto Federal do Paraná
IMAP	– <i>Internet Message Access Protocol</i> (Protocolo de Acesso de Mensagens de Internet)
IMAPS	– <i>Secure Internet Message Access Protocol</i> (Protocolo de Acesso de Mensagens de Internet Seguro)
IP	– <i>Internet Protocol</i> (Protocolo de Internet)
IPV4	– <i>Internet Protocol Version 4</i> (Versão 4 do Protocolo de Internet)
IPV6	– <i>Internet Protocol Version 6</i> (Versão 6 do Protocolo de Internet)
ISO	– <i>International Organization for Standardization</i> (Organização Internacional de Normalização)
KDE	– <i>K Desktop Environment</i> (Ambiente de Desktop K)
LAN	– <i>Local Area Network</i> (Área de Rede Local)
LDA	– <i>Local Delivery Agent</i> (Agente de Entrega Local)

LDAP	– <i>Lightweight Directory Access Protocol</i> (Protocolo Leve de Acesso ao Diretório)
LMTP	– <i>Local Mail Transfer Protocol</i> (Protocolo de Transferência de Correio Local)
LTPD	– <i>Local Transfer Protocol Daemon</i> (Serviço do Protocolo de Transferência Local)
LTS	– <i>Long Term Service</i> (Serviço de Longo Prazo)
MIME	– <i>Multipurpose Internet Mail Extensions</i> (Extensões de Correio de Internet Multiuso)
MDA	– <i>Mail Delivery Agent</i> (Agente de Entrega de Correio)
MTA	– <i>Mail Transport Agent</i> (Agente de Transporte de Correio)
MUA	– <i>Mail User Agent</i> (Agente de Usuário de Correio)
NAT	– <i>Network Address Translation</i> (Tradução de Endereços de Rede)
NTP	– <i>Network Time Protocol</i> (Protocolo de Tempo de Rede)
PAM	– <i>Pluggable Authentication Modules</i> (Módulos de Autenticação Plugáveis)
PGP	– <i>Pretty Good Privacy</i> (Privacidade Muito Boa)
PHP	– <i>Hypertext Preprocessor</i> (Pré Processador de Hipertexto)
POP3	– <i>Post Office Protocol</i> (Protocolo de Correio)
POP3S	– <i>Secure Post Office Protocol</i> (Protocolo de Correio Seguro)
POSIX	– <i>Portable Operating System Interface</i> (Interface de Sistema Operacional portátil)
PTR	– <i>Pointer Record</i> (Registro de Ponteiro)
SASL	– <i>Simple Authentication and Security Layer</i> (Camada Simples de Autenticação e Segurança)
SCP	– <i>Secure Copy Protocol</i> (Protocolo de Cópia Segura)
SFTP	– <i>Secure File Transfer Protocol</i> (Protocolo Seguro de Transferência de Arquivos)
SMB	– <i>Server Message Block</i> (Bloco de Mensagens do Servidor)
SMTP	– <i>Simple Mail Transfer Protocol</i> (Protocolo Simples de Transferência de Correio)
SNMP	– <i>Simple Network Management Protocol</i> (Protocolo Simples de Gerenciamento de Rede)
SO	– Sistema Operacional
SQL	– <i>Structured Query Language</i> (Linguagem de Consulta Estruturada)
SSH	– <i>Secure Socket Shell</i> (Encapsulamento de Conexão Segura)
SSL	– <i>Secure Sockets Layer</i> (Camada de Segurança de Conexões)
SVID	– <i>The System V Interface Description</i> (A descrição da interface do Sistema V)
TADS	– Tecnólogo em Análise e Desenvolvimento de Sistemas
TCC	– Trabalho de Conclusão de Curso

- TCP – *Transfer Control Protocol* (Protocolo de Controle de Transferência)
- TI – Tecnologia da Informação
- TLS – *Transport Layer Security* (Camada de Transporte de Segurança)
- UDP – *User Datagram Protocol* (Protocolo de Datagrama do Usuário)
- UNIX – *Uniplexed Information and Computing Service* (Informação Uniplex e Serviço de Computação)
- UTF8 – *UCS Transformation Format 8* (Transformação UCS Formato 8)
- WSL – *Windows Subsystem for Linux* (Subsistema do Windows para Linux)

SUMÁRIO

1	OBJETIVO	17
1.1	GERAL	17
1.2	ESPECÍFICOS	17
2	REFERENCIAL TEÓRICO	18
2.1	SISTEMA OPERACIONAL LINUX.....	18
2.2	COMPARATIVO ENTRE AS PRINCIPAIS DISTRIBUIÇÕES LINUX.....	20
2.3	A DISTRIBUIÇÃO UBUNTU	21
2.4	NETFILTER	22
2.5	OPENSSSH.....	23
2.6	WEBMIN	24
2.7	APACHE	25
2.8	PHP.....	25
2.9	MARIADB	26
2.10	PHPMYADMIN	27
2.11	WORDPRESS	27
2.12	POSTFIX.....	29
2.13	DOVECOT.....	30
2.14	SQUIRRELMAIL.....	31
2.15	LET'S ENCRYPT.....	32
2.16	REGISTRO DE DOMÍNIO	32
3	DESENVOLVIMENTO	34
3.1	METODOLOGIA.....	34
3.2	ETAPA PRELIMINAR PARA A INSTALAÇÃO DO SISTEMA OPERACIONAL	34
3.3	INSTALAÇÃO DO UBUNTU	35
3.4	INSTALAÇÃO DO WEBMIN	40
3.5	INSTALAÇÃO DO LAMP-SERVER	41
3.6	INSTALAÇÃO DO MARIADB	42
3.7	INSTALAÇÃO DO PHPMYADMIN	42
3.8	INSTALAÇÃO DO WORDPRESS	43
3.9	INSTALAÇÃO DO POSTFIX	46
3.10	INSTALAÇÃO DO DOVECOT	50

3.11	INSTALAÇÃO DO SQUIRRELMAIL	53
3.12	PROCESSO DE REGISTRO DE DOMÍNIO	54
3.13	INSTALAÇÃO E OBTENÇÃO DO CERTIFICADO DE CRIPTOGRAFIA.....	56
3.13.1	Instalação do Certificado de Criptografia no Postfix.....	57
3.13.2	Instalação do Certificado de Criptografia no Dovecot	58
3.13.3	Instalação do Certificado de Criptografia no Webmin	59
3.14	INSTALAÇÃO E CONFIGURAÇÃO DO FIREWALL NETFILTER	60
4	RESULTADOS	62
4.1	SISTEMA OPERACIONAL UBUNTU	62
4.2	ACESSO REMOTO SEGURO.....	62
4.3	GERENCIADOR ADMINISTRATIVO WEBMIN	63
4.4	SERVIDOR DE PÁGINAS HTTP APACHE	63
4.5	SUORTE À LINGUAGEM DE PROGRAMAÇÃO PHP PELO APACHE	64
4.6	BANCO DE DADOS RELACIONAL MARIADB.....	64
4.7	INTERFACE DE GERENCIAMENTO REMOTO PARA BANCO DE DADOS PHPMYADMIN.....	65
4.8	SISTEMA DE GERENCIAMENTO DE CONTEÚDO WORDPRESS	65
4.9	SERVIDORES DE CORREIO ELETRÔNICO POSTFIX E DOVECOT	66
4.10	SERVIÇO DE WEBMAIL SQUIRRELMAIL.....	67
4.11	CERTIFICAÇÃO DE SEGURANÇA.....	67
4.12	REGISTRO DE DOMÍNIO	68
4.13	HOSPEDAGEM DA PÁGINA INSTITUCIONAL.....	69
5	CONSIDERAÇÕES FINAIS	70
5.1	TRABALHOS FUTUROS.....	71
	REFERÊNCIAS BIBLIOGRÁFICAS	72

INTRODUÇÃO

Ao final do ano de 2019, deu-se início ao projeto Empresa Júnior (EJ) no Instituto Federal do Paraná (IFPR), campus União da Vitória. Este projeto tem como finalidade trazer a experiência de uma empresa real aos alunos, com todas as suas funcionalidades, obrigações legais e objetivos.

Uma EJ tem seu funcionamento exatamente igual a qualquer empresa, diferenciando-se apenas por não trazer renda direta aos seus participantes. Toda e qualquer renda obtida em função do trabalho efetuado reverte-se em investimento educacional aos alunos participantes e/ou infraestrutura para a própria empresa.

Este projeto foi iniciado com a turma do 2º período do curso Tecnólogo em Análise de Desenvolvimento de Sistemas (TADS).

Com todo o trabalho burocrático já realizado, surgiu a necessidade de um espaço físico para a empresa dentro do campus, assim como a infraestrutura para iniciar seu funcionamento. O campus disponibilizou este espaço e também mesas, cadeiras, armários, computadores e infraestrutura de rede. Porém, surgiu a necessidade de um servidor de rede para suprir a demanda de hospedagem do *site*, do domínio de Internet, dos *e-mails*, do servidor de arquivos, e do banco de dados institucional.

Como a empresa não possuía um computador que atendesse os requisitos de *hardware* para implantar todos esses serviços, foi submetido um projeto à Pró-reitoria de Extensão e Cultura do IFPR. Após sua aprovação, a EJ recebeu um servidor, um computador de mesa, um rack/bastidor, e um roteador de rede, correspondendo ao montante de R\$17.000,00.

Com a chegada de todos estes materiais, iniciou-se a montagem e implantação de toda a infraestrutura da EJ, assim como a instalação do Sistema Operacional no servidor e seus demais serviços.

1 OBJETIVO

Conforme solicitado pela empresa Forceteck JR Soluções, um servidor *web* funcional deverá ser instalado e conter os seguintes serviços: *Webmail*; Certificado de Criptografia; *Framework* para desenvolvimento de *sites*; *Firewall*. Bem como as Linguagens de Programação Python, Perl, PHP, e para isso são propostos os seguintes objetivos:

1.1 GERAL

Implantar um servidor de rede, baseado totalmente em *softwares* livres (gratuitos), para suprir a demanda de funcionalidades necessárias à empresa Forceteck JR Soluções.

1.2 ESPECÍFICOS

- Fazer o levantamento bibliográfico referente a pesquisa;
- Selecionar o Sistema Operacional e os softwares subsequentes;
- Efetuar a instalação e configuração do Sistema Operacional e *softwares* servidores necessários;
- Identificar se o servidor cumpre todos os requisitos relacionados às necessidades de uso da empresa Forceteck JR Soluções.
- Avaliar a performance e usabilidade do Servidor;
- Efetuar testes de segurança e mitigar quaisquer falhas devido a configuração ou atualização de software;

2 REFERENCIAL TEÓRICO

Este Capítulo descreve o Sistema Operacional e os demais *softwares* essenciais para dar início ao projeto de implantação do servidor.

2.1 SISTEMA OPERACIONAL LINUX

Linux é um sistema operacional desenvolvido por Linus Torvalds em conjunto com centenas de interessados, incluído voluntários de empresas como IBM e HP, com capacidade de rodar em múltiplas arquiteturas, em conjunto com ferramentas de terceiros (ex. Apache, KDE, PHP, GNU). Esta junção de *softwares*, *Kernel* Linux com *softwares* de terceiros, formam um robusto e flexível Sistema Operacional. Seu desenvolvimento iniciou-se em 1991, e desde então vem se disseminando pelo mundo, sendo usado não somente em servidores como atualmente, em *desktops* (computadores para usuários finais com SO baseado em interface gráfica) por ser uma alternativa aos SOs proprietários. Pode ser definido como “...sistema operacional de código-fonte aberto tipo UNIX, que reflete uma combinação de conformidade de padrões com o SVID, o POSIX e o BSD” (NEGUS, 2014).

O Linux é distribuído de forma livre pela Internet sob a Licença Pública Geral (GPL). Isso significa que qualquer pessoa pode executar, estudar, compartilhar e modificar o *software*. Porém, há também empresas que comercializam versões mais estáveis e com suporte pago com foco no mercado corporativo.

Existem inúmeras distribuições Linux. Estas distribuições englobam desenvolvedores voluntários e/ou empresas que trabalham em conjunto desenvolvendo versões melhoradas e customizadas conforme a necessidade. Há distribuições voltadas exclusivamente para servidores bem como as que têm como objetivo o uso em *desktops*. Algumas das mais populares distribuições são: Red Hat, Debian, Fedora, CentOS, Suse, Ubuntu.

Além do Linux poder ser executado em praticamente qualquer tipo de arquitetura, a necessidade de um *hardware* mais robusto nem sempre é requisito para seu funcionamento. Algumas versões minimalistas executam em roteadores domésticos, celulares, e dispositivos portáteis.

Outra vantagem em relação a outros SOs é a baixa incidência de vírus. A forma como o sistema foi projetado evita a disseminação de vírus pelo sistema, graças às características que enjaulam um processo de *software*, evitando que o programa

mal-intencionado venha a afetar outras áreas do SO. Diferente do SO Microsoft Windows, o Linux não possui um arquivo de registros, onde todas as aplicações, suas configurações, suas permissões são armazenadas. Ponto vulnerável onde pode haver um ataque.

Praticamente pode considerar-se que é um SO de alta disponibilidade e estabilidade. Permite, em sua maioria, instalação, atualização, parada e início de serviços, sem desligar a máquina. Evitando assim tempo em que os serviços ficariam indisponíveis. Há relatos de servidores Linux funcionando por meses, e até mesmo anos, sem necessidade de reiniciar a máquina uma única vez.

Atualizações de segurança, performance e correção de *bugs* são lançadas periodicamente, mensalmente, e em alguns casos até semanalmente. Em versões denominadas LTS (*Long Term Service/Serviço de Longo Prazo*), estas atualizações são tratadas de forma mais minuciosa, visando a estabilidade e o suporte por um período maior de tempo. É a escolha a ser feita quando se trata de uma implantação para uso comercial e/ou corporativo.

O Linux pode executar em *hardware* físico e também pode ser implementado utilizando máquinas virtuais, possibilitando o trabalho de várias instâncias em conjunto ou em paralelo. É amplamente utilizado em plataformas de Computação em Nuvem, oferecendo escalabilidade, balanceamento de carga, e tolerância a falhas. Empresas como o Google Cloud e Amazon AWS, utilizam-se do Linux para prover serviços no formato de Contêineres (ambiente isolado, disposto em um servidor, que divide um único host de controle) ou Kubernetes (produto de código aberto utilizado para automatizar a implantação, o dimensionamento e o gerenciamento de aplicativos em contêiner). O próprio Linux tem a capacidade de prover e gerenciar máquinas virtuais, dele mesmo ou de outros SOs.

Devido a todos estes fatores acima, empresas desenvolvedoras de SOs estão gradualmente implementando partes do código original *Kernel* do Linux em seus próprios SOs. Como é o caso da Microsoft, que implantou recentemente no Microsoft Windows 10 o *Powershell*, que se assemelha ao terminal de texto do Linux, e o WSL. WSL é a sigla para *Windows Subsystem for Linux* (Subsistema do Windows para Linux). O WSL permite que os usuários executem um ambiente Linux diretamente no Microsoft Windows, sem a necessidade de execução de uma máquina virtual completa ou instalação de inicialização dupla.

Uma vasta documentação é disponibilizada pela internet em formato de tutoriais, artigos, fóruns, página de suporte de desenvolvedores, páginas de manual dos próprios *softwares*. Inúmeros livros são encontrados em meios físicos e virtuais, abrangendo desde recursos mais simples até implementações mais complexas.

Todos os fatores relacionados impactaram diretamente na escolha do SO Linux, por sua gratuidade, estabilidade, segurança, periodicidade em atualizações e correções de erros, performance em geral, requisitos mínimos de *hardware*, ampla documentação, diversos serviços de rede disponível, englobando praticamente todos os protocolos de rede mais utilizados (TCP/IP v4 e v6, SSH, FTP, HTTP, DNS, SNMP, POP3, SMTP, IMAP, SMB, NTP, Firewall, etc.). O Linux é o SO que preenche todos os requisitos para as necessidades de um servidor de rede para a empresa Forcotech JR Soluções.

2.2 COMPARATIVO ENTRE AS PRINCIPAIS DISTRIBUIÇÕES LINUX

No Quadro 1 e Quadro 2, estão listadas as principais distribuições Linux mais utilizadas no mercado com os seus prós e contras, segundo Smith (2022).

Quadro 1 - Distribuições Linux

Distribuição	Prós	Contras
CentOS	Semelhante ao Red Hat Enterprise Linux, possível campo de testes para <i>software</i> que será usado em ambientes Red Hat.	Faltam as tecnologias Linux mais recentes; ocasionalmente, o projeto não cumpre sua promessa de fornecer atualizações de segurança oportunas e novas versões estáveis.
Ubuntu	Ciclo de lançamento fixo e período de suporte; variantes de suporte de longo prazo (LTS) com cinco anos de atualizações de segurança; amigável para iniciantes; riqueza de documentação.	Falta compatibilidade com o Debian; grandes mudanças frequentes tendem a afastar alguns usuários; versões não LTS vêm com apenas nove meses de suporte de segurança.

Fonte: (SMITH, 2022)

Quadro 2 – Distribuições Linux – complemento do Quadro 1 - página 20

Distribuição	Prós	Contras
Debian	Muito estável; controle de qualidade notável; inclui mais de 30.000 pacotes de <i>software</i> ; suporta mais arquiteturas de processador do que qualquer outra distribuição Linux.	Conservador - devido ao seu suporte a muitas arquiteturas de processador, as tecnologias mais recentes nem sempre são incluídas; ciclo de lançamento lento (um lançamento estável a cada 2 - 3 anos).
Fedora	Altamente inovador; Recursos de segurança excepcionais; grande número de pacotes suportados; adesão estrita à filosofia do <i>software</i> livre; disponibilidade de rodadas ao vivo com muitos ambientes de desktop populares.	As prioridades do Fedora tendem a se inclinar para os recursos corporativos, em vez da usabilidade do desktop; alguns recursos de ponta, como a mudança antecipada para o KDE 4 e o GNOME 3, ocasionalmente alienam alguns usuários de desktop.
openSUSE	Ferramenta de configuração abrangente e intuitiva; grande repositório de pacotes de <i>software</i> , excelente infraestrutura de web site e documentação impressa, Btrfs com ambientes de inicialização por padrão.	Sua configuração de desktop com muitos recursos e utilitários gráficos às vezes são vistos como "inchados e lentos".

Fonte: (SMITH, 2022)

2.3 A DISTRIBUIÇÃO UBUNTU

O Linux Ubuntu foi selecionado para este trabalho por possuir versões específicas para servidor, contendo atualizações de segurança de longo período (5 anos), extensível por mais 2 anos, após registro da instalação na empresa desenvolvedora (CANONICAL LTD, 2022).

Servidor é uma máquina da rede que oferece um serviço qualquer para tal rede. Cliente é uma máquina da rede que usa os serviços oferecidos pelos servidores. Podemos também atribuir os nomes cliente e servidor aos programas que utilizam ou disponibilizam os serviços da rede. Por exemplo: o Mozilla Thunderbird e o Outlook Express são dois clientes de e-mail muito conhecidos. Já o Sendmail e o Postfix são excelentes servidores de e-mail (MOTA FILHO, 2013, p. 38).

Outro motivo da escolha foi que o Ubuntu possui todos os pacotes de *softwares* e as linguagens de programação que correspondem às solicitações feitas pela empresa Forceteck JR Soluções.

O Ubuntu tem uma excelente documentação baseada no estilo da página Wikipedia (CREATIVE COMMONS, 2022), facilidade na criação de relatório de erros e abordagem profissional para os usuários finais.

Nos últimos anos, o Ubuntu causou uma reviravolta no mundo da informática e do *software* de código aberto. Do nada, o "Pequeno Sistema Operacional com Potencial" se tornou um sistema completo para desktops e servidores que ganhou o coração de milhões de usuários pelo mundo. Além da plataforma técnica consistente e de um impressionante compromisso com a qualidade, o sucesso do Ubuntu também se deve à sua gigantesca comunidade de usuários entusiastas que ajudam a prestar suporte, a criar documentação e a testar cada milímetro do universo Ubuntu (HILL; BACON, 2009).

2.4 NETFILTER

A solução nativa de segurança disponibilizada pelo *kernel* do SO Linux é o Netfilter. É o *software* responsável pelo *firewall*, que se utiliza da ferramenta iptables para gerenciamento das conexões de rede.

O *firewall* é o *software* de maior importância para a segurança do servidor, tem como principal função a primeira linha de defesa contra possíveis ataques de pessoas e/ou *softwares* mal intencionados (vírus, *malware*, *ransomware*, etc.), ataques de negação de serviço, acessos não solicitados por pessoas não autorizadas em portas TCP/UDP, esquecidas abertas, ou abertas por *softwares* maliciosos do tipo porta dos fundos.

Porém o *firewall* não se resume somente a esta linha de defesa, tem inúmeras outras finalidades/funcionalidades. Podem ser citadas entre elas: tradução de endereços de rede; redirecionamento de portas e endereços usando técnicas de tradução de endereços de rede de origem e destino; marcação de pacotes de rede; redirecionamento de rotas baseado em marcação de pacotes; balanceamento de carga utilizando marcação de pacotes e redirecionamento de rotas; rastreamento de conexões TCP/UDP para depuração de rede.

O kernel Linux apresenta um poderoso subsistema de rede chamado Netfilter. O subsistema Netfilter fornece filtragem de pacotes com ou sem estado, bem como serviços de mascaramento de NAT e IP. O Netfilter também tem a capacidade de manipular as informações do cabeçalho IP para roteamento avançado e gerenciamento de estado de conexão (FEDORA DOCUMENTATION PROJECT, 2010).

2.5 OPENSSSH

É a ferramenta essencial para acesso remoto ao servidor, pois sem o OpenSSH, a administração do servidor só pode ser feita localmente.

O OpenSSH é o *software* cliente/servidor, responsável pelo acesso remoto seguro por terminal de texto, utilizando o protocolo SSH. Sua função é criptografar todo o tráfego de conexões remotas, para eliminar espionagem, sequestro de conexão e outros ataques. Além disso, oferece um grande conjunto de recursos de encapsulamento seguro, vários métodos de autenticação e opções de configuração complexas.

SSH, o Secure Shell, é uma abordagem popular, poderosa e baseada em *software* para segurança de rede. Sempre que os dados são enviados por um computador para a rede, o SSH os criptografa (embaralha) automaticamente. Então, quando os dados chegam ao destinatário pretendido, o SSH automaticamente descriptografa (desembaralha) ele. O resultado é uma criptografia transparente: os usuários podem trabalhar normalmente, sem saber que suas comunicações estão criptografadas com segurança na rede. (BARRETT; SILVERMAN; BYRNES, 2005).

O conjunto de *softwares* que compõem o OpenSSH consiste em ferramentas para acesso a clientes remotos (SSH), para transferência de arquivos de modo seguro (SCP e SFTP). No conjunto de ferramentas de servidor, contém o próprio servidor SSH (sshd), servidor de transferência de arquivos seguros (sftp-server e ssh-agent). Gerenciamento de chaves de criptografia são feitos com ssh-add, ssh-keysign, ssh-keyscan e ssh-keygen.

O OpenSSH é disponibilizado sob uma licença BSD (*Berkeley Source Distribution*), que é um tipo de licença de baixa restrição para *software* de código aberto que não impõe requisitos de redistribuição.

Executa por padrão na porta 22/TCP IPv4 e IPv6, e esta porta pode ser alterada para qualquer outra porta disponível, a fim de dificultar possíveis tentativas de invasão remota ao SO.

Nos primórdios das redes de computadores e da Internet, usava-se o protocolo Telnet, que executava na porta 23/TCP. Era a solução que implantava um acesso ao terminal de texto remoto de uma máquina e/ou dispositivo de rede (Roteadores, *Switches*, *Modems*, etc.), e permitia acessar arquivos, efetuar configurações, monitoramento, adicionar e remover usuários, entre outros.

Telnet é um dos protocolos de aplicação mais antigos usados na Internet, e sua origem está ligada à rede ARPANET. A história do Telnet remonta a 1969, quando a palavra "Telnet" surgiu como um acrônimo para Protocolo de Rede de Telecomunicações. O RFC 764 padronizou o Telnet em 1980 e o RFC 854 o substituiu em 1983. O protocolo Telnet é usado para emular um terminal de caracteres convencional (por exemplo, o lendário VT100) em redes de computadores baseadas em TCP/IP (DOSTÁLEK; KABELOVÁ, 2006).

Porém o protocolo Telnet apesar de muito útil, apresentava uma falha grave no sentido de segurança. Todas as transmissões de dados feitas pelo Telnet ocorriam de forma não criptografada, isto quer dizer que qualquer pessoa com algum conhecimento avançado conseguiria capturar os pacotes de rede e obter informações confidenciais como nome de usuários, senhas, e o próprio conteúdo de dados transmitido.

Antes do surgimento de equipamentos de rede do tipo *Switch*, as conexões de redes eram gerenciadas por *Hubs*, equipamentos que replicavam todos os pacotes de rede que recebiam para todas as portas físicas conectadas a ele, facilitando muito a captura destes pacotes por pessoas mal-intencionadas.

A solução para esta brecha de segurança seria implantar um novo método de acesso remoto com as mesmas características do Telnet, porém com as suas transmissões de dados criptografadas. Desta necessidade surgiu o protocolo SSH, que é disponibilizado em distribuições Linux pelo *software* cliente/servidor OpenSSH.

2.6 WEBMIN

Para facilitar a administração do servidor, foi solicitado pela empresa Forcotech JR Soluções, uma *interface* de gerenciamento gráfica. Um dos *softwares* que se enquadram nesta requisição é o Webmin.

Webmin é um serviço de administração local e remoto, que executa sobre um servidor HTTP, por padrão na porta 10000/TCP, com ou sem criptografia. Fornece uma interface gráfica intuitiva com um painel principal, onde todas as funções e configurações possíveis do servidor ficam subdivididas em categorias e classes.

Uma das tarefas mais árduas em se tratando de servidores é a parte de administração. Como descrito no Capítulo 2.5, este gerenciamento pode ser feito através do terminal remoto utilizando o protocolo SSH. Porém esta maneira de administrar, mesmo sendo muito eficiente, comumente requer conhecimentos técnicos avançados por parte do administrador, em comandos do terminal de texto do Linux, suas funções, e em ferramentas de instalação e configuração.

Webmin é uma interface baseada na web para administração de sistemas para Unix. Usando qualquer navegador que suporte tabelas e formulários (e Java para o módulo Gerenciador de Arquivos), você pode configurar contas de usuário, Apache, DNS, compartilhamento de arquivos e assim por diante. (CAMERON, 2016).

2.7 APACHE

O Apache foi selecionado neste trabalho para a função de servidor de páginas http, para hospedar o *site* institucional da empresa Forcetech JR Soluções. Também é necessário como plataforma para execução de outros serviços requisitados como, *framework* de desenvolvimento de *sites*, *webmail*, administração remota de banco de dados.

Tem suporte a várias linguagens de programação como PHP, Perl, CGI e Python. Possui módulos de diversas funcionalidades como conexão a banco de dados MySQL, MariaDB, PostgreSQL, etc. É amplamente documentado e tem suporte integrado de outros projetos de *software*.

É executado sobre os protocolos IPv4 e IPv6, por padrão responde requisições nas portas 80/TCP para http sem criptografia, e/ou na porta 443/TCP para https com criptografia, utilizando certificados gratuitos ou proprietários.

Suporta criação de anfitriões virtuais, possibilitando a hospedagem de vários *sites* simultaneamente, de domínios de internet diferentes, em um único servidor.

O Apache HTTP Server Project é um esforço colaborativo de desenvolvimento de *software* destinado a criar uma implementação de código-fonte robusta, de nível comercial, com recursos e disponível gratuitamente de um servidor HTTP (Web) (THE APACHE SOFTWARE FOUNDATION, 2022).

Embora o Apache HTTP seja visto com mais frequência em execução no Linux, pode-se implantar o Apache no SO Apple OS X e no SO Microsoft Windows. O Apache é licenciado sob a Licença Apache versão 2. Usa uma arquitetura modular, na qual módulos extras podem ser carregados para estender seus recursos.

2.8 PHP

Segundo o *site* do projeto The PHP Group (2022), o PHP (um acrônimo recursivo para PHP: *Hypertext Preprocessor*) é uma linguagem de *script* de código aberto de uso geral, muito utilizada, e especialmente adequada para o desenvolvimento *web* e que pode ser embutida dentro do HTML.

O PHP é um requisito necessário para que o sistema de gerenciamento de conteúdo WordPress possa funcionar.

O PHP é uma linguagem de programação que pré processa os *scripts* das páginas dinâmicas no lado do servidor, e entrega ao programa cliente do usuário um resultado totalmente em HTML, abstraindo toda a parte de programação. E como este processamento é feito todo do lado do servidor, a página entregue ao cliente é muito mais leve e ágil de ser carregada, requerendo poucos recursos da máquina do usuário.

Em contrapartida, o servidor onde o PHP executa, exige que o *hardware* seja suficiente para que não haja gargalos em termos de performance e processamento. Para cumprir estes requisitos, foi selecionada uma máquina de alto poder de processamento, com memória e disco suficientes para sua implantação.

O PHP foi construído baseado em uma estrutura de módulos, que podem ser instalados e habilitados conforme a necessidade do projeto. Dentre estes módulos, podemos destacar o “php-mysql”, que irá fazer a conexão entre o sistema de gerenciamento de conteúdo WordPress com o banco de dados do servidor.

Desde sua criação, o PHP passou por várias atualizações e versões e atualmente está na sua versão 8.1. Por vários anos a versão mais utilizada foi o PHP 5, porém por necessidade de melhor performance e segurança, foram lançadas várias versões do PHP 7, que trouxe um aumento significativo em sua performance. Como o PHP 8 é recente, ainda não há dados suficientes para mensurar os benefícios desta nova versão. Neste caso, será utilizado o PHP 7 neste trabalho.

2.9 MARIADB

O MariaDB é um servidor de banco de dados relacional de código aberto, que pode servir como substituto ao MySQL. Apesar de que o MySQL ainda seja fornecido em versões gratuitas em distribuições Linux, não há quaisquer garantias de que futuramente estas versões continuem a existir, visto que o MySQL é de propriedade da empresa Oracle, que comercializa o MySQL. Por este motivo, foi escolhido o MariaDB para este trabalho.

É necessário para a instalação do sistema de gerenciamento de conteúdo WordPress, e para hospedagem de banco de dados utilizados por desenvolvedores de *software* da empresa Forcetech JR Soluções.

É compatível com banco de dados MySQL, facilitando a migração de dados entre servidores. Qualquer banco de dados desenvolvido em MySQL pode ser importado diretamente para o MariaDB, sem necessidade de qualquer alteração na sua estrutura.

Por padrão, o servidor MariaDB executa na porta 3306/TCP IPv4 e IPv6. Tem suporte a conexões seguras utilizando certificados de criptografia. Sua estrutura não permite que o servidor seja executado utilizando o usuário raiz do sistema, protegendo o servidor contra brechas de segurança.

O MariaDB é uma ramificação do MySQL, iniciado quando o MySQL foi adquirido pela Sun Microsystems em 2008. A Sun Microsystems e o MySQL foram adquiridos pela Oracle em 2009. Na maioria das distribuições Linux, o MariaDB agora é o pacote padrão, fornecendo um banco de dados relacional compatível com o MySQL. O MariaDB tem novos recursos interessantes, melhores testes, melhoria de desempenho e correções de bugs que não estão disponíveis no MySQL (RAZZOLI; KENLER, 2015).

2.10 PHPMYADMIN

A instalação do phpMyAdmin foi solicitada pela empresa Forceteck JR Soluções, com o objetivo de uma interface de gerenciamento de banco de dados única e exclusivamente para acesso a desenvolvedores de *software* da empresa, por motivos de segurança, visto que o phpMyAdmin somente dá acesso ao gerenciamento do servidor de banco de dados, e não a outros serviços do servidor.

O phpMyAdmin é uma *interface* gráfica *web* para administração de banco de dados. Permite efetuar todas as operações possíveis dentro de um banco de dados. Possui ferramentas interativas de criação que geram novos bancos de dados sem a necessidade de o usuário escrever código de programação SQL.

phpMyAdmin é uma aplicação web escrita em PHP; ele contém (como a maioria dos aplicativos da web) código cliente XHTML, CSS e JavaScript. Este aplicativo fornece uma interface web completa para administrar bancos de dados MySQL (DELISLE, 2012).

2.11 WORDPRESS

O WordPress é um *framework* para hospedagem, desenvolvimento e implantação de páginas *web*, sendo uma plataforma de gerenciamento de conteúdo dinâmico para *websites*. Sua instalação foi solicitada para servir de plataforma de desenvolvimento do *site* institucional da empresa Forceteck JR Soluções.

O WordPress começou em 2003 quando Mike Little e Matt Mullenweg criaram uma ramificação do b2/cafelog. A necessidade de um sistema de publicação pessoal elegante e bem arquitetado era clara desde então. Hoje, o WordPress é construído em PHP e MySQL e licenciado sob a GPLv2. É também a plataforma escolhida por mais de 43% de todos os sites na web. (WORDPRESS.ORG, 2022).

No início de seu desenvolvimento, o objetivo inicial do WordPress era servir de plataforma para *blogs*, que teriam seu conteúdo adicionado periodicamente, sem a necessidade de se desenvolver código HTML específico e de conhecimento técnico. O usuário acessava sua interface de administração, onde um painel intuitivo fornecia as ferramentas básicas para edição de texto e inserção de imagens. Com apenas alguns cliques do usuário, a notícia era postada automaticamente.

Com o passar dos anos, sua popularidade e utilização aumentou, e seus desenvolvedores implantaram outros módulos no WordPress, que de antemão só servia para *blogs*, para também servir de plataforma para publicação de páginas estáticas na Internet.

O que também colaborou muito para a sua popularidade foi a possibilidade de instalação de *plugins* para prover outras funções. *Plugins* de tradução, edição, formulários automatizados, comércio eletrônico, entre outros, trouxeram inúmeros mecanismos para o WordPress, tornando-o um *framework* completo para qualquer tipo de *site*.

Atualmente conta com mais de 55.000 *plugins* publicados em sua página oficial (WORDPRESS.ORG, 2022), dentre os quais inúmeros são gratuitos e/ou possuem versões *lite*, que são versões que incluem somente recursos básicos, e versões *pro* que entregam recursos adicionais.

O WordPress tem suporte a temas gratuitos e pagos. No *site* ThemeForest (ENVATO PTY LTD, 2022), 11.000 temas para WordPress fazem parte de seu portfólio de venda. Os temas são desenvolvidos para diversos fins, desde uma loja de produtos eletrônicos, pizzarias, fábricas de sorvete, *sites* institucionais, comércio eletrônico, *sites* pessoais, entre outros.

Quando o tema tem uma classificação *Premium*, além do visual gráfico personalizado, pode conter outros *plugins* embutidos e outras funcionalidades, como por exemplo um *Banner Slider*. Os temas pagos custam entre U\$30,00 e U\$150,00, e em alguns casos, podem passar facilmente deste valor.

2.12 POSTFIX

O Postfix é parte do conjunto de *softwares* responsáveis pela hospedagem, envio e recebimento de *e-mail* para o domínio institucional da empresa Forcetech JR Soluções.

Seu desenvolvimento foi feito com o objetivo de ser um servidor de *e-mails* mais leve, de fácil configuração, tolerante a falhas do sistema. Sua estrutura modular o torna muito mais estável e confiável que o MTA Sendmail. Consome menos recursos de memória e processamento.

O Postfix foi originalmente concebido como um substituto para o Sendmail difundido. Seu design elimina muitas oportunidades para problemas de segurança. O Postfix também elimina grande parte da complexidade que vem com o gerenciamento de uma instalação do Sendmail. A administração do Postfix é gerenciada com dois arquivos de configuração simples, e o Postfix foi projetado desde o início para lidar com problemas inesperados de *hardware* ou *software* (DENT, 2004).

O Postfix é um *software* popular gratuito e de código aberto que atua como um agente de transporte de *e-mail*, utilizando o protocolo SMTP. O trabalho do Postfix é rotear e entregar *e-mails*. Além do uso clássico, o Postfix também pode ser configurado para enviar *e-mails* apenas por aplicativos locais. Esta aplicação do Postfix é útil para implantar em várias situações. Pode ser usado ao enviar notificações por *e-mail* regularmente, trabalhando com um provedor de serviços de *e-mail* de terceiros com tráfego de saída limitado.

O Postfix é executado sobre os protocolos IPv4 e IPv6, responde requisições nas portas 25/TCP e 587/TCP. A porta 25 é somente utilizada para a intercomunicação entre servidores de *e-mail*, enquanto a porta 587 é utilizada apenas para submissão dos clientes de *e-mail*. Pode operar em conexões com e sem criptografia. No caso de uso de criptografia, utiliza os tipos de encriptação TLS/SSL SSLV2, SSLV3.

Possui vários tipos de tabelas de configurações de filtros para *e-mail*, desde checagem dos cabeçalhos das mensagens, dos remetentes, dos anfitriões, listas negras de *spams*, verificação de domínios, filtragem de conteúdo da mensagem, checagem de vírus usando *softwares* adicionais de terceiros.

Atende tanto a domínios únicos e principais, como a outros domínios secundários e/ou virtuais simultaneamente. Pode utilizar recursos de conexão a bancos de dados para verificação de autenticação de usuários, assim como conexão a bancos de dados SQL ou a servidores de diretório ativo, como o LDAP, por exemplo.

2.13 DOVECOT

Em conjunto com o Postfix, o Dovecot desempenhará a função de entrega dos e-mails institucionais da empresa Forceteck JR Soluções, para os *softwares* clientes de *e-mail*.

Desempenhando a função de um servidor IMAP e POP3, o Dovecot fornece uma maneira para que os *softwares* clientes de *e-mail* acessem seus *e-mails*. Assim, quando o *software* cliente de *e-mail* de um usuário entra em contato com o servidor de *e-mail*, o *software* que responde a essa solicitação é um servidor IMAP ou POP3.

Os servidores IMAP e POP3 recebem solicitações de *softwares* clientes de *e-mail* e respondem a estas solicitações acessando mensagens de *e-mail* armazenadas no servidor e transferindo-as aos clientes.

Dovecot é um dos agentes de entrega de correio (MDA) mais populares com suporte para protocolos IMAP e POP3. Funciona com os dois principais formatos de caixa de correio, nomeadamente mbox e Maildir (SAWANT, 2016).

O Dovecot não é responsável por receber *e-mails* de outros servidores, trata apenas dos *e-mails* que saem do armazenamento de mensagens local, indo para clientes IMAP e POP3, e mensagens que já foram recebidas pelo agente de transporte de *e-mail*, e que devem ser armazenadas localmente.

O POP3 é utilizado por usuários que não possuem uma conexão de alta velocidade com o servidor de *e-mail*. Um dos princípios básicos do POP3 é que os *softwares* clientes de *e-mail* baixem as mensagens e as armazenem localmente no computador do usuário, e então excluam as mensagens do servidor.

O IMAP destina-se a redes de área local e conexões de alta velocidade. A intenção do IMAP é entrar em contato com o servidor toda vez que uma determinada mensagem precisa ser lida. O Dovecot tem uma série de otimizações para IMAP que aumentam excepcionalmente seu desempenho.

Existem duas opções primárias de armazenamento de correio no Linux, o “mbox” e o “Maildir”. O “mbox” armazena várias mensagens, às vezes centenas ou milhares de mensagens, em um único arquivo. O “Maildir” armazena cada mensagem como um arquivo separado. Tanto o “mbox” quanto o “Maildir” têm amplo suporte em vários *softwares* de *e-mail*, incluindo agentes de transporte de *e-mail* e agentes de entrega de *e-mail*, e ambos são totalmente suportados pelo Dovecot. Dovecot também oferece seu próprio formato de caixa de correio de alto desempenho, o “dbox”.

O Dovecot suporta uma variedade de fontes de usuários e senhas, incluindo passwd, shadow, PAM, LDAP, SQL e Vpopmail. Geralmente, é selecionada uma fonte suportada por todas as partes da solução geral de *e-mail*, incluindo o agente de transporte de *e-mail*, agentes de entrega de *e-mail* e o Dovecot.

Tem suporte a autenticação no formato SASL (*Simple Authentication and Security Layer*/Camada Simples de Autenticação e Segurança). O SASL é uma lista de requisitos para mecanismos e protocolos de autenticação para serem compatíveis com SASL, conforme descrito na RFC 4422 por Melnikov e Zeilenga (2022). Os protocolos IMAP, POP3 e SMTP têm suporte para SASL.

Por padrão, responde requisições em portas 110/TCP para POP3, 143/TCP para IMAP, sem criptografia. Com criptografia, responde a requisições nas portas 993/TCP para IMAPS, e na porta 995/TCP para POP3S.

2.14 SQUIRRELMAIL

O Squirrelmail foi selecionado para este trabalho para suprir a solicitação de uma interface para acesso remoto (*webmail*) ao *e-mail* institucional da empresa Forcetech JR Soluções.

Squirrelmail é um pacote de *webmail* gratuito e de código aberto, distribuído sob a licença GNU versão 2. Inclui suporte PHP puro integrado para os protocolos IMAP e SMTP, e todas as páginas são renderizadas em HTML 4.0 puro para maior compatibilidade entre navegadores.

Tem poucos requisitos de *software* e *hardware* e é simples de configurar e instalar. O Squirrelmail tem todos os recursos de um cliente de *e-mail*, incluindo forte suporte a MIME, catálogos de endereços e manipulação de pastas. O *webmail* Squirrelmail usa uma arquitetura de *plugins* para acomodar recursos adicionais em torno do aplicativo principal, e mais de 200 *plugins* estão disponíveis no *site* do Squirrelmail (THE SQUIRRELMAIL PROJECT TEAM, 2016).

O Squirrelmail era para ser um aplicativo de Webmail fácil de instalar que exigia pouco do servidor e do cliente. Isso significava que não havia dependências de extensões PHP ou coisas como JavaScript ou HTML dinâmico (THE SQUIRRELMAIL PROJECT TEAM, 2016).

De forma alternativa a utilização de um *software* cliente de *e-mail*, surgiram as plataformas de *webmail*, que são clientes de *e-mail* previamente configurados que

executam do lado do servidor, e que se conectam diretamente a ele, apresentando uma interface de fácil acesso, intuitiva, na tela de qualquer navegador de Internet.

Webmail é normalmente um serviço gratuito acessado usando um navegador. A maioria dos serviços de webmail também pode ser acessada usando um cliente de e-mail local, como o Microsoft Outlook, se você preferir um conjunto de recursos do cliente local e não quiser permanecer online enquanto lê e compõe mensagens (PARSONS; OJA, 2013).

Pode-se citar o Gmail (GOOGLE LLC, 2022), o Outlook (MICROSOFT, 2022), antigo Hotmail, como exemplos de serviço do tipo *webmail*. Estes dois serviços também podem ser acessados diretamente por qualquer *software* cliente de *e-mail* que suporte os protocolos padrões de comunicação (POP3, POP3S, IMAP, IMAPS, SMTP, SMTPS).

É uma opção prática de acesso ao *e-mail*, principalmente quando o usuário não está utilizando seus dispositivos pessoais ou de trabalho, ou está longe do acesso a eles. Por exemplo, quando o usuário está em viagem, e não tem seu *e-mail* pessoal ou corporativo configurado em seu celular e/ou notebook, pode acessá-lo de qualquer dispositivo utilizando o navegador de Internet.

2.15 LET'S ENCRYPT

Muitos dos serviços utilizados no servidor dependem de um certificado de criptografia para assegurar que as conexões entre o servidor e clientes sejam feitas de forma segura. Este certificado pode ser compartilhado entre todos os serviços executados no servidor (Apache, Postfix, Dovecot, Webmin, Webmail, phpMyAdmin).

Como todo este trabalho se baseia em *softwares* de licença gratuita, a certificação de criptografia fornecida pela Let's Encrypt se encaixa neste requisito.

A Let's Encrypt é uma autoridade certificadora (AC) gratuita, automatizada e aberta que opera em prol do benefício público. É um serviço provido pela Internet Security Research Group (ISRG). Fornece gratuitamente os certificados digitais necessários para habilitar HTTPS (SSL/TLS) em websites da maneira mais amigável possível (THE LINUX FOUNDATION, 2022).

2.16 REGISTRO DE DOMÍNIO

Para que o servidor tenha real presença na Internet, e para que fique simples acessá-lo, foi solicitado pela empresa Forcotech JR Soluções, o registro de endereço de domínio de Internet "forcotechjr.com.br". Este registro também foi necessário para obtenção do certificado de criptografia.

Um nome de domínio é um fragmento de texto que mapeia para um endereço de IP numérico, usado para acessar um *site* a partir do *software* cliente, ou simplesmente, um nome de domínio é o texto que um usuário digita em uma janela do navegador para acessar um *site* específico. Por exemplo, o nome de domínio da empresa Google é "google.com".

O endereço real de um *site* é um endereço de IP numérico complexo (por exemplo, 200.17.100.40), mas graças ao DNS (*Domain Name System/Sistema de Nome de Domínio*), os usuários podem inserir nomes de domínio simples para humanos e serem direcionados para os *sites* que procuram. Este processo é conhecido como pesquisa de DNS.

No Brasil, O Registro.br é o departamento do NIC.br responsável pelas atividades de registro e manutenção dos nomes de domínios que usam o ".br". Também executa o serviço de distribuição de endereços IPv4 e IPv6 e de números de Sistemas Autônomos (ASN) no país (NIC.BR, 2022).

No passado, o processo para se registrar um domínio ".br" no Brasil era complexo. Exigia que a pessoa ou empresa/instituição que fosse efetuar o registro, disponibiliza-se dois servidores de DNS para responder por requisições do domínio. Isto era custoso pois quem registrava um domínio, deveria manter duas máquinas físicas executando um servidor de DNS, conectadas 24h na Internet, com dois endereços de IP válidos.

Atualmente, o Registro.br (NIC.BR, 2022) disponibiliza os seus próprios servidores de DNS para responder pelos domínios registrados, de forma gratuita, para quem registrar seus domínios nesta Instituição. Claro, a utilização do DNS é gratuita, mas o registro tem como custo a anuidade de R\$40,00. Este foi o único custo direto que a empresa Forcetech JR Soluções teve para instalar o servidor.

3 DESENVOLVIMENTO

Este é o Capítulo aborda todos os aspectos da execução, da instalação e configuração do Sistema Operacional Linux, no servidor da empresa Forcotech JR Soluções, bem como a instalação e a configuração executadas na implantação dos *softwares* servidores e serviços previamente descritos no Capítulo 2.

3.1 METODOLOGIA

Este trabalho baseia-se na sua totalidade, em escolhas das tecnologias e *softwares* para satisfazer a demanda do cliente. Seleção de *hardware* específico para comportar o servidor, definição de infraestrutura de rede e demais configurações específicas para adequação a rede existente do Instituto Federal do Paraná, campus União da Vitória.

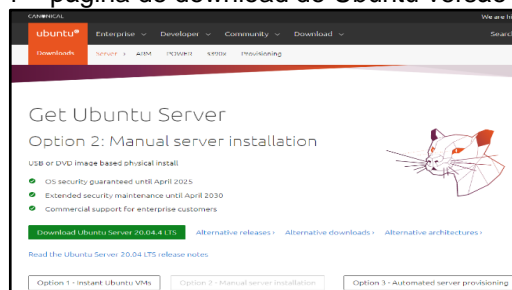
Abaixo relacionadas estão as etapas a serem cumpridas:

- Instalação e configuração do Sistema Operacional e *softwares*;
- Registro de domínio no órgão competente no Brasil;
- Hospedagem do *site* e *e-mail* institucional da empresa Forcotech JR Soluções.

3.2 ETAPA PRELIMINAR PARA A INSTALAÇÃO DO SISTEMA OPERACIONAL

Antes do início do processo de instalação do Ubuntu, foi necessário obter uma cópia de sua imagem de instalação, no formato ISO (ISO.ORG, 2022), no *site* oficial do Ubuntu (CANONICAL LTD, 2022), demonstrado na Figura 1.

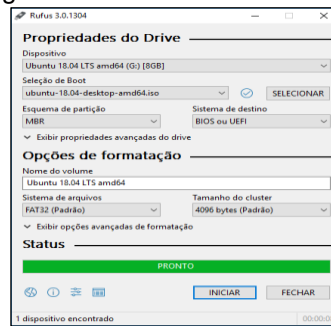
Figura 1 – página de download do Ubuntu versão servidor



Fonte: (CANONICAL LTD, 2022)

Após a obtenção da imagem, foi preciso criar um *pendrive* inicializável com a imagem de instalação do Ubuntu. Para executar esta tarefa utilizando o Microsoft Windows, foi usado o *software* gratuito Rufus (Figura 2), que pode ser obtido no *site* oficial do desenvolvedor (BATARD, 2022).

Figura 2 – tela do software Rufus



Fonte: (BATARD, 2022)

Após sua instalação, o Rufus é executado. O dispositivo onde será gravada a imagem do SO é selecionado, neste caso um *pendrive* de no mínimo 4GB de armazenamento. O arquivo contendo a imagem de instalação, o qual foi baixado anteriormente, deve ser selecionado. O tipo do sistema de destino deve ser selecionado de acordo com o *hardware* suportado pela máquina onde a instalação será feita, o restante das opções pode ser deixado como padrão. O processo é iniciado clicando no botão iniciar e, após sua conclusão, o *pendrive* com o Linux estará pronto para utilização.

3.3 INSTALAÇÃO DO UBUNTU

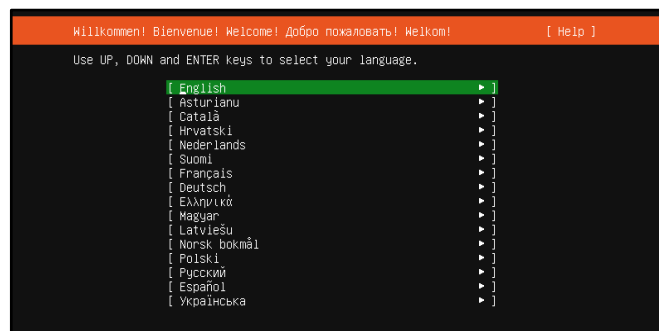
Foi disponibilizado pela empresa Forcotech JR Soluções um computador para função de servidor, conforme as especificações de *hardware* descritas abaixo:

- **Processador:** Intel(R) Xeon(R) E-2226G CPU @ 3.40GHz, 6 núcleos, 12 threads;
- **Memória RAM:** 2 pentes de memória RAM DDR4 KINGSTON 2400, de 8Gb (16Gb no Total);
- **Disco Rígido:** Hd 3tb Sata 3 64mb 7200rpm 3,5 Pull Hua723030ala641 Hitachi;
- **Placa Mãe:** Gigabyte C246M-WU4-CF, com duas interfaces GbE LAN, 8 conectores SATA, duas interfaces M.2, 6 Portas USB 3.1 Gen2 Tipo-A;
- **Fonte:** Genérica de 350W;
- **Gabinete:** Genérico do tipo *desktop*.

As especificações descritas acima foram mais do que suficientes para que o servidor da empresa Forcotech JR Soluções possa funcionar de forma adequada, e se enquadraram em todos os requisitos de *hardware* solicitados pelo SO e demais *softwares*.

Como o servidor veio de fábrica sem o SO instalado, para ser iniciada a instalação, foi conectado ao servidor um monitor e um teclado, e o *pendrive* contendo a instalação do Linux Ubuntu. Para inicializar o computador com o *pendrive*, foi necessário fazer alterações na sequência de inicialização do computador. Estas alterações foram feitas acessando o programa de inicialização da placa mãe do servidor, e selecionando o dispositivo *pendrive* como dispositivo primário da inicialização. Reinicia-se a máquina e a instalação começa, conforme ilustrado na Figura 3.

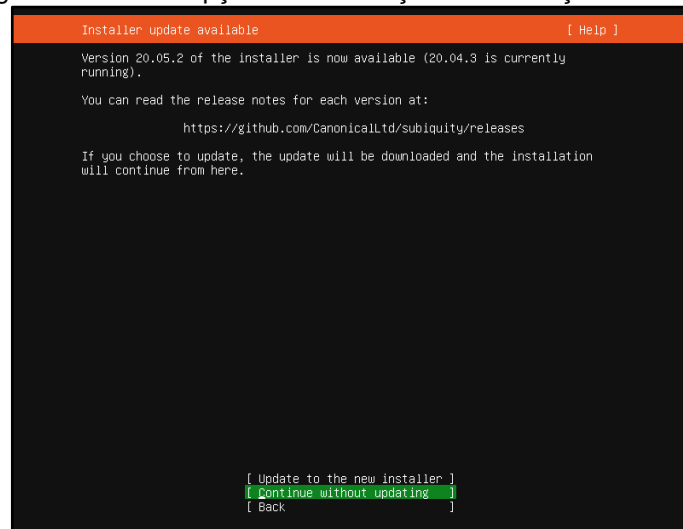
Figura 3 – tela de seleção de idioma da instalação do Ubuntu



Fonte: Instalação do Ubuntu

É feita a seleção do idioma da instalação, no caso Português Brasileiro, e procede-se ao próximo passo. O instalador pergunta se deve fazer atualizações antes de prosseguir, ou continuar sem atualizar, conforme Figura 4.

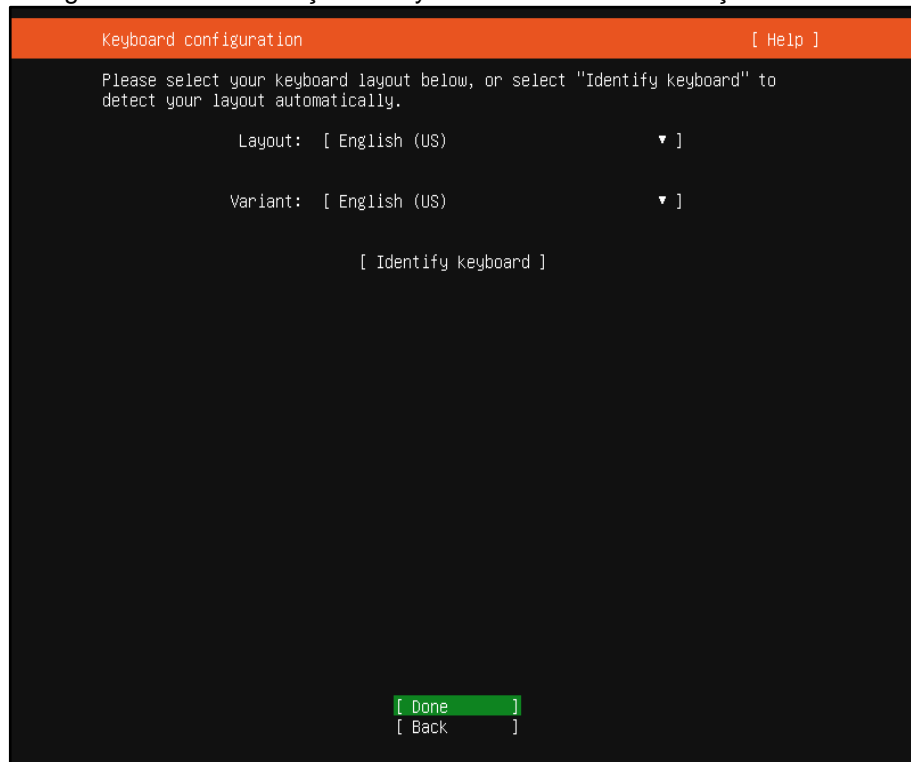
Figura 4 – tela de opção de atualização da instalação do Ubuntu



Fonte: Instalação do Ubuntu

Após este passo, uma tela para seleção de layout de teclado é exibida, conforme Figura 5.

Figura 5 – tela de seleção de layout de teclado da instalação do Ubuntu



Fonte: Instalação do Ubuntu

O tipo de teclado selecionado é do tipo PT-BR/ABNT2, que é o padrão utilizado no Brasil para teclados com suporte a acentos ortográficos e cedilha. A seguir a instalação solicita que sejam preenchidas as configurações de rede. Foi fornecido pela administração do IFPR, campus União da Vitória, as seguintes configurações de rede:

Endereço IP válido:

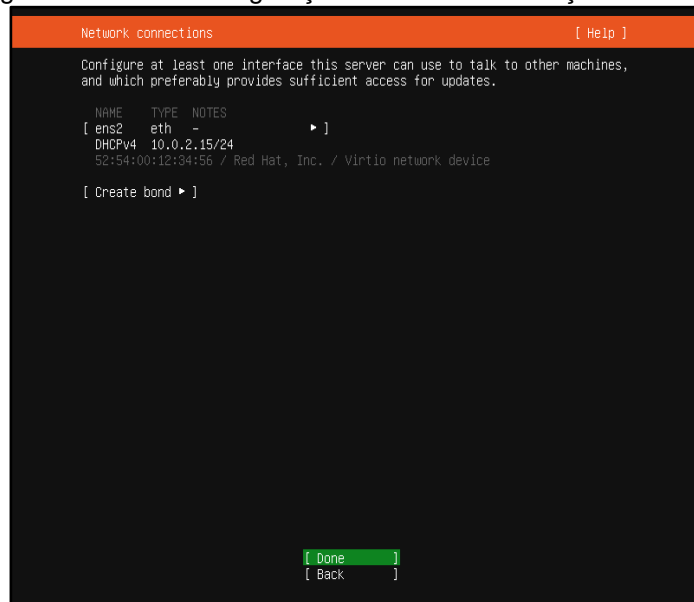
- **Endereço:** 200.17.100.40
- **Máscara de rede:** 255.255.255.240
- **Gateway:** 200.17.100.33
- **DNS:** 8.8.8.8/8.8.4.4

Endereço IP inválido para rede interna:

- **Endereço:** 10.10.0.9
- **Máscara de rede:** 255.255.252.0
- **Gateway:** 10.10.3.254

Estas configurações são inseridas na instalação (Figura 6).

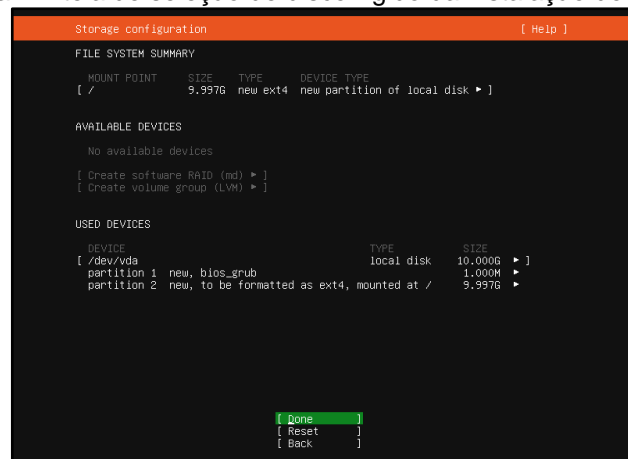
Figura 6 – tela de configuração de rede da instalação do Ubuntu



Fonte: Instalação do Ubuntu

A interface de rede enp3s0 foi configurada com o endereço 200.17.100.40 e a interface secundária de rede eno1 com o endereço 10.10.0.9, com suas respectivas máscaras e *gateways*. Algumas etapas posteriores não serão descritas por não haver necessidade de alterações nas configurações padrão da instalação. Segue-se para a etapa de seleção do disco rígido onde será feita a instalação, conforme Figura 7.

Figura 7 – tela de seleção de disco rígido da instalação do Ubuntu

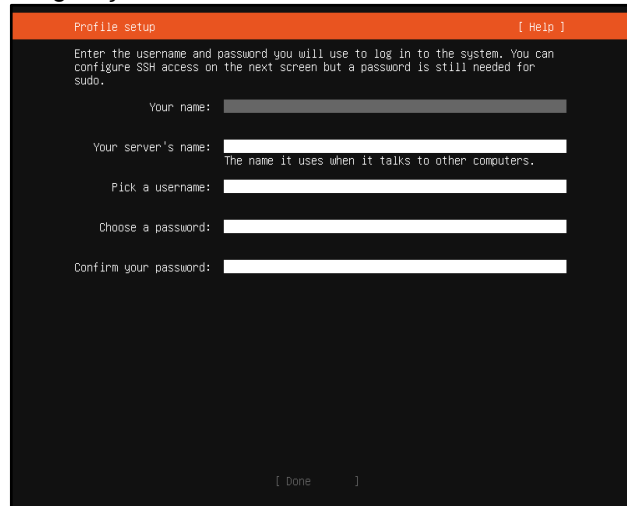


Fonte: Instalação do Ubuntu

A instalação solicita a criação de um usuário administrador para o sistema, deve-se fornecer um nome de usuário (*login*), o nome real do usuário, e a senha (*password*), ilustrado na Figura 8. O nome escolhido para este usuário foi “webmaster”, que fará parte do grupo “sudoers” (grupo de usuários do sistema Linux que podem executar comando de administração como o usuário root). O instalador também solicita a entrada para um nome para o servidor (*Hostname* / Nome do

Anfitrião). O nome escolhido foi “www.forcetechnjr.com.br”, que posteriormente será o nome de domínio institucional da empresa Forcetechn JR Soluções na Internet.

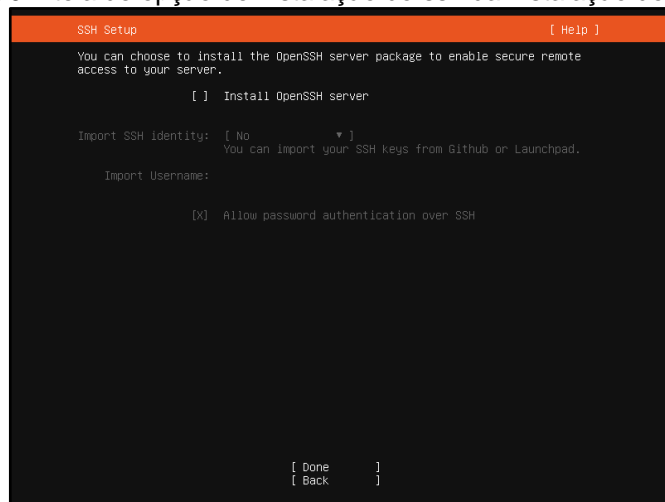
Figura 8 – tela de configuração de usuário/senha/nome do anfitrião da instalação do Ubuntu



Fonte: Instalação do Ubuntu

O programa de instalação solicita se deve ou não instalar um servidor SSH, conforme Figura 9. Como o SSH é o serviço primordial para acesso remoto, optou-se por instalá-lo.

Figura 9 – tela de opção de instalação do ssh da instalação do Ubuntu



Fonte: Instalação do Ubuntu

Algumas etapas posteriores também não serão descritas, pois tratam-se de configurações padrão que não têm necessidade de alteração. Ao final da instalação, retira-se o *pendrive*, reinicia-se o sistema, e após o carregamento do Ubuntu, já se tem acesso ao terminal de texto da máquina.

Pode-se desligar o servidor, retirar teclado e mouse, colocá-lo dentro do *rack*, efetuar as ligações físicas de energia elétrica e cabos em ambas as interfaces de rede, religá-lo, e então, o acesso ao terminal de texto já pode ser feito remotamente via *software* cliente SSH. O acesso pode ser feito via rede local do IFPR, campus União da Vitória, ou remotamente pela Internet, no endereço de rede “200.17.100.40”. Com isso, conclui-se a instalação básica do servidor.

3.4 INSTALAÇÃO DO WEBMIN

Por padrão, o Webmin não está incluso nos repositórios de *software* do Ubuntu, então seu repositório precisa ser inserido manualmente. Isto é feito adicionando o repositório ao arquivo “/etc/apt/sources.list”. A edição do arquivo é feita com o comando abaixo, no terminal de texto do Linux:

```
“#sudo vi /etc/apt/sources.list” – abre o arquivo para edição
```

A linha abaixo deve ser inserida ao final do arquivo para adicionar o novo repositório:

```
“deb http://download.webmin.com/download/repository sarge contrib”
```

Após a edição do arquivo, a chave de criptografia Webmin PGP deve ser adicionada para que o sistema confie no novo repositório. Para fazer isso, é necessário instalar o pacote gnupg1, que é a ferramenta do GNU para comunicação e armazenamento de dados seguros. A instalação do gnupg1 é feita executando o seguinte comando no terminal de texto do Linux:

```
“#sudo apt-get -y install gnupg1” – instala o gnupg1
```

O índice de pacotes do servidor deve ser atualizado, inserindo o comando abaixo no terminal de texto do Linux:

```
“#sudo apt update” – atualiza o índice de pacotes
```

A chave Webmin PGP deve ser baixada e adicionada à lista de chaves do sistema, executando o comando abaixo no terminal de texto do Linux:

```
“#wget -q -O- http://www.webmin.com/jcameron-key.asc | sudo apt-key add” – baixa a chave e adiciona a lista de chaves
```

A lista de pacotes deve ser novamente atualizada para incluir o repositório Webmin, que agora é confiável, executando o comando abaixo no terminal de texto do Linux:

```
“#sudo apt update” – atualize o índice de pacotes
```


A instalação do Webmin é feita, executando o comando abaixo no terminal de texto do Linux:

```
"#sudo apt install webmin" – instala o Webmin
```

Assim que a instalação terminar, será apresentado na tela o seguinte resultado:

```
"Output
```

```
. . .
```

```
Webmin install complete. You can now login to  
https://your_server:10000 as root with your  
root password, or as any user who can use sudo."
```

Após o término da instalação, o Webmin pode ser acessado pelo navegador de Internet, no endereço "http://200.17.100.40:10000". O Webmin sugere que a conexão seja feita através do protocolo HTTPS, apresentando um link de redirecionamento para "https://200.17.100.40:10000". Porém o navegador irá apresentar um aviso informando que o certificado de segurança do *site* não é válido.

O Webmin possui por padrão em sua instalação, um certificado de segurança auto assinado, mas que não é confiável. Este detalhe será resolvido posteriormente neste trabalho após o registro do domínio "forcetechjr.com.br", utilizando um certificado de criptografia válido e gratuito, gerado pela Let 's Encrypt.

3.5 INSTALAÇÃO DO LAMP-SERVER

Para agilizar o processo de instalação dos serviços para o servidor *web*, optou-se pelo recurso LAMP (Linux + Apache + MySQL + PHP/PERL/PYTHON), o qual instala automaticamente todos os *softwares* necessários para o servidor *web*.

A instalação do LAMP é feita utilizando o tasksel. O tasksel é uma ferramenta Debian/Ubuntu que instala vários pacotes relacionados como uma tarefa coordenada no sistema. Para instalar um servidor LAMP, são executados os seguintes comandos no terminal de texto do Linux:

```
"#sudo apt update" – atualiza a base de dados dos pacotes do Linux
```

```
"#sudo apt install tasksel" - instala a ferramenta tasksel
```

```
"#sudo tasksel install lamp-server" – instala a pilha LAMP
```

Após a instalação do LAMP-SERVER, inicia-se o servidor Apache inserindo o comando no terminal de texto do Linux:

```
"#sudo service apache2 start" – inicia o servidor Apache
```

3.6 INSTALAÇÃO DO MARIADB

Como o LAMP instala o servidor MySQL por padrão, é necessário fazer a remoção do MySQL antes de se instalar o MariaDB. O motivo de retirar o MySQL é que neste projeto foi selecionado o MariaDB para servidor de banco de dados, descrito no Capítulo 2.9. A remoção da instalação do MySQL é feita executando os comandos abaixo no terminal de texto do Linux:

```
“#sudo systemctl stop mysql” – interrompe a execução do servidor MySQL
```

```
“#sudo apt-get remove --purge mysql-server mysql-client mysql-common” – remove por completo a instalação do MySQL
```

```
“#sudo apt-get autoremove” – remove quaisquer resquícios de arquivos deixados pela desinstalação de pacotes
```

A instalação do MariaDB é feita executando os comandos abaixo no terminal de texto do Linux:

```
“#sudo apt-get install mariadb-server” – instala o servidor MariaDB
```

```
“#sudo service mysql start” – inicia o servidor MariaDB
```

A segurança da instalação do MariaDB é feita executando o comando “#sudo mysql_secure_installation” no terminal de texto do Linux. Este comando é um assistente para implementar as seguintes medidas de segurança: configurar a senha root (administrativa) do banco de dados; remover o acesso root de fora do servidor local; remover contas de usuários anônimos; remover o banco de dados “test”, que oferece acesso padrão a todos os usuários, inclusive anônimos, além de privilégios que permite acessar indiscriminadamente bancos de dados que comecem com a palavra “_test”.

As medidas são necessárias e recomendadas em um servidor de banco de dados em produção.

3.7 INSTALAÇÃO DO PHPMYADMIN

A instalação do phpMyAdmin é feita executando os comandos abaixo no terminal de texto do Linux:

```
“#sudo apt install phpmyadmin” – instala o phpMyAdmin
```

```
“#sudo service apache restart” – reinicia o servidor APACHE
```

3.8 INSTALAÇÃO DO WORDPRESS

Antes da instalação do WordPress, são necessários alguns preparativos no quesito configurações: criar um banco de dados para o WordPress; criar um usuário neste banco de dados; habilitar o “mod_rewrite” no servidor Apache; configurar o servidor Apache para permitir a leitura do arquivo “.htaccess”; instalar módulos adicionais no PHP.

A criação do banco de dados e o usuário para o acesso do WordPress é feita executando os comandos abaixo no terminal de texto do Linux:

“#sudo mysql -u root -p” – conecta ao servidor de banco de dados

“CREATE DATABASE wordpress DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;” – cria o banco de dados

“CREATE USER 'wordpressuser'@'localhost' IDENTIFIED BY 'password';” – adiciona o usuário ao banco de dados

“GRANT ALL ON wordpress.* TO 'wordpressuser'@'localhost';” – garante permissões de acesso ao banco de dados

“ALTER USER 'wordpressuser'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password;” – restringe o usuário criado ao banco de dados

“FLUSH PRIVILEGES;” – reinicia os privilégios do banco de dados

“EXIT;” – sai para o terminal de texto do Linux

A instalação dos módulos adicionais do PHP que são requisitos do WordPress, é feita executando o comando abaixo no terminal de texto do Linux:

“#sudo apt install php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip” – instala todos os módulos adicionais do PHP para o WordPress

O Apache precisa ser configurado para que possa permitir a leitura do arquivo “.htaccess”, arquivo onde o WordPress configura os endereços permanentes, isto é feito executando os comandos abaixo no terminal de texto do Linux:

“#sudo vi /etc/apache2/sites-enabled/000-default.conf” – abre o arquivo padrão de configuração de *site* do Apache

A seguinte diretiva deve ser inserida neste arquivo entre as marcações “<VirtualHost>” para permitir a leitura do arquivo “.htaccess”:

“<Directory /var/www/html> AllowOverride All
</Directory>”

Após a edição do arquivo, é necessário habilitar o “mod_rewrite” do Apache, necessário para o WordPress poder reescrever os endereços das páginas hospedadas em sua plataforma, executando os comandos abaixo no terminal de texto do Linux:

“#sudo a2enmod rewrite” – habilita o módulo rewrite do Apache

“#sudo service apache2 reload” – reinicia o serviço do Apache

A instalação do WordPress é feita executando os comandos abaixo no terminal de texto do Linux:

“#cd /tmp” – muda o diretório para o diretório temporário do sistema

“#sudo wget https://br.wordpress.org/latest-pt_BR.tar.gz” – baixa o arquivo de instalação do WordPress

“#sudo tar -zxf latest-pt_BR.tar.gz” – descompacta o arquivo baixado

“#cd wordpress/” – muda o diretório para o diretório de instalação do WordPress

“#sudo cp -ax * /var/www/html” – copia o conteúdo do diretório para o diretório raiz do servidor Apache

“#cd /var/www/html” – muda para o diretório raiz do servidor Apache

“#sudo chown www-data.www-data -Rf *” – altera as permissões de arquivos e pastas para o usuário padrão do Apache

“#sudo rm index.html” – remove a página de índice padrão do Apache

A instalação do WordPress segue agora utilizando um navegador de Internet. Isto é feito acessando o endereço raiz do servidor Apache (http://200.17.100.40/), conforme demonstrado na Figura 10.

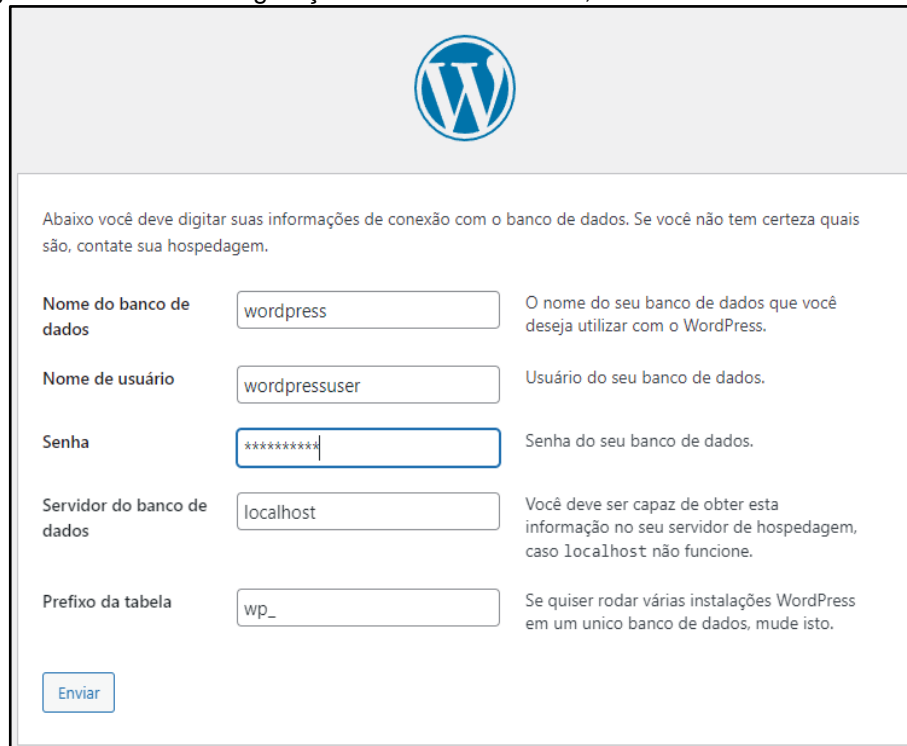
Figura 10 – tela inicial da instalação do WordPress



Fonte: instalação do WordPress

O botão “Vamos lá?” é pressionado, então a instalação pede as configurações de usuário, senha, nome do banco de dados, e endereço do anfitrião para a conexão ao servidor de banco de dados, demonstrado na Figura 11:

Figura 11 – tela de configuração do banco de dados, usuário e senha do WordPress



The screenshot shows the WordPress database configuration screen. At the top center is the WordPress logo. Below it, a message reads: "Abaixo você deve digitar suas informações de conexão com o banco de dados. Se você não tem certeza quais são, contate sua hospedagem." There are five input fields with labels and descriptions:

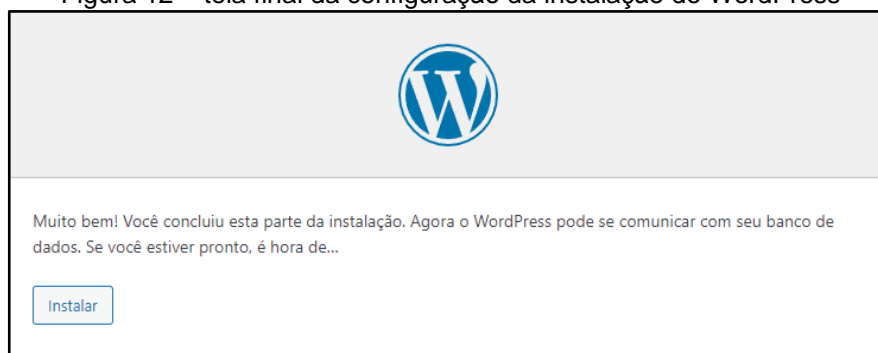
Label	Input Value	Description
Nome do banco de dados	wordpress	O nome do seu banco de dados que você deseja utilizar com o WordPress.
Nome de usuário	wordpressuser	Usuário do seu banco de dados.
Senha	*****	Senha do seu banco de dados.
Servidor do banco de dados	localhost	Você deve ser capaz de obter esta informação no seu servidor de hospedagem, caso localhost não funcione.
Prefixo da tabela	wp_	Se quiser rodar várias instalações WordPress em um único banco de dados, mude isto.

At the bottom left, there is a blue button labeled "Enviar".

Fonte: instalação do WordPress

Após a inserção das configurações, o botão enviar é pressionado, e se a configuração não apresentou erros, uma tela de confirmação aparecerá, como demonstrado na Figura 12:

Figura 12 – tela final da configuração da instalação do WordPress



The screenshot shows the final confirmation screen of the WordPress installation. At the top center is the WordPress logo. Below it, a message reads: "Muito bem! Você concluiu esta parte da instalação. Agora o WordPress pode se comunicar com seu banco de dados. Se você estiver pronto, é hora de..." At the bottom left, there is a blue button labeled "Instalar".

Fonte: instalação do WordPress

O botão “Instalar” é pressionado, e a instalação solicita que seja inserido o nome do *site*, nome do usuário administrador, e uma senha para o usuário administrador (Figura 13). O WordPress possui um gerador automático de senhas fortes, o qual é altamente recomendado utilizar.

Figura 13 – tela da instalação do WordPress com a configuração de usuário e senha administrativos

The screenshot shows the WordPress installation 'Welcome' screen. At the top is the WordPress logo. Below it, the text reads 'Bem-vindo (a)' and 'Bem-vindo (a) à famosa instalação do WordPress em cinco minutos! Basta preencher as informações abaixo e você estará a poucos passos de usar a plataforma de publicação mais extensível e poderosa do mundo.' The main section is titled 'Informação necessária' and contains the following fields and options:

- Título do site:** Formsetech IR Soluções
- Nome de usuário:** webmaster
- Senha:** Fortis (with a 'Mostrar' button)
- O seu e-mail:** rgunther13@hotmail.com
- Visibilidade nos motores de busca:** Exibir que mecanismos de busca indexem este site. Cabe aos mecanismos de busca atender esta solicitação.

At the bottom left is a button labeled 'Instalar WordPress'.

Fonte: instalação do WordPress

Após a inserção dos dados, o botão “Instalar WordPress” é pressionado.

Ao término da instalação, a tela de sucesso da instalação é exibida, demonstrada na Figura 14, finalizando a instalação.

Figura 14 – tela de sucesso na instalação do WordPress

The screenshot shows the WordPress installation 'Success' screen. At the top is the WordPress logo. Below it, the text reads 'Sucesso!' and 'O WordPress foi instalado. Obrigado e divirta-se!'. The screen displays the following information:

- Nome de usuário:** webmaster
- Senha:** Sua senha escolhida.

At the bottom left is a button labeled 'Acessar'.

Fonte: instalação do WordPress

3.9 INSTALAÇÃO DO POSTFIX

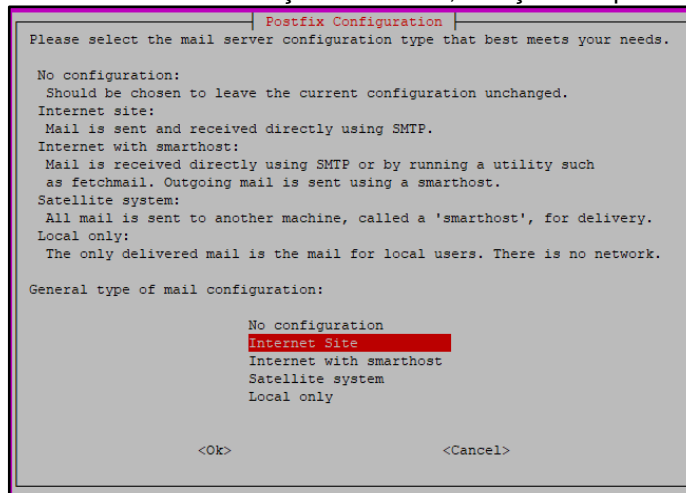
A instalação do Postfix é feita executando os comandos abaixo no terminal de texto do Linux, e o *script* de instalação inicia o processo de configuração:

“#sudo apt update” – atualiza a base de pacotes do Linux

“#sudo DEBIAN_PRIORITY=low apt install postfix” – instala o Postfix

Nesta primeira etapa, a instalação permite selecionar o tipo de servidor que será instalado. Como a empresa Forcetechn JR Soluções terá seu próprio domínio (forcetechnjr.com.br), foi selecionada a opção “Internet Site” (Figura 15).

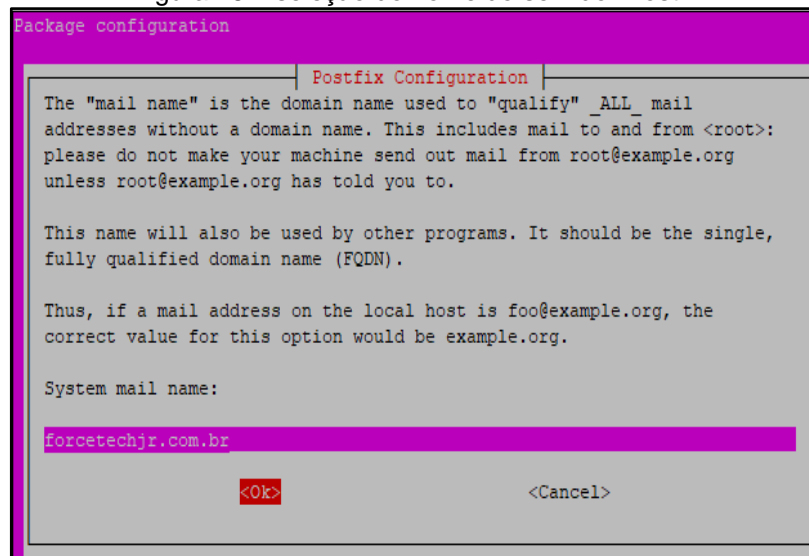
Figura 15 – tela inicial da instalação do Postfix, seleção do tipo de instalação



Fonte: instalação do Postfix

Definido o tipo de servidor que será instalado, a instalação solicita que seja dado um nome ao servidor, que será “forcetechnjr.com.br” (Figura 16).

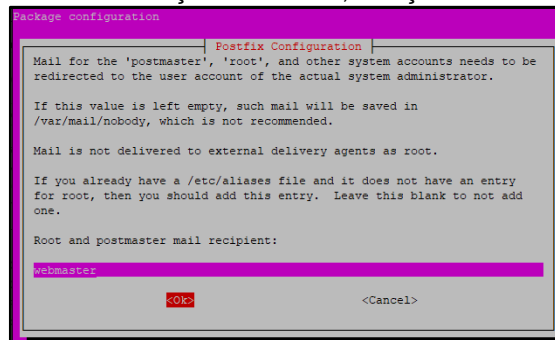
Figura 16 – seleção do nome do servidor Postfix



Fonte: instalação do Postfix

A instalação solicita que seja preenchido o nome de usuário que receberá todos os e-mails do usuário “root”, esta configuração será armazenada no arquivo de configuração de “aliases” (apelidos) de e-mail (“/etc/aliases”). Neste caso o usuário “webmaster”, administrador do sistema (Figura 17).

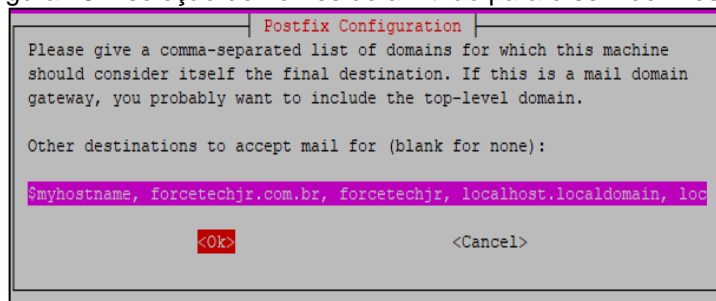
Figura 17 – tela da instalação do Postfix, seleção de aliases para o root



Fonte: instalação do Postfix

A instalação permite adicionar outros nomes para o servidor e/ou outros domínios que o servidor poderá responder. As configurações são deixadas como padrão, pois a própria instalação já faz a geração de nomes comuns para o servidor, levando em conta o nome de domínio (Figura 18).

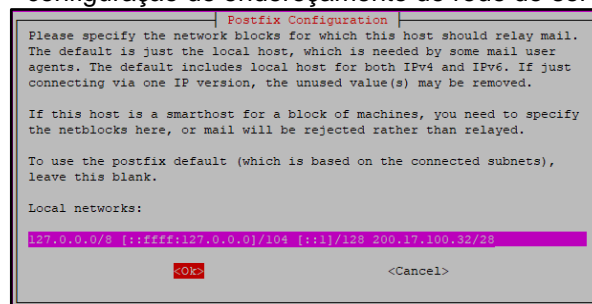
Figura 18 – seleção de nomes de anfitrião para o servidor Postfix



Fonte: instalação do Postfix

As configurações de redes e/ou endereços IP onde o servidor Postfix vai responder as requisições deverão ser preenchidas. É inserido o endereço de rede "200.17.100.38/28", que foi a rede designada pelo IFPR, campus União da Vitória, para o servidor (Figura 19).

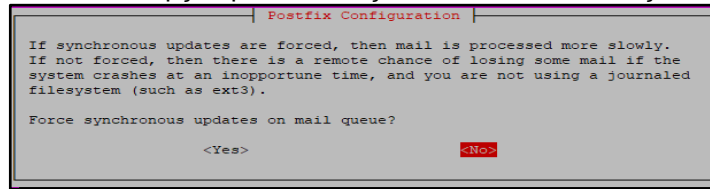
Figura 19 – configuração de endereçamento de rede do servidor Postfix



Fonte: Instalação do Postfix

O script de instalação pergunta se deve habilitar o processo de enfileiramento de *e-mails*, para ser executado de forma síncrona. Foi optado por não, pois esta opção pode causar lentidão no serviço (Figura 20).

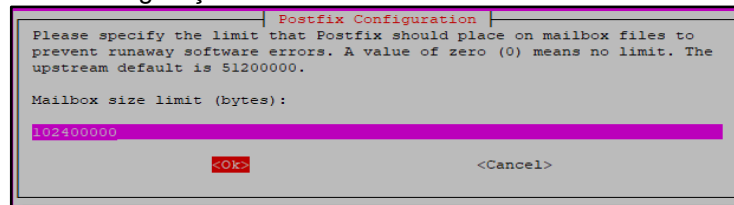
Figura 20 – tela de opção por atualização síncrona da instalação do Postfix



Fonte: instalação do Postfix

O limite de tamanho das caixas postais de cada usuário do sistema deve ser informado. Optou-se por caixas postais de tamanho 1GB (Figura 21)

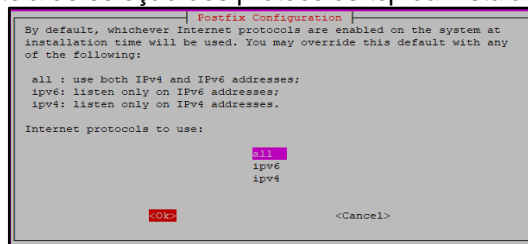
Figura 21 – tela de configuração do tamanho da caixa de correio da instalação do Postfix



Fonte: instalação do Postfix

A instalação pergunta se o Postfix vai responder às requisições nos protocolos IPv4 e/ou IPv6 (Figura 22). Como foi fornecido pelo IFPR, campus União da Vitória, ambos os endereços para os dois protocolos, foi selecionado “all” (todos) e a instalação padrão é finalizada.

Figura 22 – tela de seleção dos protocolos tcp da instalação do Postfix



Fonte: instalação do Postfix

A instalação padrão do Postfix não engloba todos os requisitos para o funcionamento correto do servidor. Então é necessário alterar algumas configurações para que o Postfix funcione adequadamente com os outros serviços do servidor.

É necessário alterar o tipo de caixa de correio de “mailbox” para “Maildir”. Esta alteração é necessária pois o formato de armazenamento “Maildir” é muito mais rápido do que o “mailbox”. Esta alteração é feita executando os seguintes comandos no terminal de texto do LINUX:

`#sudo postconf -e 'home_mailbox= Maildir/'` – adiciona a configuração de “Maildir” ao Postfix

`#sudo service postfix reload` – reinicia o servidor Postfix

A porta de submissão de e-mail 587/TCP precisa ser habilitada no Postfix, para permitir envio de mensagens de clientes ao servidor de e-mail. Isto é feito executando o comando abaixo no terminal de texto do Linux:

```
#sudo vi /etc/postfix/master.cf
```

 – abre o arquivo master.cf para edição

A linha abaixo deve ser inserida no arquivo:

```
submission inet n - n - - smtpd
```

 – linha de configuração a ser inserida no arquivo

Após a edição do arquivo, o servidor Postfix deve ser reiniciado, com o comando:

```
#sudo service postfix reload
```

 – reinicia o servidor Postfix

Após terminada a configuração do Postfix, o servidor ainda não está completo. Há necessidade de se habilitar mais algumas configurações relacionadas a autenticação SMTP, mas esta tarefa vai ser designada a outro serviço, o servidor Dovecot, que será demonstrado no Capítulo 3.10.

3.10 INSTALAÇÃO DO DOVECOT

A instalação do Dovecot é iniciada executando os seguintes comandos abaixo no terminal de texto do Linux:

```
#sudo apt install dovecot-core dovecot-imapd dovecot-pop3d
```

 – instala os pacotes do Dovecot

```
#dovecot -version
```

 – comando de checagem da versão do Dovecot

A saída do comando será semelhante a abaixo:

```
2.3.7.2 (3c910f64b)
```

É necessário habilitar os protocolos IMAP e POP3 do Dovecot, executando o comando abaixo no terminal de texto do Linux:

```
#sudo vi /etc/dovecot/dovecot.conf
```

 – abre o arquivo para edição

Deve ser feita uma alteração em uma linha de configuração conforme descrito abaixo:

```
protocols
```

 – alterar para → `protocols = imap pop3`

Também é necessário configurar o tipo de caixa de correio com o qual o Dovecot vai funcionar, isto é feito executando o comando abaixo no terminal de texto do Linux:

```
#sudo vi /etc/dovecot/conf.d/10-mail.conf
```

 – abre o arquivo para edição

Deve ser feita uma alteração em uma linha de configuração conforme descrito abaixo:

“mail_location = maildir:~/Maildir” – linha que deve ser alterada

O usuário “dovecot” também deve ser adicionado ao grupo “mail”, executando o comando abaixo no terminal de texto do Linux:

“#sudo adduser dovecot mail” - adiciona o usuário dovecot ao grupo “mail”

Embora o Dovecot tenha sido configurado para armazenar *e-mails* no formato “Maildir”, por padrão, o Postfix usa seu agente de entrega local integrado para mover *e-mails* de entrada para o armazenamento de mensagens (caixa de entrada, enviados, lixo, lixo eletrônico etc.), e será salvo no formato “mbox”.

O Postfix precisa ser configurado para passar os *e-mails* recebidos para o Dovecot, através do protocolo LMTP, que é uma versão simplificada do SMTP, para que os *e-mails* recebidos sejam salvos no formato “Maildir” pelo Dovecot.

A instalação do Dovecot LMTP é feita executando o comando abaixo no terminal de texto do Linux:

“#sudo apt install dovecot-lmtpd” – instala o dovecot-lmtpd

O protocolo LTPD deve ser adicionado no arquivo de configuração do Dovecot, isto é feito executando o comando abaixo no terminal de texto do Linux:

“#sudo vi /etc/dovecot/dovecot.conf” – abre o arquivo para edição

A linha abaixo deve ser alterada conforme demonstrado abaixo:

“protocol = imap pop3” – alterada para → “protocol = imap pop3 ltpd”

O arquivo de configuração do Dovecot para habilitar o protocolo LTPD também deve ser editado, para se adequar ao Postfix, executando o comando abaixo no terminal de texto do Linux:

“#sudo vi /etc/dovecot/conf.d/10-master.conf” – abre o arquivo para edição

A linha com a definição “service lmtp” deve ser modificada como descrito abaixo:

```
“service lmtp {
    unix_listener /var/spool/postfix/private/dovecot-lmtp {
        mode = 0600
        user = Postfix
        group = Postfix
    } }”
```

É necessário fazer uma alteração na configuração do Postfix para que os *e-mails* sejam passados para o Dovecot, isto é feito executando o comando abaixo no terminal de texto do Linux:

`#sudo vi /etc/postfix/main.cf` – abre o arquivo para edição

Ao final do arquivo duas linhas devem ser adicionadas, conforme descrito abaixo:

`mailbox_transport = lmtp:unix:private/dovecot-lmtp` – define o protocolo de transporte

`smtputf8_enable = no` – desabilita a codificação utf8

A autenticação pelo Dovecot precisa ser habilitada, isto é feito executando o comando abaixo no terminal de texto do Linux:

`#sudo vi /etc/dovecot/conf.d/10-auth.conf` – abre o arquivo para edição

A linha `disable_plaintext_auth = yes` deve ser descomentada. O mesmo é feito para a linha `auth_username_format = %Lu`, é alterado o `%Lu` para `%n`. Por padrão, quando o Dovecot tenta localizar ou entregar *e-mails* para um usuário, usa o endereço de e-mail completo. Como foi configurado somente usuários canônicos de caixa de correio (usando usuários do sistema operacional como usuários de caixa de correio), o Dovecot não consegue encontrar o usuário de caixa de correio no formato de domínio completo (`usuario@dominio.com.br`), portanto, precisa-se definir `auth_username_format = %n` para descartar a parte do domínio. O Dovecot poderá encontrar o usuário da caixa de correio. Isso também permite usar o endereço de e-mail completo (`nomedeusuario@dominio.com.br`) para fazer *login*.

Para o Dovecot poder suportar clientes antigos de *e-mail*, é alterada a linha `auth_mechanisms` para `auth_mechanisms = plain login`.

A autenticação SASL no Dovecot deve ser habilitada executando o comando abaixo no terminal de texto do Linux:

`# sudo vi /etc/dovecot/conf.d/10-master.conf` – abre o arquivo para edição

A seção de autenticação de serviço deve ser alterada para que o Postfix possa encontrar o servidor de autenticação Dovecot, conforme descrito abaixo:

```
service auth {
    unix_listener /var/spool/postfix/private/auth {
        mode = 0660
        user = postfix
        group = postfix } }
```

Ao término da edição, os serviços Dovecot e o Postfix deve ser reiniciados, isto é feito executando o comando abaixo no terminal de texto do Linux:

`#sudo systemctl restart postfix dovecot` – reinicia o Postfix e o Dovecot

O Dovecot deverá responder por requisições nas portas 110 (POP3), 143 (IMAP), 993 (IMAPS), e 995 (POP3S) como demonstrado na Figura 23.

Figura 23 – tela resultante do comando “#sudo ss -lnpt |grep dovecot

```

root@www:~# sudo ss -lnpt |grep dovecot
LISTEN 0      100      0.0.0.0:110      0.0.0.0:*      users: (("dovecot",pid=641791,fd=21))
LISTEN 0      100      0.0.0.0:143      0.0.0.0:*      users: (("dovecot",pid=641791,fd=40))
LISTEN 0      100      0.0.0.0:993      0.0.0.0:*      users: (("dovecot",pid=641791,fd=42))
LISTEN 0      100      0.0.0.0:995      0.0.0.0:*      users: (("dovecot",pid=641791,fd=23))
LISTEN 0      100      [::]:110         [::]:*         users: (("dovecot",pid=641791,fd=22))
LISTEN 0      100      [::]:143         [::]:*         users: (("dovecot",pid=641791,fd=41))
LISTEN 0      100      [::]:993         [::]:*         users: (("dovecot",pid=641791,fd=43))
LISTEN 0      100      [::]:995         [::]:*         users: (("dovecot",pid=641791,fd=24))
root@www:~# █

```

Fonte: terminal de texto do Linux

3.11 INSTALAÇÃO DO SQUIRRELMAIL

O Squirrelmail é um pouco mais trabalhoso para instalar, pois como não existe um pacote pronto para o Ubuntu, a instalação precisa ser feita manualmente.

A instalação do Squirrelmail é feita executando os seguintes comandos no terminal de texto do Linux:

“#cd /tmp” - muda o diretório para /tmp

“#sudo wget

<https://ufpr.dl.sourceforge.net/project/squirrelmail/stable/1.4.22/squirrelmail-webmail-1.4.22.tar.gz>” - baixa o arquivo de instalação

“#sudo tar -zxf squirrelmail-webmail-1.4.22.tar.gz” – descompacta o arquivo de instalação

“#cd squirrelmail-webmail-1.4.22/” - muda para o diretório descompactado

“#sudo mv squirrelmail-webmail-1.4.22 /usr/local/squirrelmail/www” – move o diretório

“#sudo chown www-data:www-data -Rf * /usr/local/squirrelmail/www/ - altera as permissões de diretórios e arquivos para o usuário padrão do Apache

“#cd /usr/local/squirrelmail/www/” – muda o diretório para o diretório de instalação do Squirrelmail

“#sudo ./configure” – executa o script de configuração do Squirrelmail

A criação de um arquivo de configuração para o Squirrelmail no Apache é necessária, isto é feito executando os seguintes comandos no terminal de texto do Linux:

“#cd /etc/apache2/conf-available” – muda o diretório

“#sudo touch squirrelmail.conf” – cria o arquivo de configuração

“#sudo vi squirrelmail.conf” – abre o arquivo para edição

As configurações do Squirrelmail devem ser inseridas neste arquivo para que o Apache permita a execução do Squirrelmail. Estas configurações são demonstradas na Figura 24:

Figura 24 – configuração do Squirrelmail para o Apache

```
Alias /webmail /usr/local/squirrelmail/www
<Directory /usr/local/squirrelmail/www>
    Options None
    AllowOverride None
    DirectoryIndex index.php
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/scripts>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/images>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/plugins>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/feeds>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/templates>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/themes>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/contrib>
    Require all granted
</Directory>
<Directory /usr/local/squirrelmail/www/doc>
    Require all granted
</Directory>
```

Fonte: configuração do Squirrelmail

Para habilitar esta configuração no Apache, os comandos abaixo devem ser executados no terminal de texto do Linux:

“#sudo a2enconf squirrelmail” – habilita a configuração do Squirrelmail no Apache

“#sudo service apache2 restart” – reinicia o servidor Apache

3.12 PROCESSO DE REGISTRO DE DOMÍNIO

O processo de registro é iniciado tendo em mãos os dados da pessoa ou da instituição para a qual será feito o registro (nome/razão social, CPF/CNPJ, endereço completo, telefones de contato, e-mail e dados pessoais da pessoa responsável pelo registro). Uma busca é necessária no site do Registro.br (NIC.BR, 2022) para verificar a existência do domínio, antes de iniciar o processo. É inserido o nome do domínio o qual deseja-se registrar, como ilustrado na Figura 25.

Figura 25 – tela inicial da página oficial do Registro.br

The screenshot shows the Registro.br homepage. At the top left is the logo 'nie.br registro.br'. To the right is a link 'ACESSAR CONTA'. Below the logo is a navigation menu with items: 'Sobre Domínios', 'Tecnologia', 'Ajuda', 'Quem Somos', 'Contato', and 'REGISTRE'. The main content area features a search bar with the text 'Registre o domínio .br certo para você' and the domain 'forcetechjr.com.br' entered. Below the search bar, it says 'Domínio não disponível para registro.' and 'Domínio já registrado'.

Fonte: (NIC.BR, 2022)

Caso o domínio esteja disponível para registro, o processo de registro pode ser continuado, e é necessário cadastrar uma conta de usuário no *site* do Registro.br (NIC.BR, 2022). A Figura 26 ilustra este processo.

Figura 26 – tela do formulário de cadastro de conta de acesso no Registro.br

The screenshot shows the 'DADOS DO ADMINISTRADOR DE CONTA' form. The fields are filled with the following information:

Nome completo		Rodrigo Cassiano güntner	
E-mail			
forcetech.jr@gmail.com			
Pais	CEP		
Brasil	84603-264		
Endereço			Número
Avenida Paula Freitas			2800
Complemento	UF	Cidade	
São Braz	PR	União da Vitória	
DDD	Telefone	Ramal	
42	8408-0007		

Fonte: (NIC.BR, 2022)

Após o cadastro da conta, as configurações do novo domínio devem ser preenchidas. Isto é feito acessando a página de configuração do domínio do Registro.br (NIC.BR, 2022). As configurações foram feitas para corresponder ao endereço de IP fornecido pela administração do Instituto Federal do Paraná, campus União da Vitória. Estas configurações são demonstradas na Figura 27.

Figura 27 – configurações do domínio forcetechjr.com.br

TIPO	NOME	DADOS	
● A	forcetechjr.com.br	200.17.100.40	×
● MX	forcetechjr.com.br	5 mail.forcetechjr.com.br	×
● A	bibliotecaifpr.forcetechjr.com.br	200.17.100.40	×
● CNAME	ftp.forcetechjr.com.br	forcetechjr.com.br	×
● CNAME	imap.forcetechjr.com.br	forcetechjr.com.br	×
● CNAME	mail.forcetechjr.com.br	forcetechjr.com.br	×
● CNAME	pop3.forcetechjr.com.br	forcetechjr.com.br	×
● CNAME	smtp.forcetechjr.com.br	forcetechjr.com.br	×
● CNAME	www.forcetechjr.com.br	forcetechjr.com.br	×

Fonte: (NIC.BR, 2022)

Ao término da configuração, é gerado um boleto correspondente ao valor da taxa anual de registro de domínio, o qual é enviado para o *e-mail* da conta institucional do usuário cadastrado no site do Registro.br (NIC.BR, 2022). Após o pagamento da taxa de registro de domínio, o domínio entra em funcionamento sendo replicado para todos os servidores DNS mundiais.

3.13 INSTALAÇÃO E OBTENÇÃO DO CERTIFICADO DE CRIPTOGRAFIA

A instalação da certificação da Let's Encrypt é feita executando os comandos abaixo no terminal de texto do Linux:

`#sudo apt install letsencrypt` – instala a certificação Let's Encrypt

`#sudo apt install python3-certbot-apache` – instala o *script* automatizado da Let's Encrypt para o Apache

O pacote de *softwares* da Let's Encrypt também instala o utilitário `certbot.timer` para renovação automática de certificados. Este utilitário verifica a validade dos certificados SSL no sistema duas vezes ao dia e estende aqueles que expiram nos próximos 30 dias. O seu funcionamento pode ser verificado executando o comando abaixo no terminal de texto do Linux:

`#sudo systemctl status certbot.timer` – verifica o funcionamento do `certbot.timer`

Caso a instalação esteja correta, este comando produzirá uma resposta como representada na Figura 28.

Figura 28 – resultado do comando “#sudo systemctl status certbot.timer”

```

root@www:~# sudo systemctl status certbot.timer
● certbot.timer - Run certbot twice daily
   Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; vendor preset: enabled)
   Active: active (waiting) since Thu 2022-03-24 16:59:45 -03; 2 weeks 5 days ago
   Trigger: Thu 2022-04-14 10:27:18 -03; 17h left
   Triggers: ● certbot.service

Warning: journal has been rotated since unit was started, output may be incomplete.
root@www:~# █

```

Fonte: terminal de texto do Linux

Com a certificação da Let’s Encrypt instalada, é possível obter o certificado para o servidor, executando o comando abaixo no terminal de texto do Linux:

“#sudo certbot certonly --standalone --agree-tos --preferred-challenges http -d forcetechjr.com.br” – obtém um novo certificado

O comando “certbot” obtém e instala automaticamente o certificado de segurança no servidor Apache, habilita o protocolo https na porta 443/TCP e redireciona automaticamente para o endereço seguro.

O “certbot” instala dois arquivos de certificado no diretório “/etc/letsencrypt/live/forcetechjr.com.br/”, o certificado em si, no arquivo “fullchain.pem”, e a chave de segurança privada no arquivo “privkey.pem”. Estes dois arquivos serão utilizados posteriormente para configurar a segurança dos *softwares* servidores.

3.13.1 Instalação do Certificado de Criptografia no Postfix

O certificado de segurança no Postfix é instalado executando o comando abaixo no terminal de texto do Linux:

“#sudo vi /etc/postfix/main.cf” – abre o arquivo para edição

As seguintes linhas devem ser adicionadas no arquivo:

Parâmetros TLS quando o Postfix recebe *e-mails*

smtpd_tls_cert_file=/etc/letsencrypt/live/forcetechjr.com.br/fullchain.pem

smtpd_tls_key_file=/etc/letsencrypt/live/forcetechjr.com.br/privkey.pem

smtpd_tls_security_level=may

smtpd_tls_loglevel = 1

smtpd_tls_session_cache_database = btree:\${data_directory}/smtpd_scache

Parâmetros TLS quando o Postfix enviar *e-mail*

smtp_tls_security_level = may

```
smtp_tls_loglevel = 1
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

Força os protocolos TLSv1.3 or TLSv1.2

```
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
smtpd_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
smtp_tls_protocols = !SSLv2, !SSLv3, !TLSv1, !TLSv1.1
```

Após a edição do arquivo, o serviço do Postfix deve ser reiniciado com o comando “#sudo service postfix restart”.

3.13.2 Instalação do Certificado de Criptografia no Dovecot

O certificado de criptografia no Dovecot é instalado executando o comando abaixo no terminal de texto do Linux:

“#sudo vi /etc/dovecot/conf.d/10-ssl.conf” – abre o arquivo para edição

A diretiva “ssl = yes” deve ser alterada para “ssl = required” para forçar a encriptação.

As linhas abaixo devem ser alteradas para apontar para o caminho do certificado de segurança obtido através da Let’s Encrypt:

```
“ssl_cert      =      </etc/dovecot/private/dovecot.pem      →      ssl_cert      =
</etc/letsencrypt/live/forcetechjr.com.br/fullchain.pem”
“ssl_key       =      </etc/dovecot/private/dovecot.key      →      ssl_key       =
</etc/letsencrypt/live/forcetechjr.com.br/privkey.pem”
```

A diretiva “ssl_prefer_server_ciphers = no” é alterada para “yes”, para forçar o Dovecot a comunicar-se com servidores que também utilizam criptografia.

E também são desabilitados alguns protocolos inseguros como o SSLv3, TLSv1 e o TLSv1.1 adicionando a seguinte linha de configuração:

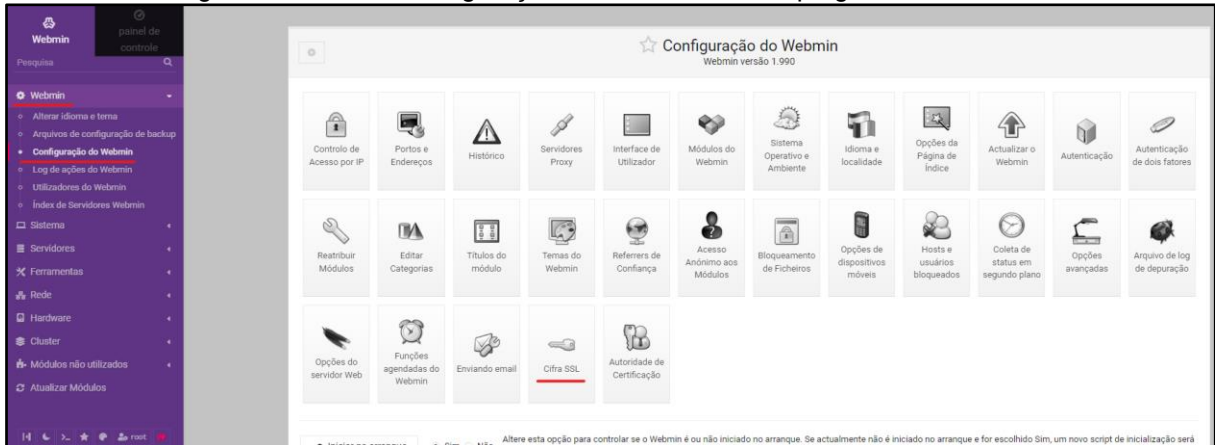
“ssl_min_protocol = TLSv1.2” – força o uso de criptografia do tipo TLSv1.2

Após a edição do arquivo, o serviço do Dovecot deve ser reiniciado executando o comando “#sudo service dovecot restart” no terminal de texto do Linux.

3.13.3 Instalação do Certificado de Criptografia no Webmin

O certificado de criptografia no Webmin é instalado pela interface de administração do Webmin, isto é feito acessando o endereço <https://forcetechjr.com.br:10000>. No menu lateral esquerdo, clica-se em “Webmin”, “Configurações do Webmin”, e após em “Cifras SSL”, como ilustrado na Figura 29.

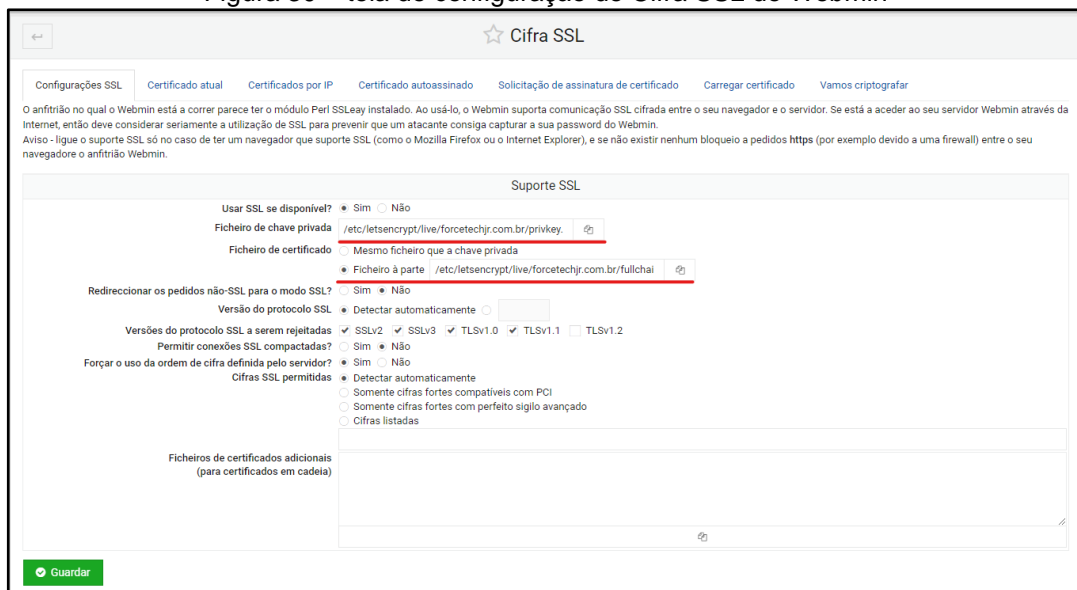
Figura 29 – tela de configuração do certificado de criptografia do Webmin



Fonte: configuração do Webmin

A tela de configuração de “Cifra SSL” do Webmin será apresentada, onde é inserido o caminho da chave privada de criptografia, e o caminho do certificado de criptografia, demonstrado na Figura 30.

Figura 30 – tela de configuração de Cifra SSL do Webmin



Fonte: configuração de SSL do Webmin

Após a configuração ser inserida, o botão “Guardar” é pressionado, o Webmin irá reiniciar automaticamente e então, já é possível acessá-lo de forma segura.

3.14 INSTALAÇÃO E CONFIGURAÇÃO DO FIREWALL NETFILTER

Como o Netfilter faz parte da solução de segurança padrão do Linux, como descrito no Capítulo 2.4, é necessário a instalação de sua ferramenta de configuração, o iptables.

A instalação do iptables é feita executando os comandos abaixo no terminal de texto do Linux:

```
#sudo apt install iptables iptables-persistent
```

 – instala o iptables

```
#sudo service iptables start
```

 – inicia o serviço iptables

O iptables não insere nenhuma regra em suas tabelas que possam restringir qualquer serviço ou porta de comunicação no momento da instalação. Mesmo em sua primeira execução, o padrão de todas as tabelas é permitir todo e qualquer acesso.

Então, é necessário a adição de algumas regras para permitir acesso aos serviços que já estão em execução no servidor, e algumas outras regras para negar qualquer outro tipo de acesso, para deixar o servidor seguro.

Pode-se adicionar regras uma a uma via terminal de texto do Linux, porém, como serão adicionadas várias regras pré definidas para os serviços que já estão executando, é necessário editar o arquivo de configuração do iptables, responsável pelas regras de *firewall* do protocolo ipv4, o arquivo “/etc/iptables/rules.v4”.

Na tabela “*filter”, são adicionadas as regras na cadeia “INPUT”, que trata de todas as conexões externas, entrando em direção ao servidor. Alterar-se o comportamento padrão da cadeia “INPUT” para “DROP”, rejeitando todas as conexões de entrada que não estejam liberadas nas regras inseridas.

No terminal de texto do Linux, o arquivo de configuração do iptables é aberto para edição com o comando “#sudo vi /etc/iptables/rules.v4”, as regras abaixo devem ser inseridas após a diretiva “:INPUT DROP [0:0]”:

```
“:INPUT DROP [0:0]” - define ação padrão para as conexões de entrada – Rejeitar todas
```

```
“-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT” - mantém as conexões abertas e relacionadas ativas
```

```
“-A INPUT -i lo -j ACCEPT” - permite a interface de rede local localhost
```

```
“-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT” - aceita conexões de entrada na porta 22 - OpenSSH
```

“-A INPUT -p tcp -m tcp --dport 25 -j ACCEPT” - aceita conexões de entrada na porta 25 – Postfix SMTP

“-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT” - aceita conexões de entrada na porta 80 – Apache HTTP

“-A INPUT -p tcp -m tcp --dport 110 -j ACCEPT” - aceita conexões de entrada na porta 110 – Dovecot POP3

“-A INPUT -p tcp -m tcp --dport 143 -j ACCEPT” - aceita conexões de entrada na porta 143 – Dovecot IMAP

“-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT” - aceita conexões de entrada na porta 443 – Apache HTTPS

“-A INPUT -p tcp -m tcp --dport 465 -j ACCEPT” - aceita conexões de entrada na porta 465 – Postfix SMTPS

“-A INPUT -p tcp -m tcp --dport 587 -j ACCEPT” - aceita conexões de entrada na porta 587 - Postfix submissão SMTP

“-A INPUT -p tcp -m tcp --dport 993 -j ACCEPT” - aceita conexões de entrada na porta 993 - Dovecot IMAPS

“-A INPUT -p tcp -m tcp --dport 995 -j ACCEPT” - aceita conexões de entrada na porta 995 – Dovecot POP3S

“-A INPUT -p tcp -m tcp --dport 3306 -j ACCEPT” - aceita conexões de entrada na porta 3306 – MariaDB SQL

“-A INPUT -p tcp -m tcp --dport 10000 -j ACCEPT” - aceita conexões de entrada na porta 10000 - Webmin

“-A INPUT -p icmp -j ACCEPT” - aceita protocolo ICMP - ping

Após a inserção das regras, o serviço do iptables deve ser reiniciado para que as regras de firewall se tornem ativas, executando o comando “#sudo service iptables restart” no terminal de texto do Linux. Após sua execução, o servidor estará protegido com o *firewall* Netfilter, permitindo somente conexões nas portas onde seus serviços estão sendo executados.

4 RESULTADOS

Este Capítulo descreve os resultados obtidos durante o desenvolvimento deste trabalho.

4.1 SISTEMA OPERACIONAL UBUNTU

A Figura 31 demonstra o acesso ao terminal de texto do Linux Ubuntu após sua instalação.

Figura 31 – terminal de texto do Linux Ubuntu

```

login as: root
root@200.17.100.40's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-105-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of sáb 09 abr 2022 20:45:08 -03

System load:          2.11
Usage of /:           4.3% of 2.68TB
Memory usage:        39%
Swap usage:          16%
Temperature:         61.0 C
Processes:           586
Users logged in:     0
IPv4 address for eno1: 10.10.0.9
IPv6 address for eno1: 2801:82:4018:1:b62e:99ff:fef3:b879
IPv4 address for enp3e0: 200.17.100.40
IPv4 address for virbr0: 192.168.122.1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

57 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Sat Apr  9 19:48:05 2022 from 138.204.25.214
root@www:~#

```

Fonte: terminal de texto do Ubuntu

4.2 ACESSO REMOTO SEGURO

O servidor pode ser acessado remotamente via protocolo SSH, utilizando qualquer *software* cliente SSH, diretamente pelo endereço IP do servidor (200.17.100.40) ou pelo endereço de domínio do servidor (forcetechjr.com.br). O acesso via cliente SSH utilizando o terminal de texto do Microsoft Windows 10, é demonstrado na Figura 32.

Figura 32 – terminal de texto do Microsoft Windows10, acesso ao servidor via ssh

```

webmaster@www: ~
Windows PowerShell
Copyright (c) Microsoft Corporation. Todos os direitos reservados.
Experimente a nova plataforma cruzada PowerShell https://aka.ms/pscore6

PS C:\Users\Rodrigo Gunther> ssh webmaster@200.17.100.40
The authenticity of host '200.17.100.40 (200.17.100.40)' can't be established.
ECDSA key fingerprint is SHA256:c1v72005cxf7f81995b84840w/mackowget.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '200.17.100.40' (ECDSA) to the list of known hosts.
webmaster@200.17.100.40's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-105-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of sáb 09 abr 2022 20:53:21 -03

System load:          1.66
Usage of /:           3.9% of 2.68TB
Memory usage:        30%
Swap usage:          16%
Temperature:         63.0 C
Processes:           608
Users logged in:     1
IPv4 address for eno1: 10.10.0.9
IPv6 address for eno1: 2801:82:4018:1:b62e:99ff:fef3:b879
IPv4 address for enp3e0: 200.17.100.40
IPv4 address for virbr0: 192.168.122.1

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

57 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

*** System restart required ***
Last login: Wed Sep 22 11:04:33 2021 from 187.95.110.128
webmaster@www:~#

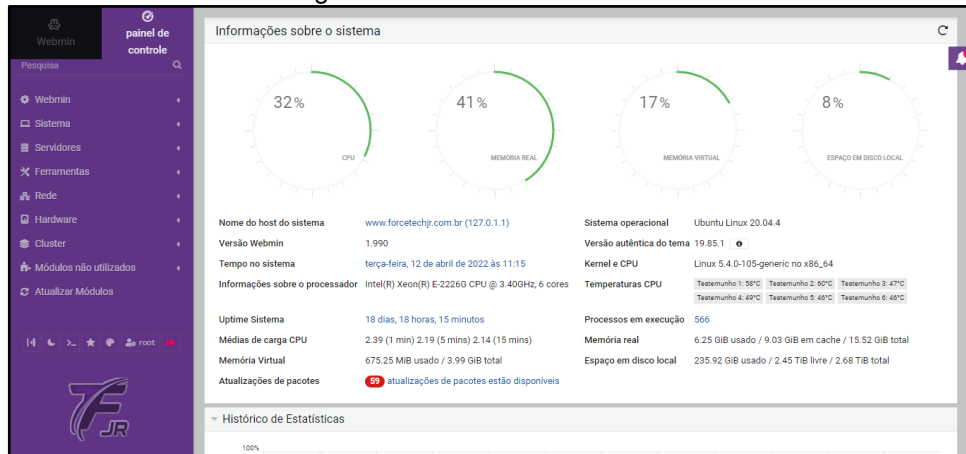
```

Fonte: Terminal de texto do Microsoft Windows 10

4.3 GERENCIADOR ADMINISTRATIVO WEBMIN

O Webmin pode ser acessado de qualquer navegador de Internet, pelo endereço <https://forcetechjr.com.br:10000/>, demonstrado na Figura 33.

Figura 33 – tela inicial do Webmin



Fonte: Webmin

4.4 SERVIDOR DE PÁGINAS HTTP APACHE

O servidor Apache pode ser acessado de qualquer navegador de Internet inserindo o endereço IP do servidor (200.17.100.40), ou o endereço de domínio (forcetechjr.com.br), na barra de endereços. Isto é demonstrado na Figura 34, onde o Apache exibe sua página de índice padrão após sua instalação.

Figura 34 – página de índice padrão do servidor Apache

The screenshot shows the Apache2 Ubuntu Default Page. It features the Apache logo and the text 'ubuntu' in a large font. A red banner with the text 'It works!' is prominent. Below this, there is a paragraph explaining that the page is used to test the correct operation of the Apache2 server after installation on Ubuntu systems. A section titled 'Configuration Overview' provides details about the configuration files and their locations. A code block shows the directory structure of the configuration files.

```

/etc/apache2/
-- apache2.conf
    |-- ports.conf
-- mods-enabled
    |-- *.load
    |-- *.conf
-- conf-enabled
    |-- *.conf
-- sites-enabled
    |-- *.conf
  
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Fonte: servidor Apache

4.5 SUPORTE À LINGUAGEM DE PROGRAMAÇÃO PHP PELO APACHE

O suporte à linguagem de programação PHP pelo servidor Apache pode ser verificado, acessando o endereço <http://forcetechjr.com.br/info.php>. Será apresentada uma tela de status demonstrando o funcionamento do PHP, ilustrada na Figura 35.

Figura 35 – tela de informações do PHP

PHP Version 7.4.3	
System	Linux www.forcetechnr.com.br 5.4.0-109-generic #123-Ubuntu SMP Fri Apr 8 09:10:54 UTC 2022 x86_64
Build Date	Mar 2 2022 15:38:52
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xsl.ini, /etc/php/7.4/apache2/conf.d/20-bz2.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-imagick.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysql.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmllreader.ini, /etc/php/7.4/apache2/conf.d/20-xmllwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress, zlib, php, file, glob, data, http, ftp, compress, bzip2, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*
<small>This program makes use of the Zend Scripting Language Engine: Zend Engine v3.4.0, Copyright (c) Zend Technologies with Zend OPcache v7.4.3, Copyright (c), by Zend Technologies</small>	

Fonte: tela de informações da instalação do PHP

4.6 BANCO DE DADOS RELACIONAL MARIADB

O funcionamento do MariaDB no servidor pode ser verificado executando o comando “#sudo service mysql status” no terminal de texto do Linux, o qual retorna como resposta o status do servidor, demonstrado na Figura 36.

Figura 36 – tela de resposta do servidor MariaDB ao comando “#sudo service mysql status”

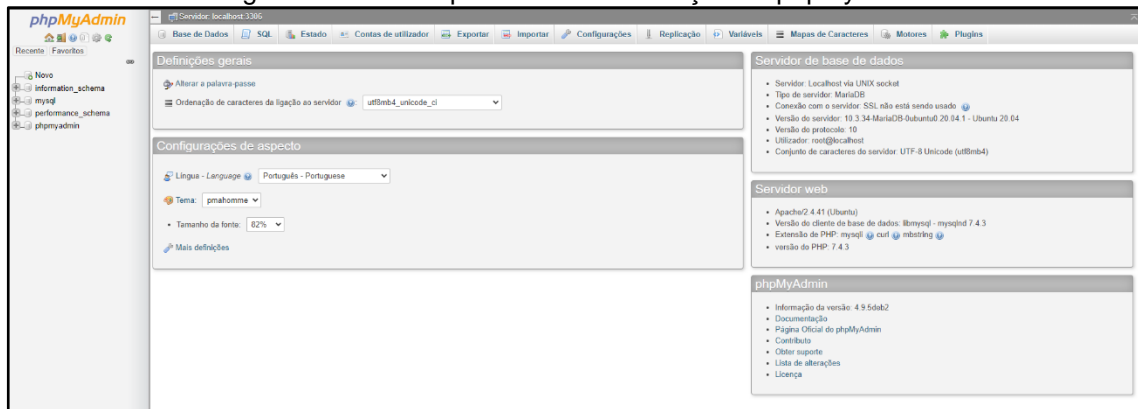
```
root@forcetechjr:/home/webmaster# service mysql status
• mariadb.service - MariaDB 10.3.34 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
  Active: active (running) since Sun 2022-04-10 21:25:45 UTC; 48s ago
    Docs: man:mysqld(8)
          https://mariadb.com/kb/en/library/systemd/
  Main PID: 1504 (mysqld)
  Status: "Taking your SQL requests now..."
    Tasks: 31 (limit: 4612)
  Memory: 63.9M
  CGroup: /system.slice/mariadb.service
          └─1504 /usr/sbin/mysqld
```

Fonte: terminal de texto do Linux Ubuntu

4.7 INTERFACE DE GERENCIAMENTO REMOTO PARA BANCO DE DADOS PHPMYADMIN

O phpMyAdmin pode ser acessado de qualquer navegador de Internet pelo endereço <http://forcetechjr.com.br/phpmyadmin/>, como demonstrado na Figura 37.

Figura 37 – tela do painel de administração do phpMyAdmin

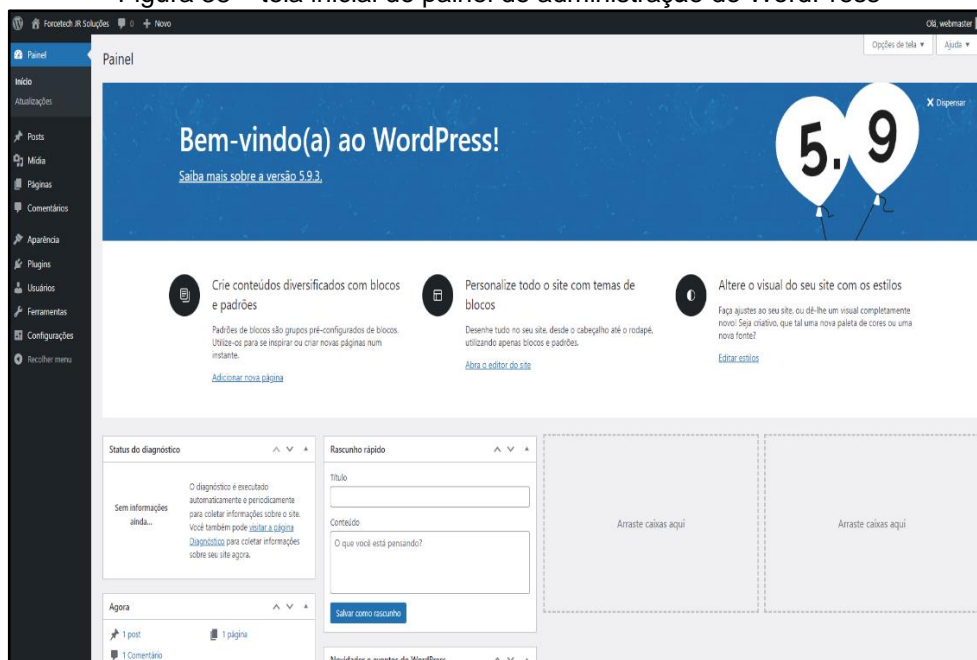


Fonte: phpMyAdmin

4.8 SISTEMA DE GERENCIAMENTO DE CONTEÚDO WORDPRESS

O sistema de gerenciamento de conteúdo WordPress, pode ser acessado de qualquer navegador de Internet, pelo endereço <https://forcetechjr.com.br/wp-admin/>, como demonstrado na Figura 38.

Figura 38 – tela inicial do painel de administração do WordPress



Fonte: WordPress

4.9 SERVIDORES DE CORREIO ELETRÔNICO POSTFIX E DOVECOT

O funcionamento dos servidores de e-mail Postfix e Dovecot pode ser verificado, por um *software* cliente de *e-mail*, configurado com as diretivas demonstradas abaixo:

Servidor IMAP: imap.forcetechnr.com.br – porta 143 (993 para IMAPS)

Servidor SMTP: smtp.forcetechnr.com.br – porta 587 (465 para SMTPS)

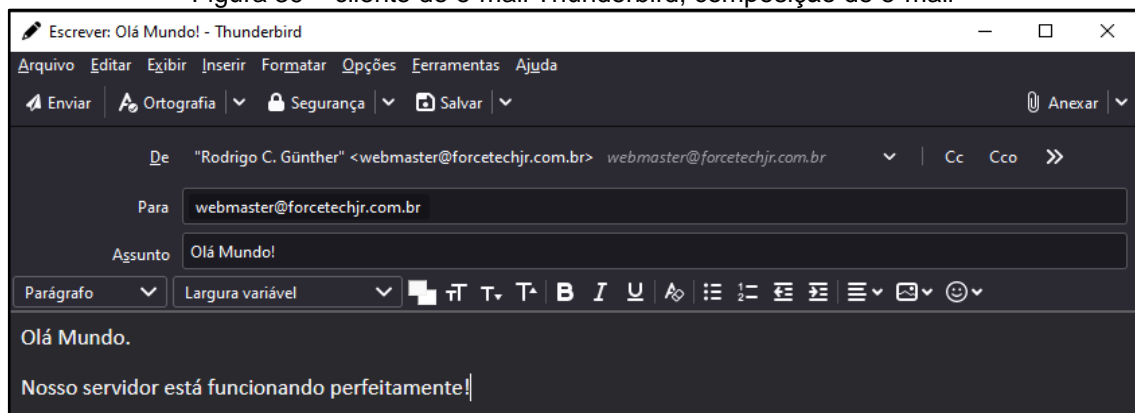
Servidor POP3: pop3.forcetechnr.com.br – porta 110 (995 para POP3S)

Tipo de criptografia SSL: STARTTLS

Tipo de Autenticação: Senha normal

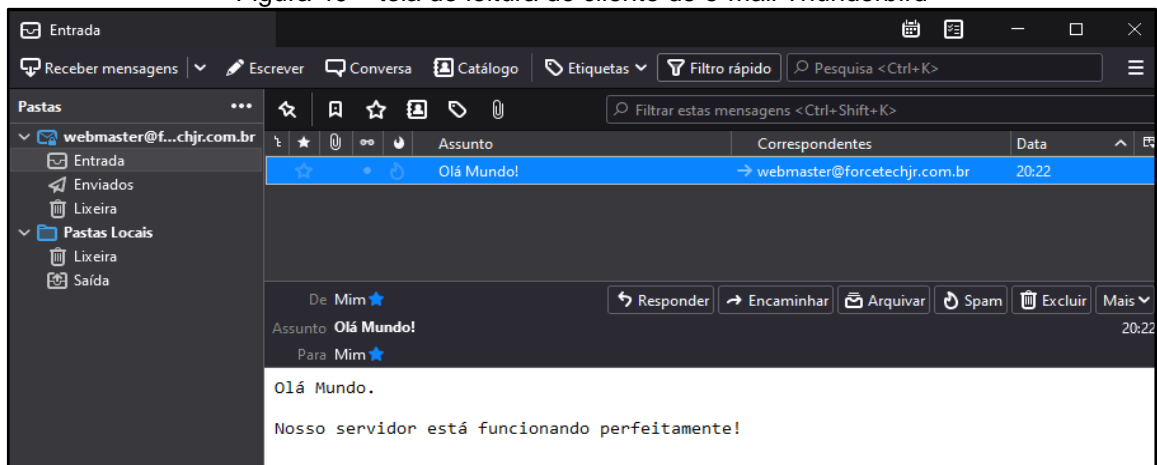
Foi configurado o *software* cliente de *e-mail* Mozilla Thunderbird, para testar o envio e recebimento de *e-mails*, conforme a Figura 39 e Figura 40:

Figura 39 – cliente de e-mail Thunderbird, composição de e-mail



Fonte: Mozilla Thunderbird

Figura 40 – tela de leitura do cliente de e-mail Thunderbird

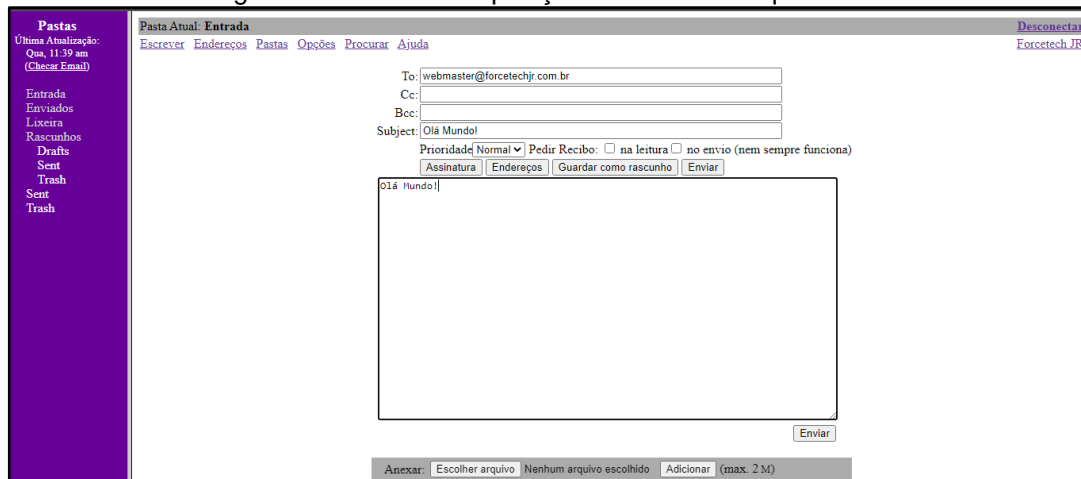


Fonte: Mozilla Thunderbird

4.10 SERVIÇO DE WEBMAIL SQUIRRELMAIL

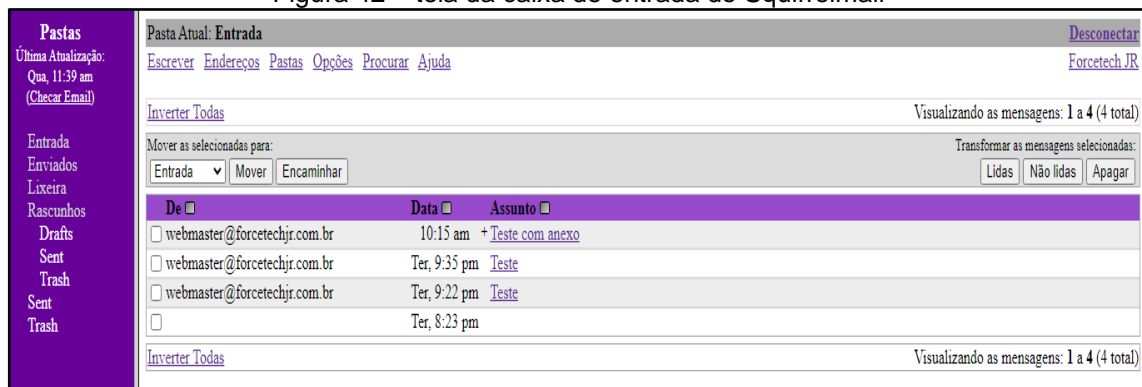
O serviço de *webmail* Squirrelmail pode ser acessado por qualquer navegador de Internet, pelo endereço <https://forcetechjr.com.br/webmail/>, como demonstrado na Figura 41 e na Figura 42.

Figura 41 – tela de composição de e-mail do Squirrelmail



Fonte: Squirrelmail

Figura 42 – tela da caixa de entrada do Squirrelmail

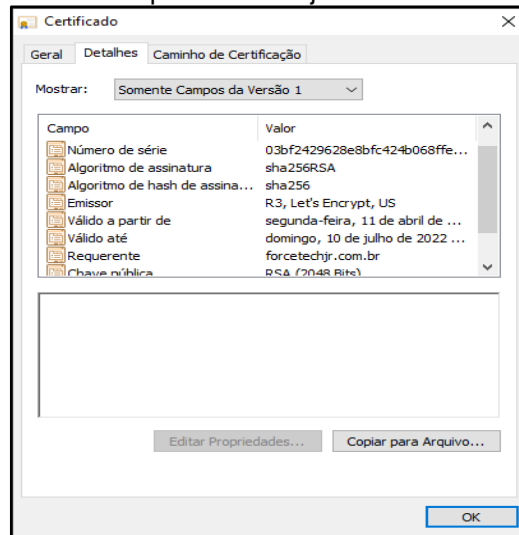


Fonte: Squirrelmail

4.11 CERTIFICAÇÃO DE SEGURANÇA

A certificação de segurança do *site* institucional da empresa Forcotech JR Soluções pode ser verificada, acessando o endereço do *site* (<https://forcetechjr.com.br/>), inserindo este endereço na barra de endereços de qualquer navegador de Internet. Após o carregamento do *site*, deve-se clicar no ícone de cadeado ao lado do endereço na barra de endereço do navegador. O navegador irá apresentar uma tela descrevendo a certificação de segurança instalada no *site*. Isto é demonstrado na Figura 43.

Figura 43 – informações de certificado de criptografia do navegador para o endereço <https://forcetechjr.com.br/>



Fonte: navegador de Internet Google Chrome

4.12 REGISTRO DE DOMÍNIO

O registro de domínio da empresa Forceteck JR Soluções pode ser verificado, acessando o *site* do Registro.br (NIC.BR, 2022), na seção “Ferramentas”, “Whois”.

Após o carregamento da página, será apresentada uma tela com as informações do registro de domínio, demonstrado na Figura 44.

Figura 44 – informações do registro de domínio forcetechjr.com.br

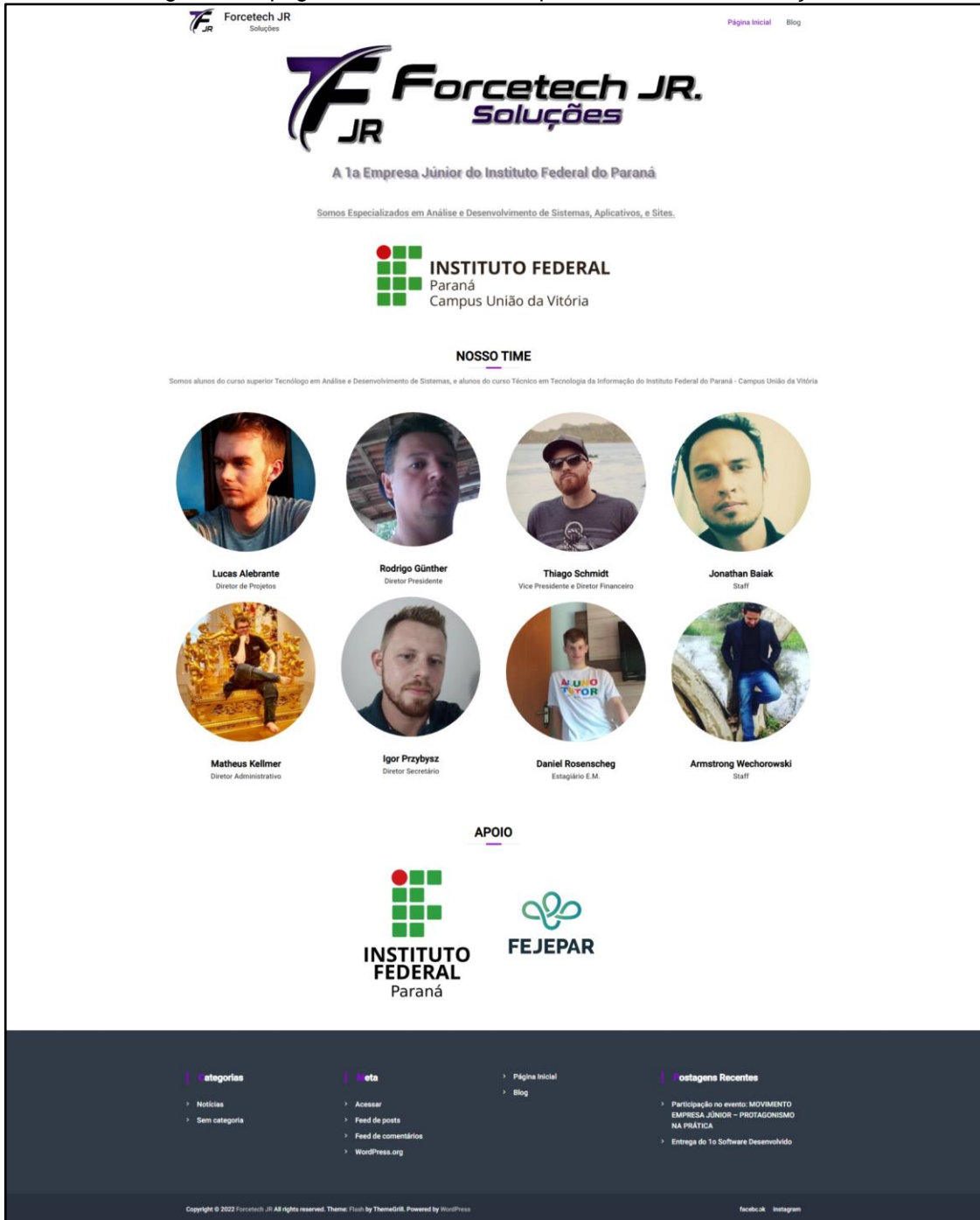
Domínio forcetechjr.com.br	
TITULAR	Forceteck Jr. Soluções
DOCUMENTO	44.157.971/0001-15
RESPONSÁVEL	Lucas Ruan Alebrante
PAÍS	BR
CONTATO DO TITULAR	ROCGU108
CONTATO TÉCNICO	ROCGU108
SERVIDOR DNS	a.sec.dns.br ▾
SERVIDOR DNS	b.sec.dns.br ▾
REGISTRO DS	55822 ECDSA-SHA-256 EB8B2FDE504B0F049FE0D074CAF8D76F762C07925FA35FDD1F7312BF2D9A7DB5 ▾
SACI	Sim
CRIADO	09/11/2021 #23664059
EXPIRAÇÃO	09/11/2022
ALTERADO	09/11/2021
STATUS	Publicado

Fonte: (NIC.BR, 2022)

4.13 HOSPEDAGEM DA PÁGINA INSTITUCIONAL

A página institucional da empresa Forcetek JR Soluções foi desenvolvida por integrantes da empresa, e hospedada no servidor. O acesso a página pode ser feito de qualquer navegador de Internet, no endereço <https://forcetekjr.com.br/>, como demonstrado na Figura 45.

Figura 45 – página institucional da empresa Forcetek JR Soluções



Fonte: página da empresa Forcetek JR Soluções

5 CONSIDERAÇÕES FINAIS

Pode-se afirmar que o principal objetivo deste trabalho foi alcançado em sua totalidade. Conforme solicitado pela empresa Forcotech JR Soluções, o servidor se encontra totalmente ativo e operacional. O registro de domínio forcotechjr.com.br foi efetuado, o *site* e o servidor de *e-mail* institucional da empresa estão em funcionamento. As diretivas para a segurança do servidor foram aplicadas, assim como seu certificado de criptografia.

Apesar de que o servidor de *e-mail* esteja em total funcionamento, o envio de *e-mail* partindo do servidor da empresa Forcotech JR Soluções para qualquer outro servidor na Internet é negado. Esta negação ocorre pelo motivo de que o endereço IP disponibilizado pela coordenação do IFPR, campus União da Vitória, não contém um registro de DNS reverso (registro PTR) configurado. O registro PTR é utilizado por servidores de *e-mail* na Internet para verificar a autenticidade dos *e-mails* recebidos de outros servidores, com objetivo de segurança e para evitar recebimento de mensagens forjadas. Até o término deste trabalho, o registro de DNS reverso (PTR) não foi obtido.

Além de todos os objetivos alcançados durante a execução deste trabalho, outros objetivos que não estavam previstos neste trabalho foram também alcançados. Durante o período da pandemia do Covid-19 (2019 – 2022), quando as aulas presenciais foram suspensas, foi implantado no servidor da empresa Forcotech JR Soluções, um servidor Linux em máquina virtual, para atender as necessidades de se ministrar aulas práticas remotas da matéria Gerenciamento de Servidor.

Foi solicitado pela coordenação do curso TADS, a hospedagem do *site* do Encontro de Tecnologia da Informação do IFPR, campus União da Vitória. O *site* foi hospedado no servidor da empresa Forcotech JR Soluções, e pode ser acessado no endereço eletrônico <https://entec.ifpr.edu.br/>.

Também foi solicitado pelo departamento da Biblioteca do IFPR, campus União da Vitória, a hospedagem do *site* de geração de ficha catalográfica para trabalhos acadêmicos. O *site* foi hospedado no servidor da empresa Forcotech JR Soluções, e pode ser acessado no endereço eletrônico <https://biblioteca.forcotechjr.com.br/>.

5.1 TRABALHOS FUTUROS

- Instalar no servidor o software Samba, que irá trazer a funcionalidade de um servidor de arquivos de rede, compatível com os serviços de rede do Microsoft Windows.
- Aumentar o nível de proteção de segurança do servidor instalando o serviço Fail2Ban, que é um software de manipulação automática de regras de *firewall* que protege o sistema contra ataques de negação de serviço e de força bruta.
- Selecionar um software para automatização de *backups* que contenha funcionalidades de cópia total da instalação do SO, de preferência com função de armazenamento em nuvem.

REFERÊNCIAS BIBLIOGRÁFICAS

BARRETT, D.J.; SILVERMAN, R.E.; BYRNES, R.G. **SSH, The Secure Shell: The Definitive Guide**. O'Reilly Media, Incorporated, 2005. ISBN 9780596008956.

BATARD, P. **Rufus: Create bootable USB drives the easy way**. [S. l.], 2022. Disponível em: <https://rufus.ie/en/>. Acesso em: 8 dez. 2021.

CAMERON, J. **Introduction To Webmin**. [S. l.], 20 jun. 2016. Disponível em: <https://www.webmin.com/intro.html>. Acesso em: 25 mar. 2022.

CANONICAL LTD (org.). **Enterprise Open Source and Linux: Ubuntu**. [S. l.], 2022. Disponível em: <https://ubuntu.com/>. Acesso em: 8 dez. 2021.

CREATIVE COMMONS (org.). **Wikipedia**. [S. l.], 2022. Disponível em: <https://www.wikipedia.org/>. Acesso em: 19 mar. 2022.

DELISLE, M. **Mastering PhpMyAdmin 3.4 for Effective MySQL Management: A Complete Guide to Getting Started with PhpMyAdmin 3.4 and Mastering Its Features**. Reino Unido: Packt Pub., 2012.

DENT, K. D. **Postfix: The Definitive Guide**. Alemanha: O'Reilly Media, Incorporated, 2004.

DOSTÁLEK, L.; KABELOVÁ, A. **Understanding TCP/IP: a Clear and Comprehensive Guide to TCP/IP Protocols**. Packt Pub., 2006.

ENVATO PTY LTD (org.). **WordPress Themes - WordPress Templates: ThemeForest**. [S. l.], 2022. Disponível em: <https://themeforest.net/category/wordpress>. Acesso em: 6 abr. 2022.

FEDORA DOCUMENTATION PROJECT (org.). **Fedora 14 Security Guide**. Fultus Corporation, 2010

GOOGLE LLC (org.). **Gmail: email gratuito, privado e seguro: Google Workspace**. [S. l.], 2022. Disponível em: <https://www.google.com/intl/pt-PT/gmail/about/>. Acesso em: 7 mar. 2022.

HILL, B. M.; BACON, J. **O Livro Oficial do Ubuntu**. Brasil: Bookman, 2009.

ISO.ORG (org.). **ISO - ISO 9660: ISO images for computer files**. [S. l.], 2022. Disponível em: <https://www.iso.org/iso-9660-images-for-computer-files.html>. Acesso em: 29 mar. 2022.

MELNIKOV, A.; ZEILENGA, K. **RFC 4422: Simple Authentication and Security Layer (SASL)**. [S. l.], 2022. Disponível em: <https://datatracker.ietf.org/doc/html/rfc4422>. Acesso em: 18 abr. 2022.

MICROSOFT (org.). **Outlook: calendário e e-mail pessoal gratuitos da Microsoft**. [S. l.], 2022. Disponível em: <https://outlook.live.com/owa/>. Acesso em: 7 mar. 2022.

MOTA FILHO, J. E. **Análise de tráfego em redes TCP/IP**: utilize tcpdump na análise de tráfegos em qualquer sistema operacional. São Paulo: Novatec, 2013. 416 p. ISBN 9788575223758 (broch.).

NEGUS, C. **Linux**: a bíblia. 8. ed. Rio de Janeiro: Alta Books, 2014. 818 p. ISBN 9788576087991 (broch.).

NIC.BR (org.). **Registro.br**. [S. l.], 2022. Disponível em: <https://registro.br/>. Acesso em: 23 mar. 2022.

PARSONS, J. J.; OJA, D. **New Perspectives on Computer Concepts 2014**: Comprehensive. Estados Unidos: Cengage Learning, 2013. p. 396

RAZZOLI, F.; KENLER, F. **MariaDB Essentials**. Reino Unido: Packt Publishing, 2015.

SAWANT, U. R. **Ubuntu Server Cookbook**. Índia: Packt Publishing, 2016. p.128.

SMITH, J. **Major Distributions**: An overview of major Linux distributions and FreeBSD. [S. l.], 2022. Disponível em: <https://distrowatch.com/dwres.php?resource=major>. Acesso em: 16 mar. 2022.

THE APACHE SOFTWARE FOUNDATION (org.). **About the Apache HTTP Server Project**: The Apache HTTP Server Project. [S. l.], 2022. Disponível em: https://httpd.apache.org/ABOUT_APACHE.html. Acesso em: 25 mar. 2022.

THE LINUX FOUNDATION (org.). **Sobre a Let's Encrypt**: Let's Encrypt - Certificados SSL/TLS Gratuitos. [S. l.], 2022. Disponível em: <https://letsencrypt.org/pt-br/about/>. Acesso em: 6 mar. 2022.

THE PHP GROUP (org.). **PHP**: O que é o PHP? [S. l.], 2022. Disponível em: https://www.php.net/manual/pt_BR/intro-what-is.php. Acesso em: 4 abr. 2022.

THE SQUIRRELMAIL PROJECT TEAM (org.). **SquirrelMail**: Webmail for Nuts! [S. l.], 2016. Disponível em: <https://squirrelmail.org/>. Acesso em: 7 mar. 2022.

WORDPRESS.ORG (org.). **Blog Tool, Publishing Platform, and CMS**: WordPress.org. [S. l.], 2022. Disponível em: <https://wordpress.org/>. Acesso em: 4 abr. 2022.

GLOSSÁRIO

All: todos;

Aliases: apelidos;

Backup: é o processo de fazer cópias de dados ou arquivos de dados para uso caso os dados ou arquivos de dados originais sejam perdidos ou destruídos;

Banner Slider: Imagem de tamanho largura total para propaganda, que desliza lateralmente em um intervalo de tempo;

Blog: é uma espécie de diário online que aborda um assunto específico escolhido pelo seu autor;

Bug: é um jargão usado no ambiente de desenvolvimento para identificar uma falha no sistema;

Contêiner: ambiente isolado, disposto em um servidor, que divide um único *host* de controle;

Covid-19: é uma infecção respiratória aguda causada pelo coronavírus SARS-CoV-2, potencialmente grave, de elevada transmissibilidade e de distribuição global;

Desktop: é o termo utilizado para nomear o ambiente principal do computador, é usado também para fazer referência ao computador de mesa no sentido de diferenciá-lo do portátil;

Drop: derrubar;

E-mail: correio eletrônico;

Filter: filtro;

Firewall: é um elemento de uma rede, sendo baseado em *software* ou em *hardware*, que controla o tráfego de entrada e saída de informação, através da análise dos pacotes de dados

Framework: é uma abstração que une códigos comuns entre vários projetos de software provendo uma funcionalidade genérica;

Gateway: é um sistema ou equipamento encarregado de estabelecer a comunicação entre duas redes;

Hardware: é o conjunto dos componentes que compõem a parte material (física) de um computador;

Host: anfitrião;

Hostname: nome do anfitrião;

Hub: é um equipamento utilizado na área da informática para realizar a conexão de computadores de uma rede e possibilitar a transmissão de informações entre essas máquinas;

Input: entrada;

Interface: elemento que proporciona uma ligação física ou lógica entre dois sistemas ou partes de um sistema que não poderiam ser conectados diretamente;

Kernel: é o componente principal de um sistema operacional Linux e a interface central entre o hardware e os processos executados por um computador;

Kubernetes: produto de código aberto utilizado para automatizar a implantação, o dimensionamento e o gerenciamento de aplicativos em contêiner;

Lite: versão mais simples, ou subconjunto, de algo, em que a complexidade é perdida por uma aplicação mais fácil;

Login: é um termo em inglês usado no âmbito da informática, um neologismo que significa ter acesso a uma conta de *e-mail*, computador, celular ou outro serviço;

Malware: é um termo genérico para qualquer tipo de *software* de computador com intenção maliciosa;

Modem: dispositivo de entrada e saída, utilizado para transmissão de dados entre computadores através da linha telefônica;

Passwd: é uma ferramenta na maioria dos sistemas operacionais Unix e tipo Unix usada para alterar a senha de usuário;

Pendrive: é um dispositivo constituído por uma memória regravável e que possui a função de armazenamento de dados;

Ping: é um sinal enviado a um anfitrião que solicita uma resposta;

Plugin: são adições ou alterações de *software* que permitem a personalização de programas de computador, aplicativos e navegadores da *web*, bem como a personalização do conteúdo oferecido pelos *sites*;

Powershell: é uma solução de automação de tarefas multiplataforma que consiste em um terminal de linha de comando, em uma linguagem de *script* e uma estrutura de gerenciamento de configuração;

Premium: é de algo com qualidade maior ou superior;

Pro: versão reduzida de *professional*, profissional;

Rack: móvel com prateleiras, destinado a conter subconjuntos de aparelhos de informática que ficam interligados;

Ransomware: é um tipo de *malware* que impede os usuários de acessarem seu sistema ou arquivos pessoais e exige o pagamento do resgate para recuperar o acesso;

Root: usuário raiz administrador de um Sistema Operacional Linux;

Roteador: é um dispositivo que encaminha pacotes de dados entre redes de computadores, criando um conjunto de redes de sobreposição;

Samba: é o conjunto de programas de interoperabilidade padrão do Windows para Linux e Unix;

Script: conjunto de instruções para que uma função seja executada em determinado aplicativo;

Shadow: senhas de sombra, são um aprimoramento para a segurança de *login* em sistemas Unix;

Site: local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações em multimídia;

Software: conjunto de componentes lógicos de um computador ou sistema de processamento de dados;

Spam: são conteúdos enviados pelo remetente sem o consentimento do destinatário;

Switch: é um equipamento de rede que permite interconectar dispositivos em uma rede de computadores, usando comutação de pacotes para receber, processar e encaminhar dados ao dispositivo de destino;

Vpopmail: é um pacote de software GPL gratuito, para fornecer uma maneira de gerenciar domínios de *e-mail* virtuais e contas de *e-mail*;

Web: nome pelo qual a rede mundial de computadores internet se tornou conhecida a partir de 1991, quando se popularizou devido à criação de uma interface gráfica que facilitou o acesso e estendeu seu alcance ao público em geral;

Webmail: um serviço de correio eletrônico que pode ser acessado por qualquer navegador conectado à Internet;

Webmaster: nomenclatura utilizada para o usuário administrador de páginas de Internet;

Website: página ou conjunto de páginas da Internet com informação diversa, acessível através de computador ou de outro meio eletrônico;

Whois: é um protocolo que armazena as informações sobre quem são os proprietários dos domínios.