

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

Projeto da Infraestrutura de Rede Híbrida da CallNet Solutions

Alunos: Alisson Anderson de Carvalho, Carlos Alberto Morais Junior, Giulia Fernandes Donato de Mattos, Isadora Aparecida Cardoso Carvalho, Rafael Fernandes Marques e Rômulo Ferraz Chaves.

Professora: Shirley Luana Ramos de Assis

**Resumo**

O presente trabalho tem como objetivo apresentar a CallNet Solutions, contextualizando sua história, missão, visão, estrutura organizacional e os serviços oferecidos. Ademais, é introduzida a proposta de implantação de uma infraestrutura de rede híbrida, composta por recursos locais e em nuvem, que suporte o crescimento da empresa de forma segura e escalável. Embora seja apresentada uma visão geral da topologia da rede, os detalhes técnicos são explorados de forma aprofundada neste relatório específico. O projeto contempla serviços de rede essenciais como DHCP, DNS, Active Directory, hospedagem de aplicação web e mecanismos de monitoramento e segurança. A infraestrutura foi planejada com base em boas práticas de documentação e organização, demonstrando a viabilidade de uma solução híbrida para uma empresa de médio porte.

# Sumário

1. Introdução 1.1. Contexto e História da Empresa 1.2. Missão e Visão 1.3. Estrutura Organizacional 1.4. Produtos e Serviços
2. Planejamento da Infraestrutura de Rede 2.1. Visão Geral da Topologia da Rede 2.2. Tabela de Equipamentos de Rede
3. Configuração do Ambiente Local 3.1. Máquina Servidor (Windows Server 2025) 3.2. Máquina Cliente (Windows 11 Enterprise)
4. Configuração do Ambiente em Nuvem 4.1. Infraestrutura AWS 4.2. Especificações da Instância EC2
5. Serviços Implantados 5.1. Serviços Locais 5.2. Serviços em Nuvem
6. Monitoramento da Infraestrutura 6.1. Arquitetura de Monitoramento 6.2. Configuração dos Hosts
7. Política de Segurança da Informação
8. Conclusão
9. Ata das Reuniões
10. Referências

# INTRODUÇÃO

Nosso projeto tem como finalidade apresentar a CallNet Solutions, sua trajetória e seus serviços, além de propor uma visão inicial da topologia de rede planejada para dar suporte às suas operações. A proposta de infraestrutura visa garantir estabilidade, segurança, expansão e continuidade dos serviços prestados pela organização.

## 1.1. Contexto e História da Empresa

A CallNet Solutions foi fundada em 2015, em Belo Horizonte, como uma startup com a visão de revolucionar o atendimento ao cliente por meio de soluções inteligentes baseadas em chatbots e automações. Inicialmente, com apenas cinco funcionários, a empresa oferecia serviços personalizados para pequenas oficinas mecânicas locais. Devido ao comprometimento da equipe e à receptividade do mercado, a CallNet rapidamente ganhou espaço.

Com o crescimento da carteira de clientes e a demanda por atendimento em outras regiões, em 2017 a empresa expandiu para o sudeste, inaugurando uma filial em São Paulo. Esta expansão foi um passo estratégico para fortalecer a presença da CallNet no maior polo econômico do Brasil. A nova unidade, embora modesta inicialmente, focou em atender clientes de médio porte e explorar parcerias com empresas da capital paulista. Este movimento marcou o início da transição da CallNet de startup para uma empresa em expansão nacional.

Em 2019, em decorrência do sucesso da filial paulista, a CallNet estabeleceu sua segunda unidade fora da matriz, no Rio de Janeiro. Contudo, a expansão fluminense enfrentou o desafio inesperado da pandemia de COVID-19. O isolamento social e as restrições impuseram à empresa uma rápida adaptação de seus processos, com a implementação de infraestrutura para trabalho remoto, o reforço da segurança de dados e a migração de parte dos serviços para a nuvem. Apesar das dificuldades, a filial do Rio de Janeiro tornou-se um exemplo de resiliência, inovação e capacidade de adaptação — características que atualmente fazem parte do DNA da CallNet Solutions.

## 1.2. Missão e Visão

Missão: Oferecer soluções inteligentes de atendimento e prospecção para oficinas mecânicas, com alta tecnologia, atendimento humanizado e suporte técnico eficiente, promovendo a produtividade e a satisfação dos clientes.

Visão: Tornar-se a principal referência no sudeste do Brasil em automação de atendimento e geração de leads para o setor automotivo até 2030.

## 1.3. Estrutura Organizacional

A CallNet Solutions possui uma estrutura organizacional distribuída, conforme detalhado a seguir:

Matriz (Belo Horizonte): Conta com 30 funcionários, com foco principal em governança, desenvolvimento e suporte técnico.

Filial São Paulo: Possui 20 funcionários, atuando em vendas corporativas e relacionamento com grandes clientes.

Filial Rio de Janeiro: Dispõe de 15 funcionários, dedicada ao suporte e prospecção de clientes.

## 1.4. Produtos e Serviços

A CallNet Solutions oferece uma gama de produtos e serviços voltados para o setor automotivo, com foco em automação de atendimento e prospecção:

Sistema de Atendimento e Gerenciamento de Clientes (CRMChat): Uma plataforma completa para a gestão de interações com clientes, utilizando chatbots para otimizar o suporte e follow-ups.

Geração de Leads Qualificados: Utilização de inteligência artificial para identificar e qualificar potenciais clientes para oficinas mecânicas.

Consultoria em Automação: Prestação de serviços de consultoria para auxiliar oficinas na implementação de processos de automação.

Suporte Técnico Especializado: Equipe dedicada para garantir o pleno funcionamento das soluções implementadas, com atendimento humanizado.

## Resumo da Seção 1:

Apresentamos a CallNet Solutions, abordando sua história de crescimento e adaptação, especialmente após a pandemia. Foram delineadas a missão de oferecer soluções inteligentes para o setor automotivo e a visão de se tornar referência em automação até 2030. A estrutura organizacional, com matriz e filiais, foi detalhada, assim como os principais produtos e serviços oferecidos pela empresa.

# Planejamento da Infraestrutura de Rede

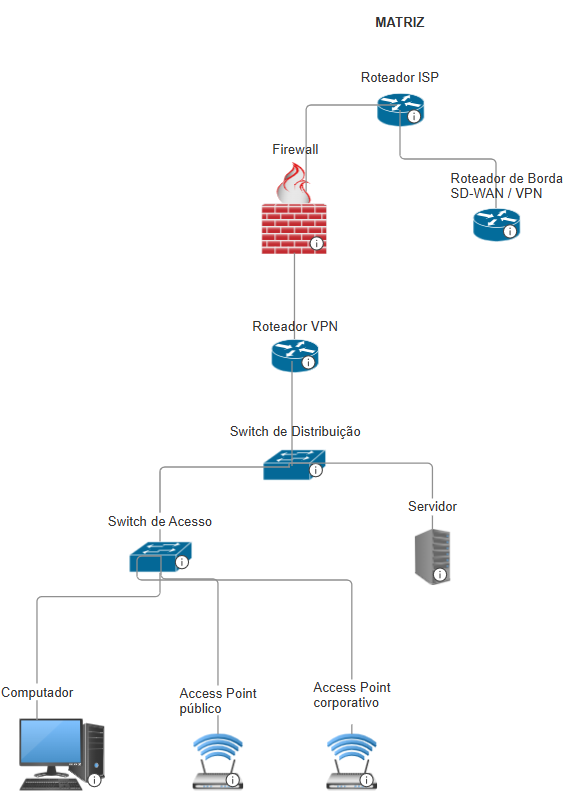
A infraestrutura de rede da CallNet Solutions foi planejada com base em boas práticas de documentação e organização, conforme demonstrado na planilha de recursos de rede elaborada para o projeto. A documentação abrange todos os dispositivos, IPs e serviços necessários para uma operação segura e funcional da rede.

Tabela de equipamentos de rede

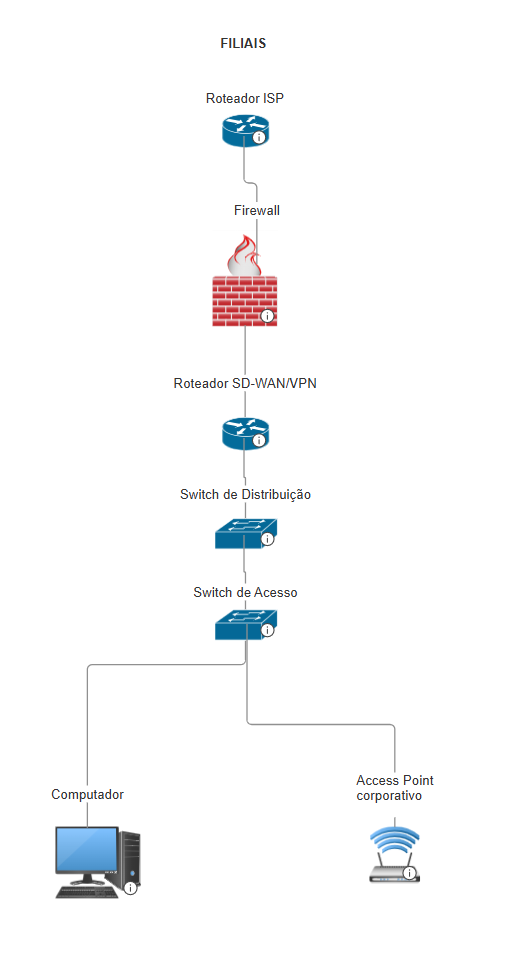
## Visão Geral da Topologia da Rede

A arquitetura de rede da CallNet Solutions é híbrida, integrando recursos locais e em nuvem para garantir segurança, escalabilidade e continuidade dos negócios. Essa infraestrutura híbrida conta com um sistema de monitoramento implementado com Zabbix, hospedado em uma VM local. Foram configurados agentes tanto no servidor local quanto na instância em nuvem (EC2 - AWS), possibilitando a coleta de métricas essenciais como uso de CPU, memória e disco. Essa solução permite o acompanhamento em tempo real da performance dos ambientes, facilitando a identificação de falhas e o planejamento de capacidade. O tráfego dos agentes é controlado por políticas de firewall locais e regras nos grupos de segurança da AWS, garantindo a segurança das informações monitoradas.

**Topologia:**   
 Na **matriz**, a conexão com a internet é protegida por um firewall dedicado, seguida por um roteador SD-WAN/VPN que estabelece a comunicação segura com as filiais. Internamente, a rede é estruturada com switches de distribuição e acesso, conectando servidores, computadores, e access points segmentados para redes corporativas e públicas.



As **filiais** seguem uma arquitetura semelhante em menor escala, com roteador ISP, firewall, roteador SD-WAN/VPN, e switches, permitindo acesso seguro tanto via rede cabeada quanto Wi-Fi corporativo.



Esta organização proporciona à empresa escalabilidade, controle sobre o tráfego de dados, e proteção contra ameaças, além de facilitar a expansão futura da rede.

## Tabela de Equipamentos de Rede

A tabela de equipamentos de rede, detalhada no planejamento da infraestrutura, abrange todos os dispositivos, IPs e serviços necessários para a operação segura e funcional da rede.

## Resumo da Seção 2:

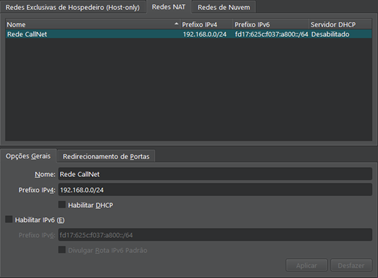
O planejamento da infraestrutura de rede da CallNet Solutions foi apresentado, destacando a abordagem híbrida que combina ambientes locais e em nuvem. A topologia da rede, com seus componentes e a interconexão entre matriz e filiais, foi descrita, enfatizando a segurança e a escalabilidade como pilares do projeto.

# Configuração do Ambiente Local

O ambiente local foi simulado utilizando o VirtualBox.

## Máquina Servidor (Windows Server 2025)

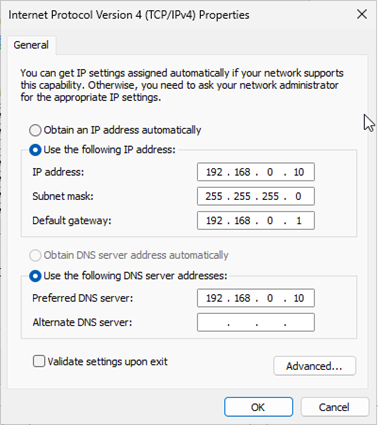
Uma nova rede NAT interna, denominada 'Rede CallNet', foi criada para simular o funcionamento de um roteador principal. A faixa de IP definida para essa rede é 192.168.0.0/24.

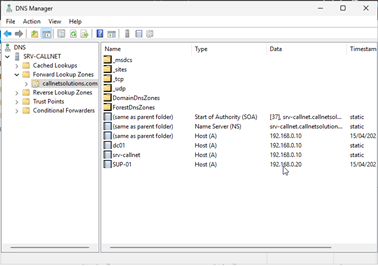
  
Faixa de IP 192.168.0.0/24

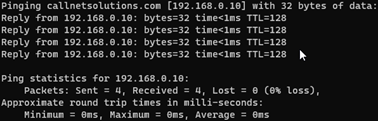
Os serviços de Active Directory Domain Services, DNS Server, DHCP Server e Remote Desktop Services foram instalados em uma máquina com Windows Server 2025, denominada ‘SRV-CALLNET’. Esta máquina opera com IP fixo 192.168.0.10 e atua como servidor DNS, DHCP e controlador de domínio (Active Directory).

* Configuração DNS: O servidor foi configurado para atuar como servidor DNS, apontando para si mesmo. Uma zona DNS primária ‘callnetsolutions.com’ foi criada. Testes de conectividade e resolução de nomes foram realizados com sucesso utilizando os comandos ‘ping callnetsolutions.com’ e ‘nslookup callnetsolutions.com’.
* Configuração DHCP: O serviço DHCP foi configurado com uma faixa de distribuição de IPs de 192.168.0.20 a 192.168.0.100. O gateway padrão (Router) foi definido como 192.168.0.1 e o DNS como 192.168.0.10. O nome de domínio pai foi configurado como ‘callnetsolutions.com’.
* Configuração Active Directory: O domínio ‘callnetsolutions.com’ foi criado no Active Directory. A estrutura de usuários e computadores foi configurada.

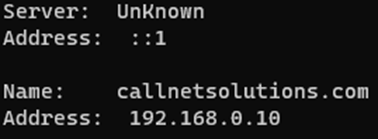
Abaixo, apresentamos evidências das configurações e testes de cada serviço:

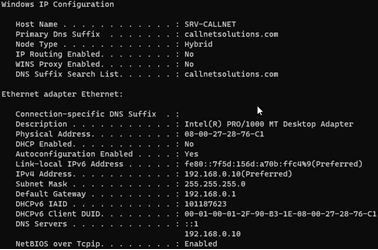
  
Configuração para atuar como servidor DNS, apontando para si mesmo

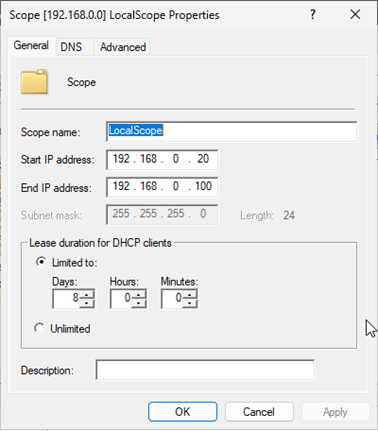
  
Zona DNS primária ‘callnetsolutions.com’

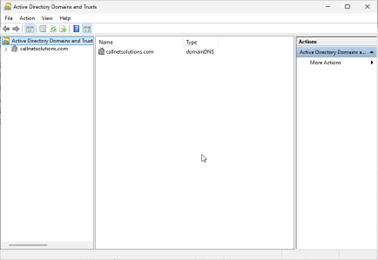


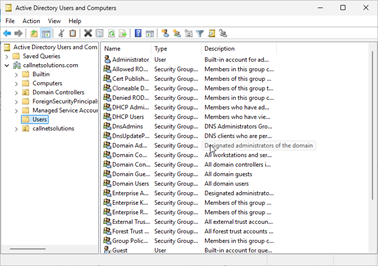
Teste com comando ‘ping callnetsolutons.com’

  
Teste com comando ‘nslookup callnetsolutions.com’

  
Teste com comando ‘ipconfig /all’

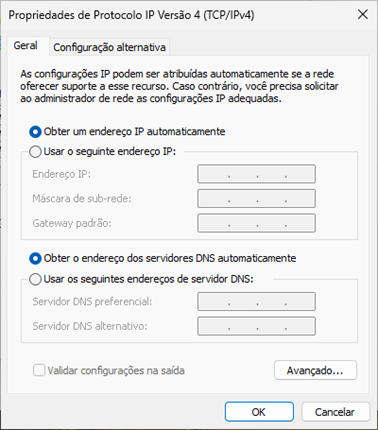
  
 DHCP com faixa de distribuição (range) 192.168.0.20 a 192.168.0.100

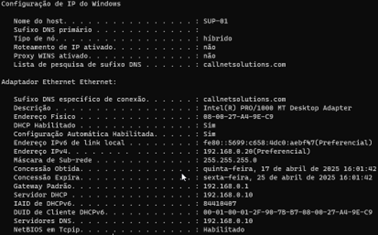
  
Domínio criado no Active Directory

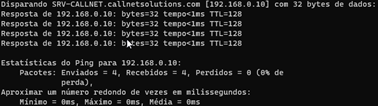
  
Usuários e Computadores do Active Directory

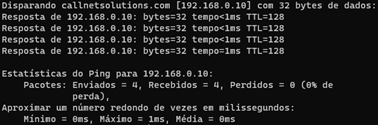
## Máquina Cliente (Windows 11 Enterprise)

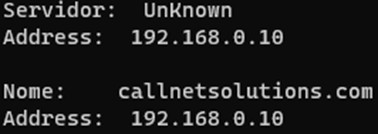
Uma nova máquina com Windows 11 Enterprise, denominada ‘SUP-01’, foi criada e conectada à ‘Rede CallNet’ para atuar como cliente. O endereço IP da máquina cliente foi atribuído automaticamente via DHCP, e a conexão ao domínio ‘callnetsolutions.com’ no Active Directory foi realizada com sucesso. Testes de conectividade foram confirmados por meio dos comandos ‘ipconfig /all’, ‘ping SRV-CALLNET’ e ‘ping callnetsolutions.com’. A resolução do domínio foi validada com ‘nslookup callnetsolutions.com’, e a máquina recebeu a mensagem de boas-vindas ao domínio.

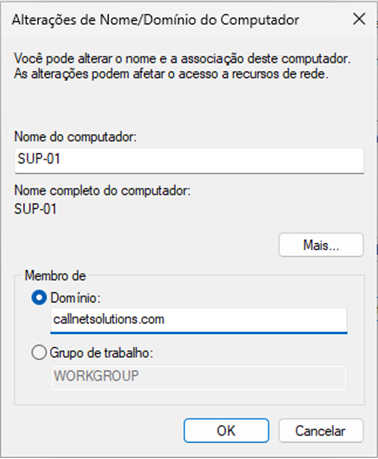
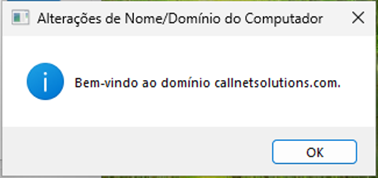
  
 Máquina obtendo endereço IP dinamicamente

  
Teste com comando ‘ipconfig /all’ (Obteve dinamicamente o IP 192.168.0.20 por meio do DHCP corretamente)

  
Teste com ‘ping SRV-CALLNET’ (Obteve resposta do servidor corretamente)

  
Teste com comando ‘ping callnetsolutions.com’ (Obteve resposta do servidor corretamente)

  
Teste com comando ‘nslookup callnetsolutions.com’ (com resolução do domínio com resposta adequada)

  
  
Mensagem de boas-vindas ao domínio

## Resumo da Seção 3:

Esta seção detalhou a configuração do ambiente de rede local. Foi explicada a criação da rede NAT interna e a configuração dos serviços essenciais (DHCP, DNS e Active Directory) no servidor Windows Server 2025. Adicionalmente, foi demonstrada a correta integração de uma máquina cliente ao domínio, com a obtenção dinâmica de IP e a resolução de nomes.

# Configuração do Ambiente em Nuvem

A infraestrutura em nuvem da CallNet Solutions foi implementada na Amazon Web Services (AWS) com uma Virtual Private Cloud (VPC) e um Grupo de Segurança exclusivos, garantindo isolamento e controle de rede.

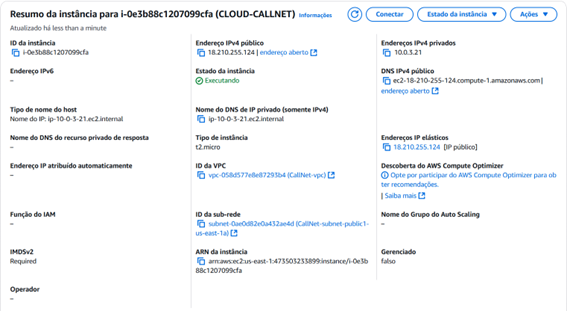
## Infraestrutura AWS

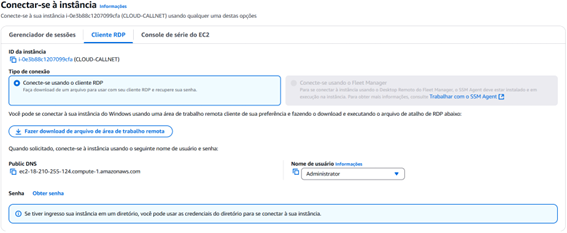
A instância EC2 utilizada opera com Windows Server 2022 e possui acesso seguro via chave .pem para autenticação por criptografia de chave pública.

## Especificações da Instância EC2

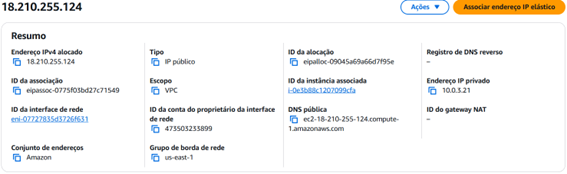
As especificações da instância em nuvem são as seguintes:

* **Provedor:** Amazon Web Services (AWS)
* **Serviço:** EC2 – Elastic Compute Cloud
* **Sistema Operacional:** Windows Server 2022 Base
* **Tipo de instância:** t2.micro
* **IP público fixo:** 18.210.255.124
* **Par de chaves:** CallNet.pem

  
Resumo da instância ‘CLOUD-CALLNET’

  
Detalhes da conexão RDP

  
Chave criptografada ‘CallNet.pem’

  
Configuração do IP elástico

## Resumo da Seção 4:

A configuração do ambiente em nuvem foi apresentada, destacando a utilização da AWS. Foi detalhada a implementação de uma VPC e um Grupo de Segurança para garantir a segurança da rede. As especificações da instância EC2, incluindo o sistema operacional, tipo e IP público, foram listadas.

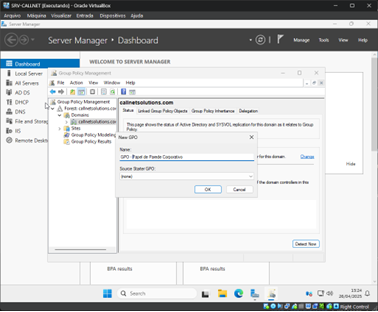
# Serviços Implantados

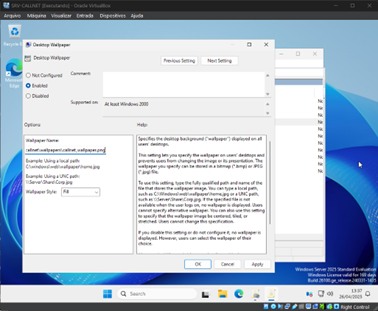
Diversos serviços essenciais foram implantados tanto no ambiente local quanto no ambiente em nuvem para suportar as operações da CallNet Solutions.

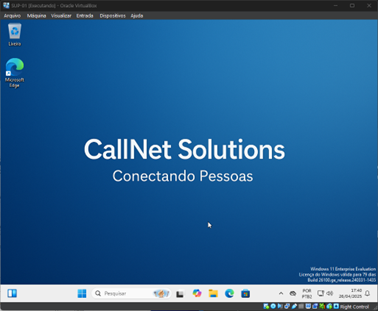
## Serviços Locais

No servidor local (Windows Server 2025), foram implantados os seguintes serviços:

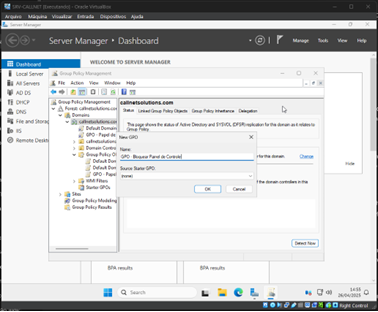
* **DNS (Domain Name System):**
* Criação da Zona de Pesquisa Direta: callnetsolutions.com (Zona Primária).
* Encaminhadores DNS (Forwarders): Configurado para utilizar o DNS externo 8.8.8.8 (Google).
* **DHCP (Dynamic Host Configuration Protocol):**
* Faixa de IPs: 192.168.0.20 a 192.168.0.100.
* Gateway padrão (Router): 192.168.0.1.
* Servidor DNS: 192.168.0.10.
* Nome do Domínio (Parent Domain): callnetsolutions.com.
* **Active Directory:**
* Nome do domínio raiz: callnetsolutions.com.
* Nome NetBIOS: CALLNET.
* **Configuração de GPOs (Group Policy Objects):**
* **Papel de Parede Corporativo:** Uma GPO foi configurada para aplicar um papel de parede corporativo em todas as máquinas da rede local. O papel de parede foi centralizado em um compartilhamento de rede, e a política foi aplicada através do Active Directory. Todos os computadores da rede, ao serem configurados e logados, terão o papel de parede corporativo aplicado automaticamente.
* **Bloqueio do Painel de Controle:** Uma GPO foi configurada para desabilitar o acesso ao Painel de Controle através das configurações de "Restrições de Controle de Acesso". Esta política impede que usuários finais modifiquem configurações críticas do sistema.
* **Papel de Parede Corporativo:**

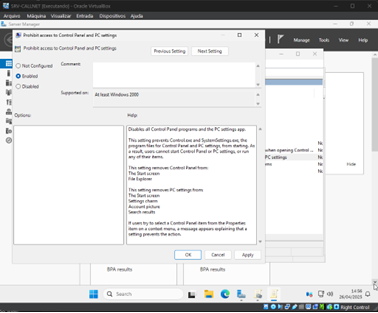
  
A GPO foi configurada para aplicar um papel de parede corporativo em todas as máquinas da rede local

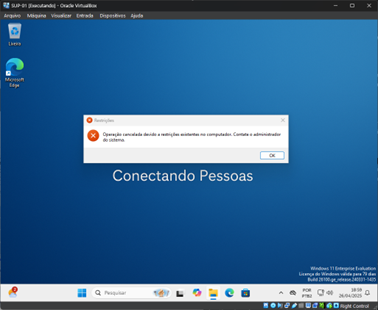
  
O papel de parede foi centralizado em um compartilhamento de rede e a política foi aplicada através do Active Directory

  
Todos os computadores da rede, ao serem configurados e logados, terão o papel de parede corporativo aplicado automaticamente

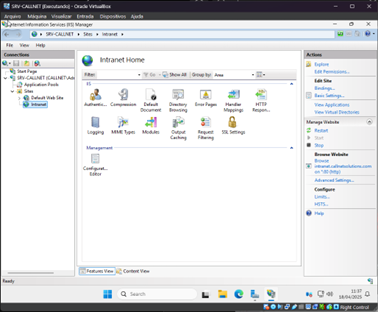
* **Bloqueio do Painel de Controle:**

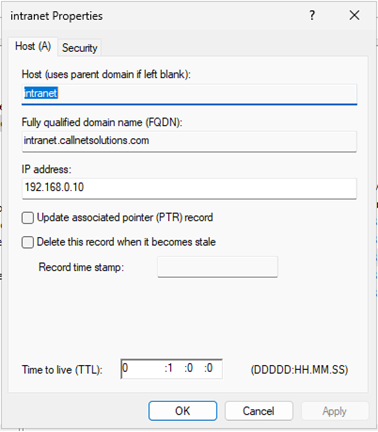
  
A GPO foi configurada para desabilitar o acesso ao Painel de Controle através das configurações de "Restrições de Controle de Acesso"

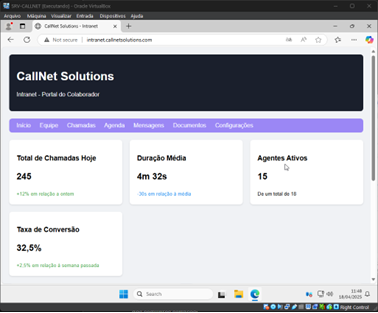
  
Política aplicada: "Proibir o acesso ao Painel de Controle e às Configurações do Sistema"

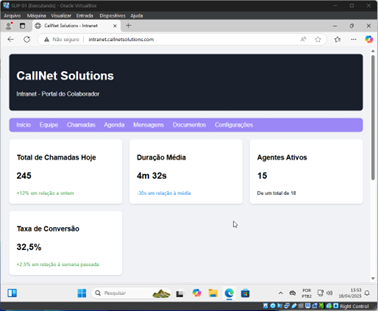
  
Usuários finais não terão acesso ao Painel de Controle e não poderão modificar configurações críticas do sistema

* **Servidor Web IIS para Intranet:**
* Um servidor IIS (Internet Information Services) foi configurado com uma página de Intranet para acesso exclusivo na rede local.
* A aplicação ‘Intranet’ foi criada no IIS.
* Foi adicionada a entrada ‘intranet’ no DNS.
* A página da intranet é acessível em intranet.callnetsolutions.com.

  
Aplicação ‘Intranet’ criada no IIS

  
Adicionada a entrada ‘intranet’ no DNS

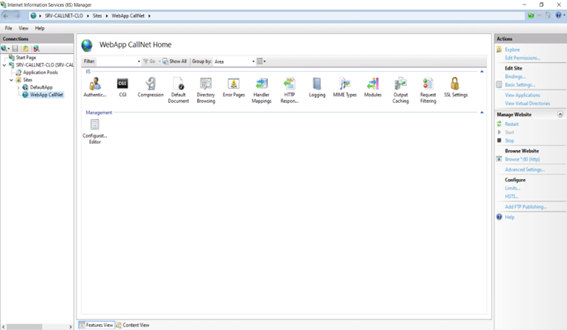
  
DNS propagado corretamente, página da intranet acessível em ‘intranet.callnetsolutions.com’

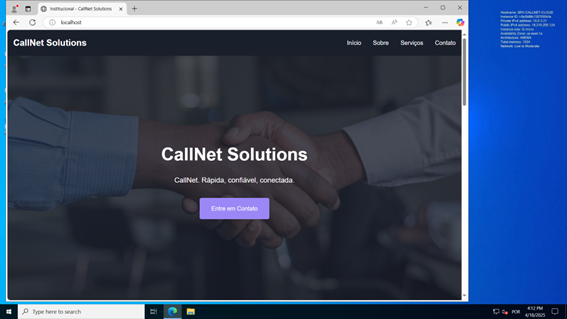
  
Acesso ao ‘intranet.callnetsolutions.com’ na máquina cliente (SUP-01)

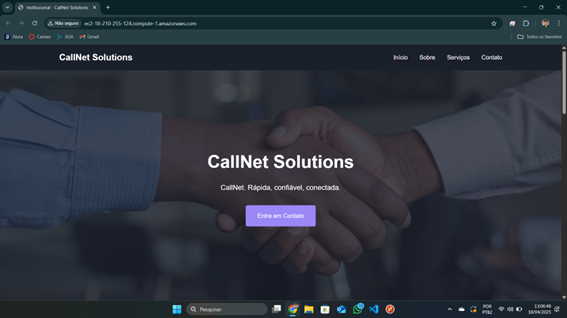
## Serviços em Nuvem

Na instância em nuvem (AWS EC2), foram configurados os seguintes serviços:

* **Servidor Web IIS para Aplicações Web Externas:**
* Um servidor IIS foi configurado para hospedar uma página de boas-vindas para acesso tanto interno quanto externo.
* A aplicação ‘WebApp CallNet’ foi criada no IIS. A aplicação pode ser executada localmente no servidor e externamente.
* **Serviço FTP (File Transfer Protocol):**
* Para facilitar a troca segura de arquivos entre a empresa e parceiros externos, um serviço FTP será implementado na instância em nuvem utilizando o IIS. Este serviço permitirá o upload e download de arquivos com controle de acesso, garantindo a integridade e confidencialidade dos dados. A configuração incluirá o mapeamento de diretórios virtuais e a definição de permissões de usuário, além da utilização de SSL/TLS para criptografia das conexões (FTPS).

Aplicação ‘WebApp CallNet’ criada no IIS

Aplicação sendo executada localmente no servidor

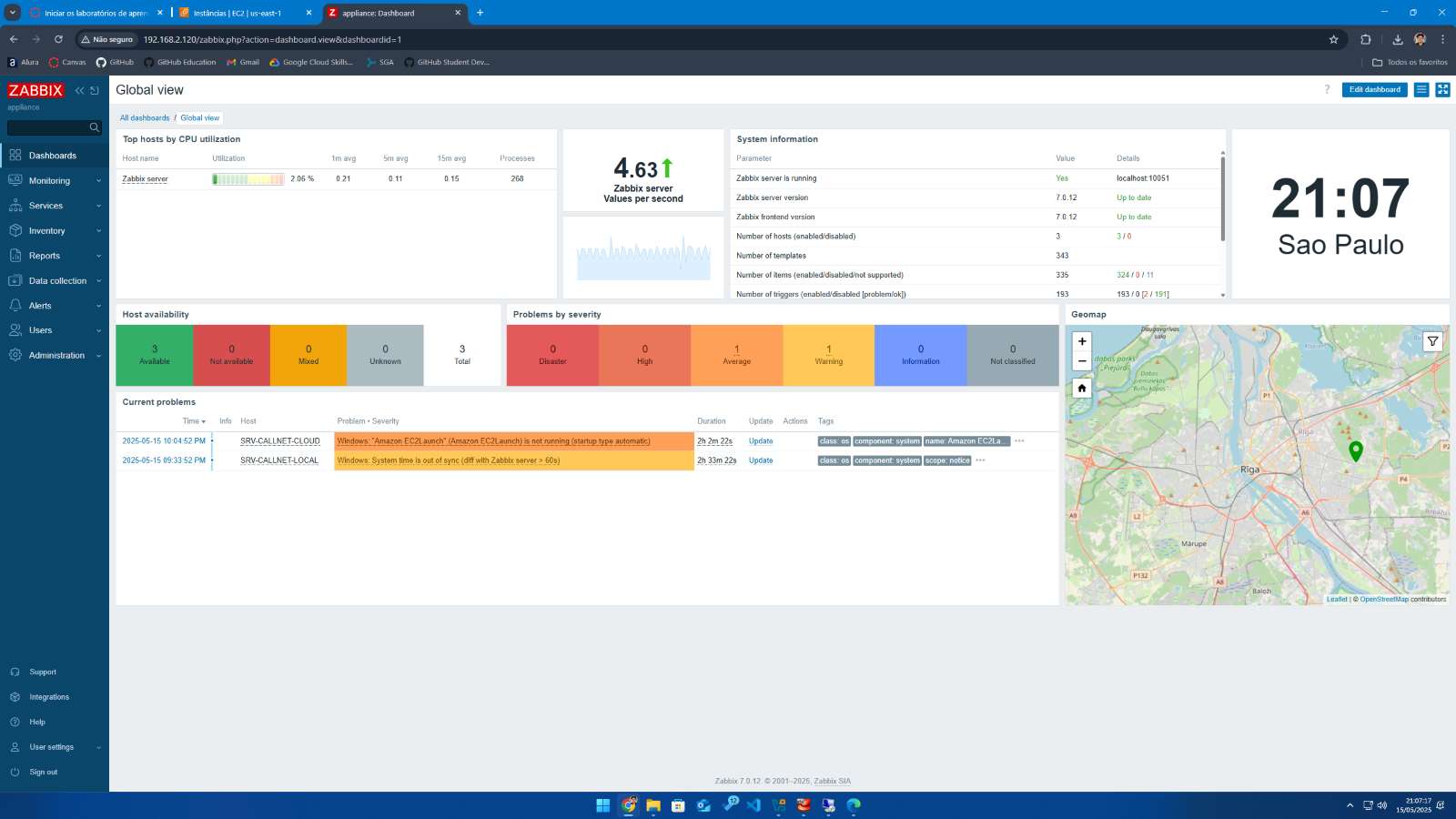
Aplicação sendo executada externamente

## Resumo da Seção 5:

Detalhamos os serviços implantados nos ambientes local e em nuvem. No ambiente local, foram configurados e testados o DNS, DHCP, Active Directory com GPOs para papel de parede e bloqueio do Painel de Controle, além de um servidor web IIS para intranet. No ambiente em nuvem, foi configurado um servidor web IIS para aplicações externas, e foi proposta a implementação de um serviço FTP para a troca segura de arquivos.

# Monitoramento da Infraestrutura

Para garantir a visibilidade e o controle da saúde dos ativos de TI, foi implementado um sistema de monitoramento utilizando o Zabbix, uma solução de código aberto amplamente adotada para monitoramento de redes, servidores e serviços.



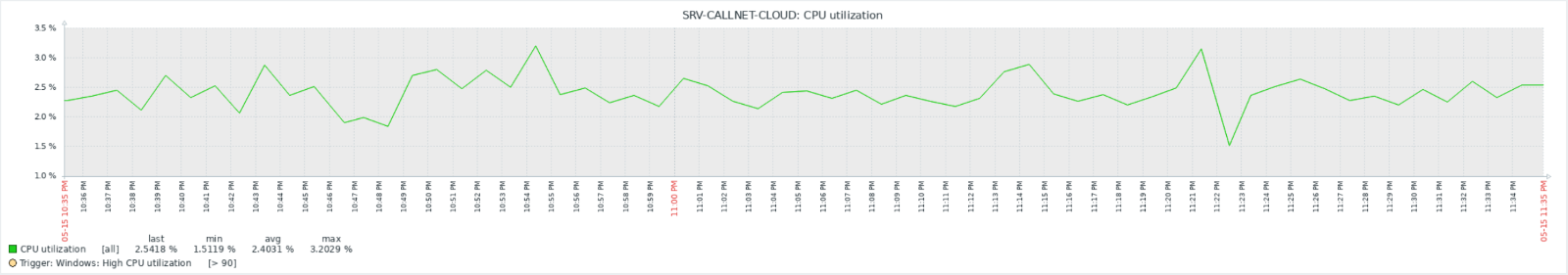
A solução de monitoramento abrange tanto o servidor local com Windows Server 2025 quanto a instância em nuvem na AWS, configurada com o Windows Server 2022.

## **Arquitetura de Monitoramento**

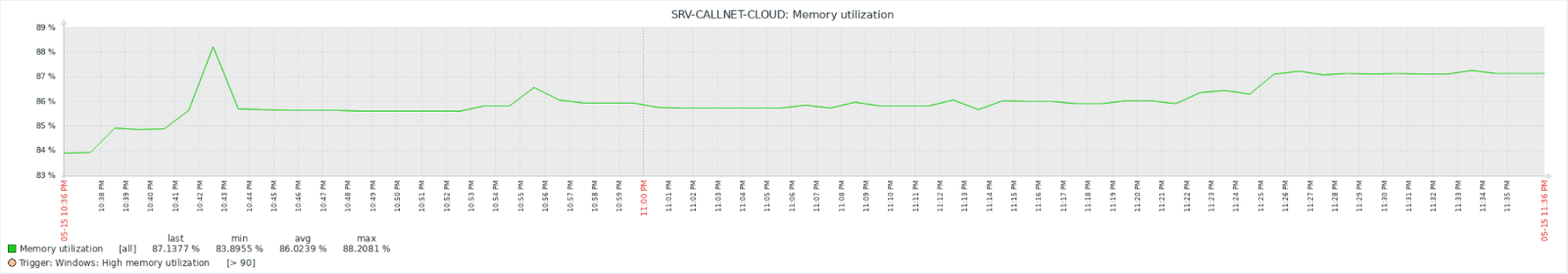
O Servidor Zabbix foi implantado em uma máquina virtual local, utilizando um appliance do Zabbix no VirtualBox, o que proporcionou rápida configuração e gerenciamento centralizado. Agentes Zabbix foram instalados tanto na instância EC2 (Windows Server 2022) quanto no servidor local (Windows Server 2025) via pacote MSI.

## **Configuração dos Hosts**

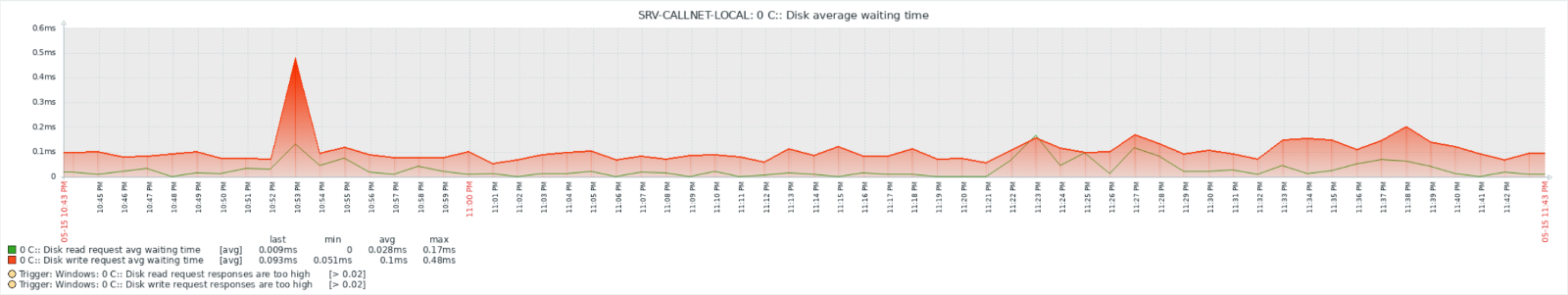
* **Instância em Nuvem (EC2 - Windows Server 2022):**
* Um host foi criado no Zabbix Server com o IP público da instância (18.210.255.124).
* O Grupo de Segurança da AWS foi configurado para permitir tráfego TCP na porta 10050, essencial para a comunicação com o agente Zabbix.
* O agente Zabbix foi instalado com MSI e configurado para apontar para o IP local do servidor Zabbix.
* Métricas monitoradas incluem Uso de CPU, Memória RAM e Utilização de Disco.
* Uso de CPU



* Memória RAM



* Utilização de Disco



* O firewall do Windows foi automaticamente configurado durante a instalação do agente Zabbix, liberando a porta 10050 para conexões de entrada.

A configuração do Zabbix permite o acompanhamento em tempo real de indicadores essenciais de desempenho (KPIs) dos dois ambientes — nuvem e local. Com isso, a equipe de TI pode agir preventivamente em casos de sobrecarga de CPU, falta de memória ou baixa disponibilidade de espaço em disco.

## Resumo da Seção 6:

Detalhamos a implementação do sistema de monitoramento Zabbix, cobrindo tanto os ambientes locais quanto em nuvem. A arquitetura de monitoramento, incluindo o servidor Zabbix e a instalação dos agentes, foi descrita. As configurações dos hosts em nuvem e locais foram especificadas, e as métricas de desempenho monitoradas, como uso de CPU, memória RAM e utilização de disco, foram listadas, destacando a capacidade de ação preventiva da equipe de TI.

# **Política de Segurança da Informação (PSI)**

Criamos a Política de Segurança da Informação (PSI) da CallNet Solutions, um documento fundamental que estabelece as diretrizes e responsabilidades para a proteção dos ativos de informação da empresa. Com um propósito claro de minimizar riscos, prevenir incidentes e assegurar a continuidade dos negócios, esta PSI abrange todos os indivíduos que interagem com os sistemas, redes e informações da CallNet Solutions, independentemente de sua localização.

O documento é estruturado em torno de princípios orientadores essenciais: Confidencialidade, Integridade, Disponibilidade, Conformidade e Responsabilidade. Estes pilares garantem que as informações sensíveis sejam acessíveis apenas a pessoas autorizadas, que os dados sejam precisos e protegidos contra modificações, que os sistemas estejam sempre operacionais, que a empresa opere dentro das leis e padrões, e que todos os colaboradores compreendam seu papel na segurança.

A PSI detalha uma série de controles técnicos e operacionais cruciais, divididos em seções chave:

* **Gestão de Acesso:** Define regras rigorosas para o controle de acesso lógico (menor privilégio, senhas complexas e periódicas, MFA, bloqueio de sessões inativas) e físico (sistemas de acesso, monitoramento, registro de visitantes).
* **Segurança de Redes e Sistemas:** Aborda a implementação de firewalls, segmentação de rede (VLANs), uso obrigatório de VPN para acesso remoto, atualização constante de software, soluções antivírus/antimalware e a configuração segura (hardening) de servidores e equipamentos.
* **Segurança da Informação em Nuvem (AWS):** Reconhece a responsabilidade compartilhada com a AWS e especifica a utilização de VPCs, sub-redes privadas, Grupos de Segurança, NACLs, AWS IAM, criptografia de dados e rotinas de backup para o ambiente em nuvem.
* **Backup e Recuperação de Desastres:** Enfatiza a necessidade de backups regulares, seguros e externos, além de testes periódicos dos planos de recuperação para garantir a resiliência.
* Resposta a Incidentes de Segurança: Estabelece a criação de um plano formal para detecção, contenção, erradicação e recuperação de incidentes, com foco na comunicação imediata.
* **Conscientização e Treinamento:** Prevê treinamentos regulares e campanhas de conscientização para manter os funcionários informados sobre as ameaças e as melhores práticas.
* **Auditoria e Revisão:** Garante que a segurança da informação seja auditada periodicamente e que a própria política seja revisada anualmente ou conforme necessário para adaptação.

Além da política formal, desenvolvemos também uma Cartilha de Boas Práticas de Acesso Seguro para Colaboradores. Esta cartilha serve como um guia prático e de fácil compreensão para o dia a dia, cobrindo tópicos como senhas fortes, acesso seguro à rede, prevenção de phishing, proteção contra malware e uso consciente da informação. Ela reforça o conceito de que a segurança é uma responsabilidade compartilhada, delineando também as penalidades associadas ao não cumprimento das normas.

Por fim, a PSI detalha os Mecanismos de Proteção, Rastreamento de Vulnerabilidades e Soluções de Atenuação. Esta seção aprofunda as ferramentas e estratégias para proteger a confidencialidade, integridade e disponibilidade (como criptografia, controle de acesso, segmentação de rede, redundância, monitoramento com Zabbix) e, crucialmente, as metodologias proativas para identificar e mitigar vulnerabilidades. Isso inclui o uso de scanners de rede (OpenVAS/Nessus) e aplicações web (OWASP ZAP/Burp Suite), análise de logs (Zabbix/SIEM) e ferramentas de auditoria de configuração. A política também elenca vulnerabilidades comuns (força bruta, phishing, RDP não autorizado, falhas em aplicações web e sistemas operacionais) e suas respectivas atenuações, demonstrando um plano robusto de defesa.

## **Resumo da Seção 7:**

Apresentamos a PSI da CallNet Solutions, que em suma, é um documento abrangente e bem estruturado, que fornece uma base sólida para a gestão da segurança da informação na empresa, abordando tanto aspectos técnicos quanto humanos, e estabelecendo um ciclo contínuo de proteção, monitoramento e aprimoramento.

# 8 CONCLUSÃO

O projeto demonstrou a viabilidade de uma solução híbrida para a CallNet Solutions, utilizando tanto ambientes locais quanto recursos em nuvem. A adoção de uma infraestrutura tecnológica robusta e híbrida é fundamental para a continuidade e expansão sustentável dos negócios. Com a implementação proposta, a empresa está apta a atender às demandas crescentes do mercado, garantindo segurança, desempenho e flexibilidade. A utilização de boas práticas de documentação, segurança, automação e organização garantiu uma entrega coerente com os critérios de aceite propostos.

# 9 Ata das Reuniões

**Etapa 1**

1. Planejamento do projeto de uma infraestrutura de redes;

2. Criação de planilha de recursos de rede seguindo boas práticas de documentação;

3. Demonstração da subdivisão da rede por meio de técnicas de endereçamento NAT;

4. Distribuição de equipamentos de rede de maneira organizada, completa e específica, de acordo com a natureza da demanda;

5. Configuração de todos os equipamentos com seus respectivos IPs, tanto fixos quanto por meio de DHCP, conforme o plano de infraestrutura;

6. Demonstração do funcionamento do protótipo e/ou serviços por meio de testes no ambiente via simulação e/ou testes adequados;

7. Articulação em equipes de trabalho: demonstrar capacidade de comunicação e colaboração em um processo de planejamento e implantação de projeto de infraestrutura de rede.

Realizamos, de forma colaborativa (exceto Carlos Alberto Morais Junior), o planejamento e a prototipação inicial da infraestrutura de redes, contemplando aspectos como escalabilidade e desempenho, além de definirmos cenários de testes, topologias propostas e estimativas de recursos necessários para cada etapa do projeto.

**Etapa 2**

1. Criação da planilha de recursos de rede;

2. Configuração de todos os equipamentos com seus respectivos IPs, tanto fixos quanto por meio de DHCP;

3. Criação de instâncias para todos os servidores mapeados em nuvem, observando as melhores práticas de utilização de serviços em nuvem;

4. Configuração do servidor de aplicação para publicação de aplicação back-end, seguindo as melhores práticas de DevOps;

5. Instalação e configuração de serviços em ambiente local (AD, DHCP, DNS, IIS e VPN) e nuvem AWS (EC2, VPC, GPO,

6. Comunicação e colaboração em um processo de planejamento e implantação de projeto de infraestrutura de rede;

Realizamos, de forma colaborativa (exceto Carlos Alberto Morais Junior), a implementação dos componentes de infraestrutura em nuvem e complementando a documentação iniciada na Etapa 2.

**Etapa 3**

1. Planejamento de uma infraestrutura de redes para uma organização de telemarketing;

2. Criação e configuração de instâncias para todos os servidores mapeados em nuvem;

3. Criação e configuração do ambiente em nuvem com publicação de um ambiente em nuvem;

4. Virtualização e monitoramento de servidores e clientes Zabbix local e nuvem, monitoramento dos serviços;

Realizamos, de forma colaborativa (exceto Carlos Alberto Morais Junior), planejamos e implementamos uma infraestrutura híbrida (on-premise + nuvem) para o telemarketing, provisionando instâncias na AWS, configurando CI/CD e definindo políticas de segurança. Instalamos também e configuramos o Zabbix local e em nuvem para monitorar servidores e serviços, com dashboards e alertas para garantir alta disponibilidade.

**Etapa 4**

1. Definição de políticas de segurança da informação em conformidade com a natureza da organização de telemarketing;

2. Rastreamento de possíveis vulnerabilidades por meio de ferramentas de exploração de vulnerabilidades e possíveis soluções de atenuação;

3. Pasta da PSI;

Realizamos, de forma colaborativa (exceto Carlos Alberto Morais Junior), uma definição de políticas de segurança da informação adaptada ao ambiente de telemarketing, rastreando vulnerabilidades com ferramentas especializadas e propondo medidas de atenuação e também, elaboramos um folder da PSI para comunicar diretrizes, responsabilidades e procedimentos de segurança a toda a equipe.

# REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14724: Informação e documentação - Trabalhos acadêmicos. Rio de Janeiro, 2011.

AMAZON WEB SERVICES. Documentação Oficial. Disponível em: https://docs.aws.amazon.com/pt\_br/.

MICROSOFT. Documentação do Windows Server. Disponível em: https://docs.microsoft.com/pt-br/windows-server.

ORACLE VM VIRTUALBOX. Documentação Oficial. Disponível em: https://www.virtualbox.org/wiki/Documentation.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS. **Orientações para elabo-**

**ração de projetos de pesquisa, trabalhos acadêmicos, relatórios técnicos e/ou científicos e artigos científicos**: conforme a associação Brasileira de Normas Técnicas (ABNT). 5. ed. Belo Horizonte: PUC Minas, 2023. Disponível em: [<http://www.pucminas.br/biblioteca/>](http://www.pucminas.br/biblioteca/). Acesso em: 29 de jul. 2024.