PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

G1 - Projeto da Infraestrutura de Rede Híbrida da CallNet Solutions

Alunos:

Alisson Anderson de Carvalho

Giulia Fernandes Donato de Mattos

Isadora Aparecida Cardoso Carvalho

Rafael Fernandes Marques

Rômulo Ferraz Chaves.

Curso: Sistemas de Informação

Disciplina: Projeto da Infraestrutura de Rede

Professor(a): Shirley Luana Ramos de Assis

Resumo

O presente trabalho detalha o projeto e a implementação de uma infraestrutura de rede híbrida para a empresa CallNet Solutions. O objetivo foi desenvolver uma arquitetura segura e escalável, integrando recursos locais (on-premise) e em nuvem (Amazon Web Services), para suportar o crescimento do negócio. A metodologia envolveu o planejamento da topologia, a configuração de um ambiente local com Windows Server 2025 para serviços de Active Directory, DNS e DHCP, e a implementação de um ambiente em nuvem para hospedar uma aplicação web em Laravel. Como resultado, obteve-se uma rede funcional, gerenciada por políticas de segurança, monitorada em tempo real com Zabbix e validada através da implantação de uma aplicação CRUD. Conclui-se que a solução híbrida proposta é viável e atende às demandas de desempenho, segurança e flexibilidade da empresa.

Palavras-chave: rede híbrida; windows server; amazon web services; zabbix; segurança da informação.

1. INTRODUÇÃO

1.1. Contextualização

A CallNet Solutions, fundada em 2015, é uma empresa de tecnologia especializada em soluções de automação para atendimento no setor automotivo, cujo principal produto é um sistema de CRMChat. Desde sua criação, a empresa apresentou um crescimento acelerado, expandindo suas operações de Belo Horizonte para filiais em São Paulo e Rio de Janeiro. Esse crescimento, aliado aos desafios impostos pela pandemia de COVID-19, que demandou uma rápida adaptação ao trabalho remoto, evidenciou as limitações da sua infraestrutura de TI, que se mostrava fragmentada e insuficiente para suportar a expansão dos negócios.

1.2. Problema e Justificativa

A ausência de um sistema centralizado, seguro e escalável representava um risco à continuidade dos negócios e um obstáculo para os planos de expansão da CallNet. A implementação de uma infraestrutura de rede moderna e híbrida tornou-se fundamental para garantir a estabilidade, segurança e continuidade das operações, suportando o aumento do número de funcionários, o volume de dados transacionados e a hospedagem de novas soluções.

1.3. Objetivos

O objetivo geral deste trabalho é apresentar o planejamento, a implementação e a validação de uma infraestrutura de rede híbrida, funcional e segura para a CallNet Solutions.

Os objetivos específicos são:

- Projetar uma topologia de rede híbrida, documentando os ativos e o plano de endereçamento.
- Configurar um ambiente de servidor local (on-premise) com Windows Server, implementando os serviços de Active Directory (AD), DNS e DHCP.
- Configurar um ambiente em nuvem na AWS para hospedar uma aplicação web externa.
- Desenvolver e aplicar políticas de segurança, incluindo GPOs e uma Política de Segurança da Informação (PSI).
- Implantar um sistema de monitoramento centralizado para os ativos locais e em nuvem.

2. METODOLOGIA

Para atender aos objetivos propostos, este projeto foi conduzido como uma pesquisa aplicada, utilizando como procedimento técnico o estudo de caso para o planejamento e a implementação da solução de infraestrutura. As etapas de execução seguiram um fluxo lógico, garantindo uma implementação organizada e documentada.

As etapas da pesquisa foram:

1. **Planejamento e Arquitetura:** Definição dos requisitos, desenho da topologia de rede híbrida (matriz e filiais) e criação da documentação de ativos, incluindo o plano de endereçamento IP.
2. **Configuração do Ambiente Simulado:** A implementação prática foi realizada em um ambiente de virtualização utilizando o Oracle VM VirtualBox para simular a rede local, com um servidor Windows Server 2025 e um cliente Windows 11.
3. **Implementação da Infraestrutura em Nuvem:** Provisionamento da infraestrutura na Amazon Web Services (AWS), incluindo a criação de uma Virtual Private Cloud (VPC) e uma instância EC2 para hospedar os serviços web.
4. **Implantação de Serviços e Aplicações:** No servidor local, foram instalados e configurados os serviços de AD, DNS, DHCP e um servidor web IIS para a intranet.

Na nuvem, o IIS foi configurado para hospedar uma aplicação CRUD desenvolvida em Laravel.

5. **Desenvolvimento da Governança de Segurança:** Elaboração de uma Política de Segurança da Informação (PSI) e de uma cartilha de boas práticas. Configuração de Políticas de Grupo (GPOs) no Active Directory para padronização e proteção dos endpoints.
6. **Implementação do Monitoramento:** Implantação da ferramenta Zabbix em uma máquina virtual dedicada para o monitoramento centralizado de ambos os ambientes (local e nuvem).
7. **Testes e Validação:** Cada serviço implementado foi validado por meio de testes funcionais, como testes de conectividade (ping, nslookup), ingresso de máquinas no domínio, acesso às aplicações web e confirmação da coleta de métricas no Zabbix.

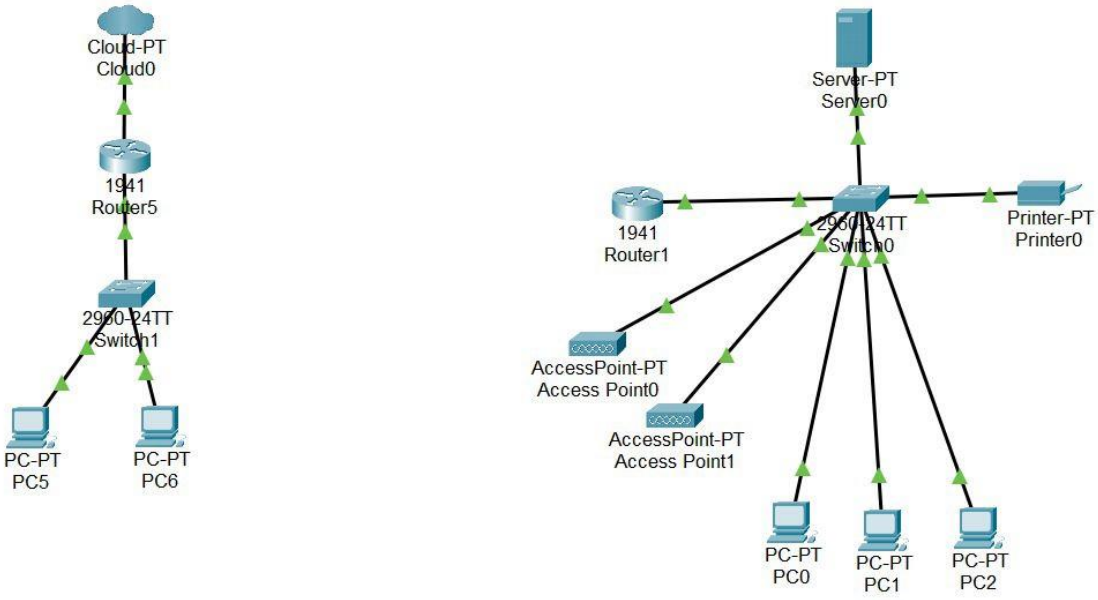
3. RESULTADOS E DISCUSSÃO

Esta seção apresenta os resultados concretos obtidos em cada etapa da implementação da infraestrutura de rede híbrida.

3.1. Arquitetura e Planejamento da Rede

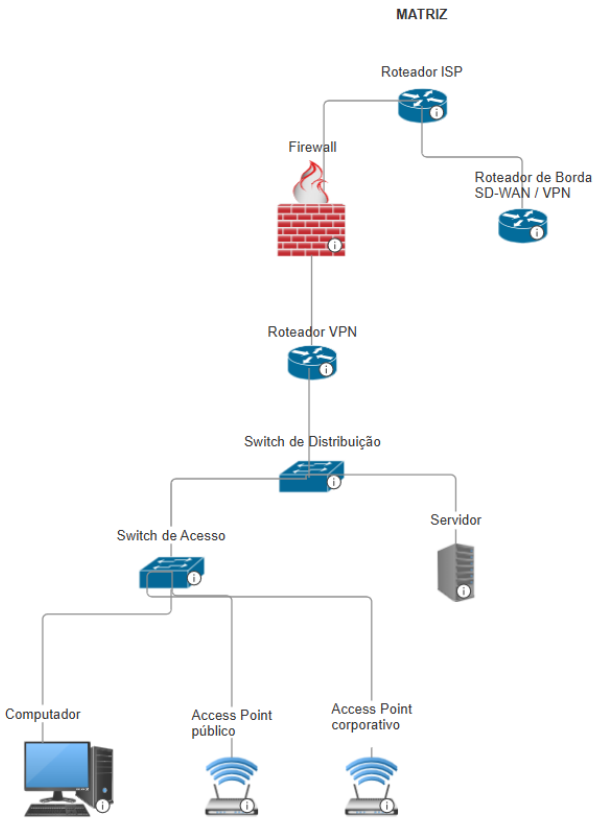
O planejamento resultou em uma arquitetura híbrida que integra recursos locais e em nuvem. A topologia foi desenhada no Cisco Packet Tracer (Figura 1) para visualizar a interconexão entre os dispositivos da matriz (Figura 2), das filiais (Figura 3) e a conexão com a nuvem. A documentação de todos os equipamentos, serviços e o plano de endereçamento IP foi consolidada em uma tabela de ativos (Figura 4), servindo como guia para a implementação.

Figura 1 – Topologia de Rede no Cisco Packet Tracer



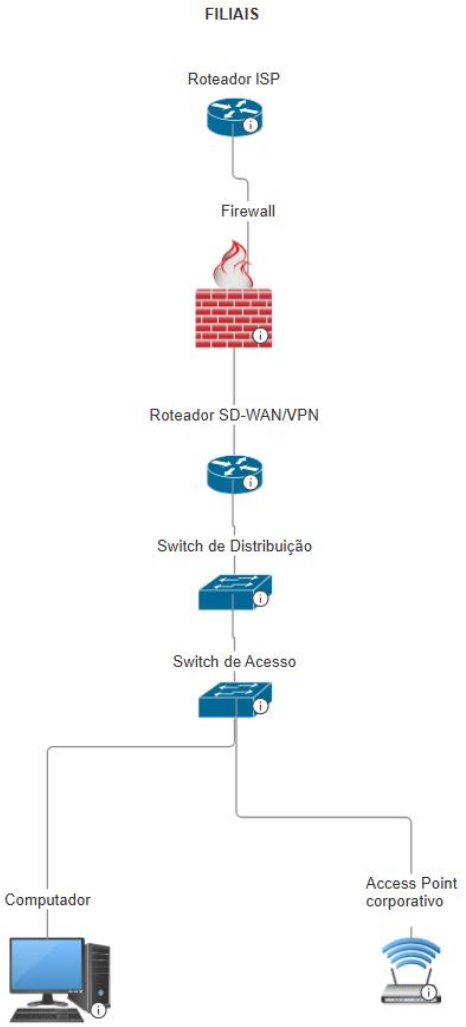
Fonte: Elaborada pelo autor (2025)

Figura 2 – Topologia de Rede Matriz



Fonte: Elaborada pelo autor (2025)

Figura 3 – Topologia de Rede Filiais



Fonte: Elaborada pelo autor (2025)

Figura 4 - Tabela de equipamentos de rede

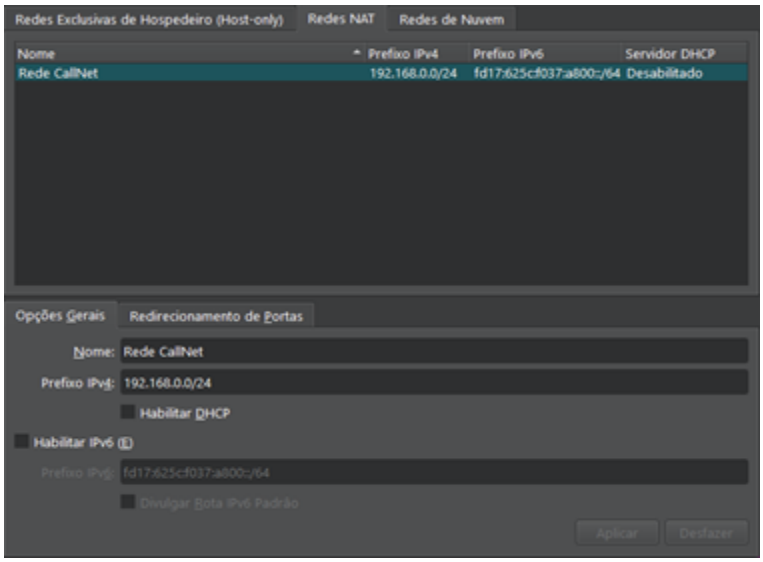
Tipo	IP Matriz	Função	Localização	Virtualização	Observações
Firewall Dedicado	-	Proteção da rede e filtragem de tráfego	Matriz	Físico	Protege a rede da matriz
Roteador SD-WAN/VPN	192.168.0.1	Gateway principal e comunicação segura ent	Matriz e Filiais	Físico	Suporte a VPN site-to-site e SD-WAN
Switch de Distribuição	192.168.0.2	Agregação de links dos switches de acesso	Matriz	Físico	Gerencia VLANs e conexões principais
Switch de Acesso	192.168.0.3	Conexão de dispositivos de usuários	Matriz	Físico	Switch gerenciável
Access Point (Corporativo)	192.168.0.4	Wi-Fi exclusivo para área administrativa	Matriz	Físico	Rede Wi-Fi interna protegida
Access Point (Visitantes)	192.168.0.5	Wi-Fi para visitantes e recepção	Matriz	Físico	Rede Wi-Fi separada da corporativa
Servidor Local (Infraestrutura)	192.168.0.10	AD DS, DNS, DHCP, Intranet (IIS), VPN, VoIP	Matriz	Físico	Servidor principal da matriz
Servidor em Nuvem	18.210.255.124	Aplicações Web, CRM, Monitoramento (Zabb	Nuvem (AWS)	AWS	Servidor EC2 na AWS
Estações de Trabalho (Administração)	Faixa DHCP	Computadores da equipe administrativa	Matriz	Físico	DHCP automático
Estações de Trabalho (Suporte Técnico)	Faixa DHCP	Computadores da equipe de suporte	Matriz	Físico	DHCP automático
Estações de Trabalho (Filiais)	Faixa DHCP	Computadores de colaboradores nas filiais	Filiais	VPN	Conectados via VPN
Estações de Trabalho (Home Office)	Faixa DHCP	Computadores de colaboradores em home o	Home Office	VPN	Conectados via VPN
Impressora de Rede	192.168.0.6	Impressão de documentos administrativos	Matriz	Físico	Impressora de rede com IP fixo
Dispositivo de Segurança (Câmera IP)	192.168.0.7	Monitoramento interno de segurança	Matriz	Físico	Câmera IP conectada à rede

Fonte: Elaborada pelo autor (2025)

3.2. Implementação e Configuração do Ambiente Local (On-Premise)

O ambiente local foi simulado no VirtualBox, com a criação de uma rede NAT interna (Rede CallNet) na faixa 192.168.0.0/24 (Figura 5).

Figura 5 – Rede NAT interna, denominada ‘Rede CallNet’, criada para simular o roteador principal

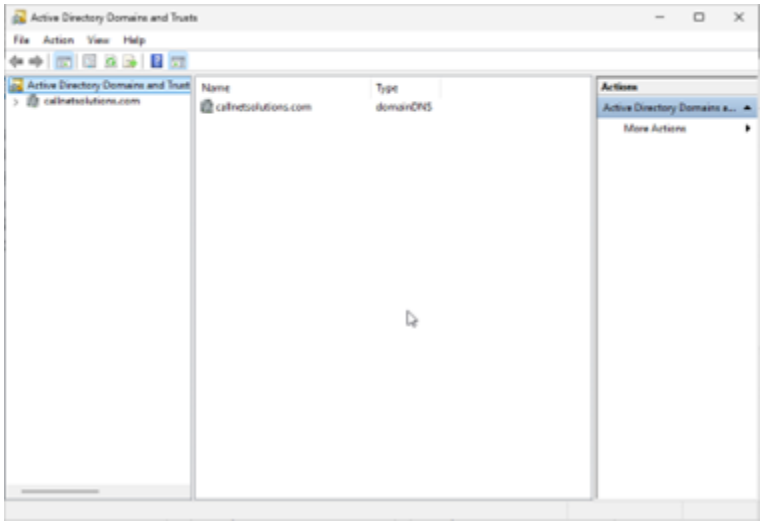


Fonte: Elaborada pelo autor (2025)

O servidor SRV-CALLNET (Windows Server 2025) foi configurado com IP fixo (192.168.0.10) e os serviços essenciais foram implantados:

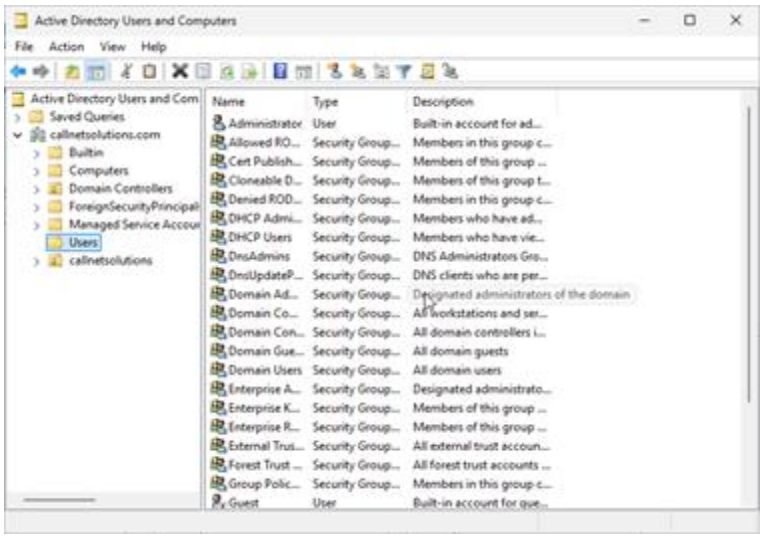
- **Active Directory:** O domínio callnetsolutions.com foi criado (Figura 6), permitindo o gerenciamento centralizado de usuários e computadores (Figura 7).
- **DNS:** O servidor foi configurado para atuar como servidor DNS primário para a zona callnetsolutions.com (Figuras 8 e 9).
- **DHCP:** O serviço foi configurado para distribuir IPs na faixa de 192.168.0.20 a 192.168.0.100 (Figura 10

Figura 6 – Domínio criado no Active Directory



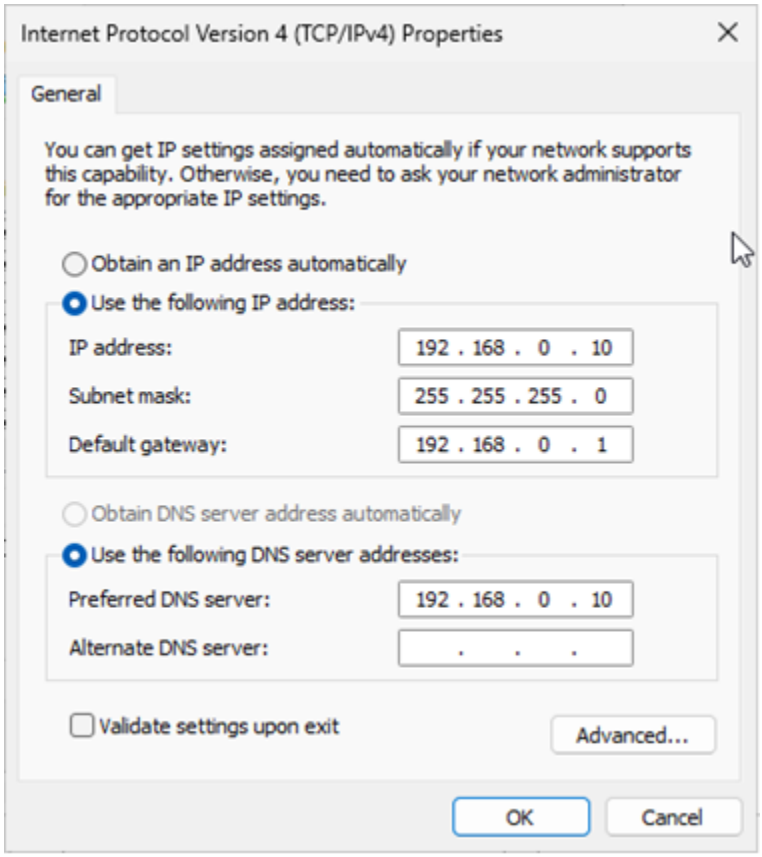
Fonte: Elaborada pelo autor (2025)

Figura 7 – Usuários e Computadores do Active Directory



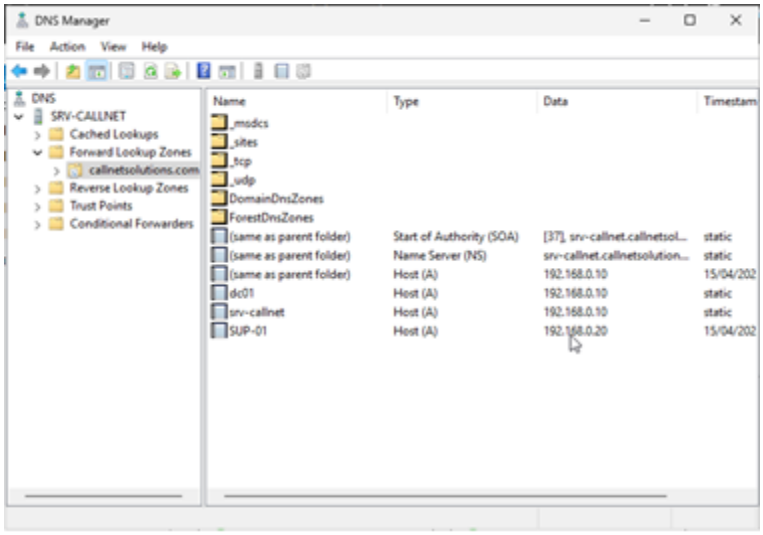
Fonte: Elaborada pelo autor (2025)

Figura 8 – Configuração para atuar como servidor DNS



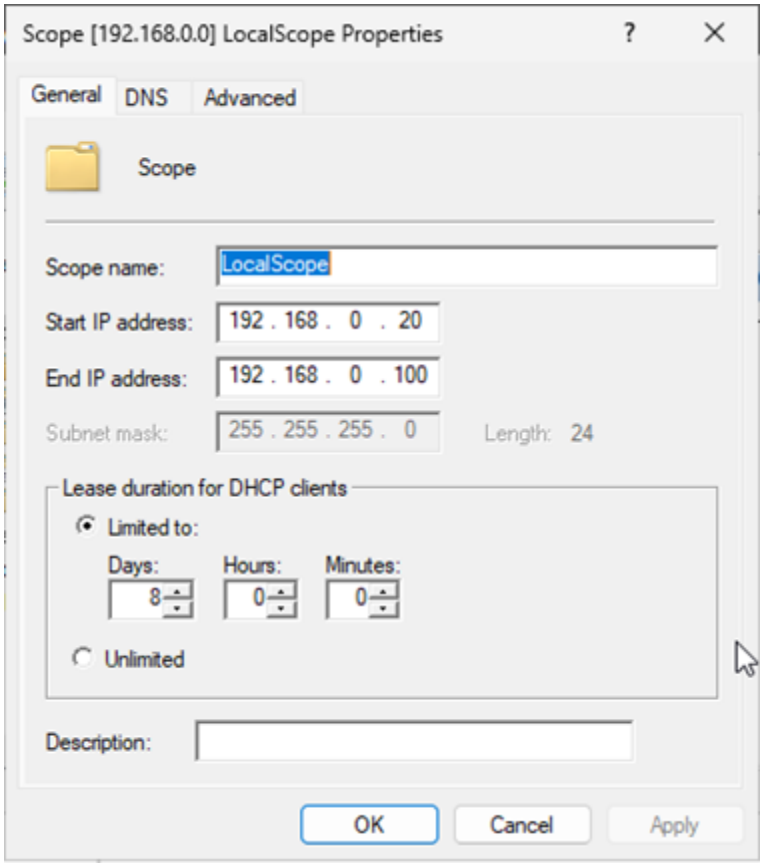
Fonte: Elaborada pelo autor (2025)

Figura 9 – Zona DNS primária ‘callnetsolutions.com’



Fonte: Elaborada pelo autor (2025)

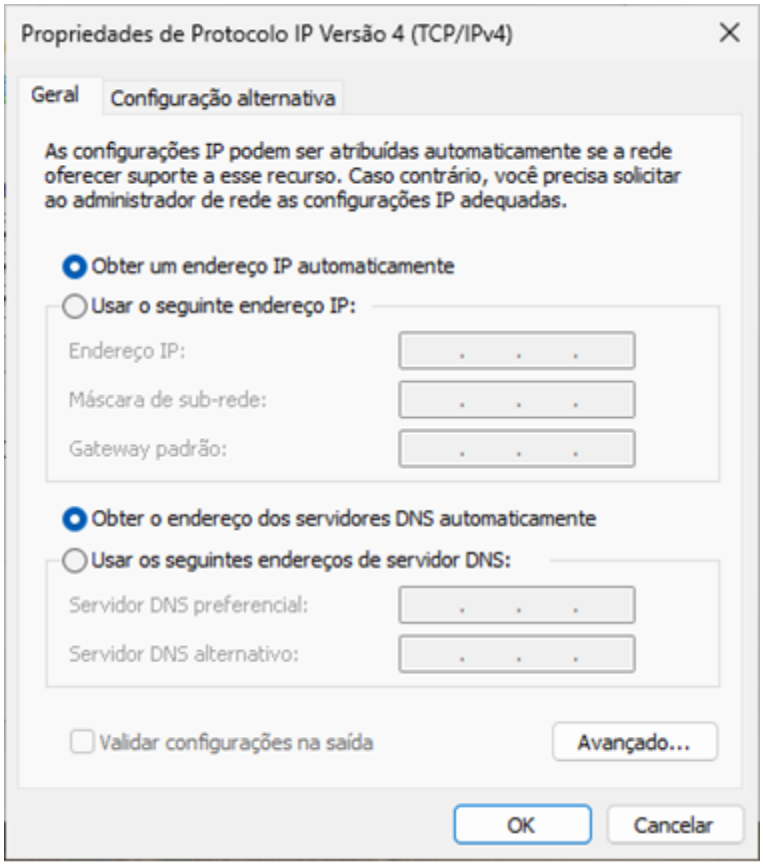
Figura 10 – DHCP com faixa de distribuição (range) **192.168.0.20** a **192.168.0.100**



Fonte: Elaborada pelo autor (2025)

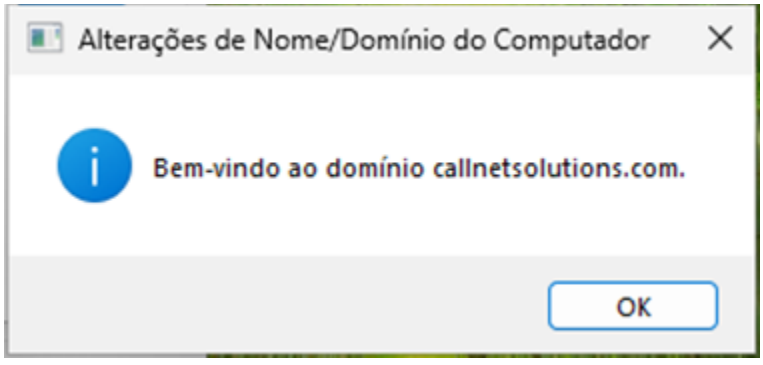
A validação foi realizada com uma máquina cliente (SUP-01, Windows 11), que obteve IP via DHCP (Figura 11) e ingressou com sucesso no domínio (Figura 12), com testes de conectividade e resolução de nomes confirmando o funcionamento (Figuras 13 e 14).

Figura 11 – Máquina obtendo endereço IP dinamicamente



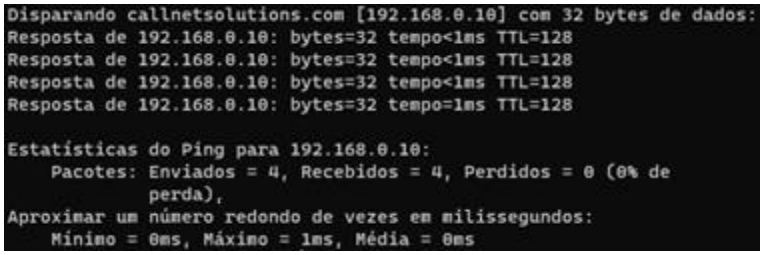
Fonte: Elaborada pelo autor (2025)

Figura 12 – Mensagem de boas-vindas ao domínio



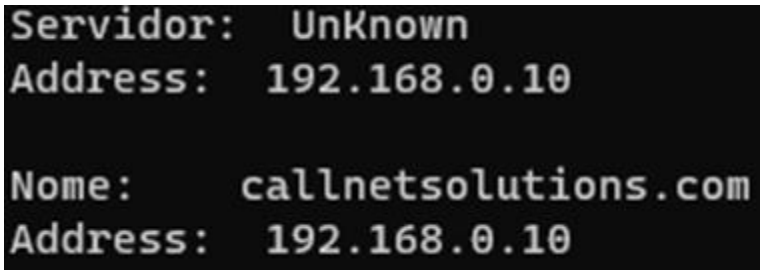
Fonte: Elaborada pelo autor (2025)

Figura 13 – Teste com comando ‘ping callnetsolutions.com’ (Obteve resposta do servidor corretamente)



Fonte: Elaborada pelo autor (2025)

Figura 14 – Teste com comando ‘nslookup callnetsolutions.com’ (com resolução do domínio com resposta adequada)

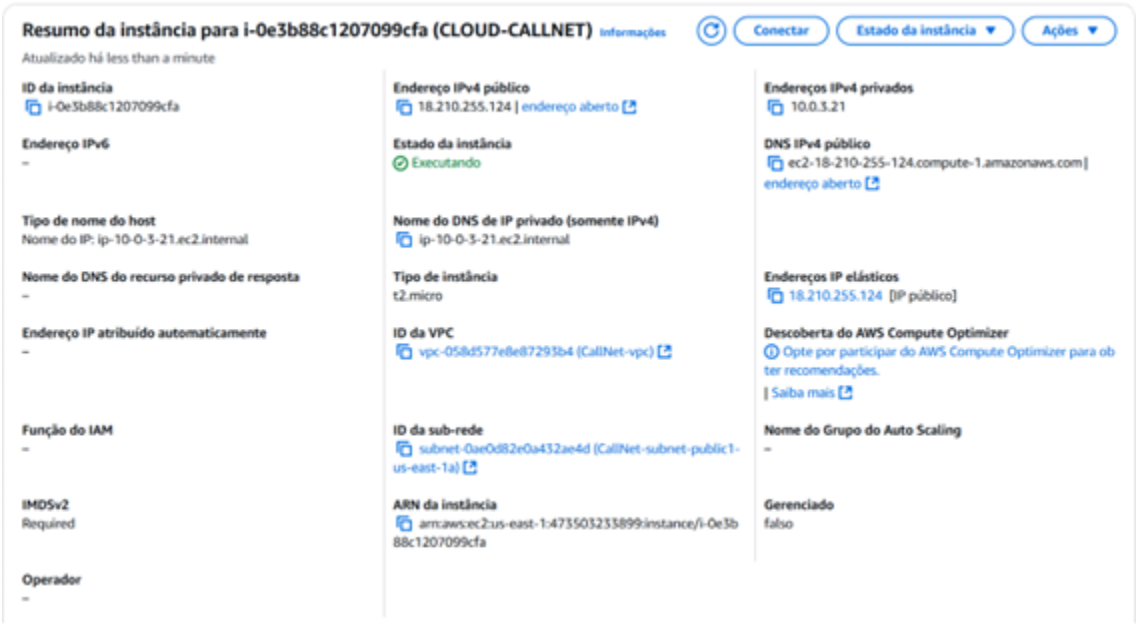


Fonte: Elaborada pelo autor (2025)

3.3. Implementação e Configuração do Ambiente em Nuvem (AWS)

A infraestrutura em nuvem foi implementada na AWS. Uma instância EC2 (t2.micro) com Windows Server 2022 foi provisionada, recebendo o IP público elástico 18.210.255.124 (Figura 15). O acesso foi protegido via par de chaves .pem (Figura 16).

Figura 15 – Resumo da instância ‘CLOUD-CALLNET’



Fonte: Elaborada pelo autor (2025)

Figura 16 – Chave criptografada ‘CallNet.pem’

Fonte: Elaborada pelo autor (2025)

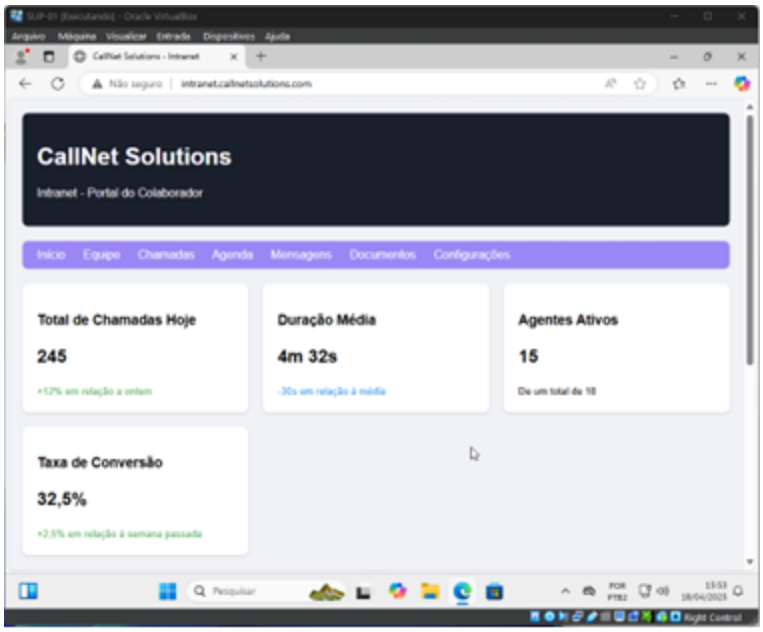
3.4. Implantação de Serviços e Aplicações

Serviços Locais:

- **Servidor Web IIS para Intranet:** Foi configurado um site de intranet no servidor SRV-CALLNET, acessível internamente pelo endereço intranet.callnetsolutions.com (Figura 17).

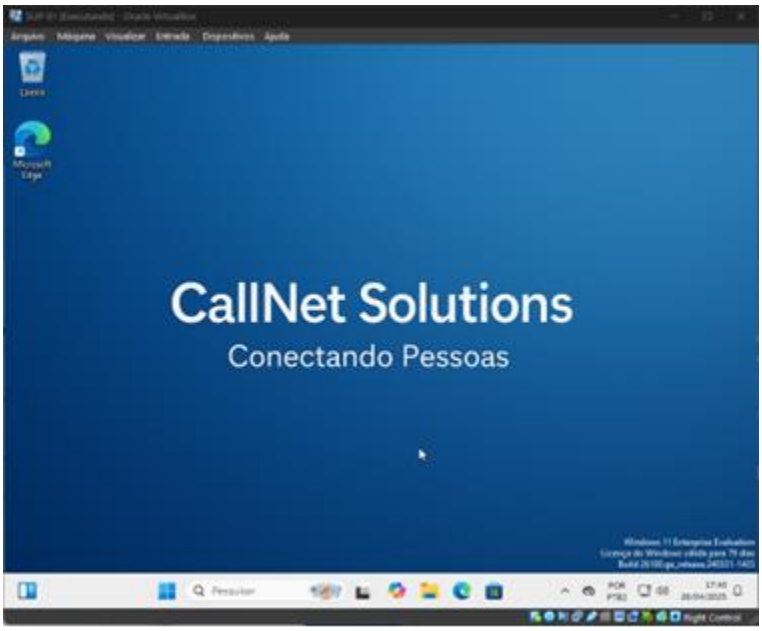
- **Políticas de Grupo (GPOs):** Foram implementadas duas GPOs centrais: uma para aplicar um papel de parede corporativo em todas as estações (Figura 18) e outra para proibir o acesso ao Painel de Controle (Figura 19), reforçando a segurança e a padronização do ambiente.

Figura 17 – Acesso ao ‘intranet.callnetsolutions.com’ na máquina cliente (SUP-01)



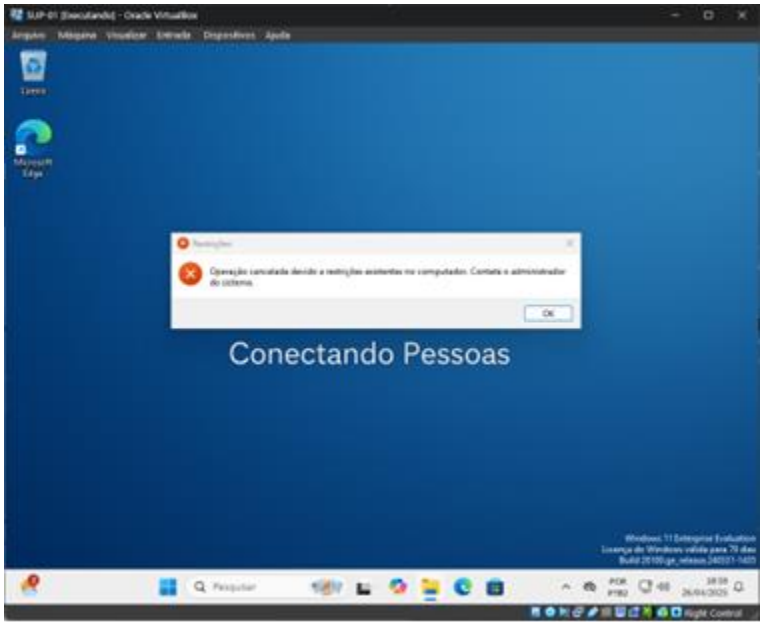
Fonte: Elaborada pelo autor (2025)

Figura 18 – Papel de Parede via GPO



Fonte: Elaborada pelo autor (2025)

Figura 19 – Print demonstrando bloqueio ao acessar painel de controle

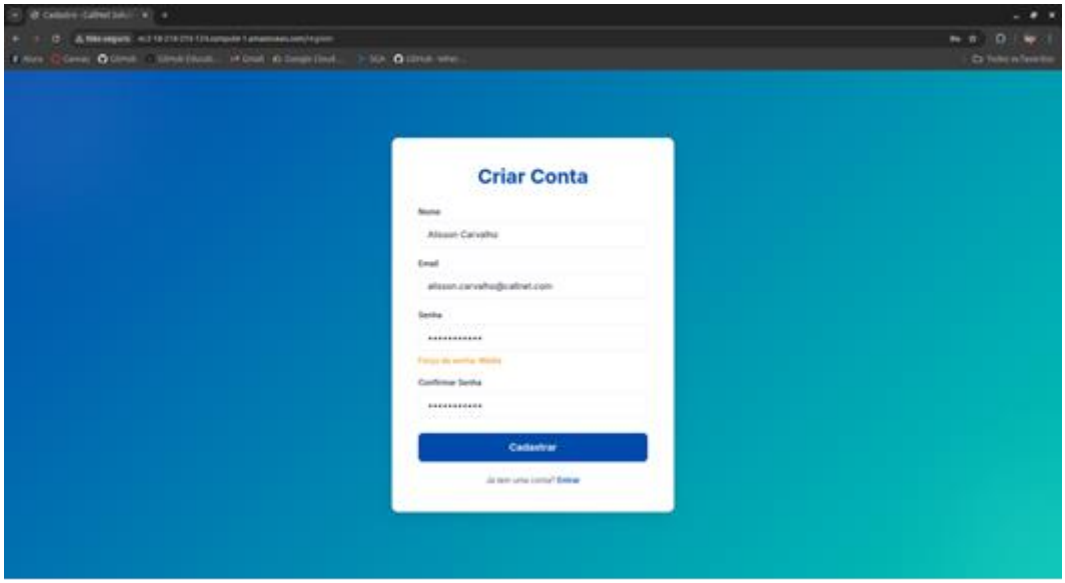


Fonte: Elaborada pelo autor (2025)

Serviços em Nuvem:

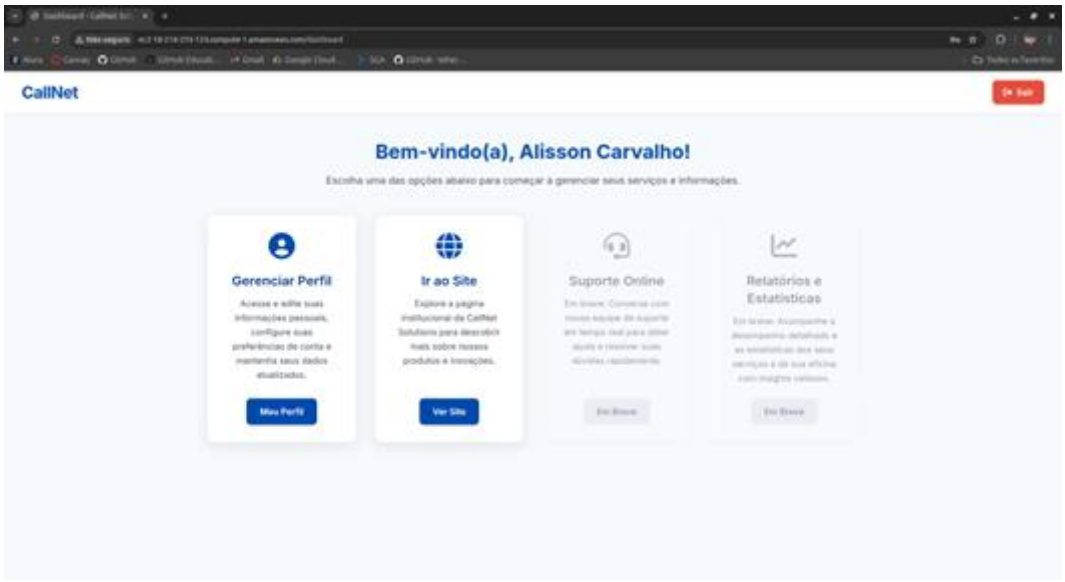
- **Aplicação CRUD com Laravel:** Para validar a infraestrutura, foi implantada uma aplicação de gerenciamento de usuários (CRUD) em Laravel na instância EC2, utilizando o IIS como servidor web. O sistema permite o cadastro (Figura 20), a edição e a exclusão de usuários (Figura 21), com os dados sendo persistidos em um banco de dados, demonstrando a capacidade do ambiente de hospedar aplicações complexas.

Figura 20 – Tela de Cadastro do usuário



Fonte: Elaborada pelos autores (2025)

Figura 21 – Dashboard após cadastro bem-sucedido com opções para edição e exclusão



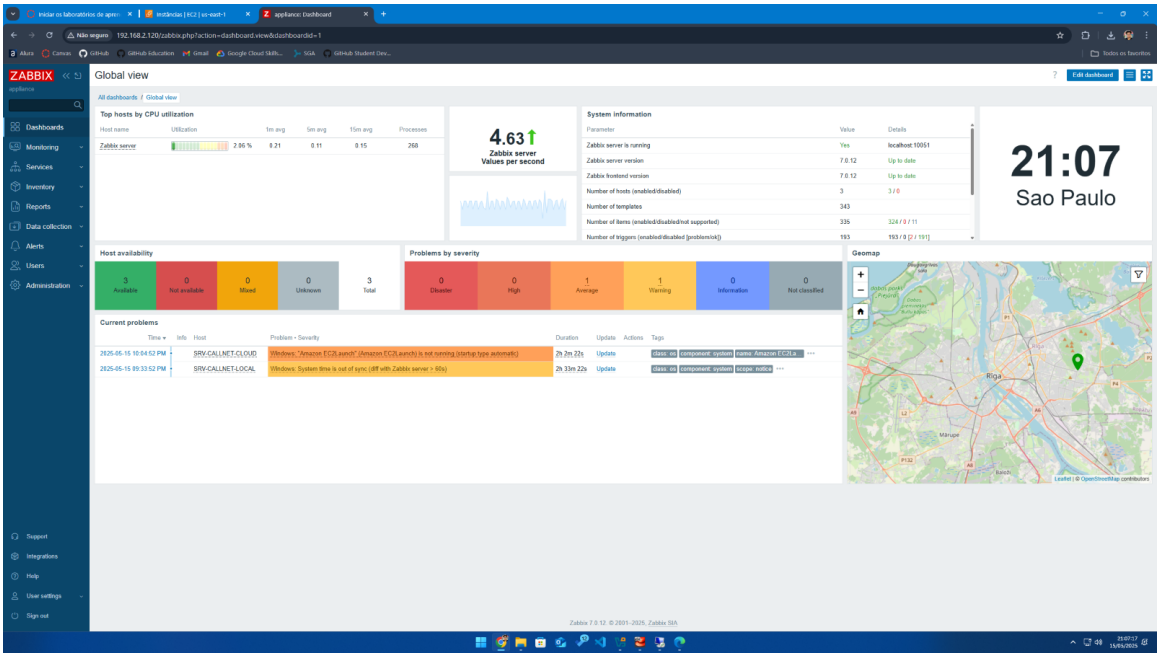
Fonte: Elaborada pelos autores (2025)

3.5. Implementação do Monitoramento e Governança

Monitoramento com Zabbix: Foi implementado um sistema de monitoramento com Zabbix para garantir a visibilidade da saúde dos ativos. Agentes foram instalados nos servidores local (SRV-CALLNET) e em nuvem (CLOUD-CALLNET), enviando métricas em tempo real. O

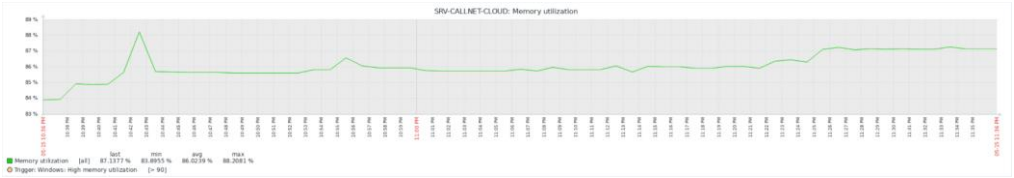
dashboard (Figura 22) permite o acompanhamento de indicadores como uso de CPU, memória (Figura 23) e disco (Figura 24), possibilitando uma administração proativa.

Figura 22 – Dashboard geral Zabbix



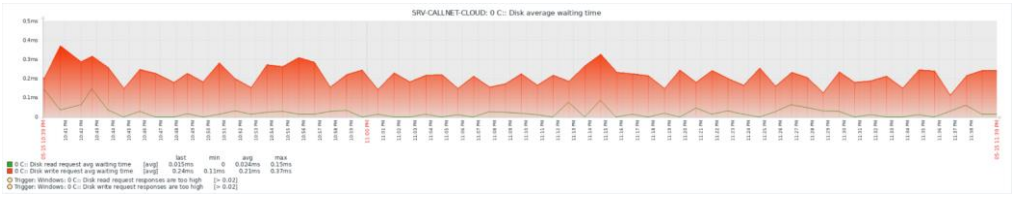
Fonte: Elaborada pelo autor (2025)

Figura 23 – Monitoramento RAM



Fonte: Elaborada pelo autor (2025)

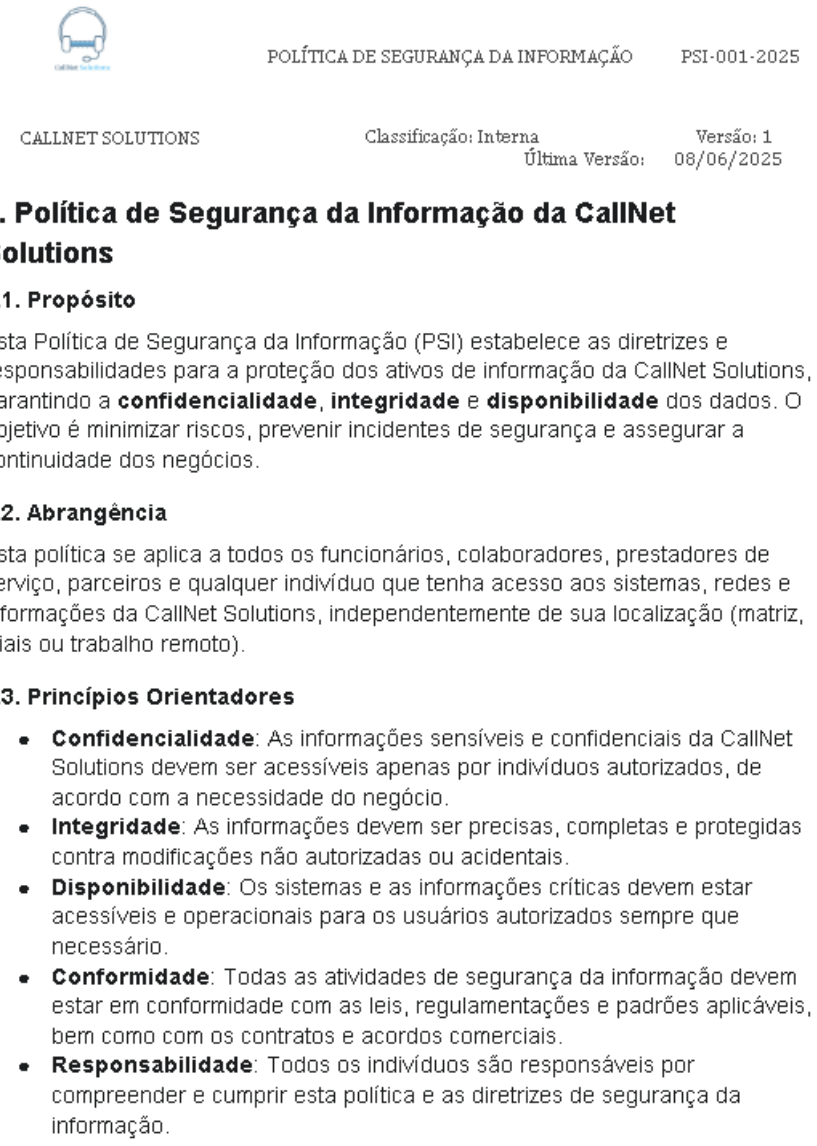
Figura 24 – Monitoramento Disco



Fonte: Elaborada pelo autor (2025)

Governança de Segurança: Para estabelecer uma base sólida de segurança, foi desenvolvida uma **Política de Segurança da Informação (PSI)** (Figura 25) e uma **Cartilha de Boas Práticas** (Figura 26) para conscientização dos colaboradores.

Figura 25 - Políticas de Segurança da CallNet Solutions



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PSI-001-2025

CALLNET SOLUTIONS Classificação: Interna Versão: 1
Última Versão: 08/06/2025

1. Política de Segurança da Informação da CallNet Solutions

1.1. Propósito

Esta Política de Segurança da Informação (PSI) estabelece as diretrizes e responsabilidades para a proteção dos ativos de informação da CallNet Solutions, garantindo a **confidencialidade**, **integridade** e **disponibilidade** dos dados. O objetivo é minimizar riscos, prevenir incidentes de segurança e assegurar a continuidade dos negócios.

1.2. Abrangência

Esta política se aplica a todos os funcionários, colaboradores, prestadores de serviço, parceiros e qualquer indivíduo que tenha acesso aos sistemas, redes e informações da CallNet Solutions, independentemente de sua localização (matriz, filiais ou trabalho remoto).

1.3. Princípios Orientadores

- **Confidencialidade**: As informações sensíveis e confidenciais da CallNet Solutions devem ser acessíveis apenas por indivíduos autorizados, de acordo com a necessidade do negócio.
- **Integridade**: As informações devem ser precisas, completas e protegidas contra modificações não autorizadas ou acidentais.
- **Disponibilidade**: Os sistemas e as informações críticas devem estar acessíveis e operacionais para os usuários autorizados sempre que necessário.
- **Conformidade**: Todas as atividades de segurança da informação devem estar em conformidade com as leis, regulamentações e padrões aplicáveis, bem como com os contratos e acordos comerciais.
- **Responsabilidade**: Todos os indivíduos são responsáveis por compreender e cumprir esta política e as diretrizes de segurança da informação.

Fonte: Elaborada pelos autores (2025)

Figura 50 e 51 – Cartilha de Segurança da CallNet Solutions

CallNet Solutions

Objetivo

Esta Cartilha visa fornecer um guia rápido e essencial sobre as boas práticas de segurança da informação na CallNet Solutions. Nosso objetivo é capacitar cada colaborador a proteger nossos dados e sistemas, garantindo a confidencialidade, integridade e disponibilidade das informações, e contribuindo para um ambiente de trabalho seguro.

Penalidades

Leve: Advertência e treinamento.

Média: Suspensão de acessos.

Grave: Demissão por justa causa e/ou ações judiciais.

Princípios básicos

A segurança da informação na CallNet Solutions é fundamentada nos seguintes princípios, que todos devemos seguir:

- **Confidencialidade:** Assegurar que as informações sensíveis sejam acessíveis apenas por pessoas autorizadas.
- **Integridade:** Garantir que os dados sejam precisos, completos e protegidos contra modificações não autorizadas.
- **Disponibilidade:** Assegurar que os sistemas e informações críticas estejam acessíveis aos usuários autorizados sempre que necessário.
- **Conformidade:** Cumprir todas as leis, regulamentações e políticas internas.
- Responsabilidade: Todos são responsáveis por compreender e seguir as diretrizes de segurança.

Regras Gerais e Boas práticas

- Use senhas fortes, únicas e mude a cada 90 dias.
- Nunca compartilhe suas senhas; use gerenciador se precisar.
- Sempre acesse a rede via VPN, especialmente em redes públicas.
- Bloqueie o computador ao se afastar.
- Instale só softwares autorizados e cheque dispositivos externos com antivírus.
- Cuidado com e-mails suspeitos: não clique em links ou abra anexos duvidosos; reporte para TI.
- Mantenha antivírus ativo e atualizado, faça varreduras regulares.
- Proteja informações confidenciais, descarte documentos com triturador.
- Avise TI se notar algo estranho.

Fonte: Elaborada pelos autores (2025)

Incidentes de Segurança

- **Perda ou roubo de equipamentos:**
  Comunique imediatamente a TI e registre BO (se necessário).
- **Vazamento de dados:**
  Notifique a Gerência de TI e o Comitê de Segurança.
- **Vazamento de dados:**
  Desconecte o dispositivo da rede e avise a TI.
- **Testes sem autorização:**
  Proibido realizar testes de vulnerabilidade sem autorização.

Responsabilidades

- **Colaboradores:**
  - Cumprir a PSI e relatar violações.
  - Assinar o Termo de Ciência e Responsabilidade.
- **Equipe de TI:**
  - Monitorar sistemas e bloquear acessos suspeitos.
  - Garantir backups e atualizações de segurança.
- **Prestador de Serviço:**
  - Seguir as mesmas regras dos colaboradores.
  - Devolver os equipamentos ao término do contrato.

Contatos Importantes

Suporte TI:
- suporteti@callnet.com.br
- (31) 0000-0000

Comitê de Segurança:
comite.seguranca@callnet.com.br

Fonte: Elaborada pelos autores (2025)

3.6. Análise de Vulnerabilidades e Mitigações

Parte fundamental do projeto foi a análise proativa de riscos de segurança específicos ao ambiente construído, com a definição de suas respectivas soluções de mitigação.

- **Vulnerabilidade: Ataques de Força Bruta ao Controlador de Domínio SRV-CALLNET**
  - **Descrição:** Tentativas automatizadas de adivinhar senhas no servidor SRV-CALLNET, que hospeda o Active Directory. Um sucesso comprometeria toda a rede interna.
  - **Atenuação:** Foi configurada, via GPO, uma política de bloqueio de conta após 5 tentativas falhas de login. Adicionalmente, foram configurados alertas no Zabbix para notificar a equipe de TI sobre múltiplas falhas de login em um curto período.
- **Vulnerabilidade: Engenharia Social Direcionada (Spear Phishing e Vishing)**
  - **Descrição:** Risco de um atacante usar informações públicas (OSINT) para se passar por um gerente e solicitar credenciais do sistema CRUD Laravel. Sendo uma empresa de telemarketing, o risco de Vishing (phishing por voz) é particularmente elevado.
  - **Atenuação:** A cartilha de boas práticas foca em treinar os colaboradores para identificar e-mails e ligações fraudulentas. A PSI estabelece a MFA como obrigatória para o acesso externo à aplicação, neutralizando o simples roubo de senhas.
- **Vulnerabilidade: Acesso Não Autorizado à Instância CLOUD-CALLNET via RDP**
  - **Descrição:** A porta de acesso remoto (RDP) da instância EC2 poderia ser explorada se deixada aberta publicamente.
  - **Atenuação:** O Security Group da AWS foi configurado para permitir o acesso à porta 3389 (RDP) apenas a partir de uma faixa de IPs pré-definida, correspondente à rede da matriz da CallNet. O acesso também exige a posse da chave criptográfica .pem do projeto.
- **Vulnerabilidade: Exposição de Informações em Fontes Abertas (OSINT)**
  - **Descrição:** Um anúncio de vaga para "Administrador de Sistemas" poderia, inadvertidamente, listar "experiência com Zabbix e Laravel", informando a um atacante as tecnologias exatas em uso.
  - **Atenuação:** A política de segurança orienta o RH a higienizar anúncios de vagas, usando termos genéricos. A cartilha orienta os funcionários a não divulgarem detalhes técnicos da infraestrutura em redes sociais.

4. CONCLUSÃO

O projeto demonstrou com sucesso a viabilidade técnica e estratégica da implementação de uma infraestrutura de rede híbrida para a CallNet Solutions. A integração de um ambiente local controlado com a flexibilidade da nuvem AWS atendeu aos requisitos de segurança, escalabilidade e gerenciamento centralizado, resolvendo o problema inicial da empresa.

Os resultados, desde a configuração funcional dos serviços de rede essenciais até a implantação de uma aplicação real e um sistema de monitoramento abrangente, confirmam que a arquitetura proposta fornece uma base tecnológica robusta para a continuidade e expansão sustentável dos negócios da CallNet.

Como trabalhos futuros, recomenda-se a configuração de uma VPN Site-to-Site para interconectar as filiais de forma segura, a implementação de uma rotina de backup e um plano de recuperação de desastres (Disaster Recovery), e a execução periódica de análises de vulnerabilidades.

5. REFERÊNCIAS

AMAZON WEB SERVICES. DOCUMENTAÇÃO OFICIAL. Disponível em: <https://docs.aws.amazon.com/?nc2=h_ql_doc_do>. Acesso em: 20/03/2025

MICROSOFT. DOCUMENTAÇÃO DO WINDOWS SERVER. Disponível em: <https://learn.microsoft.com/pt-br/windows-server/>. Acesso em: 25/03/2025

POLÍTICAS DE SEGURANÇA CALLNET SOLUTIONS. Disponível em: <https://docs.google.com/document/d/14pARBXnvax61wlGUP2UliXlumMMsbhFL/edit?usp=sharing&ouid=115405569623012032596&rtpof=true&sd=true>. Acesso em: 20/06/2025