



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Instituto de Ciências Exatas e de Informática

Projeto de Infraestrutura de Rede de uma Empresa de Telemarketing

Projeto dos alunos da faculdade de Sistemas de Informação da PUC Minas

Eduardo Henrique Moraes Costa¹
Eric Henrique Marques dos Santos²
Jeziel Suzana Pires da Silva³
Júlio dos Reis Firmino⁴
Sophia Thais Gibim Coelho⁵
Victor Hugo Carvalho de Almeida⁶
Alexandre Teixeira⁷

Resumo

Este projeto irá abordar o desenvolvimento de uma infraestrutura de rede para uma empresa de telemarketing, organizada em cinco fases distintas. Primeiramente, serão elaborados documentos fundamentais, incluindo a definição do tema, planejamento inicial, planilha de recursos de rede e protótipo da rede utilizando o Cisco Packet Tracer. Em seguida, será realizada a preparação do ambiente em nuvem e a virtualização local, com a configuração necessária para servidores tanto em nuvem quanto on-premise, utilizando ferramentas como Amazon EC2 e Oracle VirtualBox. Posteriormente, a gerência e o monitoramento dos ambientes de rede ocorrerão por meio do Zabbix, que acompanhará o desempenho dos serviços. Em uma etapa avançada, serão implementados mecanismos de segurança da informação, incluindo a análise de vulnerabilidades e a criação de uma Política de Segurança da Informação (PSI). Por fim, haverá a apresentação e a elaboração de um relatório técnico, consolidando todos os resultados obtidos ao longo do desenvolvimento.

Palavras-chave: Infraestrutura de rede. segurança da informação.

*Projeto apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais como pré-requisito para obtenção do título de Bacharel em Sistemas de Informação.

¹Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1187487@sga.pucminas.br.

²Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1405542@sga.pucminas.br.

³Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1365762@sga.pucminas.br.

⁴Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1425050@sga.pucminas.br.

⁵Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1249628@sga.pucminas.br.

⁶Aluno do Programa de Graduação em Sistemas de Informação, Brasil – 1387849@sga.pucminas.br.

⁷Professor do Programa de Graduação em Sistemas de Informação, Brasil – 107275@sga.pucminas.br.

1 INTRODUÇÃO

A empresa de telemarketing em análise tem como missão proporcionar serviços de excelência em atendimento ao cliente e vendas, integrando a eficiência do trabalho presencial em suas unidades físicas à flexibilidade oferecida pelo trabalho remoto. Com uma matriz situada em Minas Gerais e filiais em São Paulo, Rio de Janeiro e Curitiba, a empresa enfrenta o desafio de planejar e implementar uma rede de comunicação que assegure a conectividade eficiente e segura entre todas as suas unidades, garantindo a continuidade e a qualidade dos serviços prestados.

Objetivos Principais

Assegurar Conectividade e Comunicação Integradas: Desenvolver e implementar uma rede que conecte a matriz, as filiais e os colaboradores em home office, garantindo comunicação contínua e eficiente, bem como o compartilhamento de informações em tempo real. Garantir Segurança de Dados e Conformidade: Proteger os dados sensíveis da empresa, incluindo informações confidenciais de clientes e funcionários, por meio de políticas de segurança robustas e alinhadas às regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD). Promover Escalabilidade e Flexibilidade: Projetar uma rede escalável que suporte o crescimento da empresa, seja pela adição de novas filiais ou pelo aumento do número de colaboradores remotos, sem comprometer o desempenho e a segurança da infraestrutura.

2 DESENVOLVIMENTO

Esta seção tem como objetivo detalhar o desenvolvimento da infraestrutura tecnológica de uma empresa que adota uma abordagem híbrida, combinando soluções de nuvem e on-premise para otimizar custos e garantir a alta disponibilidade de serviços críticos. A organização contará com uma matriz e três filiais, distribuindo de forma eficiente suas aplicações, como CRM, VoIP, HCM e ERP, em ambientes de nuvem e locais. Além disso, será discutida a estruturação dos ativos de TI, bem como a distribuição de colaboradores e funções essenciais, visando assegurar a continuidade das operações e a integração entre os setores.

A adoção de uma infraestrutura híbrida permitirá à empresa não apenas garantir alta disponibilidade e resiliência para serviços essenciais hospedados na nuvem, mas também aproveitar as vantagens de segurança e conformidade ao manter aplicações de menor criticidade on-premise. Além disso, essa abordagem híbrida facilita a escalabilidade, permitindo que a empresa responda rapidamente a mudanças na demanda sem comprometer a performance. A integração de soluções de monitoramento e gerenciamento centralizado também será crucial para assegurar a eficiência operacional e a continuidade dos negócios, proporcionando uma visão unificada dos recursos tanto na nuvem quanto on-premise.

Aplicações

CRM (Customer Relationship Management): Essencial para gerenciar interações com

clientes, organizar o fluxo de chamadas e armazenar históricos de comunicação, o CRM será hospedado na nuvem, proporcionando acesso em tempo real, independentemente da localização dos operadores. Plataformas de VoIP: essenciais para a realização de chamadas via internet, essas plataformas se integrarão ao CRM e a outras ferramentas de comunicação. Como são críticas para as operações diárias, serão hospedadas na nuvem para garantir alta disponibilidade e flexibilidade. Sistema de Gestão de Pessoas (HCM): Ferramenta para gerenciar o ciclo de vida dos funcionários, desde o recrutamento até a rescisão. O HCM estará na nuvem, facilitando o acesso seguro a partir de qualquer unidade ou local remoto. ERP (Enterprise Resource Planning): Sistema centralizado que integra processos administrativos, financeiros e logísticos da empresa. O ERP será parcialmente hospedado na nuvem para garantir disponibilidade e suporte remoto, com módulos menos críticos mantidos on-premise.

Estrutura da empresa

A empresa possui uma Matriz com (152 Colaboradores) Operações de Telemarketing Call Center: 100 colaboradores responsáveis por atender clientes e realizar vendas. Supervisão Central: 5 supervisores que coordenam as atividades dos operadores nas filiais, estabelecendo padrões e diretrizes operacionais. Qualidade Central: 15 colaboradores que padronizam e garantem a qualidade do atendimento em toda a empresa, criando métricas e diretrizes comuns. Setor de Tecnologia da Informação (TI): 7 colaboradores responsáveis por: Gerenciamento Central de Rede: Controle e gestão da infraestrutura de rede corporativa, abrangendo matriz e filiais. Segurança da Informação: Implementação de políticas de segurança e monitoramento de ameaças em todos os locais. Desenvolvimento e Integração de Sistemas: Desenvolvimento e manutenção dos sistemas centrais, incluindo CRM e plataformas de telemarketing. Setor de Recursos Humanos: 10 colaboradores dedicados a: Recrutamento e Seleção: Gerenciamento centralizado de estratégias e processos de contratação. Treinamento e Desenvolvimento: Planejamento de programas de treinamento aplicados nas filiais. Administração de Pessoal: Gestão de políticas de pessoal, folha de pagamento e benefícios. Financeiro: 5 colaboradores responsáveis pela gestão centralizada das questões financeiras e orçamentárias. Administrativo: 10 colaboradores que cuidam de: Logística e Compras: Planejamento e aquisição de suprimentos e equipamentos para matriz e filiais. Ativos de TI na Matriz:

Operações de Telemarketing: 80 desktops, 40 notebooks. Setor de TI: 7 notebooks. Recursos Humanos: 10 notebooks. Financeiro: 5 notebooks. Administrativo: 10 notebooks. Filiais (36 Colaboradores nas 3 Filiais) Vendedores: 10 colaboradores responsáveis pelo atendimento ao cliente e vendas. Supervisão Local: 1 supervisor por filial, responsável por gerenciar as operações diárias. Tecnologia da Informação (TI): 1 colaborador por filial para suporte técnico e manutenção de equipamentos. Ativos de TI nas Filiais:

2 racks. 2 servidores em nuvem para aplicações CRM e VoIP. 10 notebooks. 10 desktops.

Figura 1 – Cálculo de Links - Links

APPs	LB (kbps)	Matriz		Filial 1		Filial 2		Filial3		Link Internet	
		152		12		12		12			
		Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB		
Web	100	152	15200	12	1200	12	1200	12	1200	18800	
E-mail	50	152	7600	12	600	12	600	12	600	9400	
CRM	100	137	13700	12	1200	12	1200	12	1200	17300	
Suporte (TI)	80	7	560	1	80	1	80	1	80	800	
VoIP	500	127	63500	12	6000	12	6000	12	6000	81500	
HCM (RH)	30	15	450	0	0	0	0	0	0	450	
SAP	50	37	1850	2	100	2	100	2	100	2150	
			Total	9180	Total	9180	Total	9180			
				M-F1		M-F2		M-F3		130400	

Fonte: Tabela realizada pelos alunos (2024)

A tabela mostra a quantidade de largura de banda (em kbps) necessária para diferentes aplicações (como Web, E-mail, CRM, Suporte, VoIP, HCM e SAP) na Matriz e em três filiais (Filial 1, Filial 2 e Filial 3). Cada aplicação tem valores específicos de largura de banda e quantidade para cada filial, e no final da tabela, há um total de largura de banda necessária para cada filial e um total geral. Isso ajuda a entender quanto de largura de banda é necessário para cada aplicação em cada filial, facilitando o planejamento de rede e a adequação dos links de internet. Para calcular a largura de banda necessária (em kbps) identificamos o consumo médio de cada aplicação por usuário. Aplicações web podem consumir entre 100 e 300 kbps por usuário, e-mails entre 50 e 100 kbps, CRM cerca de 100 kbps, VoIP pode variar de 100 a 500 kbps dependendo do codec, e sistemas como HCM e SAP geralmente consomem menos, com 30 kbps e 50 kbps por usuário, respectivamente. Com essa informação, multiplica-se a largura de banda por usuário pelo número estimado de usuários simultâneos para cada aplicação. Na matriz, há um número maior de aplicativos e, consequentemente, a maior demanda de largura de banda, destacando-se o VoIP com 63.500 kbps e o CRM com 13.700 kbps. As três filiais possuem um uso similar, cada uma com 9.180 kbps de consumo total. A demanda total de largura de banda na rede é de 130.400 kbps, sendo esse valor fundamental para o dimensionamento adequado dos links de internet e interconexões.

Figura 2 – Cálculo de Materiais com Valores - Cabeamento

Item	Valor	Matriz		Filial 1		Filial 2		Filial3		Link Internet
		152	12	12	12	12	12	12	12	
		Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	
Servidor Dell	20000	3	60000	1	20000	1	20000	1	20000	20000
Estação Dell	10000	80	800000	12	120000	12	120000	12	120000	120000
Notebook Dell	3000	72	216000	12	36000	12	36000	12	36000	36000
Roteador CISCO	5000	1	5000	1	5000	1	5000	1	5000	5000
Serial CISCO	1000	4	4000	1	1000	1	1000	1	1000	1000
Switch Dell 24p	18000	4	72000	1	18000	1	18000	1	18000	18000
Cabo UTP CAT6 cx 305 m	3000	5	15000	1	3000	1	3000	1	3000	3000
RJ45 f Cat6	30	88	2640	14	420	14	420	14	420	420
Patch Cord CAT 6 1,5 m	32	80	2560	12	384	12	384	12	384	384
Patch Panel CAT 6 24 pts	770	4	3080	1	770	1	770	1	770	770
Rack 44 U	2000	1	2000	1	2000	1	2000	1	2000	2000
Cx + placa de acabamento	30	10	300	2	60	2	60	2	60	60
AP Rukus WiFi 6	5000	4	20000	1	5000	1	5000	1	5000	5000
Organizador de Cabo	71	2	142	1	71	1	71	1	71	71
Impressora laser corporativa	4400	3	13200	1	4400	1	4400	1	4400	4400
Nobreak	10000	3	30000	1	10000	1	10000	1	10000	10000
Mesa + Cadeira	3000	152	456000	12	36000	12	36000	12	36000	36000
		Total	R\$ 1.701.922,00	Total	R\$ 262.105,00	Total	R\$ 262.105,00	Total	R\$ 262.105,00	
		Total Geral			R\$ 2.488.237,00					

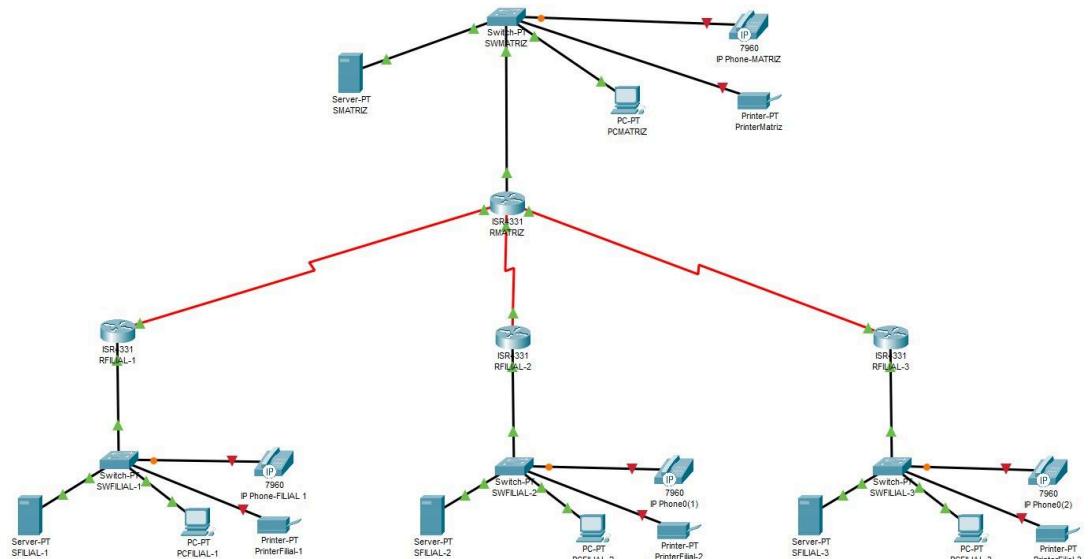
Fonte: Tabela realizada pelos alunos (2024)

A tabela apresenta uma lista de equipamentos e materiais relacionados a cabeamento e infraestrutura de TI, distribuídos entre uma matriz e três filiais. Inclui equipamentos como Servidor Dell, Estação Dell, Notebook Dell, Roteador CISCO, entre outros, com seus devidos valores. Ela é útil para visualizar e gerenciar os custos e quantidades de materiais de TI em diferentes locais da organização. Para calcular primeiro identificou-se a quantidade de pontos de rede necessários, que depende do número de dispositivos conectados (desktops, notebooks, impressoras, etc.). Com base no layout físico, calcula-se a metragem de cabos UTP (ou fibra óptica) necessária, estimado entre 30 e 50 metros por ponto, e o número de patch cords para conectar os dispositivos. A quantidade de switches é determinada pela soma de pontos de rede, considerando a capacidade das portas (ex.: switches de 24 portas). Equipamentos como patch panels e racks são dimensionados de acordo com o número de portas e a necessidade de organização física dos cabos e dispositivos. Cada patch painel geralmente possui 24 ou 48 portas, e o rack deve ser capaz de acomodar todos os switches, roteadores e outros equipamentos, com espaço para possíveis expansões futuras. Outros materiais, como conectores RJ45 e organizadores de cabos, também são calculados com base no número de pontos de rede e dispositivos. Os principais itens incluem servidores Dell, estações de trabalho, notebooks, roteadores Cisco, switches Dell, cabos e componentes de rede, além de mobiliário como mesas e cadeiras. A matriz, por ser a unidade principal, possui a maior quantidade de equipamentos, totalizando R\$ 1.698.922,00. Cada filial, embora tenha demandas similares, apresenta investimentos ligeiramente diferentes, totalizando R\$ 226.105,00 na Filial 1, R\$ 262.105,00 na Filial 2 e R\$ 262.105,00 na Filial 3.

Topologia de Rede

A imagem a seguir ilustra um esboço da proposta de projeto de redes com apresentação do cenário e como será a divisão lógica e física da rede, com os devidos Nomes e Endereços dos Servidores, as faixas de rede utilizadas em CIDR e NAT, quanto eventuais tabelas de roteamento e serviços de rede disponibilizados no protótipo.

Figura 3 – Protótipo da rede no Simulador da Cisco Packet Tracer



Fonte: esquema realizado pelos alunos (2024)

Essa imagem descreve a topologia de rede criada no packet tracer para o projeto de infraestrutura de rede da empresa de telemarketing. A matriz foi configurada com um roteador que conecta com um switch e este distribui os seguintes equipamentos:um computador, uma impressora, um telefone e um servidor central, a matriz também possui um roteador que está conectado a outros três roteadores das filiais. Cada filial também tem um switch para distribuir os equipamentos de forma lógica na rede. No software foram configurados e atribuídos de forma estática os endereçamentos IP de rede para cada um desses equipamentos: computadores, roteadores e servidores. Após isso foi feito o endereçamento de links entre eles para ter rota entre si para, por fim, serem validados.Vale ressaltar que a quantidade de ativos presentes na topologia criada não reflete a quantidade real planejada para o negócio real, se tratando somente de uma visão macro do planejamento da rede.

Preparação de Ambiente em nuvem e virtualização local

Para essa etapa do projeto foi necessário baixar e instalar o Windows Server. E como material teórico usamos de referência noções de cloud computing e sistemas operacionais, no sistema de rede terão 11 máquinas virtualizadas locais, um servidor virtualizado local e um servidor virtualizado na nuvem. A nuvem usada para este trabalho foi o Amazon AWS. Após isso foi usado o Virtualbox e Windows server para configurar o serviço de diretórios. Assim é possível ter várias unidades organizacionais refletindo a empresa de telemarketing.

Inicialmente foi utilizado o arquivo .ISO do Windows Server para iniciar a instalação no Virtualbox

Figura 4– Tela inicial de configuração do Virtualbox

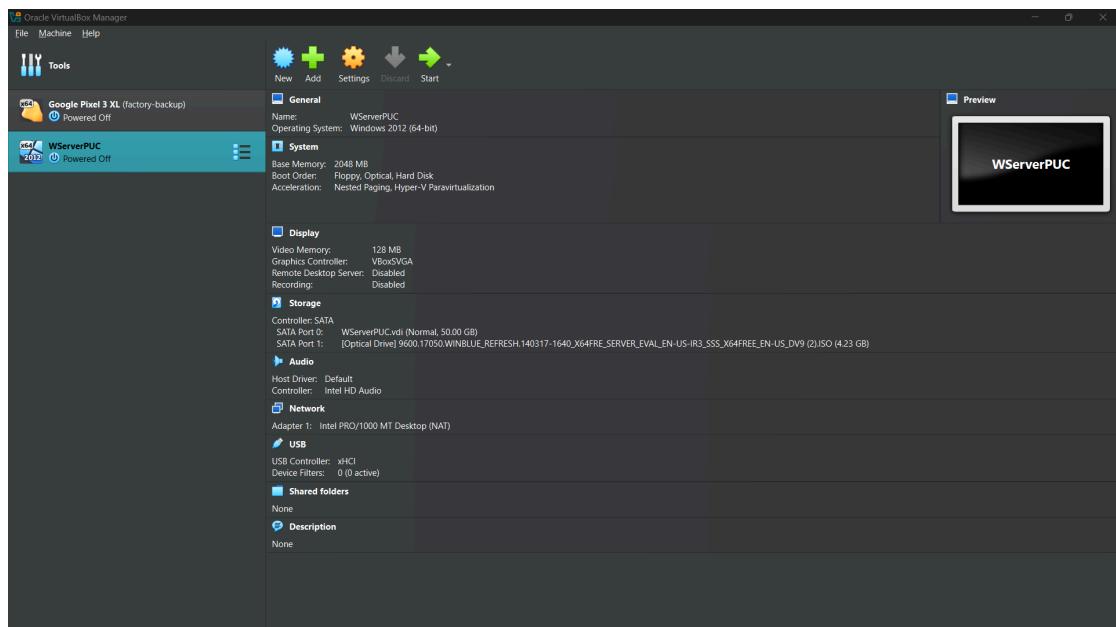
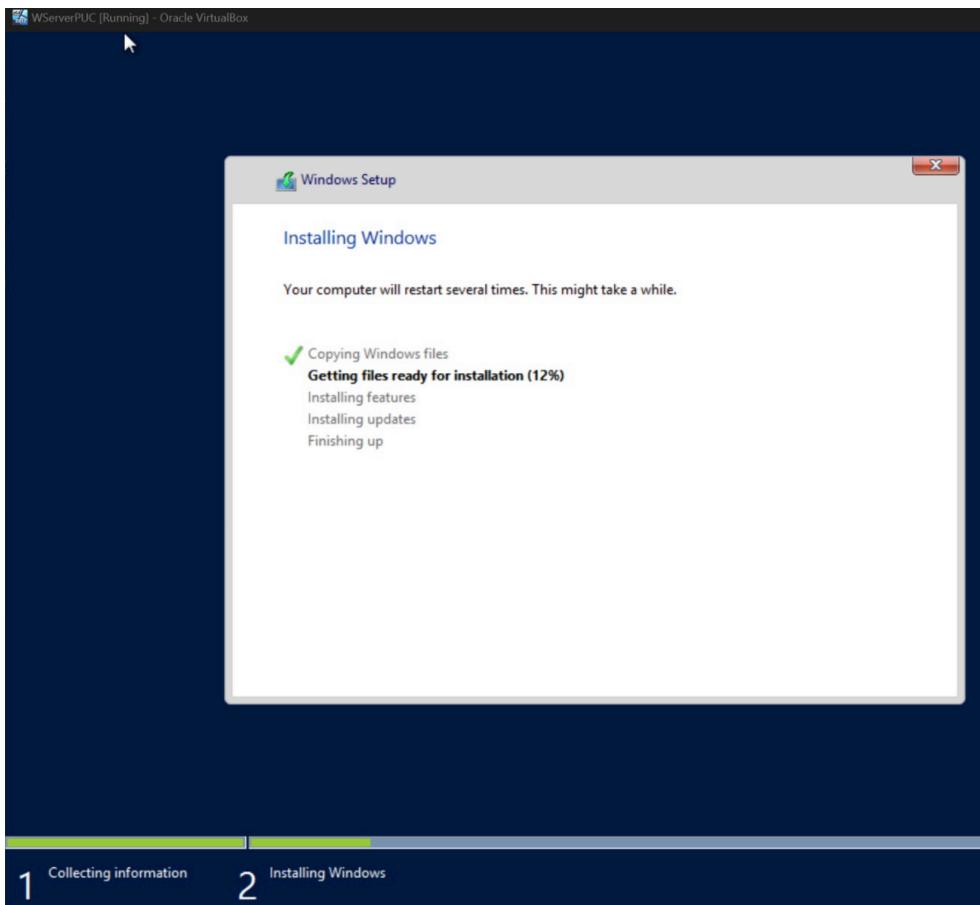
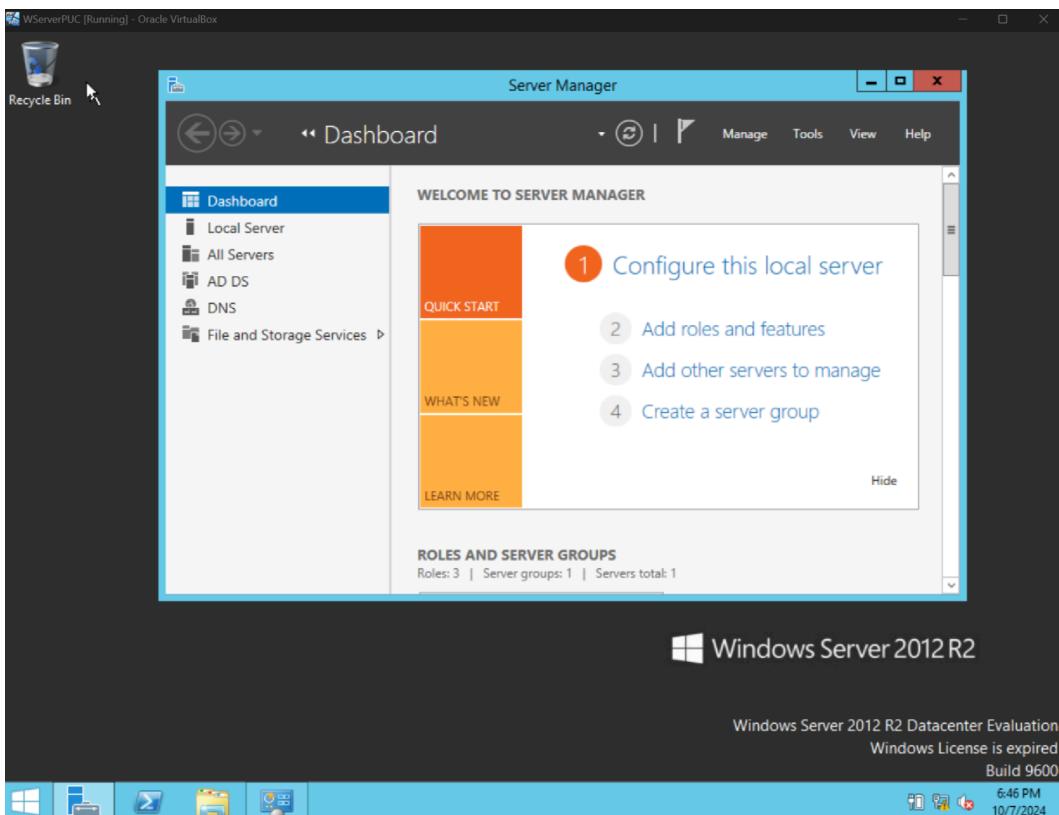


Figura 5– Carregamento das configurações do host Windows no Vbox



Após seguir as etapas de instalação e criação de um usuário administrador o servidor foi ligado e o acesso ao server manager foi validado, sendo possível configurar o domínio **telemak.corp**.

Figura 6– Tela inicial do Windows Server após configurado no Vbox



Foram então criadas unidades organizacionais (OU) para cada estado em que a matriz e as filiais estariam presentes: MG, RJ, SP, PR. Cada OU com respectivas separações para computadores e usuários.

Figura 7– Unidades Organizacionais criadas no AD.

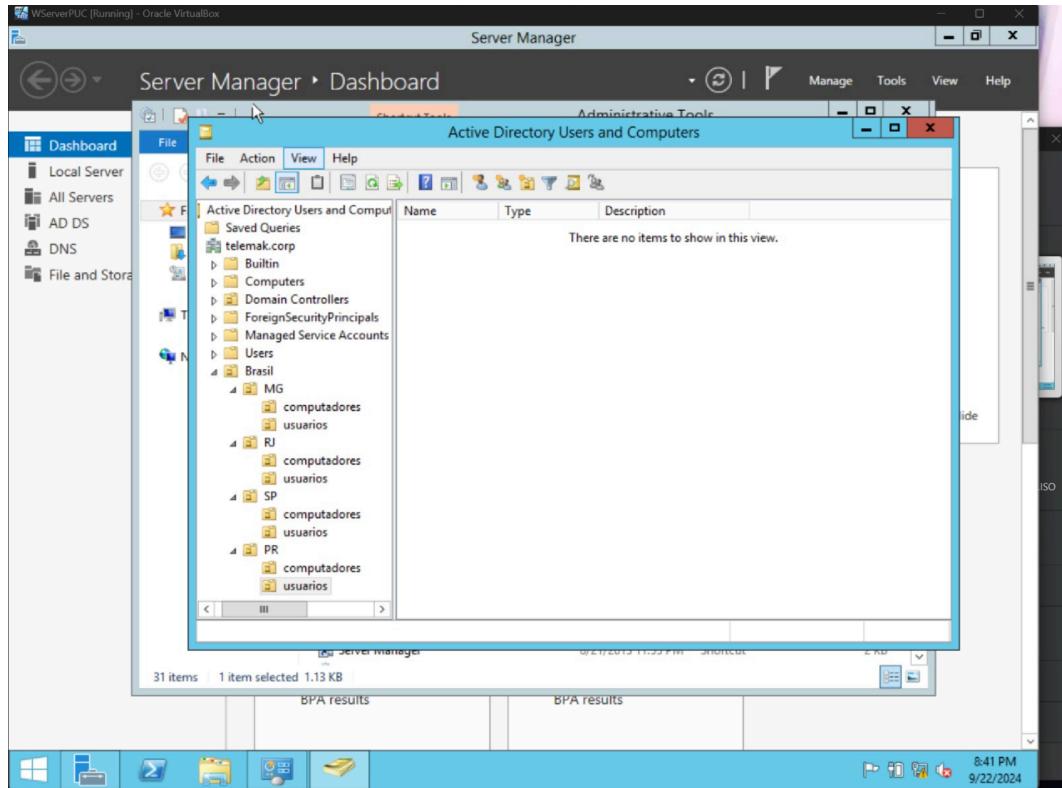
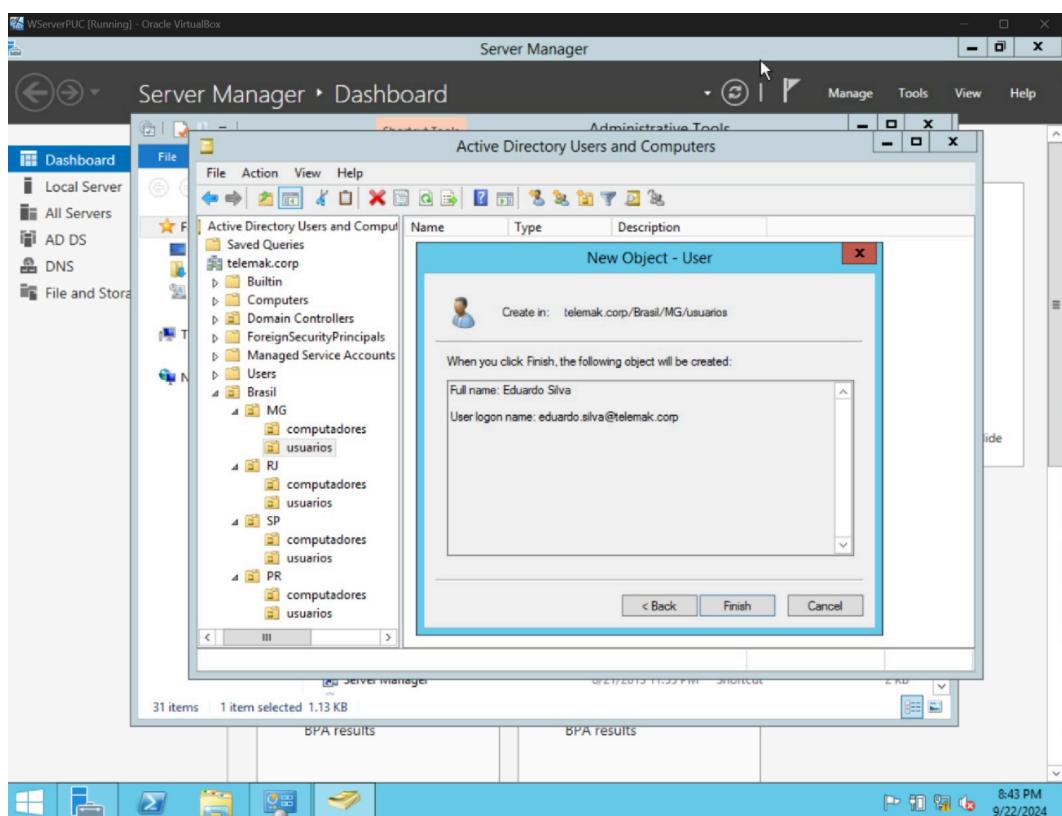


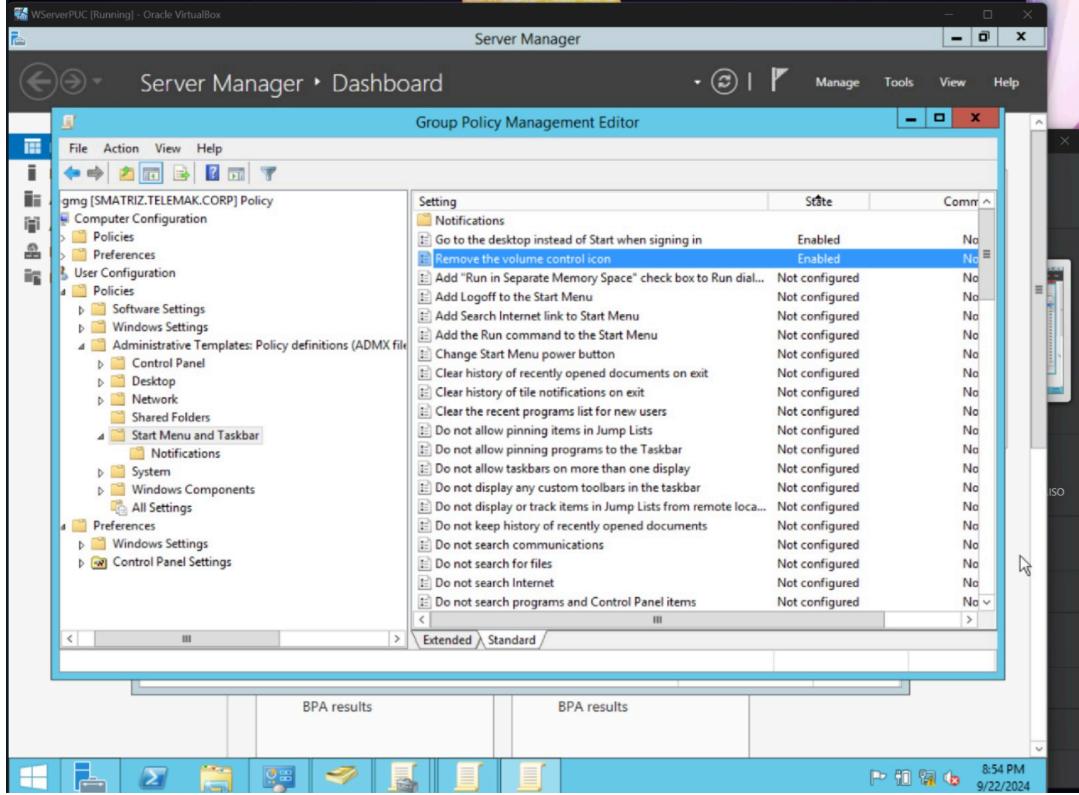
Figura 8– Criação de usuário no AD.

Além disso, foi criado também um usuário chamado eduardo.silva no domínio telemak.corp.



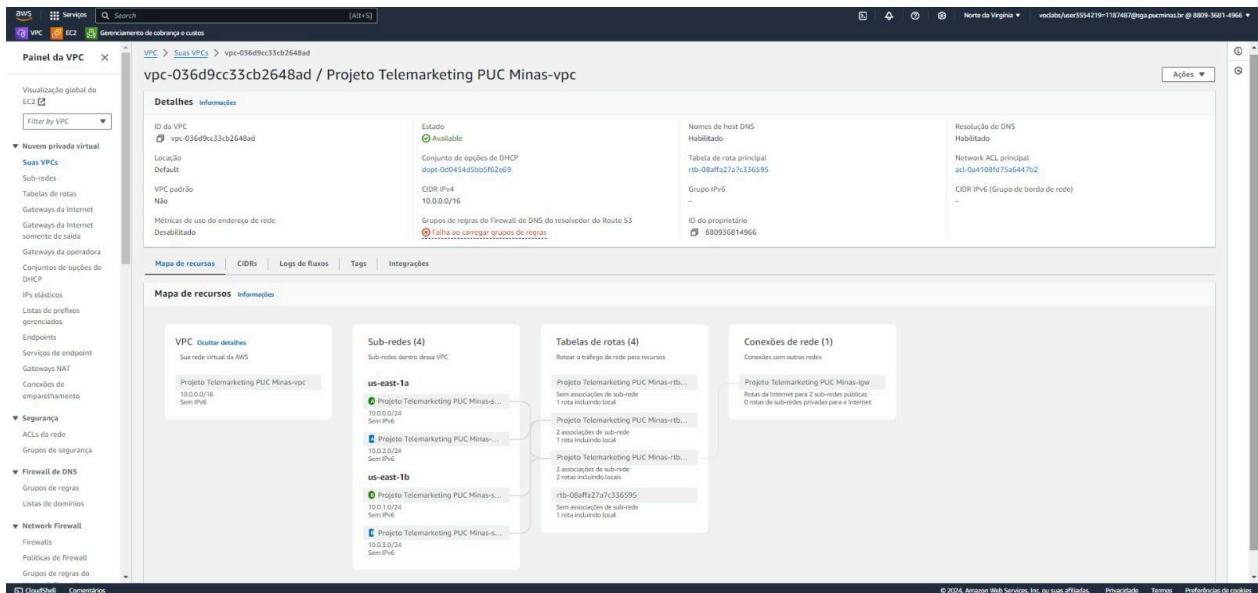
Por fim, foi criado uma política de grupo padrão no AD com algumas regras especificadas.

Figura 9 – Criação de política de grupo no AD com regras específicas.



O próximo passo foi começar a programar o back end, criando recursos, sendo essa, parte da virtualização local. Teremos 2 máquinas, uma máquina local e uma máquina na nuvem. Todos os commits do projeto foram postados no github no repositório da classe do professor do curso para registro do trabalho.

Figura 10 – Print do quadro de VPCs no AWS



Fonte: Conta AWS realizado pelos alunos (2024)

Depois de ter acesso ao ambiente da AWS, iniciaram-se a criar os recursos VPC, EC2 e

RDS para o ambiente. Começamos com a criação de recursos da AWS em uma rede virtual logicamente isolada, a VPC. Nela associamos as redes públicas e as privadas, personalizamos os blocos CIDR, todas /24.

Figura 11 – Print do quadro de Grupos de segurança no AWS

Name	ID da regra do grupo	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
sg-0de007d9e500ac2fe -	sg-0de007d9e500ac2fe	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso Web
sg-0f411af24a0b7288e	sg-0f411af24a0b7288e	IPv4	RDP	TCP	3389	0.0.0.0/0	Terminal Remoto

Fonte: Conta AWS realizado pelos alunos (2024)

A próxima etapa foi criar grupos de segurança configurando regras de entrada e de saída. Especificando para as portas 80 (HTTP) e 3389 (RDP) estarem expostas para internet, sendo possível o acesso a página web padrão do IIS configurado no servidor e o acesso remoto a partir do serviço RDP.

Figura 12– Acesso ao host Windows configurado na AWS



Fonte: Conta AWS realizado pelos alunos (2024)

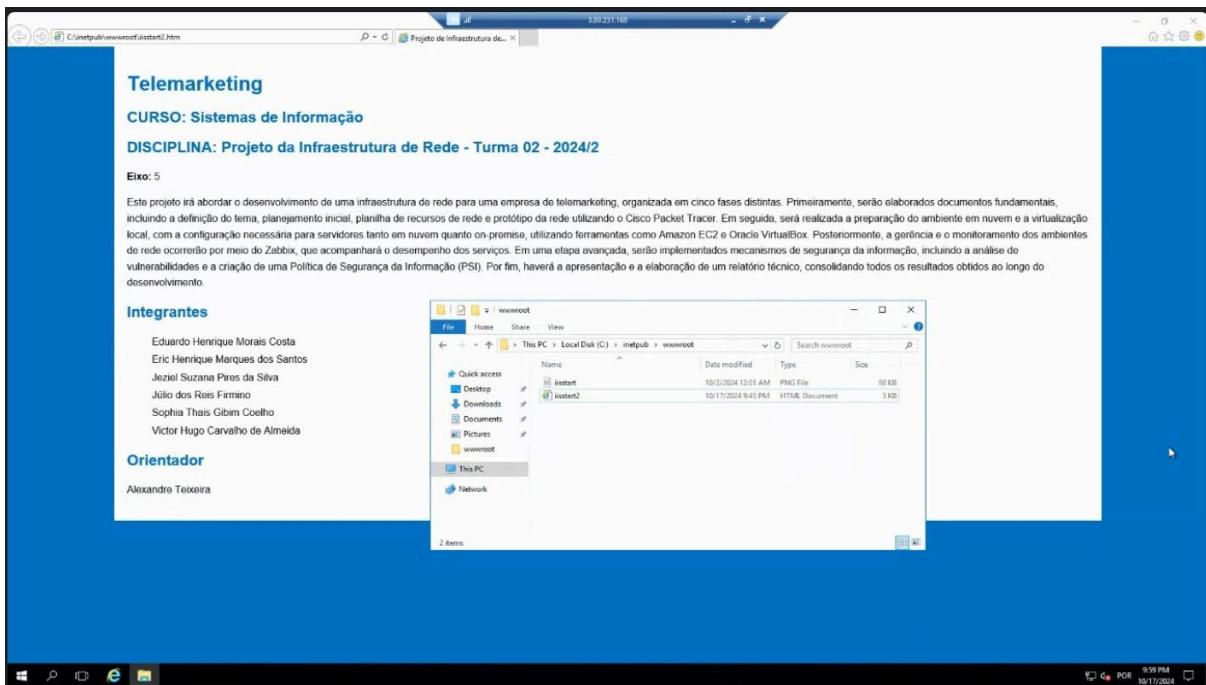
Depois de criado o VPC, foi criado um servidor EC2 dentro do servidor para reduzir os custos de hardware. Dentro da AWS se fez uma instância que foi configurada a fim de criar um endereço IP para entrar no servidor. Junto a isso também se criou uma senha para ter segurança.

Figura 13– Print da página html do server criado

Fonte: Server empresa telemarketing realizado pelos alunos (2024)

Após entrar no servidor com o IP público, foi configurado o serviço web server IIS e depois, para testar foi aberto o Internet Explorer no servidor para acessar a página HTML padrão do IIS. Essa página HTML foi personalizada para apresentação do trabalho.

Figura 14– Print da página html do server criado com o IP



Fonte: Server empresa telemarketing realizado pelos alunos (2024)

Gerência e monitoração de ambientes em redes

A seguir será demonstrado as etapas para configuração do monitoramento dos hosts em nuvem e em ambiente local previamente configurados. Para isso, utilizaremos a ferramenta Zabbix. Será configurado um appliance Zabbix, que consiste em um dispositivo específico de hardware e software para essa finalidade. O Zabbix vai monitorar o comportamento dos serviços de rede e os recursos físicos dos equipamentos, verificando se os serviços estão ativos ou inativos, o consumo de CPU, memória e a ocupação de links e portas de switches. Inicialmente o appliance do Zabbix foi configurado no Virtual Box, e seu acesso foi feito com as credenciais root:zabbix, e validado que pegou um IP da rede local:

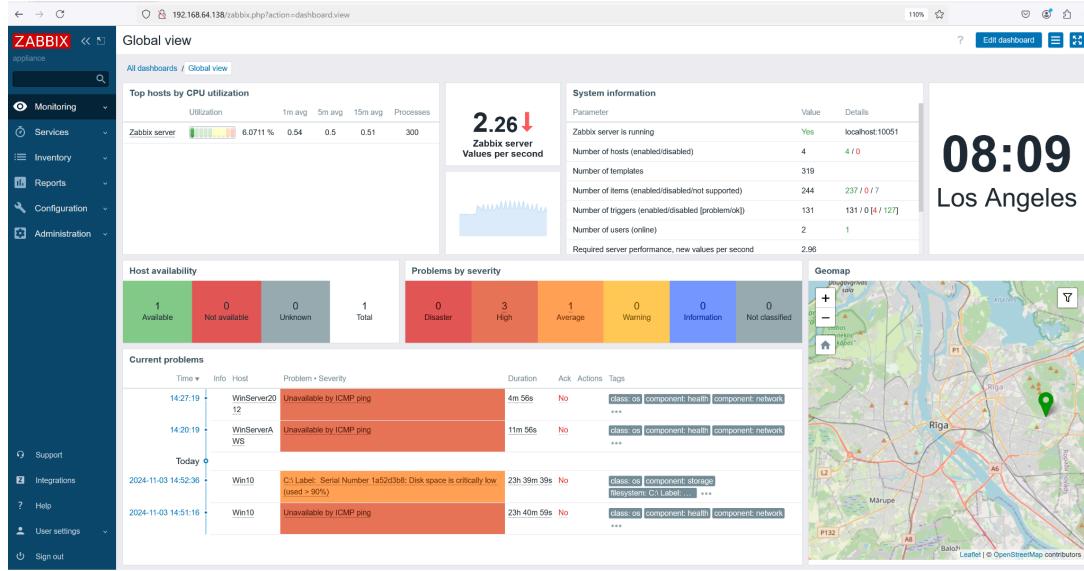
Figura 15– Print do acesso ao host do Zabbix Server

```
[root@appliance ~]# 
[root@appliance ~]# 
[root@appliance ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:b8:6e:cf brd ff:ff:ff:ff:ff:ff
        inet 192.168.64.138/24 brd 192.168.64.255 scope global dynamic eth0
            valid_lft 1805sec preferred_lft 1805sec
        inet6 fe80::20c:29ff:feb8:6ecf/64 scope link
            valid_lft forever preferred_lft forever
[root@appliance ~]# hostname
appliance
[root@appliance ~]#
```

Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

A seguir o acesso foi validado em um navegador para entrar no painel administrativo do Zabbix.

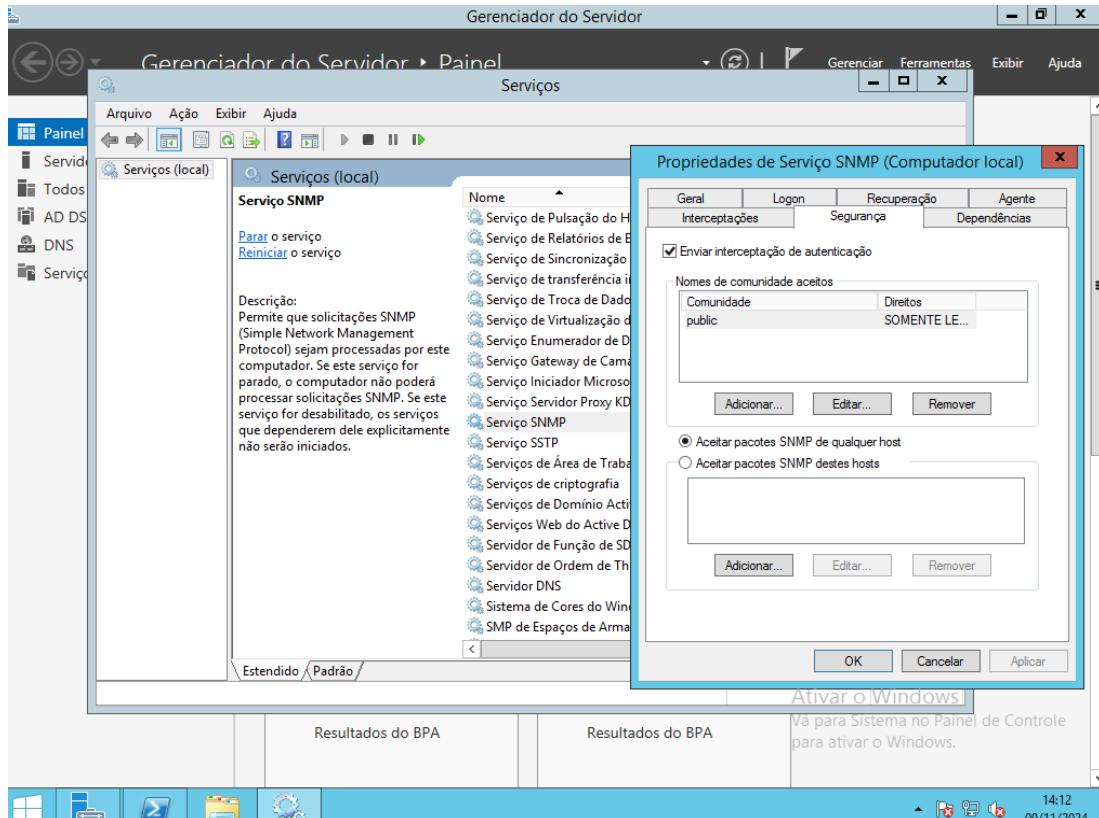
Figura 16– Print do painel administrativo



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

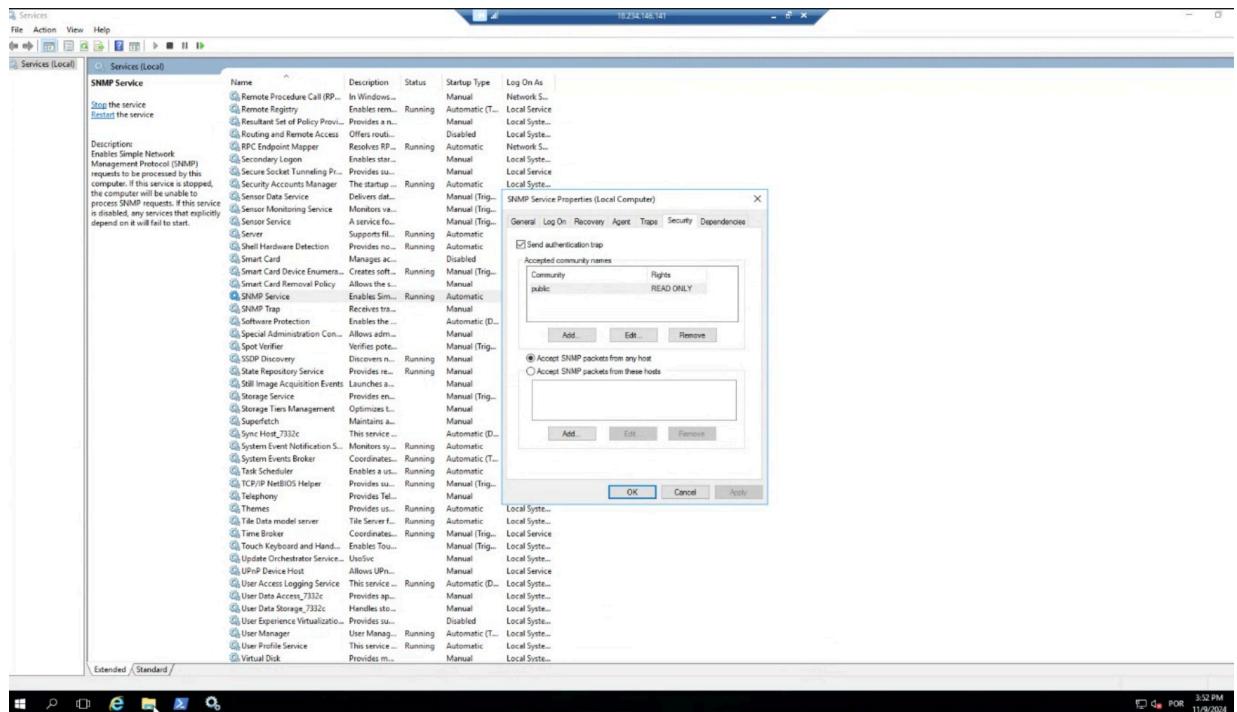
Em seguida foi configurado o serviço SNMP para o Windows Server local e para Windows Server em Cloud. Para isso, foi acessado o services do Windows e configurado para cada host aceitar pacotes SNMP de qualquer origem e para utilizar a string “public” como comunidade:

Figura 17– Configuração SNMP no Windows Server Local



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

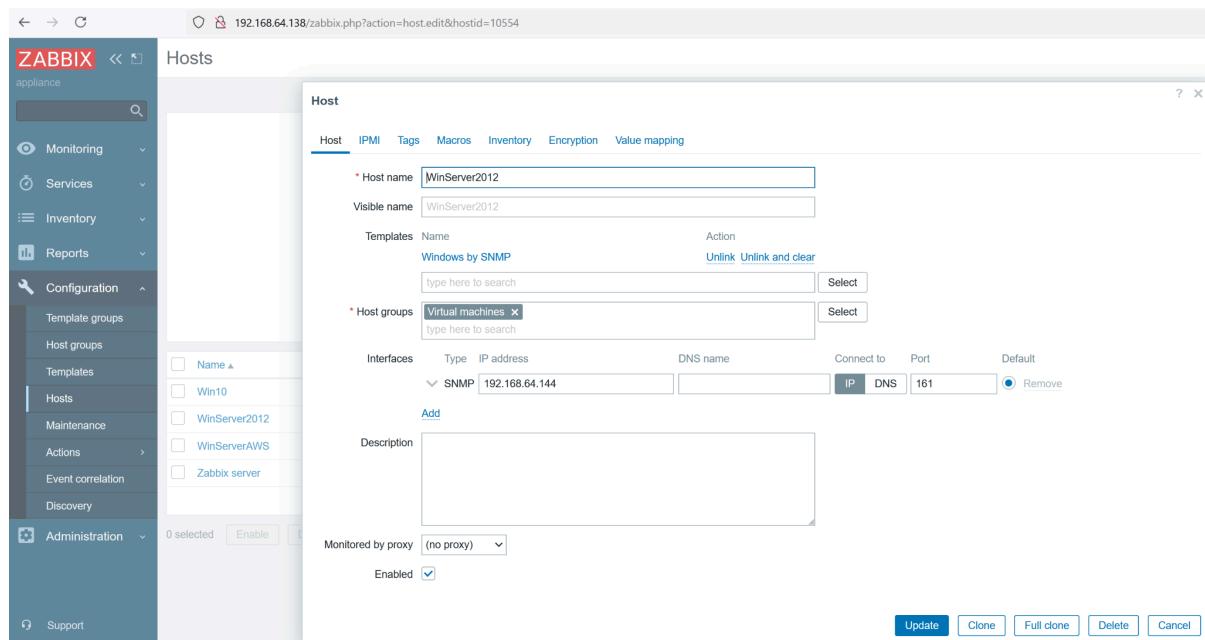
Figura 18– Configuração do SNMP no Windows Server em Cloud



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Após isso, nas configurações da interface do Zabbix, em Hosts, foi criado um host para o Windows Server local e para o Windows Server em Cloud com as respectivas configurações, especificando o IP dos servidores e a porta 161 onde o serviço SNMP está rodando.

Figura 19– Configuração hosts no zabbix server para windows server local



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Figura 20– Configuração hosts no zabbix server para windows server em cloud

The screenshot shows the Zabbix 'Hosts' configuration page. On the left, there's a sidebar with navigation links like Monitoring, Services, Inventory, Reports, Configuration (selected), Host groups, Templates, Hosts, Maintenance, Actions, Event correlation, Discovery, Administration, Support, and Integrations. The main area is titled 'Host' and contains fields for 'Host name' (WinServerAWS), 'Visible name' (WinServerAWS), 'Templates' (Windows by SNMP), 'Host groups' (Discovered hosts), and 'Interfaces' (SNMP with IP 18.234.146.141, Port 161). A large 'Description' text area is empty. At the bottom, there are buttons for 'Update', 'Clone', 'Full clone', 'Delete', and 'Cancel'.

Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Em seguida, para o Windows Server em Cloud foi necessário permitir, nos grupos de segurança de entrada e de saída da AWS, a concessão para liberar pacotes ICMP para o Zabbix Server conseguir se comunicar com o servidor:

Figura 21– Liberação regra de entrada ICMP

The screenshot shows the AWS VPC Security Groups details for a security group named 'sg-0de007d9e500ac2fe'. The 'Regras de entrada' tab is selected, displaying five entries. One entry is highlighted: 'sgr-0f932ee3666514e5' with 'Name' 'sgr-0f932ee3666514e5', 'ID da regra de grupo' 'sgr-0f932ee3666514e5', 'IPV4' 'sgr-0f932ee3666514e5', 'Tipo' 'UDP personalizado', 'Protocolo' 'UDP', 'Intervalo de portas' '161 - 162', 'Origem' '0.0.0.0/0', and 'Descrição' 'SNMP'. Other entries include rules for HTTP, RDP, and ICMP.

Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Figura 22– Liberação regra de saída ICMP

Name	ID da regra do grupo...	Versão do IP	Tipo	Protocolo	Intervalo de portas	Destino	Descrição
-	sgr-0x213ba3eb0451...	IPv4	Todos os ICMPs - IPv4	ICMP	Tudo	0.0.0.0/0	ping
-	sgr-05eacbed2bfcd6030	IPv4	UDP personalizado	UDP	161 - 162	0.0.0.0/0	SNMP
-	sgr-09554bf1cac6672ca	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso terminal Remoto
-	sgr-050f994585e8d689e	IPv4	Todo o tráfego	Tudo	Tudo	0.0.0.0/0	Todo o tráfego
-	sgr-0e1b74753dd28c4...	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso Web

Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Em seguida, foi necessário desativar o Firewall do Windows no servidor em nuvem:

Figura 23– Desativação do firewall

```

Hostname: EC2AMAZ-93BLGKC
Instance ID: i-007ea7dd172426a97
Public IPv4 address: 18.234.146.141
Private IPv4 address: 10.0.0.16
Instance size: t2.large
Availability Zone: us-east-1a
Architecture: AMD64
Total memory: 8192 MB
Network: Low to Moderate

Administrator: Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> netsh advfirewall set allprofiles state off
Ok.

PS C:\Users\Administrator> ping 18.234.146.141

Pinging 18.234.146.141 with 32 bytes of data:
Reply From 18.234.146.141: bytes=32 time=1ms TTL=127

Ping statistics for 18.234.146.141:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Administrator>

```

Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Com isso, foi possível validar que os 2 servidores (e outros de teste) estavam com rota e sendo monitorados corretamente pelo serviço Zabbix a partir da tela de configuração do serviço:

Figura 24– Tela inicial do serviço Zabbix evidenciando hosts monitorados

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
Win10	Items 55	Triggers 26	Graphs 7	Discovery 3	Web 192.168.64.128:161	Windows by SNMP	Enabled	SNMP	None				
WinServer2012	Items 28	Triggers 14	Graphs 4	Discovery 3	Web 192.168.64.144:161	Windows by SNMP	Enabled	SNMP	None				
WinServerAWS	Items 13	Triggers 7	Graphs 1	Discovery 3	Web 18.234.146.141:161	Windows by SNMP	Enabled	SNMP	None				
Zabbix server	Items 133	Triggers 77	Graphs 27	Discovery 4	Web 127.0.0.1:1050	Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None				

Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Nesta tela, os administradores podem visualizar rapidamente o status e a disponibilidade dos dispositivos conectados à rede.

Na imagem, observamos uma lista de hosts monitorados, incluindo Win10, Win Server 2012 e Zabbix Server. Cada host possui um status "Enabled", indicando que estão ativos e sob monitoramento contínuo. Além disso, a disponibilidade de cada host é exibida através de protocolos como "SNMP" (Simple Network Management Protocol) e "ZBX" (Zabbix Agent), permitindo uma coleta de dados precisa e em tempo real.

A interface também exibe, no canto inferior direito, a informação de que foram encontrados quatro hosts. Este detalhe é crucial para os administradores, pois garante que todos os dispositivos esperados estão sendo monitorados, facilitando a detecção de anomalias ou falhas na rede.

A tela inicial do Zabbix, portanto, não apenas apresenta o status atual dos hosts, mas também permite uma gestão proativa, onde os administradores podem tomar medidas imediatas em caso de problemas, assegurando assim a estabilidade e o desempenho da infraestrutura de TI.

Figura 25– Monitoramento windows server local



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Nesta figura, observamos como o Zabbix monitora o uso de espaço em disco em um servidor Windows Server 2012, apresentando informações cruciais de forma visual e acessível.

Na imagem, destacamos um gráfico de pizza no canto superior esquerdo, que fornece uma visão instantânea do espaço em disco disponível versus o utilizado. Com um espaço total de 60 GB, a porção usada é de 9.63 GB, representando 16.05% do total. Esta visualização rápida permite aos administradores identificar imediatamente o nível de uso do disco, evitando possíveis problemas de falta de espaço que podem comprometer o desempenho do servidor.

Abaixo do gráfico de pizza, dois gráficos de linha fornecem uma análise mais detalhada ao longo do tempo. O primeiro gráfico mostra a porcentagem de espaço utilizado, com uma linha verde representando o uso crescente ou estável do disco. O segundo gráfico apresenta o espaço total disponível, que neste caso permanece constante, indicando que não houve mudanças na capacidade de armazenamento do servidor.

Além dos gráficos, o painel lateral esquerdo do Zabbix apresenta várias opções de navegação, como "Monitoring", "Services", "Inventory", "Reports", "Configuration" e "Administration". Essas opções permitem que os usuários naveguem facilmente entre diferentes funções e configuram a ferramenta de acordo com suas necessidades específicas de monitoramento.

Figura 26– Monitoramento windows server local



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

A imagem apresentada exibe a interface do Zabbix, uma ferramenta essencial para o monitoramento do desempenho de servidores. No contexto específico, a interface está focada na monitoração da memória física de um servidor Windows Server 2012.

O menu lateral esquerdo fornece diversas opções de navegação, incluindo "Monitoring" e "Configuration", que permitem uma gestão eficaz e intuitiva do sistema.

No painel central, dois gráficos ilustram a utilização da memória física do servidor, facilitando a visualização do desempenho e o reconhecimento de possíveis problemas. Estes gráficos são fundamentais para que os administradores de sistemas possam acompanhar, em tempo real, o uso da memória e tomar medidas preventivas quando necessário.

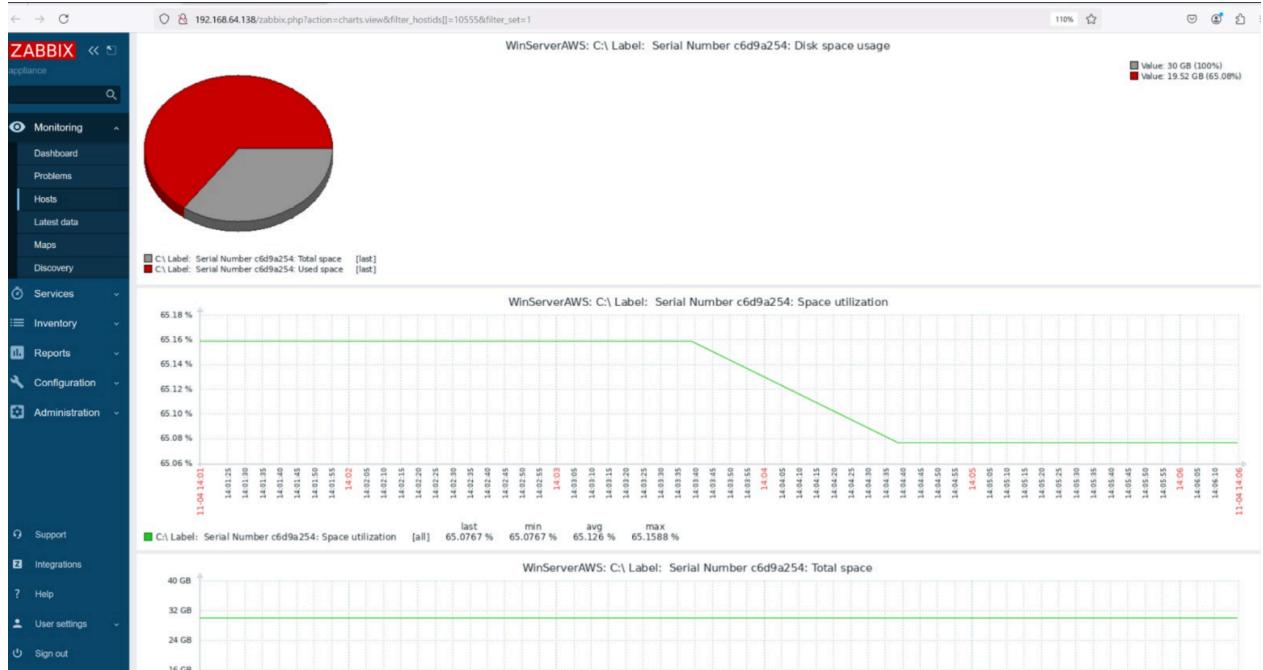
Figura 26– Monitoramento windows server local



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

- A tela apresenta gráficos de monitoramento de um servidor Windows Server 2012, incluindo gráficos de uso de espaço do disco C: e de utilização da CPU.

Figura 27– Monitoramento windows server cloud

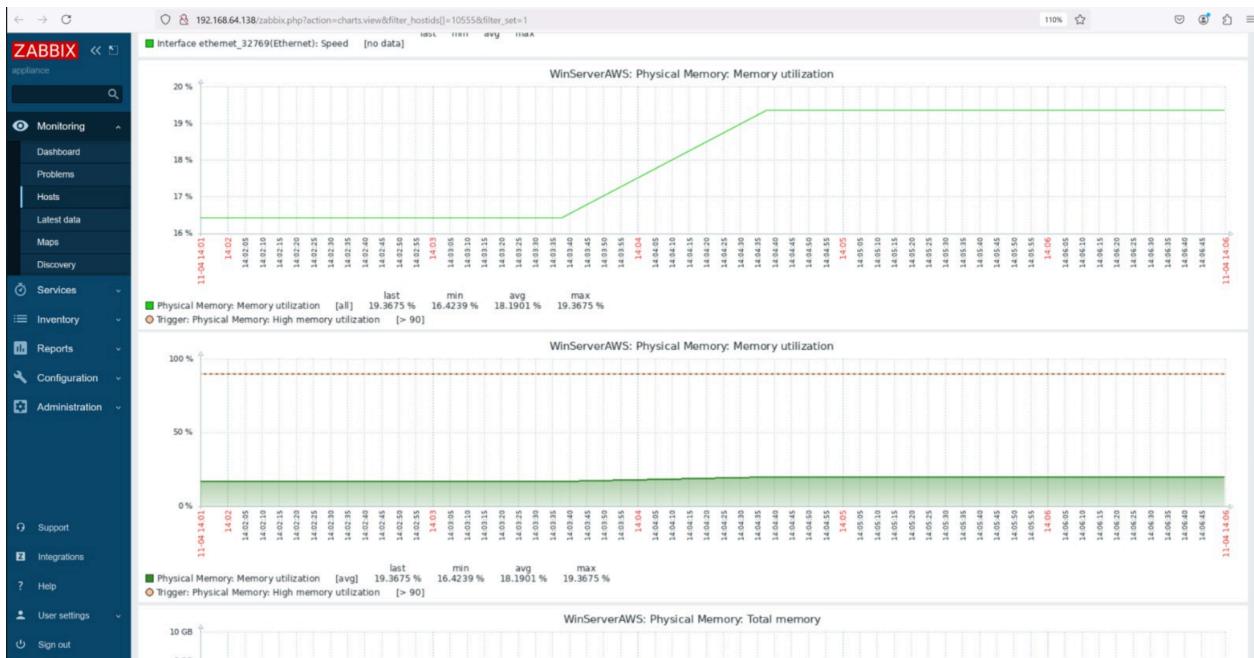


Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Nesta interface, podemos observar:

1. Gráfico de Pizza no Canto Superior Esquerdo:
 - Este gráfico representa o uso do espaço em disco do servidor.
 - Ele mostra que o espaço total do disco é de 30 GB, dos quais 19,52 GB (65,08%) estão sendo utilizados.
2. Gráficos de Linha Abaixo do Gráfico de Pizza:
 - O primeiro gráfico de linha ilustra a utilização do espaço em disco ao longo do tempo.
 - O segundo gráfico de linha mostra a capacidade total do disco, que permanece constante em 32 GB ao longo do tempo.

Figura 28– Monitoramento windows server cloud

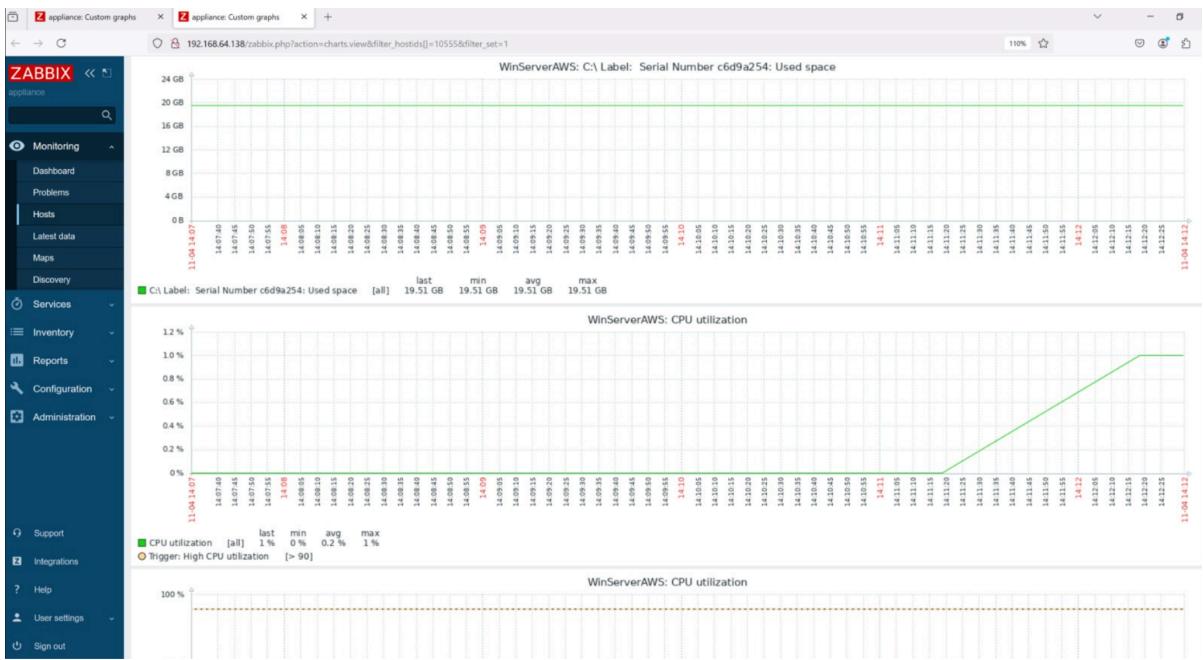


Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

A tela está dividida em três gráficos principais:

1. WinServer AWS: Physical Memory: Memory utilization - Este gráfico mostra a utilização da memória física do servidor ao longo do tempo. A linha verde representa a utilização da memória, que começa em torno de 16% e aumenta para cerca de 19%. Abaixo do gráfico, há estatísticas detalhadas:
2. WinServer AWS: Physical Memory: Memory utilization - Este gráfico também mostra a utilização da memória física, mas em uma escala diferente, com um limite de 100%. A linha verde permanece constante em torno de 19%. As mesmas estatísticas detalhadas são apresentadas abaixo do gráfico.
3. WinServerAWS: Physical Memory: Total memory.

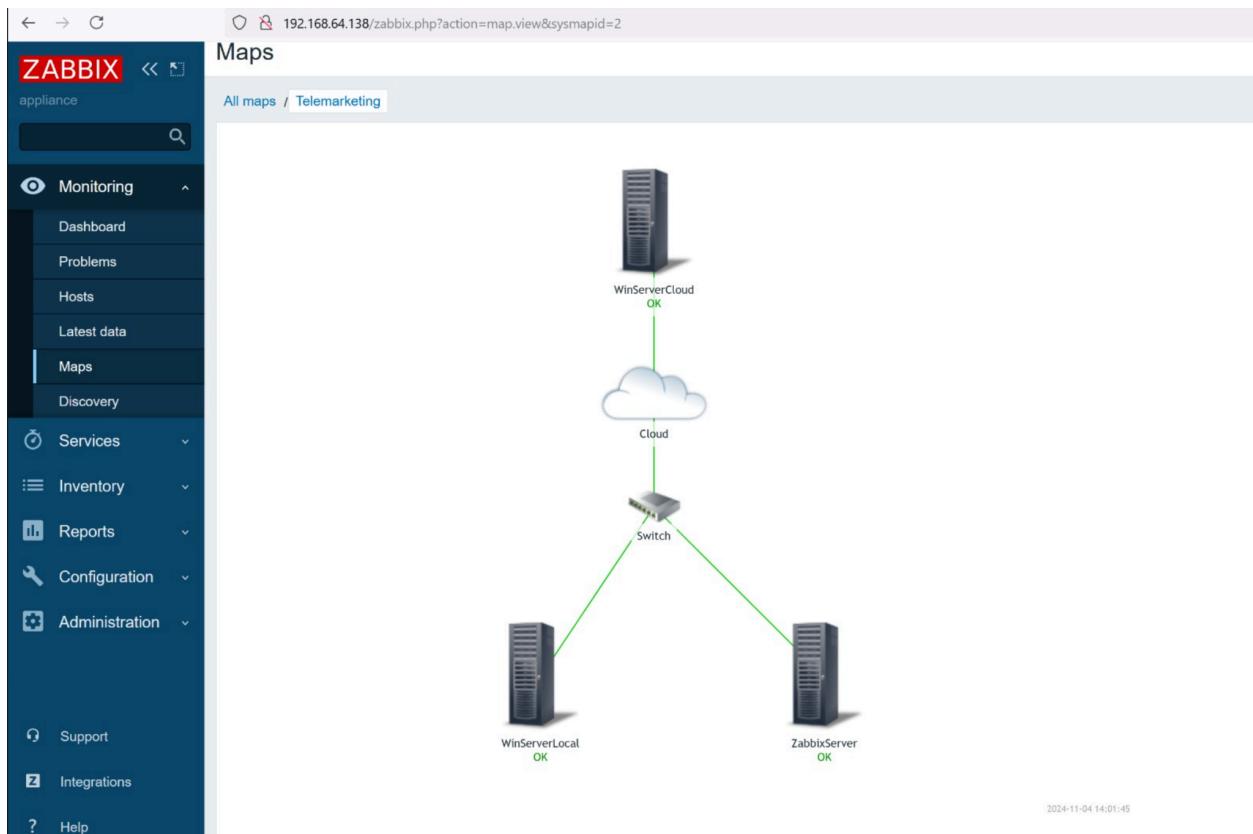
Figura 29– Monitoramento windows server cloud



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Por fim, foi criado o mapa de gráficos para os hosts que estavam sendo monitorados. No Zabbix, o Mapa de Gráficos é um recurso visual que permite criar e visualizar mapas personalizados dos dispositivos e serviços monitorados. Esses mapas podem incluir ícones e links que representam os equipamentos e suas conexões, como servidores, roteadores, switches e outros recursos da rede. Cada ícone pode exibir o status atual dos itens monitorados, como a utilização de CPU, memória e o estado dos serviços (ativo/inativo), proporcionando uma visão centralizada e intuitiva da infraestrutura. O Mapa de Gráficos ajuda a identificar rapidamente problemas e a analisar o desempenho e o comportamento dos componentes da rede em tempo real.

Figura 30– Mapa de Gráficos



Fonte: Zabbix empresa telemarketing realizado pelos alunos (2024)

Segurança da Informação da Solução

Essa etapa foi desenvolvida uma política de segurança da informação que pode ser visualizada no apêndice. Essa política vai tratar de questões que são um conjunto de regras e práticas adotadas por uma organização para garantir a segurança das informações pessoais e sensíveis. Ela visa proteger os dados contra acessos não autorizados, vazamentos e uso indevido, assegurando que sejam coletados, armazenados, processados e descartados de forma segura. Com o aumento de ataques cibernéticos e legislações como a LGPD (Lei Geral de Proteção de Dados) no Brasil, essa política tornou-se essencial. Ela inclui medidas como criptografia, autenticação robusta e treinamentos, além de procedimentos para notificação de incidentes. O objetivo é garantir a privacidade dos indivíduos e minimizar riscos legais e financeiros para a organização. Além disso, foi criada uma cartilha de segurança que é essencial para orientar os colaboradores sobre como proteger dados sensíveis e evitar riscos no ambiente de trabalho. Ela ensina comportamentos corretos, como o uso de senhas fortes, a proteção de dispositivos e o cuidado ao compartilhar informações.

Em seguida, serão evidenciados uma parte da solução de Backend do projeto que vai contar com tela inicial, cadastro de pessoas, tela de login e tabela de registros.

Figura 31– Cartilha de Segurança



Fonte: Canva, realizado pelos alunos (2024)

Este guia foi desenvolvido para promover uma cultura de segurança robusta, garantindo que todos os funcionários estejam bem informados e capacitados para proteger os ativos digitais da empresa. Além disso, reforça a importância da responsabilidade individual na segurança da informação, ajudando a prevenir incidentes que poderiam comprometer a integridade, confidencialidade e disponibilidade dos dados.

Em resumo, o guia serve como uma ferramenta essencial para educar e orientar os colaboradores sobre as melhores práticas a serem seguidas, minimizando riscos e assegurando a continuidade dos negócios de forma segura e eficiente.

Figura 32– Tela Inicial



A página inicial da **Tele Connect Solutions** apresenta um design clean e funcional. O fundo azul escuro com texto em branco e amarelo oferece um contraste eficiente e facilita a leitura. No canto superior esquerdo, encontra-se o logotipo da empresa, enquanto no canto superior direito, estão os links de navegação "Home", "Login", "Register" e "Contact", proporcionando uma navegação fácil e intuitiva.

O título principal "Conheça a empresa de Telemarketing Tele Connect Solutions" destaca-se no centro da página, acompanhado de um texto de exemplo em latim (Lorem Ipsum), servindo como placeholder. Ao lado do texto, um logotipo estilizado reforça a identidade visual da empresa. Na parte inferior esquerda, há um botão "READ MORE" que direciona os visitantes para mais informações sobre a empresa.

Fonte: Backend realizado pelos alunos (2024)

Figura 33– Tela de registro de empregado

PUC MINAS - Sistema de Informação

TELE CONNECT
SOLUTIONS

Home Login Register Contact

Cadastre os seus dados

Username Email Senha Confirme a Senha

Sign Up

- Sua senha não pode ser muito parecida com o resto das suas informações pessoais.
- Sua senha precisa conter pelo menos 8 caracteres.
- Sua senha não pode ser uma senha comumente utilizada.
- Sua senha não pode ser inteiramente numérica.

RECENT POSTS

Aliquam ac eleifend metus
March 10, 2018

Donec in libero sit amet mi vulputate
March 10, 2018

QUICK LINKS

Home Faq
About us Terms & Conditions
Services Careers
Testimonials Newsletter & Exchange

Fonte: Backend realizado pelos alunos (2024)

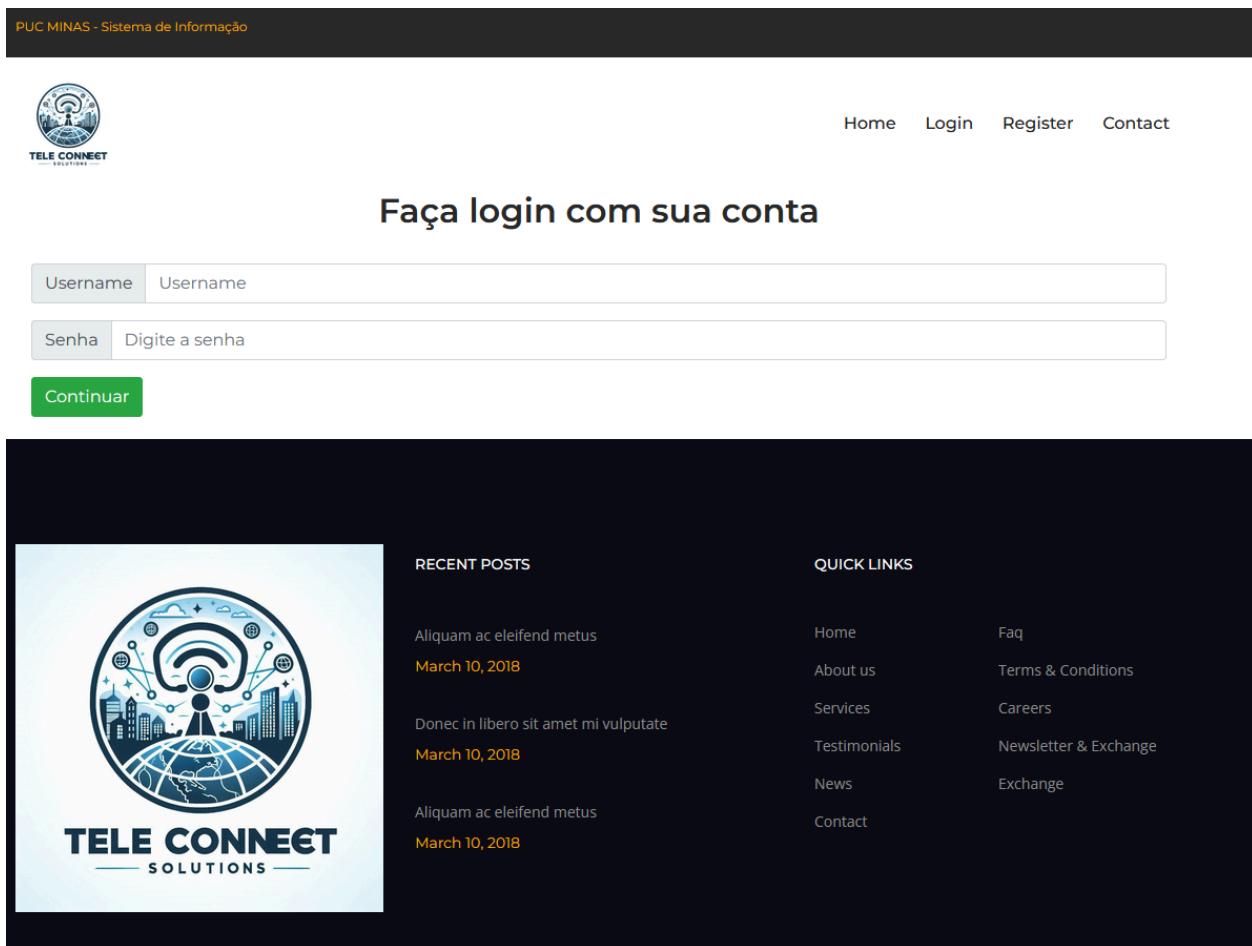
A página de cadastro "Cadastre os seus dados" permite que novos usuários se registrem no sistema. Para isso, é necessário preencher os seguintes campos:

1. Username (Nome de usuário): Escolha um nome único.
2. Email (Endereço de email): Informe um email válido.
3. Senha (Senha de acesso): Crie uma senha segura.
4. Confirme a Senha (Confirmação da senha): Repita a senha para confirmar.

Após preencher todos os campos, clique no botão Sign Up (Cadastrar-se) para concluir o registro. Certifique-se de seguir as instruções para criação de senha:

- Não pode ser muito parecida com outras informações pessoais.
- Deve conter pelo menos 8 caracteres.
- Não pode ser uma senha comumente utilizada.
- Não pode ser inteiramente numérica.

Figura 34– Tela de Login



Nossa página de login da Tele Connect Solutions tem um design limpo e organizado. No topo, há um menu de navegação com opções como "Home", "Login", "Register" e "Contact".

Logo abaixo, temos o título "Faça login com sua conta", seguido pelos campos para inserir o nome de usuário e a senha. Há placeholders que ajudam os usuários a entender o que inserir em cada campo: "Username" e "Digite a senha". Para prosseguir com o login, basta clicar no botão verde com o texto "Continuar".

Na parte inferior da página, encontra-se o logotipo da Tele Connect Solutions à esquerda, acompanhado por duas colunas de links. A coluna "Recent Posts" lista postagens recentes, e a coluna "Quick Links" fornece atalhos para várias páginas do site, como "Home", "About us", "Services", entre outras.

Essa estrutura facilita a navegação e torna o processo de login simples e eficiente para os usuários.

Fonte: Backend realizado pelos alunos (2024)

Figura 35– Tela da área logada

The screenshot shows a web application interface. At the top, there's a dark header bar with the text "PUC MINAS - Sistema de Informação" on the left and "Bem vindo, Julio." on the right. Below the header is a navigation bar with links for "Home", "Cadastrar", "Listar", and "Logout". To the left of the main content area is the "TELE CONNECT SOLUTIONS" logo. The main content features a large blue banner with white text that reads: "Conheça a empresa de Telemarketing Tele Connect Solutions". Below this text is a small paragraph of placeholder text: "Cras vitae turpis lacinia, lacinia lacus non, fermentum nisi. Donec et sollicitudin est, in euismod erat. Ut at erat et arcu pulvinar." At the bottom of the banner is a "READ MORE" button. To the right of the banner is a white rectangular box containing the company's logo, which is a circular emblem featuring a globe, buildings, and connectivity lines, with the text "TELE CONNECT SOLUTIONS" below it.

Fonte: Backend realizado pelos alunos (2024)

Após realizar o login na Tele Connect Solutions, o usuário será direcionado para a página principal da área logada. Nesta página, você encontrará:

- **Menu de Navegação:**
 - **Home:** Retorna à página principal.
 - **Cadastrar:** Redireciona para a página de cadastro.
 - **Listar:** Exibe a lista de contatos ou atividades.
 - **Logout:** Encerra a sessão do usuário.

- **Saudação:** No canto superior direito, uma mensagem personalizada dá as boas-vindas ao usuário, por exemplo, "Bem-vindo, Julio".
- **Banner Informativo:** Logo abaixo do menu, há um banner com fundo azul escuro, contendo o logotipo da empresa e uma mensagem promocional, destacando informações sobre a Tele Connect Solutions.
- **Botão de Mais Informações:** No banner, há também um botão "READ MORE" que, ao ser clicado, leva o usuário a uma página com mais detalhes sobre a empresa.

Figura 36– Tela de cadastro de clientes

PUC MINAS - Sistema de informação

Bem vindo, Julio.

TELE CONNECT

Nome*

Endereço*

Tipo de cliente*

PESSOA FÍSICA

Nº telefone celular

Nº telefone fixo

Cliente ativo

Submit

A tela de cadastro de clientes do sistema "TELE CONNECT" é organizada e funcional, e possui os seguintes itens a seguir:

Cabeçalho: No topo, à esquerda, encontra-se o logotipo do sistema "TELE CONNECT", enquanto à direita há um menu de navegação com as opções: "Home", "Cadastrar", "Listar" e "Logout".

Formulário de Cadastro: Contém os seguintes campos para inserção de dados do cliente:

- Nome* (campo de texto)
- Endereço* (campo de texto)
- Tipo de cliente* (menu suspenso)
- Nº telefone celular (campo de texto)
- Nº telefone fixo (campo de texto)

Status do Cliente: Uma caixa de seleção para indicar se o cliente está ativo.

Botão de Envio: Um botão verde com a etiqueta "Submit" para enviar o formulário.

Fonte: Backend realizado pelos alunos (2024)

Figura 37– Tela de clientes cadastrados

PUC MINAS - Sistema de Informação Bem vindo, Julio.

TELE CONNECT
SOLUTIONS

Home Cadastrar Listar Logout

Cientes Cadastrados:

Nome	Endereço	Tipo	Celular	Fixo	Status	Ação
Julio dos Reis Firmino	Travessa Igara	1	21986354789	21965231456	True	Editar Deletar
Jeziel Suzana Pires da Silva	Rua Sinimbu	1	31986325647	21987456321	True	Editar Deletar
Eric Henrique Marques dos Santos	Rua Belo horizonte	1	21986321479	31965478563	True	Editar Deletar
Eduardo Henrique Morais Costa	Rua João saldanha	1	21954236541	31896547231	True	Editar Deletar
Sophia Thais Gibim Coelho	Rua Roma	1	42965432145	31874562349	True	Editar Deletar
Víctor Hugo Carvalho de Almeida	Rua campo alegre	1	21965478955	21354789654	True	Editar Deletar
Vivo connect	Rua Faria Lima	2	31963245213	31345789642	True	Editar Deletar
star games	Rua botafogo	2	2193564786	41985632469	True	Editar Deletar

A página de clientes cadastrados da nossa plataforma é uma interface intuitiva e funcional que permite a visualização e gestão eficiente dos dados dos clientes. A tabela apresenta informações essenciais, como nome, endereço, tipo de cliente, contatos telefônicos, status e ações disponíveis (editar e deletar). Além disso, a página possui um menu de navegação com opções para cadastrar novos clientes, listar os cadastrados e realizar logout, além de uma saudação personalizada ao usuário logado. Essa organização facilita o acesso rápido e claro às informações, otimizando a administração e o atendimento ao cliente.

Fonte: Backend realizado pelos alunos (2024)

Figura 38– Tela de edição de dados de um cliente

PUC MINAS - Sistema de Informação Bem vindo, Julio.

Home Cadastrar Listar Logout

Nome*

Eric Henrique Marques dos Santos

Endereço*

Rua Belo horizonte

Tipo de cliente*

PESSOA FÍSICA

Nº telefone celular

21986321479

Nº telefone fixo

31965478563

Cliente ativo

Submit

A interface permite a edição de informações de um cliente, incluindo campos para nome, endereço, tipo de cliente, número de telefone celular e número de telefone fixo. Há também uma opção para marcar o cliente como ativo. A tela possui botões de navegação no topo, incluindo "Home", "Cadastrar", "Listar" e "Logout". A interface é simples e funcional, facilitando a atualização dos dados do cliente de maneira eficiente.

Fonte: Backend realizado pelos alunos (2024)

Figura 39–Tela de exclusão de dados de cliente

The screenshot shows a web page with a dark header bar. On the left, it says "PUC MINAS - Sistema de Informação" and on the right, it says "Bem vindo, Julio.". Below the header is the logo for "TELE CONNECT SOLUTIONS", which features a circular emblem with a globe and connectivity symbols, followed by the company name in bold capital letters. To the right of the logo is a navigation menu with links: "Home", "Cadastrar", "Listar", and "Logout". The main content area has a dark background. At the top, there is a question: "Deseja deletar este usuário?". Below this is a yellow rectangular button with the word "Delete" in black text. The lower half of the page is divided into two columns. The left column contains a placeholder image for a user profile picture and some placeholder text: "Morbi vel arcu gravida, iaculis lacus vel, posuere ipsum. Sed faucibus mauris vitae urna consectetur, sit amet maximus nisl sagittis. Ut in iaculis enim, et pulvinar mauris. Etiam tristique magna eget velit". The right column is divided into two sections: "RECENT POSTS" and "QUICK LINKS". The "RECENT POSTS" section lists three items with placeholder text and dates: "Aliquam ac eleifend metus March 10, 2018", "Donec in libero sit amet mi vulputate March 10, 2018", and "Aliquam ac eleifend metus March 10, 2018". The "QUICK LINKS" section lists several links: Home, About us, Services, Testimonials, News, Contact, Faq, Terms & Conditions, Careers, Newsletter & Exchange, and Exchange.

A página de exclusão de dados de cliente tem uma interface simples e direta. No topo, você encontrará o logotipo da "Tele Connect Solutions" e um menu de navegação com opções como "Home", "Cadastrar", "Listar" e "Logout". Há também uma mensagem de boas-vindas personalizada.

No centro da página, há uma pergunta destacada: "Deseja deletar este usuário?" acompanhada de um botão amarelo "Delete". Na parte inferior, há uma área com duas colunas: a esquerda exibe o logotipo e um texto de preenchimento, enquanto a direita contém as seções "Recent Posts" e "Quick Links" para navegação rápida.

Fonte: Backend realizado pelos alunos (2024)

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
(TELE CONNECT SOLUTIONS)



TELE CONNECT
—
SOLUTIONS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Código: PSI-TM-2024

Versão: 1.0

Classificação: Interna

Última revisão: 29/11/2024

1. Introdução

Esta Política de Segurança da Informação (PSI) estabelece diretrizes estratégicas para proteger os ativos tangíveis e intangíveis relacionados ao projeto de telemarketing. A segurança da informação é essencial para a confidencialidade, integridade e disponibilidade dos dados dos clientes, colaboradores e sistemas.

Ademais, a PSI tem como objetivo assegurar que todas as operações da empresa sejam conduzidas de maneira segura, mitigando riscos e prevenindo incidentes de segurança que possam comprometer a informação. A implementação desta política é fundamental para manter a confiança de nossos clientes e parceiros, além de garantir a conformidade com regulamentações e leis aplicáveis ao setor de telemarketing.

A nossa empresa compromete-se a criar um ambiente de trabalho seguro e a promover a cultura de segurança da informação entre seus colaboradores, fornecendo treinamento adequado e recursos necessários para identificar e tratar ameaças de segurança. Todos os colaboradores, parceiros e terceiros que tenham acesso às informações da empresa são responsáveis por proteger os dados de acordo com esta política e procedimentos relacionados.

2. Objetivos

Proteger as informações: Garantir a confidencialidade, integridade e disponibilidade dos dados.

- **Confidencialidade:** Assegurar que informações sensíveis e privadas sejam acessíveis apenas por pessoas autorizadas.
- **Integridade:** Garantir que os dados permaneçam precisos, completos e consistentes durante todo o seu ciclo de vida.
- **Disponibilidade:** Certificar que as informações estejam disponíveis para uso por pessoas autorizadas quando necessário.

Estabelecer diretrizes: Orientar a equipe sobre o uso correto dos recursos tecnológicos e informações sensíveis.

- **Políticas de Uso:** Definir regras claras para o uso de sistemas, redes, e dispositivos da empresa.

- Procedimentos de Segurança: Implementar procedimentos para proteger os recursos tecnológicos contra ameaças.

Prevenir riscos: Minimizar vulnerabilidades e proteger contra ameaças internas e externas.

- Identificação de Vulnerabilidades: Realizar auditorias e avaliações de risco periódicas para identificar e mitigar possíveis vulnerabilidades.
- Mecanismos de Proteção: Utilizar tecnologias avançadas de segurança, como firewalls, antivírus e sistemas de detecção de intrusões.

Promover a cultura de segurança: Construir uma cultura de uso seguro das informações, formando indivíduos mais preparados para agir com responsabilidade e segurança na sociedade digital.

- Treinamento e Conscientização: Oferecer programas de treinamento regulares para todos os colaboradores sobre práticas seguras de uso da informação.
- Boas Práticas: Incentivar comportamentos que promovam a segurança da informação no dia a dia dos colaboradores.

Garantir a conformidade: Assegurar que a empresa e seus colaboradores estejam em conformidade com todas as leis, regulamentos e normas de segurança da informação aplicáveis.

- Normas e Regulamentos: Cumprir todas as leis e regulamentações locais e internacionais referentes à proteção de dados e privacidade.
- Políticas Internas: Desenvolver e manter políticas internas que reflitam essas exigências legais e regulatórias.

Melhorar continuamente: Implementar uma abordagem de melhoria contínua nos processos de segurança da informação, revisando e atualizando regularmente as políticas e procedimentos.

- Revisões Periódicas: Realizar revisões regulares das políticas de segurança para identificar áreas de melhoria.
- Feedback: Coletar feedback dos colaboradores e outras partes interessadas para ajustar e melhorar as práticas de segurança.

Capacitar os colaboradores: Fornecer treinamentos e recursos adequados para que todos os colaboradores possam desempenhar suas funções de maneira segura e eficaz, protegendo os ativos da empresa.

- Desenvolvimento de Competências: Oferecer cursos e workshops para desenvolver as habilidades dos colaboradores em segurança da informação.
 - Recursos de Apoio: Disponibilizar ferramentas e recursos que auxiliem os colaboradores a protegerem as informações de forma eficiente.
-

3. Abrangência

Esta política se aplica a todos os colaboradores, prestadores de serviços e parceiros que utilizem recursos de Tecnologia da Informação e Comunicação (TIC) e dados relacionados ao projeto.

Todos os indivíduos mencionados são obrigados a cumprir as diretrizes e procedimentos estabelecidos nesta Política de Segurança da Informação (PSI). Isso inclui, mas não se limita a, a utilização de sistemas, redes, dispositivos e qualquer outro recurso tecnológico fornecido ou autorizado pela empresa. A abrangência se estende também aos dados corporativos, sejam eles armazenados, processados ou transmitidos.

Ao aderirem à política, todos os envolvidos assumem a responsabilidade de proteger as informações confidenciais e sensíveis da empresa, bem como a infraestrutura de TIC, contra acessos não autorizados, violações de dados e outros riscos de segurança.

4. Diretrizes Gerais

4.1 Propriedades e Segurança das Informações

Todas as informações geradas e manipuladas são de propriedade exclusiva da empresa.

É terminantemente proibido que os colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis, e circulem em ambientes externos à empresa com esses arquivos, sem prévia autorização do gerente imediato. Isso é necessário porque tais arquivos contêm informações que são consideradas confidenciais e/ou sensíveis.

4.1.1 - Informação Sensível e Confidencial:

- Armazenamento: Informações de caráter sensível ou confidencial da empresa ou de clientes serão armazenadas em servidores com total segurança, hospedados na Amazon. Estes servidores são mantidos com as mais rigorosas medidas de segurança para garantir a proteção dos dados.
- Descarte Digital: O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, utilizando técnicas como a sobreSCRIÇÃO segura e a criptografia de eliminação.
- Descarte Físico: O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação. A forma recomendada é a destruição total, por meio de trituradores de papel ou rasgando até perder a identificação.

4.1.2 - Utilização de Recursos Tecnológicos:

- Uso Exclusivo: Os recursos tecnológicos fornecidos pela empresa devem ser utilizados exclusivamente para fins relacionados ao projeto de telemarketing. É proibido o uso desses recursos para atividades pessoais ou que não estejam diretamente relacionadas aos objetivos profissionais da empresa.
- Monitoramento: A empresa se reserva o direito de monitorar o uso dos recursos tecnológicos para garantir a conformidade com esta política e identificar possíveis abusos ou violações.

4.1.3 - Autorizações Necessárias:

- **Cópias e Impressões:** Qualquer cópia ou impressão de arquivos utilizados, gerados ou disponíveis deve ser previamente autorizada pelo gerente imediato. Esta medida visa controlar a disseminação de informações sensíveis e garantir que apenas indivíduos autorizados tenham acesso a elas.
- **Transporte de Informações:** O transporte de informações fora dos ambientes da empresa deve ser feito somente com autorização e sob condições específicas que garantam a segurança dos dados, como o uso de criptografia e dispositivos de armazenamento seguro.

4.2 Classificação das Informações

Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que a informação for gerada, garantindo a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

4.2.1.1 - Informação Pública:

- **Descrição:** Informação que pode ou deve ser tornada disponível para distribuição pública.
- **Impacto:** Sua divulgação não causa qualquer dano à empresa ou aos stakeholders.
- **Exemplos:** Informações de contato, comunicados de imprensa, e conteúdo publicitário.

4.2.1.2 - Informação Interna:

- **Descrição:** Informação que pode ser divulgada para os colaboradores da empresa enquanto estiverem desempenhando suas funções.
- **Impacto:** Sua divulgação não autorizada ou acesso indevido podem causar impactos operacionais ou administrativos.
- **Exemplos:** Políticas internas, manuais de operação, e cronogramas de atividades.

4.2.1.3 - Informação Confidencial:

- **Descrição:** Informação exclusiva a quem se destina, que requer tratamento especial.
- **Impacto:** Contém dados pessoais e/ou sigilosos que, se divulgados, podem afetar a reputação e a imagem da empresa ou causar impactos graves, sob os aspectos financeiro, legal e normativo.
- **Exemplos:** Dados pessoais de clientes, relatórios financeiros, e estratégias de marketing.

4.2.2 - Rotulagem da Informação: Quando se tratar de informações não públicas, estas devem ser rotuladas no momento em que forem geradas, armazenadas ou disponibilizadas.

4.2.2.1 - Mídias Removíveis ou Papel: Para informações geradas e/ou armazenadas em mídias removíveis ou em papel, utilizar carimbo, etiqueta ou texto padronizado para identificação do nível de classificação da informação: interna ou confidencial.

4.2.2.2 - Ambientes Lógicos: Para informações geradas ou mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, tais como

documentos de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados, e Plano Diretor de Segurança, Políticas de Uso.

4.2.3 - Respeito à Classificação da Informação: Todos os colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusearem ou com que vierem a tomar contato.

4.2.3.1 - Tratamento de Informações em Caso de Dúvida: Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à empresa, incluindo a internet e mídias sociais, sem prévia e expressa autorização da equipe responsável pela segurança da informação.

4.2.4 - Sigilo Profissional e Contratual: Todo colaborador deve respeitar o sigilo profissional e contratual. Portanto, não podem revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros colaboradores, clientes, fornecedores, prestadores de serviços ou demais detalhes críticos da empresa.

4.2.5 - Sigilo por Parte dos Clientes: Os clientes também devem respeitar o sigilo das informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros clientes e colaboradores da empresa.

4.3 Controle de Acesso

4.3.1 - Cada colaborador deve utilizar uma identidade digital única (login e senha). O acesso aos sistemas será concedido apenas mediante autorização do gestor.

4.3.1.2 - A identidade digital de cada colaborador deve ser mantida em sigilo e não deve ser compartilhada com terceiros. É necessário que as senhas sejam complexas, contendo uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais, e que sejam atualizadas periodicamente.

4.3.2 - A política de controle de acesso também requer que os sistemas registrem todas as tentativas de acesso, bem-sucedidas ou não, para auditoria e monitoramento. Qualquer tentativa de acesso não autorizado deve ser imediatamente reportada ao departamento de segurança da informação.

4.3.3 - Os acessos devem ser revisados regularmente para garantir que apenas colaboradores autorizados mantenham acesso aos sistemas necessários para suas funções. Em caso de desligamento ou mudança de função, o acesso deve ser revogado ou ajustado prontamente.

4.4 Armazenamento de Dados

4.4.1 - Todos os dados devem ser armazenados em servidores seguros com backups diários. É proibido armazenar dados corporativos em dispositivos pessoais sem autorização prévia.

4.4.1.2 - Os backups diários devem ser regularmente testados para assegurar que os dados possam ser recuperados em caso de falha ou perda. Também é importante definir um período de retenção para os backups, garantindo que dados críticos estejam disponíveis por um período suficiente para recuperação.

4.4.2 - Os servidores utilizados para armazenamento devem estar devidamente protegidos contra acesso não autorizado, utilizando firewalls e outros mecanismos de segurança. A empresa deve implementar políticas de criptografia para garantir que os dados sejam armazenados de forma segura e que a integridade dos dados seja mantida.

4.4.3 - Todos os dados armazenados devem estar em conformidade com as regulamentações e leis aplicáveis à privacidade e proteção de dados, como a Lei Geral de Proteção de Dados (LGPD). A responsabilidade pelo gerenciamento seguro do armazenamento de dados recai sobre o departamento de TI, que deve monitorar constantemente a eficácia das medidas de segurança implementadas.

4.5 Uso de Recursos Tecnológicos

4.5.1 - O uso da internet e dos dispositivos fornecidos deve ser exclusivamente para fins profissionais. É vedada a instalação de softwares não autorizados.

4.5.1.2 - Adicionalmente, todos os colaboradores devem assegurar que os dispositivos tecnológicos sejam utilizados de maneira responsável e em conformidade com as políticas de segurança da empresa. O download e o uso de aplicativos ou extensões de navegador não autorizados são estritamente proibidos, a menos que tenham sido previamente aprovados pelo departamento de TI.

4.5.2 - Os colaboradores são instruídos a relatar qualquer atividade suspeita ou tentativa de instalação de software não autorizado imediatamente ao departamento de TI. É importante manter os dispositivos atualizados com as últimas versões de software e patches de segurança para prevenir vulnerabilidades.

4.5.3 - A empresa se compromete a fornecer recursos tecnológicos necessários para o desempenho das atividades profissionais de maneira eficiente e segura, promovendo um ambiente de trabalho que priorize a proteção das informações e a integridade dos sistemas.

4.6 Mesa e Tela Limpa

4.6.1 - Documentos e informações sensíveis não devem ficar expostos em áreas comuns. Ao se afastar do posto de trabalho, é obrigatório bloquear a tela do computador.

4.6.1.2 - Todos os documentos físicos devem ser guardados em local seguro, como gavetas trancadas ou armários, ao final do expediente ou quando não estiverem em uso. É imperativo que os colaboradores façam uma varredura de suas mesas para garantir que nenhum material sensível seja deixado à vista.

4.6.2 - Quanto às telas, a política de tela limpa deve ser rigorosamente seguida. Isso inclui não só bloquear a tela do computador ao se afastar, mas também garantir que senhas e outros dados de login não sejam escritos em papéis ou armazenados de forma insegura. Sempre que possível, utilize protetores de tela com bloqueio automático após um período de inatividade.

4.6.3 - Manter as estações de trabalho organizadas e seguras contribui significativamente para a proteção das informações da empresa, prevenindo o acesso não autorizado e minimizando riscos de vazamentos de dados.

4.7 Monitoramento e Auditoria

4.7.1 - Monitoramento das Atividades: Todas as atividades nos sistemas são monitoradas para garantir conformidade com esta política. Este monitoramento inclui, mas não se limita a, registros de login/logout, acesso a dados sensíveis, e uso de recursos tecnológicos da empresa. Ferramentas de monitoramento automatizadas são utilizadas para detectar atividades suspeitas ou não conformes em tempo real.

4.7.2 - Auditorias Periódicas: Os usuários são periodicamente auditados com o intuito de mantê-los sempre de acordo com esta política de segurança. As auditorias incluem revisões de acesso, inspeções de conformidade de procedimentos e verificações de segurança de dados. Um termo de conformidade é assinado pelo colaborador, e em caso de descumprimento das normas, o mesmo recebe uma advertência disciplinar.

4.7.3 - Gestão de Não Conformidades: Os colaboradores que não estiverem cumprindo as medidas de segurança podem receber uma advertência disciplinar, formalizada através de um e-mail e/ou impressa. Além disso, medidas corretivas são implementadas para prevenir futuras ocorrências. Isso pode incluir treinamento adicional, atualização de procedimentos e, em casos graves, ações legais.

4.7.4 - Relatórios de Monitoramento: Relatórios detalhados de monitoramento e auditoria são gerados regularmente e analisados pela equipe de segurança da informação. Esses relatórios ajudam a identificar tendências, avaliar a eficácia das políticas de segurança e implementar melhorias contínuas.

4.7.5 - Responsabilidades dos Colaboradores: Todos os colaboradores são responsáveis por:

- Cumprir com as políticas de segurança da informação estabelecidas.
- Participar de treinamentos e auditorias quando solicitados.
- Relatar imediatamente qualquer atividade suspeita ou incidente de segurança à equipe de segurança da informação.

4.7.6 - Revisão e Atualização da Política: A política de monitoramento e auditoria é revisada e atualizada periodicamente para garantir que esteja alinhada com as melhores práticas e com as necessidades da empresa. A revisão inclui a análise de novas ameaças, mudanças no ambiente regulatório e feedback dos colaboradores.

4.8 Comunicação

Informações sensíveis só devem ser compartilhadas mediante autorização e com destinatários autorizados.

4.9 Mídias Sociais e Aplicativos de Comunicação

4.9.1 - Divulgação de Informações: É proibido divulgar informações confidenciais do projeto em mídias sociais. Qualquer compartilhamento de conteúdo relacionado à empresa deve ser previamente autorizado e revisado pela gerência de segurança da informação.

4.9.2 - Uso de Aplicativos de Comunicação: O uso de aplicativos para comunicação corporativa deve respeitar as diretrizes de segurança estabelecidas pela empresa. Isso inclui a utilização de canais oficiais e aplicativos que ofereçam criptografia e outras medidas de proteção.

4.9.3 - Autenticação e Acesso: Todos os aplicativos de comunicação devem requerer autenticação de dois fatores para acesso, garantindo que apenas pessoal autorizado possa utilizar esses canais.

5. Papéis e Responsabilidades

5.1 - Todos os Colaboradores

5.1.2 - Conhecimento e Cumprimento: Conhecer e cumprir a Política de Segurança da Informação (PSI).

5.1.3 - Proteção de Recursos: Zelar pela proteção dos recursos tecnológicos e das informações manipuladas.

5.1.4 - Relato de Incidentes: Relatar imediatamente qualquer incidente de segurança ao gestor imediato.

5.1.5 - Boas Práticas de Segurança: Adotar boas práticas de segurança em suas atividades diárias, incluindo o uso de senhas fortes e a proteção contra phishing.

5.1.6 - Participação em Treinamentos: Participar regularmente de treinamentos de segurança da informação oferecidos pela empresa.

5.2 - Gestores

5.2.1 - Assegurar Conformidade: Assegurar que suas equipes compreendam e sigam as diretrizes da PSI.

5.2.2 - Monitoramento e Auditoria: Monitorar e auditar os acessos e usos dos recursos tecnológicos de sua equipe.

5.2.3 - Sensibilização e Educação: Promover a conscientização e a educação contínua sobre segurança da informação entre os membros da equipe.

5.2.4 - Gerenciamento de Incidentes: Supervisionar e coordenar a resposta a incidentes de segurança reportados pela equipe.

5.3 - Equipe de Tecnologia da Informação

5.3.1 - Proteção de Sistemas: Garantir a proteção dos sistemas e realizar backups regulares dos dados.

5.3.2 - Implementação de Segurança: Implementar e atualizar mecanismos de segurança nos sistemas e redes da empresa.

5.3.3 - Monitoramento de Segurança: Realizar o monitoramento contínuo dos sistemas para identificar e mitigar possíveis ameaças de segurança.

5.3.4 - Suporte Técnico: Fornecer suporte técnico e orientação sobre segurança da informação para todos os colaboradores.

5.3.5 - Gerenciamento de Vulnerabilidades: Identificar e corrigir vulnerabilidades nos sistemas de informação da empresa.

5.3.6 - Documentação e Relatórios: Manter documentação precisa das políticas de segurança e fornecer relatórios regulares à alta administração sobre o status da segurança da informação.

6. Disposições Finais

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com outras normas e procedimentos aplicáveis pela SMC e mantidas.

Quaisquer atitudes ou ações indevidas, ilícitas, não autorizadas ou contrárias ao recomendado por esta Política ou pelas demais normas e procedimentos de segurança da informação da SMC serão consideradas violações por si só e estarão sujeitas às sanções previstas no Regimento Geral, contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição.

7. Documento de Referência

- Política de segurança da informação PUC Minas -
<http://www.pucminas.br/si/Paginas/default.aspx>
-  Política de Segurança da Informação (PSI).pdf

REFERÊNCIAS GERAIS

CORDEIRO, Fábio Leandro Rodrigues. **Estudo comparativo entre plataforma monoprocessada e cluster computing sobre as métricas de desempenho.** 2010. 46f. Monografia (Conclusão de curso) — Pontifícia Universidade Católica de Minas Gerais, Guanhães.

ENGENHARIA DE SISTEMAS DE CONHECIMENTO. (ESC) Eletrocad módulo altimetria. **Versão 1.** [S.l.]: Engenharia de Sistemas de Conhecimento, 2013.

GÓES, L. F. W. et al. Computação em grade: Conceitos, tecnologias, aplicações e tendências. In: L. F. W. GÓES. **Escola Regional de Informática de Minas Gerais.** Belo Horizonte: ERI MG, 2005. cap. 11, p. 40.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS. **Padrão PUC Minas de Normalização:** normas da ABNT para apresentação de teses, dissertações, monografias e trabalhos acadêmicos. 9. ed. rev. ampl. atual. Belo Horizonte: PUC Minas, 2012. Disponível em: <<http://www.pucminas.br/biblioteca/>>. Acesso em: 6 de set. 2013.

https://www.canva.com/design/DAGYXy_5aDA/xFgSERn2VFQonPgvV2p-Bw/edit?utm_content=DAGYXy_5aDA&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton