



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS E INFORMÁTICA
Sistemas de Informação

Everton de Souza Kenedy

Gabriel Barboza Costa

Luís Gustavo da Silva Andrade

Roberto Santos de Almeida

Sara Caroline Vidal de Souza

PROJETO INFRAESTRUTURA DE REDES

Belo Horizonte

2024

PROJETO CAMPUS DE UMA FACULDADE NA REGIÃO METROPOLITANA

Trabalho apresentado como requisito parcial à
aprovação na disciplina Projeto: Infraestrutura
de Redes de Computadores.

Professor: Alexandre Teixeira

1.	TEMA	7
2.	APRESENTAÇÃO E ANÁLISE DE REQUISITOS	9
2.1.	A instituição e seu grupo de usuários	9
2.2.	Estrutura e tecnologias a serem utilizadas	9
2.3.	Escopo	10
2.4.	Requisitos do negócio	11
2.4.1.	Prioridades e objetivo do negócio	11
2.5.	Restrições ao projeto	11
2.5.1.	Restrição Orçamentária e de pessoal	11
2.5.2.	Cronograma de atividades	11
2.5.3.	Políticas e Normas.....	12
2.6.	Requisitos técnicos.....	12
2.6.1.	Os principais requisitos técnicos.....	12
2.6.2.	Fatores de desempenho comum demonstrados em 4.5.....	13
2.6.3.	Considerações Finais.....	13
2.7.	Localização Geográfica.....	14
3.	RESPONSABILIDADES	14
4.	PLANEJAMENTO DOS RECURSOS DE REDES	15
4.1.	Cenário	15
4.1.1.	Matriz	15
4.1.2.	Filial 1	15
4.1.3.	Filial 2	15
4.2.	Divisão Física da rede	16
4.3.	Planilha de Materiais	16
4.4.	Divisão lógica da rede	17
4.5.	Planilha de links	20
5.	IMPLEMENTAÇÃO DOS RECURSOS DE REDES.....	20
5.1.	Implementação Servidor Físico da Matriz	20
5.1.1.	Instalação e Configuração.....	21
5.1.2.	Políticas de Grupo Aplicadas.....	25
5.2.	Implementação de um servidor na nuvem para a matriz/filial	26
5.2.1.	Criação de uma rede VPC.....	26
5.2.2.	Criação de um grupo de segurança	28
5.2.3.	Servidor Web	28
5.2.4.	Acesso via RDP	30

6.	Gerenciamento dos serviços no ZABBIX	32
6.1.	Gerenciamento do servidor físico no ZABBIX	33
6.2.	Gerenciamento do servidor na nuvem no ZABBIX.....	33
6.3.	Visualização e monitoramento dos servidores no ZABBIX	35
7.	Aplicação back-end	39
8.	Referencias.....	69
9.	Anexo 1 – Política de segurança da informação (PSI).....	51
1.	INTRODUÇÃO	51
2.	OBJETIVO.....	51
3.	ABRANGÊNCIA.....	52
4.	DIRETRIZES GERAIS.....	53
4.1.	INTERPRETAÇÃO	53
4.1.1.	TERMINOLOGIA E DEFINIÇÕES.....	53
4.1.2.	RESTRIÇÃO DE INTERPRETAÇÃO	53
4.2.	PROPRIEDADE	54
4.2.1.	PROPRIEDADE E DIREITO DE USO EXCLUSIVOS:	54
4.2.2.	RECURSOS DE TIC PARA ATIVIDADES OPERACIONAIS:	54
4.2.3.	USO RESTRITO A ATIVIDADES PROFISSIONAIS:.....	54
4.2.4.	UTILIZAÇÃO DE MARCAS E IDENTIDADE VISUAL:	54
4.2.5.	MENÇÃO À MARCA EM CONTEXTOS PROFISSIONAIS:.....	54
4.2.6.	ATIVIDADES PROFISSIONAIS:	55
4.3.	CLASSIFICAÇÃO DA INFORMAÇÃO.....	55
4.3.1.	RESPEITO A CLASSIFICAÇÃO DA INFORMAÇÃO:	55
4.3.2.	SIGILO PROFISSIONAL E CONTRATUAL:	55
4.3.3.	DADOS PESSOAIS:	55
4.3.4.	MECANISMOS DE CRIPTOGRAFIA:	55
4.4.	CONTROLE PARA ACESSO DE COLABORADORES	56
4.4.1.	IDENTIDADE DIGITAL INDIVIDUAL:	56
4.4.2.	IDENTIFICAÇÃO NAS DEPENDÊNCIAS FÍSICAS:.....	56
4.4.3.	SEGURANÇA FÍSICA DE ÁREAS CRÍTICAS:	57
4.4.4.	PROTEÇÃO DE ATIVOS CRÍTICOS:.....	57
4.5.	INTERNET PARA COLABORADORES.....	57
4.5.1.	PROPÓSITO DA CONECTIVIDADE:	57
4.5.2.	ACESSO INDIVIDUAL E RESPONSABILIDADE:	57
4.6.	CORREIO ELETRÔNICO PARA COLABORADORES.....	58

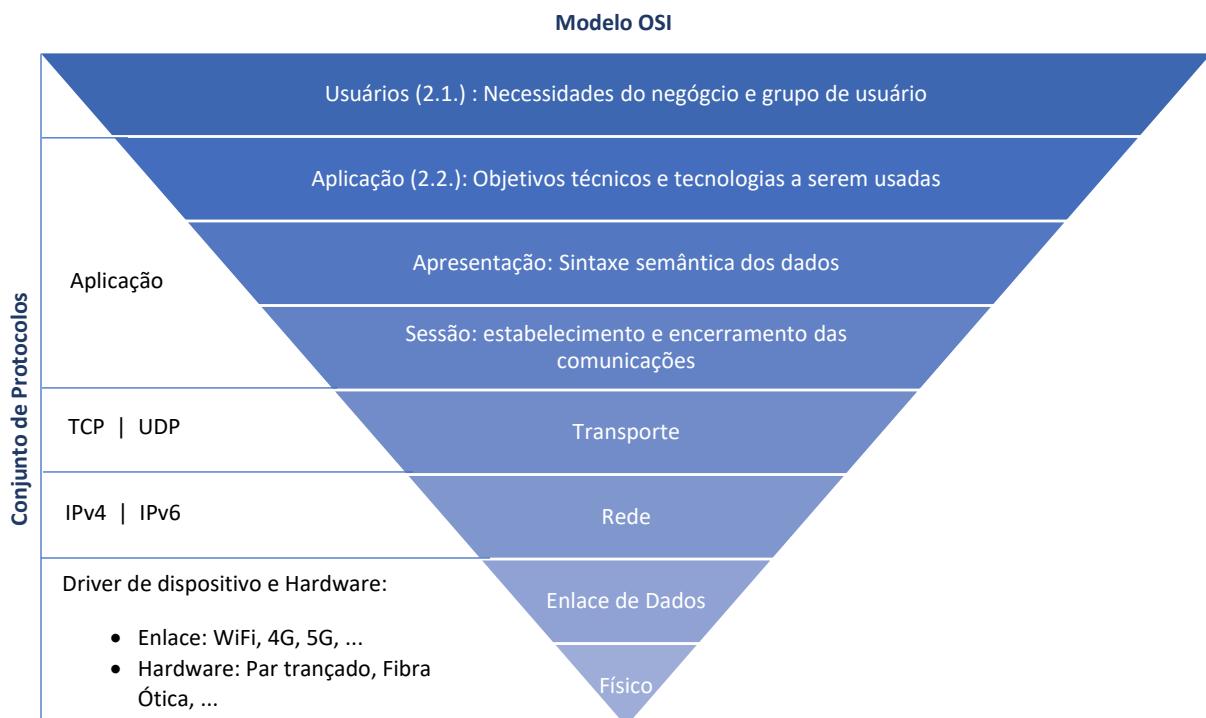
4.6.1. USO PROFISSIONAL:	58
4.6.2. ACESSO EM DISPOSITIVOS MÓVEIS:	58
4.6.3. USO DE CORREIO ELETRÔNICO PARTICULAR:.....	58
4.7. REDE SEM FIO (WI-FI) PARA COLABORADORES	58
4.7.1. USO ADMINISTRATIVO:.....	58
4.7.2. ACESSO AUTORIZADO:	58
4.8. ARMAZENAMENTO DE INFORMAÇÕES PARA COLABORADORES.....	59
4.8.1. LOCAL APROPRIADO PARA ARMAZENAMENTO:	59
4.8.2. ARMAZENAMENTO DIGITAL NOS SERVIDORES CORPORATIVOS:.....	59
4.8.3. SOLICITAÇÃO DE REMOÇÃO DE CONTEÚDOS:.....	59
4.9. Mídias Sociais para Colaboradores	60
4.9.1. Comportamento Seguro nas Mídias Sociais:	60
4.9.2. Participação Institucional Responsável:.....	60
4.10. Conteúdo Audiovisual para Colaboradores	60
4.10.1. Restrições ao Registro e Compartilhamento:	60
4.10.2. Restrições ao Registro por Colaboradores:.....	60
4.10.3. Restrições ao Conteúdo por Colaboradores:	61
4.11. Uso Responsável de Aplicativos de Comunicação para Colaboradores	61
4.11.1. Ambiente de Trabalho:	61
4.12. Monitoramento para Colaboradores.....	61
4.12.1. Registro e Monitoramento:	61
4.12.2. Finalidade do Armazenamento de Dados:.....	61
4.12.3. Colaboração em Casos de Incidentes:	62
4.13. Contratos para Colaboradores.....	62
4.13.1. Acesso e Porte de Dispositivos:	62
4.13.2. Desligamento ou Rescisão:	62
4.14. Segurança da Informação para Colaboradores.....	62
4.14.1. Repasse e Transmissão de Informações:	62
4.14.2. Cautela na Utilização de Recursos Online:.....	63
4.14.3. Salvaguarda e Restauração de Arquivos Digitais:	63
4.14.4. Descarte Seguro de Informações Confidenciais:	63
4.14.5. Proteção em Caso de Desastres:.....	63
4.14.6. Educação Continuada em Segurança da Informação:	63
5. PAPEIS E RESPONSABILIDADES	64

5.1. TODOS- DIRETRIZES PARA COLABORADORES NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	64
5.1.1. CONHECIMENTO E DISSEMINAÇÃO DAS REGRAS:.....	64
5.1.2. PRESERVAÇÃO DE ATIVOS:.....	64
5.1.3. PRESERVAÇÃO DE RECURSOS INSTITUCIONAIS:.....	64
5.1.4. ZELO PELO PATRIMÔNIO:	64
5.1.5. EVITAR EXPOSIÇÃO DESNECESSÁRIA:	64
5.1.6. PREVENÇÃO DE INCIDENTES:.....	65
5.1.7. CUMPRIMENTO E ATUALIZAÇÃO:.....	65
5.1.8. PROTEÇÃO CONTRA ACESSO NÃO AUTORIZADO:	65
5.1.9. COMBATE AO BULLYING:	65
5.1.10. REPORTE DE INCIDENTES:	65
5.2. Gestores e Coordenadores	65
5.2.1. Orientação Constante:	65
5.2.2. RESPONSABILIDADE DELEGADA:.....	66
5.2.3. CUMPRIMENTO DA POLÍTICA	66
5.2.4. INVESTIGAÇÃO DE INCIDENTES:	66
5.2.5. PARTICIPAÇÃO NO COMITÊ DE SEGURANÇA:.....	66
5.3. COLABORADORES	66
5.3.1. PRESERVAÇÃO DA VIDA PARTICULAR:.....	66
5.3.2. COMUNICAÇÃO RESPEITOSA:	66
5.3.3. USO CONSCIENTE DE MÍDIAS SOCIAIS:.....	67
6. DISPOSIÇÕES FINAIS.....	67
7. DIRETRIZES GERAIS - DOCUMENTOS DE REFERÊNCIA:	67
8. APÊNDICE – SIGLAS, TERMOS E DEFINIÇÕES	68

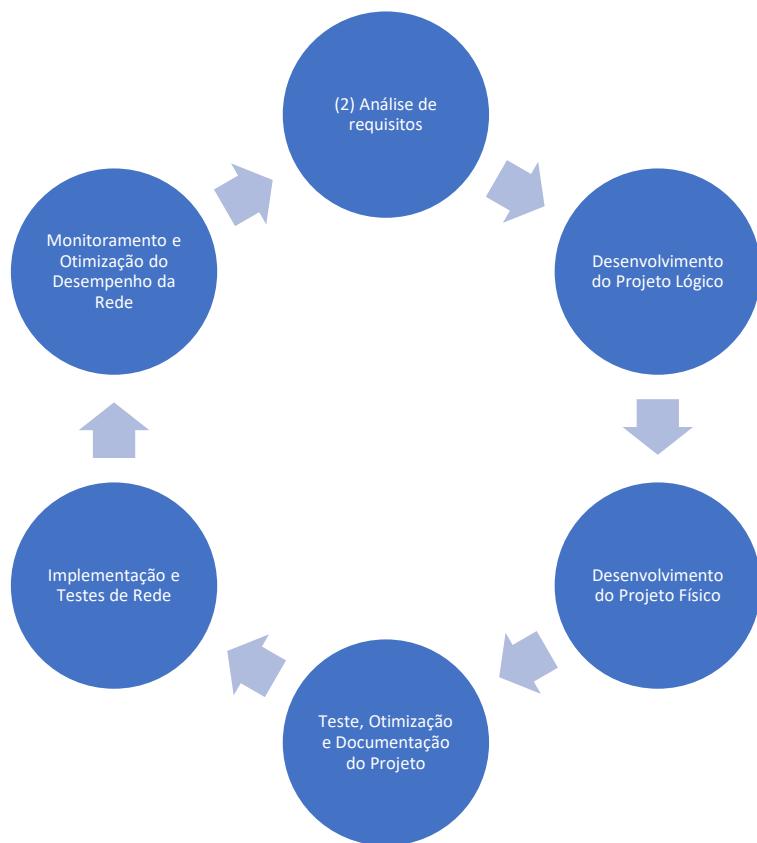
1. TEMA

O grupo optou pela escolha do tema: um novo Campus de uma Faculdade na Região Metropolitana de Belo Horizonte. Para o propósito da simulação, estamos projetando uma rede com comunicação entre três campus (uma Matriz e duas Filiais), sendo os mesmos de mesma capacidade e estrutura.

Etapas Modelo OSI a serem aplicadas no projeto:



Etapas Modelo Top-Down a serem aplicadas no projeto:



2. APRESENTAÇÃO E ANÁLISE DE REQUISITOS

2.1. A INSTITUIÇÃO E SEU GRUPO DE USUÁRIOS

A simulação do novo campus irá se compor dos seguintes fatores (simulação baseada no campus existente: PUC Unidade São Gabriel):

O campus estará localizado na região nordeste de Belo Horizonte, instalada em uma área de 50 mil m². Os **7 prédios** irão abrigar toda a infraestrutura necessária para atender aos quase **2000 estudantes** dos 6 cursos de graduação tecnológica, assim como os diversos cursos de especialização ofertados em distintas áreas do conhecimento.

A biblioteca local disponibilizará um acervo de 43 mil exemplares. A Unidade irá dispor de **3 laboratórios**, entre eles os de áudio, vídeo e fotografia. Também se destacará, na oferta de Engenharia de Software. A Unidade também possuirá um **teatro com capacidade para 320 pessoas**, com foyer amplo, e duas salas multimeios, com estrutura para atender aos eventos institucionais e acadêmicos.

O novo campus está previsto para ser inaugurado contando com um quadro de funcionários de aproximadamente **100 colaboradores**.

Para que o novo campus opere de maneira eficiente e atenda as demandas dos cursos de graduação oferecidos, infraestrutura, funcionários e compartilhamento de dados da instituição, o campus será composto por departamentos e setores diferentes, e sua rede será interconectada com a matriz, filial 1 e 2.

2.2. ESTRUTURA E TECNOLOGIAS A SEREM UTILIZADAS

Área de cobertura:

- **Salas de Aula:** o campus possui um total de 40 salas de aula, todas projetadas para proporcionar um ambiente confortável e propício ao aprendizado. Cada sala está cuidadosamente equipada com instalações modernas e funcionais, visando garantir o máximo conforto para professores e alunos durante as atividades acadêmicas.
- **Prédio administrativo (Coordenação/Reitoria/Sala de professores/Financeiro/Contabilidade):** o campus possui um prédio administrativo que conta com toda a parte administrativa, englobando a coordenação, reitoria, sala dos professores, financeiro, contabilidade entre outros. O prédio é o principal local onde os colaboradores ficam localizados e realizam seus trabalhos.
- **Laboratório com computadores/ Pesquisa:** o campus investe em laboratórios com computadores para suas aulas práticas de programação e cursos de extensão, assim como a área de pesquisa e desenvolvimento para criar softwares e/ou produtos inovadores e eficientes em termos computacionais, sendo eles para saída de Hardware e/ou Software com o intuito de ajudar a comunidade em descobertas importantes para o desenvolvimento local/global.

- **Biblioteca:** o campus conta com uma biblioteca, oferecendo suporte completo para estudantes, pesquisadores e membros da comunidade acadêmica. Com uma ampla gama de serviços, incluindo acesso a livros, periódicos e suporte técnico, a biblioteca é essencial para estudo, pesquisa e desenvolvimento intelectual.
- **Auditório:** O campus conta com um moderno auditório equipado para sediar eventos acadêmicos, palestras, seminários e apresentações. Com capacidade para acomodar muitas pessoas, o auditório oferece um ambiente propício para a troca de conhecimento e interação entre os participantes. Equipado com tecnologia audiovisual de ponta, é o local ideal para eventos que demandam recursos de projeção e som de alta qualidade.
- **Infraestrutura:** O campus se dispõe de uma área de Infra, onde está centralizado o centro de suporte técnico, sejam eles: suporte técnico a hardware ou software dos laboratórios, assim como o centro de suporte à rede da faculdade e seus sistemas integrados.

Quantidade de máquinas: 183 (*3)

- Salas de Aula – 40 máquinas (sendo uma máquina por sala)
- Prédio administrativo: Coordenação/Reitoria/Sala de professores/Financeiro/Contabilidade - 10 máquinas
- Laboratório com computadores/ Pesquisa – 120 máquinas (3 salas x 40 máquinas)
- Biblioteca – 8 máquinas
- Auditório - 1 máquina
- Infraestrutura – 4 máquinas

Serviços:

- Wi-Fi
- Pontos de rede (Ethernet par trançado/ou fibra ótica)
- Firewall/Controle de acesso
- Acesso remoto – Suporte de TI remoto
- Suporte TI
- ERP/CRM
- Acesso ao banco de dados
- Blob Storage
- Servidor na nuvem
- Acesso à web
- Acesso ao sistema interno da instituição (Portal do aluno/professor)
- Correio eletrônico
- Videoconferência

2.3. ESCOPO

Três localidades: 1 MATRIZ E 2 FILIAIS (LAN/WAN)

- Um novo campus, uma filial já existente e a Matriz, totalizando em três campuses;
- Cada Campus irá ser composto por sua própria LAN;
- WAN para interligação entre filiais e Matriz;
- Acesso remoto para serviços de suporte (VPN).

2.4. REQUISITOS DO NEGÓCIO

2.4.1. PRIORIDADES E OBJETIVO DO NEGÓCIO

A infraestrutura de rede proposta se deve a garantir eficiência operacional, qualidade de troca de informações, qualidade de acesso e troca de dados entre sistemas da instituição, qualidade na entrega do serviço oferecido aos seus alunos e gestão de sistemas internos.

Seus principais requisitos são:

- Funcionalidade na comunicação Interna e acesso a base de dados dentro da mesma instituição, sendo elas internamente no campus ou troca de informação entre Matriz/Filiais;
- Mobilidade para trabalho de home-office para funcionários;
- Segurança de Dados;
- Expansão e Escalabilidade;
- Resiliência – tolerância a falhas/determinada eficiência para a empresa;
- Acesso Remoto para suporte;
- Gestão de Manutenção da rede;
- Qualidade de acesso e troca de dados entre sistemas;
- Eficácia de custos;
- Latência necessária para aplicações em tempo real.

2.5. RESTRIÇÕES AO PROJETO

2.5.1. RESTRIÇÃO ORÇAMENTÁRIA E DE PESSOAL

- Hardware
- Software
- Implementação
- Serviços de treinamento de pessoal

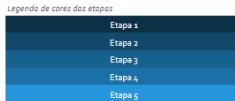
2.5.2. CRONOGRAMA DE ATIVIDADES

O cronograma irá ser adaptado e atualizado por etapa

Cronograma do projeto

Selezione um período para realizar à direita. A seguir há uma legenda que descreve o gráfico.

Reâlce do Período: **1** 



Link para visualizar melhor ([Link](#)).

2.5.3. POLÍTICAS E NORMAS

- Nenhuma restrição em relação aos softwares utilizados até o momento.
- Nenhuma restrição para hardware até o momento
- Análise de custos a ser feita para escolha do melhor cenário em termos de custo/benefício para ambos os softwares/hardwares

2.6. REQUISITOS TÉCNICOS

2.6.1. OS PRINCIPAIS REQUISITOS TÉCNICOS

- Funcionalidade na comunicação Interna e acesso a base de dados dentro da mesma instituição, sendo elas internamente no campus ou troca de informação entre Matriz/Filiais;
- Mobilidade para trabalho de home-office para funcionários;
- Segurança de Dados;
- Expansão e Escalabilidade;
- Resiliência;
- Acesso Remoto;
- Gestão de Manutenção da rede;
- Qualidade de acesso e troca de dados entre sistemas;
- Eficácia de custos;
- Redundância única (provedor único);

<u>Disponibilidade</u>	
MTBF	Tempo Médio Entre Falhas
MTTR	Tempo Médio Para o Reparo de Falhas
Disponibilidade	MTBF / (MTBF + MTTR)

Quadro de Requisitos Técnicos Para Aplicações Cálculo de Disponibilidade							
Nome da Aplicação	Custo da Atividade (kbps)	MTBF Aceitável (hrs)	MTTR Aceitável (hrs)	Meta de Vazão	Atraso deve ser menor que (sgs)	Varição do atraso deve ser menor que (sgs)	Disponibilidade
Portal do aluno e professores	410000	2000		4	2	1	99,80%
ERP/CRM	40000	4000		0,5			99,98%
Sistema de correio: E-mail	350000	2000		8			99,60%
Acesso Remoto	600	8760		0,5			99,98%
Help Desk	200	2000		2			99,90%
www	1290000	2000		0,5			99,98%

Link para visualizar melhor([Link](#)).

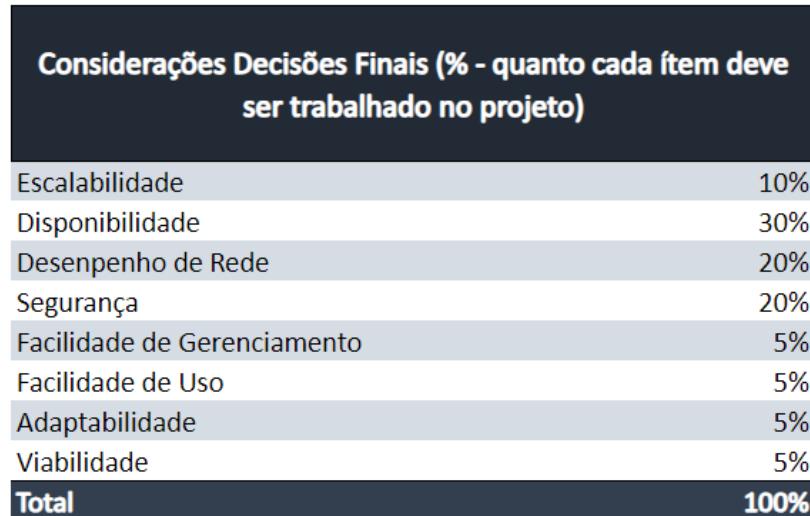
2.6.2. FATORES DE DESEMPENHO COMUM DEMONSTRADOS EM 4.5.

- Capacidade/Largura da Banda
- Vazão
- Precisão
- Eficiência
- Atraso (Latência) e tempo de resposta

Quadro de Requisitos Técnicos Para Aplicações Cálculo de Atraso							
	Numero de usuarios /portas	Taxa (pkt/seg)	Tamanho médio de cada pkt (bits)	linha de transmissão de dados (Kbps)	Carga (bps)	Utilização	N. Médio de pkt/fila (kbps/seg)
Switch	24	20	1024	560	491520	87,8%	7,177570093

Link para visualizar melhor([Link](#)).

2.6.3. CONSIDERAÇÕES FINAIS



2.7. LOCALIZAÇÃO GEOGRÁFICA

Simulação baseada no campus da PUC São Gabriel



Link para visualizar melhor([Link](#)).

3. RESPONSABILIDADES

Os integrantes do grupo se responsabilizam e comprometem-se da seguinte forma:

Nome	Papel	Responsabilidade
Everton	Pesquisa / Comunicação	<ul style="list-style-type: none"> Realizar levantamento de requisitos; Participar dos encontros semanais de acompanhamento e desenvolvimento do projeto; Definir objetivos; Desenvolvimento da documentação e planilhas;
Gabriel	Comunicação	<ul style="list-style-type: none"> Definir objetivos; Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades e contribuindo com ideias e soluções para os desafios enfrentados; Coordenar a planilha de Recursos e Redes.

Luis	Programação	<ul style="list-style-type: none"> • Definir objetivos; • Participar das reuniões periódicas de acompanhamento do projeto, compartilhando atualizações sobre o progresso das atividades e contribuindo com ideias e soluções para os desafios enfrentados; • Coordenar o Protótipo da rede no Simulador da Cisco Packet Tracer.
Roberto	Pesquisa / Coordenação	<ul style="list-style-type: none"> • Coordenar as reuniões semanais de acompanhamento do projeto; • Realizar a distribuição de tarefas entre os membros da equipe. • Acompanhar o andamento das atividades, verificando o progresso em relação ao cronograma e identificando eventuais desvios.
Sara	Liderança/Pesquisa/Implementação	<ul style="list-style-type: none"> • Levantar requisitos; • Definir Objetivos, metas, timeline de entrega; • Acompanhamento do projeto; • Coordenação e construção do protótipo de rede, juntamente com o time; • Documentação.

4. PLANEJAMENTO DOS RECURSOS DE REDES

4.1. CENÁRIO

4.1.1. MATRIZ

- 7 prédios com 40 salas de aula no total
- 3 laboratórios com computadores / pesquisa
- 1 auditório
- 1 biblioteca
- Prédio administrativo: Coordenação/Reitoria/Sala de professores/Financeiro/Contabilidade - 10 máquinas
- Sala de Infraestrutura

4.1.2. FILIAL 1

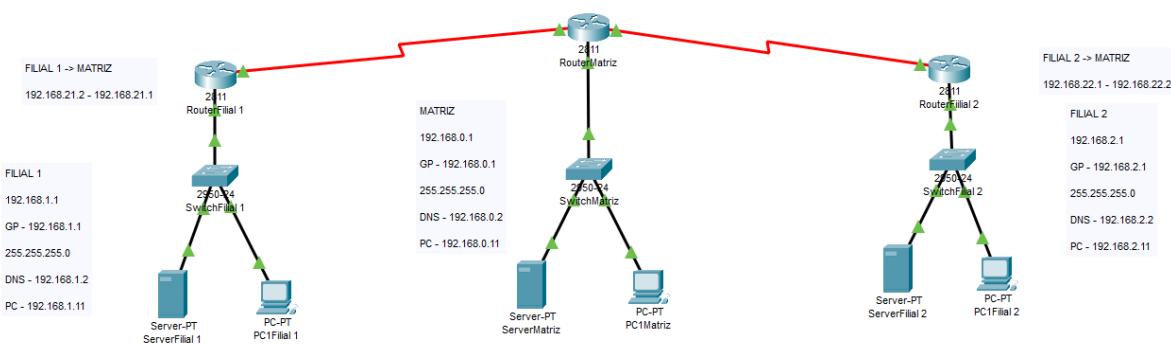
- 7 prédios com 40 salas de aula no total
- 3 laboratórios com computadores / pesquisa
- 1 auditório
- 1 biblioteca
- Prédio administrativo: Coordenação/Reitoria/Sala de professores/Financeiro/Contabilidade - 10 máquinas
- Sala de Infraestrutura

4.1.3. FILIAL 2

- 7 prédios com 40 salas de aula no total
- 3 laboratórios com computadores / pesquisa

- 1 auditório
- 1 biblioteca
- Prédio administrativo: Coordenação/Reitoria/Sala de professores/Financeiro/Contabilidade - 10 máquinas
- Sala de Infraestrutura

4.2. DIVISÃO FÍSICA DA REDE



Link para visualizar melhor a imagem([Link](#)).

4.3. PLANILHA DE MATERIAIS

Tabela de Materiais							
Necessidades Corporativas		Matriz = 2100		Filial 1 = 2100		Filial 2 = 2100	
Item	Valor	Quantidade	Valor	Quantidade	Valor	Quantidade	Valor
Servidor Rack PowerEdge R250	R\$ 9.400,00	1	R\$ 9.400,00	1	R\$ 9.400,00	1	R\$ 9.400,00
Estação Dell (Vostro Small Desktop)	R\$ 2.799,00	183	R\$ 512.217,00	183	R\$ 512.217,00	183	R\$ 512.217,00
Roteador CISCO	R\$ 2.600,00	1	R\$ 2.600,00	14	R\$ 36.400,00	14	R\$ 36.400,00
Serial CISCO	R\$ 1.000,00	2	R\$ 2.000,00	2	R\$ 2.000,00	2	R\$ 2.000,00
Switch CISCO 48 portas	R\$ 4.165,00	3	R\$ 12.495,00	3	R\$ 12.495,00	3	R\$ 12.495,00
Switch CISCO 24 portas	R\$ 2.040,00	1	R\$ 2.040,00	1	R\$ 2.040,00	1	R\$ 2.040,00
Cabo UTP cx 300 mt CAT6	R\$ 3.000,00	16	R\$ 48.000,00	16	R\$ 48.000,00	16	R\$ 48.000,00
RJ45 f CAT6 Furukawa Premium	R\$ 60,00	200	R\$ 12.000,00	8	R\$ 480,00	8	R\$ 480,00
Testador de cabo	R\$ 150,00	5	R\$ 750,00	5	R\$ 750,00	5	R\$ 750,00
Alicate de Crimpar	R\$ 180,00	5	R\$ 900,00	5	R\$ 900,00	5	R\$ 900,00
PunchDown	R\$ 175,00	5	R\$ 875,00	5	R\$ 875,00	5	R\$ 875,00
Patch Cord CAT6 1.5m	R\$ 60,00	200	R\$ 12.000,00	200	R\$ 12.000,00	200	R\$ 12.000,00
Patch Panel CAT6	R\$ 850,00	9	R\$ 7.650,00	8	R\$ 6.800,00	8	R\$ 6.800,00
Rack 44 U	R\$ 3.000,00	1	R\$ 3.000,00	1	R\$ 3.000,00	1	R\$ 3.000,00
Cx + placa (RJ45 Femea)	R\$ 40,00	200	R\$ 8.000,00	200	R\$ 8.000,00	200	R\$ 8.000,00
AP Rukus WiFi 6 r750	R\$ 3.400,00	14	R\$ 47.600,00	14	R\$ 47.600,00	14	R\$ 47.600,00
Organizador de cabos	R\$ 320,00	8	R\$ 2.560,00	8	R\$ 2.560,00	8	R\$ 2.560,00
Impressora	R\$ 2.200,00	2	R\$ 4.400,00	1	R\$ 2.200,00	1	R\$ 2.200,00
Nobreak	R\$ 5.000,00	1	R\$ 5.000,00	1	R\$ 5.000,00	1	R\$ 5.000,00
Mesa+cadeira	R\$ 650,00	183	R\$ 118.950,00	183	R\$ 118.950,00	183	R\$ 118.950,00
	Total		R\$ 812.437,00	Total	R\$ 831.667,00	Total	R\$ 831.667,00
						Total Geral	R\$ 2.475.771,00

Link para visualizar melhor a planilha([Link](#)).

4.4. DIVISÃO LÓGICA DA REDE

A tabela abaixo contém os dispositivos de rede, seus nomes, endereçamento, portas e roteamento.

Dispositivo OS	Nome	Portas/Endereçamento
Roteador	Router Matriz	<pre> Device Name: RouterMatriz Custom Device Model: 2811 IOS15 Hostname: Router Port Link VLAN IP Address IPv6 Address MAC Address FastEthernet0/0 Up -- 192.168.0.1/24 <not set> 0005.5E37.C701 FastEthernet0/1 Down -- <not set> <not set> 0005.5E37.C702 Serial0/0/0 Up -- 192.168.21.1/24 <not set> <not set> Serial0/0/1 Up -- 192.168.22.1/24 <not set> <not set> Serial0/1/0 Down -- <not set> <not set> <not set> Serial0/1/1 Down -- <not set> <not set> <not set> Vlan1 Down 1 <not set> <not set> 0000.0C2E.1C51 Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > RouterMatriz </pre>
Roteador	Router Filial 1	<pre> Device Name: RouterFilial 1 Custom Device Model: 2811 IOS15 Hostname: Router Port Link VLAN IP Address IPv6 Address MAC Address FastEthernet0/0 Up -- 192.168.1.1/24 <not set> 00E0.F975.A49C FastEthernet0/1 Down -- <not set> <not set> 0002.4A0B.6B25 Serial0/0/0 Up -- 192.168.21.2/24 <not set> <not set> Serial0/0/1 Down -- <not set> <not set> <not set> Serial0/1/0 Down -- <not set> <not set> <not set> Serial0/1/1 Down -- <not set> <not set> <not set> Vlan1 Down 1 <not set> <not set> 0004.9A86.AA79 Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > RouterFilial 1 </pre>
Roteador	Router Filial 2	<pre> Device Name: RouterFilial 2 Custom Device Model: 2811 IOS15 Hostname: Router Port Link VLAN IP Address IPv6 Address MAC Address FastEthernet0/0 Up -- 192.168.2.1/24 <not set> 0003.E4BE.E552 FastEthernet0/1 Down -- <not set> <not set> 0001.63A5.675D Serial0/0/0 Down -- <not set> <not set> <not set> Serial0/0/1 Up -- 192.168.22.2/24 <not set> <not set> Serial0/1/0 Down -- <not set> <not set> <not set> Serial0/1/1 Down -- <not set> <not set> <not set> Vlan1 Down 1 <not set> <not set> 0040.0B99.C723 Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > RouterFilial 2 </pre>
Switch	Switch Matriz	

		<pre> Device Name: SwitchMatrixz Device Model: 2950-24 Hostname: Switch Port Link VLAN IP Address MAC Address FastEthernet0/1 Up -- -- 0030.F206.B701 FastEthernet0/2 Up -- -- 0030.F206.B702 FastEthernet0/3 Up -- -- 0030.F206.B703 FastEthernet0/4 Down -- -- 0030.F206.B704 FastEthernet0/5 Down -- -- 0030.F206.B705 FastEthernet0/6 Down -- -- 0030.F206.B706 FastEthernet0/7 Down -- -- 0030.F206.B707 FastEthernet0/8 Down -- -- 0030.F206.B708 FastEthernet0/9 Down -- -- 0030.F206.B709 FastEthernet0/10 Down -- -- 0030.F206.B70A FastEthernet0/11 Down -- -- 0030.F206.B70B FastEthernet0/12 Down -- -- 0030.F206.B70C FastEthernet0/13 Down -- -- 0030.F206.B70D FastEthernet0/14 Down -- -- 0030.F206.B70E FastEthernet0/15 Down -- -- 0030.F206.B70F FastEthernet0/16 Down -- -- 0030.F206.B710 FastEthernet0/17 Down -- -- 0030.F206.B711 FastEthernet0/18 Down -- -- 0030.F206.B712 FastEthernet0/19 Down -- -- 0030.F206.B713 FastEthernet0/20 Down -- -- 0030.F206.B714 FastEthernet0/21 Down -- -- 0030.F206.B715 FastEthernet0/22 Down -- -- 0030.F206.B716 FastEthernet0/23 Down -- -- 0030.F206.B717 FastEthernet0/24 Down -- -- 0030.F206.B718 Vlan1 Down 1 <not set> 0004.9A57.3B4D </pre> <p>Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SwitchMatrixz</p>
Switch	Switch Filial 1	<pre> Device Name: SwitchFilial 1 Device Model: 2950-24 Hostname: Switch Port Link VLAN IP Address MAC Address FastEthernet0/1 Up -- -- 0020.F787.23EB FastEthernet0/2 Up -- -- 0003.E46A.C778 FastEthernet0/3 Up -- -- 0002.1704.A6D3 FastEthernet0/4 Down -- -- 0001.969A.18B2 FastEthernet0/5 Down -- -- 000B.BE3C.8C83 FastEthernet0/6 Down -- -- 0005.5E92.DE3E FastEthernet0/7 Down -- -- 0007.EC11.2393 FastEthernet0/8 Down -- -- 0020.B07D.1072 FastEthernet0/9 Down -- -- 0060.475A.BA82 FastEthernet0/10 Down -- -- 0020.8F2E.A909 FastEthernet0/11 Down -- -- 0002.4ADD.27A7 FastEthernet0/12 Down -- -- 000A.410C.9456 FastEthernet0/13 Down -- -- 0030.F231.8146 FastEthernet0/14 Down -- -- 000D.BD44.2A9A FastEthernet0/15 Down -- -- 0020.F733.2E46 FastEthernet0/16 Down -- -- 0002.17EB.21E0 FastEthernet0/17 Down -- -- 0020.A34C.D42D FastEthernet0/18 Down -- -- 0000.0CA7.6484 FastEthernet0/19 Down -- -- 0001.97BD.BC0D FastEthernet0/20 Down -- -- 0001.971D.6416 FastEthernet0/21 Down -- -- 0006.2A59.005E FastEthernet0/22 Down -- -- 0020.F96C.8AC1 FastEthernet0/23 Down -- -- 0003.E489.8475 FastEthernet0/24 Down -- -- 00D0.BA88.6EAC Vlan1 Down 1 <not set> 0002.17E9.87ED </pre> <p>Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SwitchFilial 1</p>
Switch	Switch Filial 2	

		<pre> Device Name: SwitchFilial 2 Device Model: 2950-24 Hostname: Switch Port Link VLAN IP Address MAC Address FastEthernet0/1 Up -- -- 0007.ECCA.E610 FastEthernet0/2 Up -- -- 0000.BCAA.0AB3 FastEthernet0/3 Up -- -- 0002.17DB.308D FastEthernet0/4 Down -- -- 0060.2F5B.C345 FastEthernet0/5 Down -- -- 0002.17E7.63C7 FastEthernet0/6 Down -- -- 0004.9AAA.7CBA FastEthernet0/7 Down -- -- 00E0.8F0D.4B45 FastEthernet0/8 Down -- -- 000B.BE68.4EBB FastEthernet0/9 Down -- -- 0006.2ACD.0897 FastEthernet0/10 Down -- -- 000A.F338.5BEC FastEthernet0/11 Down -- -- 0007.EC32.E24D FastEthernet0/12 Down -- -- 0030.F243.A81B FastEthernet0/13 Down -- -- 0001.C908.61A5 FastEthernet0/14 Down -- -- 000A.F3B1.71B2 FastEthernet0/15 Down -- -- 0001.97DE.A9A7 FastEthernet0/16 Down -- -- 0001.6450.646E FastEthernet0/17 Down -- -- 0002.4AOE.A858 FastEthernet0/18 Down -- -- 0001.4249.7A17 FastEthernet0/19 Down -- -- 0050.0F9B.E498 FastEthernet0/20 Down -- -- 00E0.F750.A2B8 FastEthernet0/21 Down -- -- 0009.7C6.457A FastEthernet0/22 Down -- -- 0090.2B87.3459 FastEthernet0/23 Down -- -- 0060.5C55.8444 FastEthernet0/24 Down -- -- 0007.ECBE.6047 Vlan1 Down 1 <not set> 0006.2A08.3947 </pre> <p>Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > SwitchFilial 2</p>
Computador	PC1 Matriz	<pre> Device Name: PC1Matriz Device Model: PC-PT Port Link IP Address IPv6 Address MAC Address FastEthernet0 Up 192.168.0.11/24 <not set> 0090.2BE4.A60A Bluetooth Down <not set> <not set> 0090.2102.943A Gateway: 192.168.0.1 DNS Server: 192.168.0.2 Line Number: <not set> </pre> <p>Physical Location: Intercity > Home City > Corporate Office > PC1Matriz</p>
Computador	PC1 Filial1	<pre> Device Name: PC1Filial 1 Device Model: PC-PT Port Link IP Address IPv6 Address MAC Address FastEthernet0 Up 192.168.1.11/24 <not set> 00D0.974C.C45A Bluetooth Down <not set> <not set> 0030.F29E.A17B Gateway: 192.168.1.1 DNS Server: 192.168.1.2 Line Number: <not set> </pre> <p>Physical Location: Intercity > Home City > Corporate Office > PC1Filial 1</p>
Computador	PC1 Filial2	<pre> Device Name: PC1Filial 2 Device Model: PC-PT Port Link IP Address IPv6 Address MAC Address FastEthernet0 Up 192.168.2.11/24 <not set> 0010.1111.0ECD Bluetooth Down <not set> <not set> 000A.F34D.2A52 Gateway: 192.168.2.1 DNS Server: 192.168.2.2 Line Number: <not set> </pre> <p>Physical Location: Intercity > Home City > Corporate Office > PC1Filial 2</p>
Server	Server Matriz	<pre> Device Name: ServerMatriz Device Model: Server-PT Port Link IP Address IPv6 Address MAC Address FastEthernet0 Up 192.168.0.2/24 <not set> 0040.0BD7.50EC Gateway: 192.168.0.1 DNS Server: 192.168.0.2 Line Number: <not set> </pre> <p>Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > ServerMatriz</p>

Server	Server Filial 1	Device Name: ServerFilial 1 Device Model: Server-PT Port Link IP Address IPv6 Address FastEthernet0 Up 192.168.1.2/24 <not set> MAC Address 0002.4AA4.305C Gateway: 192.168.1.1 DNS Server: 192.168.1.2 Line Number: <not set> Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > ServerFilial 1
Server	Server Filial 2	Device Name: ServerFilial 2 Device Model: Server-PT Port Link IP Address IPv6 Address FastEthernet0 Up 192.168.2.2/24 <not set> MAC Address 0060.2F93.B190 Gateway: 192.168.2.1 DNS Server: 192.168.2.2 Line Number: <not set> Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > ServerFilial 2

4.5. PLANILHA DE LINKS

Quadro de Requisitos Técnicos Para Aplicações Cálculo de Links de dados e de Internet								
Necessidades Corporativas			Matriz = 2100		Filial 1 = 2100		Filial 2 = 2100	
Aplicação	Derivação	Requisitos (kbps)	Quantidade (pior caso)	Total (kbps)	Quantidade (pior caso)	Total (kbps)	Quantidade (pior caso)	Total (kbps)
Videoconferência		1600	150	240000	150	240000	150	240000
Web (www)		1500	700	1050000	700	1050000	700	1050000
Sistema de correio: E-mail		500	700	350000	700	350000	700	350000
Suporte	Central de Atendimento	100	2	200	2	200	2	200
	Help Desk	100	2	200	2	200	2	200
SAP	Supporte/Acesso remoto	300	2	600	2	600	2	600
	ERP / CRM	400	100	40000	100	40000	100	40000
Azure/Data center	Sistema de Alunos e Professores	300	500	150000	500	150000	500	150000
	Servidor	100	500	50000	500	50000	500	50000
	Banco de Dados	300	500	150000	500	150000	500	150000
Blob Storage			300	200	60000	200	60000	200
				Total App	2091000	Total App	2091000	Total App
								2091000
				Total Internet	4830000	Total Internet	1610000	Total Internet
				Link Internet	6273000	Link Matrix <-> Filial 1	2091000	Link Matrix <-> Filial 2
								2091000

Link para visualizar melhor a planilha([Link](#)).

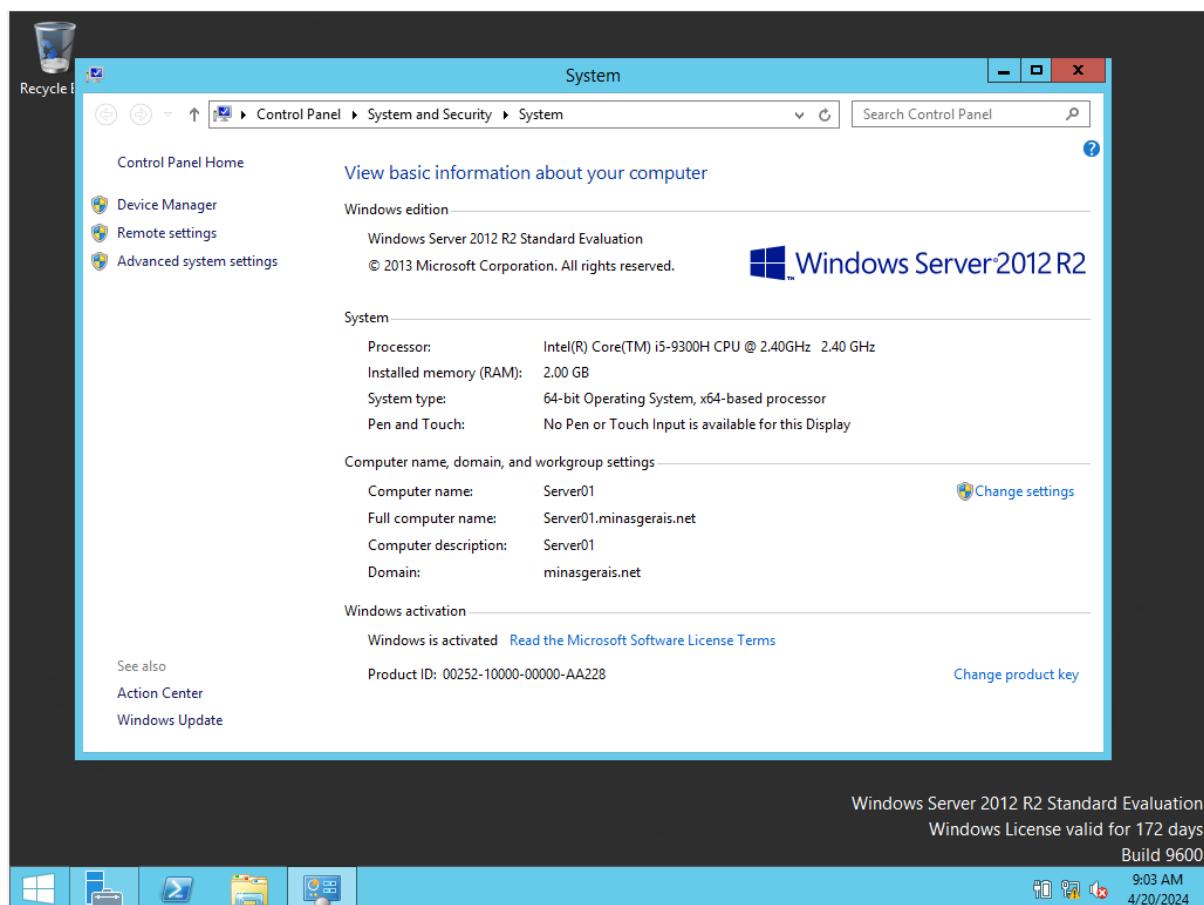
5. IMPLEMENTAÇÃO DOS RECURSOS DE REDES

5.1. IMPLEMENTAÇÃO SERVIDOR FÍSICO DA MATRIZ

Implementamos um servidor local utilizando o Oracle VM VirtualBox, o qual foi configurado para incorporar os recursos conforme ilustrado na imagem abaixo:

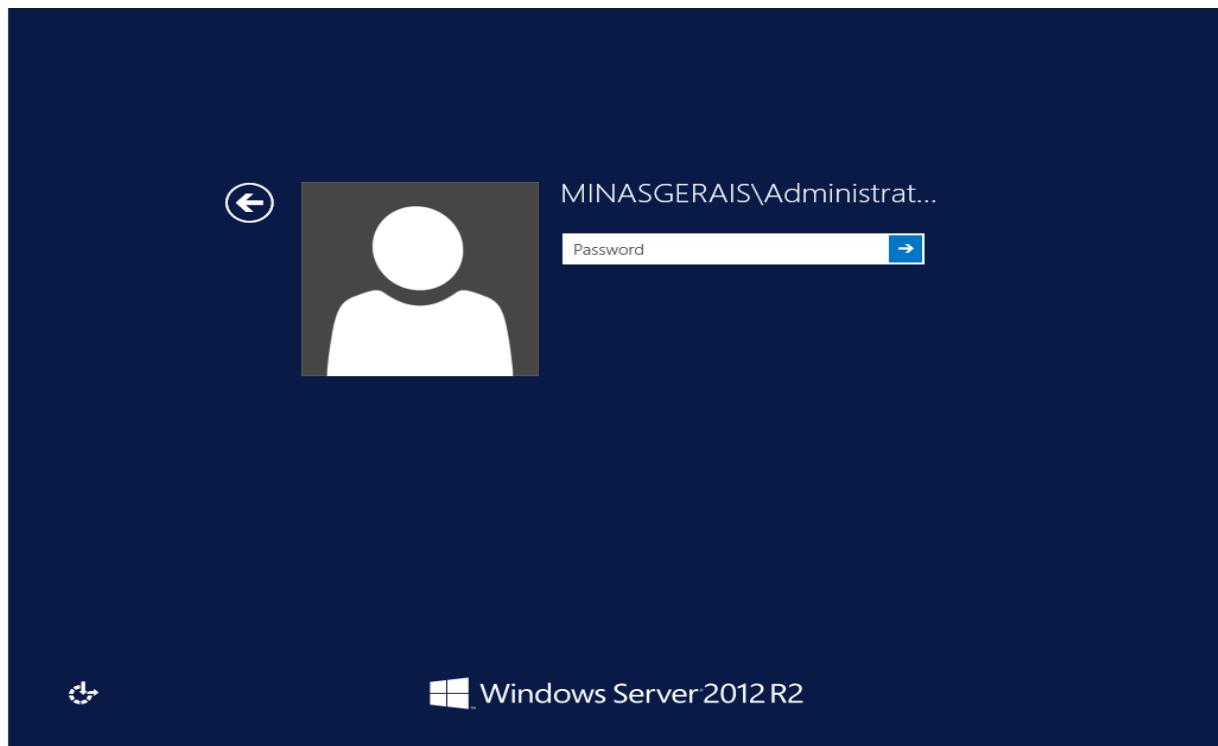


Link para visualizar melhor a imagem([link](#)).

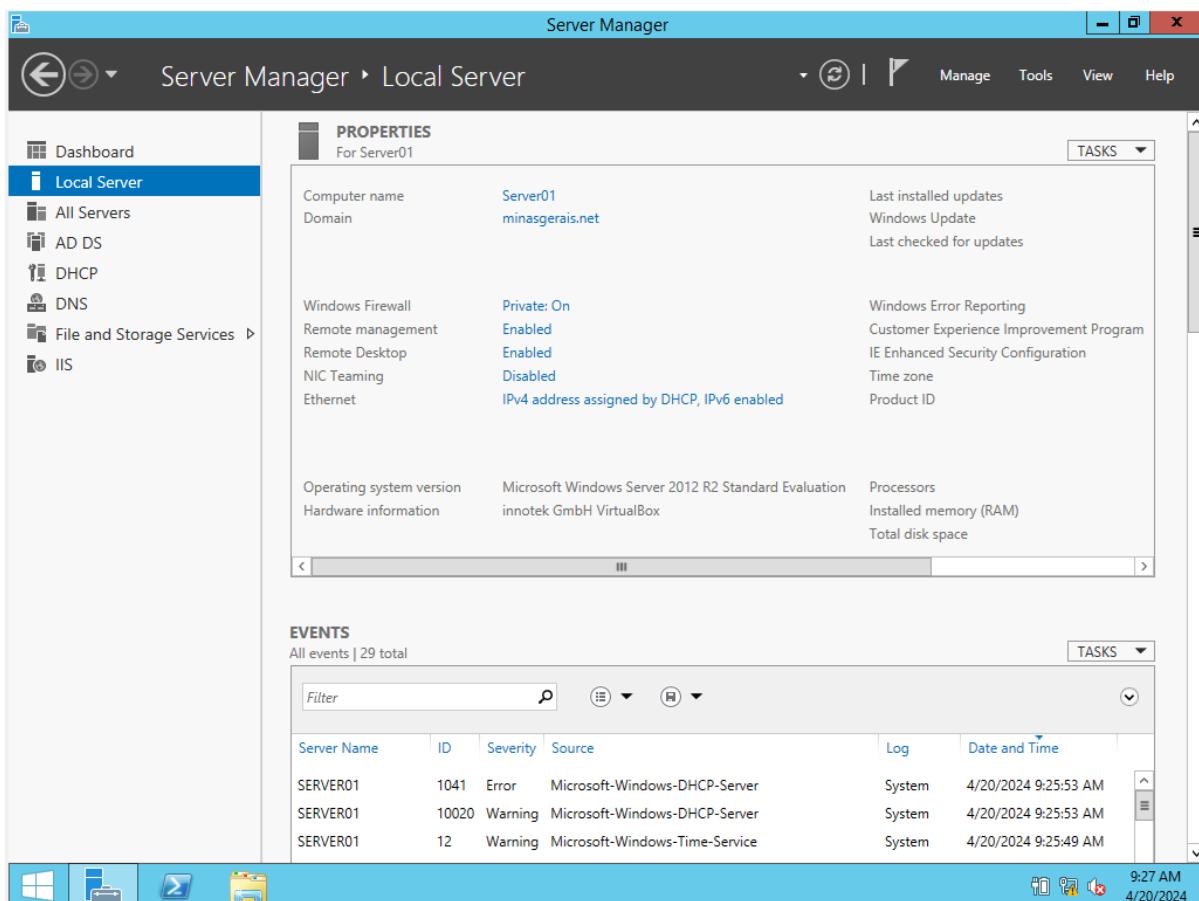


5.1.1. INSTALAÇÃO E CONFIGURAÇÃO

Após a implementação atribuímos a esse servidor funções DNS (Domain Name Server) E AD DS (Active Directory Domain Services), e transformamos em DC (Domain Controller). Adicionamos a função DHCP (Dynamic Host Configuration Protocol) ao servidor para atribuição automática de IPs.



Tela inicial



The image shows the Server Manager interface for a local server named "Server01".

Properties for Server01:

Computer name	Server01	Last installed updates
Domain	minasgerais.net	Windows Update
		Last checked for updates
Windows Firewall	Private: On	Windows Error Reporting
Remote management	Enabled	Customer Experience Improvement Program
Remote Desktop	Enabled	IE Enhanced Security Configuration
NIC Teaming	Disabled	Time zone
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID
Operating system version	Microsoft Windows Server 2012 R2 Standard Evaluation	Processors
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)
		Total disk space

Events:
All events | 29 total

Server Name	ID	Severity	Source	Log	Date and Time
SERVER01	1041	Error	Microsoft-Windows-DHCP-Server	System	4/20/2024 9:25:53 AM
SERVER01	10020	Warning	Microsoft-Windows-DHCP-Server	System	4/20/2024 9:25:53 AM
SERVER01	12	Warning	Microsoft-Windows-Time-Service	System	4/20/2024 9:25:49 AM

Informações do servidor

Belo Horizonte
2024

Server Manager

Server Manager › Dashboard

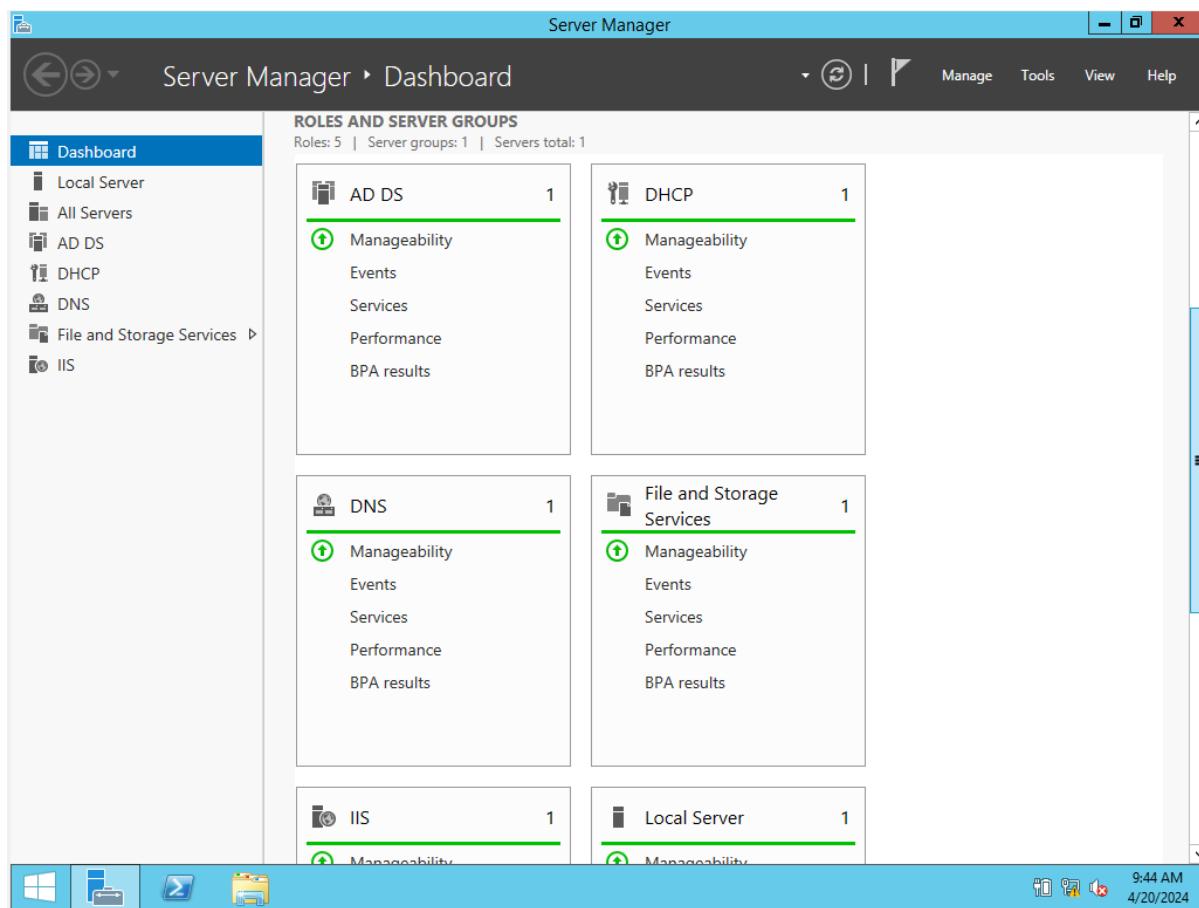
ROLES AND SERVER GROUPS

Roles: 5 | Server groups: 1 | Servers total: 1

AD DS 1	DHCP 1
Manageability Events Services Performance BPA results	Manageability Events Services Performance BPA results
DNS 1	File and Storage Services 1
Manageability Events Services Performance BPA results	Manageability Events Services Performance BPA results
IIS 1	Local Server 1
Manageability	Manageability

9:44 AM
4/20/2024

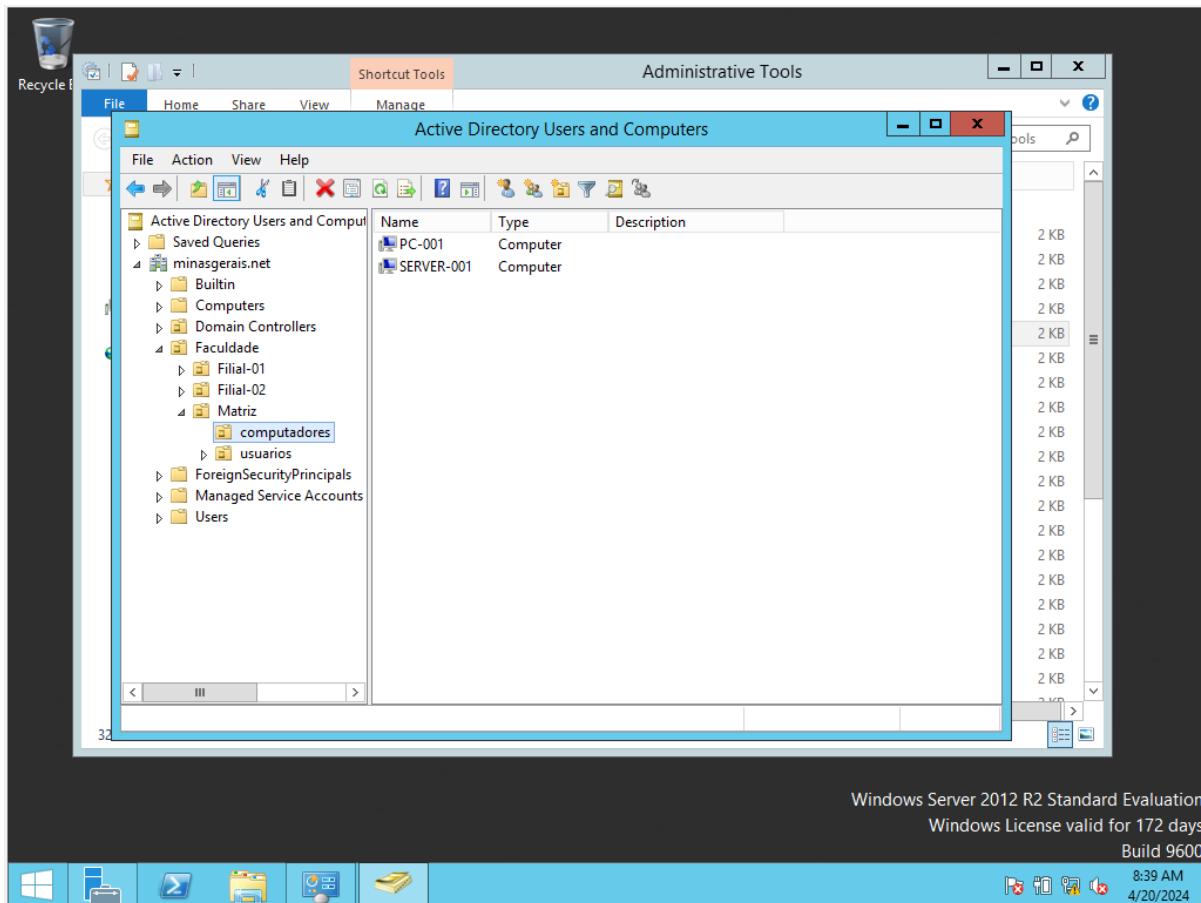
Dashboard do servidor



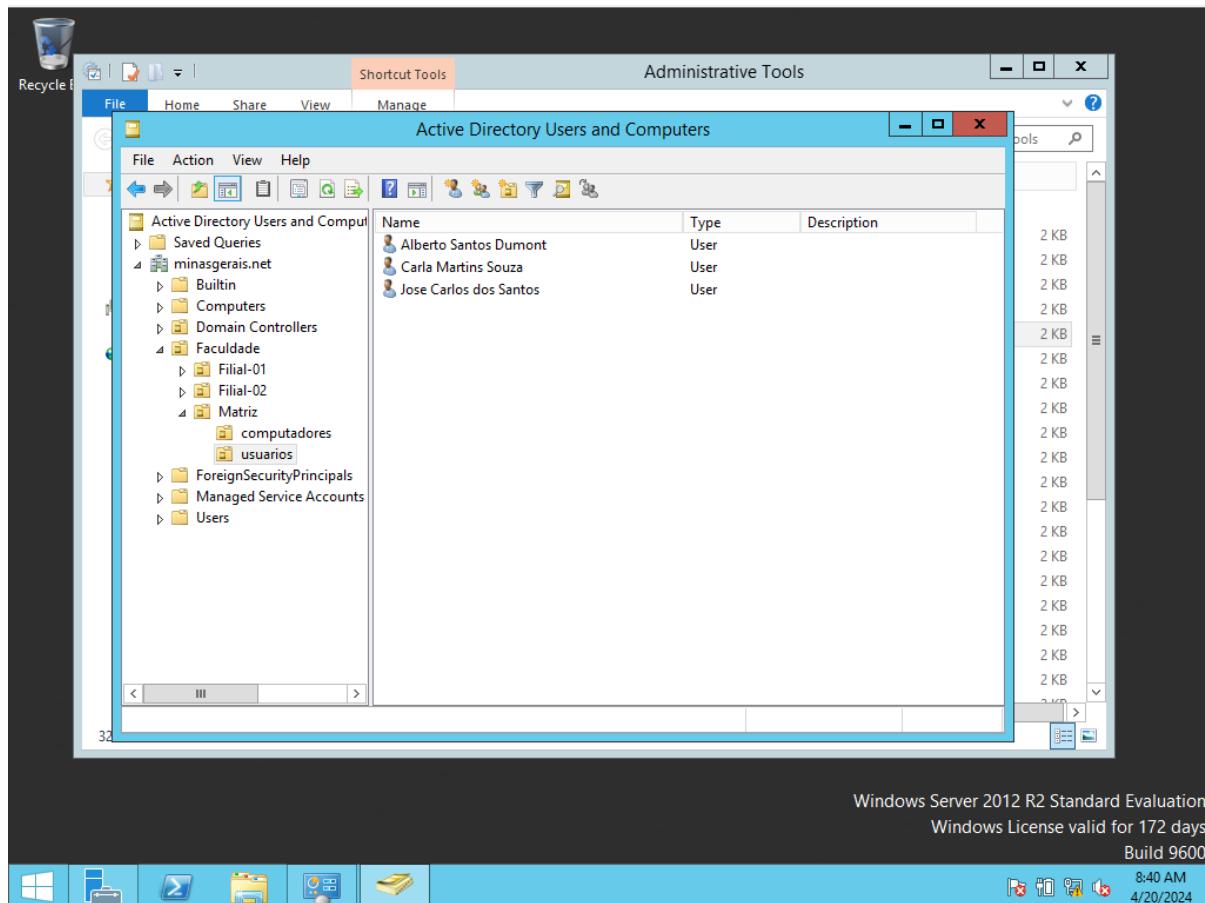
Ativamos o recurso Active Directory e procedemos à sua configuração para o domínio minasgerais.net. Dentro deste domínio, foram criadas as seguintes estruturas organizacionais:

- Matriz
- Filial 01
- Filial 02

Cada uma dessas estruturas possui usuários e computadores apropriados designados, incluindo servidores e estações de trabalho.



Computadores da Matriz.

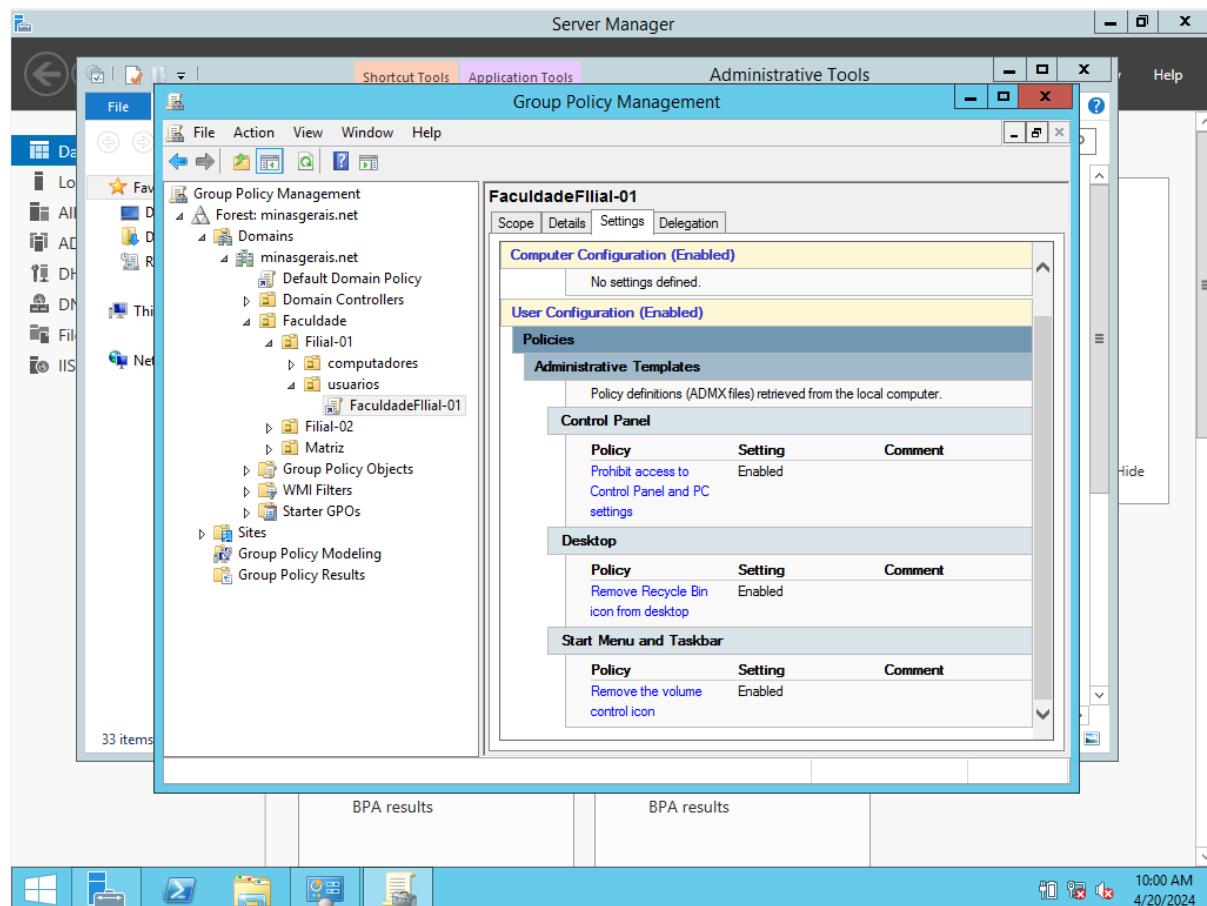


Usuários ativos da Matriz.

Nas demais estruturas, foi adotada a mesma abordagem de alocação de recursos computacionais, visto que os campos e requisitos são similares à estrutura da matriz. Foram adicionados os usuários pertinentes a cada unidade, garantindo assim a consistência e integridade das informações em todo o ambiente de rede.

5.1.2. POLÍTICAS DE GRUPO APLICADAS

Criamos uma política de grupo na Filial-01 nomeada FaculdadeFilial-01 removendo o ícone de controle de volume, removendo o ícone de lixeira do desktop e proibindo o acesso ao Painel de Controle e configurações do PC.



Controle das políticas de grupo.

5.2. IMPLEMENTAÇÃO DE UM SERVIDOR NA NUVEM PARA A MATRIZ/FILIAL

Através dos serviços da AWS realizamos a implementação do servidor na nuvem, abaixo enumeramos os processos realizados.

5.2.1. CRIAÇÃO DE UMA REDE VPC

Para isso criamos uma G11Faculdade-vpc com 2 subredes públicas e 2 subredes privadas em duas zonas de disponibilidade distintas, com a criação conseguiremos alocar um servidor dentro da rede vpc-faculdade.

Serviços Search [Alt+S]

VPC > Suas VPCs > vpc-0943730929d369b9c / G11Faculdade-vpc

Detalhes Informações

ID da VPC	vpc-0943730929d369b9c	Estado	Available	Nomes de host DNS	
Locação	Default	Conjunto de opções de DHCP	dhcp.0b1e0b509966100fd	Habilitado	Resolução de DNS
VPC padrão		CIDR IPv4	10.0.0.0/16	Tabula de rota principal	Habilitado
Não		CIDR IPv6	-	rtb-086610e9df8b6597	Network ACL principal
Métricas de uso do endereço de rede		Grupos de regras do Firewall de DNS do roteador do Route 53	-	ad-00b5ca87b0252e615	CIDR IPv6 (Grupo de borda de rede)
Desabilitado		Falha em carregar grupos de regras	-	-	-

Ações ▾

Mapa de recursos | CDRs | Logs de fluxos | Tags | Integrações

Mapa de recursos Informações



© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

Link para visualizar melhor a imagem([link](#)).

Serviços Search [Alt+S]

VPC > Suas VPCs > Sub-redes

Sub-redes (4/10) Informações

Name	ID da sub-rede	Estado	VPC	CIDR IPv4	CIDR IPv6	Endereços IPv4 disponíveis	Zona de disp
G11Faculdade-subnet-private1-us-east-1a	subnet-0f8b30d417fe54d	Available	vpc-0943730929d369b9c G11...	10.0.2.0/24	-	251	us-east-1a
-	subnet-08bf919df5cd8a0	Available	vpc-0ee566e06f0497bd	172.31.64.0/20	-	4091	us-east-1f
-	subnet-0b5281748900b9	Available	vpc-0ee3566e06f0497bd	172.31.80.0/20	-	4091	us-east-1a
G11Faculdade-subnet-private2-us-east-1b	subnet-057a9191676413539	Available	vpc-0943730929d369b9c G11...	10.0.3.0/24	-	251	us-east-1b
G11Faculdade-subnet-public1-us-east-1a	subnet-0b057885705c22844	Available	vpc-0943730929d369b9c G11...	10.0.0.0/24	-	250	us-east-1a
G11Faculdade-subnet-public2-us-east-1b	subnet-02ba31da7376dkff79	Available	vpc-0943730929d369b9c G11...	10.0.1.0/24	-	251	us-east-1b
-	subnet-024555950c2246cae	Available	vpc-0ee566e06f0497bd	172.31.16.0/20	-	4091	us-east-1b
-	subnet-04b3f0196981f8f399	Available	vpc-0ee3566e06f0497bd	172.31.32.0/20	-	4091	us-east-1c
-	subnet-09c9badc3f9f1930	Available	vpc-0ee3566e06f0497bd	172.31.0.0/20	-	4091	us-east-1d
-	subnet-0f9806be887bd92	Available	vpc-0ee3566e06f0497bd	172.31.48.0/20	-	4091	us-east-1e

Ações ▾

[Criar sub-rede](#)

Link para visualizar melhor a imagem([link](#)).

Serviços Search [Alt+S]

VPC > Suas VPCs > Tabelas de rotas

Tabelas de rotas (5) Informações

Name	ID da tabela de rotas	Associações explícitas....	Associações de ...	Princí... ▾	VPC	ID do proprietário
-	rtb-086610e9df8b6597	Z. sub-rede	-	Sim	vpc-0943730929d369b9c G11...	35661199108
G11Faculdade-rtb-public	rtb-0eb11172ca586aa0	Z. sub-rede	-	Não	vpc-0943730929d369b9c G11...	35661199108
G11Faculdade-rtb-private2-us-east-1b	rtb-04852c4722b5809	Z. sub-rede	-	Não	vpc-0943730929d369b9c G11...	35661199108
G11Faculdade-rtb-private1-us-east-1a	rtb-079a1454-d7113092	Z. sub-rede	-	Não	vpc-0943730929d369b9c G11...	35661199108
-	rtb-05474698506ed9d	-	-	Sim	vpc-0ee3566e06f0497bd	35661199108

Ações ▾

[Criar tabela de rotas](#)

Selecionar uma tabela de rotas

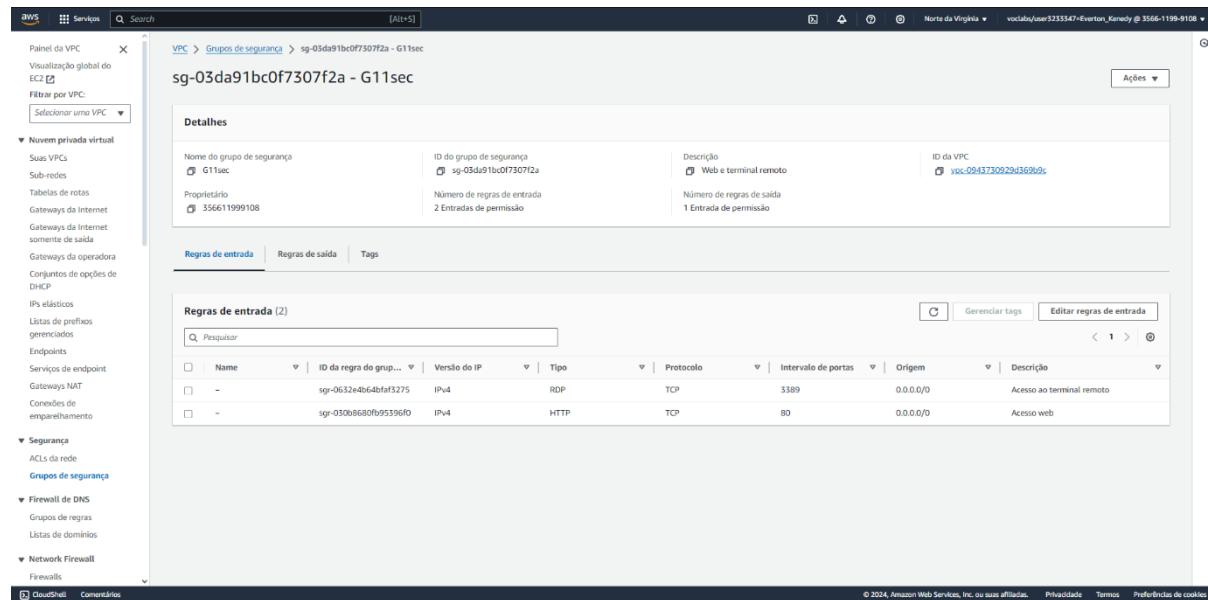
© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

Link para visualizar melhor a imagem([link](#)).

5.2.2. CRIAÇÃO DE UM GRUPO DE SEGURANÇA

O grupo de segurança funciona como um firewall para as instâncias, controlando tráfego de entrada e saída. Criamos o grupo de segurança G11sec possuindo duas regras de entrada: o HTTP e o acesso remoto (RDP).

- HTTP: permite acesso via web;
- RDP: permite acesso via terminal remoto;



The screenshot shows the AWS VPC Groups of security interface. The security group 'G11sec' is selected. The 'Detalhes' section shows the group's name, ID, owner, and various metrics. The 'Regras de entrada' tab is active, displaying two rules:

Name	ID da regra do grupo	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
-	sgr-0632e4bf64bfaf5275	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso ao terminal remoto
-	sgr-030b8680fb95396f0	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso web

Link para visualizar melhor a imagem([link](#)).

5.2.3. SERVIDOR WEB

Para o servidor web utilizamos uma instância EC2 da Amazon, seguimos as etapas abaixo:

- O nome escolhido foi G11webserver;
- Para a imagem de máquina da Amazon escolhemos o Windows Server 2016 Base e o tipo de instância foi o t2.large;
- Criamos um par de chaves para poder acessar o servidor depois com o nome de G11key do tipo RSA e com extensão .pem;
- Na configuração de rede, o servidor vai fazer parte da G11Faculdade-vpc criada anteriormente e da subrede G11-subnet-public1;
- Habilitamos a opção de atribuir IP público automaticamente;
- Em Firewall selecionamos o grupo de segurança existente G11sec;
- Na configuração de armazenamento selecionamos o gp3 por ser mais rápido;
- Em seguida executamos a instância.

Imagen de máquina da Amazon (AMI)

Microsoft Windows Server 2016 Base ami-0fce5929bccdd6390 (64 bits (x86)) Virtualização: hvm ENA habilitado: true Tipo de dispositivo raiz: ebs	Qualificado para o nível gratuito
--	-----------------------------------

Descrição

Microsoft Windows Server 2016 with Desktop Experience Locale English AMI provided by Amazon

Arquitetura

ID da AMI

64 bits (x86)

ami-0fce5929bccdd6390

Provedor verificado

▼ Tipo de instância [Informações](#) | [Obter conselhos](#)

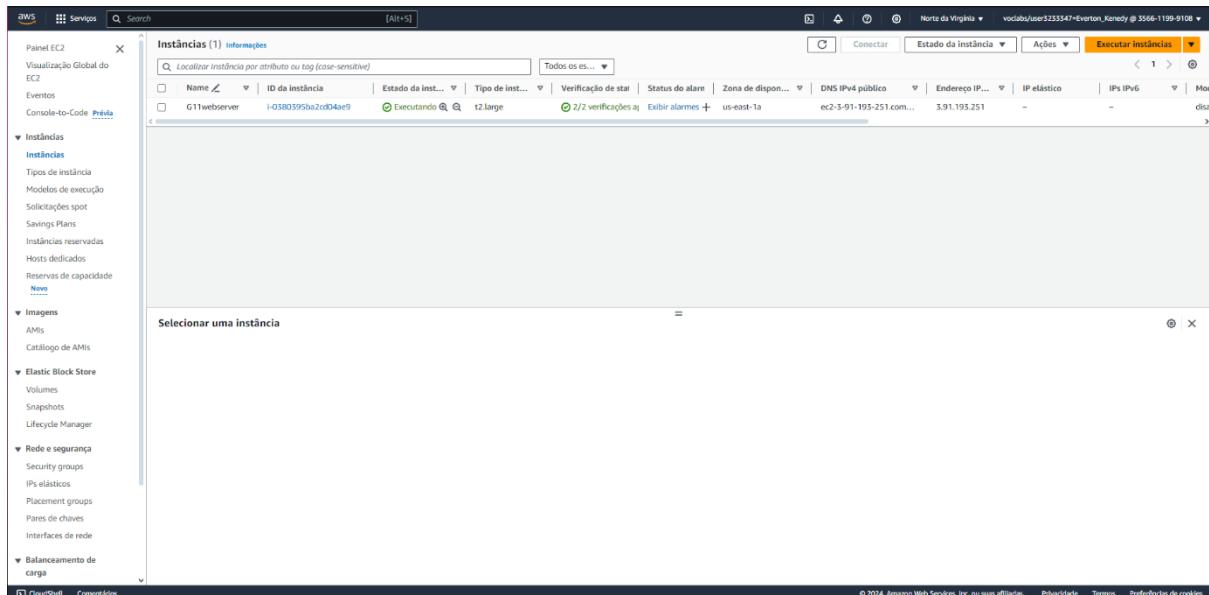
Tipo de instância

t2.large
 Família: t2 2 vCPU 8 GiB Memória Geração atual: true
 Sob demanda Windows base definição de preço: 0.1208 USD por hora
 Sob demanda RHEL base definição de preço: 0.1528 USD por hora
 Sob demanda SUSE base definição de preço: 0.1928 USD por hora
 Sob demanda Linux base definição de preço: 0.0928 USD por hora

Todas as gerações

[Comparar tipos de instância](#)

[Custos adicionais aplicáveis a AMIs com software pré-instalado](#)

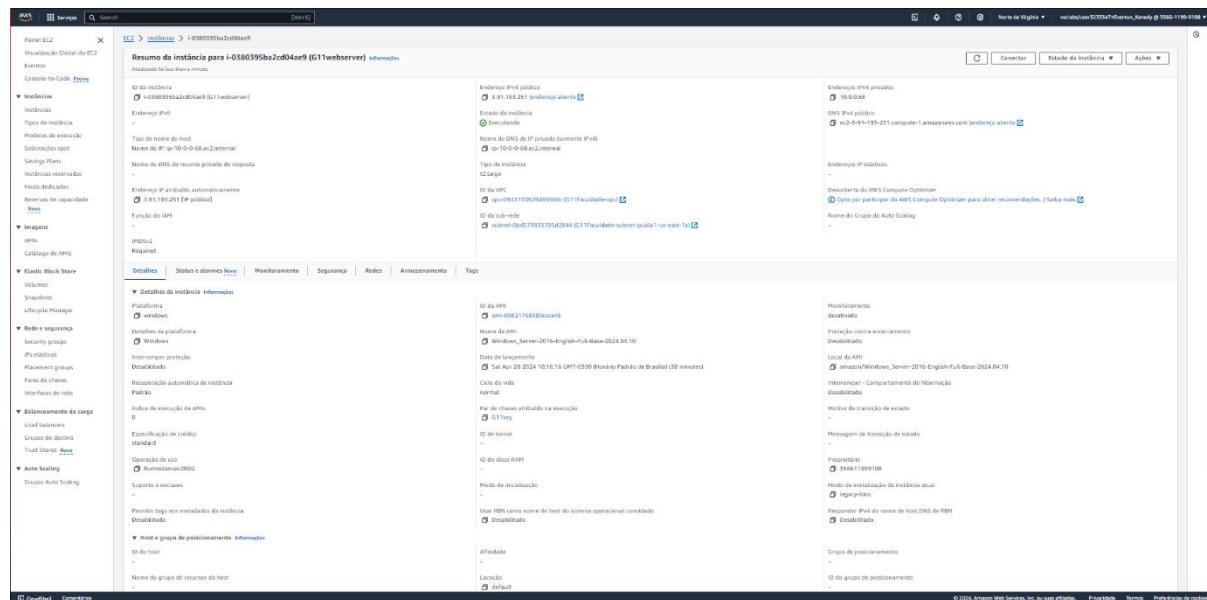
Imagen e tipo de instância


Instâncias (1) Informações

Name	ID da instância	Estado da inst...	Tipo de inst...	Verificação de stal	Status do alarm...	Zona de disponib...	DNS IPv4 público	Endereço IP...	IP elástico	IPs IPv6	Mor...
G11webserver	i-0380395a2cd04ae9	Executando	t2.large	2/2 verificações a	Exibir alarmes	us-east-1a	ec2-3-91-195-251.com...	3.91.195.251	-	-	dica

Selecionar uma instância

 Link para visualizar melhor a imagem([link](#)).

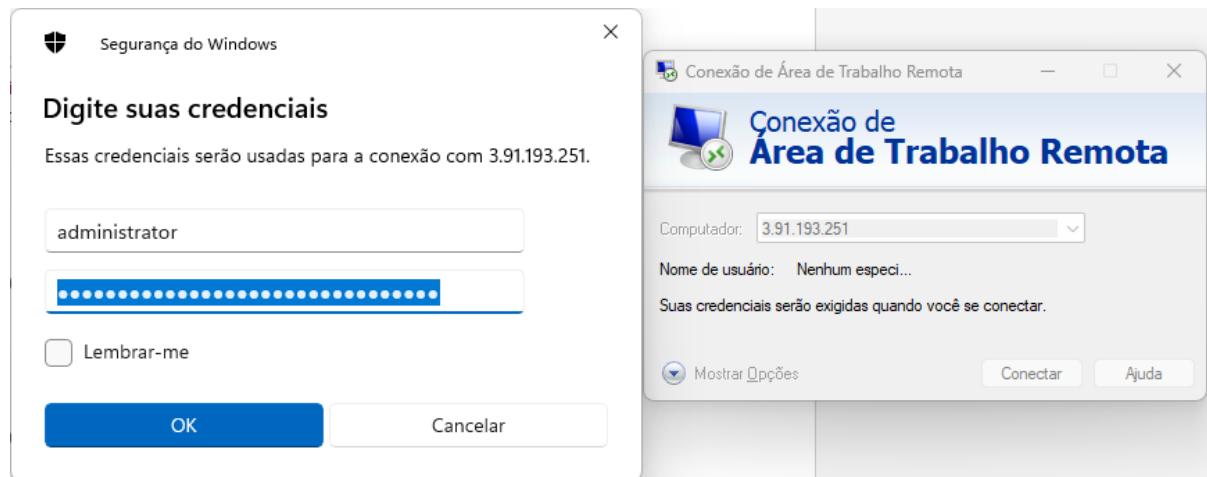


The screenshot shows the AWS CloudWatch Metrics interface for an EC2 instance. The instance ID is i-0380395ba2cd04ae9, named G11webserver. The instance is currently executing and has an IPv4 public IP address of 3.91.193.251. The status is 'Já iniciado' (Running). The instance is running Windows Server 2016 English Full Base (2024.04.10). The interface displays various metrics over time, including CPU usage, memory, and network traffic.

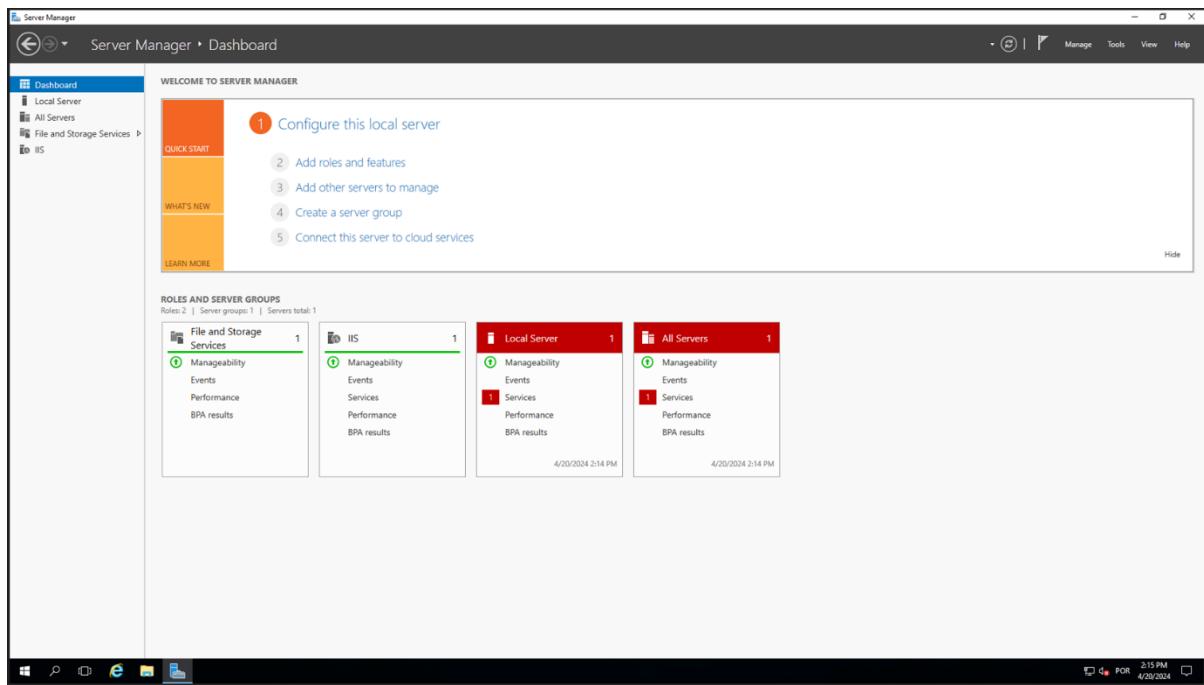
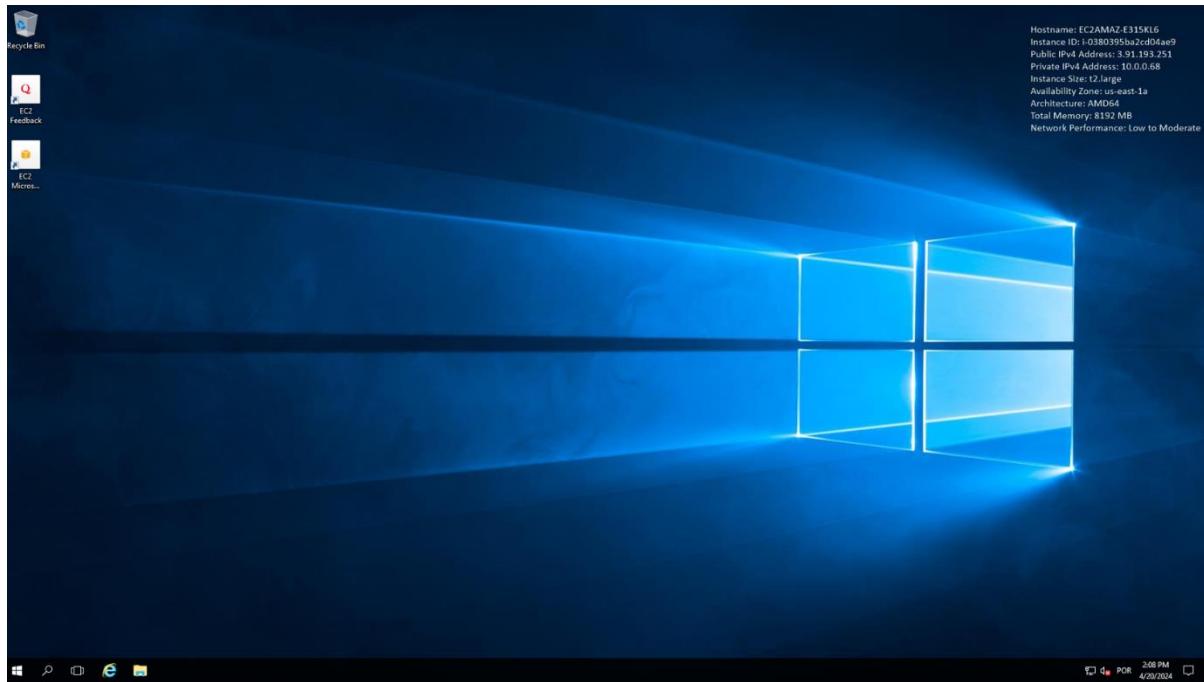
Link para visualizar melhor a imagem([link](#)).

5.2.4. ACESSO VIA RDP

Para essa etapa utilizamos a ferramenta do Windows Conexão de Área de Trabalho Remota, pegamos o IP público do servidor web e a senha no menu de Ações->Segurança->Obter Senha do Windows na instancia EC2 que criamos anteriormente.



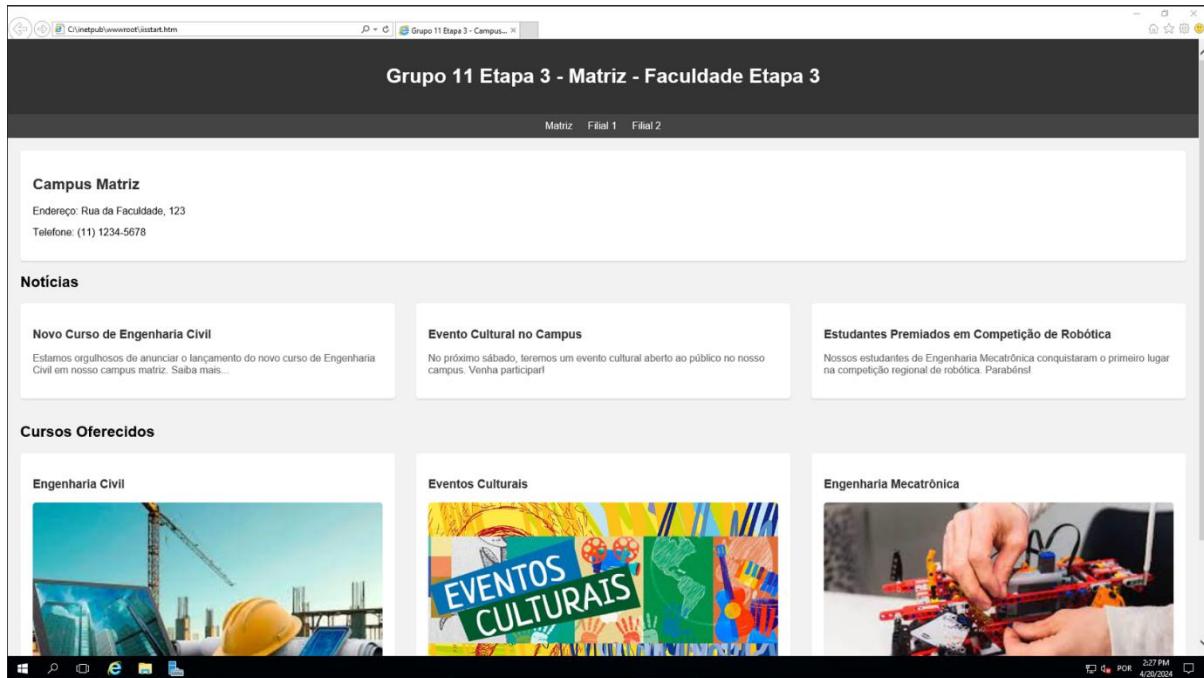
The image contains two windows. On the left is the 'Segurança do Windows' (Windows Security) dialog, titled 'Digite suas credenciais' (Enter your credentials). It shows a text input field with 'administrator' and a password field filled with a series of dots. Below the fields are checkboxes for 'Lembrar-me' (Remember me) and 'Mostrar opções' (Show options). At the bottom are 'OK' and 'Cancelar' (Cancel) buttons. On the right is the 'Conexão de Área de Trabalho Remota' (Remote Desktop Connection) dialog, titled 'Conexão de Área de Trabalho Remota'. It shows the 'Computador:' field set to '3.91.193.251'. Below it, the 'Nome de usuário:' (User name:) field is set to 'Nenhum espec...'. A message below says 'Suas credenciais serão exigidas quando você se conectar.' (Your credentials will be required when you connect.) At the bottom are 'Conectar' (Connect) and 'Ajuda' (Help) buttons.



WELCOME TO SERVER MANAGER
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services

ROLES AND SERVER GROUPS
Roles 2 | Server groups: 1 | Servers total: 1

Role/Server Group	Count	Last Update
File and Storage Services	1	4/20/2024 2:14 PM
IIS	1	4/20/2024 2:14 PM
Local Server	1	4/20/2024 2:14 PM
All Servers	1	4/20/2024 2:14 PM



The screenshot shows a web page titled "Grupo 11 Etapa 3 - Matriz - Faculdade Etapa 3". At the top, there's a navigation bar with links for "Matriz", "Filial 1", and "Filial 2". Below the header, there's a section for "Campus Matriz" with address and phone number details. A "Notícias" (News) section contains three items: "Novo Curso de Engenharia Civil" (New Civil Engineering Course), "Evento Cultural no Campus" (Cultural Event at the Campus), and "Estudantes Premiados em Competição de Robótica" (Students Awarded in Robotics Competition). Under "Cursos Oferecidos" (Courses Offered), there are three cards: "Engenharia Civil" (Civil Engineering) with an image of a construction site, "Eventos Culturais" (Cultural Events) with a colorful graphic, and "Engenharia Mecatrônica" (Mechatronics Engineering) with an image of hands working on a robotic model.

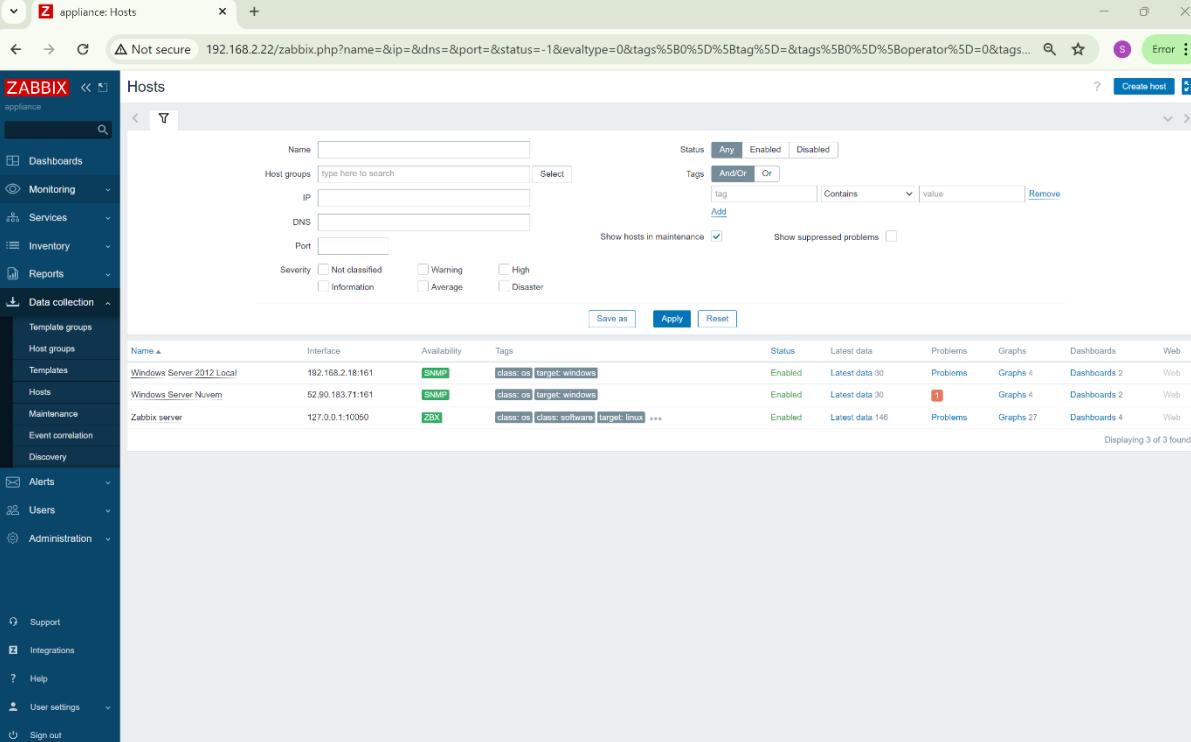
6. Gerenciamento dos serviços no ZABBIX

Para que pudéssemos monitorar o servidor físico na rede, foi necessário integrá-lo ao Zabbix, uma ferramenta de monitoramento de infraestrutura de TI. Para isso, utilizamos o protocolo SNMP, que permite o gerenciamento de dispositivos em uma rede através de seus IPs. Conforme mostrado na imagem abaixo, o serviço SNMP foi configurado no servidor local com uma string de community: "public" (para acesso somente de leitura). Essa string funciona como chaves de acesso para a integração do servidor com o Zabbix.

Com as communities configuradas no servidor local, iniciamos o processo de configuração do host no Zabbix. Para isso, foi necessário preencher algumas informações na plataforma de monitoramento, como o nome do host, o protocolo utilizado, seu IP, a porta, seu template e seu host group. Essas informações foram essenciais para que o Zabbix pudesse localizar e requisitar informações do host que desejávamos monitorar.

As regras de firewall no servidor local foram verificadas para garantir que o acesso do Zabbix pela porta 161-162 não fosse bloqueado. Felizmente, não encontramos nenhum impedimento nesse processo.

No painel de controle do Zabbix, foram criados dois hosts: um destinado à nuvem e outro ao servidor local.



Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
Windows Server 2012 Local	192.168.2.18:161	SNMP	class: os target: windows	Enabled	Latest data 30	Problems	Graphs 4	Dashboards 2	Web
Windows Server Nuvem	52.90.183.71:161	SNMP	class: os target: windows	Enabled	Latest data 30	1	Graphs 4	Dashboards 2	Web
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ***	Enabled	Latest data 146	Problems	Graphs 27	Dashboards 4	Web

Painel de controle Zabbix. Um host local e um destinado a nuvem (AWS).

6.1. GERENCIAMENTO DO SERVIDOR FÍSICO NO ZABBIX

O Zabbix foi instalado e configurado na máquina virtual, seguindo as instruções fornecidas na documentação disponível no material de apoio da etapa 4.

6.2. GERENCIAMENTO DO SERVIDOR NA NUVEM NO ZABBIX

O Zabbix foi instalado e configurado no servidor na nuvem, seguindo as instruções fornecidas na documentação disponível no material de apoio da etapa 4.

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
G11FaculdadeWebServer	i-0793fa9326f7e6dfd	Running	t2.large	2/2 checks passed	View alarms
Zabbix	i-0a514b6b6440b2197	Running	t2.micro	2/2 checks passed	View alarms

i-0793fa9326f7e6dfd (G11FaculdadeWebServer)

- [Details](#)
- [Status and alarms](#)
- [Monitoring](#)
- [Security](#)
- [Networking](#)
- [Storage](#)
- [Tags](#)

Instance summary

Instance ID	i-0793fa9326f7e6dfd (G11FaculdadeWebServer)	Public IPv4 address	52.90.183.71 open address	Private IPv4 addresses	10.0.0.226
IPv6 address	-	Instance state	Running	Public IPv4 DNS	ec2-52-90-183-71.compute-1.amazonaws.com open address
Hostname type	IP name: ip-10-0-0-226.ec2.internal	Private IP DNS name (IPv4 only)	ip-10-0-0-226.ec2.internal	Elastic IP addresses	-
Answer private resource DNS name	-	Instance type	t2.large	AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations
Auto-assigned IP address	52.90.183.71 (Public IP)	VPC ID	vpc-00c4fd49782397ccb (G11Faculdade-vpc)		

Imagen mostrando o Host na AWS

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#SecurityGroups

Security Groups (1/4) Info

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-025f5b497d32c1632	default	vpc-00c4fd49782397ccb	default VPC security group	\$11938571852
<input checked="" type="checkbox"/>	sg-04ab512a52e701124	G11FaculdadeSec	vpc-00c4fd49782397ccb	Web e Terminal Remoto	\$11938571852
-	sg-0c97f84d497376aca	launch-wizard-1	vpc-014ba66d756b681f	launch-wizard-1 created 2024-05-13T...	\$11938571852

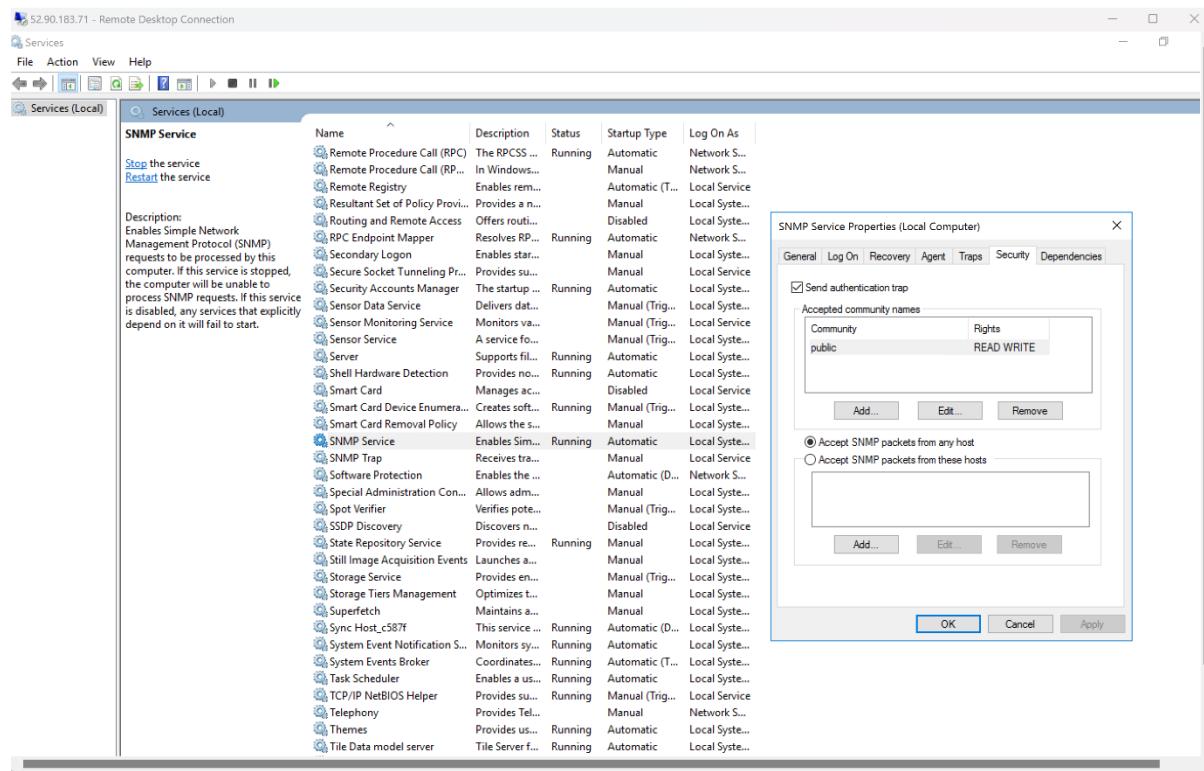
sg-04ab512a52e701124 - G11FaculdadeSec

- [Details](#)
- [Inbound rules](#)
- [Outbound rules](#)
- [Tags](#)

Inbound rules (3)

Name	Security group r...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-0dd0521e56202...	IPv4	Custom UDP	UDP	161 - 162	0.0.0.0/0	SNMP
-	sgr-037c10cc8cc5c...	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso Web
-	sgr-0494cc6e727cd...	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso Terminal Remoto

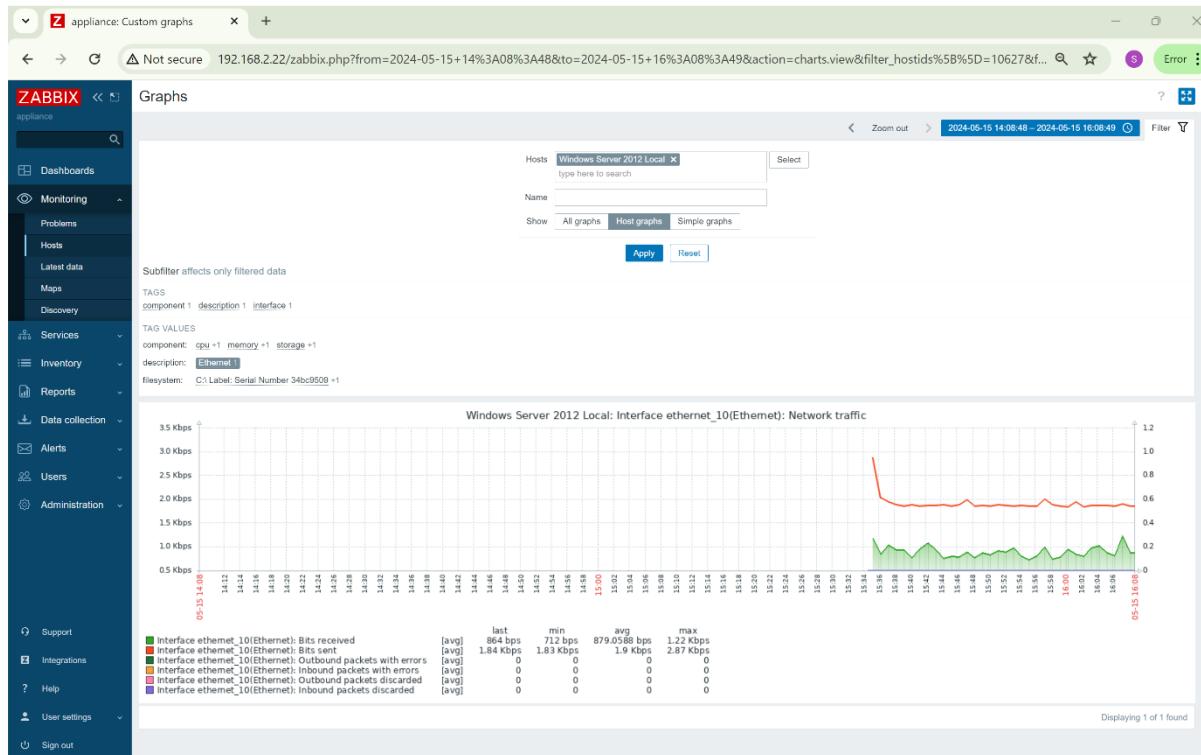
Imagen mostrando os grupos de segurança na AWS.



Serviço de SNMP no servidor da nuvem

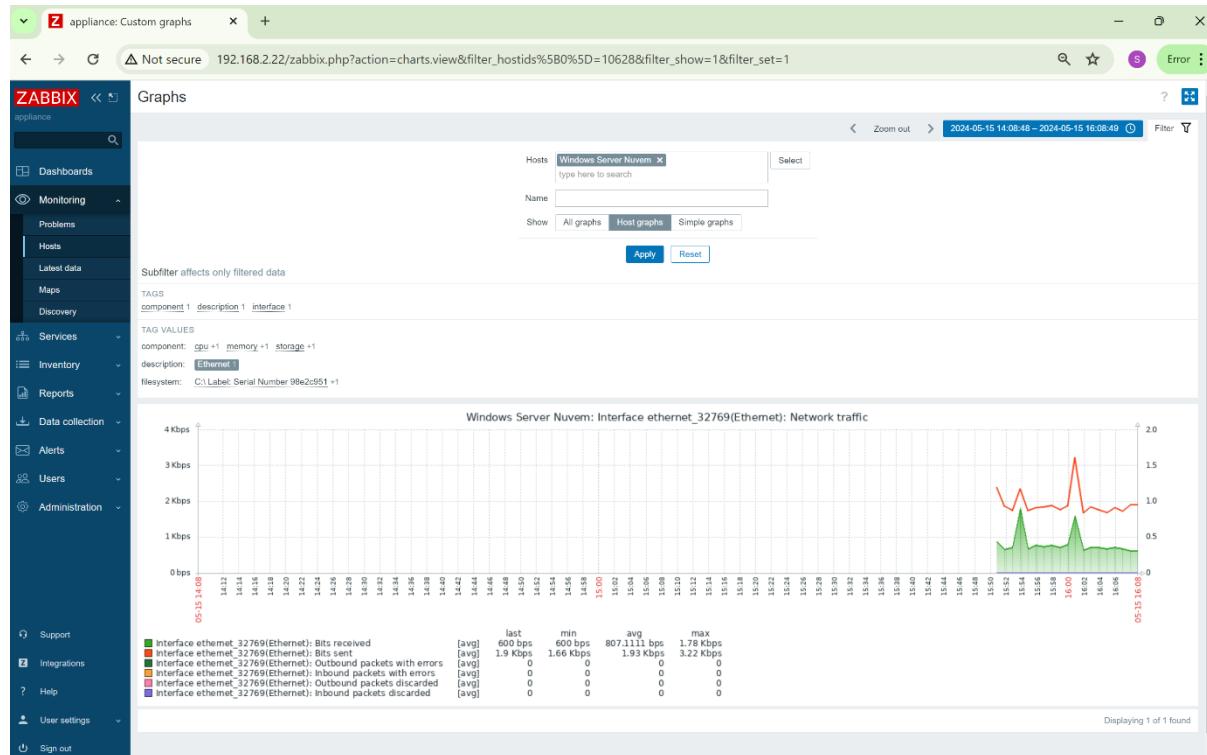
6.3. VISUALIZAÇÃO E MONITORAMENTO DOS SERVIDORES NO ZABBIX

Com a configuração realizada no servidor local e no servidor da nuvem, o Zabbix já conseguia monitorar os servidores. Verificamos na ferramenta que ambas as comunicações com os hosts estavam sendo executadas sem qualquer falha.



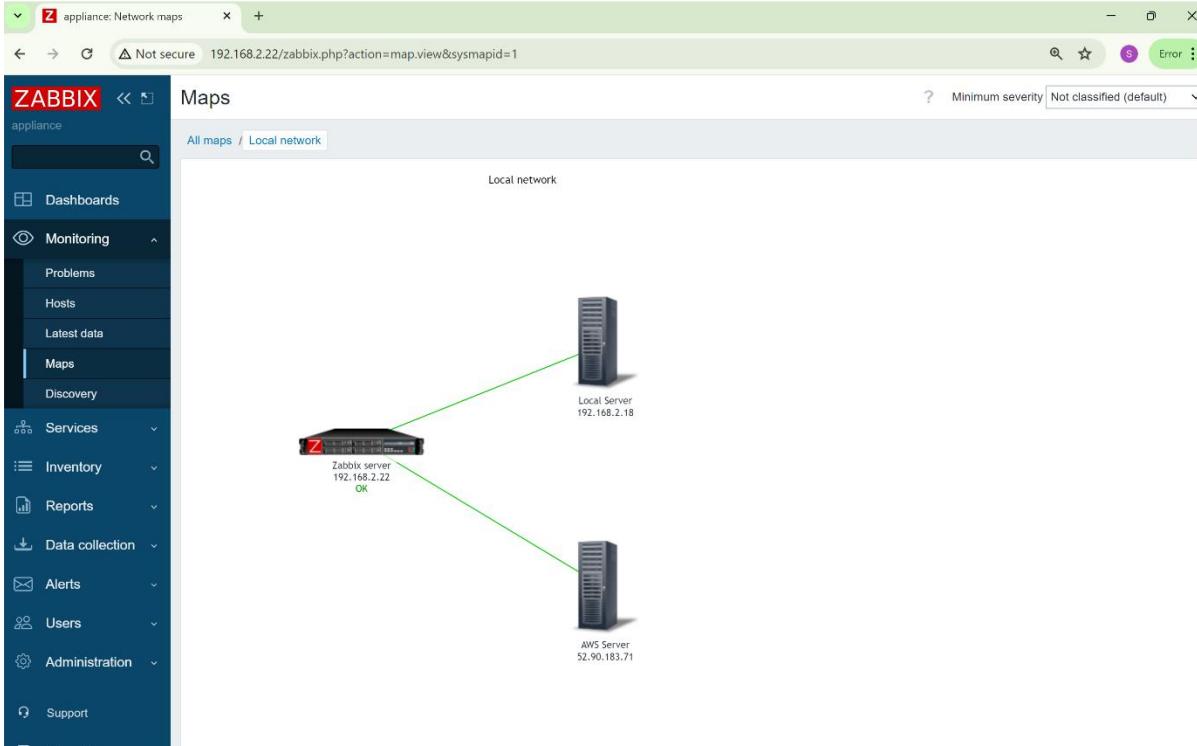
Monitoramento do tráfego de rede do servidor local no Zabbix.

Rede (Ethernet Cloud Server)

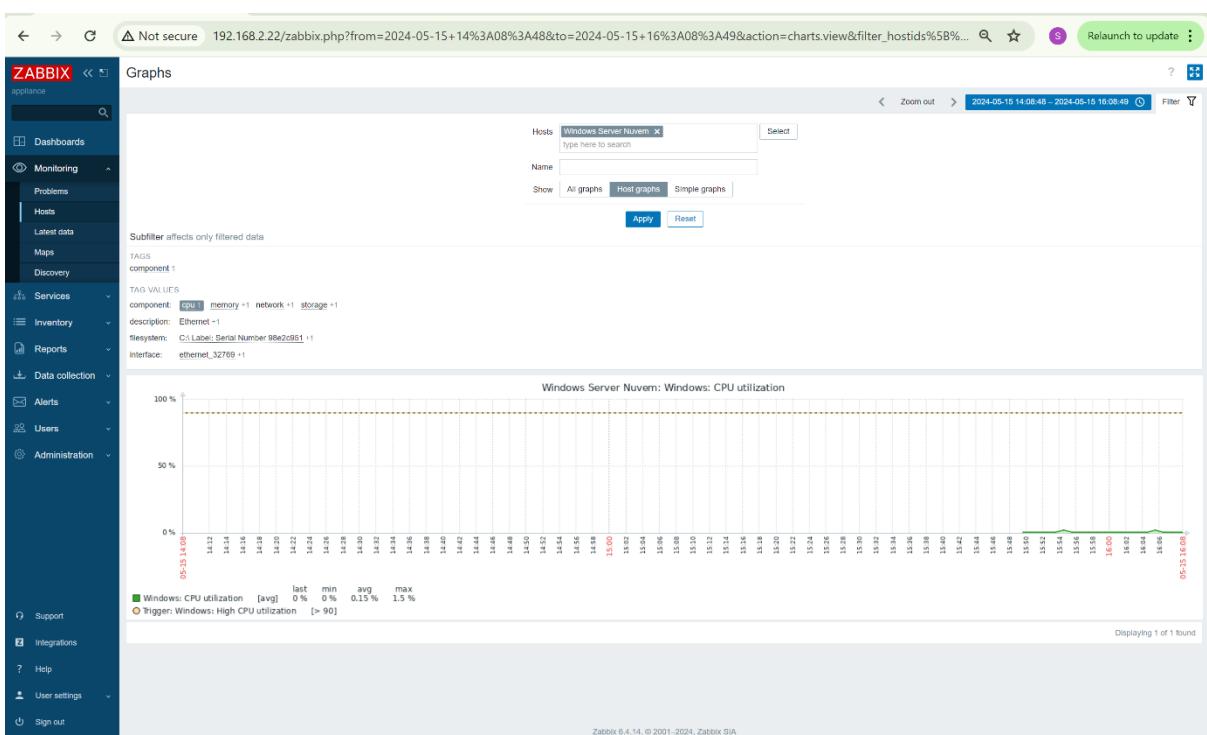


Monitoramento do tráfego de rede do servidor localizado em nuvem no Zabbix.

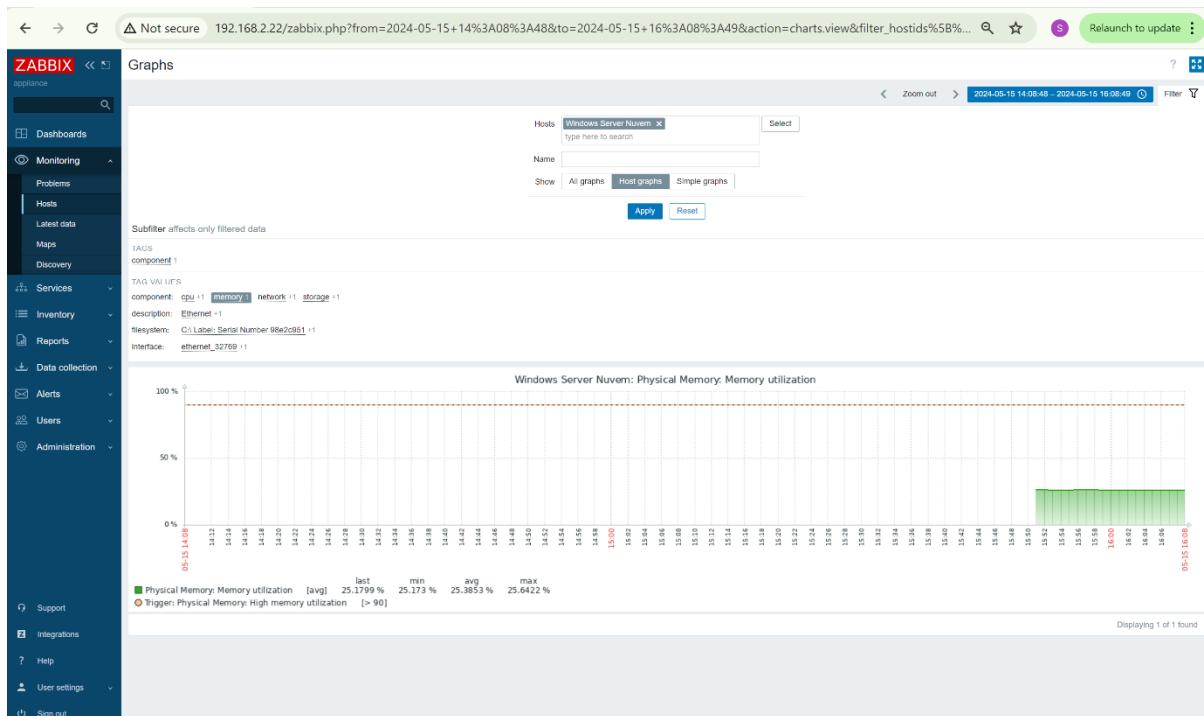
A plataforma Zabbix também permite a visualização de um mapa da nossa infraestrutura de rede monitorada.



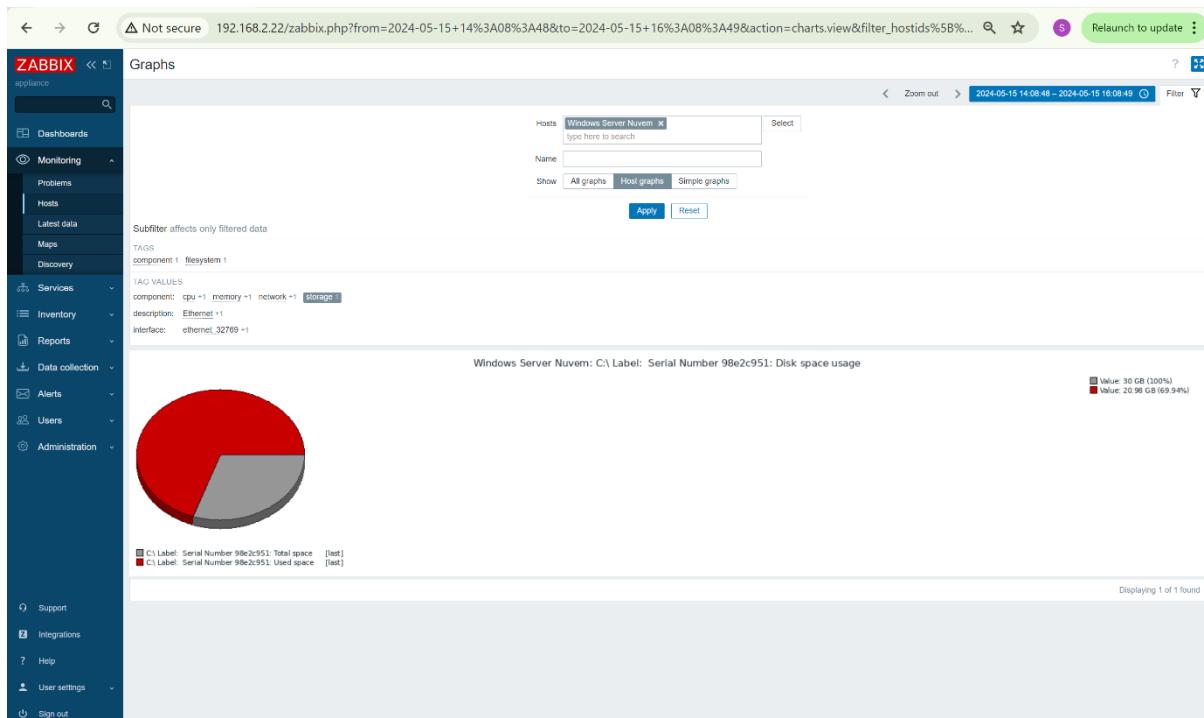
Mapa de rede



CPU (Computer Power Unit Cloud Server)



Memória (Memory Cloud Server)



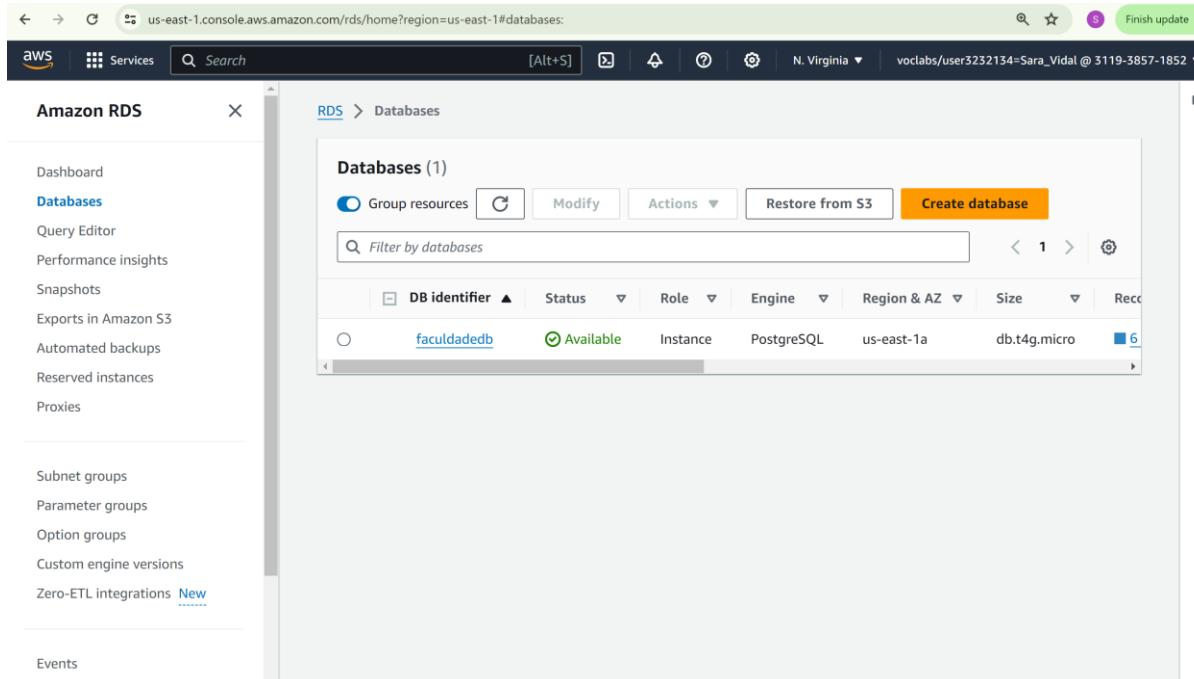
Disco (Storage Cloud Server)

Belo Horizonte
2024

7. Aplicação back-end

Repositório GitHub: <https://github.com/Saracvidal/GrupoOnzeFaculdade.git>

Banco de dados na AWS (RDS):



Databases (1)

DB identifier	Status	Role	Engine	Region & AZ	Size	Rec.
faculdadedb	Available	Instance	PostgreSQL	us-east-1a	db.t4g.micro	6

Endpoint: facultadedb.cysbrwplr9wn.us-east-1.rds.amazonaws.com

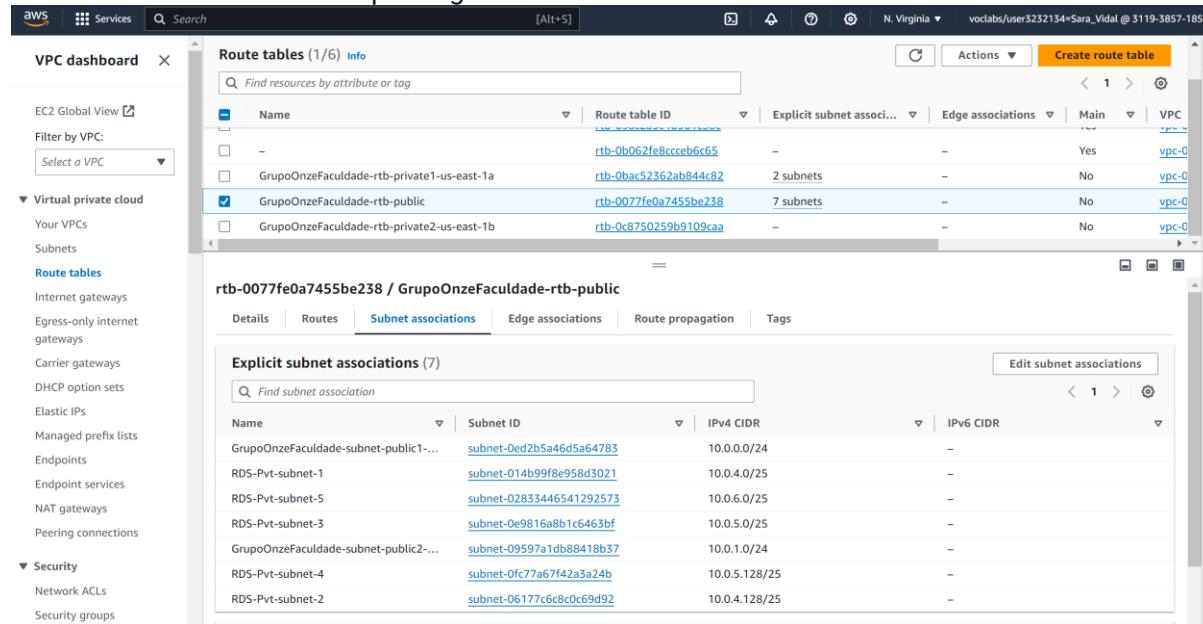
Porta: 5432

DB instance ID: facultadedb

Engine version: 16.2

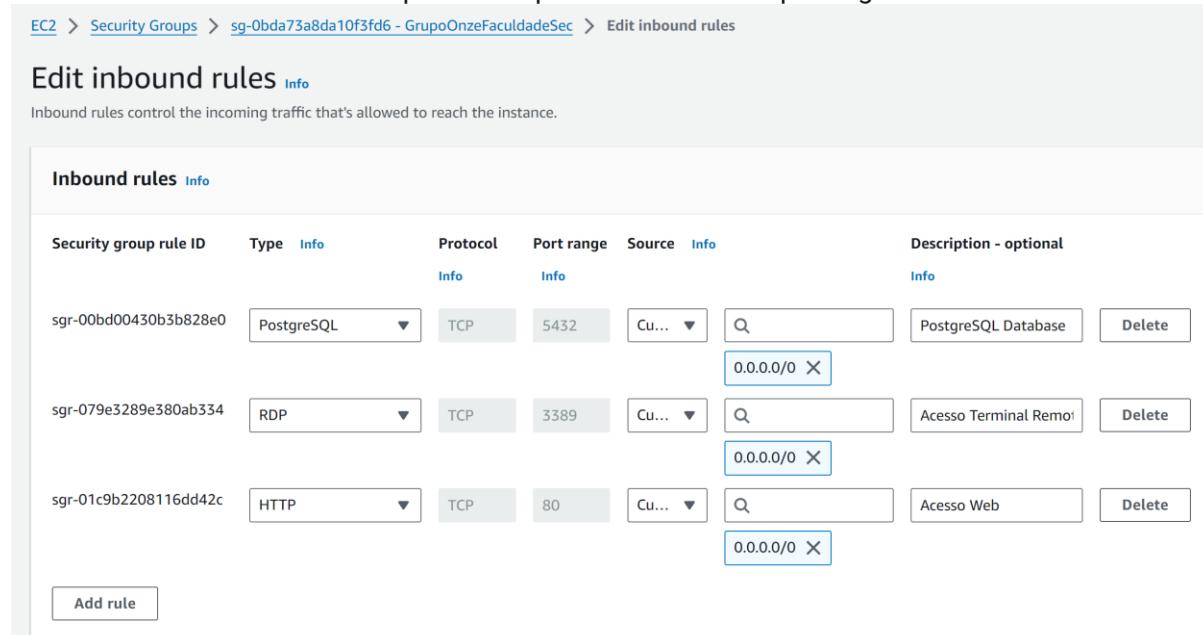
DB name: facultadedb

Adicionado o RDS na tabela de rotas do GrupoOnzeFaculdade para fazer possível a conexão no mesmo ambiente e conexão pelo PgAdmin4:



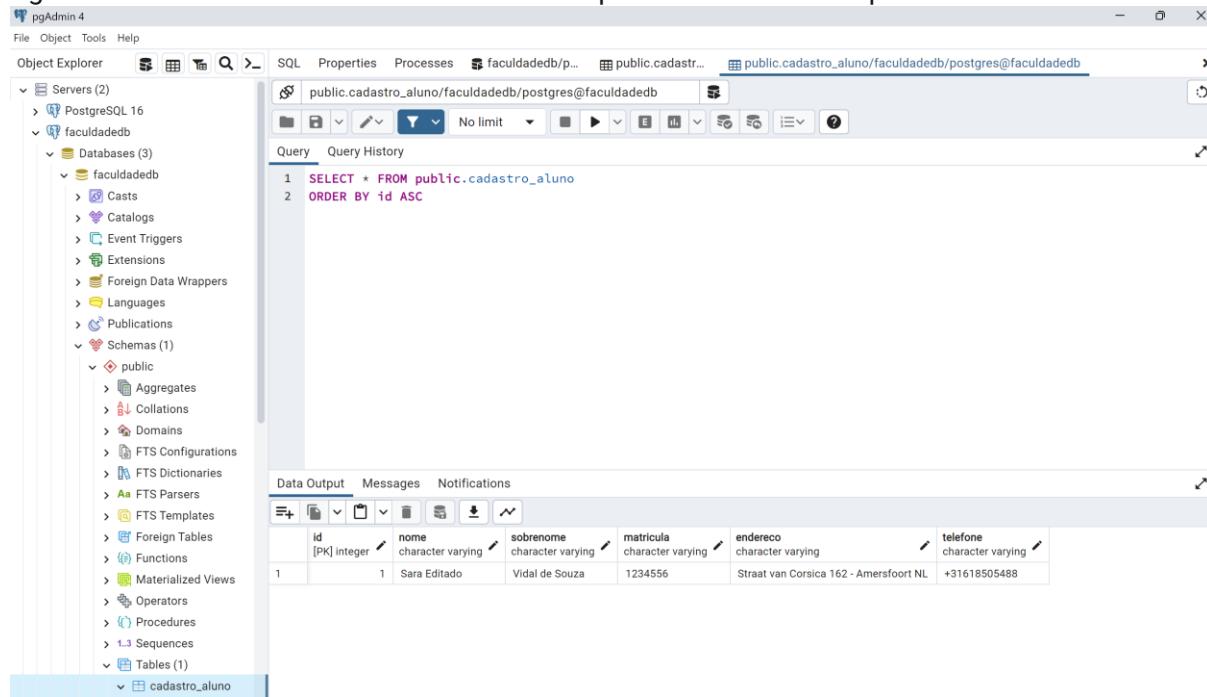
Name	Route table ID	Explicit subnet assoc...	Main	VPC
rtb-0b062fe8ccceb6c65	-	-	Yes	vpc-0
rtb-0bac52362ab844c82	2 subnets	-	No	vpc-0
rtb-0077fe0a7455be238	7 subnets	-	No	vpc-0
rtb-0c8750259b9109caa	-	-	No	vpc-0

Adicionado uma “inbound rule” para fazer possível a conexão pelo PgAdmin4:



Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-00bd00430b3b828e0	PostgreSQL	TCP	5432	Cu... ▾	PostgreSQL Database
sgr-079e3289e380ab334	RDP	TCP	3389	Cu... ▾	Acesso Terminal Remoto
sgr-01cb2208116dd42c	HTTP	TCP	80	Cu... ▾	Acesso Web

PgAdmin4 conectado com o RDS e uma tabela para o CRUD de exemplo:



The screenshot shows the PgAdmin4 interface. On the left, the Object Explorer pane displays a tree structure of databases, schemas, and tables under the 'faculdadedb' server. In the center, a query window contains the following SQL code:

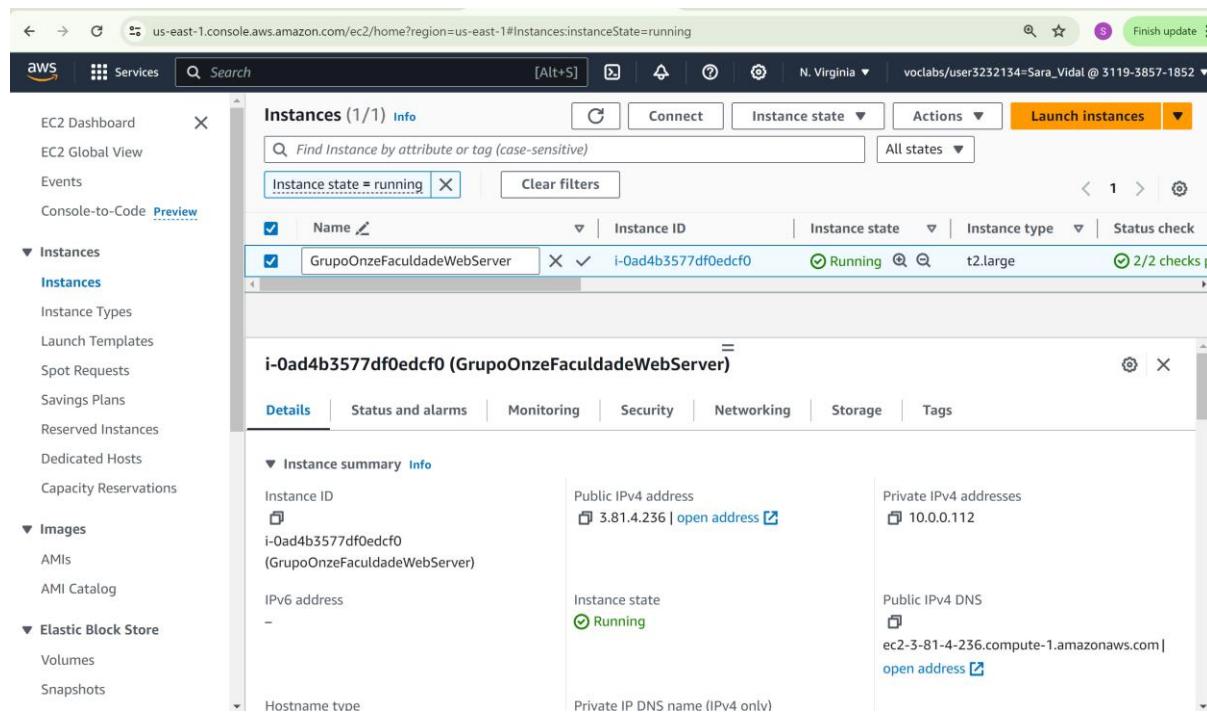
```

1 SELECT * FROM public.cadastro_aluno
2 ORDER BY id ASC
  
```

Below the query window, the Data Output pane shows the results of the query:

	id [PK] integer	nome character varying	sobrenome character varying	matricula character varying	endereco character varying	telefone character varying
1	1	Sara Editado	Vidal de Souza	1234556	Straat van Corsica 162 - Amersfoort NL	+31618505488

IP de conexão na área de trabalho remota do servidor (nesse momento usando o IP 3.81.4.236):



The screenshot shows the AWS EC2 Instances page. The sidebar navigation includes: EC2 Dashboard, EC2 Global View, Events, Console-to-Code Preview, Instances (selected), Instances Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main content area shows a table of instances with one entry:

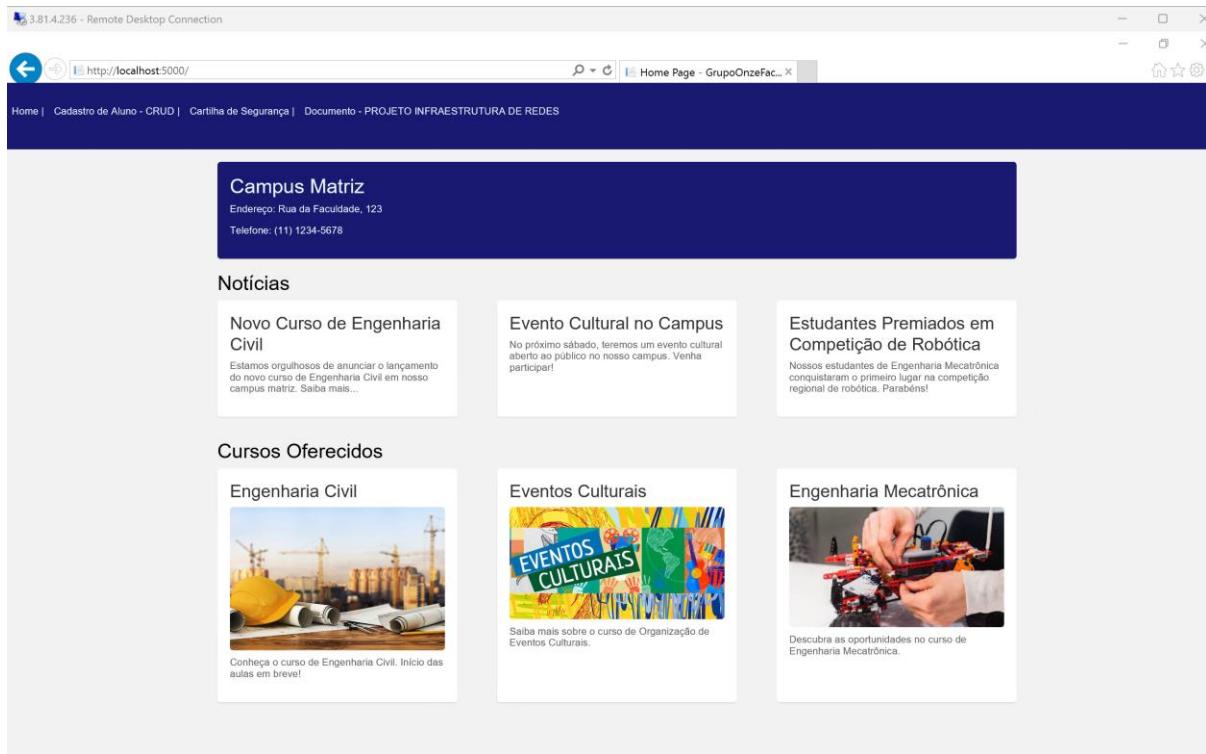
Name	Instance ID	Instance state	Instance type	Status check
GrupoOnzeFaculdadeWebServer	i-0ad4b3577df0edcf0	Running	t2.large	2/2 checks p

Details for the selected instance (i-0ad4b3577df0edcf0) are shown in a detailed view. Key information includes:

- Public IPv4 address: 3.81.4.236
- Private IPv4 addresses: 10.0.0.112
- Public IPv4 DNS: ec2-3-81-4-236.compute-1.amazonaws.com

Aplicação Rodando no servidor:

Página inicial (Home)



Campus Matriz
Endereço: Rua da Faculdade, 123
Telefone: (11) 1234-5678

Notícias

- Novo Curso de Engenharia Civil**
Estamos orgulhosos de anunciar o lançamento do novo curso de Engenharia Civil em nosso campus matriz. Saiba mais...
- Evento Cultural no Campus**
No próximo sábado, teremos um evento cultural aberto ao público no nosso campus. Venha participar!
- Estudantes Premiados em Competição de Robótica**
Nossos estudantes de Engenharia Mecatrônica conquistaram o primeiro lugar na competição regional de robótica. Parabéns!

Cursos Oferecidos

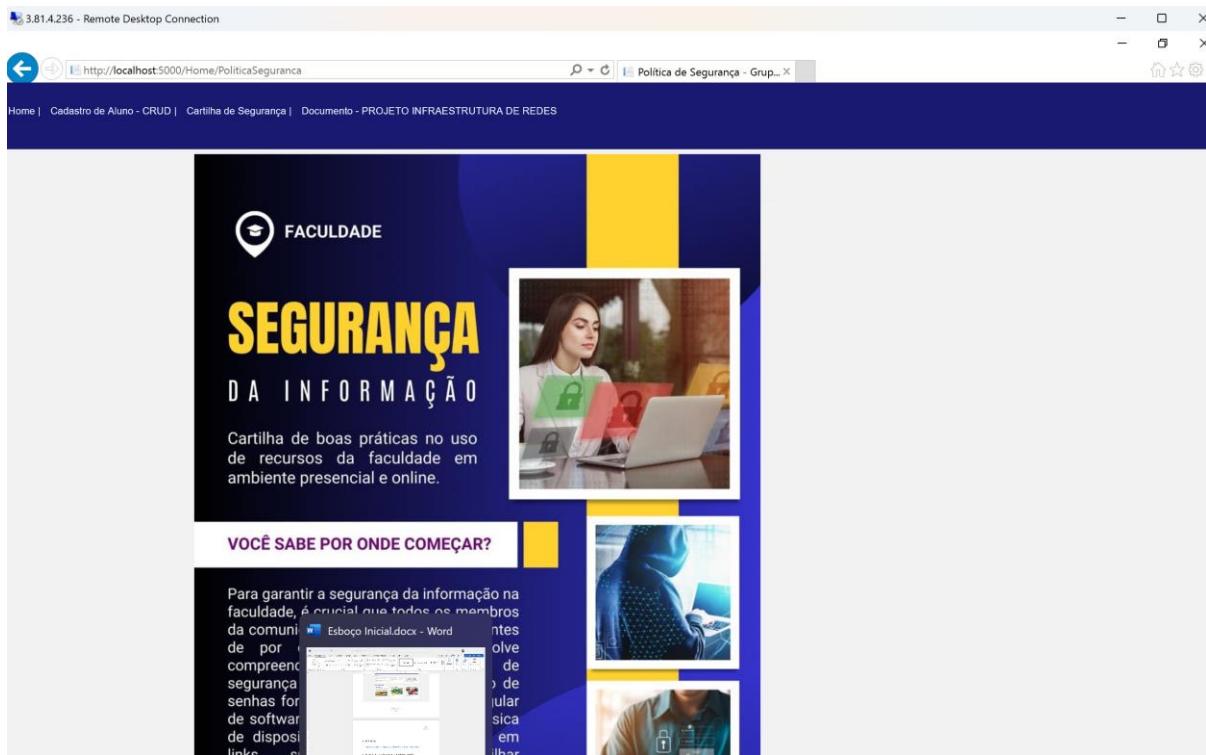
- Engenharia Civil**

Conheça o curso de Engenharia Civil. Início das aulas em breve!
- Eventos Culturais**

Saiba mais sobre o curso de Organização de Eventos Culturais.
- Engenharia Mecatrônica**

Descubra as oportunidades no curso de Engenharia Mecatrônica.

Cartilha de segurança:



FACULDADE
SEGURANÇA
DA INFORMAÇÃO

Cartilha de boas práticas no uso de recursos da faculdade em ambiente presencial e online.

VOCÊ SABE POR ONDE COMEÇAR?

Para garantir a segurança da informação na faculdade, é crucial que todos os membros da comunidade por em prática as seguintes medidas:

- Evite clicar em links suspeitos.
- Use senhas fortes e únicas para diferentes sistemas.
- Manter o software atualizado.
- Não compartilhar informações sensíveis via e-mail.
- Evitar conexões públicas para acessar serviços sensíveis.
- Manter dispositivos fisicamente seguros.

Imagens:

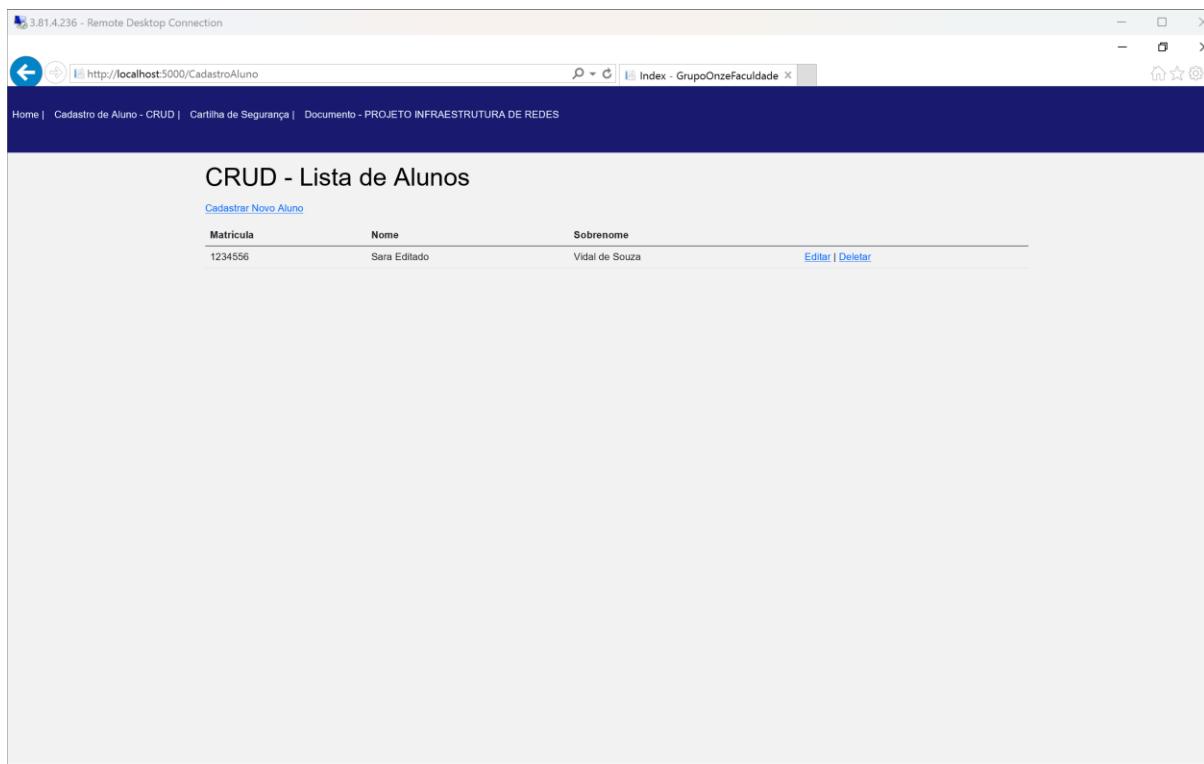
- Uma mulher usando óculos escuros e uma máscara, sentada em frente a um laptop com uma interface de usuário digital.
- Detalhe de uma mão usando um mouse com uma interface de usuário digital.
- Detalhe de uma tela de computador com uma interface de usuário digital.

Documento dando o load do pdf desse presente documento com opção para baixar/imprimir/etc:

Home | Cadastro de Aluno - CRUD | Cartilha de Segurança | Documento - PROJETO INFRAESTRUTURA DE REDES

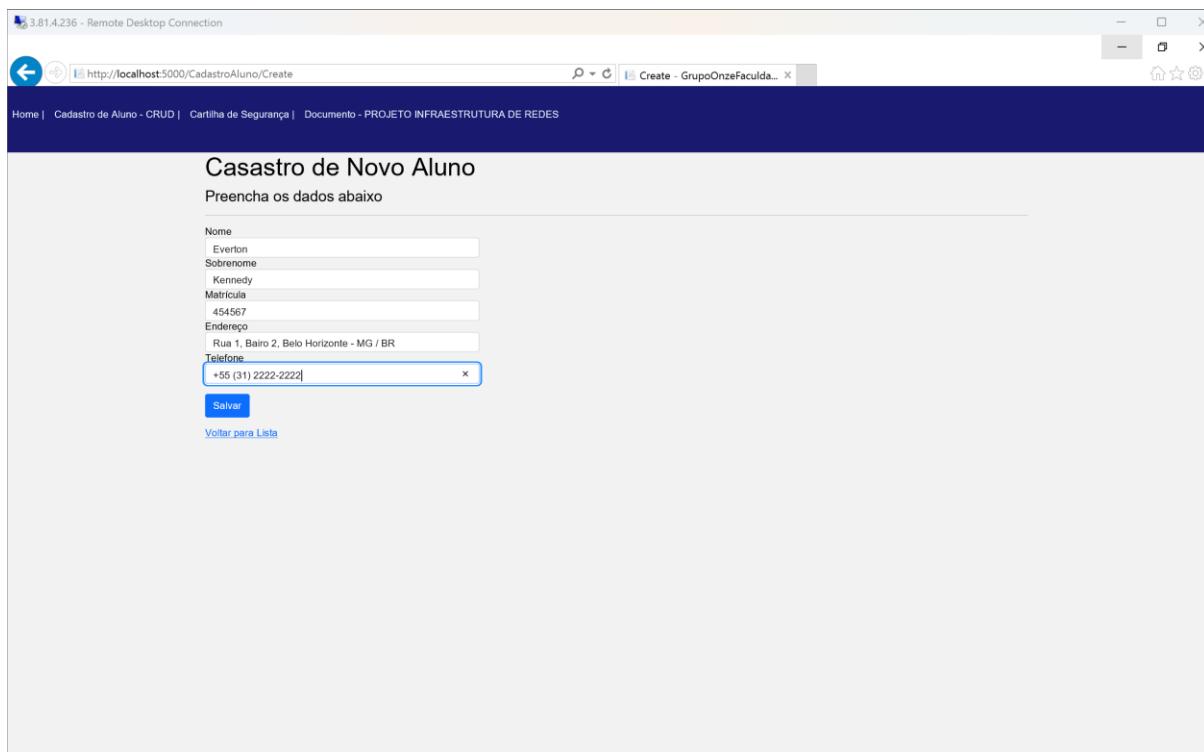
CRUD (Create/Read/Update/Delete):

Inicialmente dando o load do dado pré-populado na tabela exemplo no banco de dados RDS:

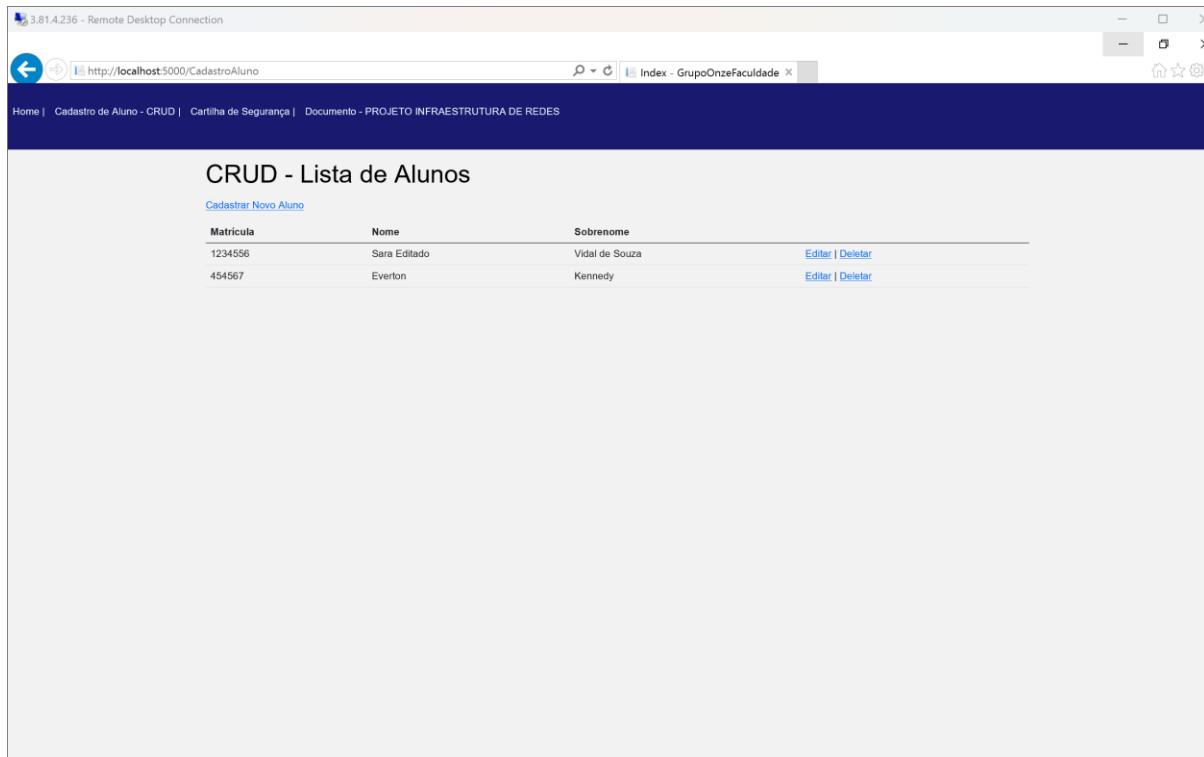


Matrícula	Nome	Sobrenome
1234556	Sera Editado	Vidal de Souza

Cadastro de um novo aluno:

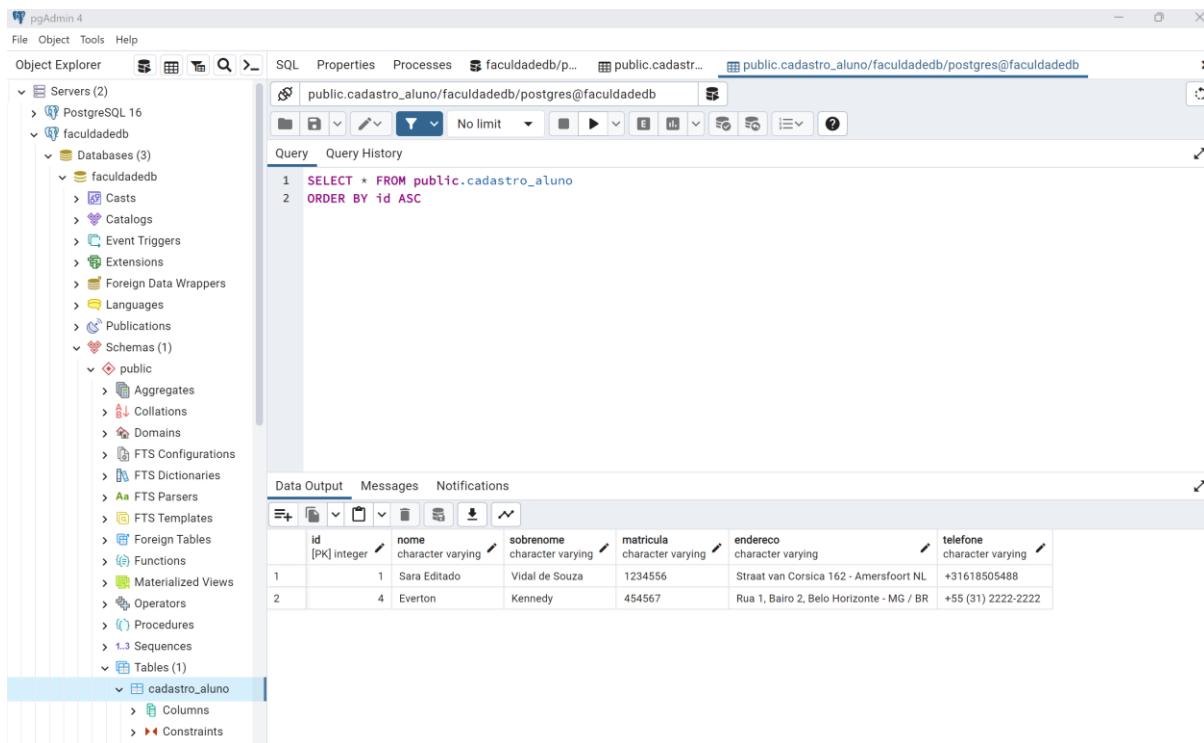


Após eventos Cadastrar/Editar/Excluir, a página se redireciona para a lista de alunos novamente com as modificações atualizadas na lista:



Matrícula	Nome	Sobrenome	
1234556	Sara Editado	Vidal de Souza	Editar Deletar
454567	Everton	Kennedy	Editar Deletar

Voltando ao banco, podemos conferir que a tabela recebeu os dados:

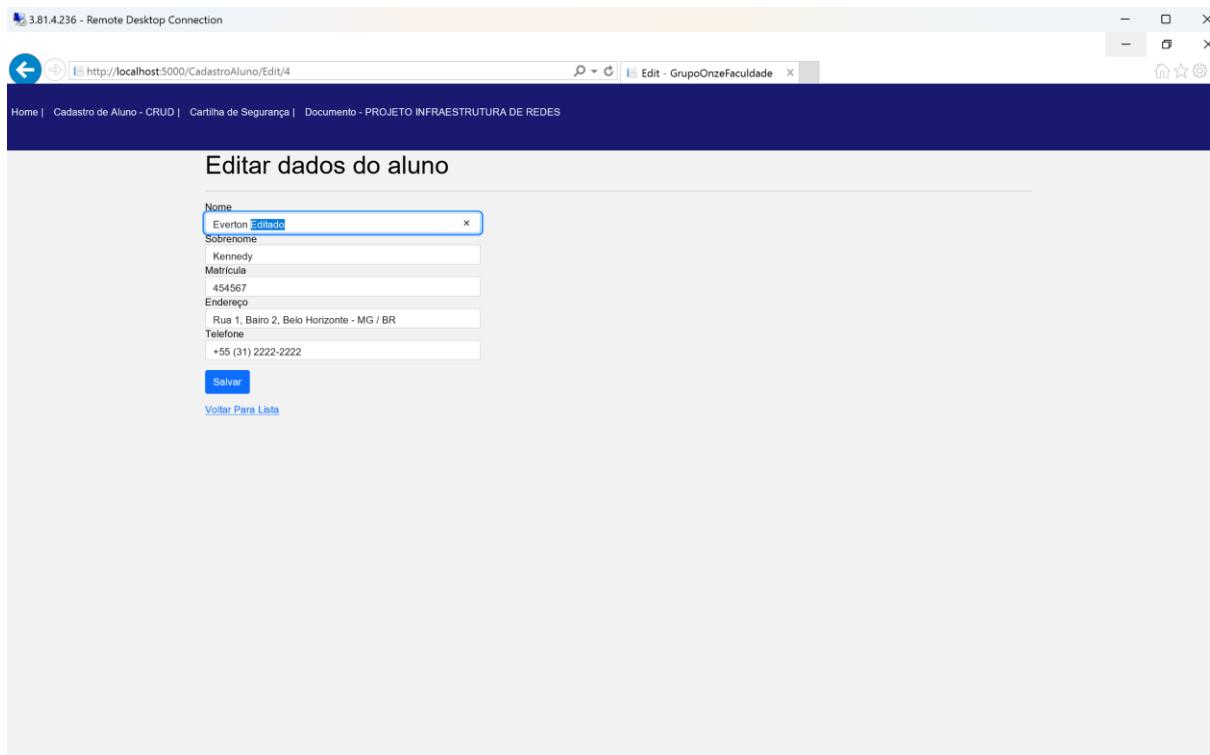


```

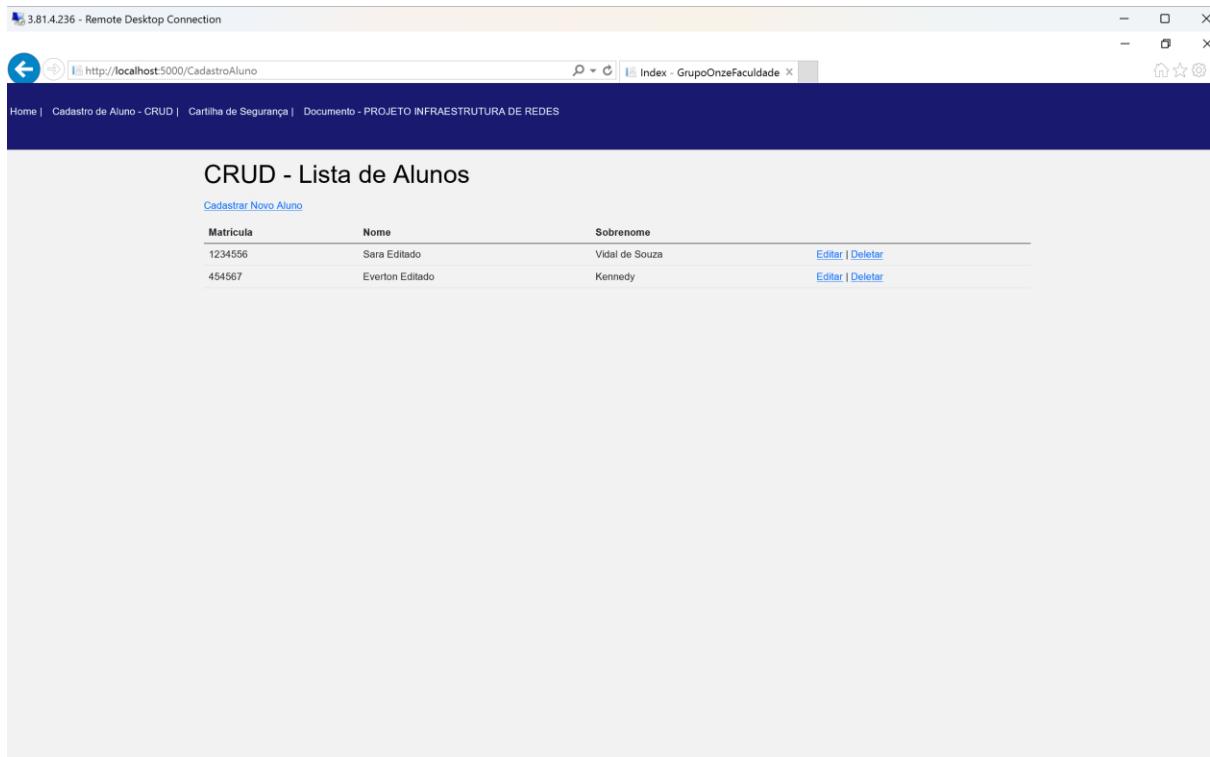
1 SELECT * FROM public.cadastro_aluno
2 ORDER BY id ASC
  
```

	id [PK] integer	nome character varying	sobrenome character varying	matricula character varying	endereco character varying	telefone character varying
1	1	Sara Editado	Vidal de Souza	1234556	Straat van Corsica 162 - Amersfoort NL	+31618505488
2	4	Everton	Kennedy	454567	Rua 1, Bairro 2, Belo Horizonte - MG / BR	+55 (31) 2222-2222

Edição dos dados do aluno (nesse exemplo adicionei a palavra “editado” após o nome do aluno):

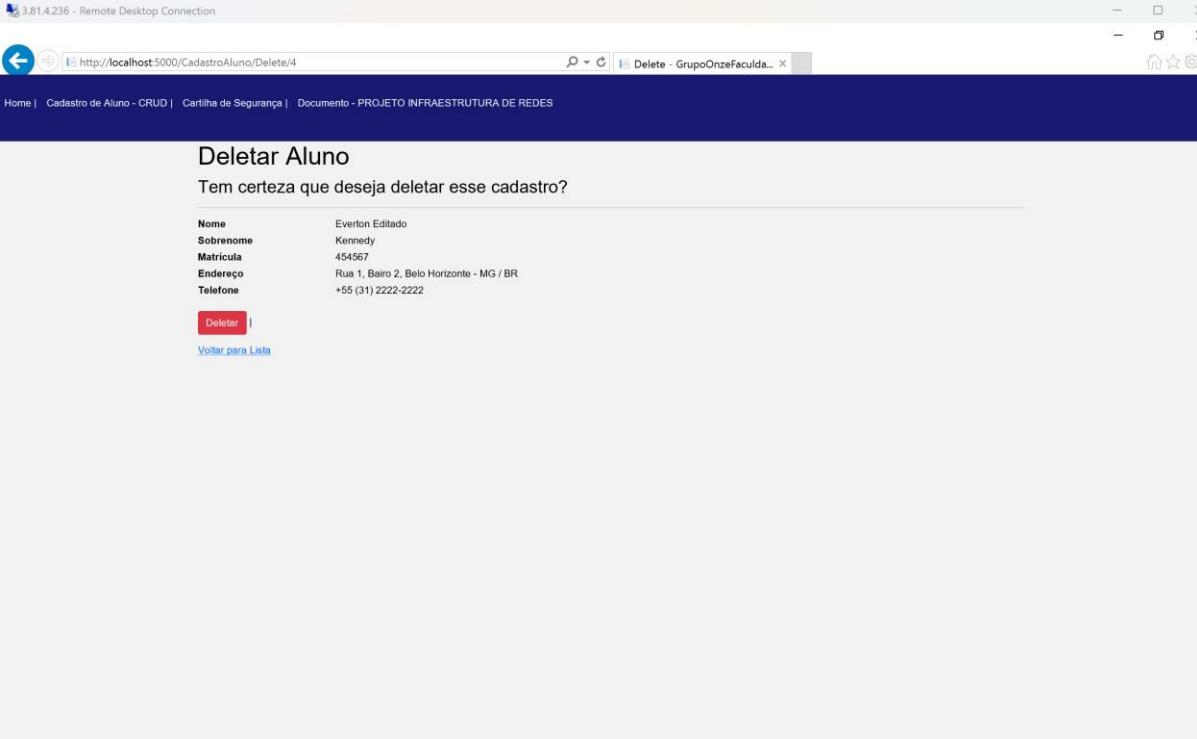


E a lista mostra o dado do aluno editado:



Matrícula	Nome	Sobrenome	
1234556	Sara Editado	Vidal de Souza	Editar Deletar
454567	Everton Editado	Kennedy	Editar Deletar

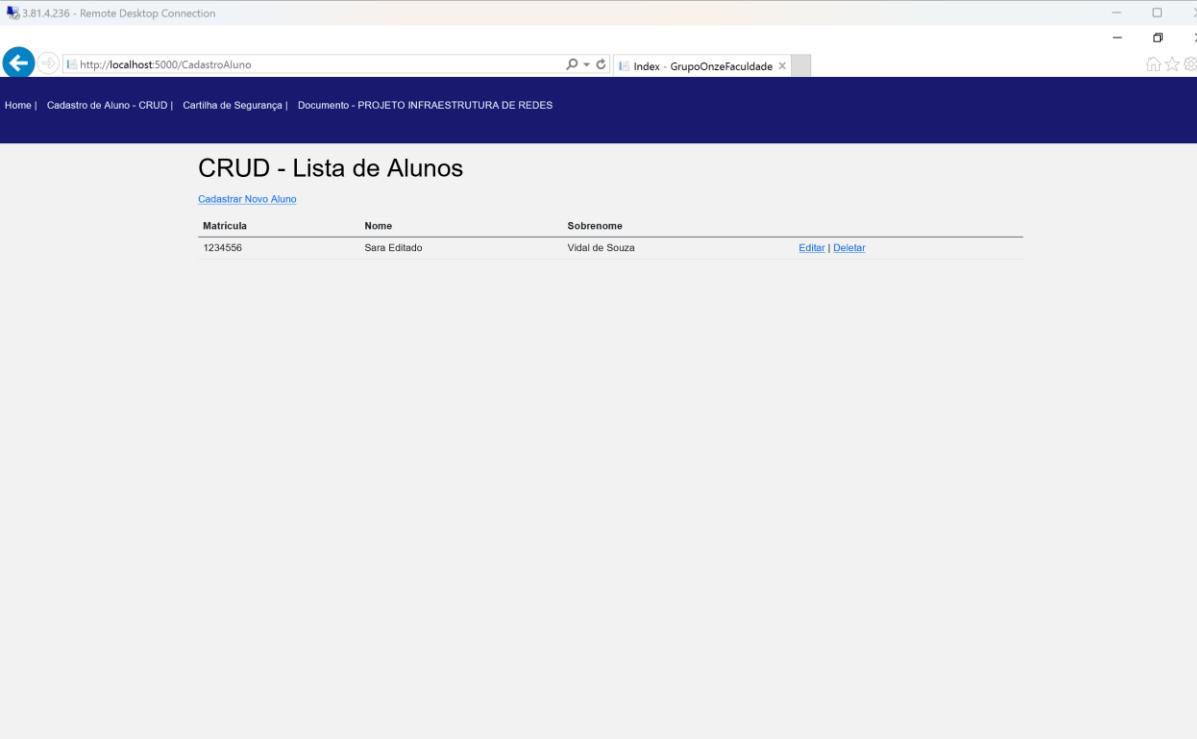
Deletar o cadastro (quando clicamos em deletar, outra janela irá abrir para confirmação da ação):



A screenshot of a Windows Remote Desktop Connection window showing a delete confirmation dialog. The title bar says "Delete - GrupoOnzeFaculdade". The main content asks "Tem certeza que deseja deletar esse cadastro?". Below it is a table with student information and a red "Deletar" button. At the bottom left is a "Voltar para Lista" link.

Nome	Everton Editado
Sobrenome	Kennedy
Matrícula	454567
Endereço	Rua 1, Bairro 2, Belo Horizonte - MG / BR
Telefone	+55 (31) 2222-2222

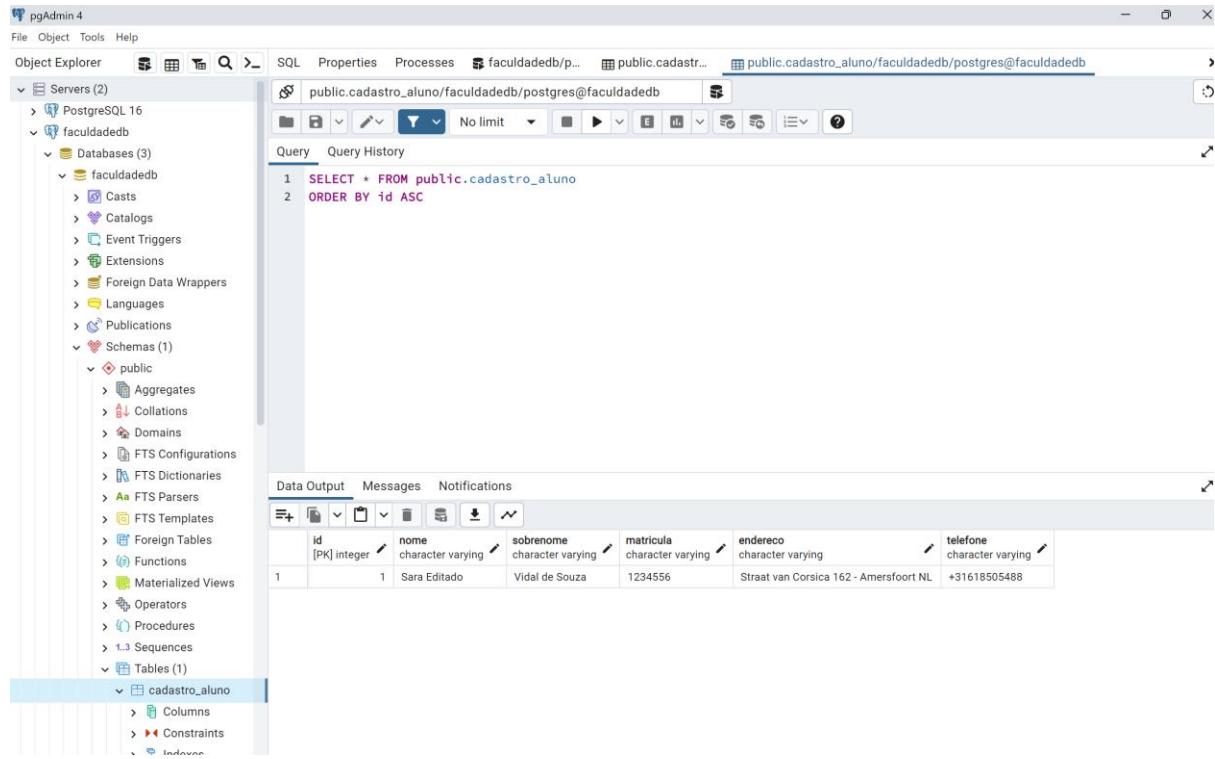
Após deletar, o aluno não estará mais na lista:



A screenshot of a Windows Remote Desktop Connection window showing the "Index" page of the application. The title bar says "Index - GrupoOnzeFaculdade". The main content displays a table titled "CRUD - Lista de Alunos" with one row of data. The row contains columns for Matrícula (1234556), Nome (Sara Editado), and Sobrenome (Vidal de Souza). To the right of the table are "Editar" and "Deletar" links.

Matrícula	Nome	Sobrenome
1234556	Sara Editado	Vidal de Souza

Após deletar, o aluno não estará mais no banco de dados:



The screenshot shows the pgAdmin 4 interface. In the Object Explorer, under the 'Servers' section, there is one server named 'faculdadedb'. Under 'Databases', there is one database named 'public'. Under 'Tables', there is one table named 'cadastro_aluno'. A query is run in the SQL tab:

```

1 SELECT * FROM public.cadastro_aluno
2 ORDER BY id ASC
  
```

The Data Output tab displays the results of the query:

	id [PK] integer	nome character varying	sobrenome character varying	matricula character varying	endereco character varying	telefone character varying
1	1	Sara Editado	Vidal de Souza	1234556	Straat van Corsica 162 - Amersfoort NL	+31618505488

8. Cartilha de Segurança da Informação

A cartilha de Segurança da Informação foi criada para orientar os usuários a respeito de boas práticas relacionadas ao uso responsável de recursos e equipamentos da faculdade. A Cartilha é fundamental para garantir que os usuários conheçam e sigam as políticas de segurança e assim ajudem a proteger o ecossistema da organização de possíveis ameaças.



FACULDADE

SEGURANÇA DA INFORMAÇÃO

Cartilha de boas práticas no uso de recursos da faculdade em ambiente presencial e online.



VOCÊ SABE POR ONDE COMEÇAR?

Para garantir a segurança da informação na faculdade, é crucial que todos os membros da comunidade acadêmica estejam cientes de por onde começar. Isso envolve compreender os princípios básicos de segurança cibernética, como a criação de senhas fortes e únicas, atualização regular de softwares e sistemas, a proteção física de dispositivos e cuidados ao clicar em links suspeitos ou compartilhar informações sensíveis.



[SAIBA MAIS](#)



www.faculdade.com.br



123-456-7890



FACULDADE

SEGURANÇA DA INFORMAÇÃO



CREDENCIAIS SEGURAS

Nunca compartilhe suas senhas ou dados de login com ninguém. Altere suas senhas regularmente e evite reutilizá-las.



USO RESPONSÁVEL

Respeite as políticas de uso dos sistemas e rede da instituição. Não acesse ou compartilhe conteúdo ilegal ou inadequado.



AMEAÇAS DIGITAIS:

Esteja atento a e-mails e links suspeitos. Reporte qualquer atividade suspeita.



REDE COM SEGURANÇA

Utilize conexões seguras, evitando redes Wi-Fi públicas para atividades sensíveis. Não compartilhe informações confidenciais em chats ou fóruns não criptografados.



PROTEJA SEU EQUIPAMENTO

Mantenha seu computador e dispositivos móveis atualizados com as últimas correções de segurança. Utilize senhas ou biometria para proteger o acesso aos seus dispositivos.



BACKUP REGULAR

Salve cópias de segurança de documentos importantes em locais seguros. Utilize os serviços de backup oferecidos pela faculdade, se disponíveis.



COMBATE AO BULLYING

Colaboradores devem cumprir o dever de combater a intimidação sistemática (bullying), adotando medidas preventivas e reativas e conscientizando para coibir toda forma de violência na instituição.



PROTEÇÃO CONTRA ACESSO NÃO AUTORIZADO

É obrigação dos colaboradores proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela PSF e mantidas.



DADOS PESSOAIS

Informações envolvendo dados pessoais de colaboradores devem ser tratadas como sigilosas, utilizadas com cautela e apenas por pessoas autorizadas.



REPORTE DE INCIDENTES

Qualquer incidente que possa impactar na segurança das informações deve ser imediatamente reportado pelos colaboradores através do endereço incidentes@matriz.com.br.



ZELO PELO PATRIMÔNIO

O zelo pela proteção do patrimônio da PSF e mantidas é fundamental, incluindo o uso responsável dos recursos físicos e lógicos fornecidos.



LOCAL PARA ARMAZENAMENTO

Todos os colaboradores devem manter as informações da Faculdade armazenadas no local designado para esse fim.

9. Anexo 1 – Política de Segurança da Informação (PSI)

1. INTRODUÇÃO

A Faculdade, com uma sede denominada Matriz e suas duas filiais, reconhece a importância crítica da segurança da informação e da infraestrutura de rede para o êxito de suas operações. Nesse contexto, a implementação de uma Política de Segurança da Rede é fundamental para atender às crescentes necessidades de comunicação e conectividade entre esses locais geograficamente dispersos.

Em resumo, este projeto de Política de Segurança da Rede tem como objetivo garantir eficiência operacional, segurança robusta e escalabilidade, atendendo às necessidades específicas de cada localidade da Faculdade. A integração de tecnologias locais e em nuvem, combinada com um monitoramento contínuo, contribui para uma infraestrutura de rede resiliente e adaptável, pronta para enfrentar os desafios dinâmicos do ambiente acadêmico atual.

2. OBJETIVO

A Política de Segurança da Faculdade tem como objetivo principal estabelecer diretrizes e práticas que assegurem a confidencialidade, integridade, disponibilidade e autenticidade das informações e sistemas críticos da organização. Esta política visa garantir uma proteção eficaz contra ameaças cibernéticas, preservando a continuidade operacional, promovendo a conformidade com regulamentações vigentes e cultivando uma cultura de segurança entre todos os colaboradores.

Para alcançar esses objetivos, a política se concentra nos seguintes pontos:

Proteção dos Ativos de Informação: Salvaguardar ativos de informação, incluindo dados sensíveis e sistemas críticos, por meio da implementação de controles de acesso, criptografia e outras medidas de segurança apropriadas.

Gestão de Acessos: Garantir que o acesso aos recursos de tecnologia da informação seja concedido de maneira criteriosa, com base nos princípios de necessidade mínima e atribuição de privilégios conforme as responsabilidades dos colaboradores.

Monitoramento e Detecção de Ameaças: Implementar sistemas de monitoramento contínuo, para identificar precocemente atividades suspeitas, ataques cibernéticos e outras ameaças à segurança da rede.

Políticas de Uso Aceitável: Estabelecer regras claras e diretrizes para o uso apropriado dos recursos de tecnologia da informação, promovendo a conscientização dos colaboradores sobre boas práticas de segurança.

Gestão de Incidentes: Desenvolver e manter um plano abrangente de gestão de incidentes, definindo procedimentos para uma resposta rápida e eficaz a eventos de segurança, minimizando o impacto e prevenindo recorrências.

Atualizações e Patching: Assegurar que todos os sistemas e softwares sejam regularmente atualizados e que as vulnerabilidades sejam corrigidas de maneira oportuna, reduzindo assim o risco de exploração.

Conformidade com Regulamentações: Manter conformidade com leis, regulamentos e padrões aplicáveis relacionados à segurança da informação, garantindo transparência e responsabilidade da instituição.

Educação e Treinamento em Segurança: Fomentar uma cultura de segurança por meio de programas regulares de treinamento e conscientização, capacitando os colaboradores a reconhecer e mitigar ameaças potenciais.

3. ABRANGÊNCIA

A abrangência inclui, mas não se limita a:

Colaboradores: Todos os funcionários, terceirizados, estagiários e qualquer outra entidade que tenha acesso aos sistemas de informação e recursos da Faculdade.

Instalações: Todas as instalações físicas da Faculdade, incluindo escritórios administrativos e centros de processamento de dados.

Sistemas de Informação: Todos os sistemas, servidores, bancos de dados, aplicativos e plataformas tecnológicas utilizadas para processar, armazenar e transmitir informações.

Redes de Comunicação: A infraestrutura de rede, incluindo equipamentos de rede, roteadores, switches, firewalls e outros dispositivos utilizados para facilitar a comunicação entre as instalações.

Dispositivos de Usuários Finais: Todos os dispositivos de propriedade da Faculdade ou utilizados por colaboradores para acessar os sistemas da organização, como computadores, laptops, tablets e smartphones.

Serviços em Nuvem: Todos os serviços em nuvem utilizados pela Faculdade, que estão integrados à infraestrutura de rede.

Processos de Negócios: Todos os processos operacionais, incluindo aqueles relacionados à produção, logística, recursos humanos, finanças e outras áreas funcionais, que dependem de sistemas de informação e infraestrutura de rede.

4. DIRETRIZES GERAIS

4.1. INTERPRETAÇÃO

4.1.1. TERMINOLOGIA E DEFINIÇÕES

Para uma interpretação uniforme desta Política de Segurança da Faculdade (PSF), são adotadas as siglas, termos e definições especificadas no Apêndice A deste documento.

4.1.2. RESTRIÇÃO DE INTERPRETAÇÃO

Esta PSF deve ser interpretada de forma restritiva. Em situações excepcionais ou não contempladas por suas disposições, a realização de atividades específicas somente é permitida mediante prévia e expressa autorização da gestão superior da Faculdade.

4.1.2.1. EXCEÇÕES E AUTORIZAÇÕES PONTUAIS

Qualquer caso excepcional ou permissão diferenciada será concedido de forma pontual, aplicável exclusivamente ao solicitante, dentro dos limites e motivos que fundamentaram a solicitação. A aprovação destas exceções é uma prerrogativa da Faculdade e ocorrerá por mera liberalidade, com duração limitada. A Faculdade reserva-se o direito de revogar tal autorização a qualquer momento, sem necessidade de aviso prévio, caso julgue necessário.

Estas diretrizes visam garantir uma interpretação consistente da PSF, ao mesmo tempo em que proporcionam flexibilidade controlada para lidar com circunstâncias excepcionais que possam surgir durante a implementação e execução das medidas de segurança.

4.2. PROPRIEDADE

4.2.1. PROPRIEDADE E DIREITO DE USO EXCLUSIVOS:

Todas as informações geradas, acessadas, recebidas, manuseadas ou armazenadas pela Faculdade, assim como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis, são de propriedade exclusiva de cada unidade.

4.2.2. RECURSOS DE TIC PARA ATIVIDADES OPERACIONAIS:

Os recursos de Tecnologia da Informação e Comunicação (TIC) fornecidos pela Faculdade para o desenvolvimento de atividades operacionais, em todas as suas localidades, são de propriedade de cada unidade ou estão a ela cedidos. Permanecem sob sua guarda e posse, devendo ser utilizados exclusivamente para o cumprimento da finalidade a que se propõem.

4.2.3. USO RESTRITO A ATIVIDADES PROFISSIONAIS:

Todos os ativos tangíveis e intangíveis da Faculdade só podem ser utilizados para o cumprimento das atividades profissionais, limitados à função do colaborador.

4.2.4. UTILIZAÇÃO DE MARCAS E IDENTIDADE VISUAL:

A utilização das marcas, identidade visual e demais sinais distintivos da Faculdade, atuais e futuros, em qualquer veículo de comunicação, incluindo internet e mídias sociais, só pode ocorrer para atender a atividades profissionais, mediante prévia e expressa autorização.

4.2.5. MENÇÃO À MARCA EM CONTEXTOS PROFISSIONAIS:

Todos os colaboradores têm o direito de fazer menção à marca em contextos profissionais, citando o local onde trabalham. Contudo, a marca não deve ser utilizada para criar perfis em mídias sociais em nome da instituição e/ou para representá-la sem a devida autorização.

4.2.6. ATIVIDADES PROFISSIONAIS:

Todos os recursos de TIC e informações devem ser utilizados de maneira prioritária para o desenvolvimento de atividades profissionais, promovendo a excelência nas operações e iniciativas relacionadas ao core business da Faculdade.

Esta seção visa preservar a propriedade intelectual e garantir que os recursos tecnológicos e informações sejam direcionados principalmente para atividades profissionais, fortalecendo assim a missão operacional da Faculdade.

4.3. CLASSIFICAÇÃO DA INFORMAÇÃO

4.3.1. RESPEITO A CLASSIFICAÇÃO DA INFORMAÇÃO:

Todos os colaboradores devem respeitar o nível de segurança indicado na classificação das informações. Em caso de dúvida, a informação deve ser tratada como de uso interno, sem divulgação externa, incluindo a internet e mídias sociais, sem autorização expressa.

4.3.2. SIGILO PROFISSIONAL E CONTRATUAL:

É fundamental que todo colaborador respeite o sigilo profissional e contratual, abstendo-se de revelar, transferir, compartilhar ou divulgar informações confidenciais, incluindo detalhes institucionais críticos, de outros colaboradores, fornecedores ou prestadores de serviços.

4.3.3. DADOS PESSOAIS:

Informações envolvendo dados pessoais de colaboradores devem ser tratadas como sigilosas, utilizadas com cautela e apenas por pessoas autorizadas.

4.3.4. MECANISMOS DE CRIPTOGRAFIA:

A equipe de Tecnologia da Informação (GTI) é responsável por homologar mecanismos de criptografia, cifragem ou codificação para o armazenamento e transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou no ambiente de conectividade.

Esta seção destaca a importância do respeito à classificação e sigilo de informações, reforçando as responsabilidades dos colaboradores na proteção de dados confidenciais da Faculdade.

4.4. CONTROLE PARA ACESSO DE COLABORADORES

4.4.1. IDENTIDADE DIGITAL INDIVIDUAL:

Cada colaborador recebe uma identidade digital individual e intransferível para acessar fisicamente e logicamente os ambientes e recursos de Tecnologia da Informação e Comunicação (TIC) da Faculdade.

4.4.1.1. MONITORAMENTO E CONTROLE DA IDENTIDADE DIGITAL:

A identidade digital é monitorada e controlada pela Faculdade.

4.4.1.2. RESPONSABILIDADE DO COLABORADOR

O colaborador é responsável pelo uso e sigilo de sua identidade digital. O compartilhamento, divulgação ou transferência não autorizados são estritamente proibidos.

4.4.2. IDENTIFICAÇÃO NAS DEPENDÊNCIAS FÍSICAS:

Quando a identidade é fornecida pela unidade, todos os colaboradores, prestadores de serviços e visitantes nas dependências físicas da Faculdade devem estar devidamente identificados, portando crachá individual de forma visível.

4.4.2.1. USO INDIVIDUAL DO CRACHÁ

O crachá de identificação é de uso individual e não pode ser compartilhado com outros colaboradores ou terceiros, nem ser utilizado fora das dependências da Faculdade. Tal transgressão pode ser punida de acordo com os artigos 299 (Falsidade Ideológica), 307 (Falsa Identidade) e 304 (Uso de Documento Falso) do Código Penal Brasileiro.

4.4.3. SEGURANÇA FÍSICA DE ÁREAS CRÍTICAS:

A Faculdade deve estabelecer espaços físicos seguros para proteger áreas que criam, desenvolvem, processam ou armazenam informações críticas e ativos essenciais, como datacenters, sala de comunicações, salas de documentação crítica, entre outras.

4.4.4. PROTEÇÃO DE ATIVOS CRÍTICOS:

Ativos críticos para a Faculdade devem ser protegidos contra falhas de energia e outras interrupções, além de receber manutenção adequada para garantir sua contínua integridade e disponibilidade.

Esta seção destaca as diretrizes específicas para o controle de acesso, garantindo a segurança física e lógica dos colaboradores na Faculdade.

4.5. INTERNET PARA COLABORADORES

4.5.1. PROPÓSITO DA CONECTIVIDADE:

Os recursos de conectividade são fornecidos para fins administrativos, reconhecendo o acesso à internet como um direito essencial para o exercício da cidadania no Brasil. No entanto, os colaboradores devem utilizar a internet em conformidade com as leis vigentes, sendo responsáveis pelo cumprimento dessas normas.

4.5.2. ACESSO INDIVIDUAL E RESPONSABILIDADE:

O acesso à internet é concedido aos colaboradores por meio de identidade digital (login e senha) pessoal e intransferível. O titular é o único responsável por suas ações e/ou danos decorrentes do uso da internet.

Esta seção destaca as diretrizes específicas para o uso da internet por colaboradores na Faculdade, ressaltando a responsabilidade individual e a observância das leis em vigor.

4.6. CORREIO ELETRÔNICO PARA COLABORADORES

4.6.1. USO PROFISSIONAL:

A utilização do correio eletrônico corporativo deve limitar-se à execução de atividades profissionais, seguindo as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade.

4.6.2. ACESSO EM DISPOSITIVOS MÓVEIS:

O correio eletrônico corporativo pode ser acessado em dispositivos móveis particulares. No entanto, o acesso fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador, sendo uma prática de liberalidade e/ou conveniência sem requisição prévia da instituição.

4.6.3. USO DE CORREIO ELETRÔNICO PARTICULAR:

A utilização de correio eletrônico particular ou público é permitida apenas para transmissão ou recebimento de conteúdo ou informações particulares, desde que não prejudique as atividades profissionais ou acadêmicas, não cause impactos negativos para outros usuários, não viole a rede corporativa e acadêmica, e não infrinja normas da Faculdade.

4.7. REDE SEM FIO (WI-FI) PARA COLABORADORES

4.7.1. USO ADMINISTRATIVO:

A Faculdade, quando possível, disponibiliza uma rede sem fio (Wi-Fi) nos ambientes autorizados, limitada ao perímetro físico da instituição, destinada a finalidades administrativas.

4.7.2. ACESSO AUTORIZADO:

Acesso à rede sem fio (Wi-Fi) é concedido apenas a colaboradores expressamente autorizados, que devem comprometer-se a fazer uso seguro desse recurso.

4.7.2.1. ACESSO PARA VISITANTES E FORNECEDORES:

Em casos excepcionais, visitantes e fornecedores podem ter acesso à rede sem fio mediante prévia autorização do gestor imediato, da equipe de Tecnologia da Informação (GTI) ou do Comitê de Resposta a Incidentes (CRC).

Esta seção estabelece diretrizes específicas para o uso da rede sem fio por colaboradores, alunos e terceiros na Faculdade, assegurando sua disponibilidade para finalidades administrativas e acadêmicas com controle de acesso autorizado.

4.8. ARMAZENAMENTO DE INFORMAÇÕES PARA COLABORADORES

4.8.1. LOCAL APROPRIADO PARA ARMAZENAMENTO:

Todos os colaboradores devem manter as informações da Faculdade armazenadas no local designado para esse fim.

4.8.2. ARMAZENAMENTO DIGITAL NOS SERVIDORES CORPORATIVOS:

As informações digitais da Faculdade devem ser armazenadas nos servidores da rede corporativa, que possuem controle de acesso e cópia de segurança. Informações físicas devem ser guardadas em locais seguros quando não estiverem em uso, especialmente aquelas relacionadas à identificação de colaboradores.

4.8.3. SOLICITAÇÃO DE REMOÇÃO DE CONTEÚDOS:

A Faculdade deve solicitar o apagamento e/ou a remoção de conteúdos em dispositivos móveis particulares, na internet, em mídias sociais e/ou em aplicativos, sempre que representarem riscos para colaboradores, contrariarem a legislação nacional vigente, prejudicarem o relacionamento ou possam causar danos à instituição.

Esta seção estabelece diretrizes específicas para o armazenamento seguro de informações por colaboradores na Faculdade, resguardando a integridade e a segurança dos dados.

4.9. Mídias Sociais para Colaboradores

4.9.1. Comportamento Seguro nas Mídias Sociais:

Colaboradores devem adotar um comportamento seguro no acesso e utilização das mídias sociais, em conformidade com todos os direitos e deveres estabelecidos pelas políticas da Faculdade.

4.9.2. Participação Institucional Responsável:

A participação institucional do colaborador em mídias sociais, durante o horário de trabalho e a partir do ambiente da Faculdade, deve estar diretamente relacionada à sua função profissional e aos objetivos da Faculdade. O colaborador é responsável por qualquer ação ou omissão resultante de sua postura e comportamento nas mídias sociais.

4.10. CONTEÚDO AUDIOVISUAL PARA COLABORADORES

4.10.1. RESTRIÇÕES AO REGISTRO E COMPARTILHAMENTO:

Não é permitido aos colaboradores tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens da Faculdade, pátios, corredores, banheiros, vestiários ou qualquer outro local pertencente ao perímetro físico, sem prévia autorização.

4.10.1.1. EXCEÇÕES PARA EVENTOS PÚBLICOS:

Exceções são permitidas para eventos administrativos, sociais e/ou esportivos, desde que previamente avisados e autorizados, e o conteúdo não exponha ao ridículo nem gere constrangimento aos envolvidos.

4.10.2. RESTRIÇÕES AO REGISTRO POR COLABORADORES:

Colaboradores devem obter autorização prévia para captar ou reproduzir imagens, vídeos ou sons no ambiente da Faculdade. O registro deve ser utilizado apenas para fins profissionais, com proibição de compartilhamento público, exceto em situações previamente avisadas e autorizadas.

4.10.2.1. EXCEÇÕES PARA EVENTOS AUTORIZADOS:

Exceções são permitidas para eventos administrativos, sociais e/ou esportivos, desde que previamente avisados e autorizados.

4.10.3. RESTRIÇÕES AO CONTEÚDO POR COLABORADORES:

Colaboradores não devem captar, reproduzir ou compartilhar imagens, vídeos ou sons que possam comprometer a segurança, sigilo das informações ou envolvam a imagem de outros colaboradores, visitantes, prestadores de serviço e fornecedores sem prévia autorização, exceto em situações previamente avisadas e autorizadas para eventos públicos.

4.11. USO RESPONSÁVEL DE APLICATIVOS DE COMUNICAÇÃO PARA COLABORADORES

4.11.1. AMBIENTE DE TRABALHO:

Colaboradores da Faculdade devem utilizar aplicativos de comunicação no ambiente de trabalho, seja dentro ou fora dele, por meio de recursos institucionais ou particulares, para compartilhar informações institucionais. Esse uso deve sempre respeitar o sigilo da informação, atender aos requisitos de segurança desta Política e cumprir as leis nacionais em vigor, evitando riscos desnecessários relacionados ao vazamento de informações ou que comprometam a instituição.

4.12. MONITORAMENTO PARA COLABORADORES

4.12.1. REGISTRO E MONITORAMENTO:

A Faculdade realiza o registro e armazenamento de atividades (logs) e monitora seus ambientes físicos e lógicos. Isso inclui a captura de imagens, áudio ou vídeo, visando a proteção do patrimônio, reputação e a segurança daqueles que se relacionam com a instituição.

4.12.2. FINALIDADE DO ARMAZENAMENTO DE DADOS:

O armazenamento dos dados monitorados tem finalidades administrativas e legais, contribuindo para colaborar com as autoridades em investigações quando necessário.

4.12.3. COLABORAÇÃO EM CASOS DE INCIDENTES:

Em casos de incidentes de segurança e eventos que comprometam a integridade física e lógica dos colaboradores, a Faculdade tem a obrigação de fornecer informações ao órgão competente para apuração, quando necessário, contribuindo com a segurança e a integridade de sua equipe.

4.13. CONTRATOS PARA COLABORADORES

4.13.1. ACESSO E PORTE DE DISPOSITIVOS:

O simples porte de dispositivos institucionais e o acesso aos recursos de TIC e/ou informações institucionais, mesmo de forma remota fora do horário normal de expediente, não implicam sobre jornada, sobreaviso ou plantão do colaborador. Essas ações podem ocorrer por ato de liberalidade ou conveniência do próprio colaborador, sem necessidade de expressa e prévia requisição da instituição.

4.13.2. DESLIGAMENTO OU RESCISÃO:

Em casos de desligamento, rescisão contratual ou término do contrato, a equipe de Tecnologia da Informação (GTI) e o Centro de Relacionamento com o Colaborador (CRC) devem desativar todas as identidades digitais do colaborador em todos os sistemas e ambientes da Faculdade.

4.13.2.1. EXCLUSÃO DE INFORMAÇÕES NO DESLIGAMENTO:

No desligamento, o colaborador deve excluir todas as informações e contas da Faculdade disponíveis em seu dispositivo móvel particular, caso tenham sido cadastradas.

4.14. SEGURANÇA DA INFORMAÇÃO PARA COLABORADORES

4.14.1. REPASSE E TRANSMISSÃO DE INFORMAÇÕES:

Ao repassar informações da Faculdade o, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais, os colaboradores

devem agir com cautela. Isso inclui confirmar a identidade do solicitante e a real necessidade do compartilhamento da informação.

4.14.2. CAUTELA NA UTILIZAÇÃO DE RECURSOS ONLINE:

Colaboradores devem exercer cautela ao acessar softwares, informações e conteúdos gratuitos na internet, como aplicativos, músicas, vídeos, trabalhos completos, livros digitais e e-mails com propostas suspeitas, devido ao risco de vetores de ataques criminosos.

4.14.3. SALVAGUARDA E RESTAURAÇÃO DE ARQUIVOS DIGITAIS:

A equipe de Tecnologia da Informação (GTI) e o Centro de Relacionamento com o Colaborador (CRC) devem manter um processo de salvaguarda e restauração dos arquivos digitais críticos para atender aos requisitos operacionais e legais, garantindo a continuidade do negócio em casos de falhas ou incidentes.

4.14.4. DESCARTE SEGURO DE INFORMAÇÕES CONFIDENCIAIS:

Informações confidenciais e recursos de TIC devem passar por procedimentos de destruição que impeçam sua recuperação e o acesso por pessoas não autorizadas quando descartados.

4.14.5. PROTEÇÃO EM CASO DE DESASTRES:

GTI e CRC devem desenvolver estratégias e planos de ação para a proteção de informações e recursos de TIC críticos, garantindo a identificação e preservação adequadas dos serviços essenciais após a ocorrência de desastres.

4.14.6. EDUCAÇÃO CONTINUADA EM SEGURANÇA DA INFORMAÇÃO:

A Faculdade está comprometida em orientar constantemente seus colaboradores sobre o uso seguro das informações e da tecnologia, podendo realizar programas de educação em segurança da informação para aumentar o nível de cultura em segurança na instituição.

5. PAPEIS E RESPONSABILIDADES

5.1. TODOS- DIRETRIZES PARA COLABORADORES NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5.1.1. CONHECIMENTO E DISSEMINAÇÃO DAS REGRAS:

Colaboradores devem conhecer e disseminar as regras e princípios da Política de Segurança da Informação.

5.1.2. PRESERVAÇÃO DE ATIVOS:

É responsabilidade dos colaboradores preservar e proteger os ativos tangíveis e intangíveis da PSF e mantidas contra ameaças, incluindo acesso, compartilhamento ou modificação não autorizados.

5.1.3. PRESERVAÇÃO DE RECURSOS INSTITUCIONAIS:

Colaboradores devem preservar e proteger os recursos institucionais, marca, reputação, conhecimento e propriedade intelectual da PSF e mantidas, especialmente suas informações e conteúdo.

5.1.4. ZELO PELO PATRIMÔNIO:

O zelo pela proteção do patrimônio da PSF e mantidas é fundamental, incluindo o uso responsável dos recursos físicos e lógicos fornecidos.

5.1.5. EVITAR EXPOSIÇÃO DESNECESSÁRIA:

Colaboradores devem evitar a exposição desnecessária de informações, projetos, trabalhos e dependências da PSF e mantidas, incluindo mídias sociais e internet, agindo com responsabilidade no uso de recursos de TIC e informações.

5.1.6. PREVENÇÃO DE INCIDENTES:

A prevenção e redução de impactos gerados por incidentes de segurança da informação são responsabilidades dos colaboradores, garantindo confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

5.1.7. CUMPRIMENTO E ATUALIZAÇÃO:

Colaboradores devem cumprir e manter-se atualizados em relação a esta Política, Regimento Interno e demais Normas de Segurança da Informação da PSF e mantidas.

5.1.8. PROTEÇÃO CONTRA ACESSO NÃO AUTORIZADO:

É obrigação dos colaboradores proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela PSF e mantidas.

5.1.9. COMBATE AO BULLYING:

Colaboradores devem cumprir o dever de combater a intimidação sistemática (bullying), adotando medidas preventivas e reativas e conscientizando para coibir toda forma de violência na instituição.

5.1.10. REPORTE DE INCIDENTES:

Qualquer incidente que possa impactar na segurança das informações deve ser imediatamente reportado pelos colaboradores através do endereço incidentes@matriz.com.br.

5.2. GESTORES E COORDENADORES

5.2.1. ORIENTAÇÃO CONSTANTE:

Gestores e coordenadores devem orientar constantemente suas equipes sobre o uso seguro de ativos tangíveis e intangíveis, e dos valores adotados pela PSF, instruindo-os a disseminar essa cultura entre os demais colaboradores.

5.2.2. RESPONSABILIDADE DELEGADA:

Devem suportar todas as consequências das funções e atividades que delegarem a outros colaboradores.

5.2.3. CUMPRIMENTO DA POLÍTICA

Gestores e coordenadores têm a responsabilidade de assegurar o cumprimento desta Política e de outras regulamentações por parte dos colaboradores sob sua supervisão.

5.2.4. INVESTIGAÇÃO DE INCIDENTES:

Devem participar ativamente da investigação de incidentes de segurança relacionados às informações, ativos e aos colaboradores sob sua responsabilidade.

5.2.5. PARTICIPAÇÃO NO COMITÊ DE SEGURANÇA:

Gestores e coordenadores devem participar, sempre que convocados, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

5.3. COLABORADORES

5.3.1. PRESERVAÇÃO DA VIDA PARTICULAR:

Colaboradores devem ser cautelosos quanto ao excesso de exposição de sua vida particular, preservando informações como rotinas, trajetos e intimidades. É fundamental manter o sigilo profissional nas mídias sociais, contribuindo para a preservação da imagem e reputação da instituição.

5.3.2. COMUNICAÇÃO RESPEITOSA:

Durante a comunicação, seja presencial ou digital, é esperado que os colaboradores usem linguagem respeitosa e adequada. Evitar termos dúbios, interpretações duplas, exposição da intimidade, abuso de poder, perseguição, discriminação ou qualquer forma de assédio moral ou sexual, contribuindo para um ambiente condizente com o contexto estudantil, acadêmico e administrativo.

5.3.3. USO CONSCIENTE DE MÍDIAS SOCIAIS:

No uso de mídias sociais, os colaboradores devem evitar excessos de exposição que possam representar riscos para sua própria imagem e reputação, assim como para a instituição. O equilíbrio na utilização dessas plataformas é essencial para manter um ambiente profissional adequado.

6. DISPOSIÇÕES FINAIS

Este documento deve ser interpretado em conformidade com as leis brasileiras, no idioma português, e em conjunto com outras normas da Faculdade.

Atitudes indevidas, ilícitas ou contrárias a esta Política e outras normas de segurança da informação serão consideradas violações, sujeitas a sanções conforme as políticas internas, contratos e normas da instituição.

A Política de Segurança da Informação (PSI) e demais normas estão disponíveis no Portal da Faculdade ou podem ser solicitadas através do e-mail seguranca@matriz.com.br em caso de indisponibilidade. Para esclarecimentos, dúvidas ou informações adicionais sobre esta Política ou outros procedimentos de segurança da informação, colaboradores podem contatar o e-mail: seguranca@matriz.com.br. Incidentes, infrações ou suspeitas devem ser comunicados imediatamente, pessoalmente ou através do endereço incidentes@matriz.com.br

7. DIRETRIZES GERAIS - DOCUMENTOS DE REFERÊNCIA:

Este documento complementa os Procedimentos, Códigos e Normas de Segurança da Informação da Faculdade e está alinhado com os seguintes padrões e normativas:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Código de prática para controles de segurança da informação;

- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Governança de segurança da informação;
- Norma ISO/IEC 27005:2011 – Tecnologia da informação — Gestão de riscos de segurança da informação;

8. APÊNDICE – SIGLAS, TERMOS E DEFINIÇÕES

PSF: Política de Segurança da Faculdade

GTI: Gerência de Tecnologia da Informação

CRC: Comitê de Resposta a Incidentes

TIC: Tecnologia da Informação e Comunicação

IDENTIDADE DIGITAL: Credencial única e intransferível para acesso aos ambientes e recursos de TIC.

CRACHÁ DE IDENTIFICAÇÃO: Dispositivo individual de identificação utilizado pelos colaboradores.

REDE SEM FIO (Wi-Fi): Infraestrutura para conectividade sem fio, restrita a ambientes autorizados.

LOGS: Registros de atividades, incluindo imagens, áudio ou vídeo, para monitoramento e proteção dos ativos.

SOBREJORNADA: Atividade além do expediente normal.

SIGILO PROFISSIONAL: Dever de não revelar informações confidenciais ou internas.

MÍDIAS SOCIAIS: Plataformas online para compartilhamento de informações, imagens e vídeos.

PLANTÃO: Atividade de prontidão fora do horário normal, requerendo requisição expressa da instituição.

INTIMIDAÇÃO SISTEMÁTICA (BULLYING): Comportamento repetitivo que visa intimidar ou prejudicar.

SOBREAVISO: Disponibilidade para ser chamado ao serviço, além do expediente normal.

10. Referencias

<https://www.pucminas.br/unidade/sao-gabriel/institucional/Paginas/default.aspx>