

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Sistema de Informação

Ana Ramos
Eduardo Passos
Geovanni Cadorin
Markus Machel
Mariana Lima
Moisés Meireles
Thiago Augusto

**PROJETO DA INFRAESTRUTURA DE REDE:
Infraestrutura de rede da empresa agropecuária Rei dos Frangos**

Belo Horizonte
2023

Índice de Tabelas

Tabela 1 - Equipamentos Matriz.....	6
Tabela 2 - Equipamentos Viçosa.....	7
Tabela 3 - Equipamentos Fazenda de Uberaba.....	8
Tabela 4 - Equipamentos Fazenda de Uberlândia.....	9

Índice de Figuras

Figura 1 - Orçamento dos materiais.....	10
Figura 2 - Requisitos de Links.....	11
Figura 3 - Protótipo da Rede.....	12
Figura 4 - Distribuição de IPs.....	14
Figura 5 - Tela inicial Servidor_Matriz.....	16
Figura 6 - Informações do servidor.....	16
Figura 7 - Informações adicionais.....	17
Figura 8 - Papéis e funções Servidor_Matriz.....	17
Figura 9 - Usuários e unidades organizacionais.....	18
Figura 10 - Política de usuários pgbh.....	18
Figura 11 - Tela inicial Estacao01.....	19
Figura 12 - Informações Estacao01.....	19
Figura 13 - Aplicação da política de usuário.....	20
Figura 14 - Site Rei dos Frangos.....	20
Figura 15 - Arquitetura da VPC.....	21
Figura 16 - Estrutura da VPC com Atribuição de Bloco CIDR.....	21
Figura 17 - Configuração de Subredes e Gateways na VPC.....	22
Figura 18 - Grupo de segurança.....	22
Figura 19 - Informações instância.....	23
Figura 20 - Conexão Remota.....	23
Figura 21 - Configurações da instancia.....	24
Figura 22 - Site Rei dos Frangos.....	24
Figura 23 - Importação do appliance.....	26
Figura 24 - Detalhe da configuração da placa de rede de uma VM.....	26
Figura 25 - Execução do appliance.....	27
Figura 26 - Configuração de Servidor Local para Monitoramento com Zabbix.....	27
Figura 27 - Tela de login do Zabbix.....	28
Figura 28 - Tela de configuração host.....	28
Figura 29 - Configuração do Grupo de Segurança com Regras de Entrada (HTTP e RDP) ..	29
Figura 30 - Página de Gráficos no Zabbix	29
Figura 31 - Exemplo de Gráfico de Dados Coletados no Zabbix.....	30
Figura 32 - Exemplo de Gráfico do uso do disco.....	31
Figura 33 - Tela de conexão à instância EC2.....	31
Figura 34 - Configuração de Segurança do Grupo na Instância EC2 para Comunicação com o Servidor Zabbix (Porta 10050 TCP, Restrito ao Endereço IP do Servidor Zabbix).....	32
Figura 35 - Instalação e Configuração do Agente Zabbix com Serviço SNMP na Instância EC2.....	32
Figura 36 - Adição de novo host.....	33
Figura 37 - Gráfico do tráfego de rede.....	33
Figura 38 - Gráficos do uso de memória física e cpu.....	34
Figura 39 - Mapa de rede.....	34

Figura 40 - Cadastro usuário Rei dos Frangos.....	35
Figura 41 - Login Rei dos Frangos.....	36
Figura 42 - Home Page Rei dos Frangos.....	37
Figura 43 - Cadastro de Granja Rei dos Frangos.....	37

Sumário

1- INTRODUÇÃO	6
2- RECURSOS DE REDE.....	6
2.1- A lista de equipamentos necessários encontra-se detalhada nas tabelas abaixo:.....	6
2.2 - Orçamento dos equipamentos.....	9
2.3- Largura de banda.....	11
3- PROTÓTIPO DA REDE.....	11
4- DISTRIBUIÇÃO DOS IPs.....	13
5 - VIRTUALIZAÇÃO LOCAL.....	14
6 - IMPLANTAÇÃO NA NUVEM.....	20
7 - MONITORAMENTO DOS AMBIENTES DE REDE	24
8 – CONFIGURAÇÃO DE SERVIDOR NA NUVEM AWS PARA MONITORAMENTO COM ZABBIX.....	29
9 – DESENVOLVIMENTO DO BACKEND REI DOS FRANGOS.....	34
10 – POLÍTICAS DE SEGURANÇA.....	37
1. INTRODUÇÃO.....	37
2. OBJETIVO.....	37
3. ABRANGÊNCIA.....	38
4. DIRETRIZES GERAIS.....	39
4.1 Interpretação.....	39
4.2 Propriedade.....	40
4.3 Classificação da informação.....	40
4.4 Controle de Acesso para Colaboradores.....	41
4.5 Internet para Colaboradores.....	41
4.6 Correio Eletrônico para Colaboradores.....	42
4.7 Rede sem Fio (Wi-Fi) para Colaboradores.....	42
4.8 Armazenamento de Informações para Colaboradores.....	43
4.9 Mídias Sociais para Colaboradores.....	43
4.10 Conteúdo Audiovisual para Colaboradores.....	43
4.11 Uso Responsável de Aplicativos de Comunicação para Colaboradores.....	44
4.12 Monitoramento para Colaboradores.....	44
4.13 Contratos para Colaboradores.....	44
4.14 Segurança da Informação para Colaboradores.....	45
5. PAPEIS E RESPONSABILIDADES.....	45
5.1 Todos - Diretrizes para Colaboradores na Política de Segurança da Informação.....	45
5.2 Gestores e Coordenadores.....	46
5.3 Colaboradores.....	47
6. DISPOSIÇÕES FINAIS.....	47
7. DIRETRIZES GERAIS - DOCUMENTOS DE REFERÊNCIA:.....	47
8. APÊNDICE – SIGLAS, TERMOS E DEFINIÇÕES.....	48

1- INTRODUÇÃO

O artigo tem como objetivo desenvolver e documentar a infraestrutura de redes para a empresa agropecuária Rei do Frango, uma renomada empresa na produção e pesquisa de frangos de corte. A empresa possui quatro locais principais, incluindo a sede em Belo Horizonte e três fazendas localizadas em Viçosa, Uberaba e Uberlândia.

A infraestrutura de redes proposta visa atender às necessidades específicas da empresa em termos de comunicação e conectividade entre esses quatro locais geograficamente dispersos.

2- RECURSOS DE REDE

Neste capítulo, serão apresentados os recursos de rede, seguindo boas práticas de documentação e explorando todas as ferramentas de maneira minuciosa.

2.1- A lista de equipamentos necessários encontra-se detalhada nas tabelas abaixo:

Tabela 1 - Equipamentos Matriz

MATRIZ (Belo Horizonte)		
Setor	Equipamento	Qtd
Recursos Humanos	WorkStation	10
	Câmera de Segurança	1
Logística e Distribuição	Notebook	10
Financeiro e Contabilidade	Notebook	5
	Câmera de Segurança	2
Comercial	Notebook	10
Pesquisa e Desenvolvimento	Notebook	2
	Câmera de Segurança	3

Jurídico	Notebook	2
T.I	WorkStation	4
	Roteador	1
	Switches	2
	Servidor	1
GERAL	Acess Point	1
	Impressora	1

Tabela 2 - Equipamentos Viçosa

Fazenda Modelo (Viçosa)		
Setor	Equipamento	Qtd
Gerência	workstation	5
	Roteador	1
	Servidor	1
	Switch	1
Geral	Impressora	1
	Acess Point	1
Aviário	Equipamentos IOT	5
	workstation	2
	Câmera de Segurança	4
	Câmera de Produção	20
Estoque	Equipamentos IOT	5
	Workstation	2
	Câmera de Segurança	4

--	--	--

Tabela 3 - Equipamentos Fazenda de Uberaba

Fazenda 2 (Uberaba)		
Setor	Equipamento	Qtd
Gerência	workstation	5
	Roteador	1
	Servidor	1
	Switch	1
Geral	Impressora	1
	Acess Point	1
Aviário	Equipamentos IOT	5
	workstation	1
	Câmera de Segurança	4
Estoque	Equipamentos IOT	5
	workstation	2
	Câmera de Segurança	4

Tabela 4 - Equipamentos Fazenda de Uberlândia

Fazenda 3 (Uberlândia)		
Setor	Equipamento	Qtd
Gerência	workstation	5
	Roteador	1
	Servidor	1

	Switch	1
Geral	Impressora	1
	Acess Point	1
Aviário	Equipamentos IOT	5
	workstation	1
	Câmera de Segurança	4
Estoque	Equipamentos IOT	5
	workstation	2
	Câmera de Segurança	4

Ao analisar as tabelas é possível notar que Belo Horizonte (tabela 1), como a sede, possui requisitos mais diversificados de equipamentos para atender a diversos setores.

As fazendas Viçosa (tabela 2), Uberaba (tabela 3) e Uberlândia (tabela 4) têm necessidades mais focadas em equipamentos IoT para Aviário e Estoque, refletindo a natureza das operações agropecuárias.

A presença de câmeras de segurança é consistente em todas as localidades, indicando um compromisso com a segurança e o monitoramento em todas as instalações.

Em resumo, os contrastes nas necessidades de equipamentos refletem as diferentes funções e operações desempenhadas em cada localidade, com Belo Horizonte atuando como a central de operações e as fazendas tendo requisitos mais específicos relacionados à produção e pesquisa agropecuária.

2.2 - Orçamento dos equipamentos

O orçamento foi meticulosamente elaborado por meio de uma pesquisa exaustiva nas lojas de tecnologia mais confiáveis e renomadas do mercado. Durante

esse processo, buscamos incessantemente pelo melhor custo-benefício, visando garantir que os recursos financeiros da empresa fossem alocados de maneira eficiente e que cada compra refletisse a qualidade e a adequação às necessidades específicas de cada local, seja na matriz em Belo Horizonte ou nas fazendas em Viçosa, Uberaba e Uberlândia. Essa abordagem rigorosa assegura que os investimentos em infraestrutura de TI estejam alinhados com os objetivos da empresa Rei do Frango, garantindo eficiência operacional e suporte às operações em todos os locais. Os dados foram organizados na tabela abaixo.

Item	Valor	Matriz		Fazenda 1		Fazenda 2		Fazenda 3	
		60		40		20		20	
		Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor
Nutanix HPC	20000	1	20000	1	20000	1	20000	1	20000
Estação Dell	5000	43	215000	10	50000	10	50000	10	50000
Roteador CISCO	2000	1	2000	1	995	1	995	1	995
Serial CISCO	1000	3	3000	1	3290	1	3290	1	3290
Switch Dell 24p	2800	1	2800	1	2800	1	2800	1	2800
Cabo UTP CAT6 cx	4500	11.80327869	53114.7541	3.93442623	17704.91803	3.93442623	17704.91803	3.93442623	17704.91803
RJ45 f Cat6	60	60	3600	30	1800	30	1800	30	1800
Patch Cord CAT 6	110	120	13200	60	6600	60	6600	60	6600
Patch Panel CAT 6 GIGALAN	1500	3	4500	1	1500	1	1500	1	1500
Rack 44 U	4500	1	4500	1	4500	1	4500	1	4500
Cx + placa	40	60	2400	40	1600	20	800	20	800
AP Rukus WiFi 6	6500	1	6500	1	6500	1	6500	1	6500
Organizador de Cabo	59	3	177	1	59	1	59	1	59
Impressora	5399	1	5399	1	5399	1	5399	1	5399
Nobreak	4173	1	4173	1	4173	1	4173	1	4173
Mesa + Cadeira	1568	43	67424	12	18816	12	18816	12	18816
		Total	407787.7541	Total	145736.918	Total	144936.918	Total	144936.918

Figura 1 - Orçamento dos materiais

Ao analisar a figura 1 de orçamento de materiais revela algumas tendências e diferenças notáveis nas necessidades de infraestrutura de TI em cada local. Esses contrastes refletem a complexidade das operações da empresa Rei do Frango em locais distintos, com a matriz atuando como o centro de operações principal e as fazendas atendendo a necessidades específicas relacionadas à produção agropecuária.

Em relação aos equipamentos específicos, observa-se que a matriz (figura 01) possui requisitos mais substanciais em alguns aspectos. Por exemplo, a matriz adquiriu um número significativamente maior de estações Dell (43) em comparação com cada fazenda (10). Isso se deve ao fato de a matriz ter uma equipe de trabalho maior, além de atuar como o centro de operações principal.

Em termos de conectividade de rede, todos os locais adquiriram roteadores CISCO, switches Dell 24p e patch cords CAT6 em quantidades semelhantes,

indicando a importância da conectividade confiável em todas as instalações.

No entanto, a quantidade de cabos UTP CAT6 variou consideravelmente, com a matriz adquirindo mais do que as fazendas. Isso reflete diferenças nas necessidades de cabeamento de rede em cada local.

2.3- Largura de banda

A figura abaixo (figura 2) apresenta uma análise detalhada da necessidade de link de internet para as várias ferramentas de rede nas diferentes localidades da empresa, incluindo a matriz e as fazendas.

APPs	LB (kbps)	Matriz		Fazenda 1		Fazenda 2		Fazenda 3		Link Internet	
		60		40		20		20			
		Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB		
Web	100	50	5000	30	3000	20	2000	20	2000	12000	
e-mail	50	40	2000	7	350	6	300	6	300	2950	
Bankline	100	10	1000	2	200	1	100	1	100	1400	
Suporte	80	2	160	3	240	2	160	2	160		
Videoconferência	500	10	5000	2	1000	2	1000	2	1000		
Legacy	30	5	150	2	60	1	30	2	60		
SAP	50	10	500	4	200	2	100	2	100		
	Total	13810	Total	5050	Total	3690	Total	3720		16350	

Figura 2 - Requisitos de Links

Através da análise da figura 2 dos requisitos de link de internet podemos perceber uma distribuição variada das necessidades de largura de banda. A matriz apresenta demandas mais substanciais em várias aplicações, com destaque para o acesso à web, onde requer 5.000 kbps (5 Mbps), e e-mail, com 2.000 kbps (2 Mbps). As fazendas 1 e 2 têm requisitos menores em comparação com a matriz, enquanto a fazenda 3 apresenta os requisitos mais baixos em todas as aplicações.

Essa análise enfatiza a importância de dimensionar adequadamente a capacidade de internet em cada localidade para garantir que todas as aplicações funcionem de maneira eficiente e confiável. Além disso, demonstra a relevância da matriz como o centro das operações com requisitos mais elevados em várias aplicações.

3- PROTÓTIPO DA REDE

A imagem abaixo (figura 3) representa o protótipo da rede desenvolvido no Simulador da Cisco Packet Trace, uma representação visual das configurações e interconexões dos dispositivos de rede planejados para a infraestrutura da empresa Rei do Frango. Essa visualização oferece uma visão detalhada e prática da rede, facilitando a análise, o teste e a otimização das configurações antes da implementação real.

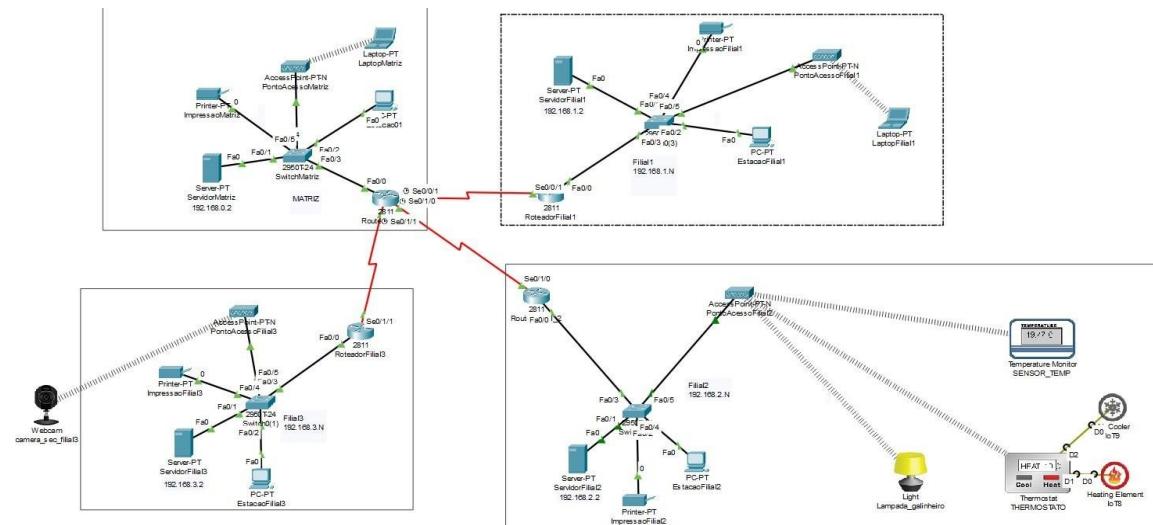


Figura 3 - Protótipo da Rede

Interpretando a figura 3 podemos observar que a topologia em estrela foi adotada, isso ocorre devido ao fato de ser uma escolha altamente adequada para o projeto de redes da empresa Rei do Frango por inúmeras razões cruciais. Primeiramente, essa topologia permite a centralização do controle da rede em um ponto central, tornando a administração e o monitoramento da rede muito mais eficiente. Isso é particularmente valioso para uma empresa com várias localidades, como a Rei do Frango, pois simplifica a gestão da rede.

Além disso, essa topologia é notável por sua facilidade de manutenção. Problemas em dispositivos ou conexões não afetam o funcionamento dos outros dispositivos da rede, facilitando a identificação e isolamento de problemas, o que reduz o tempo de inatividade.

A escalabilidade é outra vantagem importante, pois a topologia em estrela

permite a expansão simples da rede com a adição de novos dispositivos ou localidades, adaptando-se facilmente ao crescimento da empresa.

No contexto das múltiplas fazendas geograficamente dispersas da empresa Rei do Frango, a topologia em estrela se destaca como uma escolha eficaz para gerenciar e conectar todas essas localidades à sede central. Isso promove a eficiência operacional, a segurança e a escalabilidade da rede, atendendo às necessidades específicas da empresa no setor agropecuário.

4- DISTRIBUIÇÃO DOS IPs

A figura 4 abaixo descreve a alocação de endereços IP para dispositivos em diferentes localizações da rede da empresa Rei do Frango. Cada dispositivo possui um tipo específico e uma função designada, juntamente com seu endereço IP exclusivo e localização correspondente. Essa organização permite um controle preciso sobre a rede, identificando claramente a função de cada dispositivo e sua localização geográfica. Isso é essencial para a administração e o gerenciamento eficazes da rede, garantindo que todos os dispositivos estejam configurados corretamente e cumpram suas funções designadas em suas respectivas filiais ou na matriz da empresa.

Uma empresa de agropecuária com sede em uma capital e 3 fazendas espalhadas no interior do estado.					
Dispositivo	Tipo	Endereço IP	Função	Localização	
Roteador_Matriz	ROTEADOR	192.168.0.1	CONEXAO A INTERNET	SEDE / ESCRITORIO CENTRAL	
Servidor_Matriz	Servidor Dell	192.168.0.2	Servidor DHCP	SEDE	
Impressao_Matriz	Impressora	192.168.0.4	Impressão	SEDE	
Estacao01_Matriz	Estacao	192.168.0.6	Estação de trabalho	SEDE	
Ponto_Acesso_Matriz	PONTO DE ACESSO	192.168.0.3	Wi-Fi	SEDE	
Roteador_Filial01	ROTEADOR	192.168.1.1	CONEXAO A INTERNET	Filial 1	
Servidor_Filial01	Servidor Dell	192.168.1.2	Servidor DHCP	Filial 1	
Impressao_Filial01	Impressora	192.168.1.4	Impressão	Filial 1	
Ponto_Acesso_Filial01	PONTO DE ACESSO	192.168.1.3	Wi-Fi	Filial 1	
Roteador_Filial02	ROTEADOR	192.168.2.1	CONEXAO A INTERNET	Filial 2	
Servidor_Filial02	Servidor Dell	192.168.2.2	Servidor DHCP	Filial 2	
Impressao_Filial02	Impressora	192.168.2.4	Impressão	Filial 2	
Ponto_Acesso_Filial02	PONTO DE ACESSO	192.168.2.3	Wi-Fi	Filial 2	
Roteador_Filial03	ROTEADOR	192.168.3.1	CONEXAO A INTERNET	Filial 3	
Servidor_Filial03	Servidor Dell	192.168.3.2	Servidor DHCP	Filial 3	
Impressao_Filial03	Impressora	192.168.3.4	Impressão	Filial 3	
Ponto_Acesso_Filial03	PONTO DE ACESSO	192.168.3.3	Wi-Fi	Filial 3	

Figura 4 - Distribuição de IPs

A distribuição de IPs (figura 4) segue uma organização estruturada e hierárquica, levando em consideração as funções específicas dos dispositivos e suas

localizações geográficas dentro da rede da empresa Rei do Frango.

Na sede central da empresa, conhecida como "Matriz", o Roteador_Matriz (192.168.0.1) atua como ponto de conexão à internet. O Servidor_Matriz (192.168.0.2) desempenha funções de servidor e DHCP, enquanto a Impressora (Impressao_Matriz) utiliza o endereço IP 192.168.0.4 para tarefas de impressão. Além disso, o Ponto de Acesso Wi-Fi (Ponto_Acesso_Matriz) possui endereços IP na faixa 192.168.0.N para oferecer conectividade sem fio na matriz.

Nas filiais, como a "Filial 01", o Roteador_Filial01 (192.168.1.1) faz a conexão à internet, e o Servidor_Filial01 (192.168.1.2) age como servidor e fornece serviços DHCP. A Impressora (Impressao_Filial01) usa o IP (192.168.1.4) para impressão, e o Ponto de Acesso Wi-Fi (Ponto_Acesso_Filial01) disponibiliza conectividade sem fio com endereços IP na faixa (192.168.1.N). A Estacao01_Matriz possui o IP (192.168.0.6) e é designado como estação de trabalho na Matriz.

Na "Filial 02", o Roteador_Filial02 (192.168.2.1) atua como ponto de acesso à internet, e o Servidor_Filial02 (192.168.2.2) desempenha funções de servidor e DHCP. A Impressora (Impressao_Filial02) utiliza o IP (192.168.2.4) para impressão, e o Ponto de Acesso Wi-Fi (Ponto_Acesso_Filial02) (oferece conectividade sem fio com endereços IP na faixa (192.168.2.N). Além disso, o SensorTemp tem o IP (192.168.2.N) e é destinado à monitorização de temperatura no aviário da Filial 02.

Na "Filial 03", o Roteador_Filial03 (192.168.3.1) é o ponto de acesso à internet, e o Servidor_Filial03 (192.168.3.2) atua como servidor e fornece serviços DHCP. A Impressora (Impressao_Filial03) utiliza o IP (192.168.3.4) para tarefas de impressão, e o Ponto de Acesso Wi-Fi (Ponto_Acesso_Filial03) disponibiliza conectividade sem fio com endereços IP na faixa (192.168.3.N). A Cam_sec_filial03 (Câmera de Segurança) usa o IP (192.168.3.N) para fins de segurança na Filial 03.

Essa distribuição meticulosa de IPs é essencial para garantir que cada dispositivo tenha um endereço único e cumpra sua função de maneira eficaz em sua localização específica. Isso facilita a identificação, configuração e gestão de dispositivos em toda a infraestrutura de rede, contribuindo para um ambiente de trabalho organizado e eficiente na empresa Rei do Frango.

5 - VIRTUALIZAÇÃO LOCAL

Realizou-se a virtualização do servidor para simular serviços on-premises,

sendo o principal objetivo criar um servidor com função de controlador de domínio, além de possuir funções de DHCP e atribuição de DNS e por fim adicionar uma estação ao domínio seguindo as políticas estabelecidas. O serviço de virtualização utilizado foi o Virtual Box.

1. Primeiramente, foi instalada uma máquina virtual com o Sistema Operacional Windows Server 2012. Após isso, renomeamos a máquina para o nome do servidor "Servidor_Matriz". Modificamos o IP na seção da interface de rede para ser condizente com a tabela de IPs. Atribuímos a esse servidor as funções de DNS e AD DS, transformando-o em Domain Controller (DC). Em seguida, um nome de domínio raiz foi estabelecido como "ReiDoFrango.local". Adicionalmente, adicionamos a função de DHCP ao servidor para atribuição automática de IPs, conforme ilustrado nas Figuras 5, 6, 7 e 8 abaixo:

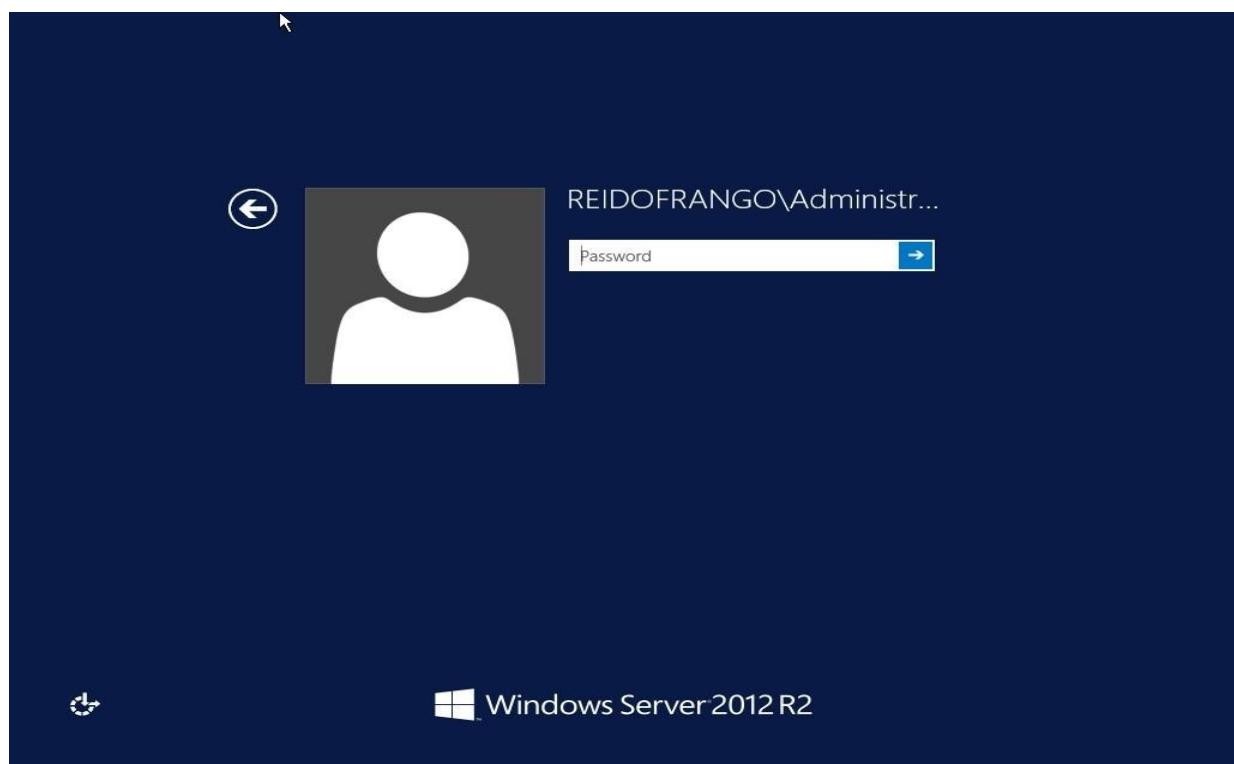


Figura 5 - Tela inicial Servidor_Matriz

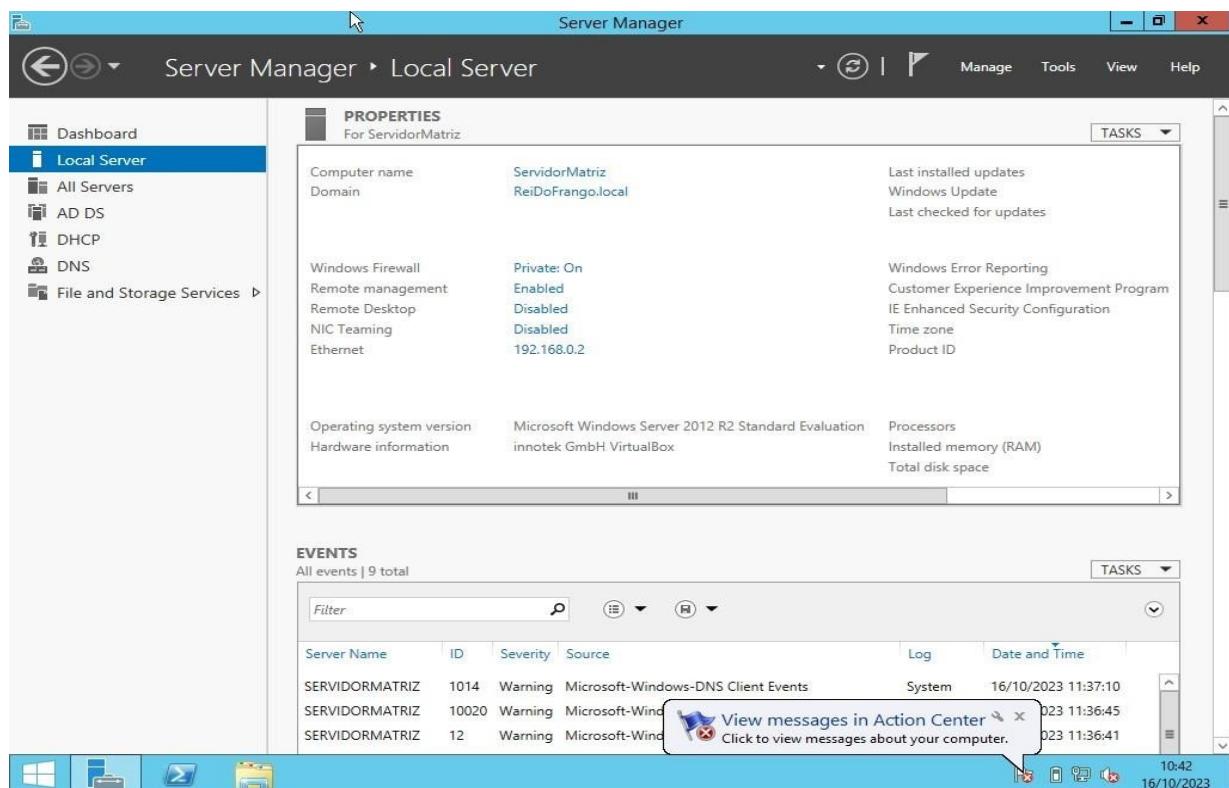


Figura 6 - Informações do servidor

```

Administrator:[C:\Windows\system32\cmd.exe]
C:\Users\Administrator>ipconfigall
'ipconfigall' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator>ipconfig /all
Windows IP Configuration

Host Name . . . . . : ServidorMatriz
Primary Dns Suffix . . . . . : ReiDoFrango.local
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : ReiDoFrango.local

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address . . . . . : 08-00-27-25-33-18
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address . . . . . : 192.168.0.2(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
DNS Servers . . . . . : 192.168.0.200
                           192.168.0.1
                           127.0.0.1
NetBIOS over Tcpip . . . . . : Enabled

Tunnel adapter isatap.{EE897FF2-23D5-490C-A6D5-C8CB58CF75DA}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : Microsoft ISATAP Adapter
Description . . . . . : Microsoft ISATAP Adapter
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

C:\Users\Administrator>_

```

Figura 7 - Informações adicionais

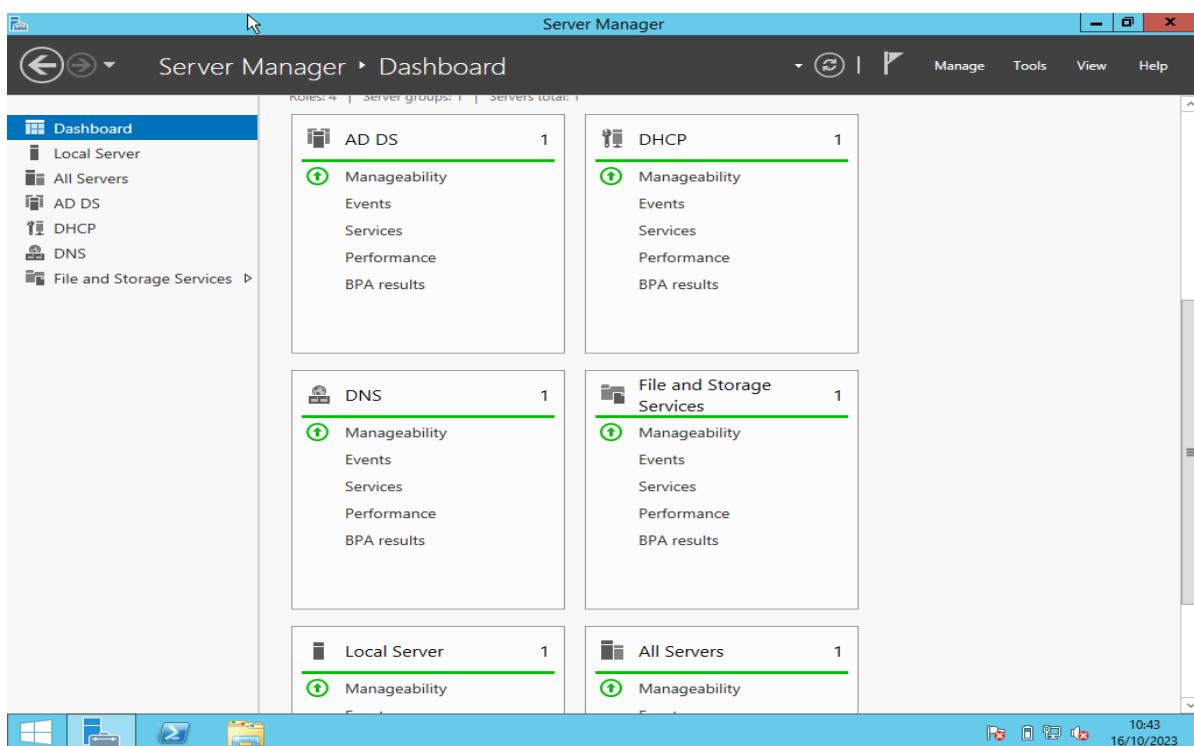


Figura 8 - Papéis e funções Servidor_Matriz

2. Após isso criou-se as unidades organizacionais Minas conforme mostra a figura 9, com as UOs dentro representando a sede Belo Horizonte e as fazendas Viçosa, Brumadinho e Uberaba:

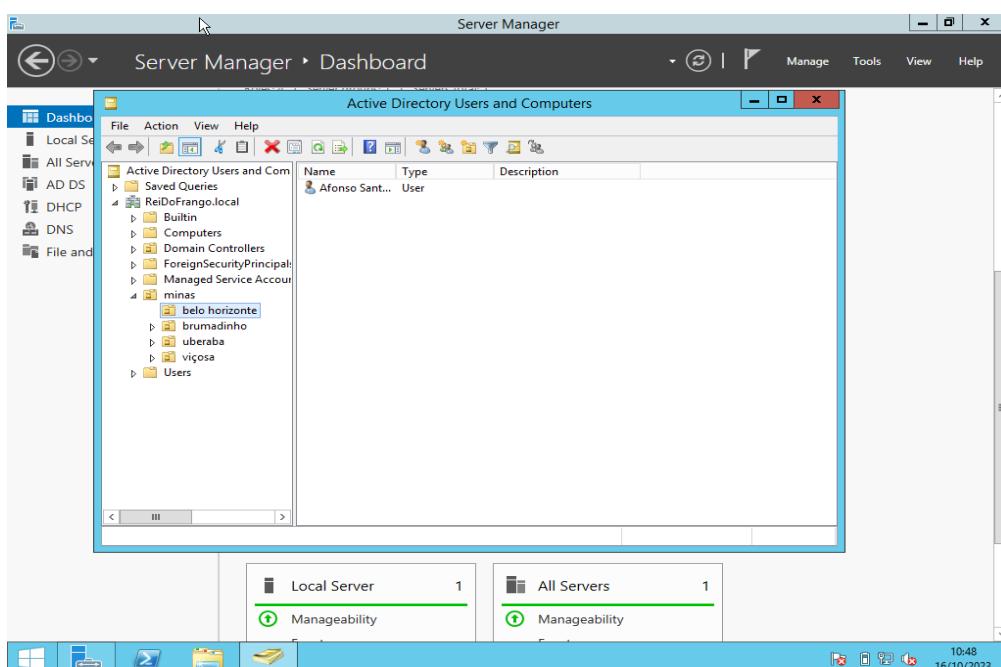


Figura 9 - Usuários e unidades organizacionais

3. Foi criada em belo horizonte a política de usuários pgbh que restringe ações como acessar o painel de controle, desinstalar e deletar programas entre outros demonstrada na figura abaixo:

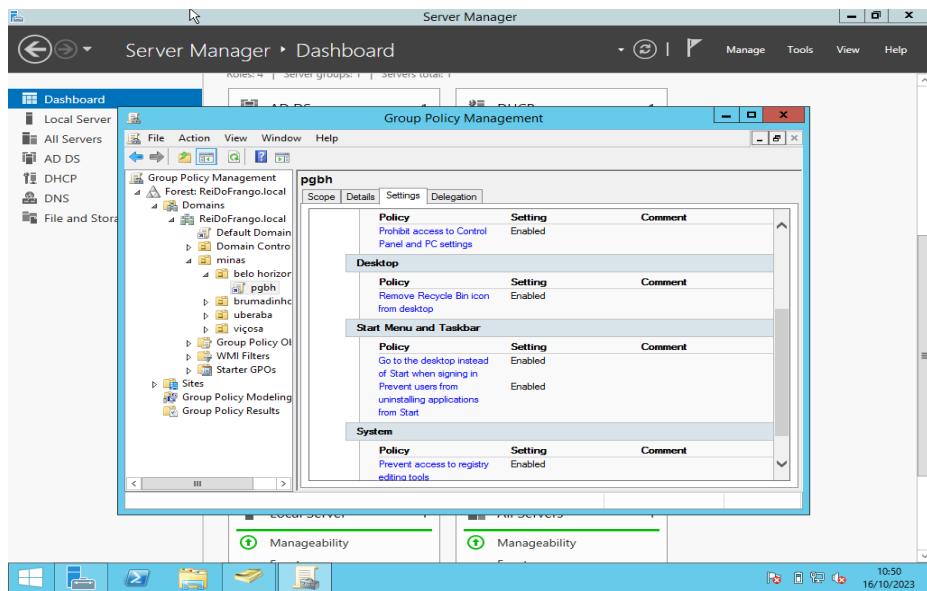


Figura 10 - Política de usuários pgbh

4. Um usuário foi criado na UO de Belo Horizonte. Por fim, adicionou-se uma estação ao domínio e forçamos a aplicação das políticas de usuário estabelecidas. Conectamos à aplicação web do Rei dos Frangos, conforme pode-se observar nas Figuras 11, 12, 13 e 14:

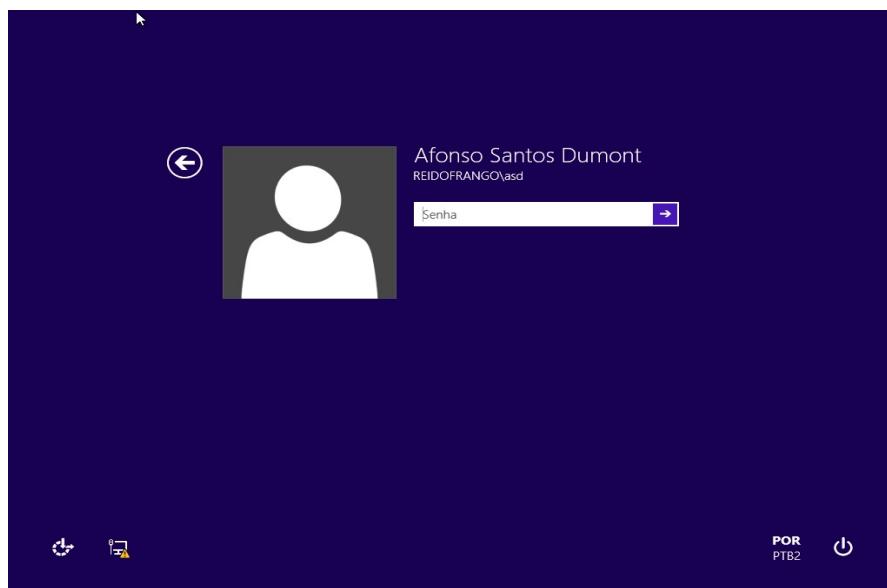


Figura 11 - Tela inicial Estacao01

C:\Windows\system32\cmd.exe

```
Sufixo DNS específico de conexão . . . . . : ReiDoFrango.local
C:\Users\asd>ipconfig /all
Configuração de IP do Windows
  Nome do host . . . . . : Estacao01
  Sufixo DNS primário . . . . . : ReiDoFrango.local
  Tipo de nó . . . . . : híbrido
  Roteamento de IP ativado. . . . . : não
  Proxy WINS ativado. . . . . : não
  Lista de pesquisa de sufixo DNS . . . . . : ReiDoFrango.local
Adaptador Ethernet Ethernet:
  Sufixo DNS específico de conexão. . . . . : ReiDoFrango.local
  Descrição . . . . . : Intel® PRO/1000 MT Desktop Adapter
  Endereço Físico . . . . . : 08-00-27-BB-E6-F0
  DHCP Habilitado . . . . . : Sim
  Configuração Automática Habilitada. . . . . : Sim
  IP V4 . . . . . : 192.168.0.6<Preferencial>
  Máscara de Sub-rede . . . . . : 255.255.255.0
  Concessão Obtida. . . . . : sexta-feira, 9 de setembro de 1982 05:27:52
  Concessão Expira. . . . . : terça-feira, 24 de outubro de 2023 10:56:07
  Gateway Padrão. . . . . : 192.168.0.1
  Servidor DHCP . . . . . : 192.168.0.2
  Servidores DNS . . . . . : 192.168.0.2
  192.168.0.200
  NetBIOS em Tcpip. . . . . : Habilitado
Adaptador de túnel isatap.ReiDoFrango.local:
  Estado da mídia. . . . . : mídia desconectada
  Sufixo DNS específico de conexão. . . . . : ReiDoFrango.local
  Descrição . . . . . : Adaptador do Microsoft ISATAP
  Endereço Físico . . . . . : 00-00-00-00-00-00-E0
  DHCP Habilitado . . . . . : Não
  Configuração Automática Habilitada. . . . . : Sim
C:\Users\asd>
```

Windows 8.1 Pro
Build 9600
POR 11:02
PTB2 16/10/2023

Figura 12 - Informações Estacao01

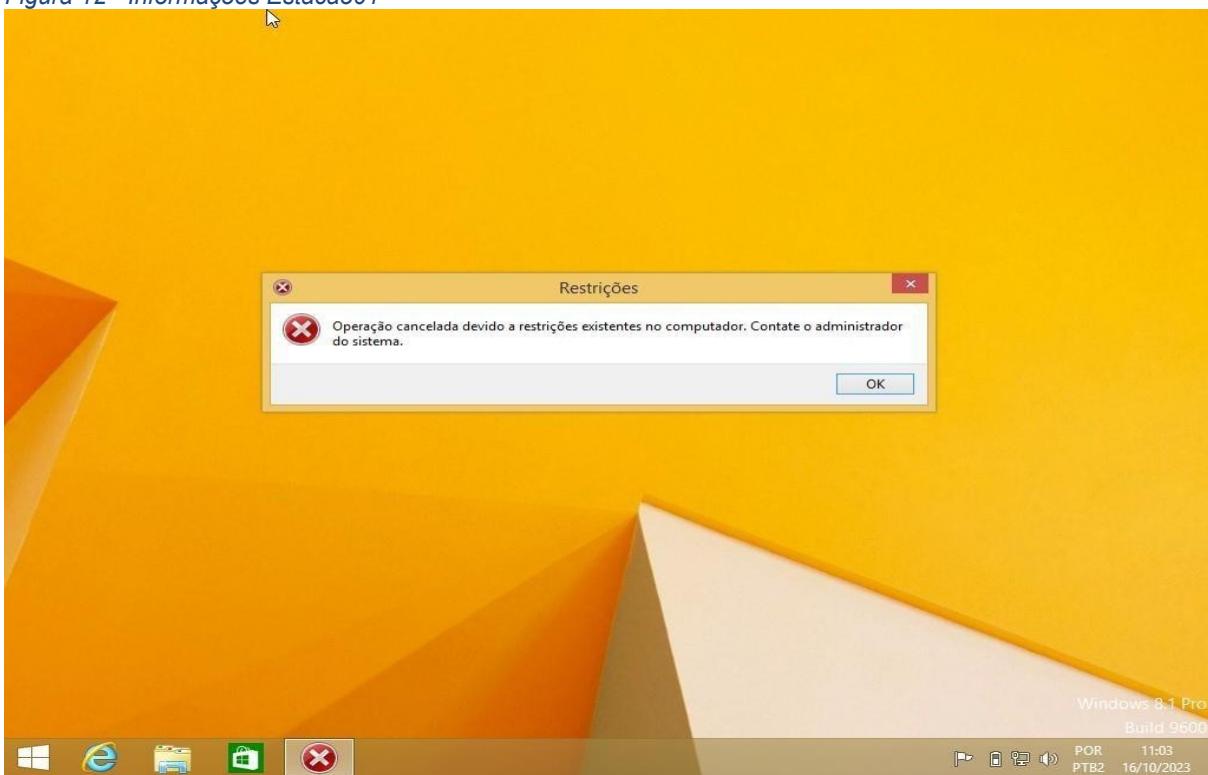


Figura 13 - Aplicação da política de usuário



Figura 14 - Site Rei dos Frangos

6 - IMPLANTAÇÃO NA NUVEM

Após realizar a virtualização local, foi realizada a implantação dos servidores na nuvem através dos serviços da AWS (Amazon Web Services). A implantação foi realizada por meio de uma VPC (Virtual Private Network) para criar uma rede privada na nuvem. A seguinte estrutura (figura 15) foi utilizada como base:

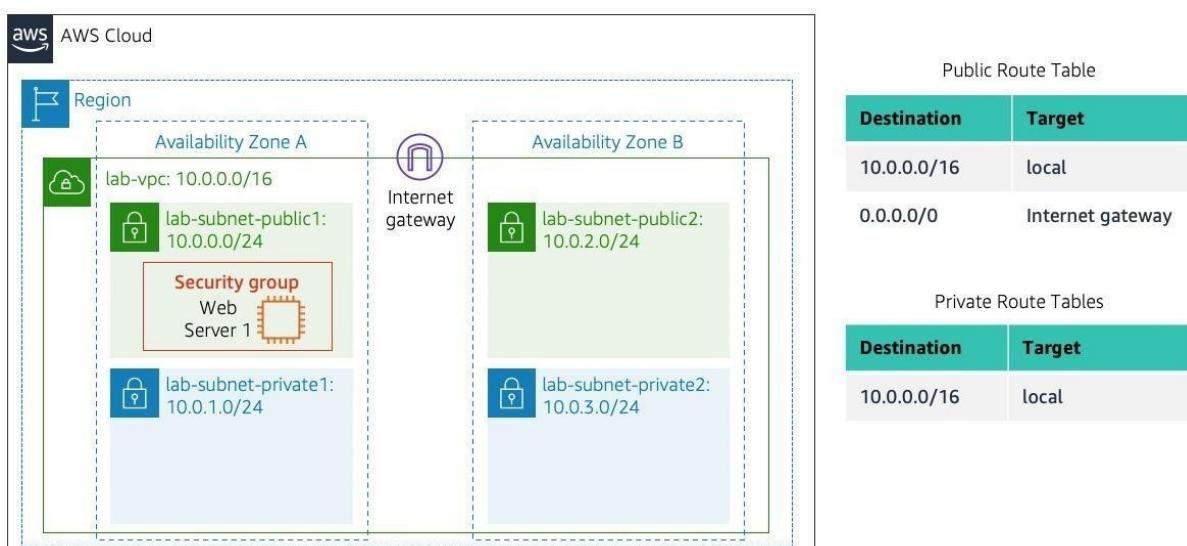


Figura 15 - Arquitetura da VPC

Os seguintes passos foram seguidos:

1. Foi criada uma VPC com um bloco CIDR conforme figura 16:

The screenshot shows the AWS VPC Details page. The top navigation bar includes 'Detalhes', 'Segurança', 'Redes' (selected), 'Armazenamento', 'Verificações de status', 'Monitoramento', and 'Tags'. Under 'Redes', the 'Informações' tab is selected. It displays details like Endereço IPv4 público (3.89.247.181), DNS IPv4 público (ec2-3-89-247-181.compute-1.amazonaws.com), and Sub-rede (subnet-00709b1400b6ec233). The 'Interfaces de rede' section shows one interface (eni-beeca161006) with details such as Endereço IPv4 privado (10.0.0.159), DNS IPv4 privado (ip-10-0-0-159.ec2.internal), and Status (attached).

Figura 16 - Estrutura da VPC com Atribuição de Bloco CIDR

2. Criaram-se as subredes (figura 17). Dentro dessa VPC há duas zonas de disponibilidade com duas subredes cada, sendo uma pública e outra privada. Cada subrede possui sua tabela de rotas para direcionar o tráfego de rede. A subrede pública direciona o tráfego roteável pela internet para o gateway da internet que executa a conversão de endereços de rede para instâncias com endereços ipv4 públicos. Já a subrede privada aponta seu tráfego vinculado à internet para o gateway NAT, que reside em uma subrede pública e faz a conversão de endereços ips privados para um ip público para acesso à internet. No nosso caso, não foi utilizado um gateway NAT.

The screenshot shows the AWS Subnets (4) configuration page. It lists four subnets under the 'Informações' tab. The subnets are: agro-rei-dos-frangos-subnet-public1-us-east-1a (subnet-00709b1400b6ec233), agro-rubens-private-02 (subnet-01eef19b0948239ea), agro-subnet-public-02 (subnet-0e97e47be3d00538a), and agro-rei-dos-frangos-subnet-private1-us-east-1a (subnet-05b6ae1f5be517eaac8f). Each subnet has its status (Available), VPC (vpc-0a5699a1300642602), CIDR IPv4 (e.g., 10.0.0.0/24, 10.0.3.0/24, 10.0.2.0/24, 10.0.1.0/24), CIDR IPv6 (e.g., 250, 251, 251, 251), and Zona de disponibilidade (us-east-1a, us-east-1b, us-east-1b, us-east-1a).

Figura 17 - Configuração de Subredes e Gateways na VPC

3. Após isso, criou-se um grupo de segurança, que funciona como um firewall para as instâncias, controlando o tráfego de entrada e de saída. O grupo de segurança possui duas regras de entrada: HTTP e acesso remoto (RDP) como demonstrado na Figura 18.

sg-Oeed22ea9546d7755 - web server agro

Detalhes

Nome do grupo de segurança sg web server agro	ID do grupo de segurança sg-Oeed22ea9546d7755	Descrição Web Security Group	ID da VPC vpc-0a5699a1300642602
Proprietário 228875960341	Número de regras de entrada: 2 Entradas de permissão	Número de regras de saída: 1 Entrada de permissão	

Regras de entrada [2]

Filtrar regras de grupo de segurança								
	Name	ID da regra do grupo...	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
-	-	sgr-05f538857524162...	IPv4	HTTP	TCP	80	0.0.0.0/0	Acesso ao servidor Web
-	-	sgr-06ef9901d79897ec6	IPv4	RDP	TCP	3389	0.0.0.0/0	Acesso terminal remoto

Figura 18 - Grupo de segurança

4. O servidor web foi implementado através de uma instância EC2 da Amazon. Atribuiu-se um nome à instância e foi escolhido o tipo de instancia e seu par chave-valor associado. A instancia escolhida foi o Windows Server 2016. Foram realizadas as configurações de rede, colocando a instancia na subrede pública da nossa VPC e com ip público automático. A instância seguirá as políticas de segurança estabelecidas, como acesso por http e remoto conforme figura 19:

Resumo da instância para i-03b9a08facfd1a8dc (Servidor Web Agro Rei dos Frangos)

Atualizado há less than a minute

ID de instância i-03b9a08facfd1a8dc (Servidor Web Agro Rei dos Frangos)	Endereço IPv4 público 3.89.247.181 [endereço aberto]	Endereços IPv4 privados 10.0.0.159
Endereço IPv6	Estado da instância Executando	DNS IPv4 público ec2-3-89-247-181.compute-1.amazonaws.com [endereço aberto]
Tipo de nome do host	Nome do DNS de IP privado (somente IPv4) ip-10-0-0-159.ec2.internal	Endereços IP elásticos
Nome do IP: ip-10-0-0-159.ec2.internal	Nome de instância t2.large	Descoberta do AWS Compute Optimizer Opte por participar do AWS Compute Optimizer para obter recomendações. Saiba mais
Nome do DNS do recurso privado de resposta	ID da VPC vpc-0a5699a1300642602 [agro-rei-dos-frangos-vpc]	Nome do Grupo do Auto Scaling
Endereço IP atribuído automaticamente	ID da sub-rede subnet-00709b1400b6ec233 [agro-rei-dos-frangos-subnet-public1-us-east-1a]	
Função do IAM		
IMDSv2 Optional		

Figura 19 - Informações instância

5. Foi feita a execução remota da instancia inserindo as credenciais de acesso como demonstrado na figura 20.



Figura 20 - Conexão Remota

6. A instancia foi configurada para rodar o servidor web conforme figura 21:

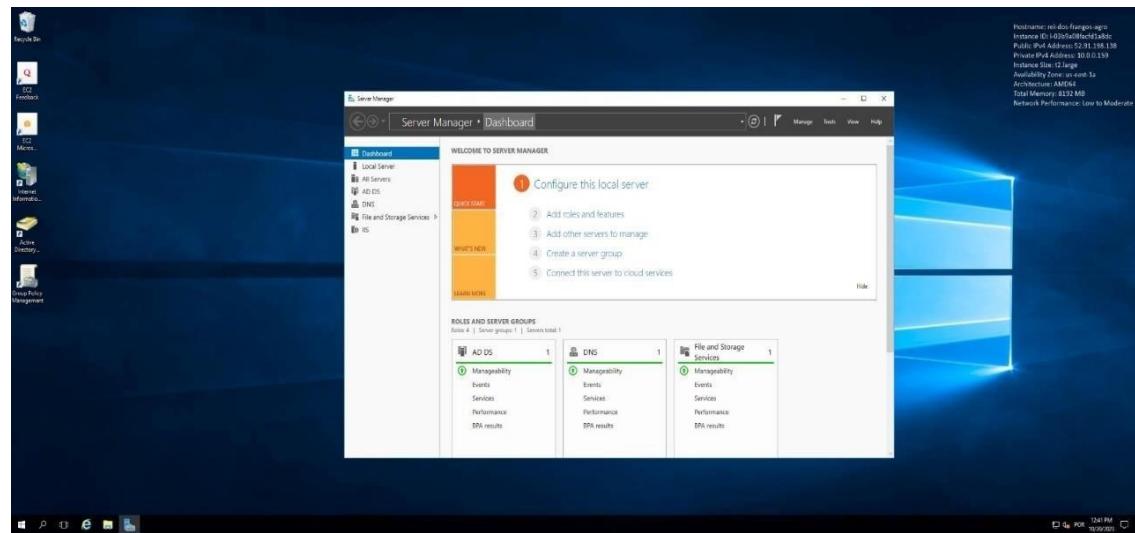


Figura 21 - Configurações da instância

7. Acesso ao site da aplicação Rei dos Frangos através do ip público da instância (figura 22):

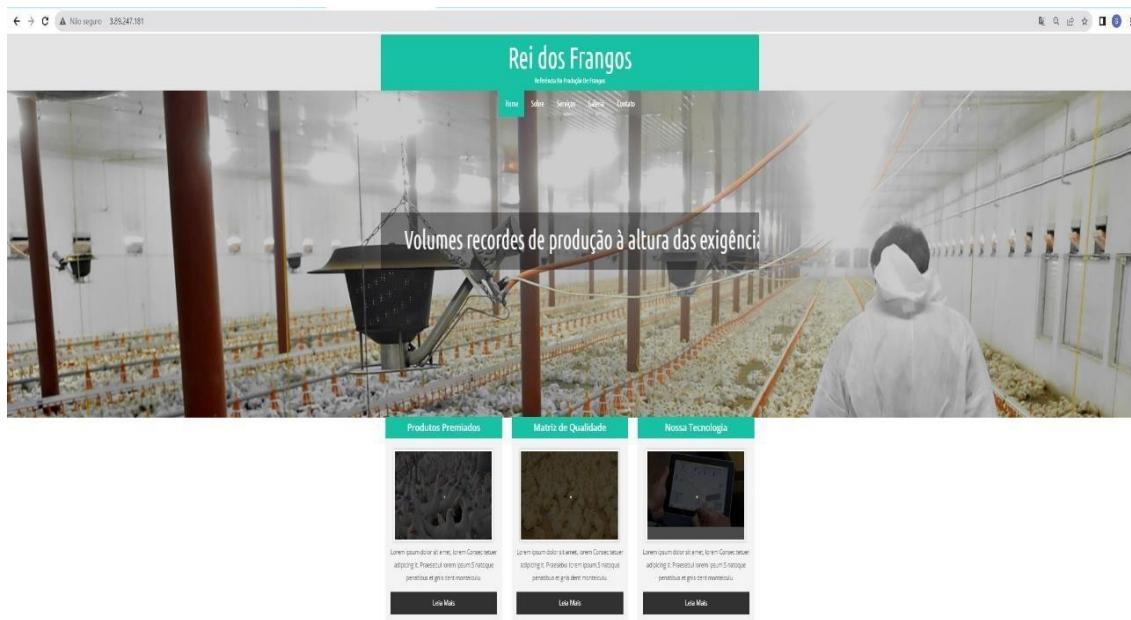


Figura 22 - Site Rei dos Frangos

7 - MONITORAMENTO DOS AMBIENTES DE REDE

Para monitorar os ambientes, será utilizada a ferramenta Zabbix. O Zabbix é uma ferramenta de software versátil que monitora uma grande variedade de parâmetros de rede e a saúde de servidores, máquinas virtuais, aplicações, bancos de dados, websites, entre outros. Ele oferece notificações flexíveis via e-mail para alertas de eventos, possibilitando uma resposta rápida a problemas que afetam os servidores.

Uma característica do Zabbix é sua capacidade de proporcionar recursos robustos para a criação de relatórios e a visualização de dados, com base nas informações armazenadas. Essa funcionalidade torna o Zabbix uma escolha ideal para o gerenciamento de capacidade, permitindo que os administradores monitorem e tomem decisões com base nos dados coletados.

O Zabbix usa principalmente o protocolo SNMP (Simple Network Management Protocol) para monitorar dispositivos de rede, mas também suporta protocolos como ICMP (Internet Control Message Protocol) para monitoramento de conectividade e agentes Zabbix para monitorar sistemas e serviços. Ele opera em uma arquitetura de gerente e agente, no qual o agente coleta os dados localmente e o gerente consolida os dados recebidos gerando relatórios e gráficos. O protocolo SNMP é amplamente utilizado para coletar informações de dispositivos de rede, como roteadores, switches e impressoras.

As seguintes etapas foram seguidas:

1. Configuração do gerente. Foi realizada a importação do appliance do zabbix para o Virtual Box conforme demonstrado na figura 23. O appliance utiliza o

sistema operacional Linux, distribuição CentOS 8 juntamente com o Apache, PHP e MySQL para implementar a ferramenta de gerência. Após importar, configurou-se a placa de rede da máquina para operar em modo bridge, para poder conectar-se a outras máquinas na rede local conforme figura 24:

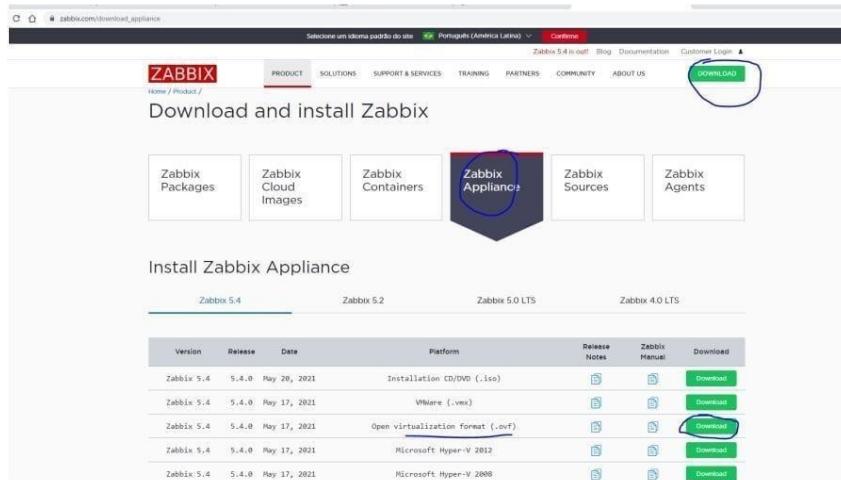


Figura 4. Site de download da imagem Virtual BOX do Zabbix

Figura 23 - Importação do appliance



Figura 24 - Detalhe da configuração da placa de rede de uma VM

2. Execução do appliance representada na figura 25. Após importar o appliance para o virtual box, foi executada a máquina virtual com o appliance e observado o ip obtido.

```

Password:
Last login: Fri Nov  3 18:46:01 on ttys1
*****
Zabbix frontend credentials:
Username: Admin
Password: zabbix

To learn about available professional services, including technical support and training, please visit https://www.zabbix.com/services
Official Zabbix documentation available at https://www.zabbix.com/documentation/current/
Note! Do not forget to change timezone PHP variable in /etc/php-fpm.d/zabbix.conf file.

*****
root@appliance ~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    Link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    Link/ether 08:00:27:9b:4c:60 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 192.168.0.8/24 brd 192.168.0.255 scope global dynamic eth0
        valid_lft 691241sec preferred_lft 691241sec
        inet6 2004:14c:5ba8:9f45:a00:27ff:fe9b:4c60/64 scope global dynamic mngtmpaddr
            valid_lft 86394sec preferred_lft 71994sec
            inet6 fe80::a00:27ff:fe9b:4c60/64 scope link
                valid_lft forever preferred_lft forever
root@appliance ~# 

```

Figura 25 - Execução do appliance

3. Instalação do agente no servidor local. Foi realizada a instalação do serviço de SNMP no servidor local (Servidor Matriz) para responder a consultas SNMP. Através do Server Manager no windows server. O serviço foi configurado com string de comunidade para segurança conforme demonstrado a seguir na figura 26:

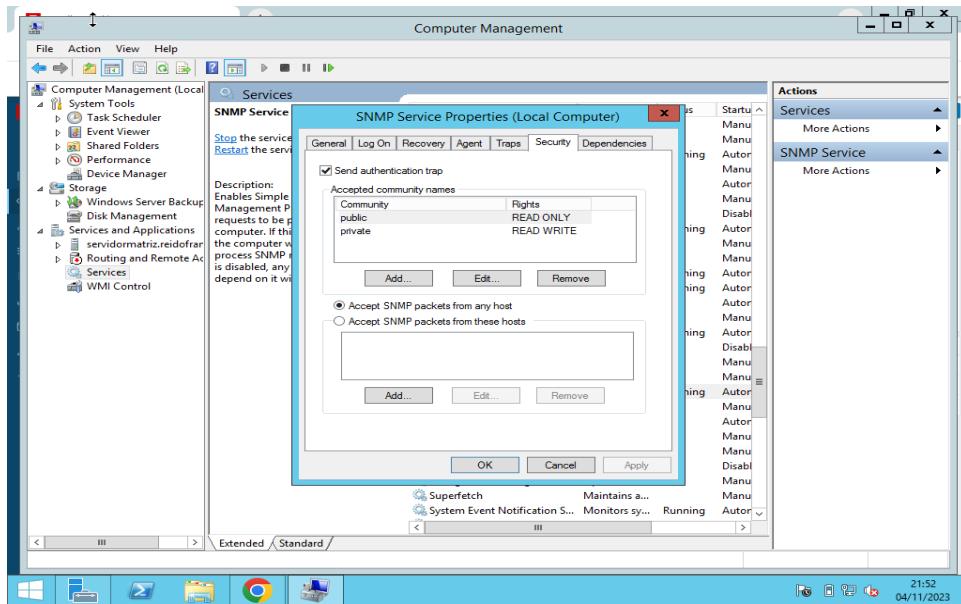


Figura 26 - Configuração de Servidor Local para Monitoramento com Zabbix

4. Acesso via navegador para o ip atribuído ao Zabbix (figura 27), neste exemplo 192.168.0.8. O usuário é Admin e a senha é zabbix.



Figura 27 - Tela de login do Zabbix

5. Adição de hosts. Na tela de configuração, após a tela de login, foi adicionado um host para que o Zabbix Server recolha seus dados. O Host foi configurado de modo a usar interface SNMP e usar a porta 161 para recebimento dos protocolos snmp conforme demonstrado na figura 28.

Figura 28 - Tela de configuração host

6. Conforme figura 29, observa-se a visualização dos hosts. Após adicionar o host, as seguintes telas aparecerão com as cores em verde indicando ausência de erros.

The screenshot shows the Zabbix 6.4.8 interface. At the top, there's a navigation bar with icons for back, forward, search, and other functions. Below it is a message about browser compatibility. The main area is titled 'Hosts' and contains a search bar and filters for Name, Host groups, IP, DNS, Port, Status (Any, Enabled, Disabled), Tags (And/Or, Or), Severity (Not classified, Warning, High, Information, Average, Disaster), and checkboxes for 'Show hosts in maintenance' and 'Show suppressed problems'. A table lists three hosts:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dash
AWS Rei dos Frangos	54.83.166.184:161	SNMP	class: os target: windows	Enabled	Latest data 30	1	Graphs 4	Dash
ServidorMatriz	192.168.0.2:161	SNMP	class: os target: windows	Enabled	Latest data 48	Problems	Graphs 6	Dash
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux	Enabled	Latest data 146	1	Graphs 27	Dash

At the bottom, there's a footer with the Zabbix logo and copyright information, along with a date and time stamp.

Figura 29 - Configuração do Grupo de Segurança com Regras de Entrada (HTTP e RDP)

7. Acesso aos gráficos. Clicando em Graphs pode-se acessar os diversos gráficos disponíveis no zabbix com os dados coletados no agente no servidor local (figuras 30, 31 e 32):

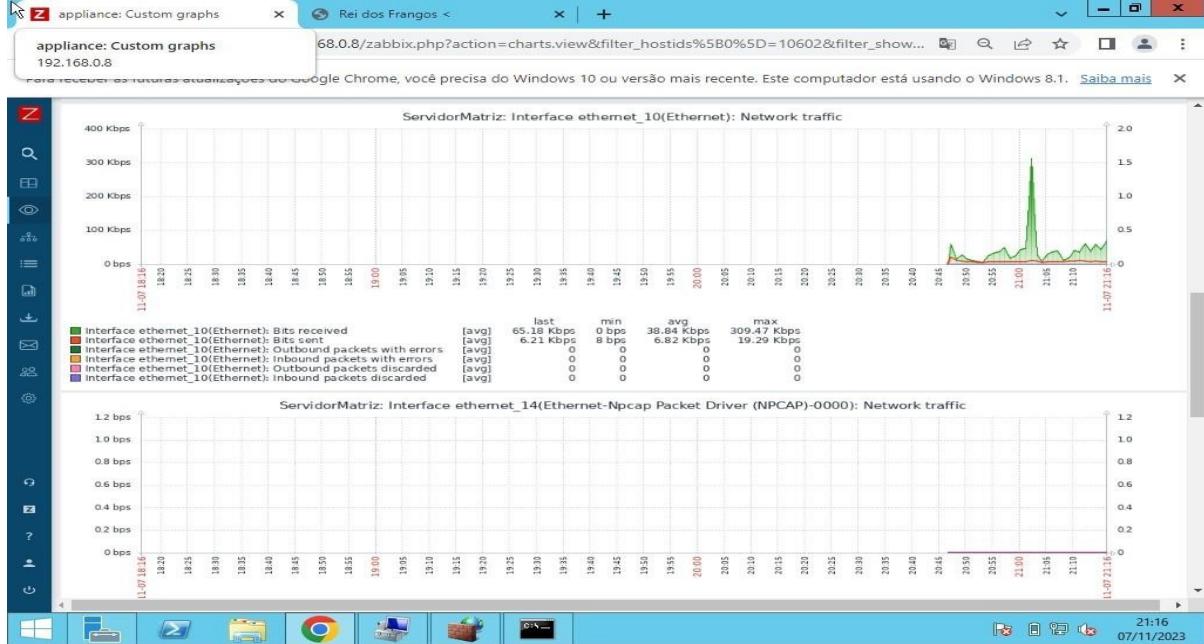


Figura 30 - Página de Gráficos no Zabbix

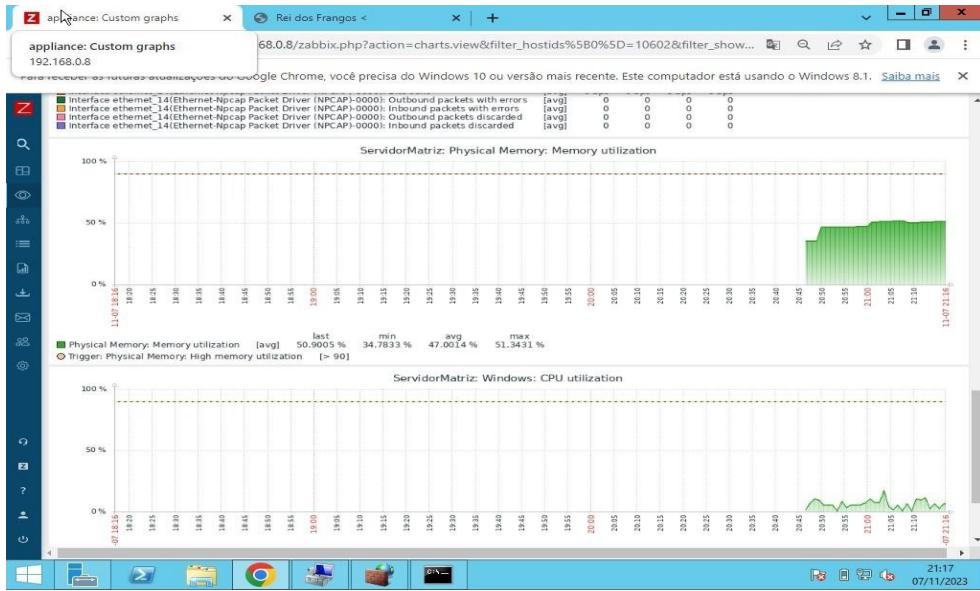


Figura 31 - Exemplo de Gráfico de Dados Coletados no Zabbix

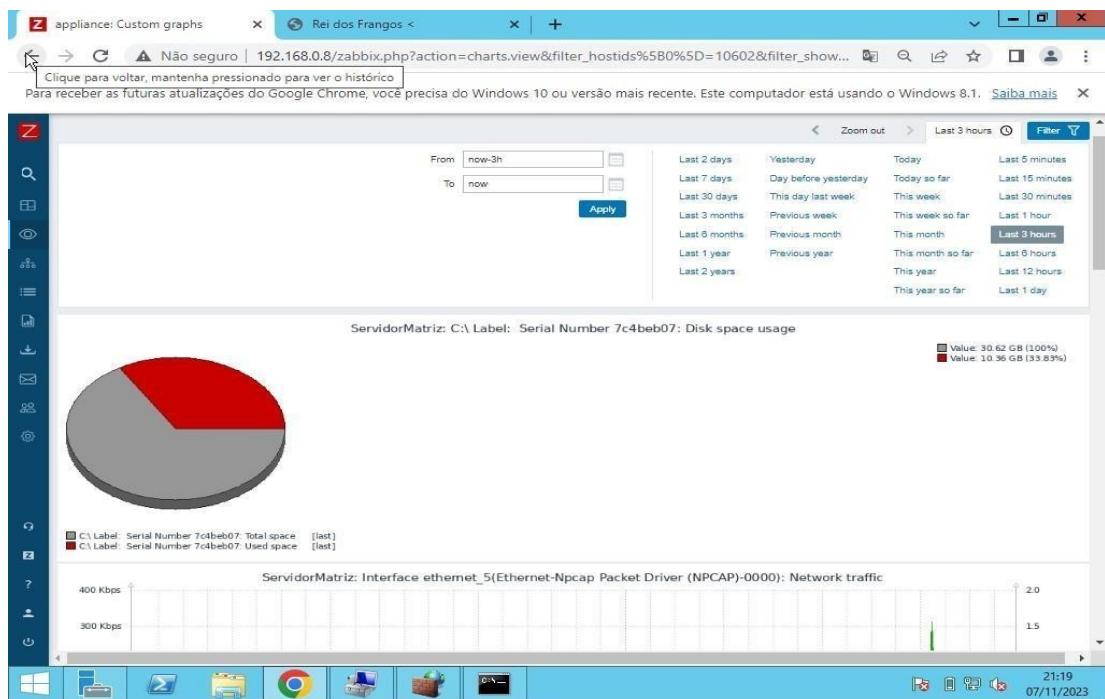


Figura 32 - Exemplo de Gráfico do uso do disco

CONCLUSÃO:

Foi apresentada uma visão da configuração do Zabbix em um servidor local, demonstrando a importância dessa ferramenta de monitoramento na gestão de sistemas e redes. Através de imagens, todo o processo de implantação e configuração do Zabbix pode ser acompanhado.

8 – CONFIGURAÇÃO DE SERVIDOR NA NUVEM AWS PARA MONITORAMENTO COM ZABBIX

INTRODUÇÃO

O objetivo da documentação é fornecer um passo a passo da configuração do servidor na plataforma de nuvem AWS (Amazon Web Services) e a integração desse servidor na rede do Zabbix, uma ferramenta de monitoramento e gerenciamento de sistemas. O Zabbix permite monitorar o desempenho e a disponibilidade de serviços, aplicativos e recursos em tempo real, tornando-o uma escolha ideal para a manutenção de servidores na nuvem.

PRÉ-REQUISITOS PARA CONFIGURAÇÃO:

- Uma conta ativa na AWS.
- Acesso às credenciais da conta AWS.
- Conhecimento básico do Zabbix e sua infraestrutura.
- Uma instância de servidor Zabbix já configurada e em funcionamento.

PASSOS PARA CONFIGURAÇÃO:

1. Acesso à instancia EC2 (figura 33). Foi feito o acesso á instancia EC2 que foi configurada na etapa 6, através do acesso remoto (RDP):



Figura 33 - Tela de conexão à instância EC2

2. Configuração Segurança de Grupo: No passo de configuração da instância EC2, foram definidas as regras de segurança do grupo para permitir a comunicação com o servidor Zabbix. Foi aberta a porta necessária para o Zabbix, geralmente a 10050 TCP, e restringindo o acesso a partir do endereço IP do servidor Zabbix conforme demonstrado em figura 34.

Regras de entrada (4)										
	Name	ID da regra do grupo	Versão do IP	Tipo	Protocolo	Intervalo de portas	Origem		Descrição	
<input type="checkbox"/>	-	sgr-05f588575241d2...	IPv4	HTTP	TCP	80	0.0.0.0/0		Acesso ao servidor Web	
<input type="checkbox"/>	-	sgr-06cf9901d7f897ec6	IPv4	RDP	TCP	3389	0.0.0.0/0		Acesso terminal remoto	
<input type="checkbox"/>	-	sgr-027ad691931cdf679	IPv4	Todos os ICMPs - IPv4	ICMP	Tudo	0.0.0.0/0		ICMP - Ping para Zabbix	
<input type="checkbox"/>	-	sgr-086d9e581a2549...	IPv4	UDP personalizado	UDP	161 - 162	0.0.0.0/0		SNMP - Zabbix	

Figura 34 - Configuração de Segurança do Grupo na Instância EC2 para Comunicação com o Servidor Zabbix (Porta 10050 TCP, Restrito ao Endereço IP do Servidor Zabbix)

3. Instalação do Agente Zabbix na Instância EC2 (figura 35). Foi feita a instalação do serviço de SNMP na instância EC2, que executa o Windows server 2016. Após a instalação o serviço é configurado para permitir a troca de mensagens SNMP.

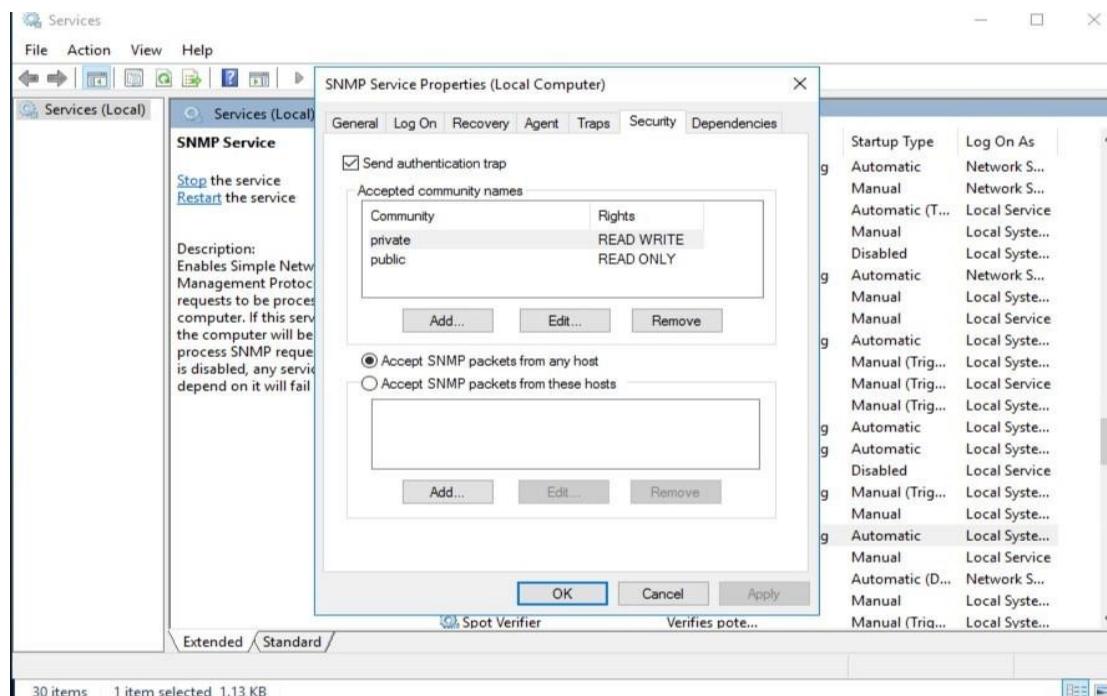


Figura 35 - Instalação e Configuração do Agente Zabbix com Serviço SNMP na Instância EC2

4. Adição e configuração do host no Zabbix: No servidor Zabbix, adicionou-se o novo host representando a instância EC2 conforme figura 36. O Host name configurado (AWS Reis dos Frangos):

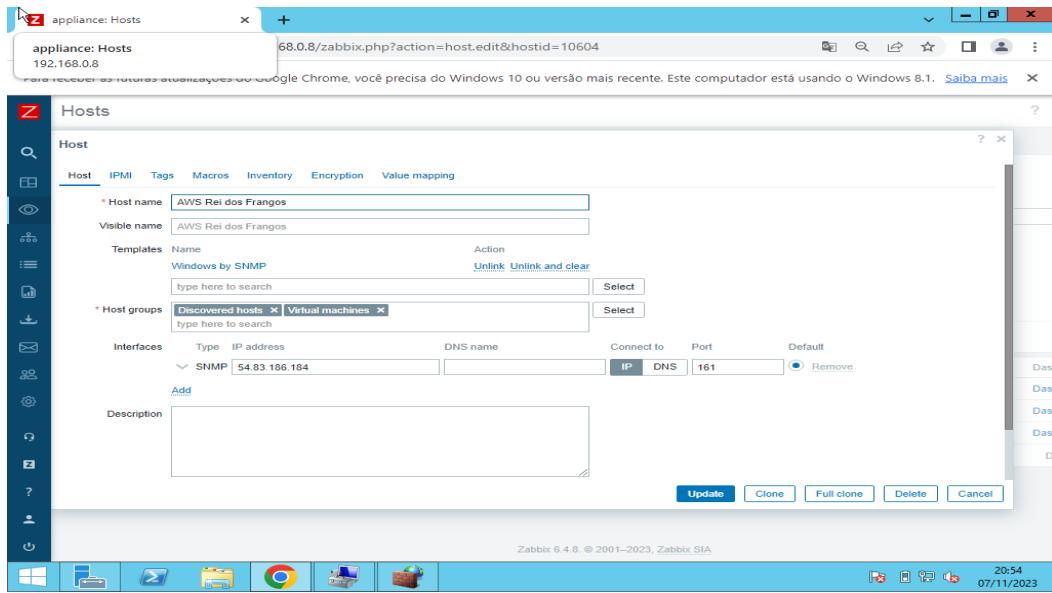


Figura 36 - Adição de novo host

5. Acesso aos gráficos. Clicando em graphs, é disponibilizado diversos gráficos sobre os dados coletados da instância EC2 como as seguintes figuras 37 e 38:

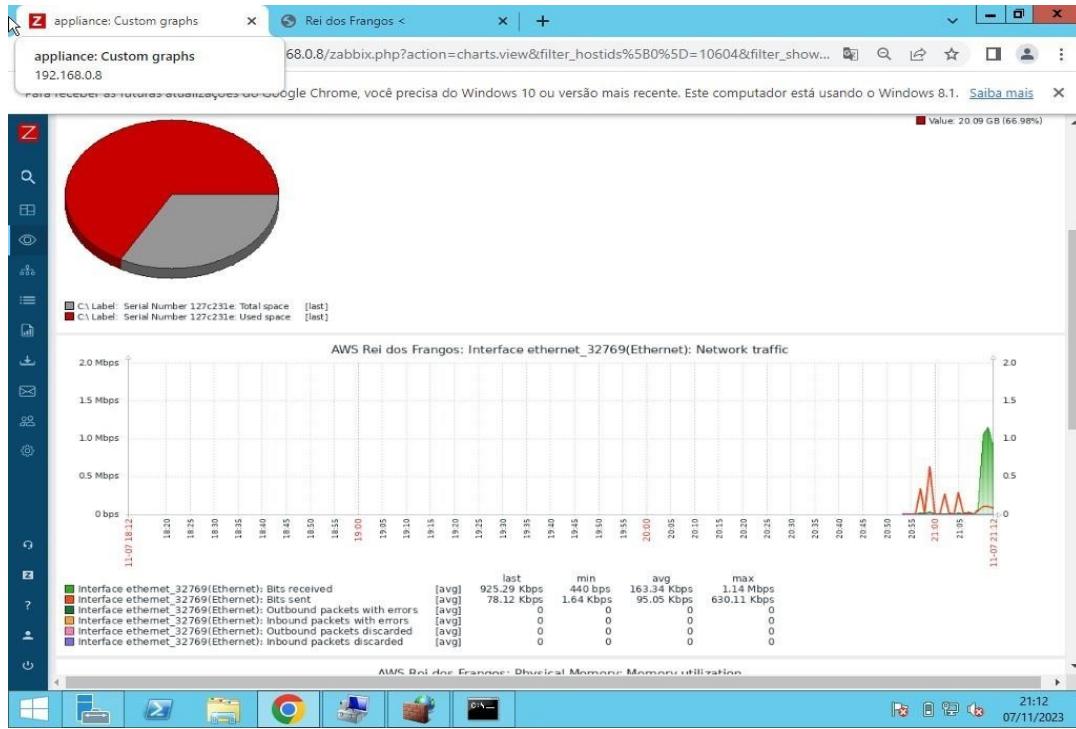


Figura 37 - Gráfico do tráfego de rede

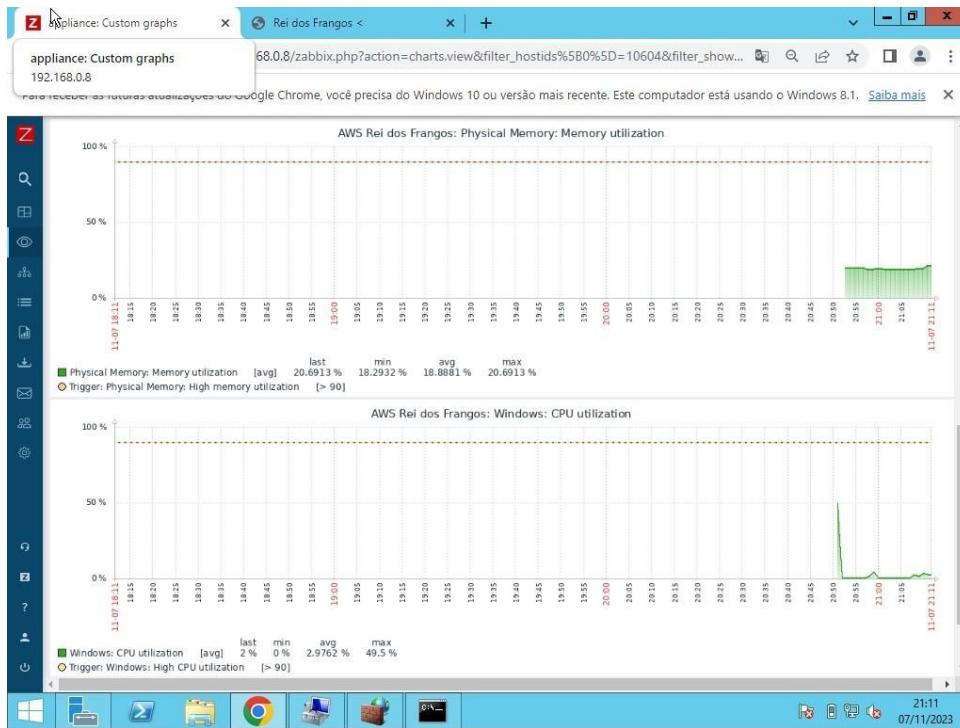


Figura 38 - Gráficos do uso de memória física e cpu

- Foi criado um mapa de rede representando as conexões entre o zabbix server, o servidor local e a instância na nuvem conforme figura 39:

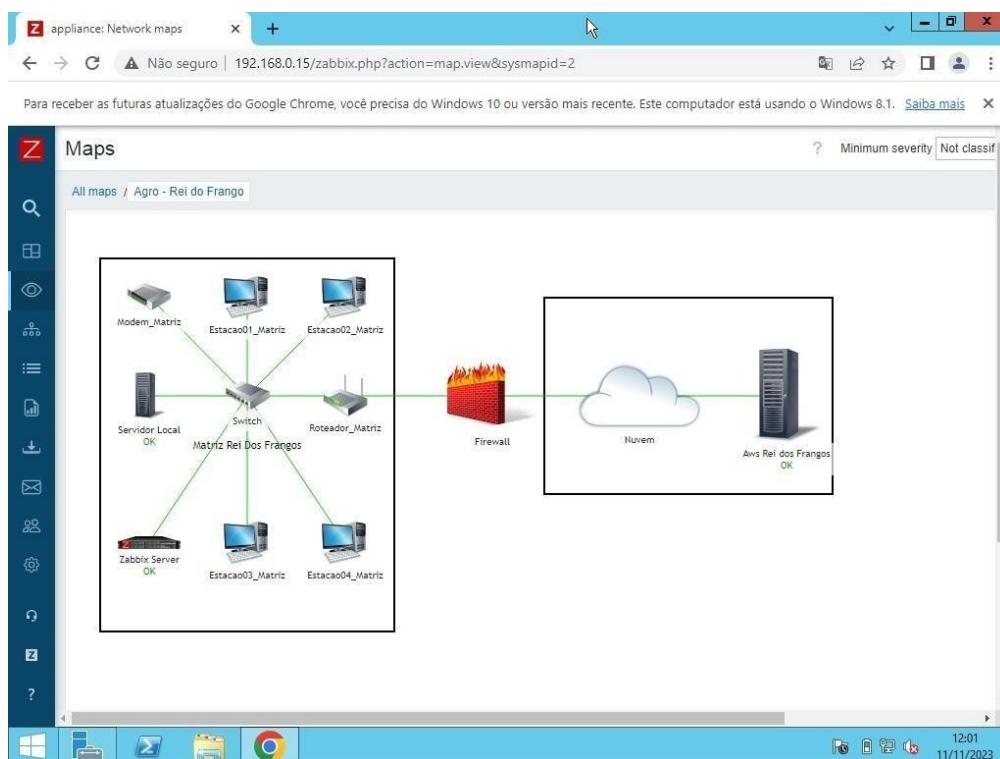


Figura 39 - Mapa de rede

CONCLUSÃO

Após a configuração com sucesso um servidor na nuvem AWS e a integração à rede do Zabbix para monitoramento contínuo. Conclui-se que o processo permitirá que se mantenha um controle detalhado das métricas de desempenho da instância EC2 (servidor virtual na nuvem) e tome medidas proativas para garantir a disponibilidade e o desempenho ideal dos recursos na nuvem.

9 – DESENVOLVIMENTO DO BACKEND REI DOS FRANGOS

O sistema backend do Rei dos Frangos foi cuidadosamente desenvolvido utilizando a linguagem de programação C# e adotando a arquitetura padrão Model-View-Controller (MVC). Essa escolha proporciona uma organização estruturada do código, facilitando a manutenção e escalabilidade do sistema. Além disso, o banco de dados SQLite foi adotado para armazenar os dados de forma eficiente e confiável, pois se trata de uma ferramenta leve e incorporada oferecendo vantagens em termos de simplicidade, desempenho e portabilidade. A combinação dessas tecnologias proporciona ao Rei dos Frangos uma base sólida e eficaz, garantindo um sistema robusto, fácil de manter e capaz de atender às demandas operacionais de maneira eficiente.

No contexto da autenticação no sistema Rei dos Frangos, o processo requer a prévia criação de um usuário, conforme ilustrado na figura 40. Tal procedimento demanda a inserção de informações essenciais, tais como nome, sobrenome, email e uma senha alfanumérica. O sistema verifica se todos os campos estão preenchidos e se a senha atende aos requisitos de segurança. Se um campo estiver vazio ou não atendenda aos requisitos, será exibida uma mensagem informando o erro.

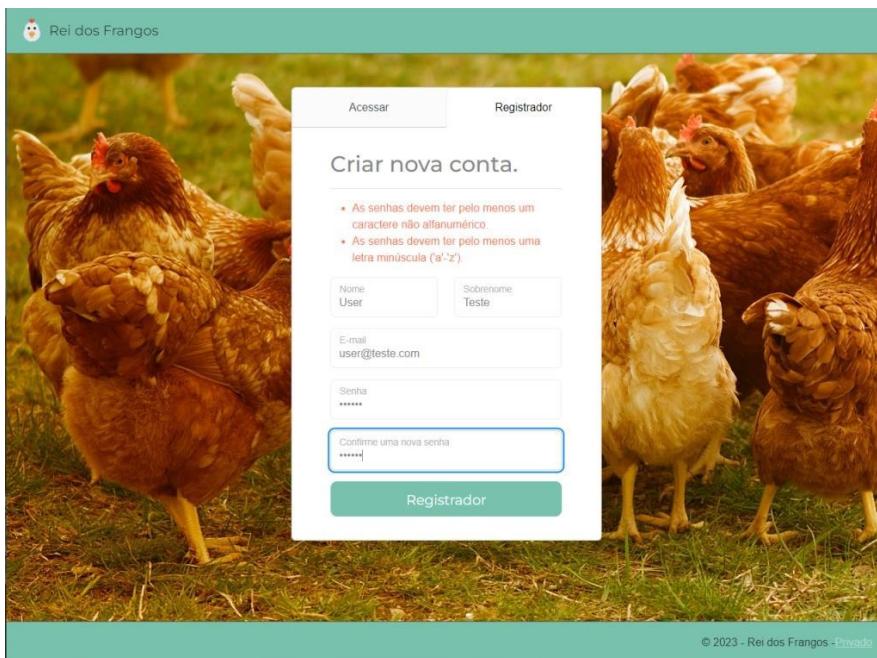


Figura 40 – Cadastro usuário Rei dos Frangos

A Figura 41 apresenta a interface de autenticação do sistema, o usuário é

solicitado a inserir as credenciais previamente cadastradas, compreendendo o email e a senha. Ao acionar o botão de login, a plataforma realiza uma verificação para assegurar a validade dos dados fornecidos. No caso de correspondência, o usuário é então autenticado e recebe a autorização para acessar o sistema.

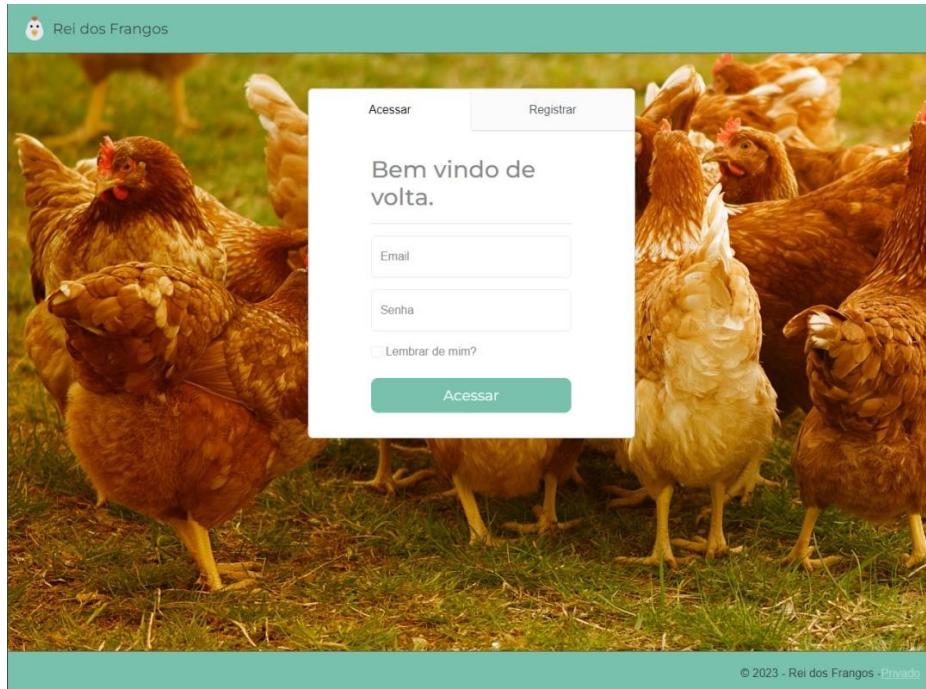


Figura 41 – Login Rei dos Frangos

Por meio da Figura 42, é possível observar a home page do site Rei dos Frangos, que se configura como uma listagem de todas as granjas pertencentes à empresa. Nessa interface, os usuários têm acesso a informações cruciais, como o nome da granja, o estado e município nos quais ela está localizada, além do seu sistema de produção. Destaca-se que, além de uma visualização informativa, os usuários contam com a capacidade de interação direta com a plataforma. Essa interatividade permite abrir a interface para cadastrar uma nova granja, editar informações das granjas já existentes e, inclusive, excluir registros, proporcionando uma administração eficiente e personalizada do conjunto de granjas cadastradas no sistema.

The screenshot shows the home page of the Rei dos Frangos application. At the top, there is a header with the logo 'Rei dos Frangos', the greeting 'Olá user@teste.com!', and a 'Logout' button. Below the header is a large image of chickens in a field. Overlaid on the image is a white modal window titled 'Suas granjas' (Your farms). The modal contains a table with the following data:

Granja	Estado	Município	Sistema de Produção	Ações
Fazenda do Sol	São Paulo	São Bernardo do Campo	Agroecológico	<button>editar</button> <button>apagar</button>
Terra Verde	Minas Gerais	Belo Horizonte	Convencional	<button>editar</button> <button>apagar</button>
Rancho Florido	Bahia	Salvador	Orgânico	<button>editar</button> <button>apagar</button>
Sítio do Céu	Rio de Janeiro	Rio de Janeiro	Agroflorestal	<button>editar</button> <button>apagar</button>
Granja da Serra	São Paulo	São Paulo	Avícola	<button>editar</button> <button>apagar</button>
Ovos de Ouro	Minas Gerais	Belo Horizonte	Produção de Ovos	<button>editar</button> <button>apagar</button>
Frangos Cariocas	Rio de Janeiro	Rio de Janeiro	Criação de Frangos	<button>editar</button> <button>apagar</button>
Pintinhos do Sul	Paraná	Curitiba	Aves Jovens	<button>editar</button> <button>apagar</button>

At the bottom of the modal, there are two small buttons: '1' and '2'. The footer of the page includes the copyright notice '© 2023 - Rei dos Frangos - Privado'.

Figura 42 – Home Page Rei dos Frangos

Como evidenciado na Figura 43, para efetuar o cadastro de uma nova granja, é imprescindível fornecer informações específicas, tais como o nome da granja, o estado e município nos quais está localizada, e o sistema de reprodução adotado. Este processo visa garantir a precisão e a completude dos dados associados a cada granja, contribuindo para uma gestão eficaz e organizada das informações dentro do sistema.

The screenshot shows the 'Adicionar nova granja' (Add new farm) form. The form has fields for 'Nome da Granja' (Farm Name), 'Estado' (State), 'Município' (Municipality), and 'Sistema de Produção' (Production System). At the bottom right of the form are two buttons: 'Fechar' (Close) and 'Salvar' (Save). The background of the form is semi-transparent, showing the same list of farms as in Figure 42. The footer of the page includes the copyright notice '© 2023 - Rei dos Frangos - Privado'.

Figura 43 – Cadastro de Granja Rei dos Frangos

Em síntese, a análise das funcionalidades e interfaces apresentadas anteriormente revela a robustez e a praticidade do sistema desenvolvido para a

empresa Rei dos Frangos. A página inicial, destacada na Figura 42, proporciona uma visão abrangente e informativa de todas as granjas, possibilitando aos usuários acesso a informações cruciais e a interação direta com a plataforma. Já a Figura 43 detalha o processo de cadastro de uma nova granja, enfatizando a necessidade de fornecer informações essenciais para manter a integridade do sistema. A conjugação dessas funcionalidades visa oferecer uma experiência de gestão eficiente e personalizada, contribuindo para a eficácia operacional da empresa Rei dos Frangos.

10 – POLÍTICAS DE SEGURANÇA

1. INTRODUÇÃO

A Empresa Agropecuária Rei do Frango, sediada em Belo Horizonte e com três fazendas estratégicamente localizadas em Viçosa, Uberaba e Uberlândia, reconhece a importância crucial da segurança da informação e da infraestrutura de rede para garantir o sucesso de suas operações. Nesse contexto, a implementação de uma Política de Segurança da Rede torna-se imperativa para atender às crescentes necessidades de comunicação e conectividade entre esses quatro locais geograficamente dispersos.

O desenvolvimento do Protótipo da Rede no Simulador Cisco Packet Trace, adotando a topologia em estrela, representa um passo significativo na busca pela eficiência operacional, segurança e escalabilidade. A distribuição cuidadosa de IPs, estruturada com base nas funções dos dispositivos em cada local, estabelece uma base sólida para o intercâmbio seguro de dados e informações cruciais para as operações diárias.

A inclusão da virtualização local, com a simulação de serviços on-premises através de um servidor virtualizado, e a implantação na nuvem AWS, conectando servidores locais e na nuvem, demonstram a abordagem inovadora e adaptável da Empresa Rei do Frango às demandas tecnológicas em constante evolução.

Essa estratégia híbrida não apenas proporciona flexibilidade, mas também assegura a continuidade operacional em diferentes cenários.

O monitoramento proativo dos ambientes de rede através do Zabbix, utilizando SNMP para coletar dados de dispositivos, representa um compromisso com a segurança e a integridade da infraestrutura. Essa abordagem preventiva, aliada à capacidade de resposta rápida a eventos adversos, reflete o empenho da empresa em manter um ambiente de rede seguro e confiável.

Em síntese, este projeto de Política de Segurança da Rede visa garantir eficiência operacional, segurança robusta e escalabilidade, atendendo às necessidades específicas de cada localidade da empresa Rei do Frango. O uso integrado de tecnologias locais e em nuvem, combinado com um monitoramento contínuo, contribui para uma infraestrutura de rede resiliente e adaptável, pronta para enfrentar os desafios dinâmicos do ambiente empresarial atual.

2. OBJETIVO

O objetivo primordial da Política de Segurança da Empresa Agropecuária Rei do Frango é estabelecer diretrizes e práticas que assegurem a confidencialidade, integridade, disponibilidade e autenticidade das informações e sistemas críticos da organização. Esta política visa garantir a proteção efetiva 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 esse objetivo, a política concentra-se 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, baseado em princípios de necessidade mínima e atribuição de privilégios de acordo com as responsabilidades dos colaboradores.

Monitoramento e Detecção de Ameaças: Implementar sistemas de monitoramento contínuo, como o Zabbix, 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 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 oportunamente, 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 empresa.

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.

Ao alinhar esses objetivos com as características específicas da infraestrutura de rede implementada, a Empresa Rei do Frango busca construir uma postura de segurança resiliente e adaptável, capaz de enfrentar os desafios em constante evolução no cenário de ameaças cibernéticas.

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.

Ao alinhar esses objetivos com as características específicas da infraestrutura de rede implementada, a Empresa Rei do Frango busca construir uma postura de segurança resiliente e adaptável, capaz de enfrentar os desafios em constante evolução no cenário de ameaças cibernéticas.

3. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, prestadores de serviços, sistemas de informação, dispositivos e recursos relacionados à infraestrutura de rede da Empresa Agropecuária Rei do Frango. Abrange todas as operações realizadas nas instalações principais em Belo Horizonte e nas fazendas localizadas em Viçosa, Uberaba e Uberlândia.

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 empresa.

Instalações: Todas as instalações físicas da Empresa Agropecuária Rei do Frango, incluindo escritórios administrativos, centros de processamento de dados, e fazendas em Viçosa, Uberaba e Uberlândia.

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 empresa 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 empresa, como os fornecidos pela AWS, 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.

Esta política se estende a qualquer atividade realizada nos locais mencionados acima, seja por funcionários internos, contratados ou visitantes, com o objetivo de promover uma cultura de segurança da informação e proteger os ativos críticos da Empresa Agropecuária Rei do Frango contra ameaças cibernéticas e garantir a conformidade com regulamentações aplicáveis.

4. DIRETRIZES GERAIS

4.1 Interpretação

4.1.1 Terminologia e Definições

Para uma interpretação uniforme desta Política de Segurança da Empresa Agropecuária Rei do Frango (PSERF), são adotadas as siglas, termos e definições especificadas no Apêndice A deste documento.

4.1.2 Restrição de Interpretação

Esta PSERF 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 Empresa. 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 Empresa Agropecuária Rei do Frango e ocorrerá por mera liberalidade, com duração limitada. A Empresa 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 PSERF, 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 Empresa Agropecuária Rei do Frango, 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 Empresa Agropecuária Rei do Frango 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 Empresa Agropecuária Rei do Frango 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 Empresa Agropecuária Rei do Frango, 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 Empresa Agropecuária Rei do Frango.

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 empresa.

4.3 Classificação da informação

4.3.3 Respeito à 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.

4.3.4 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.

4.3.6 Dados Pessoais:

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

4.3.7 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 Empresa Agropecuária Rei do Frango.

4.4 Controle de Acesso para 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 Empresa Agropecuária Rei do Frango.

4.4.1.1 Monitoramento e Controle da Identidade Digital:

A identidade digital é monitorada e controlada pela Empresa Agropecuária Rei do Frango.

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 empresa 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 Empresa Agropecuária Rei do Frango.

4.4.3 Segurança Física de Áreas Críticas:

A empresa 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 empresa 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 Empresa Agropecuária Rei do Frango.

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 Empresa Agropecuária Rei do Frango, 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 Empresa Agropecuária Rei do Frango.

Esta seção estabelece diretrizes claras para o uso do correio eletrônico por colaboradores, garantindo que sua utilização seja alinhada com as atividades profissionais, e respeite as políticas e normas da empresa.

4.7 Rede sem Fio (Wi-Fi) para Colaboradores

4.7.1 Uso Administrativo:

A Empresa Agropecuária Rei do Frango, 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 na Empresa Agropecuária Rei do Frango, assegurando sua disponibilidade para finalidades administrativas, 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 Empresa Agropecuária Rei do Frango armazenadas no local designado para esse fim.

4.8.2 Armazenamento Digital nos Servidores Corporativos:

As informações digitais da empresa 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 Empresa Agropecuária Rei do Frango 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 Empresa Agropecuária Rei do Frango, 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 Empresa Agropecuária Rei do Frango.

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 empresa, deve estar diretamente relacionada à sua função profissional e aos objetivos da Empresa Agropecuária Rei do Frango. O colaborador é responsável por qualquer ação ou omissão resultante de sua postura e comportamento nas mídias sociais.

Esta seção estabelece diretrizes para o comportamento seguro e a participação institucional responsável de colaboradores nas mídias sociais da Empresa Agropecuária Rei do Frango, assegurando a integridade da instituição e o cumprimento de suas políticas.

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 Empresa Agropecuária Rei do Frango, 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 empresa. 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 Empresa Agropecuária Rei do Frango 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 Empresa Agropecuária Rei do Frango 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 empresa 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 Empresa Agropecuária Rei do Frango.

4.13.2.1 Exclusão de Informações no Desligamento:

No desligamento, o colaborador deve excluir todas as informações e contas da empresa 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 Empresa Agropecuária Rei do Frango, 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 Empresa Rei do Frango 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 de 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 PSERF 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 PSERF e mantidas,

especialmente suas informações e conteúdo.

5.1.4 Zelo pelo Patrimônio:

O zelo pela proteção do patrimônio da PSERF 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 PSERF 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 PSERF 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 PSERF 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.seguranca@reidofrango.com.

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 PSERF, 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 Rei do Frango. 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 Rei do Frango ou podem ser solicitadas através do e-mail seguranca@reidofrango.com 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@reidosfrangos.com.

Incidentes, infrações ou suspeitas devem ser comunicados imediatamente, pessoalmente ou através do endereço incidentes.seguranca@reidofrango.com.

7. DIRETRIZES GERAIS - DOCUMENTOS DE REFERÊNCIA:

Este documento complementa os Procedimentos, Códigos e Normas de Segurança da Informação da Rei do Frango 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

PSERF: Política de Segurança da Informação da Rei do Frango

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.