

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

**Afrânio Jorge Barbosa Campos Filho**

**Gabriel Rodrigues De Lima**

**Mariana Gonzalez das Chagas**

**Vandeir De Souza Cruz**

**Victor Filipe Reis Dias**

**Vinicius Menezes Gomes**

**Projeto da Infraestrutura de Rede: Empresa de Telemarketing**

Belo Horizonte

2023

## **1. Introdução**

Inicialmente, como escopo do projeto deste semestre, foi escolhida hipoteticamente uma empresa de telemarketing com abrangência estadual com atuação em diversos setores econômicos, tendo em vista que as empresas desse ramo usualmente são contratadas por outras para exercer o atendimento à clientes.

A sede fica na capital do Estado de Minas Gerais (BH), tratando-se, portanto, de uma empresa de âmbito estadual. Além da matriz, a empresa continua em expansão na localidade, possuindo atualmente filiais em Governador Valadares, Ouro Preto e Rio Acima. As duas primeiras possuem dimensões do mesmo porte, em que a junção de ambas iguala ao funcionamento da sede em Belo Horizonte. Já a filial de Rio Acima se trata de um novo empreendimento local.

A estrutura organizacional empresarial consistente na ligação direta de cada filial com a sede, entretanto, para evitar supressões de funcionamento em razão da queda de contato com a sede, cada filial, também, possui um servidor para permanecer em funcionamento.

Deste modo, no decorrer deste trabalho, será explicitado o projeto de infraestrutura das redes das empresas e quais as escolhas de equipamentos para o seu funcionamento.

## 2. Links

Neste tópico, será abordado os links disponibilizados para cada unidade da empresa de telemarketing, como é observado na tabela a seguir:

		Matriz (BH)		Filial 1 (Gov. Valadares)		Filial 2 (Rio Acima)		Filial 3 (Ouro Preto)		Link Internet
		500		250		100		250		
APPs	LB (kbps)	Qtde	LB	Qtde	LB	Qtde	LB	Qtde	LB	
Web	100	450	45000	225	22500	90	9000	225	22500	99000
e-mail	50	400	20000	200	10000	80	4000	200	10000	44000
Suporte	80	250	20000	125	10000	50	4000	125	10000	
Videoconferência	500	25	12500	12	6000	5	2500	12	6000	
Legacy	30	50	1500	25	750	10	300	25	750	
SAP	50	50	2500	25	1250	10	500	25	1250	
SAC	100	500	50000	250	25000	100	10000	250	25000	110000
				Total	50500	Total	20300	Total	50500	
				M-F1		M-F2		M-F3		253000

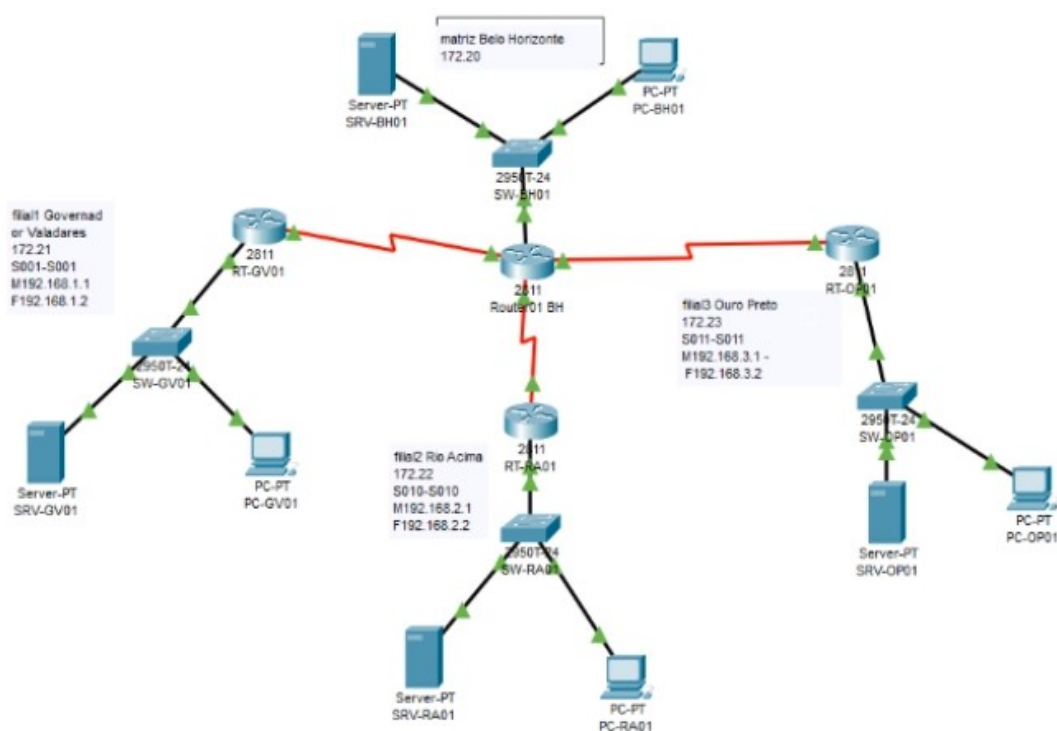
Em razão da atividade econômica desempenhada pela empresa, os links de “Web” e “SAC” são os mais importantes e de maior intensidade, já que os atendimentos são realizados pelo sistema da empresa, sem a necessidade da utilização de linha telefônica, visto que são feitas utilizando a internet. Quanto ao “SAC”, como os clientes, normalmente, estão resolvendo situações que demandam soluções, o acesso ao sistema interno com informações e guias se torna medida essencial para a manutenção da atividade.

Em relação aos demais, indique-se que o link de videoconferência é restringido, apenas, para os cargos de direção/supervisão, pois são esses em que as reuniões são mais frequentes, não existindo a necessidade de deslocamento presencial dos envolvidos.

Por fim, como já explicado anteriormente, os links das filiais estão ligados diretamente com a capital, não ocorrendo interligação entre eles. A escolha desta configuração de funcionamento consiste em evitar o número de eventuais interrupções de funcionamento em razão de problemas em determinado ponto da corrente. Logo, como as unidades desempenham atividades independentes entre si, não é vislumbrado a interrupção total do funcionamento da empresa.

### 3. Cisco Packet Tracer

Neste tópico, será explicitado uma simulação da rede da empresa utilizando o Cisco Packet Tracer, como é observado na imagem a seguir:



Conforme exposto anteriormente, cada filial (além da matriz) possui um servidor ligado a um Switch que, por consequência, estará ligado a um roteador. Este roteador (em cada filial) manterá um link com o roteador da sede. Na sede, também, terá um servidor.

Como pode ser observado na imagem retirada da plataforma Cisco Packet Tracer, percebe-se que os equipamentos foram renomeados com a sigla de cada localidade, para facilitar a identificação do equipamento correto na rede empresarial, sendo determinada as seguintes siglas: **Matriz - BH** – Belo Horizonte; **Filial 1 - GV** – Governador Valadares; **Filial 2 – RA** – Rio Acima; e **Filial 3 – OP** - Ouro Preto.

Além disso, foi adotado o seguinte padrão **XX-YYWW**, onde **XX** é a sigla do equipamento utilizado (SRV – Servidor; SW – Switch; RT – Router; PC – Computador

Pessoal), YY é referente à unidade da empresa (conforme siglas supracitadas) e WW é a numeração correspondente ao equipamento determinado. Deste modo, tem-se o seguinte exemplo: SRV-BH01 é a sigla que corresponde ao servidor 01 da matriz (Belo Horizonte) da empresa.

Na tabela existente no tópico anterior, é verificado que a sede possui 500 (quinhentas) estações de trabalho (com faixa de IP 172.20). Já nas filiais de Governador Valadares e Ouro Preto é identificado, em cada uma, 250 (duzentas e cinquenta) estações de trabalho (com faixa de IP M192.168.1.1/F192.168.1.2 e M192.168.3.1/F192.168.3.2, respectivamente). Finalmente, na unidade de Rio Acima, com 100 (cem) estações de trabalho, é utilizada a faixa de IP M192.168.2.1/F192.168.2.2.

#### 4. Equipamentos

Neste tópico, demonstrada a escolha de tipo, quantidade e valor de cada equipamento necessário para o funcionamento de todas as unidades da empresa de telemarketing, como é observado na tabela a seguir:

Item	Valor	Matriz		Filial 1		Filial 2		Filial3	
		500	250	100	250	Qtde	Valor	Qtde	Valor
Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor	Qtde	Valor
Nutanix HPC	R\$ 14.272,87	1	R\$ 14.272,87	1	R\$ 14.272,87	1	R\$ 14.272,87	1	R\$ 14.272,87
Estação Dell	R\$ 2.949,00	500	R\$ 1.474.500,00	250	R\$ 737.250,00	100	R\$ 294.900,00	250	R\$ 737.250,00
Roteador CISCO	R\$ 30.758,90	1	R\$ 30.758,90	1	R\$ 30.758,90	1	R\$ 30.758,90	1	R\$ 30.758,90
Serial CISCO	R\$ 2.376,00	4	R\$ 9.504,00	4	R\$ 9.504,00	4	R\$ 9.504,00	4	R\$ 9.504,00
Switch Dell 24p	R\$ 14.939,82	21	R\$ 313.736,22	11	R\$ 164.338,02	5	R\$ 74.699,10	11	R\$ 164.338,02
Cabo UTP CAT6 cx	R\$ 4.896,77	83	R\$ 406.431,91	42	R\$ 205.664,34	17	R\$ 83.245,09	42	R\$ 205.664,34
RJ45 f Cat6	R\$ 60,25	502	R\$ 30.245,50	252	R\$ 15.183,00	102	R\$ 6.145,50	252	R\$ 15.183,00
Patch Cord CAT 6	R\$ 27,00	1004	R\$ 27.108,00	504	R\$ 13.608,00	204	R\$ 5.508,00	504	R\$ 13.608,00
Patch Panel CAT 6	R\$ 229,99	21	R\$ 4.829,79	11	R\$ 2.529,89	5	R\$ 1.149,95	11	R\$ 2.529,89
Rack 44 U	R\$ 2.259,86	3	R\$ 6.779,58	3	R\$ 6.779,58	3	R\$ 6.779,58	3	R\$ 6.779,58
Cx + placa	R\$ 19,28	502	R\$ 9.678,56	252	R\$ 4.858,56	102	R\$ 1.966,56	252	R\$ 4.858,56
AP Rukus WiFi 6	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00	1	R\$ 6.500,00
Organizador de Cabo	R\$ 1.299,00	21	R\$ 27.279,00	11	R\$ 14.289,00	5	R\$ 6.495,00	11	R\$ 14.289,00
Impressora	R\$ 1.299,00	50	R\$ 64.950,00	25	R\$ 32.475,00	10	R\$ 12.990,00	25	R\$ 32.475,00
Nobreak	R\$ 2.401,00	1	R\$ 2.401,00	1	R\$ 2.401,00	1	R\$ 2.401,00	1	R\$ 2.401,00
Mesa	R\$ 140,90	502	R\$ 70.280,00	252	R\$ 35.506,80	102	R\$ 14.371,80	252	R\$ 35.506,80
Cadeira	R\$ 159,90	502	R\$ 78.814,00	252	R\$ 40.294,80	102	R\$ 16.309,80	252	R\$ 40.294,80
Total			R\$ 2.578.069,33	Total	R\$ 1.336.213,76	Total	R\$ 587.997,15	Total	R\$ 1.336.213,76

Deste modo, observa-se na tabela que o gasto com equipamento foi estimado, na sede, em R\$ 2.578.069,33 (dois milhões, quinhentos e setenta e oito mil, sessenta e nove reais e trinta e três centavos). Já nas filiais de Gov. Valadares e Ouro Preto totalizaram, cada uma, R\$ R\$ 1.336.213,76 (um milhão, trezentos e trinta e seis mil, duzentos e treze e setenta reais e seis centavos). Por fim, na filial Rio Acima foi observado o valor total de R\$ 587.997,15 (quinhentos e oitenta e sete mil, novecentos e noventa e sete reais e quinze centavos). Portanto, o custo total dos equipamentos de todas unidades é de R\$ 5.838.494,00 (cinco milhões, oitocentos e trinta e oito mil, quatrocentos e noventa e quatro reais).

Ainda, como exposto na imagem supracitada, segue, em sequência, a motivação da escolha de cada item indicado:

- **Nutanix HPC:** Servidor escolhido em razão da sua capacidade de armazenamento (HD e SSD), além de processador atual para as necessidades da empresa. Disponível em: <https://www.ebay.com/itm/233192070119>;

- **Estação Dell:** Estação escolhida (Dell Core i5 6ª Ger 8Gb SSD 240Gb) em razão da utilização do SSD, bem como com memória RAM e processador compatíveis com a necessidade atual e futura. Disponível em:<<https://www.magazineluiza.com.br/computador-dell-core-i5-6a-ger-8gb-ssd-240gb-monitor-19/p/gk2gb3e7e3/in/cptd/>>;

- **Roteador Cisco.** Roteador escolhido (Cisco) em razão de ser suficiente à capacidade atual da empresa, bem como ainda possui suporte ativo da fornecedora, facilitando eventuais auxílios técnicos necessários. Disponível em: <<https://netcomputadores.com.br/p/isr4321sec-k9-cisco-isr-4321-router/21675>>;

- **Serial CISCO:** Serial escolhido por ser compatível com o roteador e possuir alta performance. Disponível em:<[https://www.foxiti.com.br/products/cisco-hwic-2t-2-port-serial-wan-interface-card-itinfousa?variant=36517761745057&currency=BRL&utm\\_medium=product\\_sync](https://www.foxiti.com.br/products/cisco-hwic-2t-2-port-serial-wan-interface-card-itinfousa?variant=36517761745057&currency=BRL&utm_medium=product_sync)>;

- **Switch Dell 24p:** Switch escolhido por sua grande qualidade e economia. Ele oferece um ótimo desempenho com gerenciamento e escalabilidade simples por meio de uma arquitetura de empilhamento de alta disponibilidade. Disponível em:<<https://www.kabum.com.br/produto/307237/switch-dell-n1524-10-100-1000mbps-gigabit-ethernet-24-portas-4sfp-210-asnf>>;

- **Cabo UTP CAT6 cx:** Cabo escolhido (Furukawa GigaLan) por sua alta qualidade e performance em projetos de redes. Foco no desempenho para suportar o tamanho da empresa. Disponível em:<<https://www.eletrocenterlondrina.com.br/cabo-utp-rede-cat-6-vermelho-gigalan-cm-caixa-305mts>>;

- **Tomada RJ45 f Cat6:** Tomada escolhida (Furukawa) devido ao material do corpo do produto ser Termoplástico de alto impacto não propagante a

chama. Sendo ele indispensável para uma empresa de grande porte que visa a segurança. Disponível em:<<https://www.lojaeletrica.com.br/tomada-rj45-cat6-568ab-bege-premium-35060602-furukawa,product,2520201380070,dept,12008.aspx>>;

- **Patch Cord CAT 6:** Patch escolhido (Furukawa) tendo em vista que atende várias normas de segurança e ambientais, além de ter um excelente custo benefício. Disponível em:<<https://www.cirilocabos.com.br/caixa-de-rede-furukawa-cat6-por-metro/p?skuld=684>>;

- **Patch Panel Plus Cable:** Patch escolhido devido a sua alta qualidade, pois ele excede os requisitos da sua categoria, proporcionando uma alta desempenho para rede da empresa. Disponível em:<[https://www.kabum.com.br/produto/372761/patch-panel-plus-cable-cat6-24-portas-sem-guia-cat-6-preto-la-p624?gclid=EAlaIQobChMlv6Pe7pWXgQMV9jiUAR1SBgXLEAQYASABEGJXzPD\\_BwE](https://www.kabum.com.br/produto/372761/patch-panel-plus-cable-cat6-24-portas-sem-guia-cat-6-preto-la-p624?gclid=EAlaIQobChMlv6Pe7pWXgQMV9jiUAR1SBgXLEAQYASABEGJXzPD_BwE)>;

- **Rack 44 U:** Rack escolhido (Rack Max Eletron) por proporcionar 4 modularidades, possibilitando uma futura ampliação do sistema de rede da empresa. Disponível em:<[https://www.kabum.com.br/produto/453177/rack-max-eletron-servidor-padrao-19-polegadas-44u-x-570mm-acr-solda-piso-4784?gclid=Cj0KCQjw9MCnBhCYARIsAB1WQVXj32gjjkxiTc1gMKFm-Q4X8hWt1FTpQKFSeFyg6SAsB\\_TYotGQzpsaAt43EALw\\_wcB](https://www.kabum.com.br/produto/453177/rack-max-eletron-servidor-padrao-19-polegadas-44u-x-570mm-acr-solda-piso-4784?gclid=Cj0KCQjw9MCnBhCYARIsAB1WQVXj32gjjkxiTc1gMKFm-Q4X8hWt1FTpQKFSeFyg6SAsB_TYotGQzpsaAt43EALw_wcB)>;

- **Cx + Placa:** Módulo escolhido (módulo tomada para rj45 f. Tramontina) por ser feito em material de termoplástico antichama que não retém poeira. Disponível em:<<https://www.lojaeletrica.com.br/modulo-tomada-liz-rj45-cat6-grafite-57215056-tramontina,product,2323106631151,dept,12008.aspx>>;

- **AP Rukus WiFi 6:** ACESS Point escolhido (Ruckus) por sua alta capacidade de conexões, estabelecendo até 512 (quinhentos e doze),



atendendo assim as necessidades atuais da empresa e até mesmos possíveis ampliações futuras. Disponível em:<[https://www.magazineluiza.com.br/access-point-ruckus-r650-802-11ax-wi-fi-6-dual-band-ruckus-commscope/p/aj4791f589/in/rtdr/?seller\\_id=arptec&utm\\_source=google&utm\\_medium=pla&utm\\_campaign=&partner\\_id=70403&gclid=Cj0KCQjw9MCnBhCYARIsAB1WQVU4hZxm9ui4B0\\_JSdn5a3oKV4t3x\\_lktZogrZO2n33XtnTZSW0S5m0aAtalEALw\\_wcB&gclidsrc=aw.ds](https://www.magazineluiza.com.br/access-point-ruckus-r650-802-11ax-wi-fi-6-dual-band-ruckus-commscope/p/aj4791f589/in/rtdr/?seller_id=arptec&utm_source=google&utm_medium=pla&utm_campaign=&partner_id=70403&gclid=Cj0KCQjw9MCnBhCYARIsAB1WQVU4hZxm9ui4B0_JSdn5a3oKV4t3x_lktZogrZO2n33XtnTZSW0S5m0aAtalEALw_wcB&gclidsrc=aw.ds)>;

- **Organizador de Cabos:** Organizador de Cabos escolhido (Spiraduto 1) por ser feito de um material bastante durável e flexível, além de auxiliar na durabilidade dos cabos nele inseridos. Disponível em:<<https://www.cirilocabos.com.br/spiraduto-de-1--organizador-de-cabos-dutoplast-preto/p?skuld=7503>>;

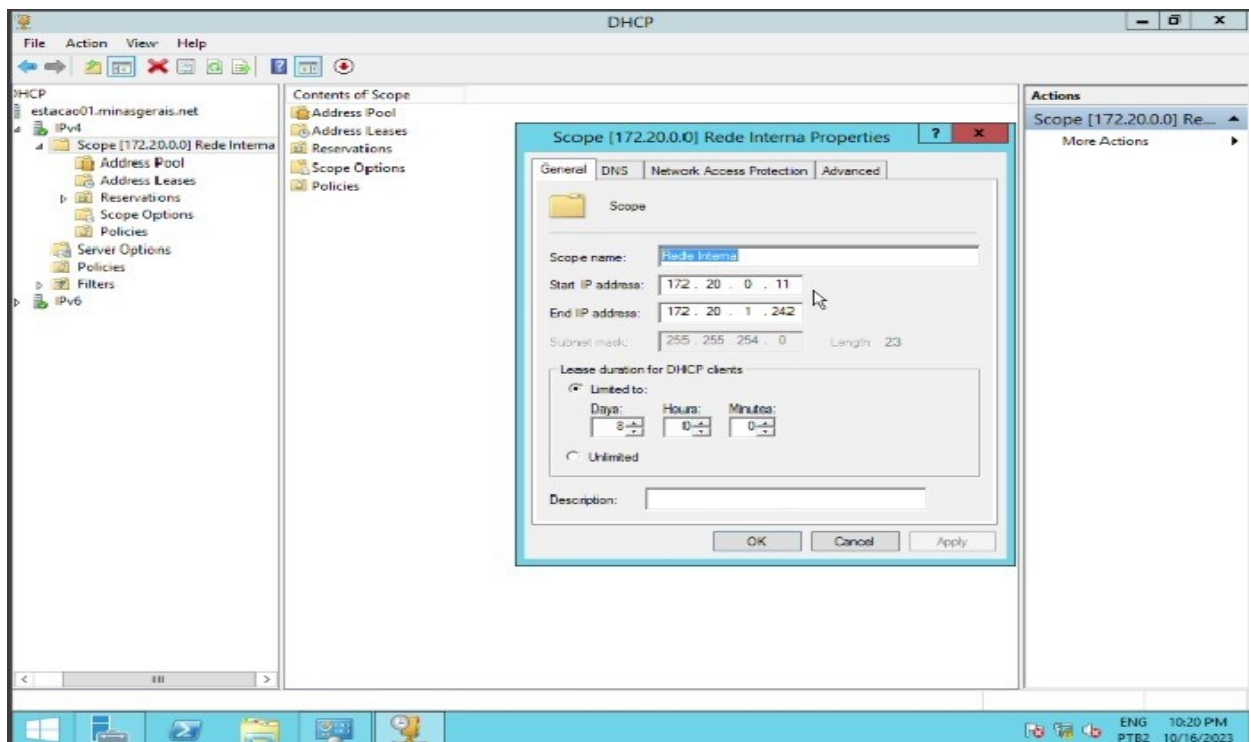
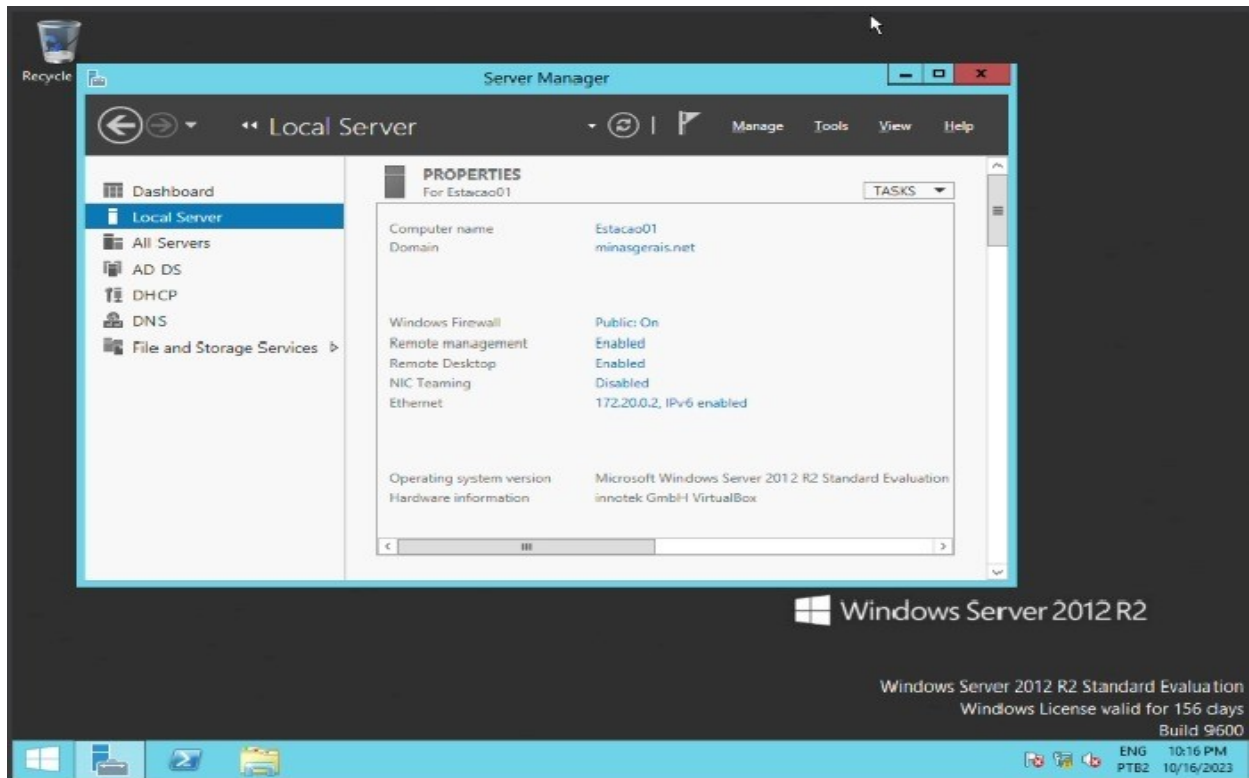
- **Impressora:** Impressora escolhida (Multifuncional G6010 Canon) por ser uma impressora completa para todas as necessidades de um escritório. Possui tecnologia EcoTank, além de conexões tanto WIFI quanto ethernet, podendo ser criada uma rede ser para conectar os computadores. Disponível em:<<https://www.kabum.com.br/produto/112869/multifuncional-canon-mega-tank-g6010-jato-de-tinta-colorido-wi-fi-bivolt-3113c005aa>>;

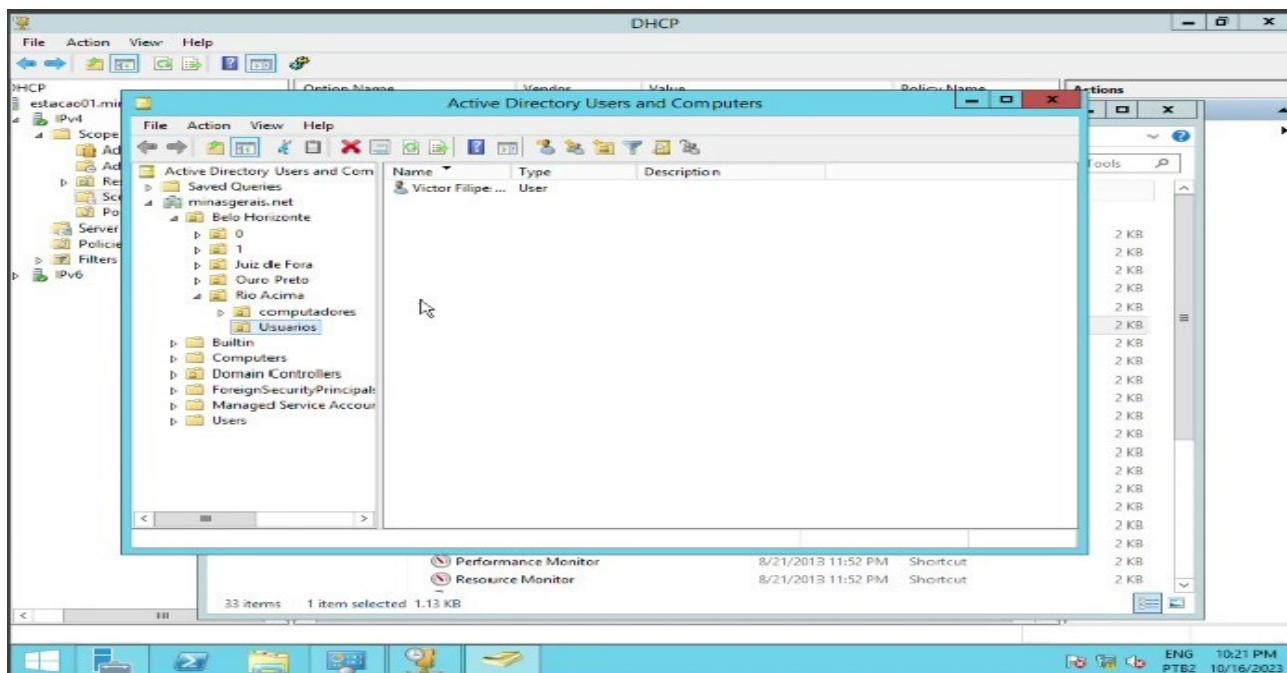
- **Nobreak:** Nobreak escolhido pensando em uma forma segura de proteger os equipamentos importantes, assim evitando o desligamento inesperado dos aparelhos, garantindo a segurança dos dados, como, por exemplo, o servidor da empresa operando 24 horas por dia. Disponível em:<[https://www.amazon.com.br/Nobreak-Senoidal-Intelbras-SNB-1500va/dp/B07LGHK1YS/ref=asc\\_df\\_B07LGHK1YS/?tag=googleshopp00=20&linkCode=df0&hvadid=379739258863&hvpos=&hvnetw=g&hvrnd=6473517275733904591&hvppone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1001566&hvtargid=pla-1106581762032&pssc=1](https://www.amazon.com.br/Nobreak-Senoidal-Intelbras-SNB-1500va/dp/B07LGHK1YS/ref=asc_df_B07LGHK1YS/?tag=googleshopp00=20&linkCode=df0&hvadid=379739258863&hvpos=&hvnetw=g&hvrnd=6473517275733904591&hvppone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1001566&hvtargid=pla-1106581762032&pssc=1)>;

- **Mesa:** Mesa escolhida tendo em vista o amplo espaço, pois é essencial que comporte o computador, com todos seus acessórios, além de possibilitar a organização de documentos. Disponível em:<<https://www.submarino.com.br/produto/5548882977/mesa-de-escritorio-108cm-1-gaveta-office-nt-2070-notavel-moveis?opn=XMLGOOGLE&offerId=62ea1cf6adbc5f39b9203a6e&cor=Preto%20Tx&condition=NEW>>;

- **Cadeira:** Cadeira escolhida visando ergonomia e conforto. Essas cadeiras se tornaram a melhor opção para o uso em escritório, pensando em todos os funcionários e no seu conforto, ao passo que comportam o peso máximo de 120kg. Disponível em:<[https://www.kabum.com.br/produto/322236/cadeira-de-escritorio-prizi-essencial-ate-120kg-com-base-cromada-preta?qclid=CjwKCAjwo9unBhBTEiwAipC115n7BB1vFk8cBDc-12K9stAAvsH0RL8EWZPP-7A6Gc3xEB1eMqW77RoCn-QQAvD\\_BwE](https://www.kabum.com.br/produto/322236/cadeira-de-escritorio-prizi-essencial-ate-120kg-com-base-cromada-preta?qclid=CjwKCAjwo9unBhBTEiwAipC115n7BB1vFk8cBDc-12K9stAAvsH0RL8EWZPP-7A6Gc3xEB1eMqW77RoCn-QQAvD_BwE)>;

## 5. Virtual Machine (Máquina Virtual)





Para este tópico, foi utilizado o programa Oracle VM Virtual Box, com o objetivo da criação de uma máquina virtual na proposta apresentada neste trabalho (empresa de telemarketing). Conforme primeira imagem, tem-se que o computador virtual criado foi nomeado como *"Estacao01"*, vinculado ao domínio *"minasgerais.net"*. Além disso, foi escolhido o *"Windows Server 2012 R2"*, com licença de Windows válida.

Assim, na fotografia em sequência, as faixas de IP da rede interna escolhidas foram, como ponto inicial, o endereço de IP 172.20.0.11 e, como ponto final, o endereço de IP 172.20.1.242.

No último *print*, é possível verificar, dentre outros pontos, as unidades vinculadas ao domínio *"minasgerais.net"*, em que a unidade principal seria Belo Horizonte (sede), ao passo que as filiais Juiz de Fora, Ouro Preto e Rio Acima estariam interligadas diretamente com a matriz, de acordo com a proposta do presente projeto, como observado em tópico anterior.

## 6. Virtual Private Cloud (Nuvem privada virtual)

The image displays a Windows desktop environment running on an AWS EC2 instance. The desktop background is the standard Windows 10 blue logo wallpaper. The taskbar at the bottom shows the Start button, search bar, and several pinned applications including File Explorer, Edge, and the AWS Management Console. The system tray in the bottom right corner shows the date and time as 12:31 AM on 10/14/2023.

On the right side of the desktop, a text box provides instance details:

- Hostname: EC2AMAZ-P07PSAI
- Instance ID: i-0e124faa01335aee1
- Public IPv4 Address: 54.144.103.231
- Private IPv4 Address: 10.0.0.182
- Instance Size: t2.large
- Availability Zone: us-east-1a
- Architecture: AMD64
- Total Memory: 8192 MB
- Network Performance: Low to Moderate

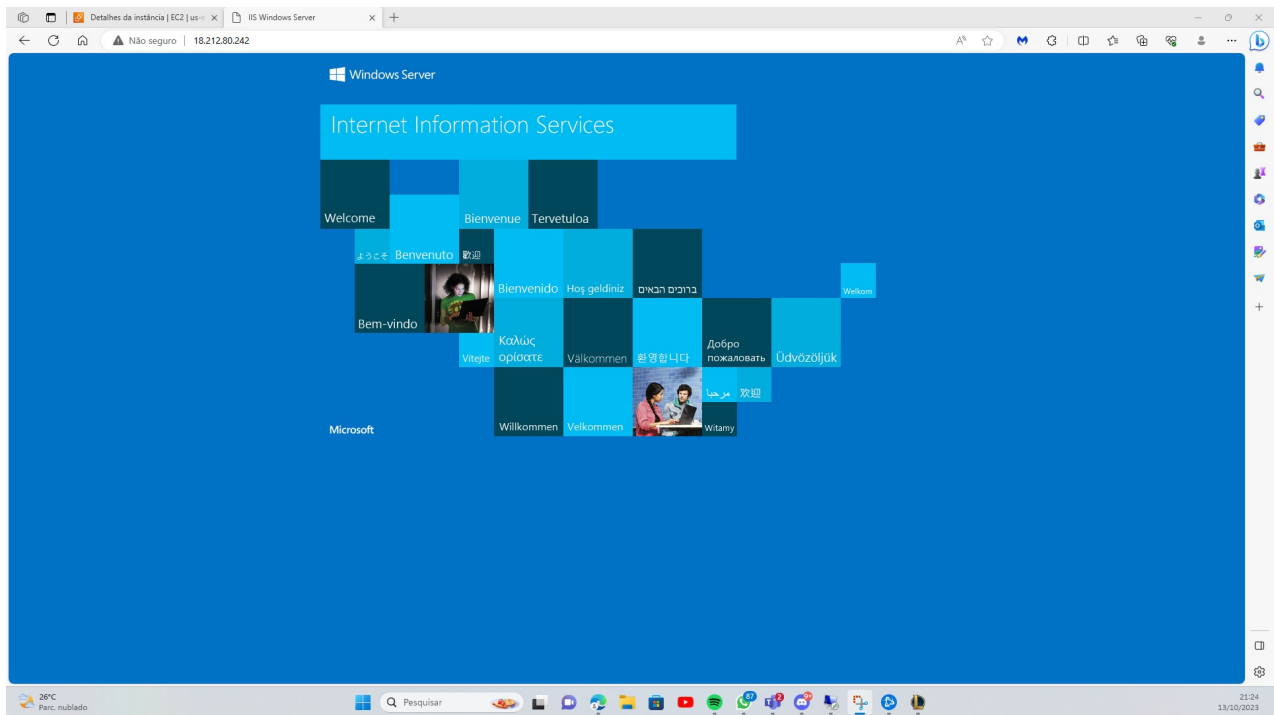
Below the desktop, the AWS Management Console is open in a web browser. The browser address bar shows the URL: <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#instanceDetails:instanceId=i-0e124faa01335aee1>. The console page is titled "Resumo da instância para i-0e124faa01335aee1 (serverwebtlmk) Informações".

The console displays the following details for the instance:

- ID de instância:** i-0e124faa01335aee1 (serverwebtlmk)
- Endereço IPv6:** -
- Tipo de nome do host:** -
- Nome do IP:** ip-10-0-0-182.ec2.internal
- Nome do DNS de recurso privado de resposta:** -
- Endereço IP atribuído automaticamente:** 18.212.80.242 [IP público]
- Função do IAM:** -
- IMDSv2:** Optional
- Endereço IPv4 público:** 18.212.80.242 [endereço aberto]
- Estado da instância:** Executando
- Nome do DNS de IP privado (somente IPv4):** ip-10-0-0-182.ec2.internal
- Tipo de instância:** t2.large
- ID da VPC:** vpc-08538f902431d62b (Telemarketing-vpc-vpc)
- ID da sub-rede:** subnet-078699c4600d46e42 (ConexMaxi-vpc-subnet-public1-us-east-1a)
- Endereços IPv4 privados:** 10.0.0.182
- DNS IPv4 público:** ec2-18-212-80-242.compute-1.amazonaws.com [endereço aberto]
- Endereços IP elásticos:** -
- Descoberta do AWS Compute Optimizer:** Opte por participar do AWS Compute Optimizer para obter recomendações. Saiba mais
- Nome do Grupo do Auto Scaling:** -

The console also shows a "Detalhes da instância" section with the following information:

- Plataforma:** windows
- Detalhes da plataforma:** Windows
- Interrupção de proteção:** Desabilitado
- ID da AMI:** ami-0173ee29ff797c346
- Nome da AMI:** Windows\_Server-2016-English-Full-Base-2023.10.11
- Data de lançamento:** Fri Oct 13 2023 20:41:22 GMT-0300 (Horário Padrão de Brasília) (41 minutos atrás)
- Monitoramento:** desativado
- Proteção contra encerramento:** Desabilitado
- Local da AMI:** amazon/Windows\_Server-2016-English-Full-Base-2023.10.11



Em todas as imagens criadas na presente seção, fora utilizado o laboratório de aprendizagem (*Learner Lab*) da AWS academy. Na primeira imagem, é possível observar, no canto direito superior, os principais dados do servidor virtual em nuvem. Além de outros pontos, o nome escolhido foi "*EC2AMAZ-PO7PSAI*", possuindo como IP (IPv4) público 54.144.103.231 e o IP (IPv4) privado 10.0.0.182. Além disso, a zona de disponibilidade escolhida foi a "*us-east-1a*". Por fim, a arquitetura do servidor é AMD64, com memória total de 8192MB.

No segundo *print*, como já indicado no parágrafo anterior, o servidor na nuvem de Telemarketing (serverwebtlmk) tem como endereço de IPv4 privado o 10.0.0.182, possuindo, nesse caso, como IPv4 público o 18.212.80.242, em razão do início de uma nova instância (a cada novo acesso o IP é alterado). Além disso, por opção, não foi gerado endereço IPv6. Ainda, na simulação, é possível notar que a instância está sendo devidamente executada.

Ao final, na terceira imagem, é possível verificar o acesso ao servidor criado (utilizando a plataforma da AWS supracitada) por meio do IPv4 público 18.212.80.242. Nesta página, ainda, é possível a total liberdade de customização do conteúdo a ser visualizado pelo usuário que irá acessar o domínio indicado.

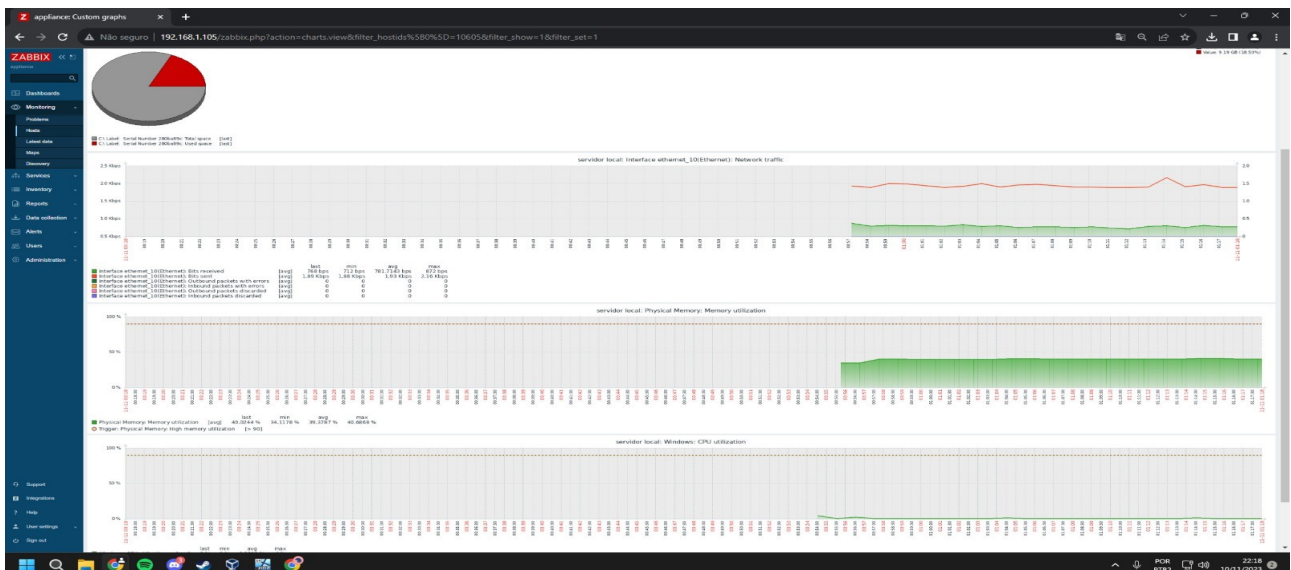
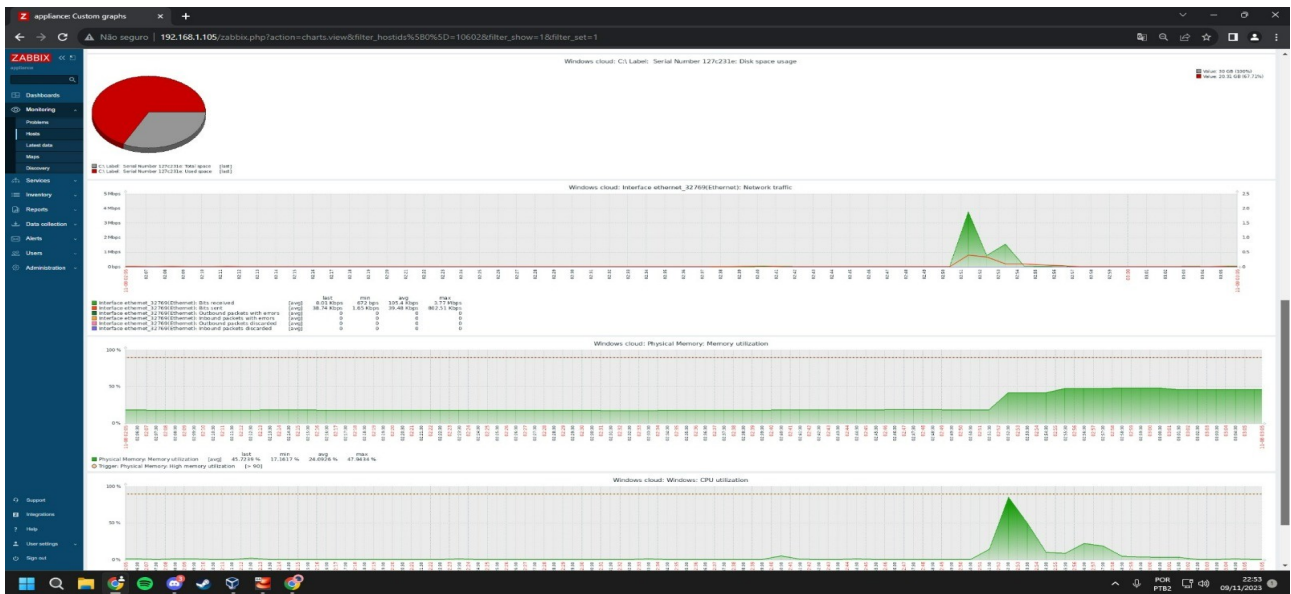


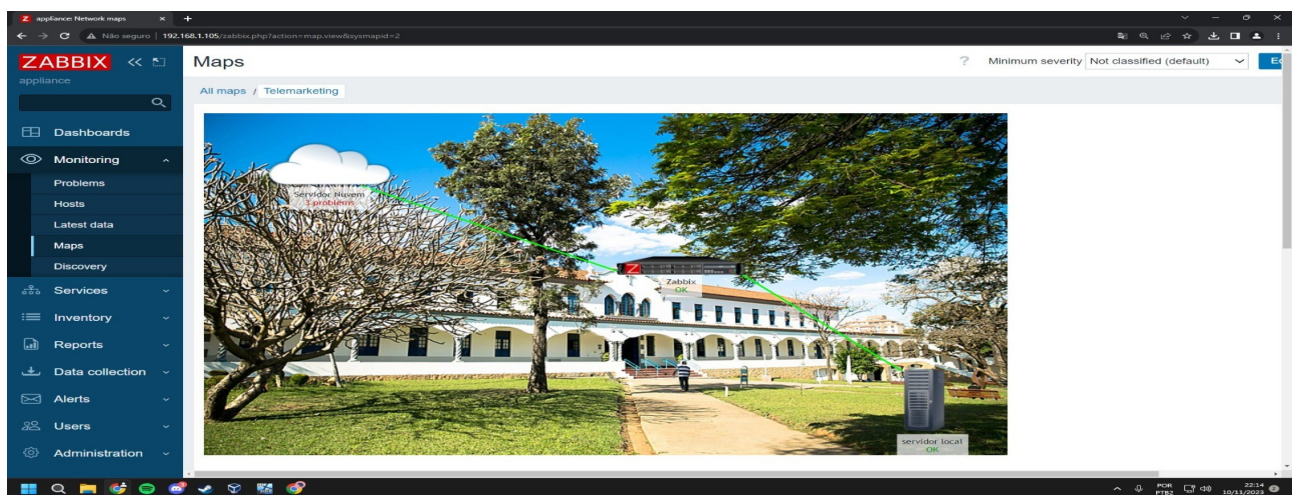
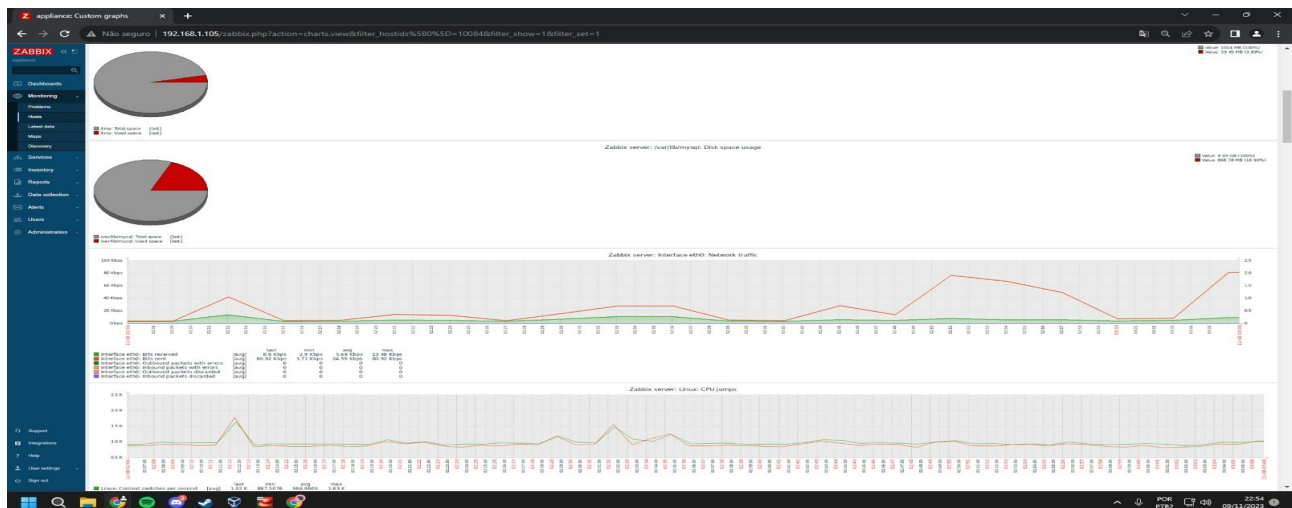
## 7. Monitoramento

Hosts configuration page in Zabbix 6.4.7. The interface shows a list of hosts with columns: Name, Interface, Availability, Tags, Status, Latest data, Problems, Graphs, Dashboards, and Web. The hosts listed are:

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
servidor local	192.168.1.140/161	OK	class: os target: windows	Enabled	Latest data 36	0	Graphs 4	Dashboards 2	Web
Windows cloud	3.95.14.17/161	ERROR	class: os class: software target: apache	Enabled	Latest data 52	1	Graphs 7	Dashboards 3	Web
Zabbix server	127.0.0.1/10959	OK	class: os class: software target: snmp	Enabled	Latest data 146	0	Graphs 27	Dashboards 4	Web

Buttons: Save as, Apply, Reset. Status: Any, Enabled, Disabled. Tags: And/Or, Or, Contains, value, Remove. Show hosts in maintenance: ☒. Show suppressed problems: ☐.





Nesta etapa do projeto, após a criação da VM e da VPC (conforme tópicos anteriores), inicialmente foi instalado a ferramenta Zabbix, com a intenção de realizar o monitoramento dos servidores virtuais previamente criados. Na primeira imagem, dentro da aba “Hosts”, tem-se o “*servidor local*” (VM), “*Windows cloud*” (VPC) e o Zabbix todos com status de habilitados (*enabled*), ao passo que o servidor Zabbix fora acessado por meio do IP 192.168.1.105. Ainda, a disponibilidade do VM e VPC ocorre pelo protocolo SNMP.

Em sequência, nos *prints* 2, 3 e 4, é verificado o monitoramento das máquinas “*servidor local*” (VM), “*Windows cloud*” (VPC) e o Zabbix. Importante frisar que, durante o monitoramento, foram gerados dados que confirmam o eficaz acompanhamento/monitoramento dos dispositivos supracitados, conforme gráficos de desempenho/uso em eixo XY “*Network Traffic*”, “*Memory Utilization*” e “*CPU Utilization*”. Por fim, na última imagem, na aba “*Maps*”, tem-se a demonstração de arquitetura entre o servidor na nuvem, Zabbix e o servidor local, mostrando o pleno funcionamento do sistema criado para a hipotética empresa de telemarketing.



## 8. CRUD - Create, Read, Update, Delete

### Criar novo cadastro

#### Cadastro

Nome do Cliente

Email do Cliente

Plano Adquirido

[Criar](#) [Voltar](#)

© 2023 - mf\_dev\_backend\_2023 - [Privacy](#)

### Lista cadastros

[Criar novo cadastro](#)

Nome do Cliente	Email do Cliente	Plano Adquirido	
Carlos	sss@gmail.com	Basic	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
Lucia	llll@gmail.com	Basic+	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
Gabriel	gabriel@gmail.com	Premium	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
Marcos	marcos@gmail.com	Basic+	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>
Marcos	marcos@gmail.com	Basic+	<a href="#">Edit</a>   <a href="#">Details</a>   <a href="#">Delete</a>

### Dados do cadastro

#### Cadastro

**Nome do Cliente** Marcos

**Email do Cliente** marcos@gmail.com

**Plano Adquirido** Basic+

[Editar](#) | [Voltar](#)

© 2023 - mf\_dev\_backend\_2023 - [Privacy](#)

### Edit

#### Cadastro

Nome do Cliente

Email do Cliente

Plano Adquirido

[Save](#)

[Back to List](#)

© 2023 - mf\_dev\_backend\_2023 - [Privacy](#)

### Remover um cadastro

Tem certeza que deseja remover esse registro?

#### Cadastro

**Nome do Cliente** Marcos

**Email do Cliente** marcos@gmail.com

**Plano Adquirido** Basic+

[Remover](#) | [Voltar](#)


© 2023 - mf\_dev\_backend\_2023 - [Privacy](#)

Utilizando o Entity Framework, ferramenta de mapeamento objeto-relacional, foi desenvolvido o CRUD (Create, Read, Update, Delete) da aplicação hipotética deste projeto. Conforme se verifica da primeira imagem, tem-se a criação do cadastro do cliente “*Marcos*”, com o e-mail “*marcos@gmail.com*”, bem como tendo sido adquirido o plano “*Basic+*”.

Em sequência, no segundo *print*, observa-se na listagem apresentada que o cadastro de “*Marcos*” consta com os demais clientes da empresa de telemarketing, ao passo que, ao selecionar o item azul “*Details*”, o operador é encaminhado para a terceira tela em que são oferecidas duas opções, “*Editar*” e “*Voltar*”.


Caso o operador decida por editar (selecionando o item amarelo “*Edit*” da tela dois ou o item azul “*Editar*” da tela três) o perfil do cliente, seja por erro ou mudança de dados cadastrais, é possível verificar que os dados como “*Nome do Cliente*”, “*Email do Cliente*” e “*Plano Adquirido*” podem ser alterados de acordo com a necessidade que seja verificada.

Ao final, caso opte por apagar o perfil do cliente (como pode ser verificado no caso hipotético em que ocorreu a duplicidade de cadastro), o operador pode pressionar o item vermelho “*Delete*” da tela dois, sendo encaminhado para a tela cinco, com as opções de “*Remover*” (item em vermelho) definitivamente o cadastro ou “*Voltar*” (item em azul) a tela de listagem de cadastro (tela dois).

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>		<b>PSI-001-2023</b>
			Versão: 1.0
	Classificação: interna		Última revisão: 26/11/2023

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>1.</b>	<b>INTRODUÇÃO .....</b>	<b>2</b>
<b>2.</b>	<b>OBJETIVOS .....</b>	<b>2</b>
<b>3.</b>	<b>ABRANGÊNCIA .....</b>	<b>3</b>
<b>4.</b>	<b>DIRETRIZES GERAIS .....</b>	<b>3</b>
4.1	INTERPRETAÇÃO .....	3
4.2	PROPRIEDADE .....	4
4.3	CLASSIFICAÇÃO DA INFORMAÇÃO .....	4
4.4	CONTROLE DE ACESSO .....	6
4.5	INTERNET .....	7
4.6	CORREIO ELETRÔNICO .....	7
4.7	REDE SEM FIO (Wi-Fi) .....	8
4.8	RECURSOS DE TIC EMPRESARIAIS.....	8
4.9	RECURSOS DE TIC PARTICULARES .....	10
4.10	ARMAZENAMENTO DE INFORMAÇÕES .....	11
4.11	REPOSITÓRIOS DIGITAIS .....	11
4.12	MÍDIAS SOCIAIS .....	12
4.13	MESA LIMPA E TELA LIMPA .....	12
4.14	ÁUDIO, VÍDEOS E FOTOS.....	13
4.15	USO DE IMAGEM, SOM DA VOZ E NOME .....	13
4.16	APLICATIVOS DE COMUNICAÇÃO .....	14
4.17	MONITORAMENTO .....	14
4.18	COMBATE AO ASSÉDIO MORAL E SEXUAL .....	15
4.19	CONTRATOS DE TRABALHO E DE PRESTAÇÃO DE SERVIÇOS .....	15
4.20	SEGURANÇA DA INFORMAÇÃO .....	15
<b>5.</b>	<b>PAPÉIS E RESPONSABILIDADES .....</b>	<b>16</b>
5.1	TODOS .....	16
5.2	GESTORES E COORDENADORES .....	17
5.3	COLABORADORES .....	18
<b>6.</b>	<b>DISPOSIÇÕES FINAIS .....</b>	<b>18</b>
<b>7.</b>	<b>DOCUMENTOS DE REFERÊNCIA .....</b>	<b>19</b>
	<b>APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES .....</b>	<b>20</b>

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

## 1. INTRODUÇÃO

A Minas Gerais Telemarketing (MGT) é uma empresa hipotética de telemarketing com abrangência estadual com atuação em diversos setores econômicos, tendo em vista que as empresas desse ramo usualmente são contratadas por outras para exercer o atendimento à clientes.

A sede fica na capital do Estado de Minas Gerais (BH), tratando-se, portanto, de uma empresa de âmbito estadual. Além da matriz, a empresa continua em expansão na localidade, possuindo atualmente filiais em Governador Valadares, Ouro Preto e Rio Acima. As duas primeiras possuem dimensões do mesmo porte, em que a junção de ambas iguala ao funcionamento da sede em Belo Horizonte. Já a filial de Rio Acima se trata de um novo empreendimento local.

A estrutura organizacional empresarial consistente na ligação direta de cada filial com a sede, entretanto, para evitar supressões de funcionamento em razão da queda de contato com a sede, cada filial, também, possui um servidor para permanecer em funcionamento.

Nesse contexto, a segurança da informação é uma atividade essencial de proteção de todos os ativos tangíveis e intangíveis da empresa, a exemplo de imagem, reputação, conhecimento, patrimônio e a própria informação. Desse modo, é fundamental que todos os integrantes, sejam os gestores ou os próprios colaboradores, pratiquem e disseminem a segurança digital.

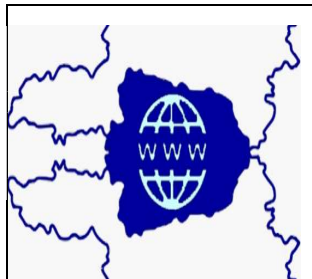
Em resposta a essas novas necessidades, está sendo implementado o Sistema de Gestão de Segurança da Informação (SGSI), que possui como diretriz principal a Política de Segurança da Informação (PSI), para atender às peculiaridades do segmento de telemarketing.

Para que a MGT alcance o resultado de proteger seus ativos na execução de sua atividade empresarial, essas novas regras devem ser cumpridas por todos.

## 2. OBJETIVOS

A Política de Segurança da Informação (PSI) é aplicável a todo ambiente da empresa e tem por objetivos:

- Estabelecer as diretrizes estratégicas e os princípios para a proteção dos ativos tangíveis e intangíveis, a exemplo da imagem, reputação, marca, propriedade intelectual, bancos de

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

dados e conhecimento, e dos recursos de tecnologia da informação e comunicação (recursos de TIC) da MGT, além das informações dos clientes;

- Nortear a tomada de decisão e a realização das atividades profissionais de todos os colaboradores da MGT, em ambientes presenciais ou digitais, sempre de acordo com as normas da empresa e a legislação nacional vigente;
- Estabelecer os princípios para o desenvolvimento de atividades empresariais seguras, que afastem danos à reputação da MGT;
- Construir uma cultura de uso seguro das informações, formando indivíduos mais preparados para agir com responsabilidade e segurança na sociedade digital;
- Preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações e dos recursos de TIC da MGT;
- Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

### 3. ABRANGÊNCIA

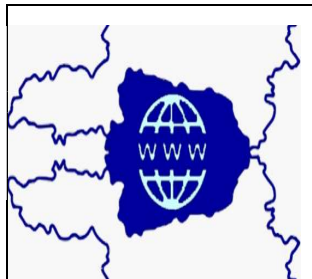
Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os empregados e empregadores, para todos os ambientes empresariais, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da empresa.

### 4. DIRETRIZES GERAIS

#### 4.1 Interpretação

4.1.1 Para efeito desta PSI, são adotadas as siglas, os termos e definições constantes no Apêndice A.

4.1.2 Esta PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização da diretoria da empresa.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.1.2.1 Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da diretoria da empresa e com duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

## 4.2 Propriedade

4.2.1 As informações geradas, acessadas, recebidas, manuseadas ou armazenadas, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis da MGT, são de propriedade e de direito de uso exclusivos de cada unidade.

4.2.2 Os recursos de TIC fornecidos pela MGT, para o desenvolvimento de atividades empresariais, são de propriedade de cada unidade ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e, por isso, devem ser utilizados apenas para o cumprimento da finalidade a que se propõem.

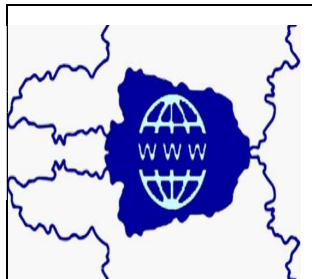
4.2.3 Todos os ativos tangíveis e intangíveis da MGT só podem ser utilizados para o cumprimento das atividades profissionais, limitados à função do colaborador.

4.2.4 A utilização das marcas, identidade visual e demais sinais distintivos da MGT, atuais e futuros, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só pode ser feita para atender a atividades profissionais, quando prévia e expressamente autorizada.

4.2.5 Todos os colaboradores poderão fazer menção da marca em conteúdos e materiais, para citação do local onde trabalha, mas, em hipótese alguma, poderá a marca ser utilizada para criação de perfis em mídias sociais em nome da empresa e/ou se fazendo passar por ela.

## 4.3 Classificação da informação

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

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.3.1.1 Informação pública: informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à empresa e aos clientes.

4.3.1.2 Informação interna: informação que pode ser divulgada para os colaboradores da empresa, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos empresariais.

4.3.1.3 Informação confidencial: informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da empresa ou causar impactos graves, sob o aspecto financeiro, legal e normativo.

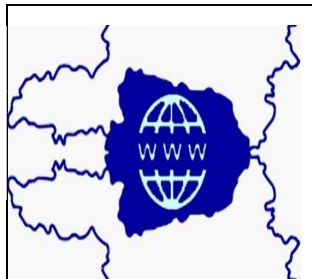
4.3.2 Rotulagem da informação: quando se tratar de informações não públicas, devem ser rotuladas no momento em que forem geradas, armazenadas ou disponibilizadas.

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

4.3.2.2 Para informações geradas ou mantidas em ambientes lógicos, utilizar documentação específica para definir o nível de classificação da informação, a exemplo de, mas não se limitando a, documento de avaliação de impacto do sistema ou banco de dados, análise de risco do sistema ou banco de dados e Plano Diretor de Segurança, Políticas de Uso.

4.3.3 Em respeito à classificação da informação, todos os colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato.

4.3.3.1 Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à empresa, incluindo a internet e mídias sociais, sem prévia e expressa autorização da MGT.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.3.4 Todo colaborador deve respeitar o sigilo profissional e contratual. Por isso, não pode revelar, transferir, compartilhar ou divulgar quaisquer informações confidenciais ou internas, incluindo, mas não se limitando a, informações de outros colaboradores, clientes, fornecedores, prestadores de serviços ou demais detalhes empresariais críticos.

4.3.5 Toda informação envolvendo dados pessoais de clientes e de colaboradores deve ser tratada como sigilosa, utilizada com cautela e apenas por pessoas autorizadas.

4.3.7 A GTI é responsável por homologar os mecanismos de criptografia, cifragem ou codificação para o armazenamento e a transmissão de conteúdos confidenciais, quando aplicáveis no desenvolvimento de sistemas internos ou no ambiente de conectividade.

#### **4.4 Controle de acesso**

4.4.1 Para cada colaborador é fornecida uma identidade digital, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos de TIC da MGT.

4.4.1.1 A identidade digital é monitorada e controlada pela MGT.

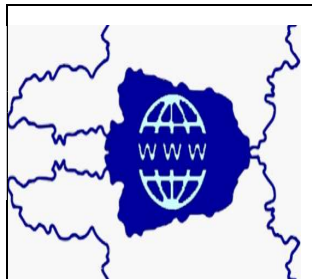
4.4.1.2 O colaborador é responsável pelo uso e o sigilo de sua identidade digital. No caso de uso não autorizado, não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros.

4.4.2 Quando a identidade for disponibilizada e fornecida pela unidade, todos os colaboradores, prestadores de serviços e visitantes, enquanto presentes nas dependências físicas da empresa, precisam estar devidamente identificados, portando o crachá individual de forma visível.

4.4.2.1 O crachá de identificação é de uso individual, não sendo autorizado o compartilhamento com outro colaborador ou terceiro, tampouco o seu uso fora das dependências da MGT.

4.4.3 Para a segurança física, a MGT deve estabelecer espaço físico seguro para proteger as áreas que criam, desenvolvem, processam ou armazenam informações críticas e que contenham ativos críticos para a empresa, a exemplo de, mas não se limitando a, datacenters, sala de Telecom, salas de documentação crítica etc.



	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.4.4 Os ativos críticos para a empresa devem estar protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas, além de ter uma correta manutenção para assegurar a sua contínua integridade e disponibilidade.

## 4.5 Internet

4.5.1 Os recursos de conectividade são fornecidos para atender ao propósito empresarial, visto que o acesso à internet é um direito essencial para o exercício da cidadania no Brasil. No entanto, os colaboradores devem fazer uso da internet em estrita observância das leis em vigor, respondendo pelo seu descumprimento.

4.5.2 O acesso à internet é concedido aos usuários e colaboradores por meio da identidade digital (*login* e senha) pessoal e intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.


## 4.6 Correio eletrônico

4.6.1 A utilização do correio eletrônico corporativo deve se ater à execução das atividades profissionais, respeitando as regras de direitos autorais, licenciamento de *software*, direitos de propriedade e privacidade.

4.6.2 O correio eletrônico corporativo pode ser utilizado no dispositivo móvel particular, porém o acesso às mensagens e às informações empresariais fora do horário normal de expediente não configura sobrejornada, sobreaviso ou plantão do colaborador, visto que pode ocorrer por ato de liberalidade e/ou conveniência sem a expressa e prévia requisição da empresa.

4.6.3 A utilização de correio eletrônico particular ou público é permitida apenas para a transmissão ou recebimento de conteúdo ou informações particulares, e desde que não lhe seja dada prioridade sobre as atividades profissionais ou acadêmicas, não provoque efeitos negativos para qualquer outro usuário, não viole ou prejudique a rede corporativa e a acadêmica e não viole norma vigente da MGT.

4.6.3.1 O correio eletrônico particular deverá ser usado somente para interesses particulares do usuário, não podendo ser utilizado para o envio ou recebimento de informações da MGT.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

#### 4.7 Rede sem fio (Wi-Fi)

4.7.1 A MGT, quando possível, oferece a todo ambiente empresarial, nos ambientes autorizados e limitados ao perímetro físico da empresa, uma rede sem fio (Wi-Fi) própria para finalidades empresariais e administrativas.

4.7.2 Somente colaboradores expressamente autorizados podem ter acesso à rede sem fio (Wi-Fi) da empresa e devem comprometer-se a fazer uso seguro desse recurso.

4.7.2.1 Em casos excepcionais, visitantes e fornecedores poderão ter acesso à rede sem fio com a prévia autorização do gestor imediato, da GTI ou do CRC.

#### 4.8 Recursos de TIC empresariais

4.8.1 Os recursos de TIC da MGT são destinados a finalidades estritamente profissionais, reservadas às atividades e permissões designadas para os usuários.

4.8.2 É vedado o armazenamento de arquivos pessoais nos recursos de TIC da MGT.

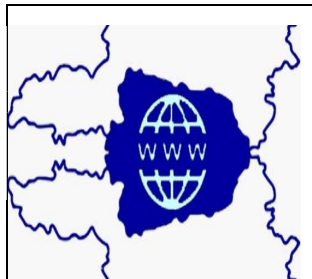
4.8.3 Para a proteção das informações, os arquivos digitais contendo informações da MGT devem ser armazenados nos servidores de arquivos destinados às áreas e setores específicos, com acesso restrito, considerando que ameaças externas, tais como vírus, interceptação de mensagens eletrônicas e fraudes eletrônicas podem afetar a segurança de tais informações.

4.8.3.1 Os colaboradores devem armazenar os arquivos digitais nos servidores de arquivos específicos e com acesso restrito, disponibilizados na rede corporativa.

4.8.3.2 A GTI e o CRC são responsáveis por realizar as cópias de segurança dos arquivos digitais (*backup*) armazenados nos servidores de arquivos específicos da MGT.

4.8.3.3 A MGT não se responsabiliza pelos arquivos digitais armazenados nas estações de trabalho, nos *notebooks*, *tablets* e *smartphones* disponibilizados pela empresa. Em casos de desligamento ou rescisão contratual, os arquivos digitais serão apagados.

4.8.4 Todos os recursos de TIC da MGT, incluindo os *softwares*, devem ser inventariados e identificados pela GTI.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.8.5 Só é permitida a utilização de *softwares* e *hardwares* legítimos, previamente homologados ou autorizados pela GTI, sejam eles onerosos, gratuitos, livres ou licenciados.

4.8.6 O desenvolvimento, a manutenção ou definição de aquisição de aplicativos e de sistemas no mercado são de responsabilidade da GTI e do CRC, e precisam atender aos requisitos de segurança em todas as etapas dos processos, a fim de garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.

4.8.7 Todas as modificações nos recursos de TIC da MGT, principalmente em sistemas e na infraestrutura tecnológica, devem ser realizadas e/ou autorizadas pela GTI ou pelo CRC, e de maneira controlada para identificar os possíveis riscos e prevenir impactos à empresa, além de garantir a disponibilidade dos recursos de TIC e a possibilidade de restauração do ambiente original em caso de incidentes não previstos.

4.8.8 A utilização de recursos deve ser monitorada pela GTI e pelo CRC, aos quais cabe realizar projeções constantes para que os recursos de TIC suportem necessidades tecnológicas futuras.

4.8.9 É vedado o uso de recurso de TIC da MGT para acessar, baixar, utilizar, armazenar ou divulgar qualquer conteúdo ilícito, impróprio, obsceno, pornográfico, difamatório, discriminatório ou incompatível com o propósito profissional e as diretrizes da MGT.


4.8.10 Todo recurso de TIC de propriedade da MGT, incluindo os dispositivos móveis, devem utilizar recursos de segurança, como senha de bloqueio automático, antivírus, *antispyware*, *firewall* e mecanismos de controle de *softwares* maliciosos.

4.8.11 A retirada de qualquer equipamento, bancos de dados ou *software* das instalações da MGT, ou da sua infraestrutura tecnológica, deve ser realizada pela GTI e pelo CRC, quando prévia e formalmente autorizada pelo gestor imediato ou por necessidade da GTI ou do CRC.

#### **4.8.12 Dispositivos móveis empresariais**

4.8.12.1 O uso de dispositivos móveis de propriedade da MGT não é permitido por terceiros, prestadores de serviços e visitantes.

4.8.12.2 Os dispositivos móveis empresariais devem conter a menor quantidade possível de informações da MGT. Arquivos digitais com informações da MGT,

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

principalmente sobre clientes, devem ser armazenados em servidores específicos para esse fim.

4.8.12.3 Em casos de roubo, perda ou furto do dispositivo móvel empresarial que contenha informações da MGT, o colaborador deve registrar o Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GTI.

## 4.9 Recursos de TIC particulares

4.9.1 É vedada a conexão dos recursos de TIC particulares na rede corporativa e acadêmica da MGT.

4.9.1.1 Os colaboradores são autorizados a utilizar os recursos de TIC particulares, conectados à rede acadêmica, exclusivamente para as suas funções no âmbito empresarial, atendendo aos princípios desta Política.

4.9.1.2 A MGT não tem qualquer responsabilidade sobre a utilização dos *softwares*, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos colaboradores.

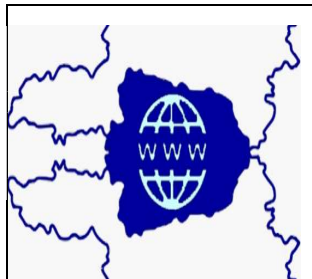
4.9.2 Os recursos de TIC particulares previamente autorizados a acessar os conteúdos e serviços fornecidos pela MGT devem ser protegidos com uso de métodos de bloqueios de acesso e ferramentas de segurança, como antivírus e *firewall*, a fim de mitigar os riscos de exposição da empresa a ameaças.

4.9.3 Todo recurso de TIC particular trazido para as dependências da MGT é de inteira responsabilidade de seu proprietário, incluindo os dados e *softwares* nele armazenados ou instalados.

4.9.4 A MGT não será responsabilizada por qualquer perda, furto ou avaria dos recursos de TIC particulares.

### 4.9.5 Dispositivos móveis particulares

4.9.5.1 O uso de dispositivos móveis particulares é permitido dentro do perímetro físico da MGT, desde que não interfira nas atividades profissionais e esteja de acordo com as leis em vigor.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.9.5.2 Dentro do perímetro físico e lógico em que informações confidenciais são armazenadas ou processadas, a MGT deve restringir a entrada e circulação de dispositivos móveis particulares.

#### 4.10 Armazenamento de informações

4.10.1 Todos devem manter as informações da MGT armazenadas no local apropriado e destinado a esse fim.

4.10.2 Os colaboradores devem armazenar as informações digitais da MGT nos servidores da rede corporativa que possuem controle de acesso e cópia de segurança. As informações físicas devem ser guardadas em gavetas, armários trancados ou local apropriado e seguro quando não estiverem sendo utilizadas, principalmente quando envolver, mas não se limitando a, documentação de identificação de clientes.

4.10.3 A MGT deve solicitar o apagamento e/ou a remoção de conteúdos que estejam nos dispositivos móveis particulares, na internet, nas mídias sociais e/ou em aplicativos, sempre que conteúdos oferecerem riscos aos clientes, colaboradores e à empresa, que forem contrários à legislação nacional vigente, que afetem o bom relacionamento dos colaboradores ou possam configurar algum tipo de dano à empresa.

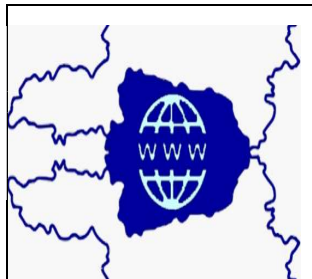
4.10.4 É vedado o uso de pendrive, cartão de memória e demais eletrônicos de uso similar nas estações de trabalho.

#### 4.11 Repositórios digitais

4.11.1 Os repositórios digitais para o uso empresarial são destinados ao armazenamento, à criação, ao compartilhamento e à transmissão de arquivos (*upload*) de informações MGT, desde que previamente autorizados, homologados e disponibilizados pela GTI.

4.11.1.1 A utilização dos repositórios digitais para o uso empresarial deve estar de acordo com os requisitos de segurança descritos nesta Política.

4.11.1.2 É vedado o armazenamento de arquivos digitais pessoais nos repositórios digitais para uso empresarial.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.11.2 É vedado armazenar, criar, compartilhar ou transmitir arquivos (*upload*) contendo informações da MGT para repositórios digitais particulares, principalmente, mas não se limitando a, informações sobre clientes e informações pessoais dos colaboradores.

4.11.3 Em caso de desligamento do colaborador, os arquivos mantidos nos repositórios digitais de uso empresarial serão excluídos.

4.11.4 Nos repositórios digitais de uso empresarial é vedada a criação, o armazenamento, o compartilhamento e a transmissão de arquivos (*upload*) de informações referentes a qualquer tipo de atividade ilegal, como pornografia infantil, jogos de azar, pirataria, violação dos direitos autorais, marcas comerciais ou outras leis de propriedade intelectual.

4.11.5 É vedado disponibilizar a identidade digital a terceiros para acessar os repositórios digitais de uso empresarial I.

#### **4.12 Mídias sociais**


4.12.1 Os colaboradores devem adotar um comportamento seguro no acesso e utilização das mídias sociais, em conformidade com todos os direitos e deveres estabelecidos no Regimento Empresarial.

4.12.2 A participação empresarial do colaborador, por meio de acesso e/ou conexão a mídias sociais a partir do ambiente da empresa e durante o horário de trabalho, deve ser diretamente relacionada à sua função profissional e aos objetivos da MGT, sendo o colaborador responsável por qualquer ação ou omissão resultante de sua postura e comportamento.

#### **4.13 Mesa limpa e tela limpa**

4.13.1 Os papéis contendo informações da MGT não devem ficar expostos em impressoras, fax, *scanner*, telas de computadores, áreas comuns, locais de trânsito de pessoas, elevador, refeitório e nas salas de reunião, principalmente quando não estiverem sendo utilizados.

4.13.2 Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciar do recurso de TIC que estiverem usando, especialmente da sua estação de trabalho ou dispositivo móvel.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

#### 4.14 Áudio, vídeos e fotos

4.14.1 Não é permitido tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens da MGT, seja do local de trabalho, corredores, banheiros, vestiários ou qualquer outro local pertencente ao perímetro físico, e, também, dos demais colaboradores, sem prévia autorização.

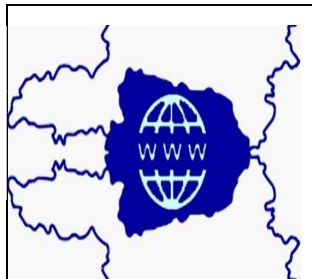
4.14.1.1 Exceto para situações já previamente avisadas e autorizadas, a exemplo de, mas não se limitando a, eventos profissionais, administrativos e/ou sociais, por sua natureza pública e de compartilhamento de informações e desde que o teor do conteúdo não exponha ao ridículo ou gere constrangimento aos envolvidos.

4.14.2 Os colaboradores da MGT não devem captar, reproduzir ou compartilhar por meio de qualquer meio tecnológico, inclusive na internet, quaisquer imagens, vídeos ou sons que:

- a) Possam comprometer a segurança dos clientes, de outros colaboradores e do ambiente empresarial ou administrativo;
- b) Possam comprometer o sigilo das informações; ou
- c) Envolvam diretamente a imagem dos colaboradores, visitantes, prestadores de serviço e fornecedores, sem a prévia e expressa anuência desses ou do gestor responsável, exceto quando autorizados em razão da sua função ou em situações já previamente avisadas e autorizadas a exemplo de, mas não se limitando a, eventos empresariais e/ou sociais, por sua natureza pública e de compartilhamento de informações.

#### 4.15 Uso de imagem, som da voz e nome

4.15.1 A MGT pode capturar, guardar, manipular, editar e usar a imagem dos colaboradores para fins de identificação, autenticação, segurança, registro de atividades, acervo histórico, uso empresarial e social, o que inclui os eventos promovidos pela empresa, inclusive em seus perfis oficiais nas mídias sociais, *website* ou intranet, quadro de avisos, entre outros conteúdos que possam ser criados ou produzidos em razão da atividade empresarial, tendo, por isso, pela própria característica técnica da internet, alcance global e prazo indeterminado, podendo inclusive alcançar *sites* e outros ambientes digitais externos.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.15.2 Para o uso de imagem, som da voz e nome dos colaboradores, estão ressalvados os direitos sobre a integridade da sua honra, sua reputação, boa fama ou respeitabilidade, sendo feito apenas nos limites acordados, sem, de forma alguma, expor o colaborador ao ridículo ou a situações constrangedoras, atendendo às leis em vigor no Brasil.

#### **4.16 Aplicativos de comunicação**

4.16.1 O uso de aplicativos de comunicação no ambiente empresarial, pelos colaboradores, a partir de recursos empresariais ou particulares, para compartilhar informações profissionais, deve ser feito de forma responsável para evitar riscos desnecessários que comprometam atividades, projetos ou a própria empresa.

4.16.2 O uso de aplicativos de comunicação no ambiente de trabalho ou fora dele, pelos colaboradores da MGT, a partir dos recursos empresariais ou particulares, para compartilhar informações profissionais, deve respeitar sempre o sigilo da informação, atender aos requisitos de segurança previstos nesta Política e respeitar as leis nacionais em vigor para evitar riscos desnecessários relacionados ao vazamento da informação ou que comprometam a empresa.

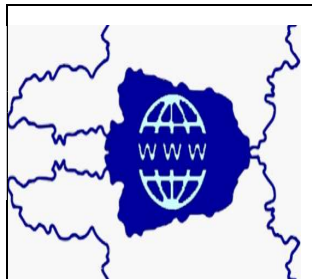
#### **4.17 Monitoramento**

4.17.1 A MGT realiza o registro e armazenamento de atividades (*logs*) e monitoram seus ambientes físicos e lógicos, com a captura de imagens, áudio ou vídeo, inclusive com a finalidade de proteção de seu patrimônio e reputação, assim como a proteção daqueles com os quais se relacionam de alguma forma.

4.17.2 O armazenamento dos dados monitorados é utilizado para fins administrativos e legais, além de colaborar com as autoridades em caso de investigação.

4.17.3 Em casos de incidentes de segurança e eventos que comprometam a integridade física e lógica dos clientes e colaboradores, a MGT tem o dever de fornecer informações ao órgão competente para apuração, e quando necessário, disponibilizar provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.



	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

#### 4.18 Combate ao assédio moral e sexual

4.18.1 Todos colaboradores devem se comprometer a participar de campanhas de conscientização promovidas pela MGT contra atos de assédio moral e sexual, bem como a cooperar de todas as formas em situações críticas para a melhor aplicação de medidas preventivas e reativas, e também contribuir para a apuração de fatos e de pessoas envolvidas em casos de assédio moral e sexual, comprometendo-se inclusive a fornecer depoimentos, quando necessários, e provas que estiverem em seu poder ou de cuja existência tiverem conhecimento.

#### 4.19 Contratos de trabalho e de prestação de serviços

4.19.1 O mero porte de dispositivos empresariais e o acesso aos recursos de TIC e/ou às informações profissionais, inclusive de forma remota, fora do horário normal do expediente, em qualquer meio ou canal, incluindo, mas não se limitando a, mensagens de clientes e colaboradores em mídias sociais, mensagens SMS, correio eletrônico, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição da empresa.

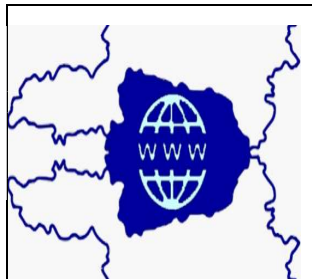
4.19.2 Em casos de desligamento, rescisão contratual ou término do contrato, a GTI e o CRC devem desativar todas as identidades digitais do colaborador em todos os sistemas e ambientes da MGT.

4.19.2.1 Nesse caso, o colaborador deve excluir todas as informações e contas da MGT, disponíveis no dispositivo móvel particular, caso tenham sido cadastradas.

#### 4.20 Segurança da informação

4.20.1 Ao repassar ou transmitir informações da MGT ou sob sua responsabilidade, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais, os colaboradores devem agir com cautela, confirmando antes a identidade do solicitante e a real necessidade do compartilhamento da informação solicitada.

4.20.2 Os colaboradores devem ter cautela ao acessar *softwares*, informações e conteúdos disponibilizados gratuitamente na internet, a exemplo de aplicativos, músicas, vídeos e e-mails com propostas suspeitas, pois podem ser vetores de ataques criminosos.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

4.20.3 A GTI e o CRC devem manter um processo de salvaguarda e restauração dos arquivos digitais críticos, a fim de atender aos requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes.

4.20.4 As informações confidenciais, assim como os recursos de TIC que as contenham, quando descartados, devem passar por procedimento de destruição que impossibilite sua recuperação e o acesso às informações armazenadas por pessoas não autorizadas.

4.20.5 Para a proteção das informações e recursos de TIC críticos, a GTI e o CRC devem elaborar um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.

4.20.6 A MGT está comprometida com o dever de orientar constantemente seus colaboradores no uso seguro das informações e da tecnologia. Por isso, podem realizar programas de educação em segurança da informação para aumentar o nível de cultura em segurança na empresa.

## **5. PAPÉIS E RESPONSABILIDADES**

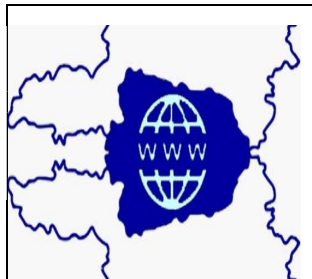
### **5.1 Todos**

5.1.1 Conhecer e disseminar as regras e princípios da Política de Segurança da Informação.

5.1.2 Preservar e proteger os ativos tangíveis e intangíveis de propriedade ou sob a custódia da MGT, inclusive todas as suas informações e conteúdos, independentemente do formato ou suporte utilizado, contra todo e qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.

5.1.3 Preservar e proteger os recursos empresariais, a marca, a reputação, o conhecimento, a propriedade intelectual da MGT, principalmente todas as suas informações e conteúdos.

5.1.4 Zelar pela proteção do patrimônio da MGT, usando com responsabilidade os recursos físicos e lógicos fornecidos;

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

5.1.5 Evitar a exposição desnecessária das informações, projetos e dependências da MGT, inclusive nas mídias sociais e na internet, além de agir com responsabilidade no uso dos recursos de TIC e das informações.

5.1.6 Prevenir e/ou reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

5.1.7 Cumprir e manter-se atualizado com relação a esta Política, ao Regimento Interno e às demais Normas de Segurança da Informação da MGT.

5.1.8 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela MGT.

5.1.9 Cumprir o dever de combater o assédio moral e sexual, por meio da adoção de medidas preventivas e reativas, bem como da conscientização para coibir e conter toda forma de violência dentro da empresa.

5.1.10 Reportar os incidentes que possam impactar na segurança das informações da MGT, imediatamente, por meio do endereço eletrônico [seguranca@mgt.br](mailto:seguranca@mgt.br).

## 5.2 Gestores

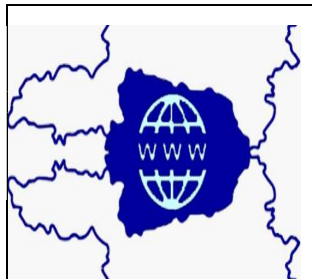
5.2.1 Orientar constantemente suas equipes quanto ao uso seguro dos ativos tangíveis e intangíveis, e dos valores adotados pela MGT, instruindo-as, inclusive, a disseminar a cultura para os demais colaboradores.

5.2.2 Suportar todas as consequências das funções e atividades que delegar a outros colaboradores.

5.2.3 Assegurar o cumprimento desta Política e das demais regulações por parte dos colaboradores supervisionados.

5.2.4 Participar da investigação de incidentes de segurança relacionados às informações, ativos e aos colaboradores sob sua responsabilidade.

5.2.5 Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

### 5.3 Colaboradores

5.3.1 Ser cauteloso em relação ao excesso de exposição de sua vida particular, a exemplo de rotinas, trajetos, contatos e intimidades, além do dever de sempre preservar o sigilo profissional nas mídias sociais, a imagem e reputação da empresa.

5.3.2 Durante a comunicação, presencial ou digital, com demais colaboradores, visitantes, fornecedores, prestadores de serviços e outros profissionais, utilizar linguagem respeitosa e adequada, condizente com o ambiente profissional, sem o uso de termos dúbios, com dupla interpretação, que exponham a intimidade ou que denotem excesso de intimidade, abuso de poder, perseguição, discriminação, algum tipo de assédio moral ou sexual.

5.3.3 Utilizar as mídias sociais evitando excessos de exposição e riscos para a sua própria imagem e reputação, bem como para a empresa.

## 6. DISPOSIÇÕES FINAIS

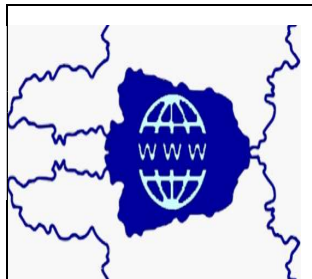
O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com outras normas e procedimentos aplicáveis pela MGT.

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

A PSI, bem como as demais normas de segurança da informação da MGT encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas por meio do endereço [seguranca@mgt.br](mailto:seguranca@mgt.br).

Em caso de dúvidas quanto a esta Política ou aos demais procedimentos de segurança da informação da MGT, o cliente, gestor e colaborador podem solicitar os esclarecimentos necessários pelo e-mail: [seguranca@mgt.br](mailto:seguranca@mgt.br).

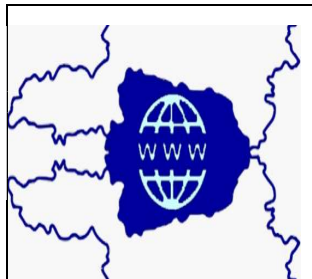
Os casos de incidente, infração ou suspeita dessas ocorrências deverão ser comunicados imediatamente, pessoalmente ou por meio do endereço [incidentes.seguranca@mgt.br](mailto:incidentes.seguranca@mgt.br).

	<b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	<b>PSI-001-2023</b>
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

## 7. DOCUMENTOS DE REFERÊNCIA

O presente documento será complementado pelos Procedimentos, Códigos e Normas de Segurança da Informação da MGT e está em consonância com os seguintes documentos:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação;
- Norma ISO/IEC 27005:2011 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;
- COBIT 5® Foundation.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

## APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES

### A

---

**Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano à empresa.

**Aplicativos de comunicação:** Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de *Whatsapp*, *Telegram* e *Snapchat*.

**Ativo:** Qualquer coisa que tenha valor para a empresa e precisa ser adequadamente protegida.

**Ativos críticos:** Todos os recursos considerados essenciais para a empresa que, se não estiverem intactos, disponíveis ou acessíveis, poderão acarretar danos graves à empresa.

**Ativo intangível:** Todo elemento que possui valor para a empresa e que esteja em meio digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à, reputação, imagem, marca e conhecimento.

**Ativo tangível:** Bens de propriedade da empresa que são concretos, que podem ser tocados, a exemplo, mas não se limitando a, computadores, imóveis, móveis.


**Antivírus:** Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.

**Antispyware:** Programa espião de computador que tem o objetivo de observar e roubar informações pessoais do usuário, transmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário.

**Autenticidade:** Garantia de que as informações sejam procedentes e fidedignas, bem como capazes de gerar evidências não repudiáveis da identificação de quem as criou, editou ou emitiu.

### B

---

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

**Backup:** Salvaguarda de sistemas ou arquivos, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de retorno.

## C

---

**Colaborador:** Empregado, estagiário ou menor aprendiz da empresa.

**Correio eletrônico:** Também denominado e-mail, é um recurso que permite compor, enviar e receber mensagens através de programas eletrônicos de comunicação.

**Correio eletrônico corporativo:** Destinado a gestores e colaboradores da empresa, dentro do domínio de cada empresa (Exemplo: joao@mgt.br).

**Correio eletrônico particular:** Estrutura de correio eletrônico particular não mantido pela empresa (Exemplo: jose@gmail.com).

**Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.

**CRC:** Centro de Recursos Computacionais, vinculado ao ICEI.

**Criptografia:** Mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos etc.) ininteligível para quem não tem acesso aos códigos de “tradução” da mensagem.

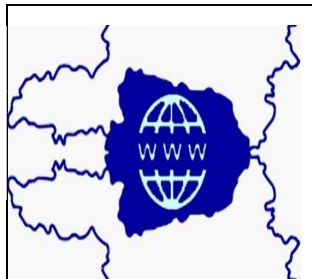
## D

---

**Dados:** Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processados ou agrupados, produzem informações.

**Datacenter:** Ambiente altamente crítico, projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como *switches*, roteadores e outros.

**Disponibilidade:** Garantia de que as informações e/ou recursos estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

**Dispositivos móveis:** Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido à sua portabilidade. Exemplos: *smartphone*, *notebook*, *tablet*, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.

## F

---

**Firewall:** Dispositivo de segurança de uma rede de computadores que monitora, autoriza e bloqueia o tráfego que entra e sai da rede.

## G

---

**GTI:** Gerência de Tecnologia da Informação, vinculada à Diretoria de Infraestrutura da MGT.

## I

---

**Identidade digital:** Identificação do usuário em ambientes lógicos, sendo composta por *login* e senha ou por outros mecanismos de identificação e autenticação, como crachá magnético, certificado digital, *token* e biometria.

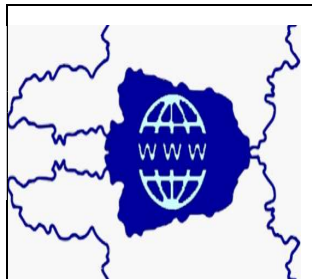
**Incidente de segurança da informação:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação e levando à perda de um ou mais princípios básicos de confidencialidade, integridade e disponibilidade.

**Informação:** Conjunto de dados que, processados ou não, pode ser utilizado para produção e transmissão de conhecimento, contido em qualquer meio, suporte ou formato.

**Internet:** Rede mundial de computadores em que o usuário pode, a partir de um dispositivo, caso tenha acesso e autorização, obter informação de qualquer outro dispositivo também conectado à rede.

**Integridade:** Garantia de que as informações estejam íntegras durante o seu ciclo de vida.



	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

## L

---

**Legalidade:** Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento jurídico em vigor no Brasil.

**Login:** Nome da identificação única dos usuários para acessarem sistemas computacionais ou recursos tecnológicos.

## R

---

**Recursos de tecnologia de informação e comunicação (recursos de TIC):** Todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Exemplos: computadores, *notebooks*, *smartphones*, *tablets*, discos externos, mídias, impressoras, *scanner*, entre outros.

**Rede corporativa ou administrativa:** Conjunto de recursos de conexão (rede local, rede internet e rede sem fio) para provimento de serviços internos à empresa, disponível para colaboradores, mantida e administrada pela GTI.

**Repositórios digitais:** Coleções de informação digital ou serviços de armazenamento, que podem ser mantidos internamente ou armazenados na internet, a exemplo de, mas não se limitando a, Wikipédia, *Microsoft One Drive*, *Google Drive*, *SkyDrive*, *Dropbox*, *iCloud*.

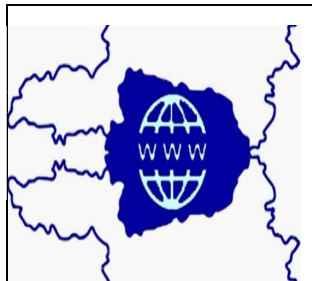
**Risco:** Possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo para prejudicar a empresa.

## S

---

**Sala de Telecom:** Ambiente para armazenar equipamentos de telecomunicações, de conexão e instalações de aterramento e de proteção de rede.

**Segurança da informação:** Preservação da confidencialidade, integridade e disponibilidade da informação na empresa.

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	PSI-001-2023
		Versão: 1.0
	Classificação: interna	Última revisão: 26/11/2023

**SMS:** Sigla de *Short Message Service* (Serviço de Mensagens Curtas). Serviço muito utilizado para o envio de mensagens de textos curtos, através de telefones celulares.

## T

---

**TIC:** Tecnologia da Informação e Comunicação.

## V

---

**Violação:** Qualquer atividade que desrespeite as diretrizes estabelecidas na política de segurança da informação ou em quaisquer das demais normas que as complementem.

## W

---

**Wi-Fi:** Abreviação de *Wireless Fidelity*, que significa fidelidade sem fio, em português. *Wi-fi*, ou *wireless*, é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.