**ATENÇÃO:**

No meio acadêmico o plágio configura se pelo ato de assinar ou apresentar como seu o resultado produzido por outra pessoa ou grupo, ou seja, copiar o trabalho alheio.

Além de uma conduta imoral e antiética, plágio pode ser qualificado como crime de violação de direito autoral no Brasil, com repercussões negativas em sua carreira acadêmica e profissional.

Entre as atitudes consideradas como plágio no meio acadêmico estão:

* entregar um trabalho acadêmico que contenha cópia parcial ou total de trabalho entregue por outra pessoa ou equipe;
* usar as ideias de outra pessoa sem indicar a autoria;
* utilizar o texto de outra pessoa, alterando algumas das palavras, ou a ordem das palavras, sem a devida citação da fonte;
* usar as ideias de outra pessoa, sem referência ao autor;
* recortar e colar da Internet conteúdo sem a devida citação da fonte.

Atividades classificadas como plágio receberão, a critério do professor, **NOTA ZERO**, independente da autoria.

Portanto, tenha isso em mente antes de compartilhar sua atividade ou realizar cópia, mesmo que parcial, de atividade desenvolvida por algum colega.

**BOM TRABALHO A TODOS!**

**Forneça o(s) nome(s) do(s) responsável (eis) pelo desenvolvimento desta avaliação:**

**Vitor Torres Dantas RM: 88415**

**Matheus de Oliveira RM: 88430**

**\***

**Preencha esse *template* e, ao final, faça *upload* de um arquivo no formato PDF na área de trabalhos da disciplina**

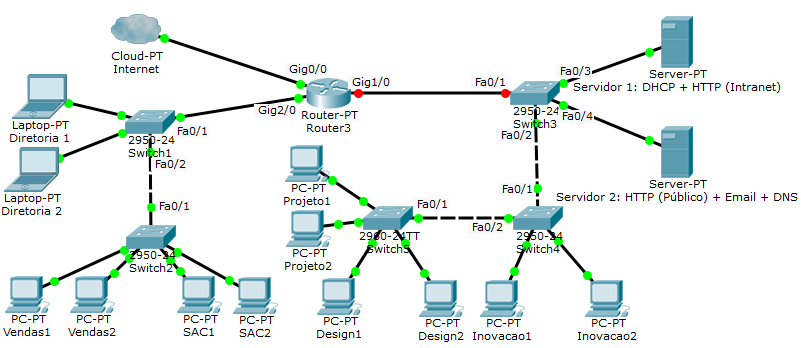
A empresa **"*GS 1 ODS2*”**  atua na área de Ias Generativas aplicadas no contexto dos Objetivos de Desenvolvimento Sustentável (ODS) da ONU.

Para resolução desta avaliação considere que vocêacaba de ser contratado pela empresa **"*GS 1 ODS2*”** para propor configurações para a ***Rede Local de Comunicação de Dados (LAN)*** existente e em funcionamento na empresa, visando, sobretudo, melhoria dos aspectos de **segurança** e **desempenho**.

A ***Empresa “GS 1 ODS2”,*** com um modelo de governança moderno e audacioso, apresenta uma estrutura de decisão revolucionária, com 6 áreas autônomas (sendo 1 diretoria e 5 setores) com igual poder de decisão. Essa estrutura de decisão revolucionária é apresentada a seguir:

**Figura 1:** Estrutura de Decisão da ***Empresa “GS 1 ODS2”***

A topologia da LAN da ***Empresa “GS 1 ODS2”***, modelada no simulador **CISCO Packet Tracer**, é apresentada na figura 2.



**Figura 2:** Topologia representando a conexão da rede local (LAN) da ***Empresa “GS 1 ODS2”*** à Internet.

**Informações complementares:**

* os *hosts* foram configurados para receber endereçamento IP via DHCP (*Dynamic Host Configuration Protocol*) onde houver configurado o serviço DHCP;
* onde não houver configurado o serviço DHCP foram realizadas configurações estáticas nos *hosts* para endereçamento IP.
* no servidor 1 estão configurados os serviços DHCP (porta UDP 67) e HTTP (porta tcp 8080);
* no servidor 2 estão configurados os serviços HTTP (porta tcp 80), Email (porta tcp 25) e DNS (porta TCP 53);
* a empresa adquiriu os seguintes endereços de rede para uso em expansões futuras: 222.222.221.0/24; 222.222.222.0/24; 222.222.223.0/24; 222.222.224.0/24; 222.222.225.0/24; 222.222.226.0/24; 222.222.227.0/24.

A tabela 1, a seguir, apresenta as portas de conexão dos equipamentos da ***Empresa “GS 1 ODS2”*** aos Switches e ao Roteador, além dos respectivos endereços IP recebidos via DHCP.

**Tabela 1:** informações de conexão dos equipamentos existentes na Empresa “***GS 1 ODS2***”

|  |  |  |  |
| --- | --- | --- | --- |
| **Equipamento** | **Porta de conexão utilizada no:** | **Endereço IP** | **Máscara** |
| Diretoria 1 | Switch1= Fa0/3 | 222.222.222.2 | 255.255.255.0 |
| Diretoria 2 | Switch1= Fa0/4 | 222.222.222.3 | 255.255.255.0 |
| Vendas 1 | Switch2= Fa0/2 | 222.222.221.2 | 255.255.255.0 |
| Vendas 2 | Switch2= Fa0/3 | 222.222.221.3 | 255.255.255.0 |
| SAC 1 | Switch2= Fa0/4 | 222.222.221.4 | 255.255.255.0 |
| SAC 2 | Switch2= Fa0/5 | 222.222.221.5 | 255.255.255.0 |
| Servidor 1 | Switch3= Fa0/3 | 222.222.223.2 | 255.255.255.0 |
| Servidor 2 | Switch3= Fa0/4 | 222.222.223.3 | 255.255.255.0 |
| Inovacao 1 | Switch4= Fa0/3 | 222.222.223.4 | 255.255.255.0 |
| Inovacao 2 | Switch4= Fa0/4 | 222.222.223.5 | 255.255.255.0 |
| Projeto 1 | Switch5= Fa0/2 | 222.222.223.6 | 255.255.255.0 |
| Projeto 2 | Switch5= Fa0/3 | 222.222.223.7 | 255.255.255.0 |
| Design 1 | Switch5= Fa0/4 | 222.222.223.8 | 255.255.255.0 |
| Design 2 | Switch5= Fa0/5 | 222.222.223.9 | 255.255.255.0 |
| Switch 1 | Switch1=Fa0/1 <--> Roteador=Gig2/0 |  | |
| Switch1=Fa0/2 <--> Switch2=Fa0/1 |
| Switch1=Fa0/3 <--> Diretoria1 |
| Switch1=Fa0/4 <--> Diretoria2 |
| Switch 2 | Switch2=Fa0/1 <--> Switch1= Fa0/2 |
| Switch2=Fa0/2 <--> Vendas1 |
| Switch2=Fa0/3 <--> Vendas2 |
| Switch2=Fa0/4 <--> SAC1 |
| Switch2=Fa0/5 <--> SAC2 |
| Switch 3 | Switch3=Fa0/1 <--> Roteador= Gig1/0 |
| Switch3=Fa0/2 <--> Switch4= Fa0/1 |
| Switch3=Fa0/3 <--> Servidor1 |
| Switch3=Fa0/4 <--> Servidor2 |
| Switch 4 | Switch4=Fa0/1 <--> Switch3= Fa0/2 |
| Switch4=Fa0/2 <--> Switch5= Fa0/1 |
| Switch4=Fa0/3 <--> Inovacao1 |
| Switch4=Fa0/4 <--> Inovacao2 |
| Switch 5 | Switch5=Fa0/1 <--> Switch4= Fa0/2 |
| Switch5=Fa0/2 <--> Projeto1 |
| Switch5=Fa0/2 <--> Projeto2 |
| Switch5=Fa0/3 <--> Design1 |
| Switch5=Fa0/4 <--> Design2 |
| Roteador | Roteador=Gig0/0 <--> Internet | 100.100.100.1 | 255.255.255.252 |
| Roteador=gig2/0.1 <--> Switch1= Fa0/1 | 222.222.221.1 | 255.255.255.0 |
| Roteador=gig2/0.2 <--> Switch1= Fa0/1 | 222.222.222.1 | 255.255.255.0 |
| Roteador=gig1/0 <--> Switch3= Fa0/1 | 222.222.223.1 | 255.255.255.0 |

Este documento deverá ser utilizado como um *TEMPLATE* a ser preenchido durante a resolução das atividades apresentadas a seguir. Ao final, salve este arquivo **no formato .pdf** e realize *upload* na área de trabalhos da disciplina.

**----------------------------------------------------------------------------------------------------------------------------------------------Preencha os espaços a seguir com sua proposta de configuração:**

**----------------------------------------------------------------------------------------------------------------------------------------------**

**Atividade 1 (0,5 ponto):** Apresente as configurações a serem realizadas no **SWITCH1** para:

* 1. criar uma vlan de nome DIRETORIA que permita a ligação dos Laptops **DIRETORIA 1** e **Diretoria 2**
  2. configuração das interfaces **TRUNK** quando se fizerem necessárias

# Switch>enable

# Switch#configure terminal

**Criar a VLAN "DIRETORIA" no SWITCH1:**

vlan 2

name DIRETORIA

end

**Configurar as interfaces dos laptops "DIRETORIA 1" e "DIRETORIA 2" como membros da VLAN "DIRETORIA":**

interface range fa0/3-4

switchport mode access

switchport access vlan 10

end

**Configure a interface como TRUNK:**

interface fa0/1

switchport mode trunk

end

**Atividade 2 (0,5 ponto):** Apresente as configurações a serem realizadas no **SWITCH2** para:

* 1. configuração das interfaces **TRUNK** quando se fizerem necessárias

# Switch>enable

# Switch#configure terminal

**Configure a interface como TRUNK:**

interface fa0/1

switchport mode trunk

end

**Atividade 3 (0,5 ponto):** Apresente as configurações a serem realizadas no **ROTEADOR** para:

3.1. configurar endereço IPv4 na interface gig0/0;

3.2. configurar subinterfaces e atribuir endereços IPv4 (1 subinterface para a VLAN DEFAULT e outra subinterface para a VLAN DIRETORIA);

3.3. configurar o serviço DHCP no roteador para uso dos equipamentos na VLAN DIRETORIA;

3.4. configuração de regras ACL para bloquear qualquer tipo de tráfego com origem no host 222.222.221.4 com tendo como destino a INTERNET;

Os demais tráfegos com origem na rede da ***Empresa “GS 1 ODS2”*** com destino à INTERNET deverão estar liberados;

3.5. configuração de regras ACL para bloquear o tráfego com origem no host 222.222.222.1 e com destino na porta TCP 8080 do host 222.222.223.2. Os demais tráfegos deverão estar liberados;

3.6. aplicar as regras ACL nas interfaces do roteador:

# Router>enable

# Router#configure terminal

**Configurar endereço IPV4 na interface gig0/0:**

interface GigabitEthernet0/0

ip address 100.100.100.1 255.255.255.252

no shutdown

**Configurar subinterfaces e atribuir endereços IPv4:**

interface gigabitEthernet 0/2.1

encapsulation dot1Q 2

ip address 222.222.222.1 255.255.255.0

no shutdown

interface gigabitEthernet 0/2.2

encapsulation dot1Q 1

ip address 222.222.221.1 255.255.255.0

no shutdown

**Configurar o serviço DHCP para a VLAN DIRETORIA:**

ip dhcp pool DIRETORIA

network 222.222.222.0 255.255.255.0

default-router 222.222.222.1

dns-server 222.222.223.3

**Configuração de regras ACL:**

access-list 1 deny host 222.222.221.4

access-list 1 permit 222.222.221.0 255.255.255.0

access-list 1 permit 222.222.222.0 255.255.255.0

access-list 1 permit 222.222.223.0 255.255.255.0

access-list 105 deny tcp host 222.222.222.1 host 222.222.223.2 eq 8080

access-list 105 permit ip any any

**Aplicação das regras:**

interface gig0/0

ip access-group 1 out

**interface gig0/2.1**

**ip access-group 105 in**

**Atividade 4 (0,5 ponto):** Considerando o sucesso e crescimento da ***Empresa “GS 1 ODS2”*** acrescente na topologia pelo menos mais:

* 5 PCs que deverão ser conectados aos switches existentes;
* 1 access-point para permitir conexão via Wi-Fi à rede da empresa;
* 2 aparelhos celulares para fazer uso da conexão Wi-Fi;

Os equipamentos poderão ser inseridos na topologia em qualquer posição à escolha da equipe (CUIDADO: esse é o momento de apresentar uma proposta exclusiva de sua equipe. EVITEM PLÁGIO!)

*Cole a seguir um PRINTSCREEN da nova topologia configurada no software CISCO Packet Tracer:*

Diagrama

Descrição gerada automaticamente

**Atividade 5 (2 pontos):** Nos espaços a seguir, da letra a) até a letra f), apresente as configurações a serem realizadas nos equipamentos para que:

1. os 5 PCS acrescentados na atividade 4 façam uso de em uma VLAN EXCLUSIVA para esses equipamentos;
2. o *access-point* e os 2 aparelhos celulares façam uso de em uma VLAN EXCLUSIVA para esses equipamentos;
3. os 5 PCS e os 2 aparelhos celulares recebam endereço IP de um serviço DHCP a ser configurado por sua equipe.

**Observação:** Mantenha vazio os espaços relativos a equipamentos que não irão receber configuração

1. Espaço para as configurações a serem realizadas no **SWITCH4** (se for necessária a configuração deste equipamento):

**VLAN para os PCS:**

vlan 3

name CONVIDADOS

end

interface range fa0/6-10

switchport mode access

switchport access vlan 3

end

**VLAN para os celulares:**

vlan 4

name CELULARES

end

interface fa0/5

switchport mode access

switchport access vlan 4

end

**Serviço DHCP no switch 4:**

ip dhcp pool CONVIDADOS

network 222.222.223.0 255.255.255.0

default-router 222.222.223.1

dns-server 222.222.223.3

exit

interface vlan 3

ip address 222.222.223.30 255.255.255.0

no shutdown

ip dhcp pool CELULARES

network 222.222.223.0 255.255.255.0

default-router 222.222.223.1

dns-server 222.222.223.3

exit

interface vlan 4

ip address 222.222.223.40 255.255.255.0

no shutdown

**Atividade 6 (2 pontos).** Apresente a descrição de 3 regras de uma política de segurança a ser implementado na topologia. Sigam o exemplo a seguir:

**Regra 0:** Os hosts destinados ao SAC (SAC1 e SAC2) não poderão ter acesso ao serviço HTTP configurado no SERVIDOR1 na porta TCP 8080;

**Regra 1:** Preencha o espaço a seguir com uma proposta de regra de uma política de segurança a ser implementada na topologia.

O tráfego SSH de entrada para todos os dispositivos da rede, exceto para o SERVIDOR2, será permitido apenas a partir da sub-rede de gerenciamento.

**Regra 2:** Preencha o espaço a seguir com uma proposta de regra de uma política de segurança a ser implementada na topologia.

Os hosts da sub-rede da diretoria não poderão estabelecer conexões de saída para endereços IP externos, exceto para o servidor de e-mail na porta TCP 25.

**Regra 3:** Preencha o espaço a seguir com uma proposta de regra de uma política de segurança a ser implementada na topologia.

O tráfego ICMP (ping) será bloqueado em todos os dispositivos da rede, exceto para os hosts da sub-rede de servidores (SERVIDOR1 e SERVIDOR2) que precisam responder a solicitações de monitoramento de rede.

**Atividade 7 (2 pontos).** Apresente os comandos para implantação das regras da política de segurança proposta por sua equipe na atividade 6.

**Regra 1:** Preencha o espaço a seguir com TODOS os comandos para implementar a regra 1 da política de segurança proposta por sua equipe na atividade 6.

access-list 101 permit tcp 222.222.222.0 255.255.255.0 any eq 22

access-list 101 deny tcp host 222.222.223.3 any eq 22

interface gig0/2.1

ip access-group 101 in

**Regra 2:** Preencha o espaço a seguir com TODOS os comandos para implementar a regra 2 da política de segurança proposta por sua equipe na atividade 6.

access-list 102 deny tcp 222.222.222.0 255.255.255.0 any neq 25

access-list 102 permit ip 222.222.222.0 255.255.255.0 any

interface gig0/2.1

ip access-group 102 in

**Regra 3:** Preencha o espaço a seguir com TODOS os comandos para implementar a regra 3 da política de segurança proposta por sua equipe na atividade 6.

access-list 103 permit icmp host 222.222.223.3 any

access-list 103 permit icmp host 222.222.223.2 any

access-list 103 deny icmp any any

interface gig0/2.1

ip access-group 103 in

**Atividade 8 (1 ponto).** Apresente os comandos necessários para configurar roteamento RIP no roteador existente.

router rip

network 222.222.221.0

network 222.222.222.0

network 222.222.223.0

**Atividade 9 (1 pontos).** Realize todas as configurações apresentadas nas atividades anteriores utilizando o software CISCO Packet Tracer e faça ***upload*** do arquivo .pkt (compactado na versão .zip) juntamente com este documento salvo na versão .PDF no Portal da FIAP, na área de trabalhos da disciplina.