ISPGAYA

instituto superior politécnico

Escola Superior de Ciência e Tecnologia

CTeSP RSI / TPSI

2022/2023

Segurança de Redes Informáticas

Alunos:

Miguel Magalhães (Nº2021103166)
Rui Reis (Nº2021101434)

Docente: Prof. Henrique Teixeira

19 de Janeiro de 2023

ÍNDICE DE CONTEÚDOS

ÍNDICE DE FIGURAS

ABREVIATURAS

- IP – Internet Protocol;
- WPA - Wi-Fi Protected Access;
- WPA2 - Wi-Fi Protected Access II;
- IPS – "Intrusion Prevention System" ou Sistema de Prevenção de Intrusão;
- DHCP - Dynamic Host Configuration Protocol;
- DMZ - Demilitarized Zone;
- DNS - Domain Name System;
- LAN – Local Area Network;
- VLAN – Virtual LAN;
- URL - Uniform Resource Locator.

GLOSSÁRIO

- "Stakeholders primários" – partes interessadas no projeto, como são primários, tratam-se de partes interessadas dentro da empresa;

- Switch – dispositivo que conecta todos os elementos de uma rede.

INTRODUÇÃO

ENQUADRAMENTO

Este projeto foi proposto pelo Sr. Professor Henrique Teixeira, no âmbito da unidade curricular de Segurança de Redes Informáticas, tendo por objetivo a elaboração e desenvolvimento de políticas e procedimentos de segurança de uma rede de uma empresa.

OBJETIVOS

O objetivo principal deste projeto, assim como foi referido na introdução, é elaborar e desenvolver políticas e procedimentos de segurança de uma rede de uma empresa. Para isso, simulamos a criação de uma empresa, em que a mesma, tinha de seguir princípios e regras específicas, das quais: ter um edifício com, no mínimo, 3 pisos; na sua estrutura interna ou "stakeholders primários"(ou partes interessadas) conter, no mínimo30 funcionários e, no mínimo, 4 departamentos; a mesma poderá conter diversos silos em diferentes regiões e deverá ser indicado qual o tipo de segurança definida e utilizada.

ESTRUTURA DO RELATÓRIO

O relatório encontra-se estruturado em 7 capítulos. No capítulo *Introdução* é realizado um breve enquadramento do tema do projeto e são apresentados sumariamente os seus objetivos. Todos os restantes capítulos têm como função fornecer informação sobre o projeto.

STORYTELLING

O projeto trata-se de uma empresa ou organização, que tem como nome "RMTech", que será responsável pela montagem de um escritório para expandir o seu negócio. A RMTech é uma empresa especializada em montagem de sistemas de rede, por isso, será a mesma que irá construir um sistema de redes para o seu novo escritório. O edifício escolhido para tal oportunidade, foi um edifício com cerca de 4 andares. O primeiro passo para a empresa começar a montar o seu escritório, visto que é uma empresa especializada em redes, é certificar-se dos melhores locais para colocar todo o seu futuro equipamento técnico. Com as escolhas do local, também é importante ter em conta o lugar de cada departamento, por exemplo, é importante de ver o lugar onde o departamento do servidor irá ser alocado, pois este lugar terá de ter uma segurança especifica para diminuir diversos riscos ou problemas do futuro servidor.

CISCO E CISCO PACKET TRACER

CISCO

No começo Cisco Systems fabricava apenas routers de grande porte para empresas, mas, conforme foi ganhando renome se diversificou, passando atender também ao consumidor final com tecnologias como o Voip.

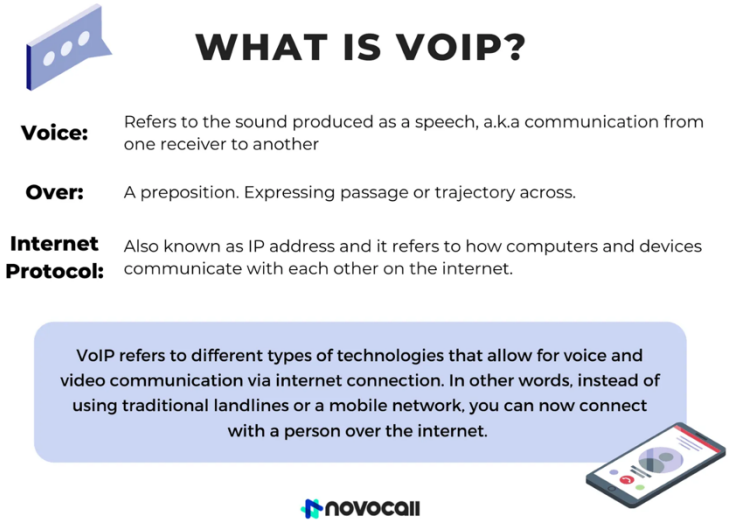


Figura 1.: Definição de Voip.

Fundada em 1984 na Universidade de Stanford, a Cisco Systems rapidamente tornou-se líder no desenvolvimento de soluções de hardware e software para tecnologias de redes baseadas no Internet Protocol (IP), tornando-se uma das empresas pioneiras na utilização da Internet , servindo-se dela não só para apresentar e vender os seus produtos, como também para oferecer e implementar uma vasta gama de serviços, que vão desde o apoio ao cliente ou formação de funcionários, até à gestão de finanças e processos de fabrico.

Internet Protocol é o protocolo de comunicação da camada de rede no conjunto de protocolos da Internet para retransmitir datagramas através dos limites da rede. A sua função de roteamento permite interconexão de redes.

Atualmente, a Cisco Systems é responsável pelo fabrico mundial de equipamentos para redes informáticas, a mesma prioriza o desenvolvimento e produção de equipamentos para interligar redes de computadores, como routers e switch's.

A mesma também é responsável por uma diversidade de produtos relacionados com redes locais de Internet, servidores de acesso remoto, variados equipamentos de

comunicação pela transmissão de voz , dados via IP, ou ainda sistemas de segurança e manutenção de redes.

Embora tenha como clientes preferenciais as grandes empresas de telecomunicações e os ISP, a Cisco também desenvolve produtos adequados às pequenas empresas e utilizadores individuais.

A atividade principal da Cisco é a oferta de soluções para redes e comunicações quer seja na fabricação e venda como na prestação de serviços por meio de suas subsidiárias.

CISCO PACKET TRACER

O Cisco Packet Tracer é um programa de simulação de um esquema de rede específico.

Este software foi desenvolvido para o ensino de redes de computadores, e tem como objetivo principal realizar simulações de redes, avaliações, medições complexas e tem a capacidade de criar novas redes, sendo possível trabalhar com múltiplos usuários no mesmo projeto.

Através do uso deste software, o usuário tem vantagens na sua utilização, devido às diversas funcionalidades que permite ao mesmo criar cenários de redes personalizadas para avaliação de diversas áreas, nomeadamente, informáticas.

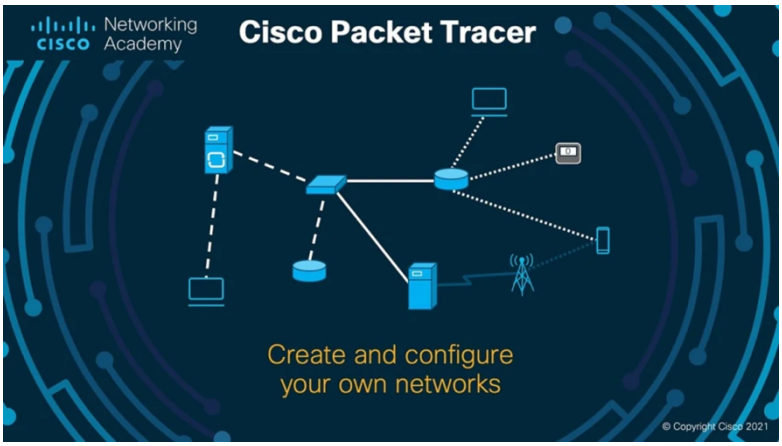


Figura 2.: Cisco Packet Tracer.

Uma das ferramentas que a empresa RMTech escolheu para auxiliar na construção da sua nova rede, é o Cisco Packet Tracer. No resto do projeto, será focado a criação de toda a rede.

CONSTRUÇÃO DA REDE

SERVIDORES

Para uma melhor organização na nova rede criada, e como começo do projeto, foi realizada a criação de uma sala de servidores. Na mesma sala, estavam contidos servidores "WEB", "DHCP", seguidos de dois "Switch's". Outro ponto focado neste projeto, foi a criação de uma rede segura. Para isso, e antes de ser iniciada a criação de uma rede LAN, foi criada uma DMZ. A função da DMZ é servir de proteção à rede privada, pois é na mesma que a firewall se encontra.

Na imagem a seguir, é possível visualizar a sala de servidores, que se encontra no piso -1.

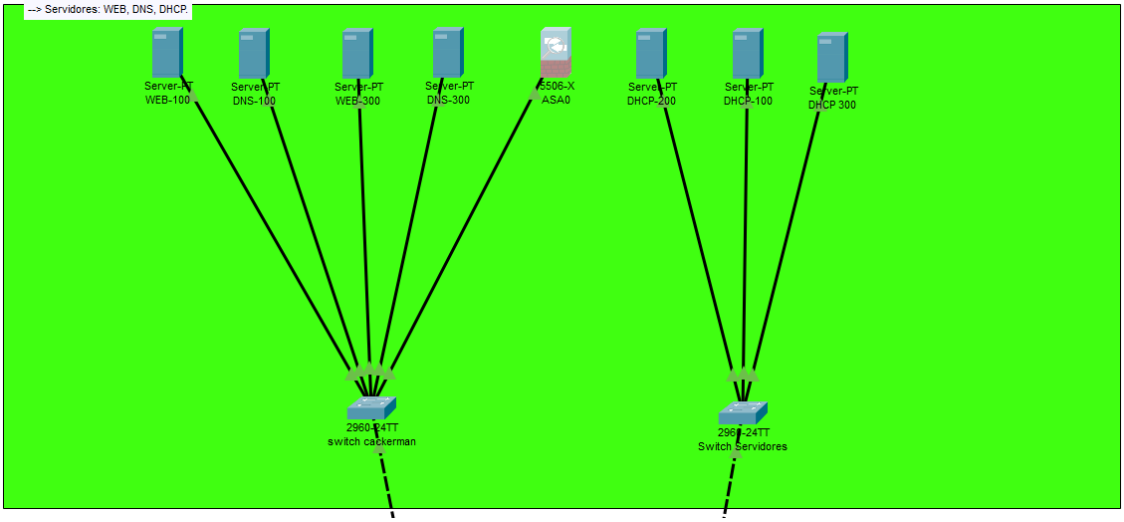


Figura 3.: Sala de servidores.

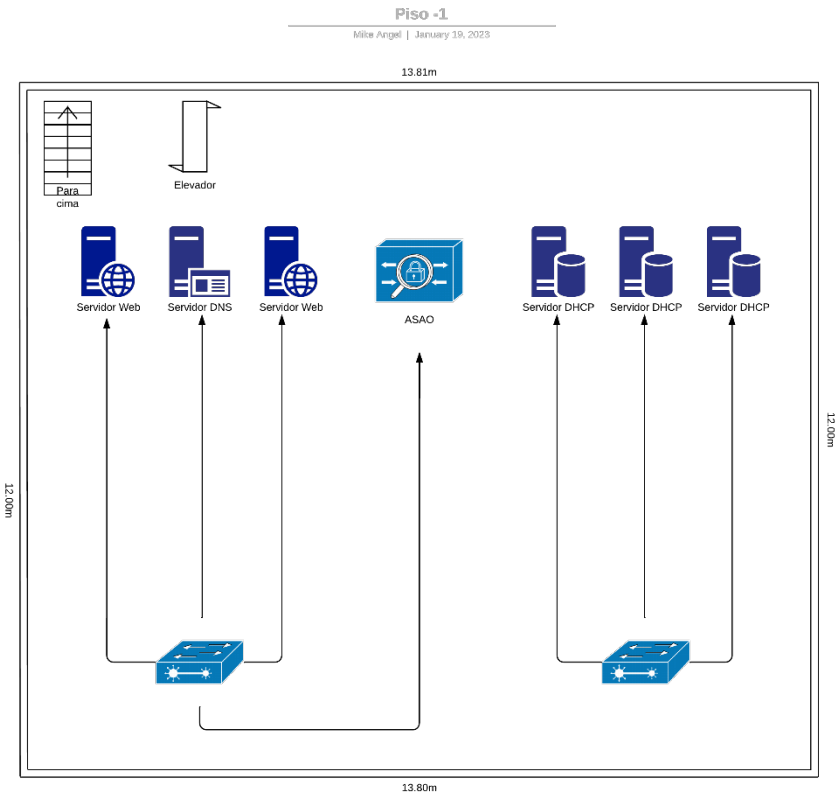


Figura 4.: Planta do piso da sala de servidores.

ORGANIZAÇÃO DOS IP'S DE CADA DEPARTAMENTO

Em todo o projeto, foram usados 6 departamentos: Servidores, Receção, Refeitório, Contabilidade/Logística, Administração/Recursos Humanos e Escritório/Equipa Técnica/ Call center. Cada departamento foi organizado em andares, sendo que um andar pode conter mais do que um departamento. Ao longo deste relatório, será possível destacar cada departamento por piso.

Apesar de apenas serem usados 6 departamentos, nesta empresa, os switch's de toda a infraestrutura de rede foram implementados com, na sua base, 3 VLAN's. No seguimento dessa implementação, as VLAN's sofreram uma padronização: o número "100" indica a VLAN da administração/recursos humanos com IP's da faixa 192.172.100.0/24.

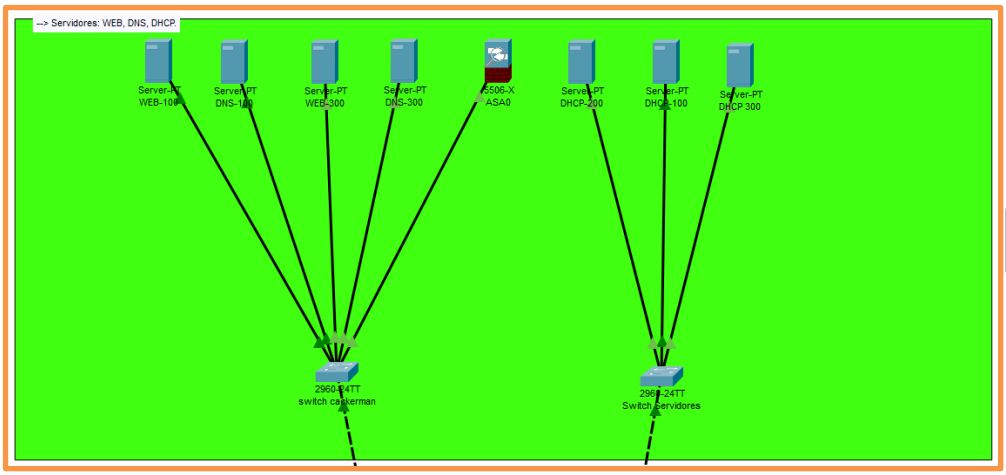
Colocando de parte o departamento administrativo e de recursos humanos, foi aplicada também uma VLAN "200" para o departamento da Contabilidade/Logística, com a faixa de IP a variar a partir de outra faixa de IP, sendo esta: 192.172.200.0/24.

Por último e por seguimento lógico, foi criada a VLAN "300", que representa o departamento dos escritórios/equipa técnica/ call center.

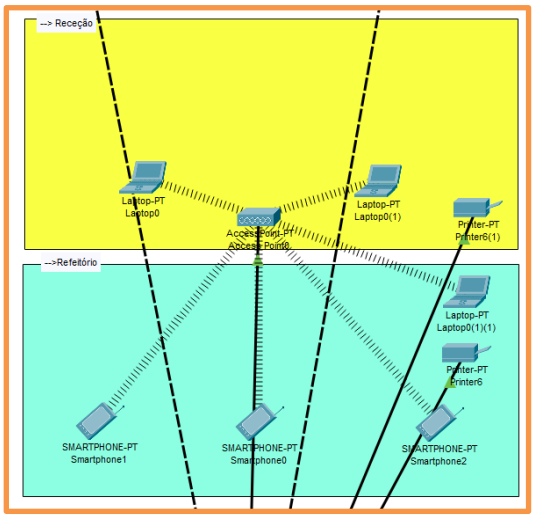
Com toda a estrutura de rede e todos seus padrões de segurança definidos, o próximo passo, é realizar a ligação dos servidores com o switch principal, usando as VLAN's que foram definidas da base de dados do mesmo switch. Esta ligação será realizada através de um cabo que , em termos de organização da infraestrutura de rede no prédio da empresa, fará com que seja obrigatório uma passagem via Trunk para que todas as diferentes VLAN's tenham um tráfego em conjunto.

CISCO PACKET TRACER – CONSTRUÇÃO DO ESQUEMA DE REDE

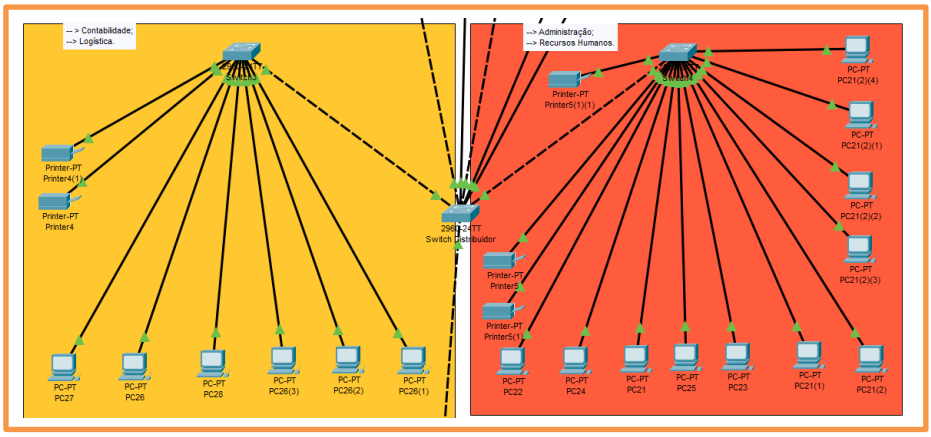
Após o uso da ferramenta "Cisco Packet Tracer" e de um estudo aprofundado de todo o esquema de rede criado na mesma ferramenta, foi possível realizar uma verificação de todos os nós da rede até aos switch's que fazem ligação com todas as máquinas da empresa. Para auxiliar essa verificação, foi usada a opção "Trunk" do software para permitir o envio das respetivas VLAN's para cada um dos departamentos.



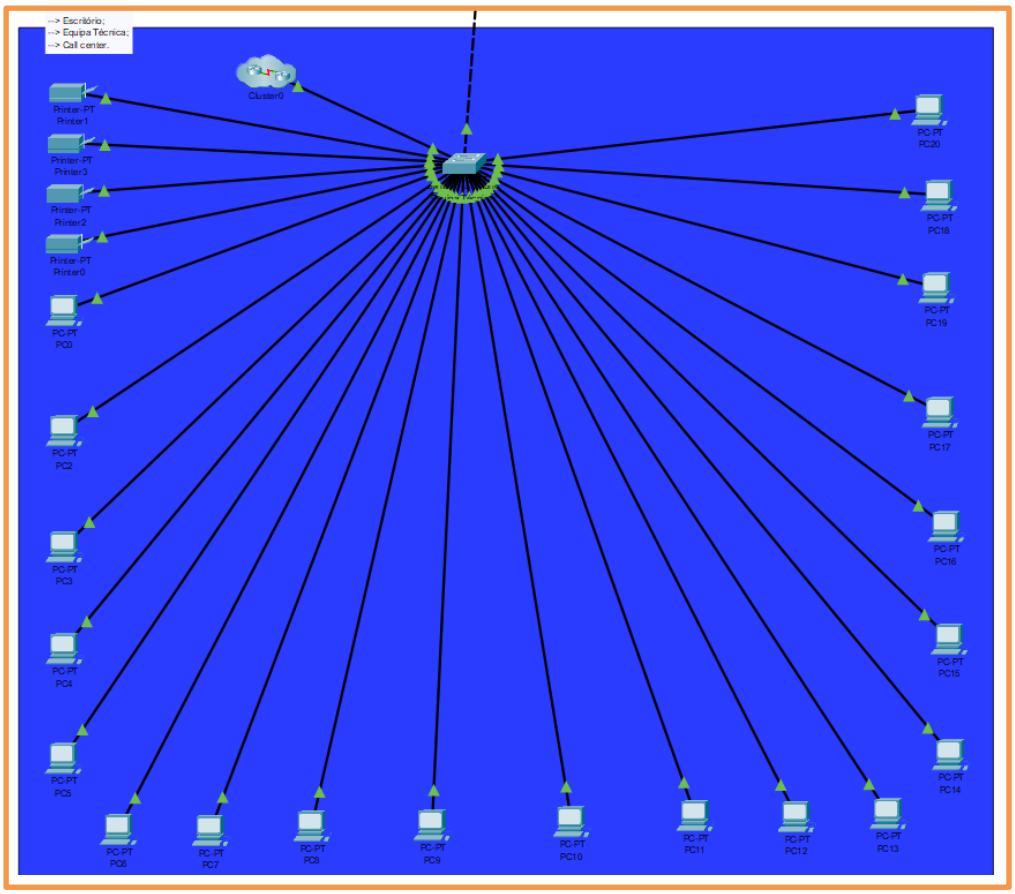
Piso -1



Piso 0



Piso 1



Piso 2

Figura 5.: Esquema de Rede realizado na ferramenta Cisco Packet Tracer.

Com todas as VLAN's centradas para o seu switch correto, as mesmas serão filtradas e enviadas para as respetivas faixas de IP. Através da realização de toda a devida configuração, vai ser possível que cada departamento seja independente entre si, fazendo com que haja uma maior segurança. Com o aumento da segurança, é possível com que os dados pessoais sejam repartidos e com acessos devidamente restritos.

PLANTA DO EDIFÍCIO

Para uma melhor compreensão da estrutura da empresa RMTech, foi usada a ferramenta "Lucidhart" para a criação de uma planta para cada piso.

Figura 6.: Planta do edifício da empresa.

CONFIGURAÇÃO DE REDES E DISPOSITIVOS

VLAN'S - CONFIGURAÇÃO

Para uma melhor organização e uma menor margem de erro, em todas as VLAN's de todos os departamentos, a opção "DHCP" de configuração dos switch está ativa. Esta opção faz com que todos os IP's sejam requisitados aos servidores principais (IPV4) referente ao IP da rede , sendo este mesmo previamente distribuído pelo servidor de DHCP. Uma das principais funções do servidor DHCP é o fornecimento, por parte do mesmo, da Gateway e servidor DNS. Isto permite com que haja uma ligação entre o utilizador e a máquina do mesmo com o servidor Web.

A máscara da rede é outro ponto a ser focado: no caso específico da nossa rede, essa máscara representa 24 bits. É possível concluir isso pois, na máscara deste projeto, existem 3 octetos preenchidos. Como estas configuração são iguais para todos os equipamentos usados no projeto, é possível visualizar apenas numa figura todas as configurações de segurança do IP da rede (tanto para uma rede Ethernet como uma rede wireless) executadas no trabalho:

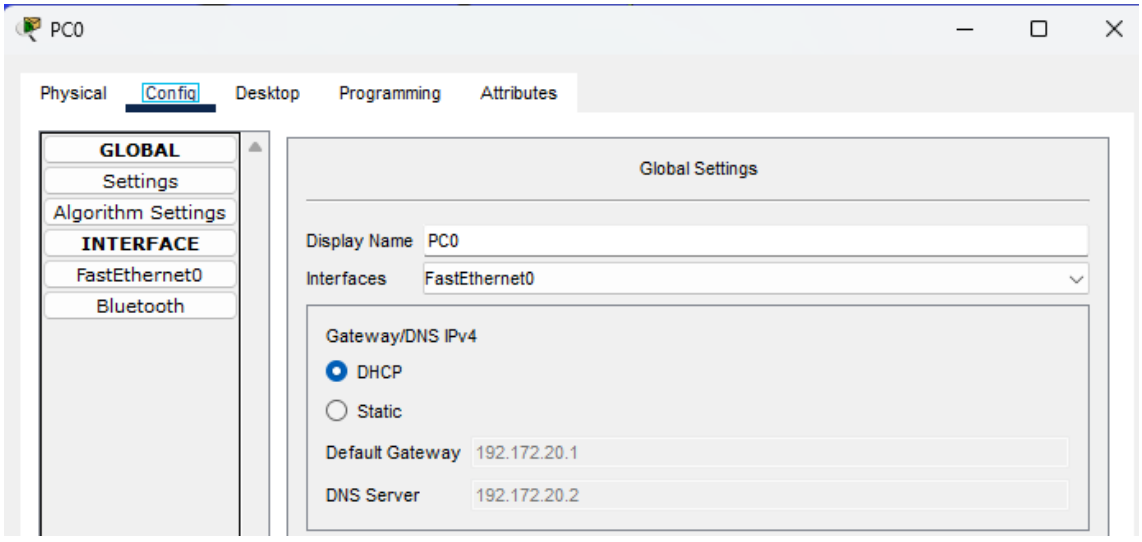


Figura 4.: Exemplo da configuração de IP de um computador na VLAN 100, por cabo.

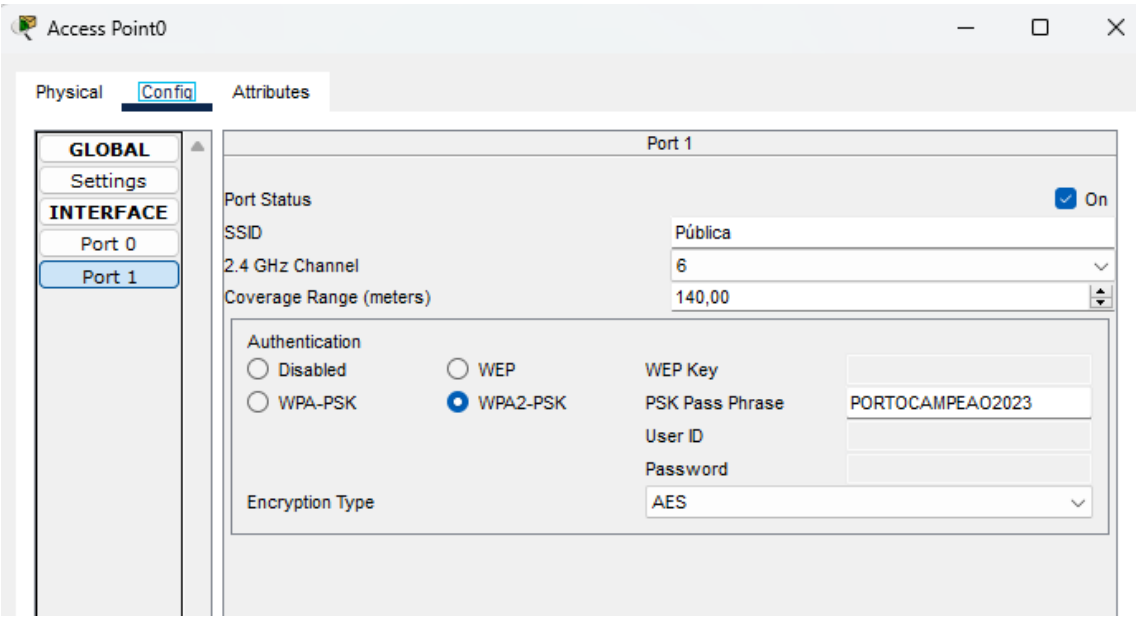


Figura 5.: Exemplo da configuração IP de um router com a segurança do tipo "WPA2-PSK" e com uma palavra-passe específica.

A "WPA2-PSK" trata-se de uma das chaves de segurança ou senha mais seguras da atualidade. Esta é uma versão melhorada da anterior (WPA) e esta começou a ser usada em meados de 2006, sendo que, atualmente, trata-se do protocolo de segurança mais usado no mundo. Apesar de não ser totalmente eficaz, esta é considerada como a escolha mais segura para rede wireless.

A empresa RMTech decidiu apenas focar-se em colocar redes públicas para visitantes que usufruíssem do refeitório e para funcionários da receção e refeitório.

Figura 7.: Escala de segurança, em termos de rede Wireless.

WIRELESS - COMUNICAÇÕES

Para ser possível no Cisco Packet Tracer, qualquer dispositivo com placa de rede, conectar à rede wireless é necessário que o mesmo insira a palavra-passe correta, nas configurações. Na figura seguinte, é possível ver, passo a passo, um simples tutorial para ser possível inserir uma rede wireless numa máquina.

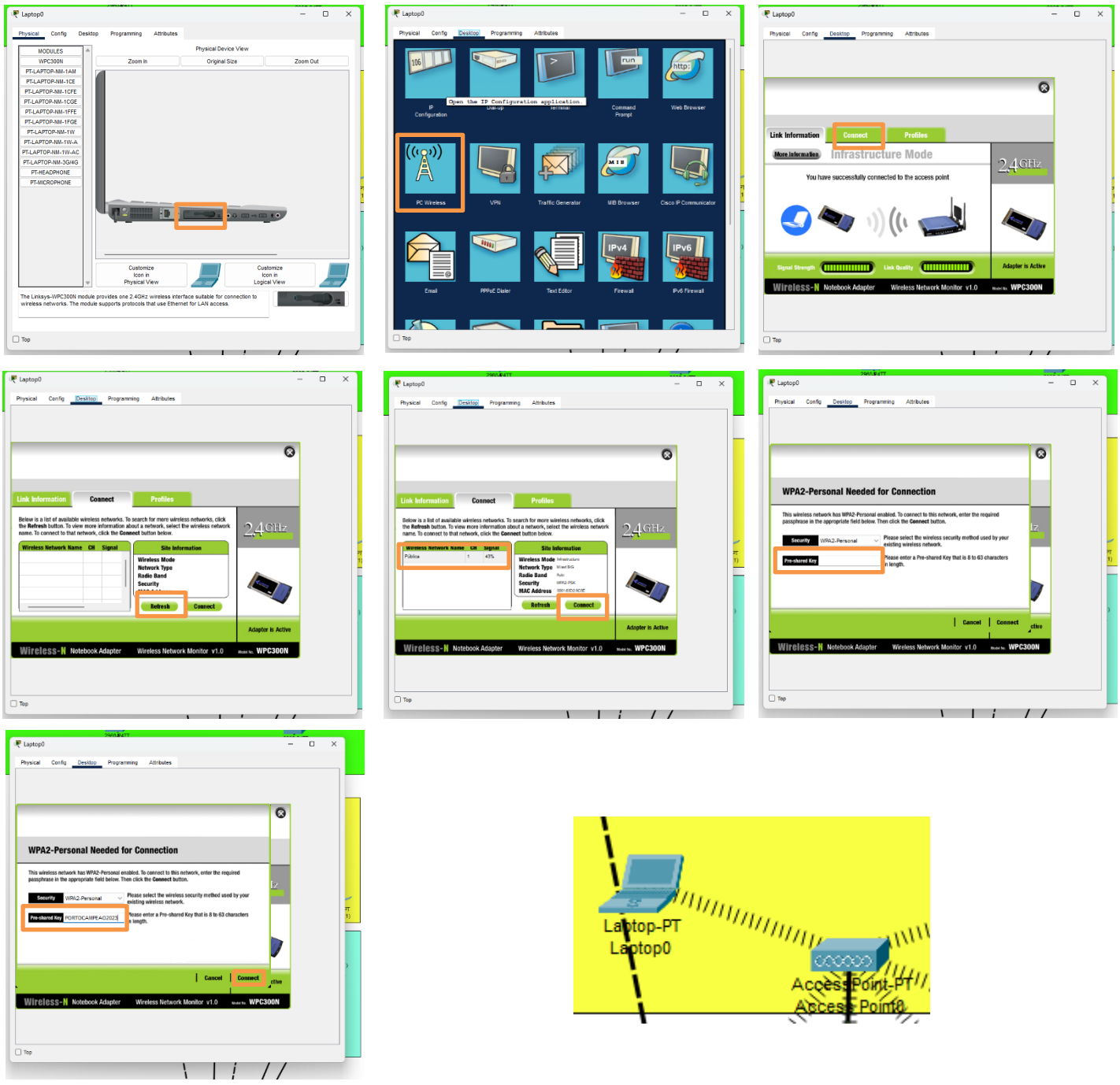


Figura 8.: Demonstração, em passos, da configuração de um dispositivo numa rede com segurança.

EXEMPLO – PÁGINA WEB

Para ser demonstrado que a máquina está conectada a uma rede funcional, foi criado um site com o URL www.adm.pt. Quando se realiza esta pesquisa no browser de qualquer computador do projeto, este mesmo, irá diretamente ao servidor DNS e fará o requisito ao servidor web através do IP correto. Depois destes passos, a página pretendida irá aparecer. Exemplo de uma página web:

Figura 9.: Exemplo da Criação de uma página Web através de um servidor Web.

Riscos e Desafios de Segurança

Phishing

Identificador	*Phishing*
Descrição do Risco	Phishing é uma técnica na qual o hacker usa falsos sorteios e eventos, por exemplo, para extrair dados pessoais e/ou confidenciais da vítima.
Medidas definidas pelo RGPD	A empresa deve contactar as autoridades no prazo limite de 3 dias. Podem ser aplicadas coimas, dependendo da gravidade da situação.
Resolução do risco	As melhores práticas para proteger a empresa de um ataque de phishing é utilizar software antivírus e filtros anti-phishing nos servidores de email.

Ransomware

Identificador	Ransomware
Descrição do Risco	O ransomware consiste em um tipo de vírus que impede o acesso do utilizador a sistemas e ficheiros, exigindo pagamento para devolvê-los ou libertá-los.
Medidas definidas pelo RGPD	A empresa deve contactar as autoridades no prazo limite de 3 dias. Podem ser aplicadas coimas, dependendo da gravidade da situação.
Resolução do risco	A proteção contra esta ameaça requer a atualização dos nossos softwares, instalação de antivírus e demais sistemas de segurança eficazes, que bloqueiam as tentativas de invasão.

ARMAZENAMENTO INSEGURO DE DADOS

Identificador	Armazenamento inseguro de dados
Descrição do Risco	Problemas com armazenamento devido à fraca política de instruções dadas aos funcionários e colaboradores sobre como e onde os dados devem ser guardados.
Medidas definidas pelo RGPD	Elaborar uma política que seja condizente com as necessidades e expectativas da empresa, e o mais importante, ter a certeza que os colaboradores vão compreender e colocar as normas estabelecidas em prática.
Resolução do risco	Usar bons métodos de segurança, eliminar os dados que não podem ser protegidos e manter os sistemas operativos atualizados.

USO INDEVIDO DE DADOS PESSOAIS

Identificador	Uso indevido de Dados pessoais
Descrição do Risco	O mau uso dos dados pode resultar no vazamento de informações pessoais, a não oferta ao titular da opção de parar de receber contactos indesejados com ofertas de produtos no e-mail pessoal.
Medidas definidas pelo RGPD	Direito a uma indemnização caso a empresa ou entidade não tenha respeitado as leis da proteção de dados e, na sequência disso, o cidadão tenha sofrido prejuízos materiais ou de outro tipo, nomeadamente, danos de reputação.

Resolução do risco	Informar os clientes sobre o incidente e notificar a APD.

ACESSO NÃO AUTORIZADO A DADOS

Identificador	Acesso não autorizado aos dados
Descrição do Risco	Caso alguém os roube ou aceda ilegalmente aos dados.
Medidas definidas pelo RGPD	Apresentar queixa e indemnização à empresa.
Resolução do risco	Escolher um encarregado de proteção de dados.

ROUBO DE DADOS

Identificador	Roubo de dados
Descrição do Risco	Roubo de dados é o ato de roubar informações armazenadas em computadores, servidores ou outros dispositivos de uma vítima com a intenção de comprometer a privacidade ou obter informações confidenciais.
Medidas definidas pelo RGPD	A empresa deve contactar as autoridades no prazo limite de 3 dias.
Resolução do risco	Informar os clientes sobre o ocorrido. É importante também fazer backups frequentes das informações armazenadas nos dispositivos.

BIBLIOGRAFIA

O que é a senha WPA2? — DE HANWAY (2006). Obtido 19 de janeiro de 2023, de https://definirtec.com/ampliar/35377/o-que-e-uma-senha-wpa2

Mapa de risco — Luís Cyrino (2016). Obtido 19 de janeiro de 2023, de https://www.manutencaoemfoco.com.br/mapa-de-risco/

Redes: Saiba o que é o Gateway e para que serve — NETWORKING (2018). Obtido 19 de janeiro de 2023, de https://pplware.sapo.pt/tutoriais/networking/gateway-para-que-serve/

What's the best wife encryption protocol for home networks? — COX (2020). Obtido 19 de janeiro de 2023, de https://www.cox.com/residential/internet/guides/securing-wifi/wep-vs-wpa-vs-wpa2.html

O que é o Cisco Packet Tracer? — Acervo Lima (2017). Obtido 19 de janeiro de 2023, de https://acervolima.com/o-que-e-cisco-packet-tracer/

O que é Cisco IOS? — The Astrology Page (2023). Obtido 19 de janeiro de 2023, de https://pt.theastrologypage.com/cisco-ios

ANEXOS

MAPA DE RISCOS EM REDES

Risco	Descrição	Grupo de risco	Nível de risco
Destruição ou alteração acidental/ ilegal de dados	Acesso a dados com intuito de alterar ou modificar sem permissão.	Interno	Elevado
Divulgação não autorizada de dados	Exposição de dados pessoais de forma ilegal, e invasão de privacidade.	Interno / Externo	Elevado
Roubo de dados	Roubo de dados é o ato de roubar informações armazenadas em computadores, servidores ou outros dispositivos de uma vítima com a intenção de comprometer a privacidade ou obter informações confidenciais.	Interno / Externo	Elevado
Recolha de dados em excesso	Recolha de dados, muitas vezes desnecessárias.	Interno	Baixo
Vírus, worms e cavalos de Tróia	Ataques externos, com o objetivo de atacar e extorquir dados internos.	Externo	Elevado
Acesso não autorizado a dados	Caso alguém os roube ou aceda ilegalmente aos dados.	Interno	Elevado
Hackers.	Pessoa com grandes conhecimentos de informática e programação, que se dedica a encontrar falhas em ou a aceder ilegalmente a sistemas e redes computacionais.	Externo	Elevado
Spyware.	Spyware é um tipo de malware que tenta se esconder enquanto regista secretamente informações e rastreia as nossas atividades online em nos computadores ou dispositivos móveis.	Externo	Elevado

MAPA DE RISCOS DE SEGURANÇA DA EMPRESA RMTECH

GRUPO 1: VERDE	GRUPO 2: VERMELHO	GRUPO 3: MARROM	GRUPO 4: AMARELO	GRUPO 5: AZUL
RISCOS FÍSICOS	RISCOS QUÍMICOS	RISCOS BIOLÓGICOS	RISCOS ERGONÔMICOS	RISCOS DE ACIDENTES
RUÍDO	POEIRAS	VÍRUS	ESFORÇO FÍSICO INTENSO	ARRANJOS FÍSICOS INADEQUADOS
VIBRAÇÕES	FUMOS	BACTÉRIAS	LEVANTAMENTO E TRANSPORTE MANUAL DE CARGAS	MAQUINAS E EQUIPAMENTOS SEM PROTEÇÃO
RADIAÇÕES IONIZANTES	NÉVOAS	PROTOZOÁRIOS	EXIGÊNCIA DE POSTURA INADEQUADA	FERRAMENTAS INADEQUADAS OU DEFEITUOSAS
RADIAÇÕES NÃO IONIZANTES	NEBLINAS	FUNGOS	CONTROLE RÍGIDO DE PRODUTIVIDADE	ILUMINAÇÃO INADEQUADA
FRIO	GASES	PARASITAS	IMPOSIÇÃO DE RITMOS EXCESSIVOS	ELETRICIDADE
CALOR	VAPORES	BACILOS	TRABALHO EM TURNOS E NOTURNOS	PROBABILIDADE DE INCENDIO OU EXPLOSÃO
PRESSÕES ANORMAIS	SUBSTÂNCIAS COMPOSTAS PRODUTOS QUÍMICOS EM GERAL	PRÍONS*	JORNADA PROLONGADA	ARMAZENAMENTO INADEQUADO
UMIDADE	AERODISPER-SÓIDES	INSETOS NOCIVOS E ANIMAIS PEÇONHENTOS	MONOTONIA E REPETIVIDADE	ANIMAIS PEÇONHENTOS
OUTRAS SITUAÇÕES CAUSADORAS DE RISCOS FÍSICOS	OUTRAS SITUAÇÕES GERADORAS DE RISCOS QUÍMICOS	OUTRAS SITUAÇÕES DE RISCO QUE PODERÃO CONTRIBUIR PARA OCORRENCIA DE RISCOS BIOLÓGICOS	OUTRAS SITUAÇÕES CAUSADORAS DE STRESS FÍSICO E/OU PÍQUICO	OUTRAS SITUAÇÕES DE RISCO QUE PODERÃO CONTRIBUIR PARA OCORRENCIA DE ACIDENTES

Figura 10.: Mapa de riscos de segurança.