**SIMULACIÓN DE UNA RED LAN CON PROTOCOLOS DE SEGURIDAD**

**ASIGNATURA: REDES DE COMPUTADORAS**

**REALIZADO POR: LUIS FELIPE VELASCO TAO – JUAN DAVID GONZALES DIMATÉ**

**DESCRIPCIÓN:**

Una empresa pequeña, requiere la implementación de una red LAN pequeña, que tenga distintos equipos, los cuales puedan comunicarse entre sí, sin ningún problema, hacer uso de una impresora, además de requerir un servidor de donde se tenga acceso a la información de la empresa, y a esta red, aplicarle los protocolos de seguridad acordes a la estructura de la red

**OBJETIVO:**

Diseñar una red LAN con protocolos de seguridad, aplicando pruebas para corroborar el correcto funcionamiento.

**OBJETIVOS ESPECÍFICOS:**

* Simular el diseño de la red LAN en Cisco Packet Tracer
* Configurar los dispositivos requeridos para la red
* Aplicar medidas de seguridad a la red
* Realizar validaciones del funcionamiento de la red

**TEMÁTICAS:**

En este proyecto se tocarán las siguientes temáticas:

* Topologías de red: para el caso que se planteara en donde se requiere una red LAN, se requiere saber la forma en que se encontraran conectados los nodos o Hosts que conformaran la red.
* Configuración de dispositivos: luego de plantear la topología y los dispositivos requeridos, se deben realizar las configuraciones básicas de seguridad y conectividad de la red, como lo es el cableado, configuración de direcciones IP, seguridad de consola de dispositivos, etc.
* Medidas de seguridad en redes: Al momento de tener ya un diseño en específico y una configuración básica de dispositivos, lo importante es saber ahora que medidas de seguridad podemos aplicar acorde a la estructura que hayamos creado.

**RECOPILACIÓN DE INFORMACIÓN**

Las redes son parte importante hoy en día en la comunicación, en los entornos de trabajo y en el entretenimiento, enfocándonos en uno de los entornos en donde la información es preciada y de vital importancia como lo son las empresas, las cuales tienen acceso a volúmenes de información considerables, y requieren de mecanismos que les permitan delimitar el acceso a dicha información. Como parte de la funcionalidad de una red LAN se puede considerar la importancia del diseño que delimite las zonas o los hosts de una empresa que tendrán acceso a la información y a cuál.

Como ejemplo práctico, una pequeña empresa de no más 10 trabajadores, requiere una red en donde todos los equipos puedan enviar y recibir información entre sí, pero se priorice la división del personal en dos oficinas, y que estos puedan compartir información entre sí de forma práctica, además de tener una única impresora en toda la empresa. Aunque se plantee el escenario de una pequeña empresa, esa estructura que se describe es el inicio de una red que puede expandirse a la par de las necesidades de una empresa.

Dentro de estas prioridades, hay una que es vital: la seguridad de la misma red. Esta seguridad, sin importar el tamaño de la red, es prioridad debido al transito de información que tendrá la red. Como primera recomendación dada por (Locura InformaticaDigital, 2020) “*Una estrategia común es instalar un recurso de firewall detrás de un solo punto de acceso, como un enrutador inalámbrico inicial* .”, recordemos la funcionalidad de los firewalls o cortafuegos, la cual es interrumpir el acceso a conexiones externas a la red, en este caso, se recomienda que el firewall sea un dispositivo programable, el cual pueda definir las conexiones permitidas y bloquear cual intento de acceso por parte de intrusos o personal no autorizado.

Siguiendo las recomendaciones dadas por (Locura InformaticaDigital, 2020) ,tenemos que realizar un reconocimiento de la red a proteger, ver aquellos componentes de mayor fragilidad o por medio de los cuales, los atacantes pueden tener acceso a la información, delimitar las funciones que pueden realizar los usuarios desde los equipos conectados en la red, esto pudiendo realizarse por medio de políticas de seguridad que la misma empresa puede implantar con el soporte de expertos en seguridad. Acompañados de estas políticas, si en la red existen puntos de conexión inalámbrica, (Culturacion, 2018) recomienda lo siguiente “*es apropiado usar protocolos de seguridad específicos, como WPA, WPA2o WPA3 para el cifrado de contraseñas en el tráfico procedente de Internet.*” Entender que de estos protocolos implicaran el uso de dispositivos y de personal capacitado para su implantación dentro de la red.

Ya que hablamos de dispositivos para la seguridad, podemos hablar de los Routers, como lo indica (Engineering, 2019):

*Otra medida que debemos tomar con un router, es verificar los logs o los registros. De esta manera, podremos tener información valiosa sobre las direcciones IP que se han intentado conectar de forma irregular a nuestra red, para que podamos tomar medidas de protección al respecto.*

Se menciona aquí algo importante: los registros. Sin importar el tamaño de la red, es importante destacar que estos registros que realizan los Routers, ya que les servirá a los administradores de las redes conocer el comportamiento de los equipos dentro de la red, y, dado sea el caso que haya habido algún ingreso indebido a la red, poder detectar desde donde se realizó, y si se realizó alguna actividad ilegal, poder aplicar las medidas legales correspondientes.

Con relación al control de accesos, debemos entender la importancia del uso de contraseñas y sistemas criptográficos que le provean mayor seguridad, además de la implementación de claves públicas y privadas, como lo indica (Sist de Información UNAN & Estelí Manuel Rivas Chavarría, n.d.) quien habla de la importancia de la autenticación de lo usuarios, los controles periódicos para revisar las credenciales de los empleados, las páginas de internet o intranet a las cuales tendrán acceso desde los equipos de la red, la forma de autenticar su acceso a información contenida en el servidor, dicha información también se recomienda estar bajo un sistema de cifrado que le dificulte al atacante de la red la obtención inmediata de la información.

Otro punto importante en la seguridad, de cualquier red, es el conocimiento de las amenazas de dicha red, esto es importante ya que, cualquier empresa debe considerar la implementación de un Sistema de Gestión de Seguridad de la Información todo esto de la mano de profesionales de la seguridad informática conocedores de los estándares ISO 27000. Especialmente de las normas ISO 27001 (Organización Internacional de Estándares, 2013) y 27002 (Organización Internacional de Normalización, 2013c, 2013a, 2013b) en donde se especifica el proceso de implementación de un SGSI y las medidas relacionadas con el acceso a la información, seguridad de los servidores y mantenimiento de el hardware, entre demás ítems importantes dentro de una red.

Finalmente, adentrándonos en la seguridad de Hosts, hay que reconocer los riesgos a los que se están los disipativos con acceso a internet, dando directrices al acceso a la red, las paginas a las cuales los empleados tienen o no tiene permiso para acceder, como también al acceso de documentos que se encuentren en internet y los sitios de donde son extraídos. Frente e a estos y otros riesgos podemos mencionar el libro Seguridad y Alta Disponibilidad (Costas, 2011) en donde se nos da un amplio recorrido frente a amenazas, medidas de protección a los dispositivos de la red, protocolos de seguridad y demás medidas importantes para la gestión de una red lo más segura posible.

**COMPETENCIAS A DESARROLLAR:**

1. Manejo de Cisco Packet Tracer
2. Diseño de una red LAN inalámbrica
3. Configuración básica de dispositivos (PC, Laptops, Switches, etc.)
4. Medidas y protocolos de seguridad en redes LAN inalámbricas

**CONOCIMIENTOS PREVIOS REQUERIDOS:**

1. Direcciones IP
2. Topologías de red
3. Conectividad entre equipos

**RECURSOS A NIVEL HARDWARE Y SOFTWARE:**

1. Computadores Personales
2. Repositorios institucionales (Aclarar Repositorios)
3. Cisco Packet Tracer

**METODOLOGÍA:**

Para el desarrollo de este proyecto se va a usar la **metodología CISCO** para el diseño de redes, en la cual se busca definir actividades mínimas requeridas, de modo cual se pueda basarse en la tecnología y la complejidad de la red, para de este modo presentar un buen producto a nuestros clientes, instalando y finalmente operando

1. **Preparación**En esta etapa se generará un caso de uso financiero en el cual se soporte el uso de una red, empezando a pensar la arquitectura en la cual se soportará la red requerida.
2. **Planeación**

En esta etapa se identificarán los requerimientos de la red, todo esto por medio de un análisis, identificación y valoración de la red que se planteo previamente, de este modo se evaluaran las mejoras que se deben realizar sobre la arquitectura establecida previamente.

1. **Diseño**

En esta etapa se generará un diseño detallado basado en los requerimientos, la arquitectura y la naturaleza del negocio, de este modo se ejemplificará la forma de la red, la conectividad, los dispositivos que se van a usar en la red, la configuración de estos y demás particularidades propias de la red. (en este caso, el mismo diseño será la simulación sobre la cual se realizarán las pruebas).

1. **Implementación**

En esta etapa se aplicarán en el entorno físico de la organización todos los dispositivos, configuraciones y conectividad entre los disipativos, además de que cabe resaltar que en esta etapa se debe garantizar que a futuro se puede ampliar en base a la misma arquitectura la red creada.

1. **Operación**

En esta etapa se entrará en ejecución la red, de modo tal se compruebe el correcto funcionamiento de esta, o mejoras requeridas para su correcta operación, además de que podrán a prueba la estabilidad y seguridad de la red.

1. **Optimización**

En esta etapa, basándose en los resultados dados en la etapa de Operación, se harán los cambios requeridos para el correcto funcionamiento de la red.

1. **Documentación**

Finalmente se realiza la etapa de documentación, por medio de la cual se dejará constancia de todo lo realizado a lo largo del proyecto, de este modo se conocerán las configuraciones realizadas, los disipativos y demás actividades que se llevaron a cabo para cumplir el objetivo del proyecto.

**DESARROLLO**

1. **Preparación**

Como parte del proceso en la identificación de los requerimientos de la red, en este caso supositorio, se va a generar una lista de requerimientos y una descripción del negocio.

* + Descripción: “Estoy iniciando una nueva empresa de textiles en la cual voy a tener varios trabajadores, requiriendo una oficina donde se encuentre un equipo para mí y mi secretaria, en otras dos oficinas tendré a unos trabajadores encargados de actividades propias de la empresa, como el manejo de contratos, recibos, control de personal y demás actividades propias, por el momento también requeriré una impresora para toda la empresa, y también a futuro planeo poder tener algún servicio web para la administración de toda la empresa. Por otro lado, también quisiera una conexión inalámbrica para los clientes en la sala de espera”

Por medio de esta descripción generada por el cliente se puede suponer la necesidad de una red de bus, la cual requiera un servidor web y con un segmento inalámbrico externo a la red.

1. **Planeación**

Basado en esta descripción se generan los siguientes requerimientos

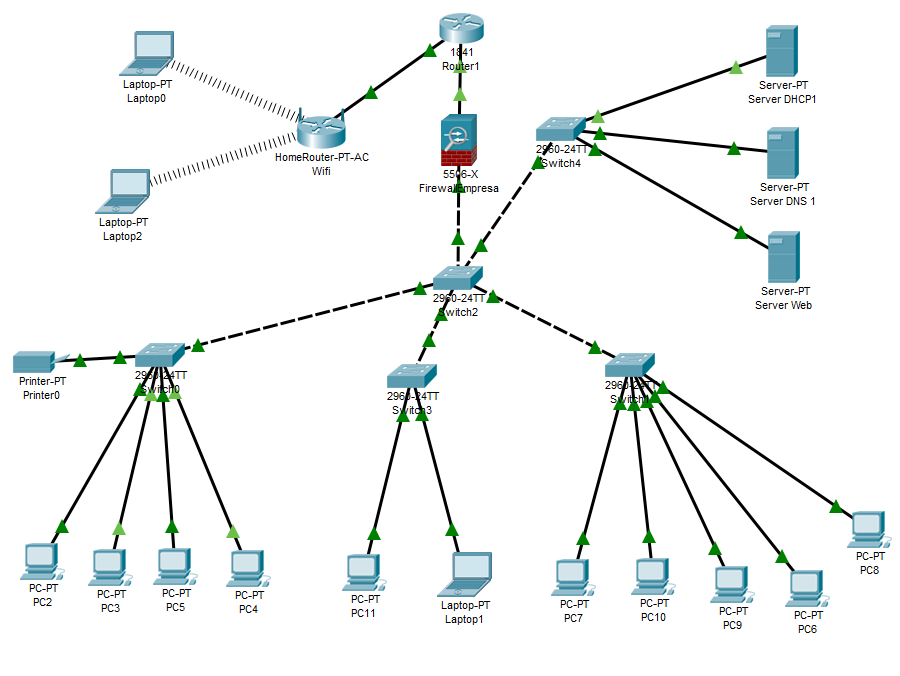
* 1. Se requiere la construcción de una red local
  2. Se requieren el uso de algunos servidores, tanto para poder gestionar el crecimiento de la red, como para una futura implementación de una aplicación web
  3. Según el cliente, no se requiere delimitar la conexión entre nodos, por lo que será una red que posibilite la comunicación entre todos los nodos
  4. Se requiere una parte de la red inalámbrica que no permita la conexión con los demás nodos internos de la empresa

Como parte de los requerimientos que le prestaran seguridad y garantizan un funcionamiento eficaz para la red se incluyen los siguientes:

* 1. Se requiere una red conexa
  2. Se requiere algún método de protección para la red empresarial
  3. Se requiere un servidor DHCP por medio del cual se administren las direcciones IP para los equipos, de este modo se posibilitará la expansión de la red.

1. **Diseño**

Con los requerimientos establecidos previamente, se genera un diseño como el que se encuentra a continuación, por medio del cual se



**La red cuenta con:**

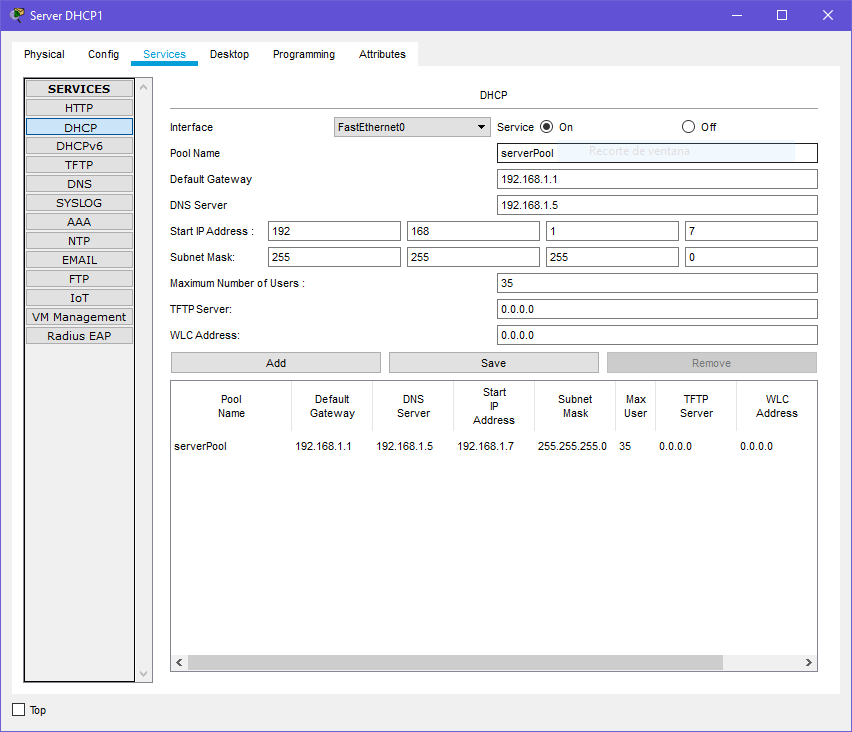
1. 11 equipos, entre PCs y Portátiles los cuales se encuentran dentro de la red de la empresa.
2. Una impresora la cual servirá para la impresión de archivos dentro de la empresa.
3. 5 Switches configurados con protocolos básicos de seguridad y VLANS activas, por medio de los cuales se genera la distribución requerida por la empresa.
4. 1 Router configurado con protocolos básicos de seguridad y las IPs correspondientes, junto a este se encuentra un equipo que servirá como administrador de la red.
5. 1 servidor DHCP por medio del cual, los nuevos equipos que se anexen a la red, se les asigne automáticamente una dirección de IP.
6. 1 servidor DNS en el cual servirá para definir el dominio de la empresa.
7. 1 servidor web en el cual se encontrará una página que requiere la empresa para su funcionamiento (aplicación web)
8. 1 firewall por medio del cual se garantizará la seguridad de la red local de la empresa.
9. Un router Wifi por medio del cual se brinde el servicio de conectividad para los clientes que lleguen a la empresa.

**Se adjunta archivo con la simulación de la red realizada en Packet Tracer**

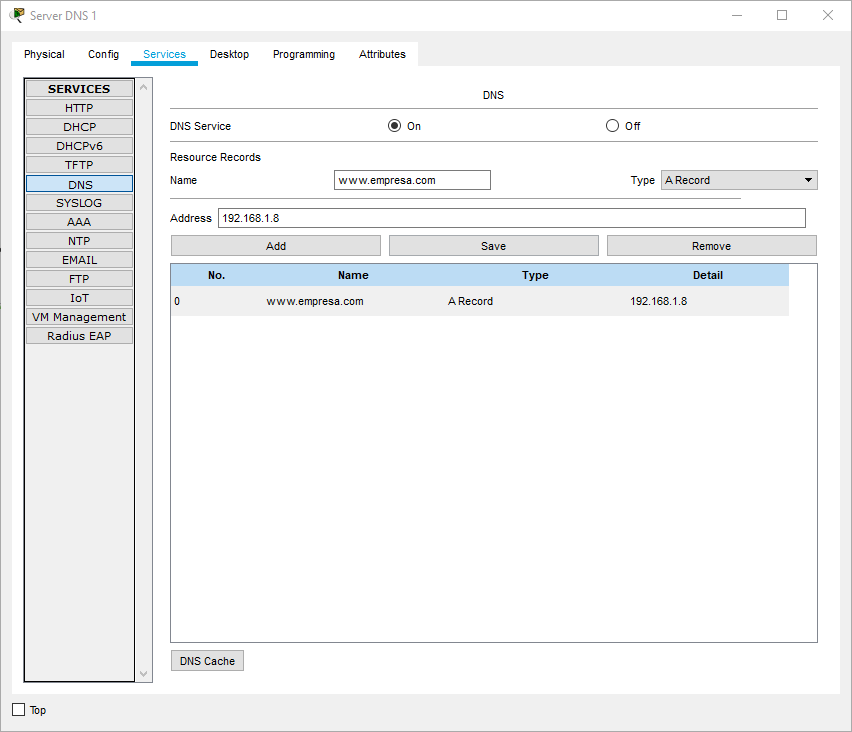
1. **Implementación**

Como parte de la implementación, vendría la configuración de los servidores

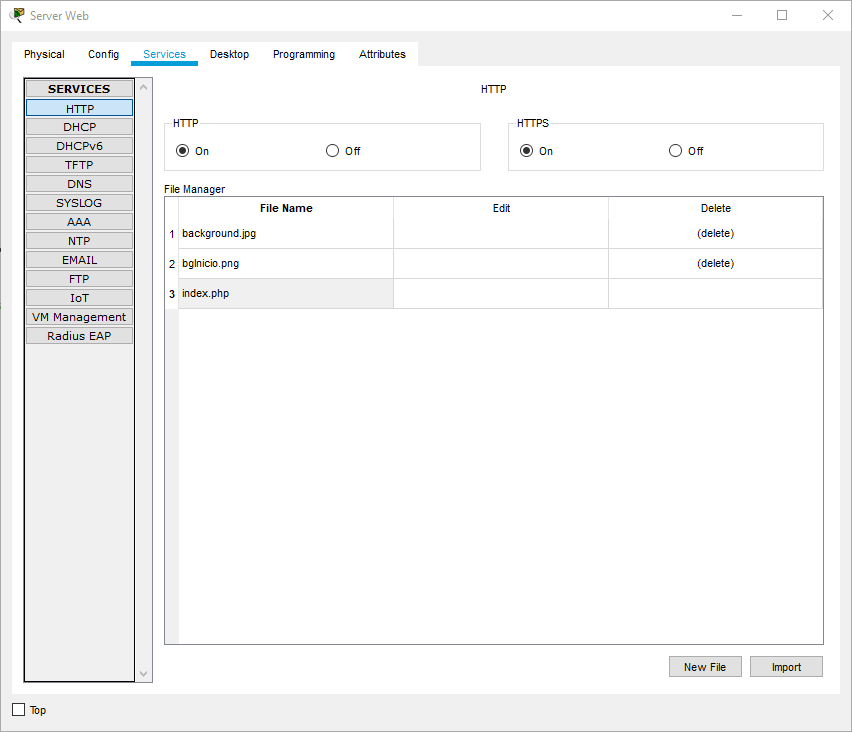
* 1. Servidor DHCP



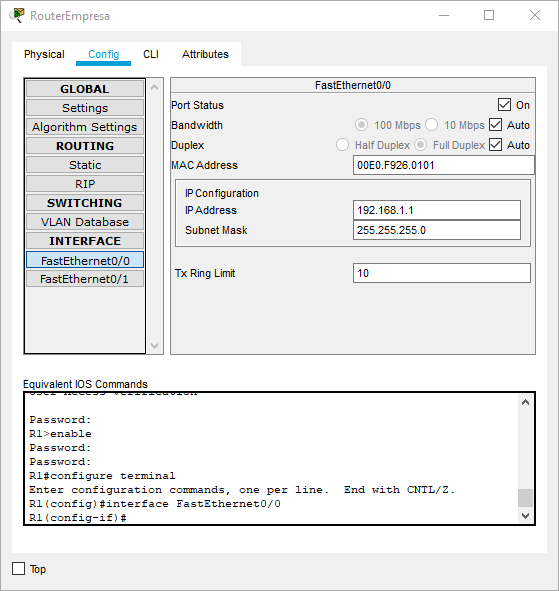
* 1. Servidor DNS



* 1. Servidor Web



También configuramos el router, este tiene aplicado medidas de seguridad básicas.



**PRODUCTOS Y RESULTADOS ESPERADOS:**

Como resultado final de este proyecto se espera una simulación realizada en Cisco Packet Tracer por medio de la cual se ejemplifique el funcionamiento de la red requerida en el planteamiento del proyecto.

**BIBLIOGRAFÍA LIBROS DIGITALES DE LA UNIVERSIDAD:**

**BIBLIOWEB:**

Costas, J. (2011). *Seguridad y Alta Disponibilidad* (1st ed., Vol. 1). RA-MA Editorial. https://www.academia.edu/8334995/Seguridad\_y\_Alta\_Disponibilidad\_RAMA

Culturacion. (2018, November 1). *Cómo proteger una red LAN - Culturación*. https://culturacion.com/como-proteger-una-red-lan/

Engineering, N. (2019, May 6). *Ingeniería de redes, telecomunicaciones y ciberseguridad en Barcelona*. Net Cloud Engineering; NetCloud Engineering. https://netcloudengineering.com/funcionamiento-redes-lan/

Locura InformaticaDigital. (2020). *¿Cómo dar seguridad a una Red de Área Local (LAN)? | guía práctica*. ¿Cómo Dar Seguridad a Una Red de Área Local (LAN)? https://www.locurainformaticadigital.com/2018/06/27/seguridad-a-una-red-de-area-local/

Organización Internacional de Estándares. (2013). *ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online*. NORMA ISO 27001:2013. https://normaiso27001.es/#h4

Organización Internacional de Normalización. (2013a). *ISO 27002 punto por punto A12 Seguridad de las Operaciones*. A12 SEGURIDAD DE LAS OPERACIONES. https://normaiso27001.es/a12-seguridad-de-las-operaciones/

Organización Internacional de Normalización. (2013b). *ISO 27002 Punto por punto A7 Seguridad relativa a los recursos*. A7 SEGURIDAD RELATIVA A LOS RECURSOS. https://normaiso27001.es/a7-seguridad-relativa-a-los-recursos/

Organización Internacional de Normalización. (2013c). *ISO 27002 punto por punto A9 Control de acceso - Caso Práctico*. A9 CONTROL DE ACCESO. https://normaiso27001.es/a9-control-de-acceso/

Sist de Información UNAN, I., & Estelí Manuel Rivas Chavarría, F. (n.d.). *Asignatura: Redes Telemáticas*.

**AUTOR: Luis Felipe Velasco Tao – Juan David González Dimaté**