**INSTITUTO DE EDUCACIÓN SUPERIOR TECNOLÓGICO PRIVADO CERTUS**

**“Año …“**

Un hombre sentado frente a una computadora

Descripción generada automáticamente con confianza media

**DISEÑO E IMPLEMENTACION DE UNA RED PARA LA EMPRESA ..**

**ALUMNOS:**

* **Angel Arteaga Gonzales**
* **Brad Rodriguez Bardales**
* **Maruan Piter Quezada**

**CICLO: 3**

**SECCIÓN:**

**TURNO: Noche**

**DOCENTE: ALDO HUMBERTO AMAYA**

**EVALUACIÓN DE LA ACTIVIDAD DE APRENDIZAJE AA2**

**INDICE**

**CAPITULO I – LA EMPRESA**

* 1. Descripción
  2. Ubicación

**CAPITULO II – INVESTIGACIÓN TECNOLOGICA**

* 1. Conceptos básicos de redes LAN
  2. Conceptos de VLAN
  3. Enrutamiento entre VLAN
  4. Conceptos de enrutamiento de redes
     1. Protocolo de enrutamiento OSPFv2
     2. Traducción de direcciones de red
  5. Arquitectura de seguridad de red
     1. Terminología de seguridad
     2. Seguridad en dispositivos de red
  6. Seguridad en capa 3
     1. Control de lista de accesos
  7. Redes privadas virtuales
     1. Conceptos sobre redes privadas virtuales

**CAPITULO III – APORTE PRACTICO**

* 1. Diseñando la red
     1. Implementando el diseño en Packet Tracer
  2. Asignación del direccionamiento de red
  3. Implementación VLAN
     1. Creación las VLAN en los switches
     2. Asignación VLAN a los puertos de los switches
     3. Configurando los enlaces troncales
  4. Configuración de enrutamiento entre VLAN
  5. Enrutamiento entre sedes
     1. Configuración de router
     2. Configuración de direccionamiento en cada interfaz
     3. Implementación de enrutamiento OSPFv2
     4. Implementación NAT
  6. Seguridad de red
     1. Implementar reglas de seguridad en los dispositivos de red
     2. Configuración de Port security
     3. Implementar reglas de control de acceso
     4. Configuración de acceso remoto
  7. Evaluando los costos de red
     1. Evaluando costos de hardware
     2. Evaluando costos de software

**BIBLIOGRAFIA**

**CAPITULO I – LA EMPRESA**

* 1. Descripción

La empresa Ranbank se dedica al rubro financiero desde hace 17 años y, debido a la coyuntura de la pandemia covid-19, ha tenido que implementar nuevos servicios tecnológicos para sus clientes con el objetivo de mejorar su infraestructura actual y brindarles un correcto soporte a sus operaciones.

* 1. **Ubicación**

Av. Santiago de Surco N° 4717, Santiago de surco 15039

**CAPITULO II – INVESTIGACIÓN TECNOLOGICA**

* 1. **Conceptos básicos de redes LAN**

Entre las redes informáticas se encuentra la llamada red LAN, una sigla que refiere a Local Area Network (Red de Área Local). Estas redes vinculan computadoras que se hallan en un espacio físico pequeño, como una oficina o un edificio. La interconexión se realiza a través de un cable o de ondas.

A través de una red LAN pueden compartirse recursos entre varias computadoras y aparatos informáticos (como teléfonos celulares, tabletas, etc.), tales como periféricos (impresoras, proyectores, etc.), información almacenada en el servidor (o en los computadores conectados) e incluso puntos de acceso a la Internet, a pesar de hallarse en habitaciones o incluso pisos distintos.

Este tipo de redes son de uso común y cotidiano en negocios, empresas y hogares, pudiendo presentar una topología de red distinta de acuerdo a las necesidades específicas de la red, tales como:

* Red en bus: En la que un mismo cable (o backbone) conecta a las computadoras y permite la transmisión de datos en línea recta, haciéndola sencilla pero susceptible a daños del cable o a la interrupción del tráfico.
* Red en estrella: En la que todos los computadores se conectan a un servidor central que administra los recursos de la red y los asigna según se le solicite.
* Red en anillo: En la que todos los computadores están conectados con sus vecinos mediante una transmisión unidireccional, que interrumpe la red de haber un fallo en algún nivel de la misma.
  1. **Conceptos de VLAN**

Una VLAN – Virtual Local Área Network o Red de Área Local Virtual- es una división de red que se realiza de forma virtual. Como su nombre indica, la técnica consiste en crear una red virtual dentro de un único dispositivo, normalmente un switch.

Características de una VLAN

* Las VLAN pueden mejorar significativamente la seguridad dentro de una red física. Aunque un atacante se aproveche de un punto de seguridad vulnerable, este no puede acceder a toda la red si está dividida en VLAN.
* Es posible que diferentes áreas de una misma empresa tengan sus propias redes. Esto permite, por ejemplo, un intercambio de datos más rápido y la distribución de diferentes programas entre los ordenadores o servidores.
* Las VLAN permiten además plasmar cambios más fácilmente.

Tipos de VLAN:

* VLAN basada en puertos:

Las VLAN basadas en puertos dividen los modificadores físicos (también llamados switches) en múltiples modificadores lógicos. Los puertos individuales se asignan a un switch lógico o a una VLAN. Para ello es necesario que los modificadores se puedan configurar. Por regla general, sólo se puede acceder a la dirección IP del switch a través de los puertos asignados de forma permanente a esta VLAN. Los paquetes de datos no se marcan por separado para las VLAN basadas en puertos. Basándose en el número del puerto en el que recibe un paquete de datos, el modificador sabe a qué VLAN debe asignar el paquete de datos.

* VLAN etiquetadas:

Las VLAN etiquetadas no tienen una asignación fija entre la red virtual y un puerto. La asignación se realiza marcando los paquetes de datos. Los paquetes de datos están provistos de etiquetas en las que se almacena el ID de la VLAN. Este proceso se denomina VLAN trunking. Según IEEE 802.1Q, esto se realiza mediante el dispositivo final correspondiente (por ejemplo, un servidor habilitado para etiquetado) o mediante un switch. Mediante el ID de VLAN, un modificador puede reconocer a qué VLAN pertenece el paquete de datos. De este modo, el enlace VLAN permite utilizar varias VLAN a través de un único puerto de conmutación. Así se pueden utilizar una o varias líneas concatenadas.

* 1. **Enrutamiento entre VLAN**

Las VLAN se utilizan para segmentar las redes de switch de Capa 2 por diversas razones. Independientemente del motivo, los hosts de una VLAN no pueden comunicarse con los hosts de otra VLAN a menos que haya un router o un switch de capa 3 para proporcionar servicios de enrutamiento.

* 1. **Conceptos de enrutamiento de redes**
     1. **Protocolo de enrutamiento BGP**

El protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos AS

* + 1. **Traducción de direcciones de red**

La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT, es un mecanismo utilizado por routers IP para cambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

* 1. **Arquitectura de seguridad de red**
     1. **Terminología de seguridad:**

La terminología de seguridad se refiere al conjunto de términos y conceptos utilizados en el campo de la seguridad de la información y la protección de activos. A continuación, se presentan algunas de los principales términos utilizados en este ámbito:

1. Seguridad de la información: Conjunto de medidas y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información.
2. Amenaza: Cualquier evento o circunstancia que pueda causar daño a los activos de información o interrumpir los procesos normales de una organización. Pueden incluir ataques cibernéticos, desastres naturales, errores humanos, entre otros.
3. Vulnerabilidad: Debilidad o fallo en un sistema o proceso que podría ser aprovechado por una amenaza para comprometer la seguridad. Las vulnerabilidades pueden existir en software, hardware, configuraciones incorrectas, entre otros.
4. Riesgo: Probabilidad de que una amenaza se aproveche de una vulnerabilidad y cause un impacto negativo. El riesgo se calcula evaluando la probabilidad de ocurrencia de una amenaza y su impacto potencial.
5. Ciberseguridad: Conjunto de medidas y técnicas utilizadas para proteger los sistemas y datos en el entorno digital, especialmente contra ataques informáticos y el acceso no autorizado.
6. Ataque: Acción deliberada realizada por un individuo o grupo con el objetivo de comprometer la seguridad de un sistema o red. Los ataques pueden incluir malware, phishing, denegación de servicio, entre otros.
7. Firewall: Dispositivo o software utilizado para controlar el tráfico de red y aplicar políticas de seguridad. Un firewall actúa como una barrera entre redes confiables y no confiables, y ayuda a prevenir el acceso no autorizado.
8. Intrusión: Acceso no autorizado a un sistema o red por parte de un individuo no autorizado. Una intrusión puede ser el resultado de un ataque exitoso.
9. Autenticación: Proceso de verificar la identidad de un usuario o dispositivo para garantizar que tenga los permisos necesarios para acceder a un sistema o recurso. La autenticación puede involucrar contraseñas, tarjetas inteligentes, biometría, entre otros.
10. Encriptación: Proceso de codificar la información de manera que solo pueda ser leída por aquellos que poseen la clave de desencriptación. La encriptación se utiliza para proteger la confidencialidad de los datos.
    * 1. **Seguridad en dispositivos de red**

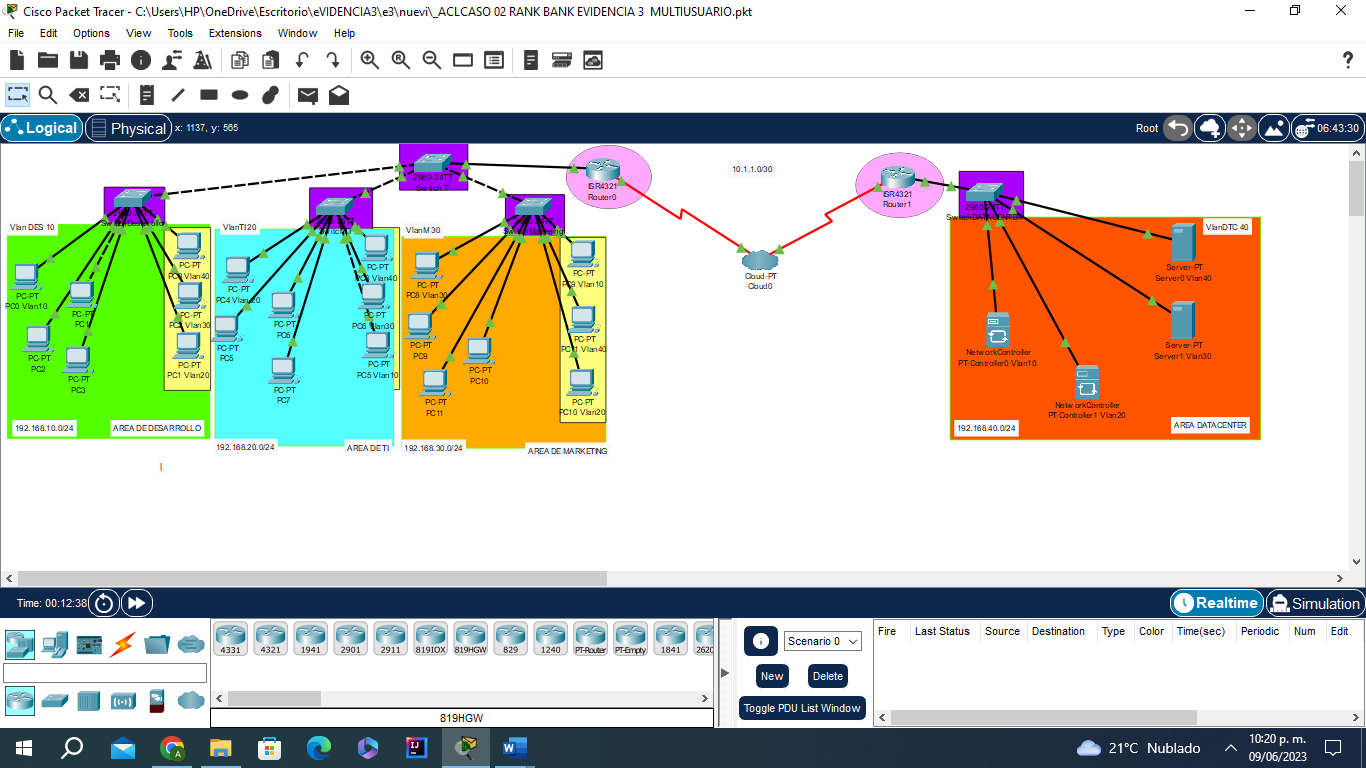
La seguridad en dispositivos de red es crucial para proteger la integridad, confidencialidad y disponibilidad de los datos y recursos que se transmiten a través de una red. Aquí hay algunos aspectos clave relacionados con la seguridad en dispositivos de red:

1. Firewall: Un firewall es una medida de seguridad fundamental en cualquier red. Actúa como una barrera entre redes confiables y no confiables, controlando el tráfico de red y aplicando políticas de seguridad. Los firewalls pueden ser hardware o software y ayudan a prevenir accesos no autorizados y ataques externos.
2. Actualizaciones de firmware: Los dispositivos de red, como routers, switches y puntos de acceso inalámbrico, tienen firmware que requiere actualizaciones periódicas. Estas actualizaciones a menudo incluyen correcciones de seguridad importantes para abordar vulnerabilidades conocidas. Es esencial mantener los dispositivos actualizados para evitar posibles brechas de seguridad.
3. Configuración segura: Configurar los dispositivos de red de manera segura es crucial para mitigar riesgos. Esto incluye cambiar las contraseñas predeterminadas, deshabilitar servicios innecesarios, aplicar políticas de seguridad, establecer cortafuegos internos y segmentar la red en zonas de confianza.
4. Autenticación: Es importante utilizar mecanismos de autenticación fuertes para controlar el acceso a los dispositivos de red. Esto puede incluir el uso de contraseñas seguras, autenticación de dos factores y certificados digitales.
5. Control de acceso: Implementar un control de acceso adecuado es fundamental para limitar quién puede acceder a los dispositivos de red y qué acciones pueden realizar. Esto se logra a través de políticas de acceso basadas en roles, listas de control de acceso (ACL) y autenticación de usuarios.
6. Monitoreo y registro de eventos: Los dispositivos de red deben contar con capacidad de monitoreo y registro de eventos para detectar actividades sospechosas o inusuales. Esto permite una respuesta rápida a incidentes de seguridad y facilita la auditoría de la red.
7. Seguridad inalámbrica: En el caso de dispositivos de red inalámbricos, como puntos de acceso Wi-Fi, se deben utilizar mecanismos de seguridad como el protocolo de seguridad Wi-Fi (WPA2 o WPA3), segmentación de redes inalámbricas y configuración de contraseñas fuertes.
8. Seguridad física: Además de las medidas de seguridad lógica, es importante proteger físicamente los dispositivos de red. Esto implica ubicarlos en lugares seguros, restringir el acceso físico no autorizado y asegurarse de que los cables y conectores estén protegidos.
   1. Seguridad en capa 3
      1. **Control de lista de accesos**

El control de lista de accesos (ACL) es una herramienta de seguridad utilizada en redes informáticas. Consiste en una lista de reglas que determinan qué direcciones IP, usuarios o grupos tienen permiso para acceder a recursos específicos y qué acciones están permitidas. Las ACL se aplican en dispositivos de red como routers, switches y firewalls. Permiten restringir el acceso a recursos sensibles, filtrar el tráfico no deseado y segmentar la red. Configurar y mantener las ACL adecuadamente es importante para garantizar la seguridad de la red.

**CAPITULO III – APORTE PRACTICO**

* 1. Diseñando la red
     1. Implementando el diseño en Packet Tracer



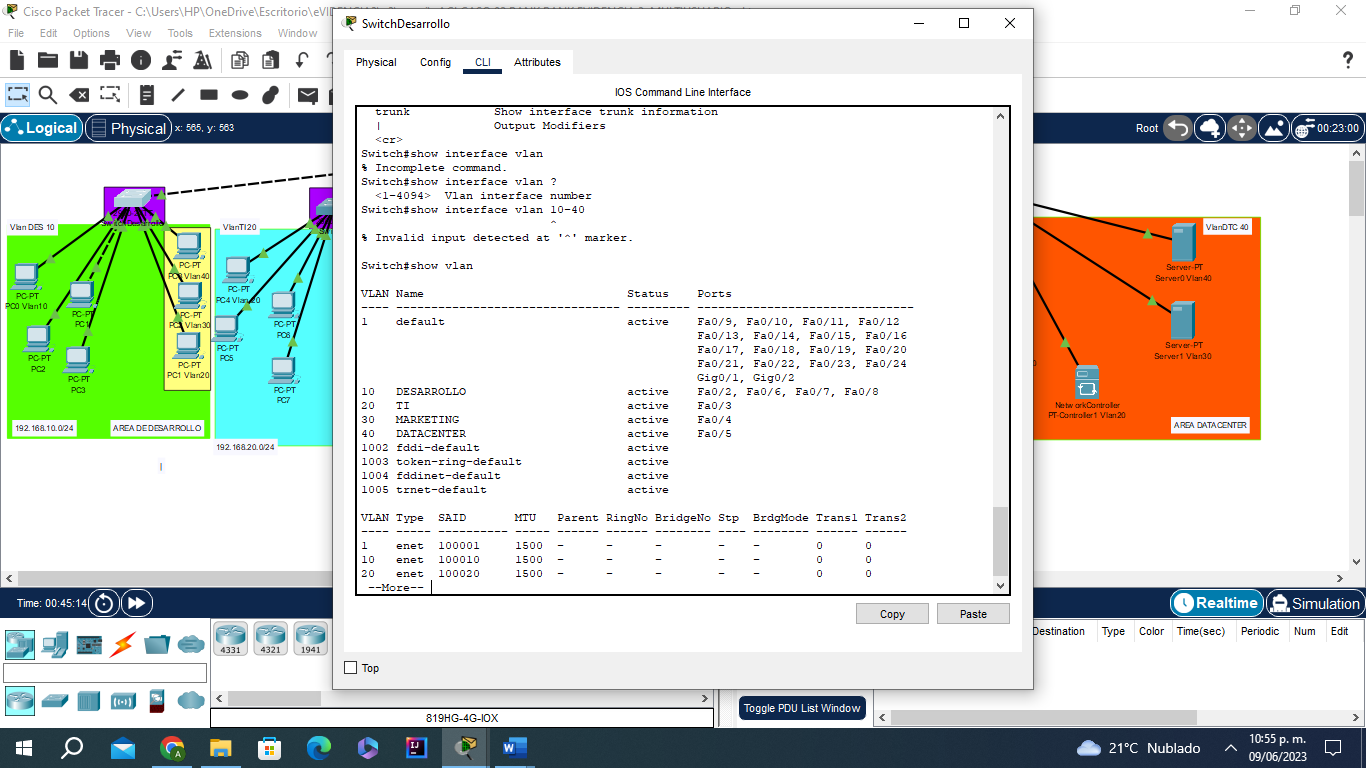
* 1. Asignación del direccionamiento de red

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| --- | --- | --- | --- | --- |
| PC-0 | F0/2 | 192.168.10.2 | 255.255.255.0 | 192.168.10.1 |
| PC-1 | F0/6 | 192.168.10.5 | 255.255.255.0 | 192.168.10.1 |
| PC-2 | F0/7 | 192.168.10.6 | 255.255.255.0 | 192.168.10.1 |
| PC-3 | F0/8 | 192.168.10.7 | 255.255.255.0 | 192.168.10.1 |
| PC-4 | F0/2 | 192.168.20.2 | 255.255.255.0 | 192.168.20.1 |
| PC-5 | F0/6 | 192.168.20.5 | 255.255.255.0 | 192.168.20.1 |
| PC-6 | F0/7 | 192.168.20.6 | 255.255.255.0 | 192.168.20.1 |
| PC-7 | F0/8 | 192.168.20.7 | 255.255.255.0 | 192.168.20.1 |
| PC-8 | F0/2 | 192.168.30.2 | 255.255.255.0 | 192.168.30.1 |
| PC-9 | F0/6 | 192.168.30.5 | 255.255.255.0 | 192.168.30.1 |
| PC-10 | F0/7 | 192.168.30.6 | 255.255.255.0 | 192.168.30.1 |
| PC-11 | F0/8 | 192.168.30.7 | 255.255.255.0 | 192.168.30.1 |
| R-1 | G0/0/0  [SUB-IF (0.10 - 0.40)] | 192.168.(10.1-30.1) / .4.1 | 255.255.255.0 | -- |
| R-2 | G0/0/0  [SUB-IF (0.10 - 0.40)] | 192.168.(1.1-3.1) / .40.1 | 255.255.255.0 | -- |
| R-1 | S0/1/0 | 10.1.1.1 | 255.255.255.252 | -- |
| R-2 | S0/1/0 | 10.1.1.2 | 255.255.255.252 | -- |
| SERVER\_PT-0 | F0/5 | 192.168.40.2 | 255.255.255.0 | 192.168.40.1 |
| SERVER\_PT-1 | F0/4 | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 |
| NETWORK CONTROLLER0 | G/0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| NETWORK CONTROLLER1 | G/0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.1 |

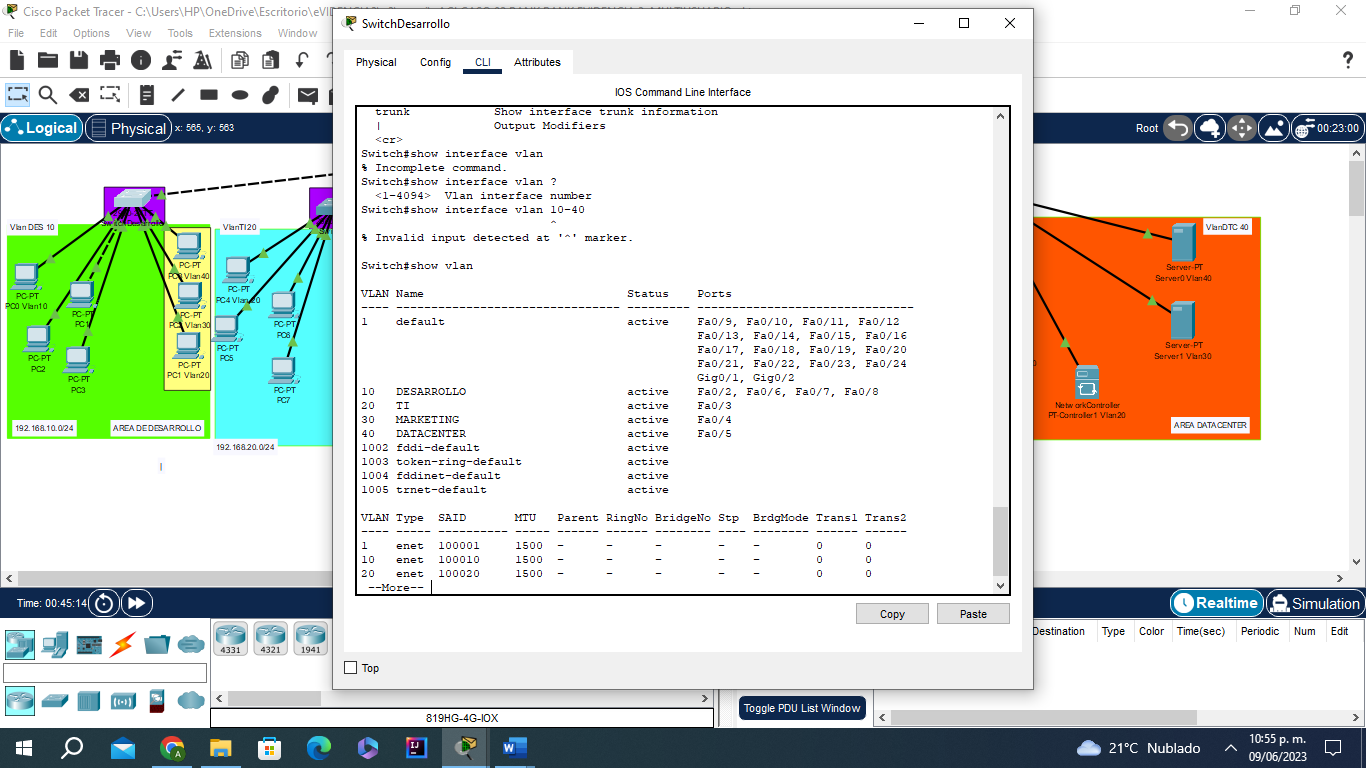
* 1. Implementación VLAN

| VLAN | Nombre | Interfaz asignada |
| --- | --- | --- |
| 10 | DESARROLLO | F0/2 – F0/6 – F0/7 – F0/8 |
| 20 | TI | F0/2 – F0/6 – F0/7 – F0/8 |
| 30 | MARKETING | F0/2 – F0/6 – F0/7 – F0/8 |
| 40 | DATACENTER | F0/2 – F0/6 – F0/7 – F0/8 |

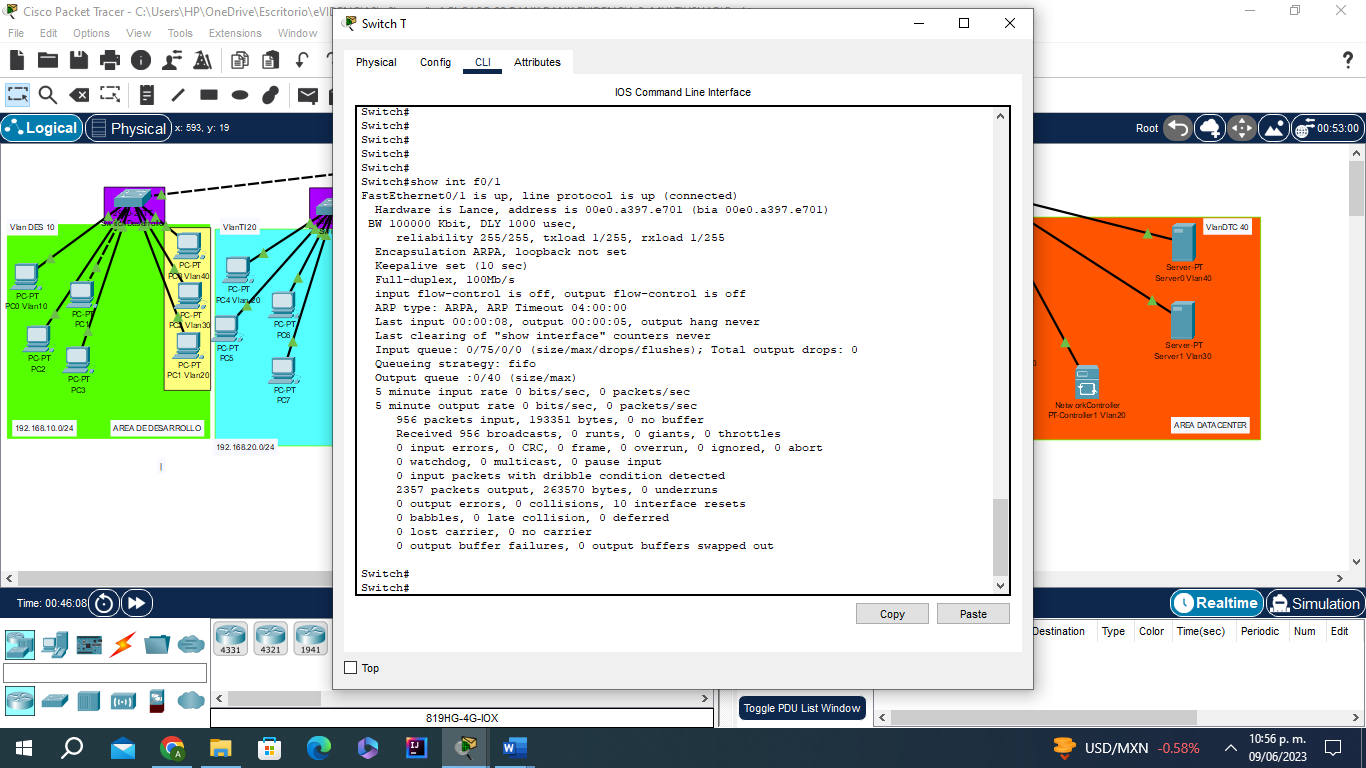
* + 1. Creación las VLAN en los switches



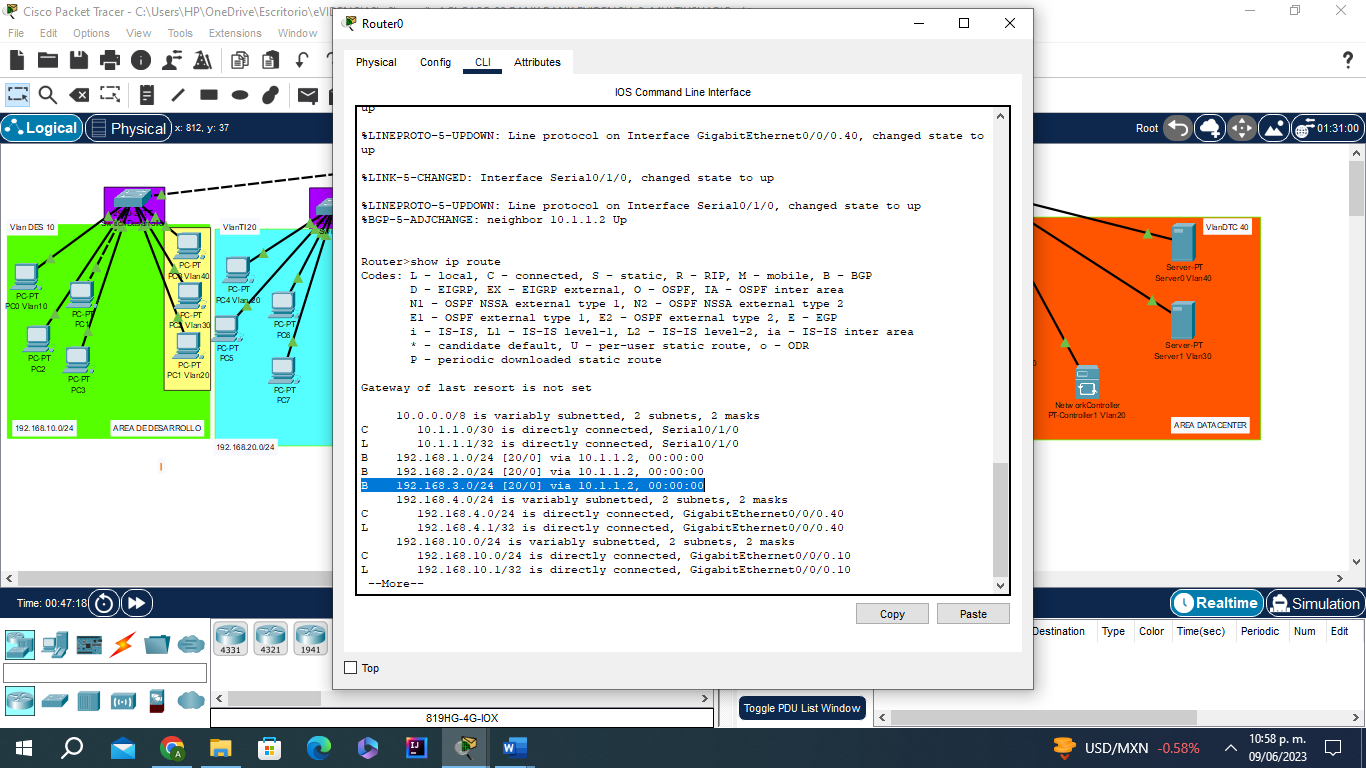
* + 1. Asignación VLAN a los puertos de los switches



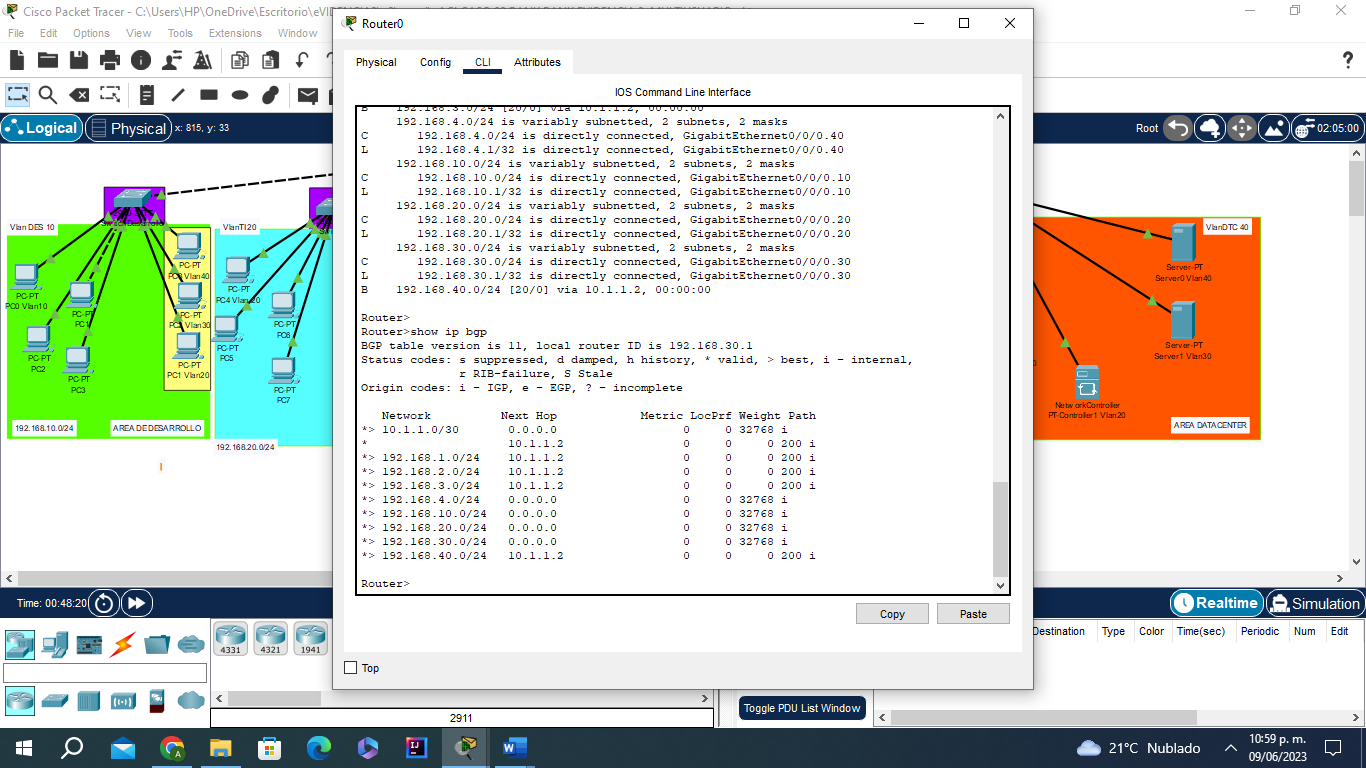
* + 1. Configurando los enlaces troncales



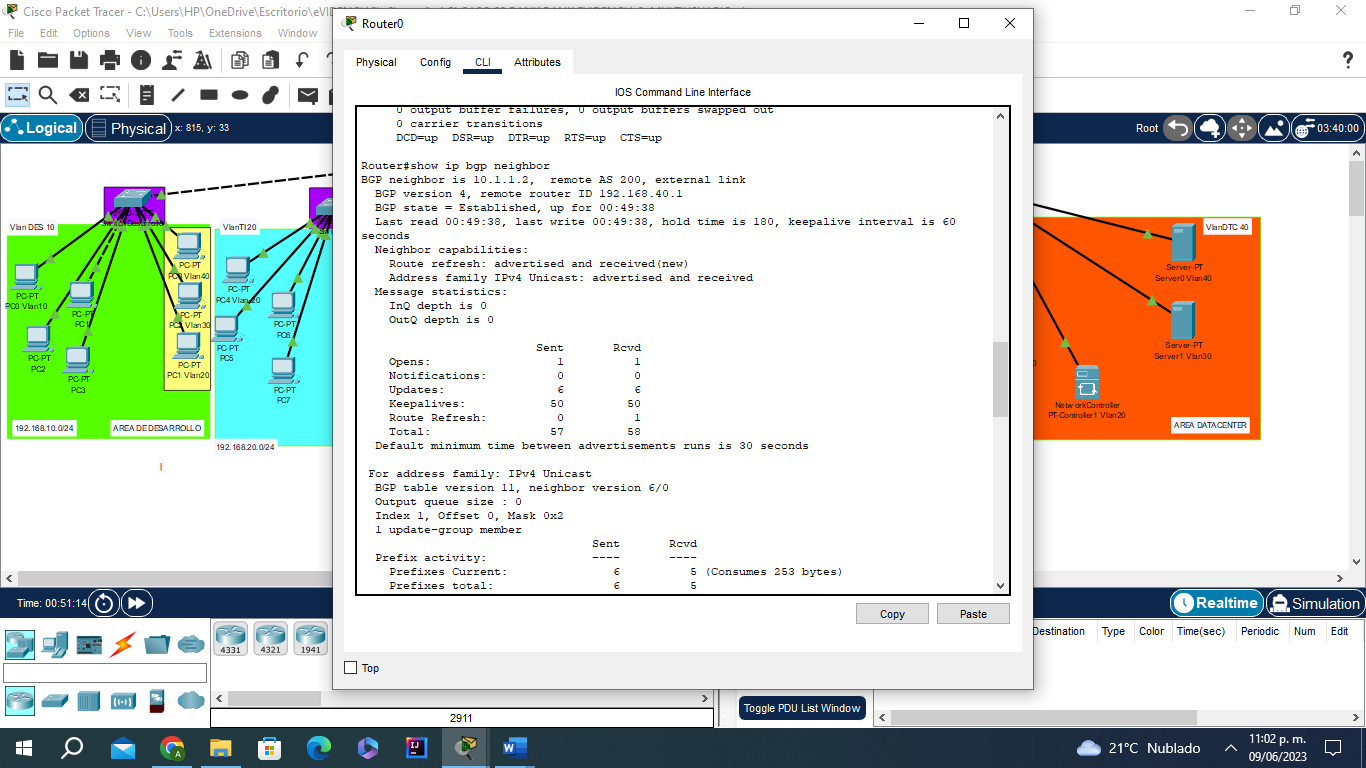
* 1. Configuración de enrutamiento entre VLAN
     1. Configuración del router



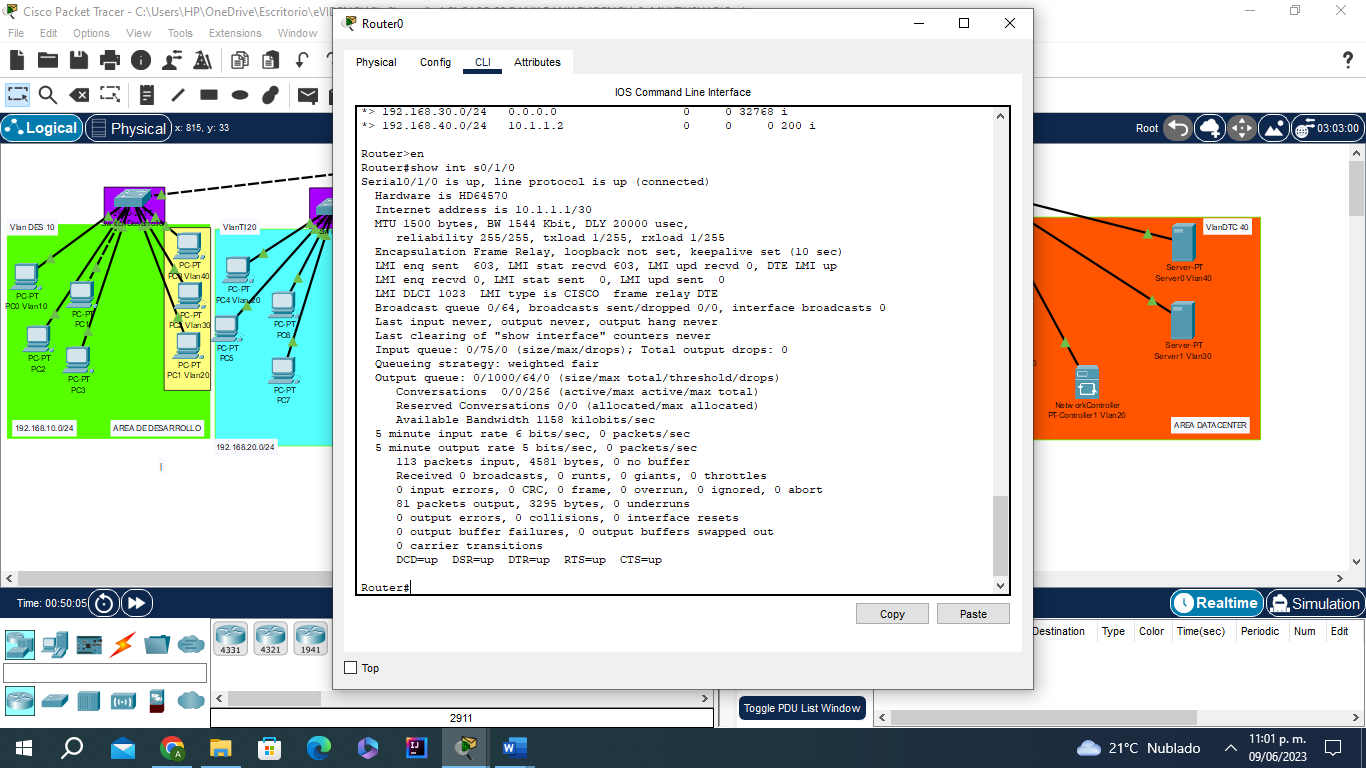
* + 1. Verificación de enrutamiento



* 1. Enrutamiento entre sedes
     1. Configuración de routers

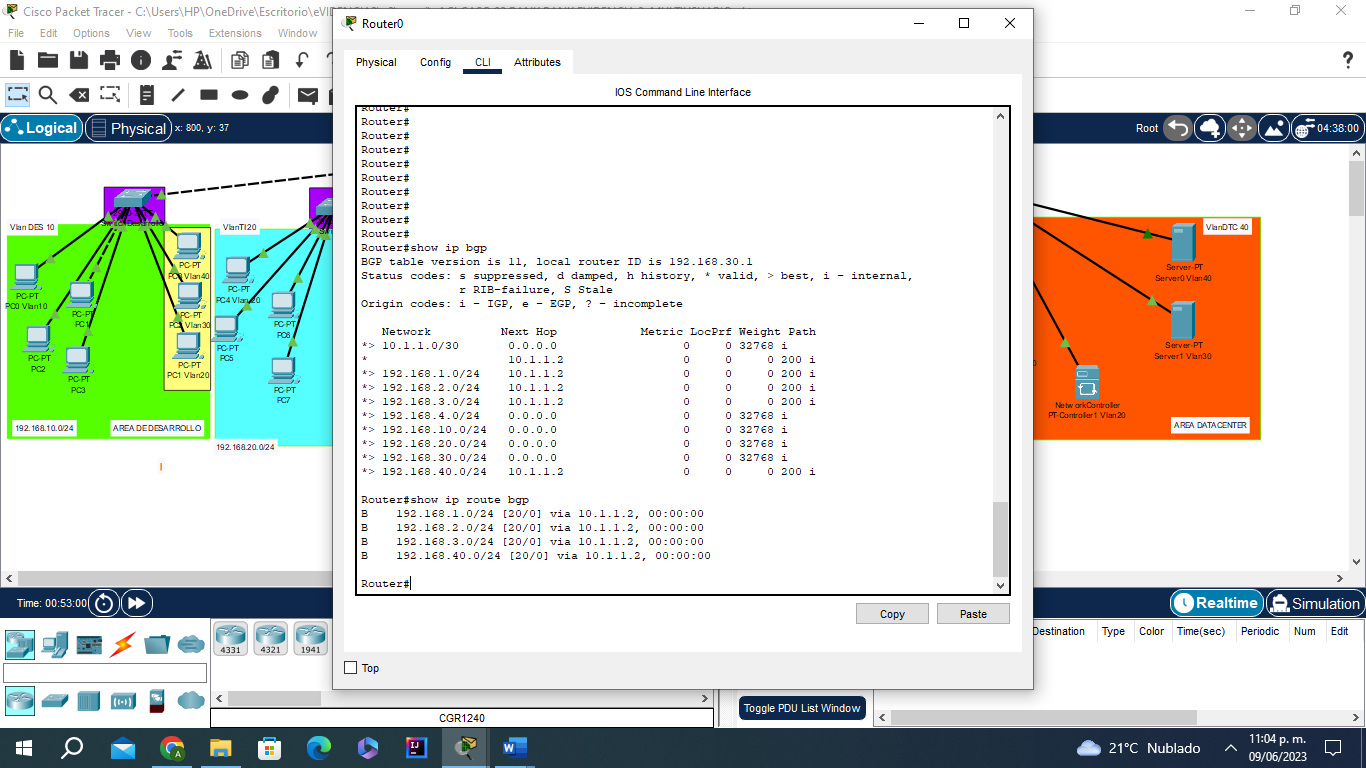


* + 1. Configuración de direccionamiento en cada interfaz



|  |  |  |  |
| --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
| R1 | S0/1/0 | 10.1.1.1 | 255.255.255.252 |
| R1 |
| R2 | S0/1/0 | 10.1.1.2 | 255.255.255.252 |
| R2 |

* + 1. Implementación de enrutamiento BGP



* 1. Evaluando los costos de red
     1. Evaluando costos de hardware

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre de Dispositivo** | **Costo** | **Cantidad** | **Costo Total** |
| Switch | s/4138.19 | 5 | s/ 20,690.95 |
| Pc | 2000 | 11 | s/22.000 |
| router | s/6435 | 2 | s/6.435 |
| Servidor | s/5000 | 2 | s/10.000 |
| NetworkController | s/3000 | 2 | s/6.000 |

* + 1. Evaluando costos de software

|  |  |  |  |
| --- | --- | --- | --- |
| **Sistema Operativo** | **Costo Unitario** | **Cantidad** | **Costo Total** |
| Windows | 80 | 3 | 240 |