**PRÁCTICO INTEGRADOR**

TALLER DE REDES LOCAL

**AÑO 2019**

* ***TUTOR:*** *Omar Antonio.*
* INTEGRANTES:

|  |  |  |  |
| --- | --- | --- | --- |
| **NOMBRE** | **MATRÍCULA** | **CARRERA** | **CORREO ELECTRÓNICO** |
| Martínez, Martín | 66743 | Ingeniería en Informática | [goofy\_2009@hotmail.com](mailto:goofy_2009@hotmail.com) |
| Rodríguez, Rodrigo | 66700 | Ingeniería en Informática | [rodriguezrodrigo127@gmail.co](mailto:rodriguezrodrigo127@gmail.co) m |

DESCRIPCIÓN GENERAL

MisioTIC S.A. es una empresa encargada del desarrollo y comercialización de software y equipos de comunicaciones en la región noreste del país.

Para el inicio de sus actividades la empresa decide alquilar un edificio de 3 pisos ubicado en

pleno centro de la ciudad de Posadas. Se trata de tres pisos con una superficie de 600 𝑚2 cada uno (20 x 30 m), de los cuales un espacio de 2 x 7 m en cada piso está reservado para el ascensor, palier y baños. Estas instalaciones no tiene divisiones internas de mampostería por lo que se recurriría a una estructura de tabiques y cielorraso colgante. La altura entre piso y techo de cada planta es de 3,2 m y el cielorraso se encuentra suspendido a 0,6 m del techo. El punto de ingreso de los servicios externos es a través de un conducto junto a la caja del ascensor.

En el piso inferior se ha dispuesto ubicar el sector de atención al cliente (12 puestos de trabajo), y el sector de ayuda on-line para clientes (24 boxes). En el mismo piso están la oficina del Gerente de Ventas, la del Gerente de Atención al Cliente (2 puesto de trabajo para cada uno), una sala para sus auxiliares (5 puestos) y una sala de reuniones (2 puestos).

En el segundo piso se instalarán: un show room (16 conexiones), el área de gestión de calidad (4 puestos), depósito (4 puestos), laboratorio de pruebas (20 puestos) y el área de comercio exterior (8 puestos).

En el tercer piso se prevé instalar: el Área de Investigación y Desarrollo (30 puestos), la oficina del Administrador y su auxiliar (2 puestos), las del Gerente de Sucursales, el Gerente General y Directorio (2 puesto cada uno) y la sala de sus auxiliares (8 puestos). También en este piso está el Área de Sistemas (10 puestos) y la Granja de Servidores (servidor de archivos, servidor de correo, servidor web, servidor DNS y servidor/firewall proxy-cache). Considerar un crecimiento a futuro de un 30% para todos los puestos de trabajo.

La empresa decide contratarlo a Ud. como encargado del diseño, análisis de costos e implementación de su red, incluyendo la configuración de las estaciones de trabajo y servidores.

PRIMERA PARTE:

“Diseño del cableado estructurado”

Paso 1: Identificar las secciones y sus requerimientos de conexión

|  |  |  |  |
| --- | --- | --- | --- |
| **Sección** | **Descripción de sección: puestos de trabajo** | **Identificación de sección** | **Requerimientos de conexión** |
| **Primer piso** | | | |
| Atención al cliente | 12 | PP-AC | 16 rosetas de telecomunicaciones |
| 32 jacks Rj45 hembra - Cat. 6 |
| Ayuda on-line para clientes | 24 | PP-AO | 32 rosetas de telecomunicaciones |
| 64 jacks Rj45 hembra - Cat. 6 |
| Oficina del gerente de ventas | 2 | PP-GV | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat.6 |
| Oficina del gerente de atención al cliente | 2 | PP-GAC | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat.6 |
| Sala para auxiliares de gerentes | 5 | PP-SAG | 7 rosetas de telecomunicaciones |
| 14 jacks Rj45 hembra - Cat. 6 |
| Sala de reuniones | 2 | PP-SR | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat. 6 |
| **Segundo piso** | | | |
| Showroom | 16 | SP-SR | 21 rosetas de telecomunicaciones |
| 42 jacks Rj45 hembra - Cat.6 |
| Area de gestion de calidad | 4 | SP-GC | 6 rosetas de telecomunicaciones |
| 12 jacks Rj45 hembra - Cat.6 |

|  |  |  |  |
| --- | --- | --- | --- |
| Depósito | 4 | SP-D | 6 rosetas de telecomunicaciones |
| 12 jacks Rj45 hembra - Cat.6 |
| Laboratorio de pruebas | 20 | SP-LP | 26 rosetas de telecomunicaciones |
| 52 jacks Rj45 hembra - Cat.6 |
| Área de comercio exterior | 8 | SP-CE | 11 rosetas de telecomunicaciones |
| 22 jacks Rj45 hembra - Cat.6 |
| **Tercer piso** | | | |
| Area de investigacion y desarrollo | 30 | TP-AID | 39 rosetas de telecomunicaciones |
| 78 jacks Rj45 hembra - Cat.6 |
| Oficina del administrador y su auxiliar | 2 | TP-OAA | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat.6 |
| Oficina del gerente de sucursales | 2 | TP-OGS | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat.6 |
| Oficina del gerente general | 2 | TP-OGG | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat.6 |
| Oficina del directorio | 2 | TP-OD | 3 rosetas de telecomunicaciones |
| 6 jacks Rj45 hembra - Cat.6 |
| Sala de auxiliares | 8 | TP-SA | 11 rosetas de telecomunicaciones |
| 22 jacks Rj45 hembra - Cat.6 |
| Área de sistemas | 10 | TP-AS | 13 rosetas de telecomunicaciones |
| 26 jacks Rj45 hembra - Cat.6 |

|  |  |  |  |
| --- | --- | --- | --- |
| Granja de servidores | 5 | TP-GS | 7 rosetas de telecomunicaciones |
| 14 jacks Rj45 hembra - Cat.6 |

OBS: Por cada puesto de trabajo se consideró un crecimiento futuro de un 30%.

En este paso lo que se realizó es, de acuerdo al enunciado, indicar la cantidad de puestos de trabajo asignado para cada sección. Posteriormente, se prosiguió con la determinación de una determinada identificación de cada una de las mismas, lo que se logró colocando siglas en base al piso que se encontraba y el correspondiente nombre de cada sección.

Para finalizar, y con un crecimiento al futuro de un 30%, se indicó por sección la cantidad de rosetas de telecomunicación, junto con la cantidad de Jacks Rj45 hembras cat. 6.

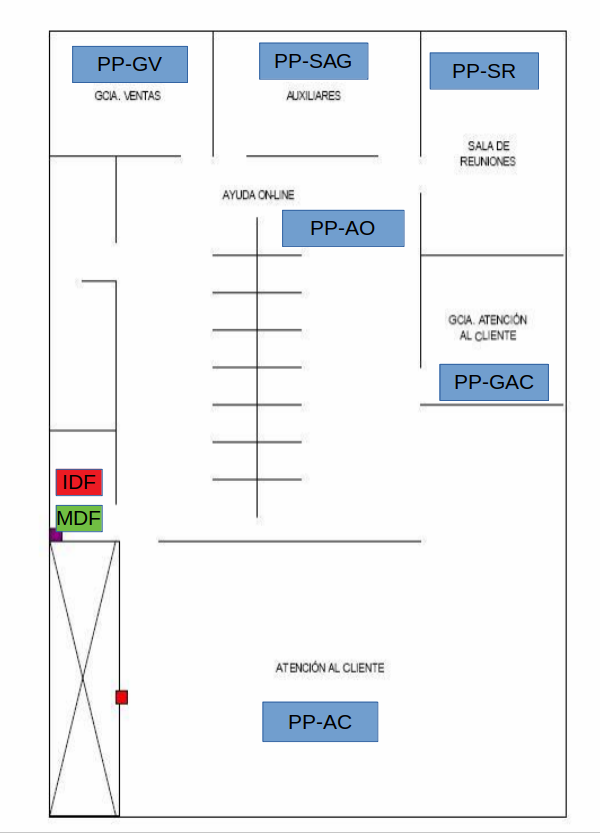
Paso 2: Determinar ubicación de las facilidades de distribución

Cada piso del edificio posee una superficie de 600 m2, sin embargo, el área utilizable es de 586 m2 en cada piso. Esto es así, debido a que 14m2 (7x2 metros) en cada piso está reservado para el ascensor, palier y baños. Por lo tanto, el área utilizable en cada piso es de 586 m2 (600 - 14). Además, se puede estimar el área utilizable como el 75 % del área total: por lo que utilizaremos 450 m2.

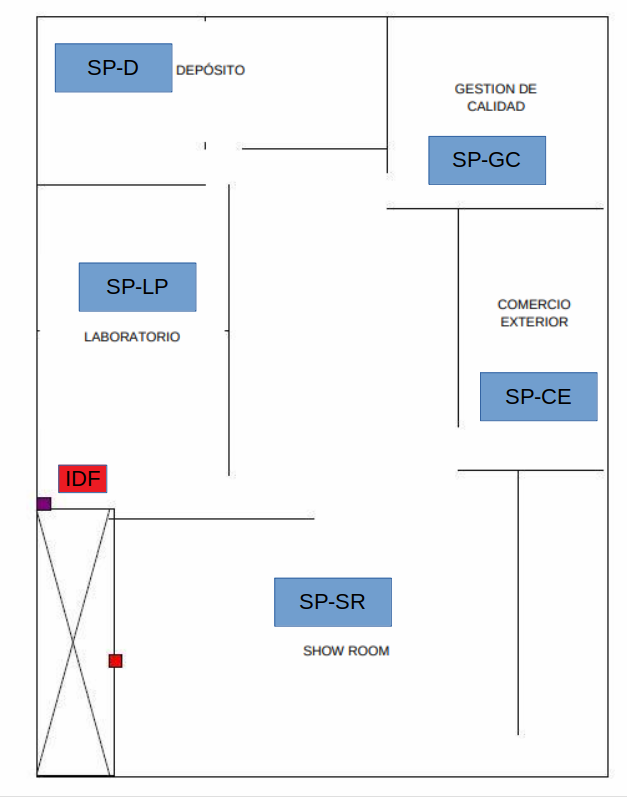
Entonces para calcular el espacio estimado para la sala de equipos, tenemos que considerar 0,07 m2 por cada 10 m2 de área utilizable del edificio. Por lo que en nuestro caso, tenemos que 0,07 x (586 / 10) = 4,102 m2.

Sin embargo, hay que tener en cuenta que el tamaño mínimo por recomendación es de una sala de 3,7 x 3,7 (13,5 m2). Como se puede observar, el tamaño calculado es menor al tamaño mínimo recomendado.

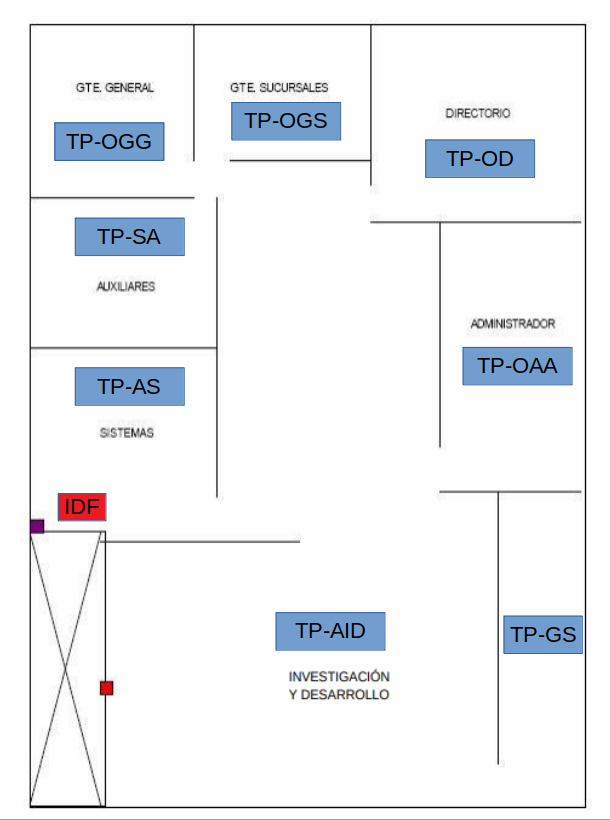
Distribución primer piso:



***Distribución segundo piso***



***Distribución tercer piso:***

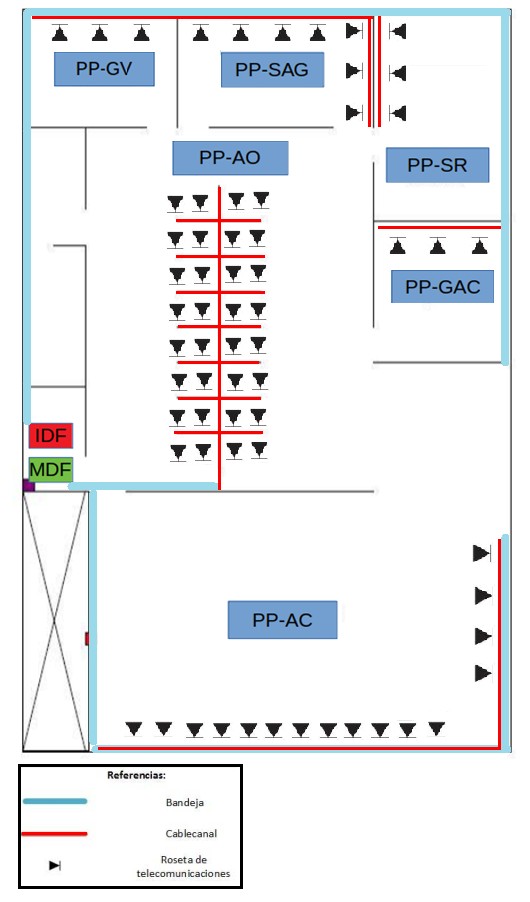


|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Facilidad de Entrada** | **Sección** | **Conexiones** | **Distancia Promedio (mts)** | **Total (mts)** |
| **MDF** | **IDF 1** | **1** | **0** | **0** |
| **IDF 2** | **1** | **10** | **10** |
| **IDF 3** | **1** | **15** | **15** |
| **TOTAL: 25 metros** | | | | |
| **IDF 1** | **PP-AC** | **32** | **32** | **1.024** |
| **PP-AO** | **64** | **14** | **896** |
| **PP-GV** | **6** | **29** | **174** |
| **PP-GAC** | **6** | **58** | **348** |
| **PP-SAG** | **14** | **37** | **518** |
| **PP-SR** | **6** | **43** | **258** |
| **TOTAL: 3.218 metros** | | | | |
| **IDF 2** | **SP-SR** | **42** | **30** | **1.260** |
| **SP-GC** | **12** | **43** | **516** |
| **SP-D** | **12** | **35** | **420** |
| **SP-LP** | **52** | **38** | **1.144** |
| **SP-CE** | **22** | **60,5** | **1.331** |
| **TOTAL: 4.671 metros** | | | | |
| **IDF 3** | **TP-AID** | **78** | **38** | **2.964** |
| **TP-OAA** | **6** | **47,5** | **285** |
| **TP-OGS** | **6** | **35** | **210** |

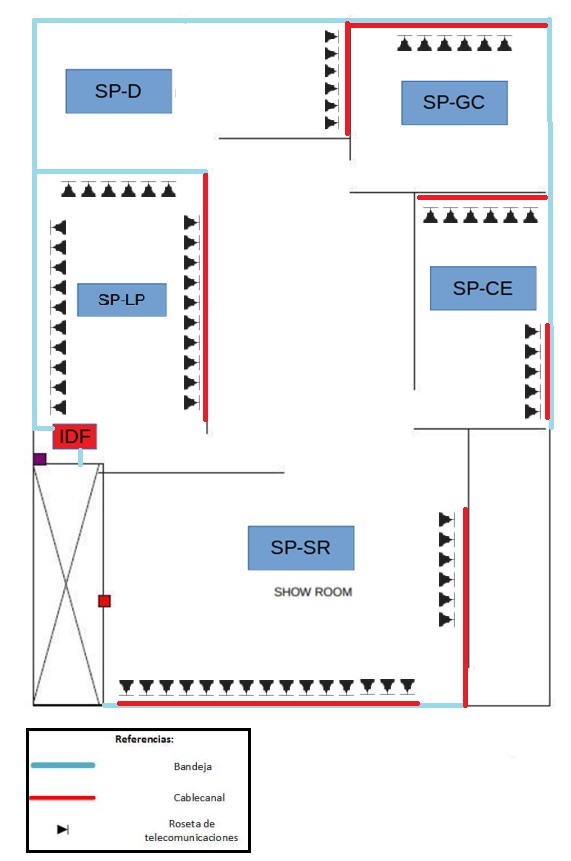
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IDF 3** | **TP-OGG** | **6** | **29** | **174** |
| **TP-OD** | **6** | **50,5** | **303** |
| **TP-SA** | **22** | **15,2** | **335** |
| **TP-AS** | **26** | **7,6** | **198** |
| **TP-GS** | **14** | **37,5** | **525** |
| **TOTAL: 4.994 metros** | | | | |
| ***TOTAL DE TODAS LAS FACILIDADES DE ENTRADA: 12.908 metros.*** | | | | |

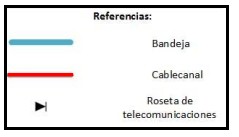
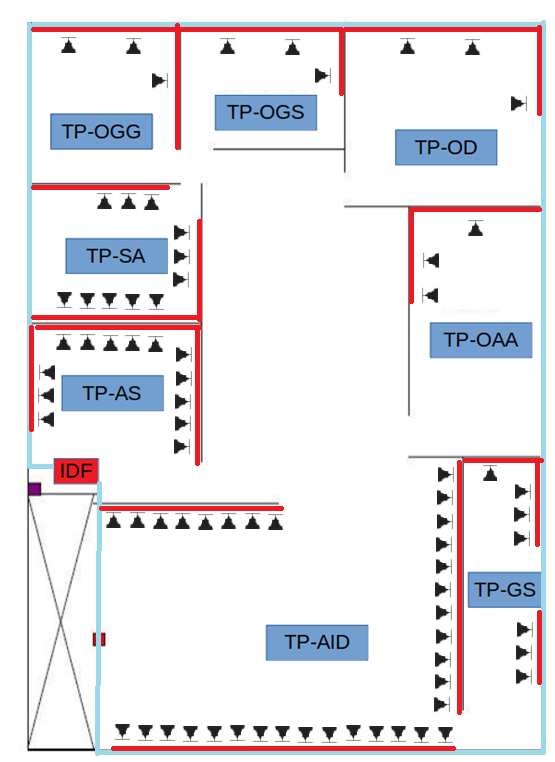
**Paso 3: Realizar el diseño del cableado horizontal de cada piso.**

***Cableado Horizontal en el primer piso:***

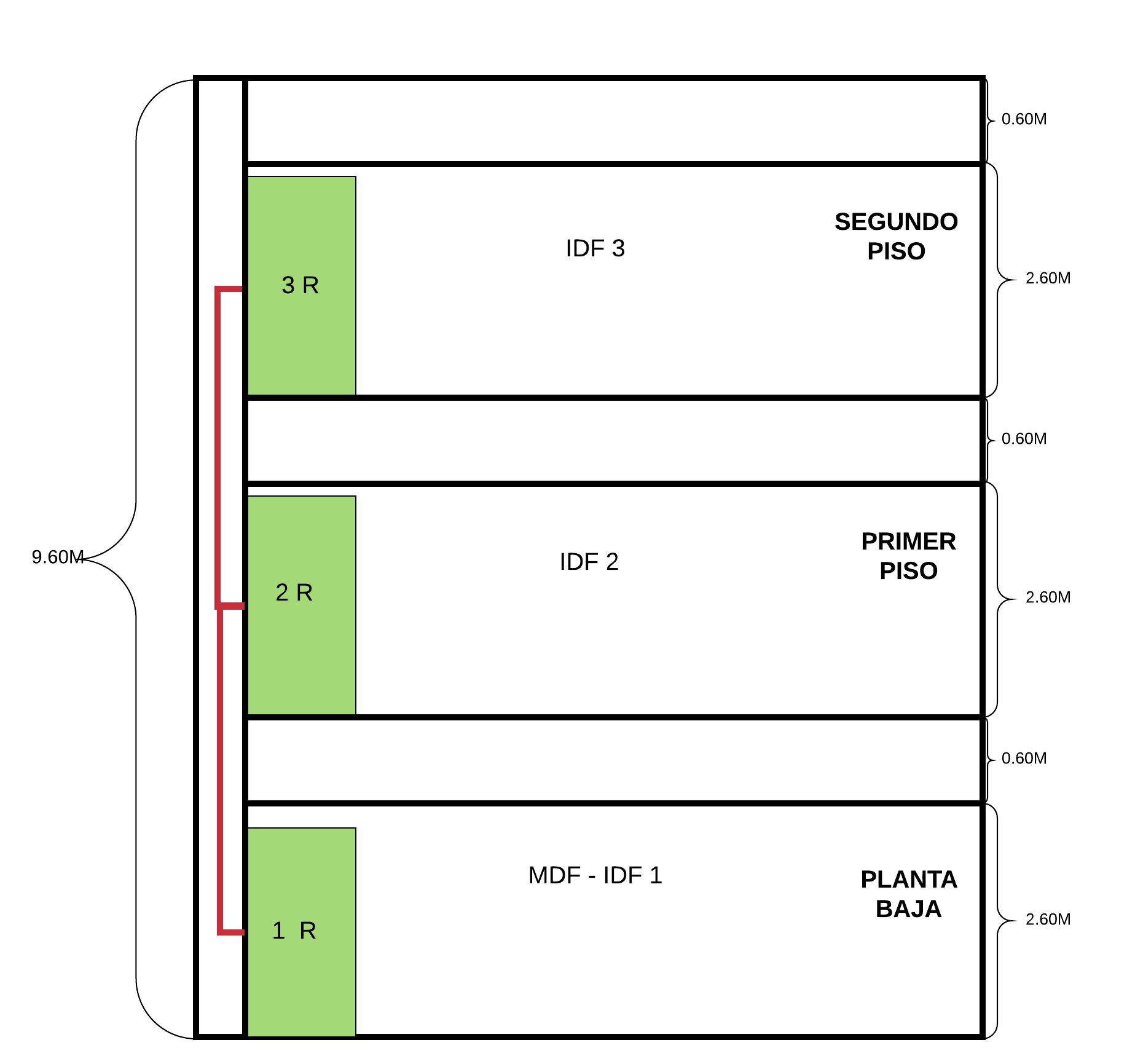


***Segundo piso:***





**Paso 4: Realizar el diseño del cableado vertical de cada piso.**



Como se puede observar en la figura, la cantidad de cable utilizado es de 9.6 metros. Por su parte, el tipo de cable de red es UTP - Categoría 6.

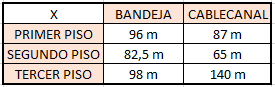
**Paso 5: Identificar las necesidades de cada facilidad de distribución.**

|  |  |
| --- | --- |
| **DESCRIPCIÓN** | **CANTIDAD** |
| **MDF/IDF 1 - PISO 1** | |
| Roseta RJ45 de 2 bocas | 64 |
| Switch CISCO SG 220 - 48 puertos | 3 |
| Patchera Patch Rj45 - 48 puertos - Cable Cat. 6 | 3 |
| Plug Macho Rj45 Cat.6 - Sólido Intellinet X10 unidades. | 13 |
| Jack RJ45 Cat 6 | 128 |
| Bobina cable red UTP exterior Cat.6 - Rollo 305 metros. | 11 |
| Rack Pie 32 Unidades 19 Pulgadas 1000mm Prof Server Prosoft | 1 |
| Cable interlock. | 6 |
| Canal de tension Rack 5 tomas. | 2 |
| Bandeja porta cable 100 x 50 mm - 3 metros | 32 |
| Cablecanal Hellermanntyton 100x50mm, 2 metros de largo. | 44 |
| **IDF 2 - PISO 2** | |
| Roseta RJ45 de 2 bocas | 70 |
| Switch CISCO SG 220 - 48 puertos | 3 |
| Patchera Patch Rj45 - 48 puertos - Cable Cat. 6 | 3 |
| Plug Macho Rj45 Cat.6 - Sólido Intellinet X10 unidades. | 14 |
| Jack RJ45 Cat 6 | 140 |
| Bobina cable red UTP exterior Cat.6 - Rollo 305 metros. | 16 |
| Rack Pie 32 Unidades 19 Pulgadas 1000mm Prof Server Prosoft | 1 |



|  |  |
| --- | --- |
| Cable interlock. | 6 |
| Canal de tension Rack 5 tomas. | 2 |
| Bandeja porta cable 100 x 50 mm - 3 metros | 28 |
| Cablecanal Hellermanntyton 100x50mm, 2 metros de largo. | 33 |
| **IDF 3 - PISO 3** | |
| Roseta RJ45 de 2 bocas | 82 |
| Switch CISCO SG 220 - 48 puertos | 4 |
| Patchera Patch Rj45 - 48 puertos - Cable Cat. 6 | 4 |
| Plug Macho Rj45 Cat.6 - Sólido Intellinet X10 unidades. | 17 |
| Jack RJ45 Cat 6 | 164 |
| Bobina cable red UTP exterior Cat.6 - Rollo 305 metros. | 17 |
| Rack Pie 32 Unidades 19 Pulgadas 1000mm Prof Server Prosoft | 1 |
| Cable interlock. | 8 |
| Canal de tension Rack 5 tomas. | 2 |
| Bandeja porta cable 100 x 50 mm - 3 metros | 33 |
| Cablecanal Hellermanntyton 100x50mm, 2 metros de largo. | 70 |

Las estimaciones para el cable UTP se basaron en la tabla realizada en el punto 2. Por su parte, para la cantidad de bandejas porta cables, así como el cablecanal se basaron en estimaciones realizadas en el gráfico del punto 3.





Paso 6: Confeccionar el diagrama de conectividad.

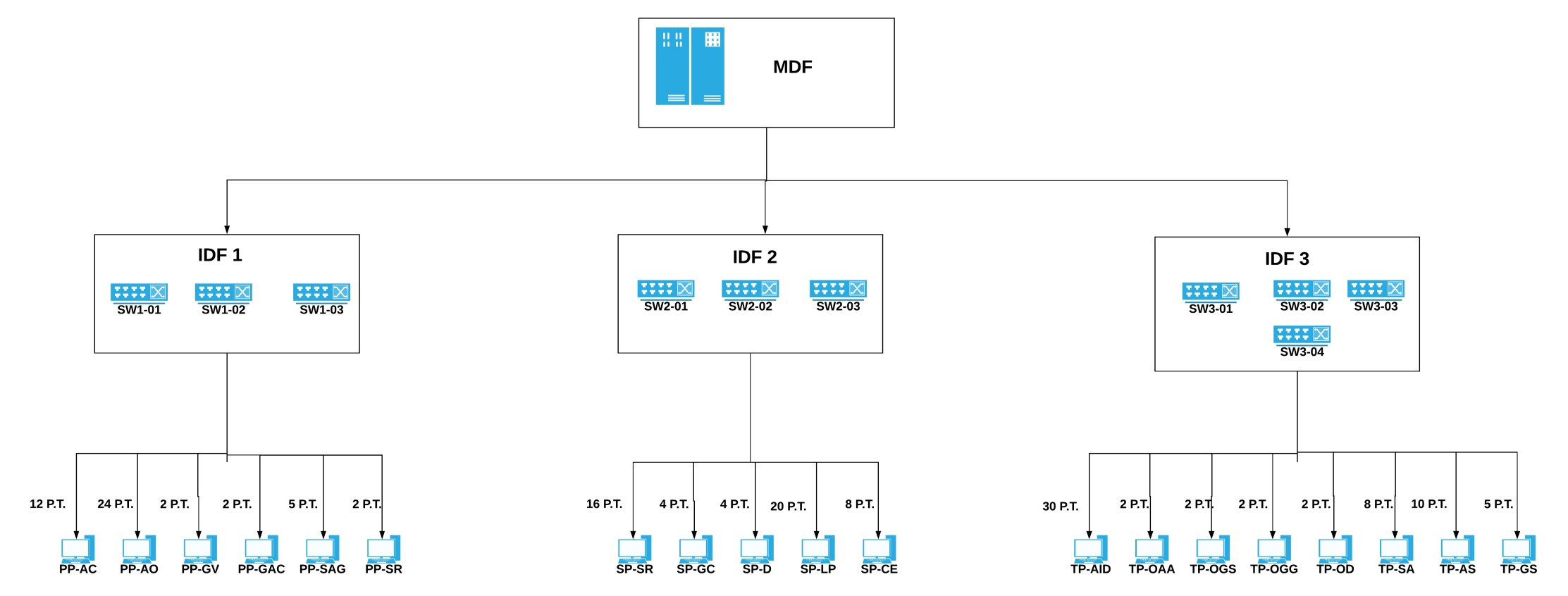


Diagrama de Conectividad 1.



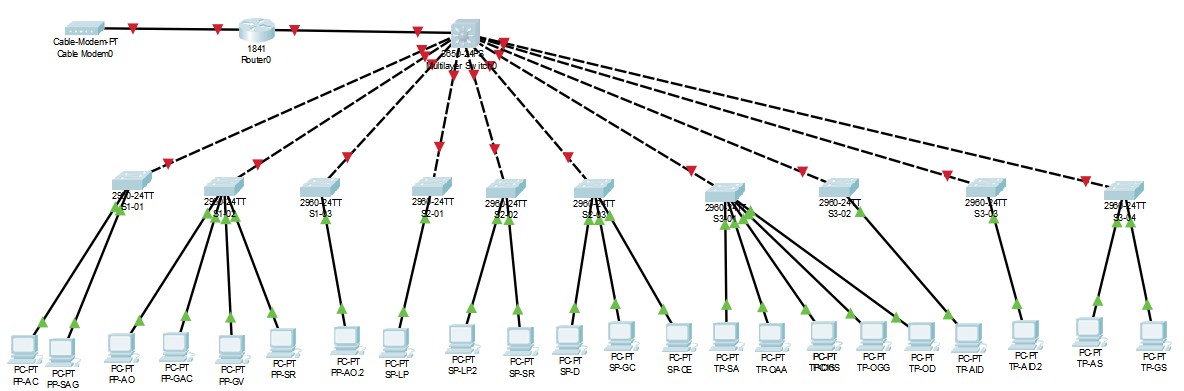


Diagrama de Conectividad 2.

Paso 7: Describir el esquema de etiquetado.

|  |  |
| --- | --- |
| **DISPOSITIVO** | **ETIQUETA** |
| **Rack Pie 32 Unidades 19 Pulgadas 1000mm Prof Server Prosoft** | |
| **Piso 1** | **ARM-01** |
| **Piso 2** | **ARM-02** |
| **Piso 3** | **ARM-03** |
| **Switch CISCO SG 220 - 48 puertos** | |
| **Piso 1** | **SW1-01** |
| **SW1-02** |
| **SW1-03** |
| **Piso 2** | **SW2-01** |
| **SW2-02** |
| **SW2-03** |
| **Piso 3** | **SW3-01** |
| **SW3-02** |
| **SW3-03** |
| **SW3-04** |
| **Patchera Patch Rj45 - 48 puertos - Cable Cat. 6** | |
| **Piso 1** | **P1-01** |
| **P1-02** |
| **P1-03** |
| **Piso 2** | **P2-01** |
| **P2-02** |
| **P2-03** |

|  |  |
| --- | --- |
| **Piso 3** | **P3-01** |
| **P3-02** |
| **P3-03** |
| **P3-04** |
| **Roseta RJ45 de 2 bocas** | |
| **Piso 1** | **R1-001 / R1-064** |
| **Piso 2** | **R2-001 / R2-070** |
| **Piso 3** | **R3-001 / R3-082** |

***ACLARACIÓN:*** El etiquetado de las Rosetas hace referencia que en el “Piso 1” el etiquetado de las mismas van desde el R1-001, luego el R1-002, R1-003… y así consecutivamente hasta el R1-064.

Para los demás pisos, se utiliza el mismo método de etiquetado.

Breve descripción de componentes:

SWITCH CISCO | SG220-50

* Tipo de dispositivo:Conmutador - 50 puertos - Gestionado
* Tipo de caja:Sobremesa, montaje en rack 1U
* Subtipo:Gigabit Ethernet
* Puertos:48 x 10/100/1000 + 2 x Gigabit SFP combinado
* Rendimiento:Rendimiento de reenvío (tamaño de paquete de 64 bytes): 74.4 mpps ¦ Capacidad de conmutación: 100 Gbps
* Tamaño de tabla de dirección MAC:8.192 entradas
* Admite carcasa Jumbo:9216 bytes
* Protocolo de gestión remota:SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, http, https, TFTP, CLI
* Método de autentificación:RADIUS, TACACS+
* Características:Control de flujo, conmutación Layer 2, soporte BOOTP, soporte VLAN, snooping IGMP, soporte para Syslog, prevención contra ataque de DoS (denegación de servicio), copia de puertos, soporte DiffServ, Cola Round Robin (WRR) ponderada, filtrado de dirección MAC, Broadcast Storm Control, soporte IPv6, Multicast Storm Control, Unicast Storm Control, actualizable por firmware, soporte SNTP, admite Spanning Tree Protocol (STP), admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), rastreador MLD, botón de reinicio, con LLDP, relé DHCP, cliente DHCP, Energy Efficient Ethernet, búfer de paquetes de 12KB, Generic Attribute Registration Protocol (GARP), Generic VLAN Registration Protocol (GVRP), Type of Service (ToS)
* Cumplimiento de normas:IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3az
* Memoria RAM:128 MB
* Memoria Flash:32 MB
* Indicadores de estado:Velocidad de transmisión del puerto, sistema, enlace/actividad



PLUG :

-Características:

-Modelo: 502344

-Cat 6

-Conector solido

-Marca: Intellinet



JACK:

Jack Cat-6 Marca JA Encastre Clásico



CABLECANAL:

Marca : Hellermanntyton Dimensión : 100x50 2 Metros



BANDEJA PORTACABLE:

Tramo bandeja portacable perforada 100mm x 3 mts. Altura 50 mm.

Espesor de la chapa 0.7m.



ROSETA RJ45:

Roseta Rj45 Doble Para Jack Cat6 Cable Red Utp Pared. Material plástico.





RACK DE PIE:

* Rack Pie 32 Unidades 19 Pulgadas 1000mm.
* Marca: PROSOFT

- Modelo: 32U6001000

* Tipo: PIE
* Armado/desarmado: DESARMADO.
* Aptas para interior.
* Cerradura tipo gatillo.
* Capacidad de carga estática: 800kg (con el pie fijo)
* Puerta: Cristal templado
* Espesor de la puerta: 5mm



CABLE INTERLOCK:

Cable Interlock tipo Power, con ficha C13 inyectada recta y Ficha C14 inyectada Recta. Cable de 3 x 1,00 mm2.

Longitud de 1,5 metros.



CANAL DE TENSION RACK:

* Marca: GLC
* Modelo: R1001.
* Tomas IRAM: Richi (o similar).
* Unidad estandarizada.
* Canales de tensión se proveen con 2 mts de cable bajo goma, tripular
* Dimensiones 6 x 46 x 5 cm (Alto x Ancho x Profundidad)
* Peso: 1 kg



Paso 8: Elaborar el presupuesto de materiales.

|  |  |  |  |
| --- | --- | --- | --- |
| **EQUIPAMIENTO** | | | |
| **Cantidad** | **Descripción** | **Precio Unitario** | **Subtotal** |
| 216 | Roseta RJ45 de 2 bocas. | $63,00 | $13.797,00 |
| 10 | Switch CISCO SG 220 - 48 puertos | $47.900,00 | $479.000,00 |
| 10 | Patchera Patch Rj45 - 48 puertos - Cable Cat. 6 | $3.336,00 | $33.360,00 |
| 432 | Plug RJ45 Cat 6. x10. | $478,00 | $21.032,00 |
| 432 | Jack RJ45 Cat 6. | $144,00 | $62.208,00 |
| 44 | Bobina cable red UTP exterior Cat.6 - Rollo 305 metros. | $6.789,00 | $298.716,00 |
| 3 | Rack Pie 32 Unidades 19 Pulgadas 1000mm Prof Server Prosoft | $37.578,00 | $112.734,00 |
| 20 | Cable interlock. | $120,00 | $2.400,00 |
| 9 | Canal de tension Rack 5 tomas. | $1.300,00 | $11.700,00 |
| 93 | Bandeja porta cable 100mm x 50 mm - 3 metros. | $952,00 | $88.536,00 |
| 147 | Cablecanal Hellermanntyton 100x50 mm, 2 metros. | $1.024,00 | $150.528,00 |
| **COSTO TOTAL** | | $1.274.011,00 | |

SEGUNDA PARTE:

“Configuración de la Red”

Paso 1. Asignación del direccionamiento IP.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sección** | **Dirección de subred** | **Máscara de subred** | **VLAN** | **Rango de hosts** | **Dirección de Gateway** |
| Atención al Cliente | 10.0.1.0 | 255.255.255.128 | 10 | 10.0.1.2 - 10.0.1.126 | 10.0.1.1 |
| Gerencia | 10.0.2.0 | 255.255.255.192 | 20 | 10.0.2.2 - 10.0.2.62 | 10.0.2.1 |
| Sistemas | 10.0.0.0 | 255.255.255.0 | 30 | 10.0.0.2 - 10.0.0.254 | 10.0.0.1 |
| Ventas | 10.0.1.128 | 255.255.255.128 | 40 | 10.0.1.130 - 10.0.1.254 | 10.0.1.129 |
| Conexión Switch con Router | 10.0.2.72 | 255.255.255.252 | - | 10.0.2.74 - 10.0.2.75 | 10.0.2.74 |
| Granja de servidores (DMZ) | 10.0.2.64 | 255.255.255.248 | - | 10.0.2.66- 10.0.2.70 | 10.0.2.66 |

En nuestro trabajo integrador se optó por dividir en una VLAN para cada uno de los diferentes sectores que integran al edificio del planteamiento. Debido a esto, los sectores que nos quedarían en su respectivos pisos son:

* + Sección Atención al Cliente: (114 hosts)
    - Primer Piso:
      * Atención al cliente. PP-AC (32 hosts)
      * Ayuda on-line para clientes. PP-AO (64 hosts)
    - Segundo Piso:
      * Depósito. SP-D (12 hosts)
    - Tercer Piso:
      * Oficina de administrador y su auxiliar. TP-OAA (6 hosts)
  + Sección Gerencia: (50 hosts)
    - Primer Piso:
      * Oficina del gerente de ventas. PP-GV (6 hosts)
      * Oficina del gerente de atención al cliente. PP-GAC (6 hosts)
      * Sala para auxiliares de gerentes. PP-SAG (14 hosts)
      * Sala de reuniones. PP-SR (6 hosts)
* Tercer Piso:
  + Oficina del gerente de sucursales. TP-OGS (6 hosts)
  + Oficina del gerente general. TP-OGG (6 hosts)
  + Oficina del directorio. TP-OD (6 hosts)
* Sección Sistemas: (204 hosts)
  + Segundo Piso:
    - Área de gestión de calidad. SP-GC (12 hosts)
    - Laboratorio de pruebas. SP-LP (52 hosts)
  + Tercer Piso:
    - Área de investigación y desarrollo. TP-AID (78 hosts)
    - Sala de auxiliares. TP-SA (22 hosts)
    - Área de sistemas. TP-AS (26 hosts)
    - Granja de servidores. TP-GS (14 hosts)
* Sección Ventas: (64 hosts)
  + Segundo Piso:
    - Área de comercio exterior. SP-CE (22 hosts)
    - Showroom. SP-SR (42 hosts)
* Granja de servidores (DMZ)
  + 10.0.2.66 - correo electronico.
  + 10.0.2.67 - servidor Web.
  + 10.0.2.68 - servidor DNS.
  + 10.0.2.69 - transferencia de archivos.

Como observación podemos mencionar que se agregó una dirección IP para conectar el Router con el Switch principal.

Para llevar a cabo el cálculo de los rangos de los hosts y el cálculo de las subredes, se utilizó la siguiente página:

<https://www.arcadio.gq/calculadora-subredes-vlsm.html>

Paso 2: Configuración de ruteo entre VLANs e Internet

En este trabajo decidimos aplicar un ruteo estático. El enrutamiento estático proporciona un método que otorga control absoluto sobre las rutas por las que se transmiten los datos, se crean manualmente.

Con esto dicho, la descripción es la siguiente:

Configuración del Router *Configuración con Switch principal*

Router (config)#interface f0/1

Router (config-if)#ip address 10.0.2.74 255.255.255.252 Router (config-if)#no shutdown

*Configuración con la granja de servidores (DMZ)*

Router(config)#interface f0/2

Router(config-if)#ip address 10.0.2.65 255.255.255.248 Router(config-if)#no shutdown

Switch (config)#ip routing

Configuración Switch Principal

Switch (config-if)#vlan 10

Switch (config-vlan)#name AtencionAlCliente Switch (config-vlan)#int vlan10

Switch (config-if)#ip address 10.0.1.1 255.255.255.128

Switch (config-if)#description Gateway del sector de Atención al Cliente Switch (config-if)#no shutdown

Switch (config-if)#vlan 20

Switch (config-vlan)#name Gerencia Switch (config-vlan)#int vlan20

Switch (config-if)#ip address 10.0.2.1 255.255.255.192 Switch (config-if)#description Gateway del sector de Gerencia Switch (config-if)#no shutdown

Switch (config-if)#vlan 30

Switch (config-vlan)#name Sistemas Switch (config-vlan)#int vlan30

Switch (config-if)#ip address 10.0.0.1 255.255.255.0

Switch (config-if)#description Gateway del sector de Sistemas Switch (config-if)#no shutdown

Switch (config-if)#vlan 40

Switch (config-vlan)#name Ventas Switch (config-vlan)#int vlan40

Switch (config-if)#ip address 10.0.1.129 255.255.255.128 Switch (config-if)#description Gateway del sector de Ventas Switch (config-if)#no shutdown

Configuración de los puertos TRUNK

Como observación, podemos mencionar que decidimos que cada uno de los switches se conectan al switch principal a través de la interfaz f0/1 de cada switch correspondiente. Esto lo determinamos así para mejorar la comprensión.

// **Trunk** sirve para indicar que siempre va a ser utilizado este enlace como un enlace troncal. **IEEE 802.1Q**, también conocido como **dot1Q**, es un mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

SW1-01

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW1-02

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW1-03

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW2-01

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW2-02

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW2-03

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW3-01

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW3-02

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW3-03

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

SW3-04

Switch(config)#interface f0/1

Switch(config-if)#switchport trunk encapsulation dot1q Switch(config-if)#switchport mode trunk

Configuración de los puertos de acceso

Como consideración con respecto a este apartado, hay que tener en cuenta que para mayor claridad conviene revisarlo junto con el diagrama de conectividad correspondiente.

***Primer Piso***

SW1-01

Switch(config)#vlan 10

Switch(config-vlan)#name AtencionAlCliente Switch(config-vlan)#exit

Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit

Switch(config)#vlan 20 Switch(config-vlan)#name Gerencia Switch(config-vlan)#exit Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

SW1-02

Switch(config)#vlan 10

Switch(config-vlan)#name AtencionAlCliente Switch(config-vlan)#exit

Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name Gerencia Switch(config-vlan)#exit Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#int f0/4

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#int f0/5

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

SW1-03

Switch(config)#vlan 10

Switch(config-vlan)#name AtencionAlCliente Switch(config-vlan)#exit

Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

Segundo Piso

SW2-01

Switch(config)#vlan 30 Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

SW2-02

Switch(config)#vlan 30 Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#vlan 40 Switch(config-vlan)#name Ventas Switch(config-vlan)#exit Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 40 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

***SW2-03***

Switch(config)#vlan 10

Switch(config-vlan)#name AtencionAlCliente Switch(config-vlan)#exit

Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 10 Switch(config-if)#exit

Switch(config)#vlan 30 Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#vlan 40 Switch(config-vlan)#name Ventas Switch(config-vlan)#exit Switch(config)#int f0/4

Switch(config-if)#switchport access vlan 40 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

Tercer Piso

SW3-01

Switch(config)#vlan 30 Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#vlan 10

Switch(config-vlan)#name AtencionAlCliente Switch(config-vlan)#exit

Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#vlan 20 Switch(config-vlan)#name Gerencia Switch(config-vlan)#exit Switch(config)#int f0/4

Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit

Switch(config)#int f0/5

Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit

Switch(config)#int f0/6

Switch(config-if)#switchport access vlan 20 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

SW3-02

Switch(config)#vlan 30

Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

SW3-03

Switch(config)#vlan 30 Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

SW3-04

Switch(config)#vlan 30 Switch(config-vlan)#name Sistemas Switch(config-vlan)#exit Switch(config)#int f0/2

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit

Switch(config)#int f0/3

Switch(config-if)#switchport access vlan 30 Switch(config-if)#exit Switch(config)#interface f0/1

Switch(config-if)#switchport mode trunk

Configuración de ruteo desde el Switch al Router

Switch(config)#interface f0/1

Switch(config-if)#no switchport

Switch(config-if)#ip address 10.0.2.75 255.255.255.252 Switch(config-if)#exit

Switch(config)#ip router 10.0.2.74 255.255.255.252

Switch(config)#exit

Paso 3: Configuración del servidor DNS.

Comenzamos con NAMED.CONF.LOCAL

//

// Do any local configuration here

//

// Consider adding the 1918 zones here, if they are not used in your organization

//include "/etc/bind/zones.rfc1918";

//Zona Directa

zone "misiotic.net"{ type master;

file "/etc/bind/db.misiotic.net";

};

//Zona Inversa

zone “2.0.10.in-addr.arpa”{ type master;

file “/etc/bind/db.10.0.2”

};

Luego, proseguimos con el archivo de resolución de zona directa

;

; BIND data file for misiotic.net

;

$TTL 1D

@ IN SOA dns.misiotic.net. ayuda.misiotic.net. (

1 ; Serial

3600 ; Refresh

3600 ; Retry

36000 ; Expire

604800 ) ; Negative Cache TTL

;

|  |  |  |  |
| --- | --- | --- | --- |
| @ | IN | NS | dns.misiotic.net. |
|  | IN | MX | email.misiotic.net |
| Email | IN | A | 10.0.2.66 |
| www | IN | A | 10.0.2.67 |
| ns1 | IN | A | 10.0.2.68 |
| File | IN | A | 10.0.2.69 |

Archivo de resolución de zona inversa

;

; BIND data file for misiotic.net

;

$TTL 1D

@ IN SOA dns.misiotic.net. ayuda.misiotic.net. (

1 ; Serial

3600 ; Refresh

3600 ; Retry

36000 ; Expire

604800 ) ; Negative Cache TTL

;

|  |  |  |  |
| --- | --- | --- | --- |
| @ | IN | NS | dns.misiotic.net. |
| 5 | IN | PTR | email.misiotic.net. |
| 10 | IN | PTR | [www.misiotic.net.](http://www.misiotic.net/) |
|  | IN | PTR | file |
|  | IN | PTR | ns1 |

Por último, el NAMED.CONF.OPTIONS

options {

directory "/var/cache/bind";

//PERMITIR LA RECURSIVIDAD PARA TODA LA RED

acl goodclients {

10.0.1.0/25

10.0.2.0/26

10.0.0.0/24

10.0.1.128/25

10.0.2.72/30

10.0.2.64/29

} ;

//PERMITIR RECURSIVIDAD A LOS CLIENTES DEFINIDOS EN EL ACL ANTERIOR

recursion yes;

allow query{goodclients;};

// If there is a firewall between you and nameservers you want

// to talk to, you may need to fix the firewall to allow multiple

// ports to talk. See <http://www.kb.cert.org/vuls/id/800113>

// If your ISP provided one or more IP addresses for stable

// nameservers, you probably want to use them as forwarders.

// Uncomment the following block, and insert the addresses replacing

// the all-0's placeholder.

//DNS Forwaders que configuramos

forwarders {

8.8.8.8;

1.1.1.1;};

=======================================================================

// If BIND logs error messages about the root key being expired,

// you will need to update your keys. See [https://www.isc.org/bind-keys](http://www.isc.org/bind-keys) //

=======================================================================

dnssec-validation auto;

auth-nxdomain no; # conform to RFC1035 listen-on-v6 { any; };

};

Paso 4: Configuración del firewall de la red.

Las ​tablas filter​ se usan por defecto para gestionar paquetes de datos. Son responsables del filtrado de los paquetes según se ha configurado el firewall. Todos los paquetes pasan a través de esta tabla, y para la modificación tiene tres opciones predefinidas que también vimos en el artículo de introducción:  
● INPUT: ​para la entrada, es decir, todos los paquetes destinados a entrar en nuestro sistema deben pasar por esta cadena.  
● OUTPUT:​ para la salida, todos aquellos paquetes creados por el sistema y que van a salir de él hacia otro dispositivo.  
● FORWARD: ​redireccionamiento, simplemente los redirecciona a su nuevo destino, afectando a todos los paquetes que pasan por esta cadena.

Reglas aplicadas:

* *Permitir al servidor DNS hacer consultas a los servidores DNS forwarders.*

**//8.8.8.8** es el servicio de DNS oficial de Google. **1.1.1.1** es un servicio gratuito de Sistema de nombres de dominio (DNS). El servicio público de DNS y los servidores son de propiedad de Cloudflare.

iptables -A FORWARD -s 10.0.2.68 -d 8.8.8.8 -p udp --sport 53 --dport 53 -j ACCEPT

iptables -A FORWARD -s 10.0.2.68 -d 1.1.1.1 -p udp --sport 53 --dport 53 -j ACCEPT

* *Permitir el acceso al firewall desde Internet a través de SSH (puerto 22) para configurarlo de forma remota.*

iptables -A INPUT -p tcp --dport 22 -i eth0 -j ACCEPT

* *Permitir a toda la LAN acceder al proxy en el puerto correspondiente (puerto 8080).*

iptables -A INPUT -s 10.0.1.0/25 -p tcp --dport 8080 -i eth1 -j ACCEPT

iptables -A INPUT -s 10.0.2.0/26 -p tcp --dport 8080 -i eth1 -j ACCEPT

iptables -A INPUT -s 10.0.0.0/24 -p tcp --dport 8080 -i eth1 -j ACCEPT

iptables -A INPUT -s 10.0.1.128/25 -p tcp --dport 8080 -i eth1 -j ACCEPT

* *Permitir a los usuarios de sistemas acceder al firewall en todos sus puertos.*

iptables -A INPUT –s 10.0.0.0/24 -i eth1 -p tcp -j ACCEPT

* *Permitir las conexiones ya establecidas desde cualquier red.*

iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT

* *Permitir a los usuarios de sistemas conexiones nuevas con cualquier red.*

iptables -A FORWARD –s 10.0.0.0/24 -m state -- state NEW -p tcp -j ACCEPT

* *Permitir a la LAN conexiones nuevas con la DMZ.*

iptables -A FORWARD -s 10.0.1.0/25 -d 10.0.2.64/29 -p tcp –m state --state NEW -j ACCEPT

iptables -A FORWARD -s 10.0.2.0/26 -d 10.0.2.64/29 -p tcp –m state --state NEW -j ACCEPT

iptables -A FORWARD -s 10.0.0.0/24 -d 10.0.2.64/29 -p tcp –m state --state NEW -j ACCEPT

iptables -A FORWARD -s 10.0.1.128/25 -d 10.0.2.64/29 -p tcp –m state --state NEW -j ACCEPT

* *Enmascarar (NAT) todo el tráfico de la LAN hacia la WAN con la dirección IP pública del firewall.*

// La opción *“-t”* permite al usuario seleccionar una tabla diferente a la tabla predeterminada ***filter*** a usar con el comando. En este caso se hace referencia a la tabla ***nat***. La cadena POSTROUTING permite modificar paquetes justo antes de que salgan del equipo. Además, se utiliza MASQUERADE cuando la dirección IP pública que sustituye a la IP origen es dinámica.

iptables -t nat -A POSTROUTING -s 10.0.1.0/25 -d 0/0 -o eth0 -p tcp - j MASQUERADE

iptables -t nat -A POSTROUTING -s 10.0.2.0/26 -d 0/0 -o eth0 -p tcp - j MASQUERADE

iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -d 0/0 -o eth0 -p tcp - j MASQUERADE

iptables -t nat -A POSTROUTING -s 10.0.1.128/25 -d 0/0 -o eth0 -p tcp - j MASQUERADE

* *Hacer una redirección de direcciones (DNAT) para permitir que usuarios de Internet se conecten al servidor web, correo, archivos y DNS dentro de la DMZ, utilizando el bloque de direcciones públicas 200.1.1.0/29.*

//Para conectarse con el Puerto de destino 80 (HTTP). PREROUTING permite modificar paquetes entrantes antes de que se tome una decisión de enrutamiento. Además, ***-j DNAT –to-destination 10.0.2.67*** cambia la dirección IP destino (inicialmente el bloque de direcciones ***200.1.1.0/29***) a 10.0.2.67.

iptables -t nat -A PREROUTING -s 0/0 -d 200.1.1.0/29 -p tcp --dport 80 -eth0 -j DNAT --to-destination 10.0.2.67:80

//Para conectarse con el Puerto de destino 53 (DNS)

iptables -t nat -A PREROUTING -s 0/0 -d 200.1.1.0/29 -p tcp --dport 53 -eth0 -j DNAT --to-destination 10.0.2.68:53

//Para conectarse con el Puerto de destino 25 (SMTP)

iptables -t nat -A PREROUTING -s 0/0 -d 200.1.1.0/29 -p tcp --dport 25 -eth0 -j DNAT --to-destination 10.0.2.66:25

//Para conectarse con el Puerto de destino 21(FTP-CONTROL)

iptables -t nat -A PREROUTING -s 0/0 -d 200.1.1.0/29 -p tcp --dport 21 -eth0 -j DNAT --to-destination 10.0.2.69:21

//Para conectarse con el Puerto de destino 20 (FTP-DATOS)

iptables -t nat -A PREROUTING -s 0/0 -d 200.1.1.0/29 -p tcp --dport 20 -eth0 -j DNAT --to-destination 10.0.2.69:20

* *Permitir al firewall/proxy cualquier paquete de salida (cadena OUTPUT).*

//-P permite configurar la política por defecto para una cadena en particular, de tal forma que, cuando los paquetes atraviesen la cadena completa sin cumplir ninguna regla, serán enviados a un objetivo en particular.

iptables -P OUTPUT ACCEPT

* *Denegar el tráfico restante en las cadenas FORWARD e INPUT.*

iptables -P INPUT DROP iptables -P FORWARD DROP

* *Habilitación del ruteo.*

echo 1 > /proc/sys/net/ipv4/ip\_forward

Paso 5: Configuración del proxy web.

Dentro de la sección ACL en squid.conf, se debe de hacer las siguientes modificaciones, en modo de resúmen debe ser:

http\_port 8080

cache\_mem 1000 MB

cache\_dir ufs /var/spool/squid 10000 16 256 acl CONNECT method CONNECT

acl local\_network src 10.0.1.0/25 10.0.2.0/26 10.0.0.0/24 10.0.1.128/25

acl horario\_oficina time M T W H F 7:00-19:00

acl sitios dstdomain "/usr/local/etc/sitios\_prohibidos.squid"

acl multimedia urlpath\_regex "/etc/squid/listas/multimedia\_prohibido.squid"

http\_access deny sitios\_prohibidos

http\_access deny multimedia http\_access allow horario\_oficina

http\_access allow local\_network

http\_port 8080 transparent

En donde el archivo sitios\_prohibido.squid contiene: facebook, twitter, instagram, youtube, olé.

En donde el archivo multimedia\_prohibido.squid contiene: mp3, mpg, avi, mpe