

---

## Diseño de una Red

---

SERGIO MUÑUMER  
DAVID PASTOR

23 de diciembre de 2018

---

### Índice

<b>1. Resumen Ejecutivo</b>	<b>2</b>	5.5.1. Analisis de riesgos . . . . .	16
<b>2. Objetivo del Proyecto</b>	<b>3</b>	5.5.2. Amenazas . . . . .	16
<b>3. Alcance del Proyecto</b>	<b>3</b>	5.5.3. Contramedidas . . . . .	17
<b>4. Requisitos de Diseño</b>	<b>3</b>	5.6. Discusión . . . . .	18
4.1. Requisitos del Negocio	3	<b>6. Diseño Físico</b>	<b>18</b>
4.2. Requisitos Técnicos . .	4	<b>7. Pruebas del Diseño</b>	<b>27</b>
4.3. Grupos de Usuarios y Almacenamiento de Datos . . . . .	4	<b>A. Apéndices</b>	<b>27</b>
4.4. Aplicaciones en Red . .	7	A.1. Configuración . . . . .	27
<b>5. Diseño Lógico</b>	<b>9</b>	A.1.1. Configuración de Router-A-F . . . . .	28
5.1. Topología . . . . .	10	A.1.2. Configuración de Router-A-01 . . . . .	29
5.2. Nombres . . . . .	11	A.1.3. Configuración de Router-A-02 . . . . .	32
5.3. Direcciones . . . . .	12	A.1.4. Configuración de Router-A-W1 . . . . .	35
5.4. Protocolos de Red . .	12		
5.5. Seguridad . . . . .	15		

### Índice de figuras

1.	Diagrama del Diseño Lógico de la Red . . .	10	3.	Figura Capa de Distribución . . . . .	10
2.	Figura del Núcleo de la Red . . . . .	10	4.	Figura Capa de Acceso	11
			5.	Figura DMZ . . . . .	11

## Índice de tablas

1.	Requisitos del Negocio	5	10.	Direcciones Servidores	15
2.	Requisitos Técnicos . .	6	11.	Identificación de activos	16
3.	Grupos de Usuarios . .	7	12.	Interfaces Routers . .	19
4.	Servidores . . . . .	8	13.	Puertos Switches (1)	20
5.	Aplicaciones en red y características del tráfico asociado . . . . .	9	14.	Puertos Switches (2)	21
			15.	Puertos Switches (3)	22
6.	Esquema de nombres .	12	16.	Puertos Switches (4)	23
7.	Dispositivos instalados	13	17.	Puertos Switches (5)	24
8.	Direccionamiento . . .	14	18.	Puertos Switches (5)	25
9.	VLANs . . . . .	14	19.	Puertos Switches (6)	26
			20.	Pruebas . . . . .	27

---

## 1. Resumen Ejecutivo

Este documento presenta el diseño de la red basado en la actividad de un periódico moderno. La organización en cuestión ofrece servicios de información clásicos (basados en papel impreso) y servicios de información digitales (basados en plataforma online), gracias a la infraestructura descrita en el documento presente.

Dicha infraestructura será necesaria para proveer los servicios de red principales (nombre, DNS, DHCP, control/mantenimiento de dispositivos), así como el acceso a Internet a través de varios enlaces contratados con distintos proveedores de servicios de acceso a Internet (ISP), logrando la diversidad de circuitos, y como consecuencia una alta disponibilidad de la red. El diseño soporta escalabilidad, permitiendo el desarrollo y crecimiento de la empresa, debido a su estructura en 2 partes bien diferenciadas: la parte referente a la actividad interna de la organización y la parte externa cuya finalidad es mantener la plataforma digital de noticias.

La infraestructura permitirá el acceso de los trabajadores a sus recursos desde diferentes localizaciones, incluyendo soporte para trabajo remoto. El portal online estará situado en una zona desmilitarizada, posterior al firewall, y aislado de la red interna. El objetivo es mejorar las prestaciones en este segmento crítico de la red, conllevando una mejora en las condiciones de trabajo para los empleados de la organización, aumento de la calidad para los visitantes del portal web y por tanto, mejorando los beneficios de la organización.

## **2. Objetivo del Proyecto**

El objetivo principal del proyecto es dotar de una infraestructura de red rápida y fiable, diseñada específicamente para satisfacer las necesidades inherentes de la actividad de un periódico, facilitando la expansión de la empresa, habilitando su llegada a nuevos mercados y estableciendo unas condiciones óptimas de trabajo para los empleados.

## **3. Alcance del Proyecto**

Instalación e implementación de una red confeccionada para facilitar el crecimiento de la organización, permitiendo su ampliación hasta 6000 trabajadores, sin entrar en grandes presupuestos sobre el material. Premiando la escalabilidad y la calidad del tráfico, la infraestructura soporta balanceo de carga, ofreciendo condiciones óptimas para el desarrollo de la actividad de la empresa en todo momento, contando con contramedidas planificadas en situaciones excepcionales de carga.

El diseño se basa únicamente en las necesidades de la organización. Está, tiene dos facetas de cara al público, por lo que el diseño también implementa dos sectores. Podría ser una cuestión práctica, sin embargo, es una cuestión de seguridad. El aislamiento de ambas actividades proporciona una buena cobertura frente atacantes externos, que junto con la implementación de mecanismos eficientes de seguridad, dan lugar a una situación cómoda donde poder almacenar información sensible al público, fuentes de información privadas, etc.

En definitiva, la creación de la infraestructura proporcionará un alto grado de confidencialidad, garantizando la unicidad de las actividades, tratando ambas tareas como servicios diferenciados e independientes.

## **4. Requisitos de Diseño**

En esta sección se definen los requisitos de diseño de la red, atendiendo a dos dimensiones. En primer lugar se concretarán los requisitos de la red desde la perspectiva del negocio, que harán posible mejorar los servicios que ofrece el periódico a sus clientes y garantizar la fiabilidad de la red, facilitando la labor diaria de los empleados. Estos requisitos del negocio van a determinar los objetivos técnicos del desarrollo de la red.

### **4.1. Requisitos del Negocio**

El proyecto de diseño de la red permitirá la creación de un canal de comunicaciones, abriendo puertas a la organización a nuevos mercados del negocio. El diseño proveerá acceso a servicios web, tanto internos como externos, manteniendo la independencia entre ambas partes. De cara a la visión

interna de la organización, el proyecto garantiza el acceso a los servidores de administración, y a las aplicaciones necesarias en la labor diaria del periódico. Al mismo tiempo, garantiza el acceso a clientes a la plataforma online pública de la organización. La gestión de las 2 caras del diseño se llevará a cabo de manera compartida, considerando los costes derivados de una gestión aislada de cada parte.

El segmento de acceso a internet estará compuesto por 2 enlaces contratados con 2 proveedores de servicio de internet distintos, es una cuestión de prestaciones y redundancia. Se dispondrá de un enlace WAN con la empresa de servicio de impresión garantizando la disponibilidad, asegurando plazos de trabajo para la organización.

El diseño de la red contempla la posibilidad de teletrabajo. Se establecerán medidas de prevención para facilitar el acceso privado a los recursos de la empresa, por parte de los trabajadores de la empresa. Se establecerán las medidas de prevención oportunas para asegurar la red frente a ataques provenientes de Internet y que pudieran dificultar o impedir ofrecer el servicio de navegación a sus clientes.

La enumeración de los requisitos del negocio puede tener la forma de la Tabla 1.

## **4.2. Requisitos Técnicos**

Para diseñar una red que permita alcanzar los requisitos del negocio se establecen los siguientes requisitos técnicos que se recogen en la Tabla 2.

## **4.3. Grupos de Usuarios y Almacenamiento de Datos**

El proyecto del diseño de la red contempla la existencia de varios grupos con roles diferenciados, estableciendo una división entre el ámbito interno y externo de la organización. La cara externa esta compuesta por dos partes la de los clientes y de administración del servicio web.

La parte interna constará de tantos grupos de usuarios como roles haya en el desarrollo de la actividad de la organización, contando a mayores un trato especial para los usuarios de teletrabajo.

El proyecto incluye 2 servidores principales, uno dedicado a la administración de la organización y al desarrollo de su actividad (SRV-A), y otro para el servicio online ofrecido a los clientes (SRV-B). Un tercer servidor (SRV-C) para el servicio de nóminas, dedicado a la parte de administración y contabilidad de la empresa. Además el proyecto considera la posibilidad de redundancia en el almacenamiento de datos, manteniendo activo un tercer servidor (SRV-Z) de recuperación del sistema (Ver tabla 3.). A mayores tendríamos los servidores proveedores de servicios de configuración automática DNS (SRV-S1) y DHCP (SRV-S2).

Tabla 1: Requisitos del Negocio

Num.	Descripción del Requisito	Crítico (S/N)
1	La red soportará la creación de un canal de comunicaciones, abriendo puertas a la organización a nuevos mercados del negocio.	S
2	En donde sea posible se utilizarán enlaces de fibra óptica	N
3	La red deberá ser capaz de permitir el acceso a la red Internet	S
4	La red permitirá teletrabajo	S
5	La red permitirá el acceso a servicios web, tanto internos como externos, manteniendo la independencia entre ambas partes.	S
6	La red garantiza el acceso a los servidores de administración, y a las aplicaciones necesarias en la labor diaria del periódico.	S
7	La red garantiza el acceso a clientes a la plataforma online pública de la organización.	S
8	La red permitirá establecer alianzas con otras compañías.	S
9	La red permitirá la conexión con el exterior	N
10	El diseño de la red contara con multiples salidas a internet con diferentes proveedores	N
11	La red dispone de mecanismos de proteccion frente a ataques provientes de Internet y que pudieran dificultar o impedir ofrecer el servicio de navegación a sus clientes.	S
12	La red deberá mejorar la accesibilidad para sus clientes.	S
13	La red facilitará la expansión del negocio.	S

Tabla 2: Requisitos Técnicos

Num.	Descripción del Requisito	Crítico (S/N)
1	La red soportará un ancho de banda mínimo de 100 Mbps y estará soportada por enlaces UTP Cat 6	S
2	La red permitirá el acceso a recursos por parte de los empleados desde cualquier ubicación	S
3	La red permitirá el aislamiento del tráfico en función del departamento	S
4	La red realizará la configuración automática de los hosts	S
5	La red contará con diversidad de circuitos	N
6	La red implementará un firewall.	S
7	Se maximizará la disponibilidad de la red.	S
8	La red implementará redundancia en los routers.	S
9	La red implementará redundancia en los switches.	S
10	La red implementará métodos de balanceo de carga.	S
11	La red dispondrá de una DMZ	S
12	La red implementará tecnología VPN.	S
13	La conexión de servidores y la capa de el núcleo se realizará mediante fibra óptica	S

A continuación, se muestran los principales almacenes de datos (servidores) y su localización (Ver tabla 4).

Tabla 3: Grupos de Usuarios

<b>Grupo Usuarios</b>	<b>Tamaño</b>	<b>Localización</b>	<b>Aplicaciones Utilizadas</b>
Dirección	10	Edificio A	Aplicacion de streaming, Correo, Web, Bases de datos
Redacción	30	Edificio A	Servidor de fotografia y video, Correo, Web, Bases de datos
Jefes de sección	10	Edificio A	Servidor de fotografia y video, Correo, Web, Bases de datos, Servicio de impresion
Maquetación	30	Edificio A	Servidor de fotografia y video, Correo, Web, Bases de datos
Corrección	30	Edificio A	Servidor de fotografia y video, Correo, Web, Bases de datos
Teletrabajo	15	X	Aplicacion de streaming, Correo, Web, Bases de datos, Teletrabajo
Contabilidad	5	Edificio A	Servicio de contabilidad, Nóminas, Administrativo
Administración Interna	5	Edificio B	Servicio de Backup, Bases de datos
Administración Web	5	Edificio B	Servicio de Backup, Bases de datos
Usuarios online	¿?	X	Web

#### 4.4. Aplicaciones en Red

La red esta diseñada para soportar la carga producida por aplicaciones de streaming(vídeo/audio)<sup>1</sup>. La gestión sobre la base de datos, el servicio de correo electrónico interno y los de impresión fotografía y video están soportados por el SRV-A. El servicio web online y el de trabajo remoto se

<sup>1</sup>Las estimaciones están basadas en los cálculos proporcionados por Microsoft[Mic]

Tabla 4: Servidores

<b>Servidor</b>	<b>Localización</b>	<b>Aplicaciones</b>	<b>Usado por Grupo Usuarios</b>
SVR-A	Edificio A, planta Baja	Aplicacion de streaming, Base de datos, Teletrabajo, Servicio de impresión, Servicio de fotografía y vídeo	Dirección, Redacción, Jefes de sección, Maquetación, Corrección
SVR-B	Edificio A, planta Baja	Servicio Web, Servidor de correo	Usuarios online, Administración Web
SVR-C	Edificio A, planta Baja	Servicio de contabilidad, Nóminas, Administrativo	Contabilidad
SVR-S1	Edificio A, planta Baja	DNS	Red Interna
SVR-S2	Edificio A, planta Baja	DHCP	Red Interna
SVR-Z	Edificio A, planta Baja	Servicio de Backup	Administración interna, Administración web



soportan en un servidor SRV-B, por motivos de seguridad y prestaciones, donde almacenaremos la información de los usuarios online en una base de datos aislada de la actividad interna. El servicio contable, referente a lo administrativo, nóminas, etc, se soporta en el servidor SRV-C. El servicio de backup/mantenimiento es sostenido por el SRV-Z. En esta sección se enumeran y caracterizan las aplicaciones de red (Ver tabla 5).

Tabla 5: Aplicaciones en red y características del tráfico asociado

<b>Aplicación</b>	<b>Nueva (S/N)</b>	<b>Crítica (S/N)</b>	<b>Grupo-Usuarios</b>	<b>Servidor</b>	<b>Ancho de Banda Estima- do</b>
Aplicacion de streaming	S	S	Teletrabajo,Dirección	SVR-A	500 Kbps
Bases de datos	S	S	Todos	SVR-A	100 Kbps
Servidor de correo	S	N	Todos	SVR-B	50 Kbps
Teletrabajo	S	S	Teletrabajo	SVR-A	256 Kbps
Servicio de impresión	S	S	Jefes de sección,Redacción	SVR-A	50 Kbps
Servicio Web	S	N	Usuarios online,Teletrabajo	SVR-B	256 Kbps
Servicio de Backup	S	S	Administración Interna y Web	SVR-Z	1000 Kbps
Servicio Contable	S	S	Contabilidad	SVR-C	300 Kbps
Servidor de fotografía y video	S	S	Todos	SVR-A	500 Kbps

## 5. Diseño Lógico

En esta sección se muestran los aspectos de diseño de la red relacionados con la topología y los esquemas de denominación y numeración de los dispositivos, así como los principales protocolos implicados en la red.

## 5.1. Topología

La topología de la red es un reflejo directo de la disposición de los elementos a conectar y de los requisitos impuestos por el negocio. Desde una perspectiva de alto nivel, la red a diseñar responderá al diseño mostrado en la figura 1.

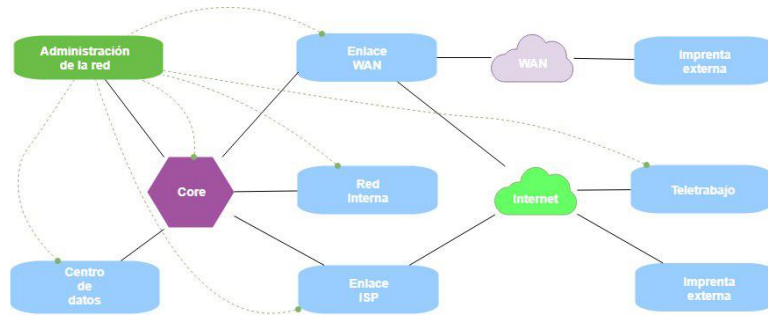


Figura 1: Diagrama del Diseño Lógico de la Red

Entrando un poco más en detalle sobre la distribución de dispositivos, nos encontramos con 3 capas especializadas, más la DMZ:

- Capa del núcleo (Figura 2).

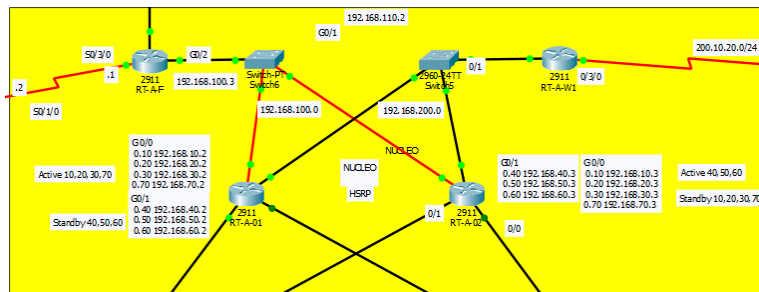


Figura 2: Figura del Núcleo de la Red

- Capa de distribución (Figura 3).

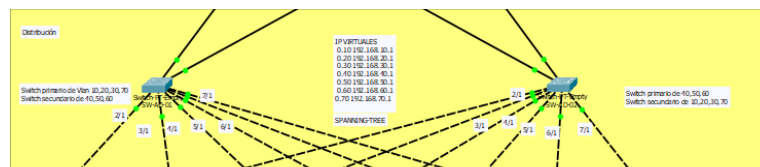


Figura 3: Figura Capa de Distribución

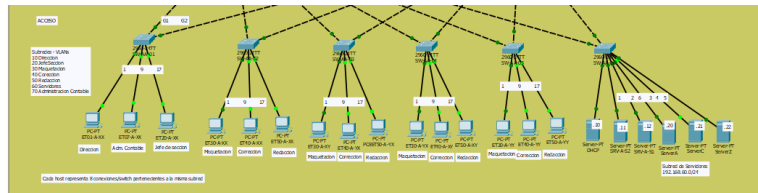


Figura 4: Figura Capa de Acceso

- Capa de acceso (Figura 4).
- DMZ (Figura 5).

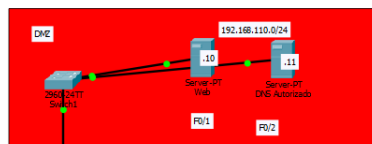


Figura 5: Figura DMZ

## 5.2. Nombres

La asignación de nombres de los dispositivos, sigue la lógica descrita a continuación (Ver tabla 6).

- Para los Router, RT, seguidas del identificador de la sede física, y del identificador único del dispositivo. El router que implementa el firewall recibirá el siguiente identificador: RT-X-F, siendo X el identificador de la sede física. Los routers que soportan los enlaces WAN, reciben el siguiente identificador: RT-X-WY, siendo X el identificador de la sede, e Y el identificador único de conexiones WAN. En caso de establecer un nuevo enlace WAN, el router que los soporte recibirá el siguiente nombre: RT-X-W2. El router principal de la sede A sería: RT-A-01, y el firewall de la sede B: RT-B-F.
- Para los Switch, SW, seguidas del identificador de la sede física unido a una letra que determina su nivel (Distribución D, Acceso A), más el

identificador único del dispositivo. Por ejemplo, el switch principal de Distribucion de la sede A sería: **SW-AD-01**, y el tercero de la sede B en el nivel de acceso: **SW-BA-03**.

- La identificación de los servidores seguirá la lógica usada hasta ahora, utilizando **SRV**, más la letra identificadora del dispositivo. El orden para asignar letras será alfabético, reservando **W,X,Y,Z** para los dispositivos de recuperación/mantenimiento y la **S** para servicios. Hacemos una distinción para aquellos servidores proveedores de servicios de configuración, asignándoles la letra **S**, más un número identificador del servicio. Por ejemplo, el servidor de DNS será **SRV-S2**.
- Para la estaciones de trabajo, **ET**, seguidas de su localizador físico y de su identificador único de dispositivo. Así, la cuarta estación de trabajo de la sede A sería: **ET-A-04** y la decimosegunda de la sede B: **ET-B-12**.

La relación de dispositivos instalados en la red se dispone en las tablas 6 y 7.

Tabla 6: Esquema de nombres

<b>Dispositivo</b>	<b>Nombre</b>
Estación de trabajo	ET
Servidor	SRV
Router	RT
Switch	SW

### 5.3. Direcciones

Para cumplir los requisitos de aislamiento de tráfico interdepartamental, facilidad administrativa y futura expansión, hemos dividido la LAN de la empresa en varias subredes. Estas subredes se enumeran en la tabla 8.

En la tabla 9 se muestra la correspondencia entre grupos de usuarios, subred y las VLANs designadas.

Los servidores instalados de la red, se corresponden con la siguiente denominación (Tabla 10).

### 5.4. Protocolos de Red

En esta sección enumeraremos y describiremos los protocolos de red seleccionados para el diseño de la red. Su elección es una consecuencia directa de los requisitos técnicos y de negocio descritos anteriormente.

Tabla 7: Dispositivos instalados

ID	Tipo	Ubicación	Función
RT-A-F	Router	Edificio A	Firewall
RT-A-W1	Router	Edificio A	Enlace WAN-1
RT-A-01	Router	Edificio A	Core
RT-A-02	Router	Edificio A	Core
SW-AD-01	Switch	Edificio A	Distribución
SW-AD-02	Switch	Edificio A	Distribución
SW-AA-01	Switch	Edificio A	Acceso
SW-AA-02	Switch	Edificio A	Acceso
SW-AA-03	Switch	Edificio A	Acceso
SW-AA-04	Switch	Edificio A	Acceso
SW-AA-05	Switch	Edificio A	Acceso
SW-AA-06	Switch	Edificio A	Acceso
SRV-A	Servidor	Edificio A	Servicio Interno
SRV-B	Servidor	Edificio A	Servicio Externo
SRV-C	Servidor	Edificio A	Servicio Contable
SRV-S0	Servidor	Edificio A	DNS Autorizado
SRV-S1	Servidor	Edificio A	Servicio DHCP
SRV-S2	Servidor	Edificio A	Servicio DNS
SRV-Z	Servidor	Edificio A	Servicio Recuperación
ET-A-X	Servidor	Edificio A	Estaciones de trabajo / X perteneciente (1,120)

Tabla 8: Direccionamiento

Segmento o Subred	Dirección IP/Máscara	Router por Defecto	Servidor DHCP
Dirección	192.168.10.0/24	192.168.10.1/24	192.168.60.10/24
Jefes Sección	192.168.20.0/24	192.168.20.1/24	192.168.60.10/24
Maquetación	192.168.30.0/24	192.168.30.1/24	192.168.60.10/24
Corrección	192.168.40.0/24	192.168.40.1/24	192.168.60.10/24
Redacción	192.168.50.0/24	192.168.50.1/24	192.168.60.10/24
Servidores	192.168.60.0/24	192.168.60.1/24	
Contabilidad	192.168.70.0/24	192.168.70.1/24	192.168.60.10/24
Segmento 1	192.168.100.0/24	192.168.100.2/24	
Segmento 2	192.168.200.0/24	192.168.200.2/24	
DMZ	192.168.110.0/24	192.168.110.2/24	

Tabla 9: VLANs

Grupo Usuarios	Subred IP/máscara	Número VLAN
Dirección	192.168.10.0/24	10
Jefes Sección	192.168.20.0/24	20
Maquetación	192.168.30.0/24	30
Corrección	192.168.40.0/24	40
Redacción	192.168.50.0/24	50
Servidores	192.168.60.0/24	60
Contabilidad	192.168.70.0/24	70

Tabla 10: Direcciones Servidores

Host	Dirección IP
SVR-S0	192.168.110.11
SVR-S1	192.168.60.10
SVR-S2	192.168.60.11
SVR-A	192.168.60.20
SVR-B	192.168.110.10
SVR-C	192.168.60.21
SVR-Z	192.168.60.60

Para obtener un alto grado de fiabilidad, utilizaremos el protocolo HSRP (Hot Standby Router Protocol). Dicho protocolo (propiedad de CISCO) actúa en la capa 3, permitiendo el despliegue de routers redundantes tolerantes a fallos y evitando así, la existencia de puntos únicos de fallo. En cuestión de disponibilidad y prestaciones, la elección del protocolo PVST (Per VLAN Spanning Tree) ha sido nuestra opción. Este protocolo (propiedad de CISCO) actúa en la capa 2, trata cada VLAN como una red independiente, manteniendo una instancia de Spanning Tree (STP) por cada una. El protocolo Spanning Tree controla la activación o desactivación automática de los enlaces de conexión, garantizando la inexistencia de bucles en la malla de switches, garantizando la disponibilidad de las conexiones.

Respecto a los protocolos de encamio (Capa 3), la recomendación en el diseño es OSPF (Open Shortest Path First). Es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos. Favoreciendo un menor consumo del ancho de banda, minimizando retardos. Todo con el objetivo de mejorar la carga de tráfico y la fiabilidad de la infraestructura.

## 5.5. Seguridad

En esta sección daremos una visión mínimamente detallada sobre el modo en que se ha abordado la seguridad en el diseño de la red.

En primer lugar, no podemos permitir que la red interna de la organización se comunique directamente con el exterior, pues podría ser un punto de fuga de información. Por ello, hemos decidido introducir en el diseño una zona desmilitarizada (DMZ), a través de la cuál se permitirá el acceso a la plataforma online de noticias.

La recién citada zona, contiene un servidor web, que podrá comunicarse

tanto con el interior de la red para obtener datos, como al exterior para ofrecerlos. En otras palabras, dicho servidor resolverá las consultas de los clientes y las devolverá a través de la página web. Esta estrategia nos dará la cobertura necesaria para mantener la privacidad de nuestros servidores internos. En la zona desmilitarizada también proveeremos el servicio DNS, implementando un DNS autorizado.

La división de la estructura en dos partes, servicio externo y LAN interna es una cuestión de seguridad.

#### 5.5.1. Análisis de riesgos

Comenzaremos realizando una identificación de los activos.(Tabla 11).

Tabla 11: Identificación de activos

ID	Descripción	Ubicación	Crítico (S/N)
SRV-A	Servidor interno	Edificio A	S
SRV-B	Servidor externo	Edificio A	S
SRV-C	Servidor contable	Edificio A	S
SRV-Z	Servidor mantenimiento	Edificio A	S
RT-A-F	Router frontera	Edificio A	S
RT-A-01	Core	Edificio A	S
RT-A-02	Core	Edificio A	S
ET-A-X	Estaciones de trabajo	Edificio A	S
SRV-SX	Servidor configuración	Edificio A	S

#### 5.5.2. Amenazas

A continuación, se muestra una clasificación<sup>2</sup> de las amenazas principales del diseño. Esto es solo un pequeño índice, el desglose total, y la evaluación de riesgos, será detallada en el Plan Director de Seguridad (PDS).

- Naturales:
  - Daños por fuego

---

<sup>2</sup>El estudio de amenazas ha sido realizado en base a las recomendaciones del Instituto Nacional de Ciberseguridad[Inc]



- Daños por inundación.
- Daños por fallo eléctrico.
- Desastre natural.
- Funcionales:
  - Perdidas de información.
  - Modificación de la información.
  - Interceptación de la información.
  - Introducción de falsa información.
  - Envenenamiento de los routers.
  - Envenenamiento de las estaciones de trabajo.
  - Acceso no autorizado
  - Pérdida de equipos de trabajo.
  - Difusión de software dañino.
  - Caída del sistema por sobrecarga.
- Negligencias:
  - Errores de usuarios.
  - Errores del administrador.
  - Errores de configuración.
- Sociales:
  - Robo.
  - Extorsión.
  - Ingeniería social.
  - Denegación de servicio.

### 5.5.3. Contramedidas

En esta sección se muestran las medidas preventivas tomadas para minimizar amenazas.

- Acomodación de un espacio, en condiciones de temperatura y humedad óptimas para la instalación del CPD.
- Para evitar todo tipo de accesos indebidos, y así mantener la información segura, estableceremos como frontera entre nuestra red interna (LAN), y el mundo exterior un cortafuegos. Su misión es el filtrado de paquetes, denegando el acceso a todos aquellos paquetes no reconocidos (posibles intenciones maliciosas), enrutando solo tráfico conocido

y esperado. Para mayor seguridad, el router frontera, también contará con la implementación de reglas de filtrado de tráfico, así reparten la carga de análisis de paquetes.

- Contratación de personal cualificado, con el conocimiento adecuado para el manejo/mantenimiento de la red.
- Prohibir la tenencia de dispositivos electrónicos personales, evitará posibles fugas de información.
- Prohibir las conexiones con el mundo exterior, excepto las mencionadas en este documento.

## 5.6. Discusión

La infraestructura diseñada cumple con los requisitos del negocio, ofreciendo un alto grado de disponibilidad de la red, soportado por la redundancia de dispositivos. El diseño garantiza altas prestaciones, minimizando el tráfico de protocolos de configuración de la red, ofreciendo balanceo de carga, optimizando el ancho de banda disponible. La estructuración de dispositivos y los esquemas de direcciones y nombres permiten una gran ampliación de la organización, escalable hasta 8000 usuarios. La división del tráfico en función de su propósito garantiza el aislamiento de la información, y la integridad de la misma. Por último cabe mencionar, la posibilidad brindada de crear puestos de trabajo remoto en la organización.

## 6. Diseño Físico

Esta sección describe las características y usos recomendados de las tecnologías y los dispositivos elegidos para implementar el diseño.

Los dispositivos elegidos para la implementación de la red, son los siguientes:

- Router Cisco 2911 (Núcleo)
- Switches Cisco 2960 (Capa Acceso)
- Switches Cisco SG-200-08P (Capa Distribución)

El cableado de la instalación será UTP Cat 6. El ancho de banda previsto para la capa de acceso es de 100 Mbps, mientras que el núcleo y la capa de distribución operarán a 1 Gbps. Se dispone de un enlace WAN para la conexión directa con la empresa de impresión. Los detalles de configuración de los routers se muestran en la tabla 12, y los de los switches se muestran en las tablas 13, 14, 15, 17, 18, 19.

Tabla 12: Interfaces Routers

Router	Interfaz	Dirección IP	Dot 1Q	IP Helper	IP Helper 2	ACL
RTR-A-W1	Gi0/1	192.168.200.3		192.168.60.10	192.168.60.12	
	Se0/3/0	200.10.20.1		192.168.60.10	192.168.60.12	
RTR-A-01	Gi0/0.10	192.168.10.2	10	192.168.60.10	192.168.60.12	
	Gi0/0.20	192.168.20.2	20	192.168.60.10	192.168.60.12	
	Gi0/0.30	192.168.30.2	30	192.168.60.10	192.168.60.12	
	Gi0/1.40	192.168.40.2	40	192.168.60.10	192.168.60.12	
	Gi0/1.50	192.168.50.2	50	192.168.60.10	192.168.60.12	
	Gi0/1.60	192.168.60.2	60	192.168.60.10	192.168.60.12	
	Gi0/0.70	192.168.70.2	70	192.168.60.10	192.168.60.12	
	Gi0/2	192.168.200.1		192.168.60.10	192.168.60.12	
	Gi0/3/0	192.168.100.1		192.168.60.10	192.168.60.12	
RTR-A-02	Gi0/0.10	192.168.10.3	10	192.168.60.10	192.168.60.12	
	Gi0/0.20	192.168.20.3	20	192.168.60.10	192.168.60.12	
	Gi0/0.30	192.168.30.3	30	192.168.60.10	192.168.60.12	
	Gi0/1.40	192.168.40.3	40	192.168.60.10	192.168.60.12	
	Gi0/1.50	192.168.50.3	50	192.168.60.10	192.168.60.12	
	Gi0/1.60	192.168.60.3	60	192.168.60.10	192.168.60.12	
	Gi0/0.70	192.168.70.3	70	192.168.60.10	192.168.60.12	
	Gi0/2	192.168.200.2		192.168.60.10	192.168.60.12	
	Gi0/3/0	192.168.100.2		192.168.60.10	192.168.60.12	
RTR-A-F	Gi0/1	192.168.110.2		192.168.60.10	192.168.60.12	
	Gi0/2	192.168.100.3		192.168.60.10	192.168.60.12	
	Se0/3/0	200.30.30.1		192.168.60.10	192.168.60.12	

Tabla 13: Puertos Switches (1)

Switch	Puerto	VLAN
SW-AD-01	Gi0/1	Trunk
	Gi1/1	Trunk
	Gi2/1	Trunk
	Gi3/1	Trunk
	Gi4/1	Trunk
	Gi5/1	Trunk
	Gi6/1	Trunk
	Gi7/1	Trunk
	Gi8/1	Trunk
	Gi9/1	Trunk
SW-AD-02	Gi0/1	Trunk
	Gi1/1	Trunk
	Gi2/1	Trunk
	Gi3/1	Trunk
	Gi4/1	Trunk
	Gi5/1	Trunk
	Gi6/1	Trunk
	Gi7/1	Trunk
	Gi8/1	Trunk
	Gi9/1	Trunk

Tabla 14: Puertos Switches (2)

Switch	Puerto	VLAN
SW-AA-01	Fa0/1	10
	Fa0/1	10
	Fa0/2	10
	Fa0/3	10
	Fa0/4	10
	Fa0/5	10
	Fa0/6	10
	Fa0/7	10
	Fa0/8	10
	Fa0/9	70
	Fa0/10	70
	Fa0/11	70
	Fa0/12	70
	Fa0/13	70
	Fa0/14	70
	Fa0/15	70
	Fa0/16	70
	Fa0/17	20
	Fa0/18	20
	Fa0/19	20
	Fa0/20	20
	Fa0/21	20
	Fa0/22	20
	Fa0/23	20
	Fa0/24	20
	Gi0/1	Trunk
	Gi0/2	Trunk

Tabla 15: Puertos Switches (3)

Switch	Puerto	VLAN
SW-AA-02	Fa0/1	30
	Fa0/1	30
	Fa0/2	30
	Fa0/3	30
	Fa0/4	30
	Fa0/5	30
	Fa0/6	30
	Fa0/7	30
	Fa0/8	30
	Fa0/9	40
	Fa0/10	40
	Fa0/11	40
	Fa0/12	40
	Fa0/13	40
	Fa0/14	40
	Fa0/15	40
	Fa0/16	40
	Fa0/17	50
	Fa0/18	50
	Fa0/19	50
	Fa0/20	50
	Fa0/21	50
	Fa0/22	50
	Fa0/23	50
	Fa0/24	50
	Gi0/1	Trunk
	Gi0/2	Trunk

Tabla 16: Puertos Switches (4)

Switch	Puerto	VLAN
SW-AA-03	Fa0/1	30
	Fa0/1	30
	Fa0/2	30
	Fa0/3	30
	Fa0/4	30
	Fa0/5	30
	Fa0/6	30
	Fa0/7	30
	Fa0/8	30
	Fa0/9	40
	Fa0/10	40
	Fa0/11	40
	Fa0/12	40
	Fa0/13	40
	Fa0/14	40
	Fa0/15	40
	Fa0/16	40
	Fa0/17	50
	Fa0/18	50
	Fa0/19	50
	Fa0/20	50
	Fa0/21	50
	Fa0/22	50
	Fa0/23	50
	Fa0/24	50
	Gi0/1	Trunk
	Gi0/2	Trunk

Tabla 17: Puertos Switches (5)

Switch	Puerto	VLAN
SW-AA-04	Fa0/1	30
	Fa0/1	30
	Fa0/2	30
	Fa0/3	30
	Fa0/4	30
	Fa0/5	30
	Fa0/6	30
	Fa0/7	30
	Fa0/8	30
	Fa0/9	40
	Fa0/10	40
	Fa0/11	40
	Fa0/12	40
	Fa0/13	40
	Fa0/14	40
	Fa0/15	40
	Fa0/16	40
	Fa0/17	50
	Fa0/18	50
	Fa0/19	50
	Fa0/20	50
	Fa0/21	50
	Fa0/22	50
	Fa0/23	50
	Fa0/24	50
	Gi0/1	Trunk
	Gi0/2	Trunk



Tabla 18: Puertos Switches (5)

Switch	Puerto	VLAN
SW-AA-05	Fa0/1	30
	Fa0/1	30
	Fa0/2	30
	Fa0/3	30
	Fa0/4	30
	Fa0/5	30
	Fa0/6	30
	Fa0/7	30
	Fa0/8	30
	Fa0/9	40
	Fa0/10	40
	Fa0/11	40
	Fa0/12	40
	Fa0/13	40
	Fa0/14	40
	Fa0/15	40
	Fa0/16	40
	Fa0/17	50
	Fa0/18	50
	Fa0/19	50
	Fa0/20	50
	Fa0/21	50
	Fa0/22	50
	Fa0/23	50
	Fa0/24	50
	Gi0/1	Trunk
	Gi0/2	Trunk

Tabla 19: Puertos Switches (6)

Switch	Puerto	VLAN
SW-AA-06	Fa0/1	60
	Fa0/1	60
	Fa0/2	60
	Fa0/3	60
	Fa0/4	Trunk,60,70,10
	Fa0/5	60
	Fa0/6	60
	Fa0/7	60
	Fa0/8	60
	Fa0/9	60
	Fa0/10	60
	Fa0/11	60
	Fa0/12	60
	Fa0/13	60
	Fa0/14	60
	Fa0/15	60
	Fa0/16	60
	Fa0/17	60
	Fa0/18	60
	Fa0/19	60
	Fa0/20	60
	Fa0/21	60
	Fa0/22	60
	Fa0/23	60
	Fa0/24	60
	Gi0/1	Trunk
	Gi0/2	Trunk

## 7. Pruebas del Diseño

En esta sección se indicarán los resultados de las pruebas realizadas para validar el diseño propuesto. Se describirán los objetivos de las pruebas, el test realizado y el resultado obtenido.(Tabla 20).

Tabla 20: Pruebas

Objetivo del Test	Prueba Realizada	Resultado
Comunicación entre departamentos y servidores centrales	Ping entre ET1-A-01 y SRV-A	Positivo
Comunicación entre departamento de dirección y otros departamentos	Ping entre ET1-A-01 y ET2-A-03	Positivo
Comunicación entre departamento de dirección con servidor web mediante DNS	HTTP ENTRE ET1-A-01 y SRV-WEB	Positivo
Bloqueo de Conexión a internet de todos los departamentos excepto dirección	Ping entre ET2-A-03 y RT-ISP	Positivo
Comunicación con servicios de impresión de los departamentos dirección y jefes de sección	Ping entre ET1-A-01 y SRV-Impresion	Positivo
Funcionamiento de DHCP primario	ET1-A-01 pide DHCP	Positivo
Funcionamiento de DHCP secundario en caso de fallo del primario	SRV-DHCP apagado y ET1-A-01 pide DHCP	Positivo
Funcionamiento de redundancia en routers con HSRP	RT-1 apagado RT2 da acceso	Positivo
Clientes pueden acceder a servicios DNS y WEB	HTTP entre CLI1 y SRV-WEB	Positivo
Teletrabajo puede comunicarse con departamento de dirección	Ping entre TELE1 y ET1-A-01	Positivo
Departamento de dirección puede comunicarse con el exterior	Ping ET1-A-01 a RT-ISP	Positivo

## A. Apéndices

### A.1. Configuración

A continuación se puede ver la configuración de los routers.

### A.1.1. Configuración de Router-A-F

```
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface GigabitEthernet0/1  
  ip address 192.168.110.2 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/2  
  ip address 192.168.100.3 255.255.255.0  
  ip access-group 101 in  
  ip nat inside  
  duplex auto  
  speed auto  
!  
interface Serial0/3/0  
  ip address 200.30.30.1 255.255.255.0  
  ip access-group 102 in  
  ip nat outside  
  clock rate 2000000  
!  
interface Serial0/3/1  
  no ip address  
  clock rate 2000000  
  shutdown  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
router ospf 1  
  log-adjacency-changes  
  network 192.168.100.0 0.0.0.255 area 1  
  network 192.168.110.0 0.0.0.255 area 1  
  default-information originate  
!  
router rip  
!  
ip nat inside source list 1 interface Serial0/3/0 overload  
ip classless  
ip route 0.0.0.0 0.0.0.0 200.30.30.2
```

```

!
ip flow-export version 9
!
!
access-list 1 permit 192.168.100.0 0.0.0.255
access-list 102 permit ip host 10.10.10.10 192.168.10.0 0.0.0.255
access-list 102 permit tcp any host 192.168.110.10 eq www
access-list 102 permit udp any host 192.168.110.11 eq domain
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 101 permit ospf any any
access-list 101 permit ip 192.168.10.0 0.0.0.255 any
access-list 101 deny ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!
!
end

```

### A.1.2. Configuración de Router-A-01

```

spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 192.168.10.2 255.255.255.0
  ip helper-address 192.168.60.10
  ip helper-address 192.168.60.12
  ip access-group 103 out
  standby 1 ip 192.168.10.1
  standby 1 priority 150

```

```

    standby 1 preempt
!
interface GigabitEthernet0/0.20
    encapsulation dot1Q 20
    ip address 192.168.20.2 255.255.255.0
    ip helper-address 192.168.60.10
    ip helper-address 192.168.60.12
    ip access-group 104 out
    standby 1 ip 192.168.20.1
    standby 1 priority 150
    standby 1 preempt
!
interface GigabitEthernet0/0.30
    encapsulation dot1Q 30
    ip address 192.168.30.2 255.255.255.0
    ip helper-address 192.168.60.10
    ip helper-address 192.168.60.12
    ip access-group 105 out
    standby 1 ip 192.168.30.1
    standby 1 priority 150
    standby 1 preempt
!
interface GigabitEthernet0/0.70
    encapsulation dot1Q 70
    ip address 192.168.70.2 255.255.255.0
    ip helper-address 192.168.60.10
    ip helper-address 192.168.60.12
    ip access-group 106 out
    standby 1 ip 192.168.70.1
    standby 1 priority 150
    standby 1 preempt
!
interface GigabitEthernet0/1
    no ip address
    duplex auto
    speed auto
!
interface GigabitEthernet0/1.40
    encapsulation dot1Q 40
    ip address 192.168.40.2 255.255.255.0
    ip helper-address 192.168.60.10
    ip helper-address 192.168.60.12
    ip access-group 107 out
    standby 1 ip 192.168.40.1
!
interface GigabitEthernet0/1.50
    encapsulation dot1Q 50
    ip address 192.168.50.2 255.255.255.0
    ip helper-address 192.168.60.10
    ip helper-address 192.168.60.12
    ip access-group 108 out
    standby 1 ip 192.168.50.1
!
interface GigabitEthernet0/1.60

```

```

encapsulation dot1Q 60
ip address 192.168.60.2 255.255.255.0
ip helper-address 192.168.60.12
standby 1 ip 192.168.60.1
!
interface GigabitEthernet0/2
ip address 192.168.200.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/0/0
ip address 192.168.100.1 255.255.255.0
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 1
network 192.168.20.0 0.0.0.255 area 1
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 1
network 192.168.50.0 0.0.0.255 area 1
network 192.168.60.0 0.0.0.255 area 1
network 192.168.70.0 0.0.0.255 area 1
network 192.168.100.0 0.0.0.255 area 1
network 192.168.200.0 0.0.0.255 area 1
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 103 permit ip 192.168.10.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 106 permit ip 192.168.70.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255

```

```

access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 107 deny ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 107 deny ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 107 deny ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 107 deny ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 107 deny ip 192.168.40.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 107 permit ip any any
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 108 deny ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 108 deny ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 108 deny ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 108 deny ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 108 deny ip 192.168.50.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 108 permit ip any any
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.70.0 0.0.0.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!
!
end

```

### A.1.3. Configuración de Router-A-02

```

spanning-tree mode pvst
!
!
!
!
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto

```



```

!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.3 255.255.255.0
 ip helper-address 192.168.60.10
 ip helper-address 192.168.60.12
 ip access-group 103 out
 standby 1 ip 192.168.10.1
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.3 255.255.255.0
 ip helper-address 192.168.60.10
 ip helper-address 192.168.60.12
 ip access-group 104 out
 standby 1 ip 192.168.20.1
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.3 255.255.255.0
 ip helper-address 192.168.60.10
 ip helper-address 192.168.60.12
 ip access-group 105 out
 standby 1 ip 192.168.30.1
!
interface GigabitEthernet0/0.70
 encapsulation dot1Q 70
 ip address 192.168.70.3 255.255.255.0
 ip helper-address 192.168.60.10
 ip helper-address 192.168.60.12
 ip access-group 106 out
 standby 1 ip 192.168.70.1
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 192.168.40.3 255.255.255.0
 ip helper-address 192.168.60.10
 ip helper-address 192.168.60.12
 ip access-group 107 out
 standby 1 ip 192.168.40.1
 standby 1 priority 150
 standby 1 preempt
!
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 192.168.50.3 255.255.255.0
 ip helper-address 192.168.60.10
 ip helper-address 192.168.60.12
 ip access-group 108 out

```

```

standby 1 ip 192.168.50.1
standby 1 priority 150
standby 1 preempt
!
interface GigabitEthernet0/1.60
encapsulation dot1Q 60
ip address 192.168.60.3 255.255.255.0
ip helper-address 192.168.60.12
standby 1 ip 192.168.60.1
standby 1 priority 150
standby 1 preempt
!
interface GigabitEthernet0/2
ip address 192.168.200.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/3/0
ip address 192.168.100.2 255.255.255.0
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.10.0 0.0.0.255 area 1
network 192.168.20.0 0.0.0.255 area 1
network 192.168.30.0 0.0.0.255 area 1
network 192.168.40.0 0.0.0.255 area 1
network 192.168.50.0 0.0.0.255 area 1
network 192.168.60.0 0.0.0.255 area 1
network 192.168.70.0 0.0.0.255 area 1
network 192.168.100.0 0.0.0.255 area 1
network 192.168.200.0 0.0.0.255 area 1
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 103 deny ip 192.168.10.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 103 permit ip 192.168.10.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 104 deny ip 192.168.20.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255

```

```

access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 105 deny ip 192.168.30.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 106 deny ip 192.168.70.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 106 permit ip 192.168.70.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.70.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 107 permit ip 192.168.40.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 108 permit ip 192.168.50.0 0.0.0.255 192.168.70.0 0.0.0.255
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
  login
!
!
!
end

```

#### A.1.4. Configuración de Router-A-W1

```

spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.200.3 255.255.255.0
  ip access-group 111 in
  duplex auto

```

```

    speed auto
!
interface GigabitEthernet0/2
    no ip address
    duplex auto
    speed auto
!
interface Serial0/3/0
    ip address 200.10.20.1 255.255.255.0
    ip access-group 112 in
    clock rate 2000000
!
interface Serial0/3/1
    no ip address
    clock rate 2000000
    shutdown
!
interface Vlan1
    no ip address
    shutdown
!
router ospf 1
    log-adjacency-changes
    network 200.10.20.0 0.0.0.255 area 1
    network 192.168.200.0 0.0.0.255 area 1
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
access-list 111 permit ospf any any
access-list 111 permit ip 192.168.10.0 0.0.0.255 any
access-list 111 permit ip 192.168.20.0 0.0.0.255 any
access-list 111 permit ip 192.168.60.0 0.0.0.255 any
access-list 111 deny ip any any
access-list 112 permit ospf any any
access-list 112 permit ip 172.16.0.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 112 permit ip 172.16.0.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 112 permit ip 172.16.0.0 0.0.0.255 192.168.60.0 0.0.0.255
access-list 112 deny ip any any
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
    login

```

!  
!  
!  
end

## Referencias

- [Inc] Incibe. Plan director de seguridad. Technical report, Incibe.
- [Mic] Microsoft. Cantidad de ancho de banda - skype. Technical report, Microsoft.