# PROYECTO DE INFRAESTRUCTURA

# TERNERAS DE TAMBO



# GNC

# Gestión de Nacimiento y Cría

Integrantes:

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

Contenido

[PROYECTO DE INFRAESTRUCTURA 1](#_Toc534503130)

[TERNERAS DE TAMBO 1](#_Toc534503131)

[GNC 1](#_Toc534503132)

[Gestión de Nacimiento y Cría 1](#_Toc534503133)

[WINDOWS SERVER: 3](#_Toc534503134)

[DNS o Domain Name System 3](#_Toc534503135)

[Directorio Activo. 4](#_Toc534503136)

[Dominio. 4](#_Toc534503137)

[Unidad Organizativa(OU). 4](#_Toc534503138)

[Grupos. 4](#_Toc534503139)

[Objetos. 4](#_Toc534503140)

[DHCP 5](#_Toc534503141)

[SERVICIOS A IMPLEMENTAR 5](#_Toc534503142)

[Servidor DHCP Y DNS 5](#_Toc534503143)

[Equipos finales 8](#_Toc534503144)

[Servidor de archivos (FILE SERVER) 10](#_Toc534503145)

[Servidor de IMPSRESIÓN (PRINT SERVER) 10](#_Toc534503146)

[ conectar impresora a red 10](#_Toc534503147)

[ imprimir trabajos desde cualquier equipo 10](#_Toc534503148)

[ impresión en internet 10](#_Toc534503149)

[Zona DMZ: la zona segura de la red 11](#_Toc534503150)

[¿Qué es una DMZ? 11](#_Toc534503151)

[Virtualización 12](#_Toc534503152)

[Falla en Servicios 12](#_Toc534503153)

[¿Qué es el Análisis FODA? 14](#_Toc534503154)

## WINDOWS SERVER:

Es un sistema operativo para empresas y para ejecutar servidores de red o los servidores de archivo. Dentro de las tareas que puede realizar se incluyen: crear cuentas de usuarios, asignar recursos y privilegios, actuar como servidor web, FTP, servidor de impresión, DNS o resolución de nombres de dominio, servidor DHCP, entre otros servicios básicos. Otra de las funciones que tiene, es como en todo sistema Windows la opción de utilizarlo como una estación de trabajo más de la red. Dicho sistema operativo es muy eficiente y su principal punto fuerte es el Active Directory (Directorio Activo), herramienta desde la cual se puede administrar toda la infraestructura de una organización.

Un servidor es un ordenador que permite compartir sus recursos con otros ordenadores que están conectados a él.

Los servidores pueden ser de varios tipos y entre ellos se encuentran los siguientes:

**Servidor de archivos.** Mantiene los archivos en subdirectorios privados y compartidos para

los usuarios de la red.

**Servidor de impresión.** Tiene conectadas una o más impresoras que comparte con los demás usuarios.

**Servidor de comunicaciones.** Permite enlazar diferentes redes locales o una red local con grandes ordenadores o miniordenadores.

**Servidor de correo electrónico.** Proporciona servicios de correo electrónico para la red.

**Servidor Web.** Proporciona un lugar para guardar y administrar los documentos HTML que pueden ser accesibles por los usuarios de la red a través de los navegadores.

**Servidor FTP.** Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red.

**Servidor proxy.** Se utiliza para monitorizar y controlar el acceso entre las redes. Cambia la dirección IP de los paquetes de los usuarios para ocultar los datos de la red interna a Internet y cuando recibe contestación externa, la devuelve al usuario que la ha solicitado. Su uso reduce la amenaza de piratas que visualicen el tráfico de la red para conseguir información sobre los ordenadores de la red interna.

El sistema operativo de red se encarga de la gestión de los usuarios, de la gestión de la red, de controlar el acceso a los datos de los archivos que se encuentran en las unidades de discos compartidas del servidor, de la utilización de los periféricos compartidos.

Windows Server es un sistema operativo de red que trabaja sobre un modelo denominado dominio que es un conjunto de equipos (clientes y servidores) que comparten una política de seguridad y una base de datos común (Directorio Activo). Cada dominio debe tener un nombre único.

## DNS o Domain Name System

**DNS o Domain Name System** (Sistema de Nombres de dominio): es un sistema de nomenclatura jerárquica para ordenadores, servicios o cualquier recurso que forme parte de una red pública o privada. Que se traduce Sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente

## Directorio Activo.

Es un servicio de red que guarda en una base de datos toda la información sobre los recursos de red y permite el acceso de los usuarios a dichos recursos y determinadas aplicaciones. Directorio Activo separa la estructura lógica de la organización (dominios) de la estructura física (topología de red).

Este servicio de directorio es un servicio de red que almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio de organizar, controlar y administrar centralizadamente el acceso a los recursos de la red.

### Dominio.

Estructura fundamental. Permite agrupar todos los objetos que se administran de forma estructural y jerárquica. Es una agrupación de equipos y usuarios que facilita la administración de los equipos y cuentas de usuarios

### Unidad Organizativa(OU).

Es la unidad jerárquica inferior al dominio y que puede estar compuesta por una serie de objetos y/o por otras UO. Las unidades organizativas son contenedores del Directorio Activo.

### Grupos.

Conjunto de objetos del mismo tipo que se utilizan fundamentalmente para la asignación de los derechos de acceso a los recursos. Normalmente son de usuarios.

### Objetos.

Forman una representación de un recurso de red, como puede ser usuarios, impresoras, ordenadores, unidades de almacenamiento, etc.

**Directorio** Activo utiliza los nombres y servicios DNS para tres funciones principales:

1. **Resolución de nombres:** DNS permite realizar la resolución de nombres al convertir de host (nombre de equipo) a dirección IP.
2. **Definición del espacio de nombres:** el DA utiliza las conversiones de nomenclatura de DNS para asignarles nombre a los dominios.
3. **Búsqueda de los componentes de DA:** para iniciar una sesión de red y utilizar los recursos de DA, el equipo que se conecta al dominio debe encontrar primero un controlador de dominio o **servidor de catálogo global** para procesar la autenticación de inicio de sesión o la consulta.

Algunos términos de los utilizados habitualmente en DA son los siguientes:

1. **Espacio de nombres**. Directorio Activo usa las convenciones de nomenclatura de DNS para asignar nombre a los dominios. Los nombres de dominio pueden o están formados por dos o más palabras separadas por puntos gracias a una estructura jerárquica denominada **espacio de nombres (Name space**).
2. **Resolución de nombres**. Domain Name Server o DNS permite realizar la resolución de nombres al convertir de hosts a direcciones IP y viceversa.
3. **Controlador de dominio.** Servidor con DA instalado En el equipo se almacena, mantiene y gestiona la base de datos de usuarios y recursos de la red. Los controladores de dominio tienen una serie de responsabilidades. Una de ellas es la autentificación. La autentificación es el proceso de garantizar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña. No es que les permita a los usuarios validar para ser partes de clientes.
4. **Nombre de dominio**. Son las denominaciones asignadas a los ordenadores de la red.
5. **Árbol de dominio**. Es el conjunto de dominios formado por el nombre de dominio raíz y el resto de dominios cuyos nombres constituyen un espacio contiguo con el nombre raíz.
6. **Bosque de árboles de dominios**. Es el conjunto de árboles de dominio

## DHCP

Que se traduce Protocolo de configuración dinámica de servidores) es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de sub-red, puerta de enlace, etc.) a partir de un servidor DHCP.

Teniendo en cuenta que la empresa GNC que busca implementar una intranet que consta de 2 o más tambos; la organización consta de una Sede Matriz donde está alojado el Data center principal, que contiene el dominio raíz (**gnc.local**), tendrá una unidad organizativa para los administradores del dominio. Cada tambo será un subdominio y se conectará al dominio raíz por un enlace WAN.

Los subdominios tendrán el siguiente formato **tambo** + (**.**) + **gns.local**, por ejemplo el tambo de Las Novillas el subdominio será **lasnovillas.gnc.local**

En la sede principal se encuentra el servidor de la empresa, el cual es el encargado de proporcionar los principales servicios de red. Dentro de él, estarían contenidas varias unidades organizativas, una por cada tambo. Se crearán unidades organizativas anidadas a las últimas, las anidadas representarán a cada sector de la empresa (Administración, Ti, Planta y Laboratorio)

## SERVICIOS A IMPLEMENTAR

El sistema operativo a implementar en el servidor será Windows server 2008.

### Servidor DHCP Y DNS

Se debe dar dirección de forma automática a través del GNCSERVER a todas las vlan (laboratorio), (planta), (administración), (IT), (Voice ip).

Se reservan el rango de IP para el dominio Raíz de las IP 10.10.0.0 a 10.10.20.254.

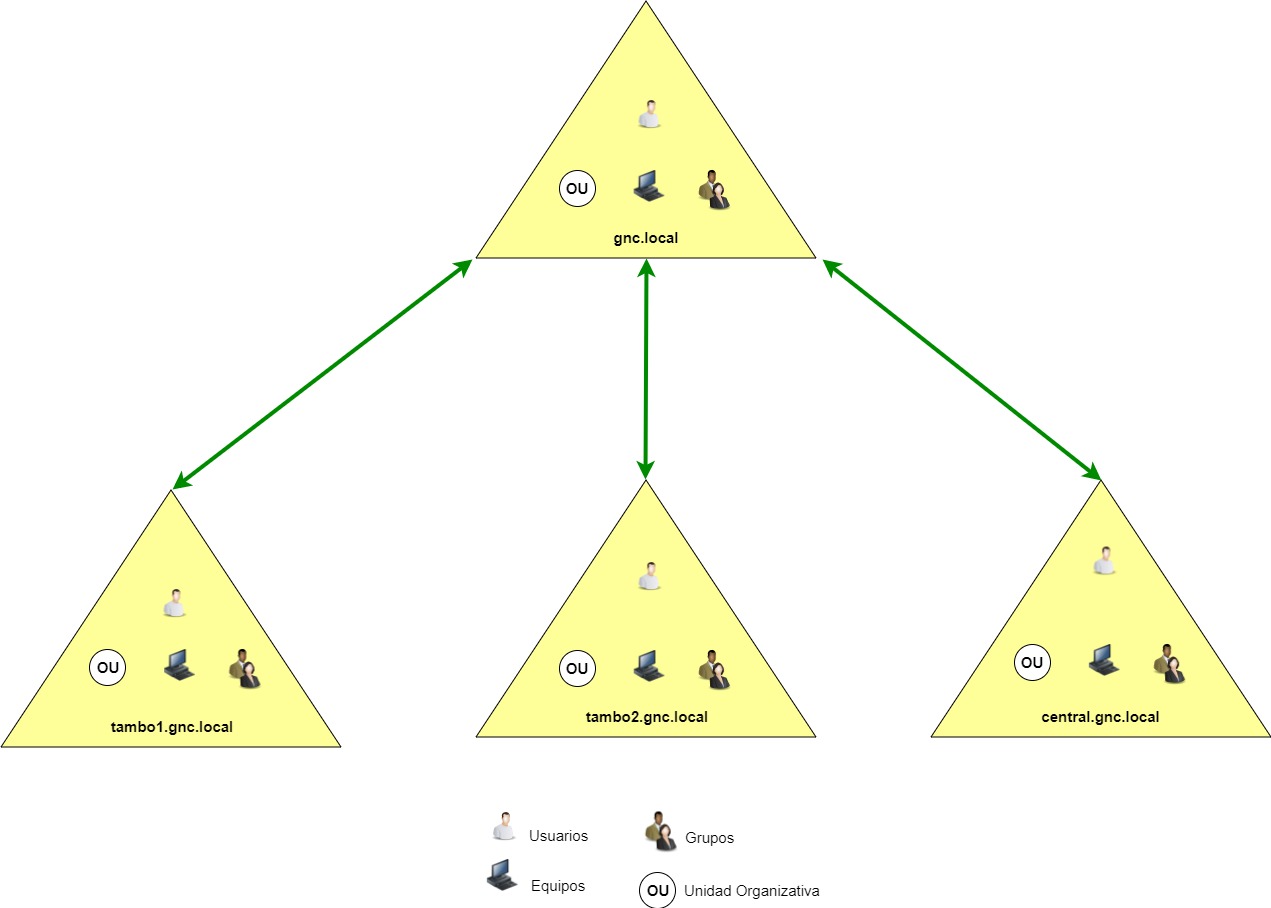
Tambos a Implementar.

Cada tambo tendrá una IP asignada de forma automática por el servidor DHCP.

La estructura física de la organización está compuesta por un tambo principal y varias sucursales.

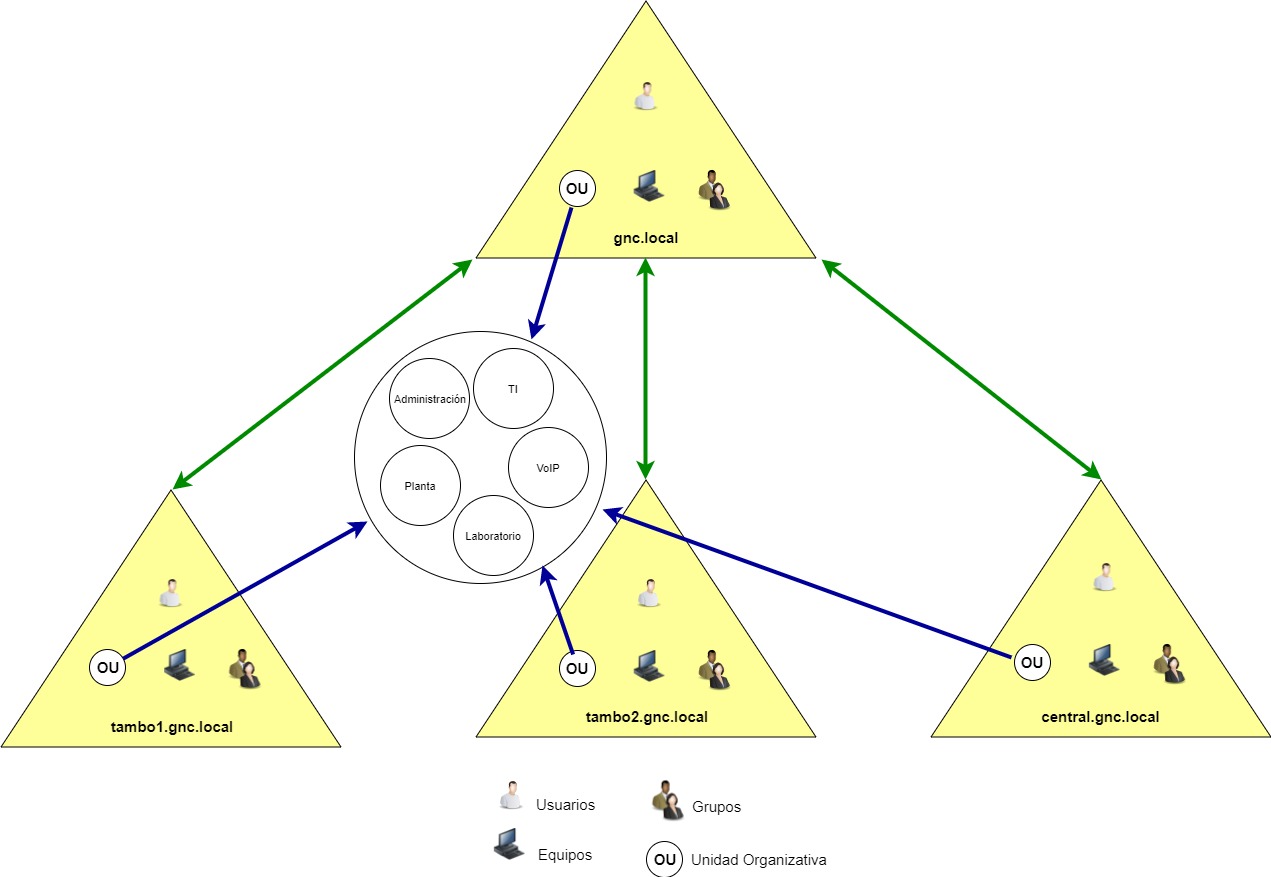
En el tambo principal o sede central están los servidores de la organización (o dominio raíz), además el subdominio **central.gnc.local**.

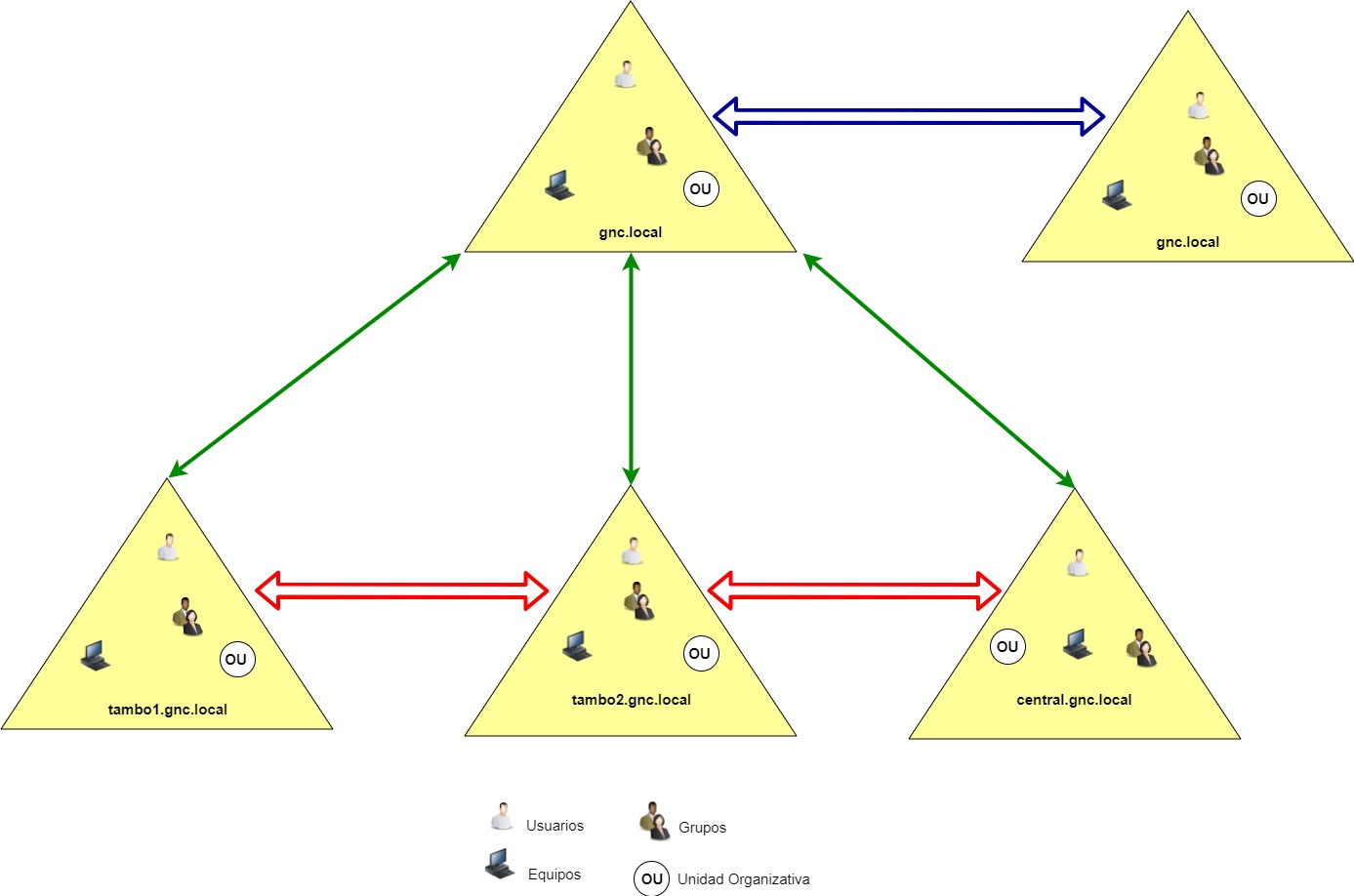
Se implementará un servidor de nombres de dominio, para que los usuarios tengan acceso al servidor a través del dominio gnc.local.



Relación de confianza

Esquema del Dominio gnc.local y sus subdominios





Replicación entre los subdominios

Replicación del dominio principal

DESCRIPCIÓN Y EQUIPOS DE LA RED

### Equipos finales

Esos serán los equipos de los usuarios, estos equipos harán parte de la intranet corporativa, estarán dividas por segmentos a través de vlans y cada vlan tendrá ciertas políticas para el manejo de la información. Los equipos finales quedaran segmentados de la siguiente manera:

Configuraciones del dominio gnc.local

|  |  |
| --- | --- |
| TABLA DE ENRUTAMIENTO | |
| Mascara de Red | 255.255.254.0 = 23 |
| Red | 10.10.0.0/27 |
| Broadcast | 10.10.0.31 |
| HostMin | 10.10.0.1 |
| HostMax | 10.10.22.30 |
| Hosts/Net | 30 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NOMBRE | SERVICIOS | IP | DNS | Puerta de enlace |
| GNCAD | AD DC / DNS | 10.10.0.1 | 10.10.0.1 | 10.10.0.1 |
| GNCWSUS | PARCHEO | 10.10.0.2 | 10.10.0.1 | 10.10.0.1 |

Ejemplo de asignación de IP por DHCP para el tambo **central** ubicada en San José.

central.gnc.local

|  |  |
| --- | --- |
| TABLA DE ENRUTAMIENTO | |
| Mascara de Red | 255.255.254.0 = 23 |
| Red | 10.10.21.0/23 |
| Broadcast | 10.10.21.255 |
| HostMin | 10.10.21.1 |
| HostMax | 10.10.22.254 |
| Hosts/Net | 510 |

Rangos de direcciones de IP para los equipos de comunicación y servidores.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Red | Mascara | Puerta de enlace | Broadcast |
| Servidores | 10.10.21.0/26 | 255.255.255.192 | 10.10.21.1 | 10.10.21.63 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NOMBRE | SERVICIOS | IP | DNS | Puerta de enlace |
| CENTRALAD | AD DC / DNS | 10.10.21.2 | 10.10.21.2 | 10.10.21.1 |
| CENTALFS | FILE SERVER / PRINTER SERVER | 10.10.21.3 | 10.10.21.2 | 10.10.21.2 |
| CENTALBD | BASE DE DATOS | 10.10.21.4 | 10.10.21.2 | 10.10.21.2 |
| CENTRALAPP | APLICACIONES | 10.10.21.5 | 10.10.21.2 | 10.10.21.2 |
| CENTRALWSUS | PARCHEO | 10.10.21.6 | 10.10.21.2 | 10.10.21.2 |

Rangos de direcciones de IP para los equipos finales y dispositivos a través de Vlans.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Red Vlan | Vlan | Host | Red | Mascara | Puerta de enlace | Broadcast |
| IT | 10 | 60 | 10.10.21.64/26 | 255.255.255.192 | 10.10.21.64 | 10.10.21.127 |
| laboratorio | 20 | 60 | 10.10.21.128/26 | 255.255.255.192 | 10.10.21.128 | 10.10.21.191 |
| administración | 30 | 60 | 10.10.21.192/26 | 255.255.255.192 | 10.10.21.192 | 10.10.21.192 |
| planta | 40 | 120 | 10.10.22.1/25 | 255.255.255.128 | 10.10.22.1 | 10.10.22.127 |
| Voice ip | 50 | 60 | 10.10.22.128/26 | 255.255.255.192 | 10.10.22.128 | 10.10.22.191 |

Tambo1.gnc.local

|  |  |
| --- | --- |
| Red Vlan | Vlan |
| Mascara de Red | 255.255.254.0 = 23 |
| Red | 10.10.23.0/23 |
| Broadcast | 10.10.24.255 |
| HostMin | 10.10.23.1 |
| HostMax | 10.10.24.254 |
| Hosts/Net | 510 |

Rangos de direcciones de IP para los equipos de comunicación y servidores.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Red | Mascara | Puerta de enlace | Broadcast |
| Servidores | 10.10.23.0/26 | 255.255.255.192 | 10.10.23.1 | 10.10.23.63 |

Rangos de direcciones de IP para los equipos finales y dispositivos a través de Vlans.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Red Vlan | Vlan | Host | Red | Mascara | Puerta de enlace | Broadcast |
| IT | 10 | 60 | 10.10.23.64/26 | 255.255.255.192 | 10.10.23.64 | 10.10.23.127 |
| laboratorio | 20 | 60 | 10.10.23.128/26 | 255.255.255.192 | 10.10.23.128 | 10.10.23.191 |
| administración | 30 | 60 | 10.10.23.192/26 | 255.255.255.192 | 10.10.23.192 | 10.10.23.191 |
| planta | 40 | 120 | 10.10.24.1/25 | 255.255.255.128 | 10.10.24.1 | 10.10.24.127 |
| Voice ip | 50 | 60 | 10.10.24.128/26 | 255.255.255.192 | 10.10.24.128 | 10.10.24.191 |
| planta | 50 | 120 | 10.10.24.64 | 255.255.255.128 | 10.10.24.64 | 10.10.24.128 |

### Servidor de archivos (FILE SERVER)

Un servidor de archivos es un equipo responsable del almacenamiento y administración central de archivos de datos para que otros equipos de la misma red puedan acceder a los archivos, permite a los usuarios compartir información a través de una red sin tener que transferir físicamente archivos por dispositivo de almacenamiento externo.

Se crearán unidades de red para cada equipo, con un espacio de almacenamiento determinada según

las necesidades que se requieran.

Aquí también se almacenará la base de datos del Active Directory

#### Función de servidor de archivos:

* proporciona una ubicación central en la red
* almacenar y compartir los archivos con usuarios de la red
* archivos y aplicaciones accesibles a través de la red

### Servidor de IMPSRESIÓN (PRINT SERVER)

* administración de impresión

### conectar impresora a red

### imprimir trabajos desde cualquier equipo

### impresión en internet

## Zona DMZ: la zona segura de la red

### ¿Qué es una DMZ?

Una **red DMZ** “Zona desmilitarizada” o “franja de terreno neutral”) corresponde a una red segura y aislada del resto.

Es una red que está aislada del resto de redes de la empresa (incluyendo la red interna) y en la que se controla cualquier tráfico que se establezca con el resto. Es un terreno neutral que separa los recursos de varias redes. El acceso a esta red es restringido y limitado exclusivamente a los servicios a los que los usuarios pueden acceder.

Es decir, colocamos en una red independiente los equipos que prestan un servicio y que deben ser accesibles desde Internet. De modo que aun estando dentro de la empresa, no están en la misma red que los usuarios. si uno de los equipos se ve comprometido, no afectará a la seguridad del resto de la compañía.

Dentro de la ***zona desmilitarizada*** incluimos todos aquellos servicios, máquinas, dispositivos etc, que consideremos críticos para nuestro negocio y que debamos tener bajo un especial control.

Debemos incluir servidores de DNS, servidores de correo electrónico, servidor web, servidores de base de datos.

#### ****DMZ con un firewall****

Para implementar una zona desmilitarizada utilizaremos un único cortafuego de gran alcance con terminales para tres conexiones de red separadas: una para Intranet, otra para Internet y otra para la DMZ.

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Una zona DMZ se conoce como una zona desmilitarizada, es decir, una zona segura que no está dentro de nuestra red local, pero que tampoco es externa a nuestra empresa. Por lo tanto, se plantea como un paso intermedio entre nuestra red y el acceso a Internet, que si protegemos por un Firewall debidamente dejaremos como una zona segura dentro de nuestra empresa.

La política de seguridad aplicada en la DMZ, normalmente es la siguiente:

* Tráfico de la red externa hacia la DMZ autorizada.
* Tráfico de la red externa hacia la red interna prohibida.
* Tráfico de la red interna hacia la DMZ autorizada.
* Tráfico de la red interna hacia la red externa autorizada.
* Tráfico de la DMZ hacia la red interna prohibida.
* Tráfico de la DMZ hacia la red externa rechazada.

Flujo de Trafico

|  |  |  |  |
| --- | --- | --- | --- |
| Origen | Destino | Acceso | Puertos |
| WAN | DMZ | Permitido | (DNS)TCP/UDP port 53  (VPN)UDP port 4500, 500 -IP port 51  (HTTP) TCP port 443  (HTTPS) port 80  DHCP UDP port 67  (S Archivos)SMB TCP/UDP port 445 |
| LAN | DMZ | Permitido | (DNS) TCP/UDP port 53  (Oracle) port 8080  (S Archivos)SMB TCP/UDP port 445  (Radius) UDP 1812 |
| DMZ | LAN | Permitido | (DNS) TCP/UDP port 53  DHCP UDP port 68 |
| DMZ | WAN | Permitido | (DNS) TCP/UDP port 53  DHCP UDP port 68 |
| DMZ | Internet | Rechazada |  |
| DMZ | LAN | Rechazada |  |
| WAN | LAN | Rechazada |  |

## Virtualización

tecnología que permite crear múltiples entornos simulados o recursos dedicados desde un solo sistema de hardware físico, mediante el software llamado "hipervisor" conecta el hardware y permite dividir un sistema en entornos separados, distintos y seguros (máquinas virtuales" (VM)).

Con la virtualización logramos:

* Reducción de costos por consumo de energía eléctrica.
* Menos equipos para la refrigeración de los datacenter.
* Reducción de espacios para el datacenter.
* Menor costo de actualización de los servidores.
* Reducción de costos de hardware, espacio físico y mano de obra.
* Rápida incorporación de nuevos recursos para los servidores virtualizados.

Desventajas

* Necesidad de mayor cantidad de recursos hardware (memoria RAM, procesadores y disco).
* Se pueden presentar problemas con los administradores de virtualización.
* Problemas de compatibilidad con los dispositivos Hardware virtualizados.

### Falla en Servicios

Para el servicio de resolución de nombres AD DC / DNS se cuenta con los siguientes servidores:

La estructura de los servidores es la siguiente:

Dominio raíz está formado por el GNCAD que provee los servicios Active Directory y DNS de toda la organización.

Cada tambo tendrá servidores de AD DC / DNS, FILE SERVER / PRINTER SERVER, BASE DE DATOS, APLICACIONES, EMAIL y WSUS. Estos se ejecutarán sobre un servidores:

* System x3550 M5 Rack Server con procesadores Intel® Xeon® E5-2600 v3 Series
* System x3650 M5 Rack Server con procesadores Intel® Xeon® E5-2600 v3

|  |  |  |  |
| --- | --- | --- | --- |
| SERVIDOR |  | DIRECCION IP | TIPO |
| GNCAD y DNS | Primario | 10.10.0.1 | Virtual |
| Aplicaciones | Primario | 10.10.0.15 | Virtual |
| Archivos | Primario | 10.10.0.2 | Virtual |
| Base de datos | Primario | 10.10.0.3 | Virtual |
| WSUS | Primario | 10.10.0.4 | Virtual |

Cada uno con su contingencia:

Los servidores de contingencia estarán ubicados en Montevideo en el Datacenter de Antel.

|  |  |  |  |
| --- | --- | --- | --- |
| SERVIDOR |  | DIRECCION IP | TIPO |
| GNCAD2 | Secundario | 10.10.0.1 | Virtual |
| Aplicaciones2 | Secundario | 10.10.0.15 | Virtual |
| Archivos2 | Secundario | 10.10.0.2 | Virtual |
| Base de datos2 | Secundario | 10.10.03 | Virtual |
| WSUS | Secundario | 10.10.0.4 |  |

Con ésta configuración en caso de falla del servidor Primario GNCAD resuelve el secundario GNCADII. En caso de falla de los dos servidores se activan sus contingencias virtuales.

#### SERVIDORES POR TAMBOS.

Configuración de los servidores primarios

|  |  |  |  |
| --- | --- | --- | --- |
| NOMBRE | SERVICIOS | IP | TIPO |
| CENTRALAD | AD DC / DNS | 10.10.21.2 | VIRTUAL |
| CENTALFS | FILE SERVER / PRINTER SERVER | 10.10.21.3 | VIRTUAL |
| CENTALBD | BASE DE DATOS | 10.10.21.4 | VIRTUAL |
| CENTRALAPP | APLICACIONES | 10.10.21.5 | VIRTUAL |
| CENTRALEMAIL | EMAIL | 10.10.21.6 | VIRTUAL |
| CENTRALWU | WSUS | 10.10.21.7 | VIRTUAL |

Configuración de los servidores secundarios, este se encuentra en el Datacenter de Antel

|  |  |  |  |
| --- | --- | --- | --- |
| NOMBRE | SERVICIOS | IP | TIPO |
| CENTRALAD | AD DC / DNS | 10.10.21.12 | VIRTUAL |
| CENTALFS | FILE SERVER / PRINTER SERVER | 10.10.21.13 | VIRTUAL |
| CENTALBD | BASE DE DATOS | 10.10.21.14 | VIRTUAL |
| CENTRALAPP | APLICACIONES | 10.10.21.15 | VIRTUAL |
| CENTRALEMAIL | EMAIL | 10.10.21.16 | VIRTUAL |
| CENTRALWU | WSUS | 10.10.21.17 | VIRTUAL |

## ¿Qué es el Análisis FODA?

El **análisis FODA** es una herramienta de planificación estratégica muy utilizada por las empresas, consiste en realizar un análisis interno, revisando las fortalezas y debilidades y un análisis externo, revisando las oportunidades y amenazas de la empresa.

La **palabra FODA**, está creada a partir de las letras iniciales de los términos que hemos mencionado:

* Fortalezas
* Oportunidades
* Debilidades
* Amenazas

Fortalezas: debemos añadir los atributos o puntos positivos que nos pueden servir para alcanzar nuestros objetivos.

Oportunidades: aquí debemos tener en cuenta las condiciones externas, revisando la industria y otros factores como las regulaciones que pueden afectar de forma positiva a nuestro objetivo.

Debilidades: en esté cuadrante debemos de añadir lo que es perjudicial o los factores que pueden ser desfavorables para nuestro objetivo.

Amenazas: añadiremos lo perjudicial, todo lo que puede amenazar nuestra supervivencia y la potencial ganancia de resultados de forma externa.

Para desarrollar el análisis, debemos crear 4 listas:

* Crear una lista de fortalezas actuales
* Crear una lista de debilidades actuales
* Crear una lista de oportunidades para el futuro
* Crear una lista con las amenazas para el futuro

Las listas deben tener información real y con puntos especificados de forma sencilla y fácil de entender. Una vez tenemos todas las listas, debemos de evaluar los resultados que hemos obtenido y definir las estrategias a corto y largo plazo.