# 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](#_Toc529825612)

[TERNERAS DE TAMBO 1](#_Toc529825613)

[GNC 1](#_Toc529825614)

[Gestión de Nacimiento y Cría 1](#_Toc529825615)

[WINDOWS SERVER: 3](#_Toc529825616)

[DNS o Domain Name System 4](#_Toc529825617)

[Directorio Activo. 5](#_Toc529825618)

[Dominio. 5](#_Toc529825619)

[Unidad Organizativa(OU). 5](#_Toc529825620)

[Grupos. 5](#_Toc529825621)

[Objetos. 5](#_Toc529825622)

[DHCP 6](#_Toc529825623)

[SERVICIOS A IMPLEMENTAR 6](#_Toc529825624)

[Servidor DHCP 6](#_Toc529825625)

[Servidor DNS 6](#_Toc529825626)

[Equipos finales 9](#_Toc529825627)

[DEFINICIÓN DE CONTRASEÑA 10](#_Toc529825628)

[¿Cómo me protejo? 11](#_Toc529825629)

[Creación de contraseñas robustas 11](#_Toc529825630)

[¿Con qué frecuencia debemos cambiar las contraseñas? 11](#_Toc529825631)

[Servidor de archivos (FILE SERVER) 12](#_Toc529825632)

[Función de servidor de archivos: 12](#_Toc529825633)

[Servidor de IMPSRESIÓN (PRINT SERVER) 12](#_Toc529825634)

[DISEÑO DE LA SEGURIDAD FISICA 12](#_Toc529825635)

[AREAS SEGURAS 12](#_Toc529825636)

[Perímetro Físico 13](#_Toc529825637)

[Controles de acceso físico 13](#_Toc529825638)

[Protección de oficinas 13](#_Toc529825639)

[SEGURIDAD DE LOS EQUIPOS 13](#_Toc529825640)

[Ubicación y protección de los equipos 13](#_Toc529825641)

[Suministros de Energía 14](#_Toc529825642)

[Seguridad del Cableado 14](#_Toc529825643)

[Mantenimiento de Equipos 14](#_Toc529825644)

[Baja o reutilización de equipos 14](#_Toc529825645)

[DISEÑO DE LA SEGURIDAD LOGICA 14](#_Toc529825646)

[DISEÑO DE LA RED 14](#_Toc529825647)

[Computadores móviles 14](#_Toc529825648)

[Trabajo remoto 14](#_Toc529825649)

[Políticas de seguridad del hardware 15](#_Toc529825650)

[Seguridad física del equipo 15](#_Toc529825651)

[Mantenimiento de equipos 15](#_Toc529825652)

[Políticas de seguridad del software 15](#_Toc529825653)

[Políticas de seguridad para el control de acceso a los sistemas de información 15](#_Toc529825654)

[Acceso Físico 15](#_Toc529825655)

[Acceso a la información (archivos y documentos) 15](#_Toc529825656)

[Respaldos y Recuperación de archivos, aplicaciones y bases de datos 15](#_Toc529825657)

[Acceso a los servicios de red 16](#_Toc529825658)

[Administración de usuarios 16](#_Toc529825659)

[Correo electrónico e Internet 16](#_Toc529825660)

[Políticas de seguridad para contingencia 16](#_Toc529825661)

[Concepto Seguridad Informática 16](#_Toc529825662)

[Amenazas Informáticas 16](#_Toc529825663)

[Ataques internos 17](#_Toc529825664)

[Ataques externos 17](#_Toc529825665)

[SEGURIDAD PERIMETRAL 17](#_Toc529825666)

[Zona DMZ: la zona segura de la red 19](#_Toc529825667)

[¿Qué es una DMZ? 19](#_Toc529825668)

[POR QUÉ ES NECESARIO VIRTUALIZAR. 20](#_Toc529825669)

[Escenarios de virtualización 21](#_Toc529825670)

[Falla en Servicios 24](#_Toc529825671)

[¿Qué es el Análisis FODA? 26](#_Toc529825672)

## 

## 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.

Los servidores dentro de un dominio pueden tomar uno de los papeles siguientes:

**Controladores de dominio**. Pertenecen al dominio y contienen una copia de las cuentas de usuario y de otros datos del Directorio Activo. Es obligatorio que haya, al menos, un controlador de dominio.

**Servidores miembro.** Pertenecen al dominio y no contienen una copia de las cuentas de usuario y de otros datos del Directorio Activo. Se utilizan para almacenar los archivos y otros recursos de red.

Los servicios más habituales que proporciona este tipo de sistema operativo para la gestión de la red son los siguientes:

**Seguridad.** Al igual que los sistemas operativos de red más importantes, Windows Server proporciona seguridad para cualquier recurso de la red.

El servidor de red Windows mantiene todos los registros de las cuentas de usuario y gestiona los permisos y derechos de usuario. Para acceder a cualquier recurso de la red, el usuario deberá tener los derechos necesarios para realizar la tarea y los permisos adecuados para utilizar el recurso.

**Servicios de compartición de recursos.** Este servicio es con el que se pone a disposición de los usuarios de la red los archivos, carpetas, impresoras o cualquier otro recurso, de forma centralizada y con un nivel de seguridad determinando y decidido por el administrador de la red.

**Servicios de impresión**. En una red con Windows Server, cualquier servidor o cliente puede funcionar como servidor de impresión. La diferencia es que, si el servicio de impresión está montado en un cliente, el administrador de la red no tendrá control total sobre el mismo. Lo normal es instalar estos servicios en el servidor y gestionarlos desde

dicho equipo.

**Servicios de red.** Windows Server proporciona diferentes servicios de red que ayudan a la gestión global de un entorno de red.

## 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.

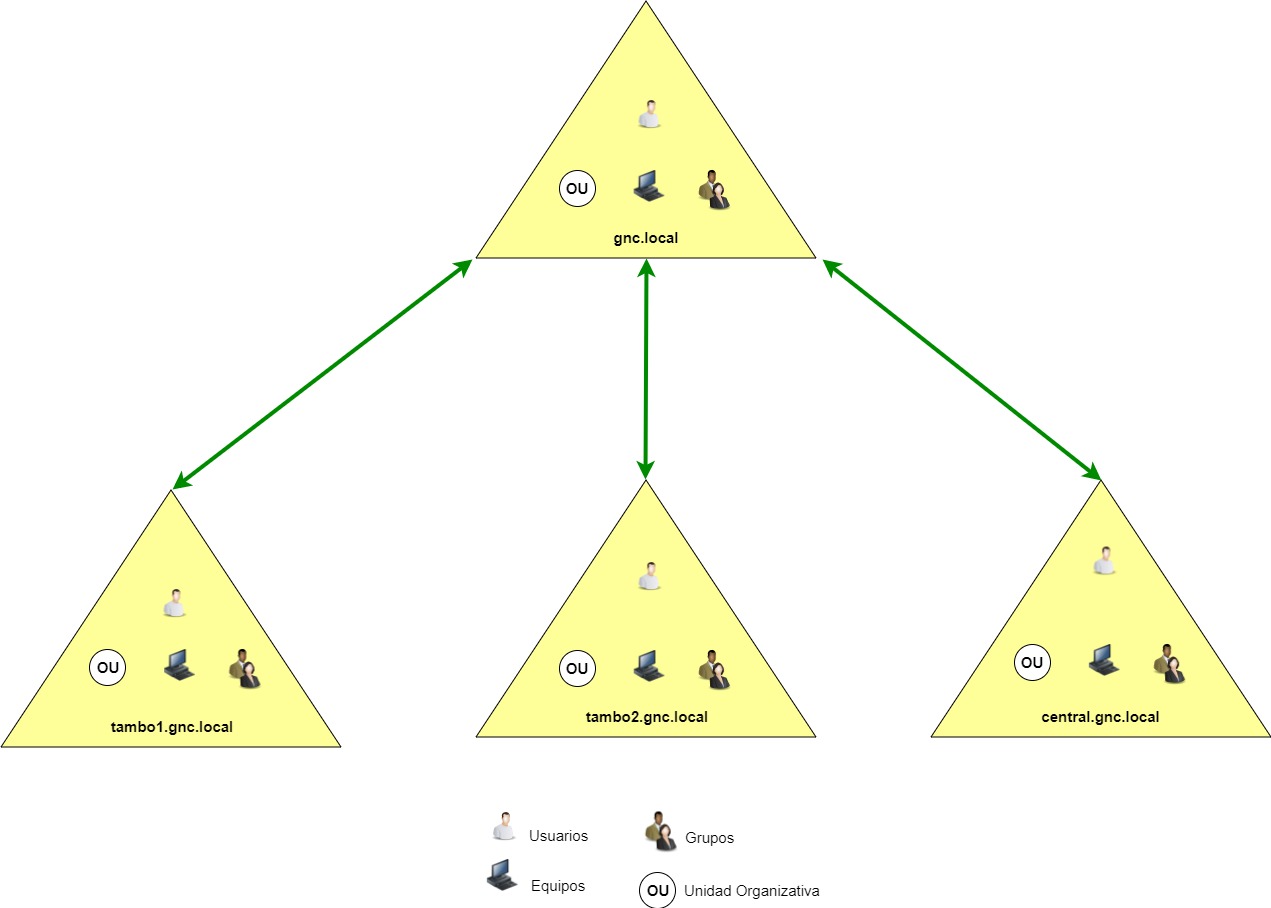
Tambos a Implementar.

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.

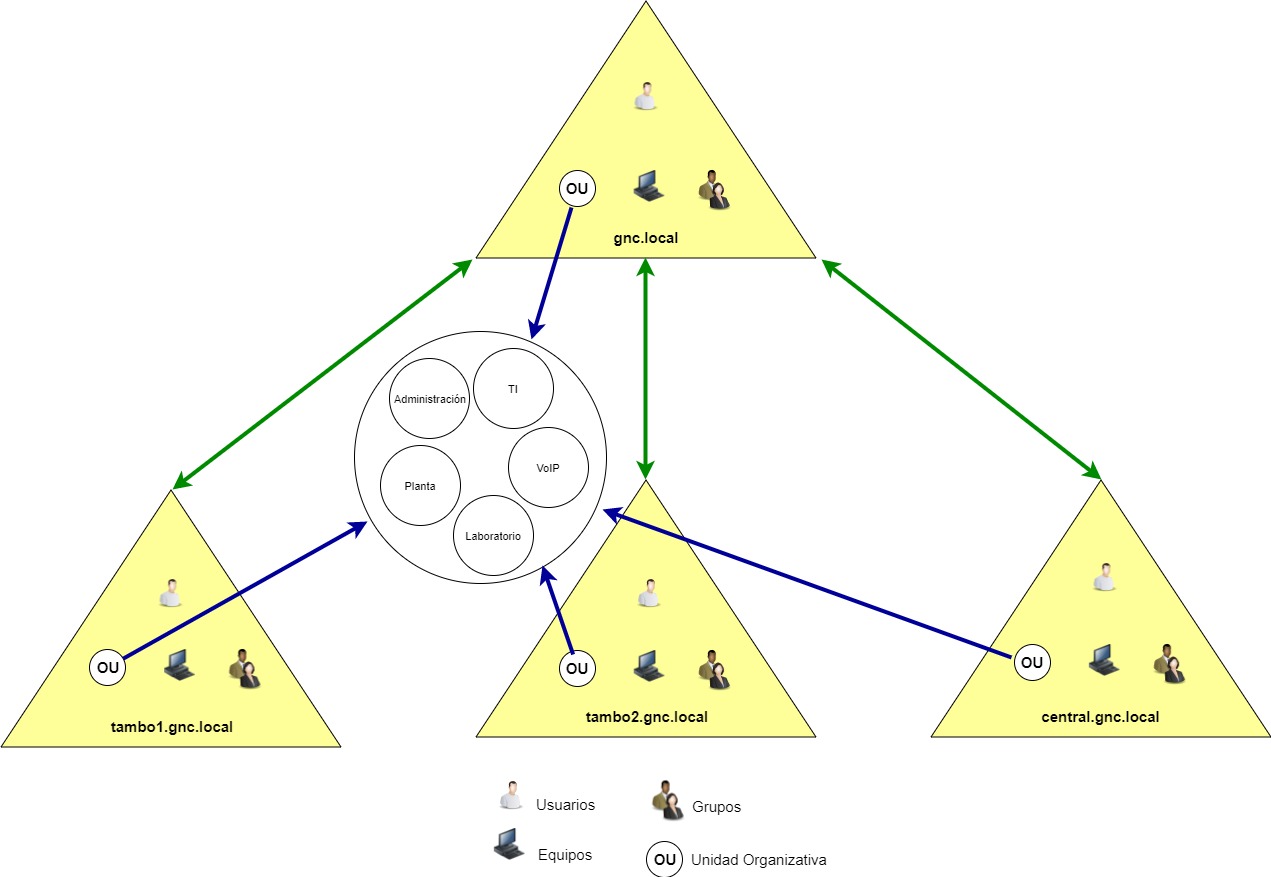
En el tambo principal o sede central están los servidores de la organización (o dominio raíz), además el subdominio **central.gnc.local**.

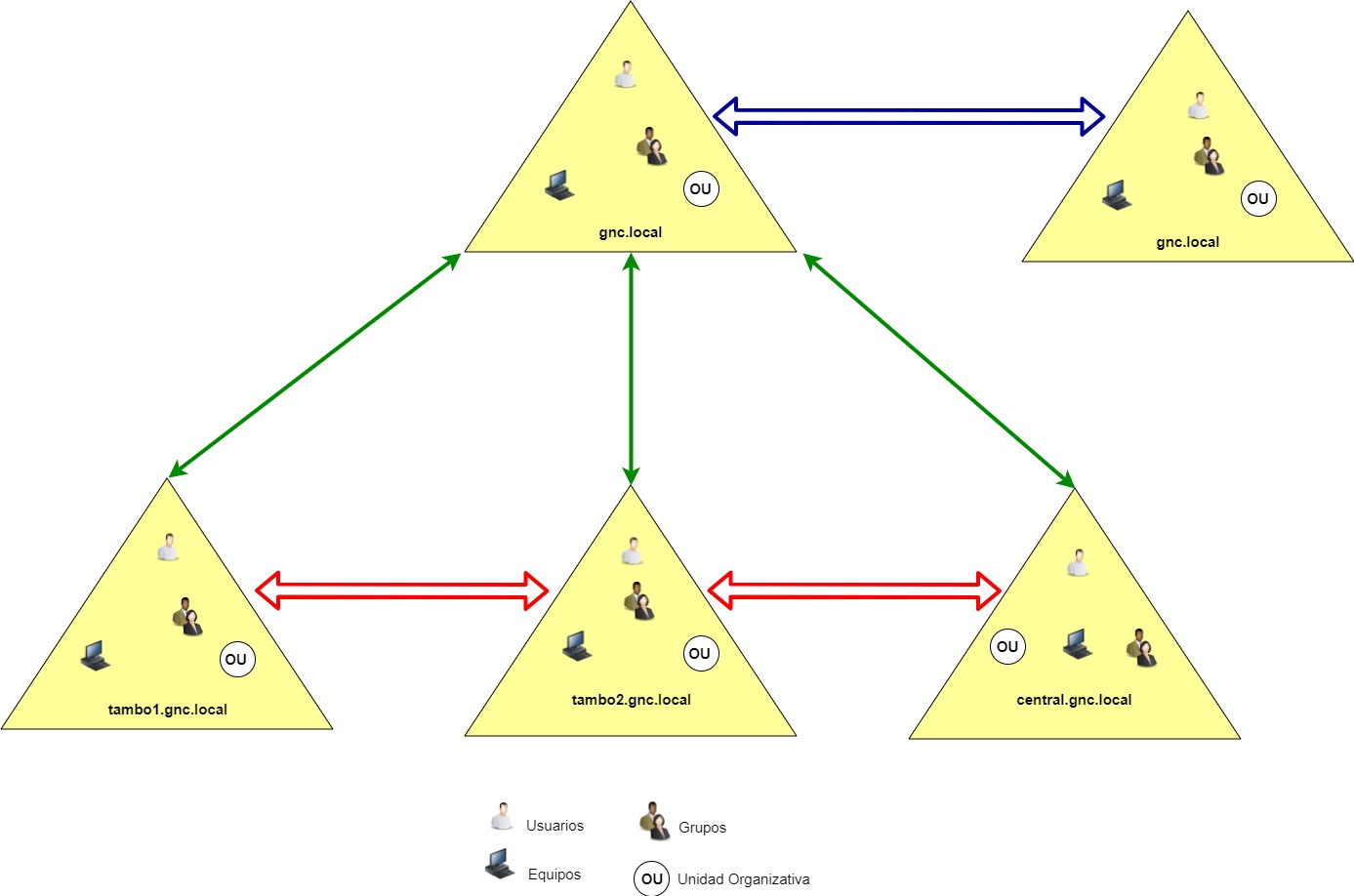
Se implementará un servidor de nombres de dominio, para que los usuarios tengan acceso al servidor a través del dominio gnc.local.



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  GNCWSUS | AD DC / DNS  PARCHEO | 10.10.0.1  10.10.0.2 | 10.10.0.1  10.10.0.1 | 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 |
| Voice ip | 40 | 60 | 10.10.22.1/26 | 255.255.255.192 | 10.10.22.1 | 10.10.22.63 |
| planta | 50 | 120 | 10.10.22.64 | 255.255.255.128 | 10.10.22.64 | 10.10.22.124 |

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 | 10.10.23.192 |
| Voice ip | 40 | 60 | 10.10.24.1/26 | 255.255.255.192 | 10.10.24.1 | 10.10.24.63 |
| planta | 50 | 120 | 10.10.24.64 | 255.255.255.128 | 10.10.24.64 | 10.10.24.128 |

### [DEFINICIÓN DE CONTRASEÑA](https://definicion.de/contrasena/)

Una contraseña es una [clave](https://definicion.de/clave/) que brinda acceso a algo que, sin dicho código, resulta inaccesible. Se trata de un método de autentificación que apela a los datos secretos necesarios para superar una barrera de seguridad. La contraseña es una información secreta que se nos solicita para acceder a algún tipo de recurso, y que solo debe conocer el propietario del mismo.

Es necesario invertir un poco de tiempo y esfuerzo en generar una contraseña segura. Si un usuario malintencionado consiguiera apoderarse de una contraseña podría acceder a información personal, violando la privacidad, o incluso tener acceso a servicios financieros.

### ¿Cómo me protejo?

La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.

Construir las contraseñas con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &).

Usar contraseñas diferenciadas en función del uso (por ejemplo no debe usarse la misma para una cuenta de correo que la usada para acceso a servicios bancarios).

Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.

Se deben cambiar las contraseñas regularmente. (Dependiendo de la criticidad de los datos puede ser cada X meses).

Se debe evitar:

* La contraseña no debe contener el nombre de usuario de la cuenta, o cualquier otra información personal fácil de averiguar (cumpleaños, nombres de hijos, cónyuges, etc). Tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)
* No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea.
* Se deben evitar contraseñas que contengan palabras existentes en algún idioma (por ejemplo “campo”). Uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en un diccionario y/o palabras de uso común.
* No se deben almacenar las contraseñas en un lugar público y al alcance de los demás (encima de la mesa escrita en papel, etc…).
* No compartir las contraseñas en Internet (por correo electrónico) ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que le soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se tratará de un fraude. La Universidad de Almería nunca le va a solicitar ese tipo de información.
* No utilizar la opción de “Guardar contraseña” que en ocasiones se ofrece, para evitar reintroducirla en cada conexión.

### Creación de contraseñas robustas

Cuando se cree una contraseña segura, es una buena idea seguir las siguientes pautas:

No haga lo siguiente:

*No utilice solamente palabras o números* — Nunca debería utilizar únicamente letras o sólo números en una contraseña.

*No utilice palabras reconocibles* — Palabras tales como nombres propios, palabras del diccionario o hasta términos de shows de televisión o novelas deberían ser evitados, aún si estos son terminados con números.

*No utilice palabras en idiomas extranjeros* — Los programas de descifrado de contraseñas a menudo verifican contra listas de palabras que abarcan diccionarios de muchos idiomas. No es seguro confiarse en un idioma extranjero para asegurar una contraseña.

*No utilice información personal* —Si un atacante conoce quién es usted, la tarea de deducir su contraseña será aún más fácil.

*No invierta palabras reconocibles* — Los buenos verificadores de contraseñas siempre invierten las palabras comunes, por tanto, invertir una mala contraseña no la hace para nada más segura.

### ****¿Con qué frecuencia debemos cambiar las contraseñas?****

No cabe ninguna duda que debemos cambiar las contraseñas regularmente, buscando evitar períodos muy largos de uso de las mismas. Una buena sugerencia es**cambiar las contraseñas cada dos o tres meses.**

### Servidor de archivos (FILE SERVER)

En el modelo cliente/servidor, 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.

Un servidor de archivos permite a los usuarios compartir información a través de una red sin tener que transferir físicamente archivos por disquete o algún otro dispositivo de almacenamiento externo.

Se crearan 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:

Un servidor de archivos proporciona una ubicación central en la red, en la que puede almacenar y compartir los archivos con usuarios de la red. Cuando los usuarios necesiten un archivo importante, como un plan de proyecto, podrán tener acceso al archivo del servidor de archivos en lugar de tener que pasarlo entre distintos equipos. Si los usuarios de la red necesitan tener acceso a los mismos archivos y aplicaciones accesibles a través de la red, configure este equipo como un servidor de archivos.

### Servidor de IMPSRESIÓN (PRINT SERVER)

El rol de servidor de impresión sirve para crear un servidor de impresión de Windows e incluye el complemento de consola de administración de impresión, que es útil para administrar varias impresoras o servidores de impresión, así como para migrar impresoras a y desde otros servidores de impresión de Windows.

Servicios de impresión y documentos permite centralizar las tareas de las impresoras de red y los servidores de impresión.

Windows permite compartir impresoras en una red, además de centralizar la administración del servidor de impresión y de las impresoras de red.  
  
El rol de Servicios de Impresión incluye servidor de impresión, servidor LDP e impresión en internet, una vez instalado podemos acceder al administrador de impresión que nos proporcionará detalles sobre el estado de las impresoras y los servidores de impresión de la red y supervisar colas de impresión, además de faciltar la búsqueda de las impresoras que tengan errores mediante filtros y la posibilidad de enviar notificaciones por correo o ejecutar scripts cuando una impresora o servidor de impresión precisen su atención.  
  
**Impresión en Internet**

Con el servicio Impresión de Internet se crea un sitio web en el que los usuarios pueden administrar los trabajos de impresión de un servidor de impresión. También permite que los usuarios que tienen instalado el Cliente de impresión en Internet usen un explorador web para conectarse a las impresoras compartidas y realicen impresiones en ellas usando el Protocolo de impresión en Internet (IPP).

Servicio LPD

El servicio Line Printer Daemon permite que los equipos basados en UNIX u otros equipos que usan el servicio Line Printer Remote (LPR) puedan imprimir en las impresoras compartidas de un servidor de impresión de Windows.

## DISEÑO DE LA SEGURIDAD FISICA

Para realizar el diseño de seguridad se debe considerar la estructura Física como Lógica.

Los objetivos de la seguridad física:

* Proteger los activos del T.I de los riesgos de desastres naturales y/o actos accidentales o mal intencionados.
* Minimizar la pérdida de información y garantizar la recuperación de la misma.
* Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.

## AREAS SEGURAS

Objetivo Principal: Proteger físicamente contra el acceso no autorizado o daño a la información de los sistemas a todos los departamentos, especialmente donde se procesan datos sensibles.

### Perímetro Físico

El área de los servidores debe ser cerrada desde el piso real hasta el techo real contando con una ventilación adecuada y sus respectivas instalaciones eléctricas, donde el acceso solo será para las personas autorizadas tales como administradores de las aplicaciones, bases de datos y red.

El departamento de Tecnologías de la Información deberá crear normas a seguir para acceder y modificar al hardware. Cada empleado será responsable de sus computadores personales y no se

permitirá que personas no autorizadas a los sistemas de información tengan acceso a los computadores sin autorización. Cualquier modificación del hardware será registrada previo a la comprobación de fallo o problemas de funcionamiento con el hardware por parte del departamento de TI.

El acceso a los diferentes departamentos deberá ser controlado en primera instancia por la guardia de seguridad y segundo por la secretaria de cada departamento en horas laborables; en horas no laborables no ingresará ninguna persona no autorizada a los departamentos.

### Controles de acceso físico

El área de información debe estar ubicada al ingreso del edificio, de tal manera que todos los usuarios que requieran información para algún trámite la obtenga en esta área y así evitar que pasen a otro departamento si no es necesario.

Toda persona externa que ingrese a la institución por motivos específicos y/o autorizados deberá registrar su información en un documento: nombre, hora de ingreso, departamento al que se dirige y además el guardia deberá retener algún documento de identidad.

La información sensible como: respaldos de datos y códigos fuentes de los sistemas de información será almacenada en un lugar de condiciones ambientales adecuadas, lejos de canalizaciones de agua y energía, se utilizarán archivadores ignífugos (resistente al calor y al fuego) y su acceso solo será permitido por las personas autorizadas en este caso al departamento de sistemas y alguna autoridad de la Institución.

### Protección de oficinas

Cada departamento deberá contar con un acceso principal con cerradura, el responsable del cuidado del edificio cerrará cada acceso principal con llave luego de que todo el personal del área se haya retirado, además, deberá revisar las ventanas que se encuentren también cerradas.

Se debe instalar un sistema de detección de intrusos en todas las puertas y ventanas accesibles y que será activado después de cerrar los departamentos.

Las áreas donde se procesan datos y el departamento de TI, no deben ser accesibles al público todo el tiempo; deberá definirse un horario para la atención al cliente en el caso de Registro de Títulos; el ingreso de llamadas telefónicas también deberá restringirse a un determinado horario.

El área donde se almacena la información sensible, deberá estar ubicado en un lugar que no esté expuesto al acceso público.

Cada departamento debe tener un extintor de CO2 o espuma para que el personal pueda sofocar cualquier pequeño incendio si existiere.

Dado a que el hardware de cada usuario esta desprotegido por estar en los puestos de trabajo, el departamento de Tecnologías de la Información deberá organizar a los sistemas para que los usuarios finales puedan acceder a su información a través de la red local y trabajar directamente en los servidores de ficheros y servidores de aplicaciones y así mantener a los datos importantes de la Institución a salvo de errores o manipulaciones del hardware.

## SEGURIDAD DE LOS EQUIPOS

Objetivo Principal: Proteger físicamente a los equipos para reducir toda clase de daño, pérdida o acceso no autorizado a los datos y que ocasionen la interrupción a las actividades de la Institución

### Ubicación y protección de los equipos

En cada departamento los equipos deberán ser ubicados en lugares que no sean afectados por la lluvia, polvo o por robo.

Se prohibirá comer, beber o fumar cerca de las instalaciones de los equipos de procesamiento de información.

Se deberá realizar por los menos cuatro veces al año un monitoreo de las condiciones ambientales en los departamentos especialmente en los de procesamiento de datos para prevenir cualquier problema en los equipos.

### Suministros de Energía

El área de los servidores debe contar con un UPS para asegurar el trabajo continuo hasta que el generador de energía sea activado.

El edificio contará con una puesta a tierra para proteger de rayos a los equipos.

Los interruptores de energía deben ser colocados en lugares fuera del alcance de personas externas para que no se ocasionen alguna interrupción de energía al edificio.

### Seguridad del Cableado

El cableado de red debe estar protegido por conductos como canaletas y ubicados en lugares que no obstruyan el paso a las personas para evitar daños al cable y que se vean interrumpidos los servicios de red.

La instalación de cableado eléctrico deberá ser independiente del cableado de red para evitar interferencias.

### Mantenimiento de Equipos

Contaremos con un plan de mantenimiento preventivo de equipos que será calendarizado por departamentos, para evitar que el trabajo se vea interrumpido por falla de algún hardware del equipo y que exista pérdida de información.

Llevar una bitácora de daños más frecuentes en los equipos para estar prevenidos de futuros problemas con los mismos.

Debemos contar con un sistema de backups distribuidos para asegurar la información sensitiva de los usuarios finales replicando los backups entre el edificio y la casa, es decir, replicar los datos del servidor principal de archivos a otro secundario y éste deberá contar con las seguridades respectivas para los servidores.

### Baja o reutilización de equipos

Los equipos que serán sustituidos por otros deberán ser formateados y configurados nuevamente para el nuevo usuario después de sacar los respaldos respectivos, con el fin de que no exista información del antiguo dueño.

## DISEÑO DE LA SEGURIDAD LOGICA

Los objetivos de la Seguridad lógica son:

Definir y controlar los permisos y accesos a los programas y archivos

* Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos
* Asegurar que los datos y programas que no correspondan a un departamento sean modificados por los usuarios de dicho departamento
* Asegurar que la información trasmitida sea recibida por el destinatario al cual fue enviada.
* Asegurar que la información recibida sea la misma que fue transmitida

## DISEÑO DE LA RED

Para el diseño de la seguridad de la red se consideró la arquitectura de seguridad

### Computadores móviles

Se implementará políticas para el manejo de computadores móviles o portátiles donde se deberá incluir protección física, controles de acceso y protección contra virus.

### Trabajo remoto

Implementar políticas e implementar la protección para el acceso al trabajo remoto de usuarios que deban trabajar fuera de la organización, además este trabajo deberá ser autorizado y controlado. Se utilizara un cliente vpn para conectarse a la empresa.

## Políticas de seguridad del hardware

### Seguridad física del equipo

Todo equipo que sale de la institución debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la organización, motivo y responsable del equipo, además notificar a la sección TI si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

Todo equipo que sale de la organización debe contar con la respectiva autorización del jefe del departamento y llenar un formulario donde indique el tiempo que estará afuera de la institución, motivo y responsable del equipo, además notificar al departamento de TI si el equipo es un computador para proceder a las seguridades del equipo ya establecidas.

### Mantenimiento de equipos

TI estará a cargo del mantenimiento preventivo de los servidores y computadoras personales además será realizado dos meses y deberá ser registrado.

Cualquier problema de falla del equipo deberá reportarse inmediatamente TI porque podría ocasionar pérdida de la información o interrupción de los servicios.

Mantenimiento correctivo de los equipos y de la red supervisado por el Jefe de Administración Sistemas.

El personal que realice pasantías en el departamento de Sistemas estará bajo la supervisión del jefe del departamento para realizar algún tipo de mantenimiento de equipos.

TI se responsabilizará de mantener la adecuada instalación de la infraestructura de red.

### Políticas de seguridad del software

Para la adquisición, instalación y actualización será TI quien instale software adicional a los equipos si es necesario para el usuario.

TI realizara un chequeo previo de las actualizaciones de software y de los parches de seguridad para evitar que estos puedan ocasionar alguna clase de conflicto con el HW y SO. Las actualizaciones serán distribuidas por un servidor WSUS.

### Políticas de seguridad para el control de acceso a los sistemas de información

### Acceso Físico

Los equipos deberán estar ubicados bajo condiciones que ofrezcan seguridad física, eléctricas y además que permitan el acceso físico sin ninguna restricción al personal de Tecnologías de la Información

Tecnologías de la Información será quien tenga acceso al cuarto de servidores sin ninguna restricción y en caso urgente pueden acceder las autoridades de la empresa.

### Acceso a la información (archivos y documentos)

Las portátiles serán protegidas por software de control de acceso, antivirus y firewalls para evitar que cuando salgan de la institución no regresen con problemas de mal manejo y borren programas, virus o software no deseado.

Tecnologías de la Información no será responsable de la información personal de los usuarios que se encuentre en los discos duros de cada computador.

Instalar software de monitoreo que notifique la presencia de algún virus en el equipo, que deberá notificar inmediatamente a Tecnologías de la Información y deberá desconectar al equipo de la red hasta solucionar el problema.

Cada usuario deberá cerrar la sesión en su computador personal cuando no lo esté utilizando.

### Respaldos y Recuperación de archivos, aplicaciones y bases de datos

Tecnologías de la Información será responsable para realizar los backups de la información almacenada en las portátiles.

Garantizaremos la seguridad de la información de los usuarios que se encuentra almacenada en los servidores de archivos, servidores de bases de datos, servidores de aplicaciones; mediante la replicación ya sea haciendo uso de raids o en otro lugar físico (Datecenter de Antel, nubes, etc).

Garantizaremos la protección de la información asegurando su integridad, disponibilidad de acuerdo a sus normas establecidas.

Garantizaremos la seguridad de las bases de datos, los respaldo de las mismas y la restauración si hubiera

la necesidad.

### Acceso a los servicios de red

El acceso del personal a los servicios de red y de la información en horas no laborables será con previa autorización del responsable del área y coordinado para asignar los permisos.

Otorgar permisos a los empleados para el acceso a la información y los servicios de la red dependiendo de su perfil.

Controlar que el acceso a la red y a la información esté disponible las 24 horas del día, los 365 días del año.

Asegurar la disponibilidad de los servicios para los usuarios de acceso remoto, con previa autorización de las autoridades.

Monitoreo de la red y si encontrara alguna actividad sospechosa ocasionado por un computador personal, lo desconectará de la red hasta solucionar el problema mediante el uso de Kasperky Endpoint Security Cloud.

### Administración de usuarios

Tecnologías de la Información será quien cree la cuenta al nuevo usuario en la red con su respectiva identificación y autenticación.

Cada usuario en su primer ingreso deberá cambiar su contraseña que será única e intransferible, es decir, queda prohibido que el usuario comparta su contraseña a los compañeros.

La vida útil de la clave será de 90 días.

Se eliminaran o bloquearan las cuentas de las personas que ya no laboran en la institución.

Tecnologías de la Información será quien modifique las cuentas de los usuarios con previa autorización del departamento al que pertenezca el usuario.

### Correo electrónico e Internet

Tecnologías de la Información será quien administre la información que ingresa por el correo electrónico.

Controlar la navegación de los usuarios y limite el acceso a páginas de internet que no tienen ningún vínculo con las funciones de la empresa.

Definir qué tamaño de archivos podrá enviar y recibir cada usuario dependiendo de las normas del departamento.

El usuario no abrirá correo electrónico enviado por un remitente que no conoce, no responderá el mensaje ni mucho menos ejecutará archivos adjuntos en dichos correos.

### Políticas de seguridad para contingencia

Contar con planes de contingencia que pueda garantizar la recuperación de la información por algún desastre sin el mayor número de pérdidas y a un bajo costo.

Para el caso de un colapso total de aplicaciones o de bases de datos, se deberá definir un procedimiento de restauración de los respaldos de las mimas.

### Concepto Seguridad Informática

La seguridad informática se encarga de implementar técnicas de protección, es decir, se refiere a la protección de infraestructuras de las tecnologías de la información y comunicación que soportan la operación de una

organización, centrándose en hardware y software, como son antivirus, firewalls, detección de intrusos, entre otros elementos, además, de los enfoques técnicos los especialistas en seguridad se manejan con las

vulnerabilidades y con amenazas bajo la forma de ataques, para poder mitigar los riesgos, teniendo en cuenta políticas de seguridad para poder alizar y diseñar posibles responsabilidades y reglas para evitar amenazas o minimizar los efectos.

### Amenazas Informáticas

Se define a amenaza a todo elemento o acción que sea capaz de atentar a la seguridad informática, que surgen a partir de la existencia de vulnerabilidades.

La seguridad informática se hizo presente en los años 80’s debido que se tenía la necesidad de evitar o contrarrestar los ataques informáticos, y gracias a la utilización del Internet los riesgos y amenazas fueron mayores, afectando a varias empresas y usuarios de la red, ya que la inexistencia de restricciones en el

Internet provocó que los virus, troyanos y otros códigos maliciosos se propaguen a través de correos electrónicos, publicidad o páginas web, de esta manera ayuda a que los ataques tomen el control o la información de la empresa o usuario para causar daño.

### Ataques internos

Estos ataques son iniciados por individuos o grupos de colaboradores de una empresa que conocen el negocio y tienen accesos autorizados a la red interna o incluso a cualquier Server que quiera atacar, son los más comunes y los más peligrosos

### Ataques externos

Son iniciados desde fuera de la compañía, no tienen un acceso autorizado a la red, siendo más fáciles de detectar y mitigarlos que los ataques internos, su origen es por el Internet, redes de proveedores, accesos remotos.

## SEGURIDAD PERIMETRAL

no es una tecnología, sino se considera un sistema que se compone de varios elementos de tecnología, de hardware y de software, que actúan de manera conjunta con el fin de vigilar y proteger el perímetro o “borde”, aísla a la red de entradas externas (Internet) o amenazas, defendiendo, al estilo de estrategias militares, un perímetro de seguridad se utiliza mediante el uso de equipamiento especifico configurado para realizar filtros de paquetes de datos, controla todo acceso a la red interna de la empresa.

Teniendo en cuenta que la seguridad y la integridad de la información son primordiales para el funcionamiento de una empresa, y que los ataques y amenazas crecen constantemente ocasionando trastornos económicos,

mala imagen, funcionamiento y progreso para la empresa, nace la seguridad perimetral que es la forma para controlar el acceso y protección de los servicios informáticos.

En este proyecto para lograr la autentificación y el control de acceso se implementara un servidor radius (Remote Authentication Dial-In User Service) junto con el correspondiente servidor NPS(servidor de directivas). El servidor radius será el IAS (Internet autentication server) que viene incluido en Windows Server 2008R2. La aplicación se realizara tanto para la virtual private network(VPN) y para la red wifi.

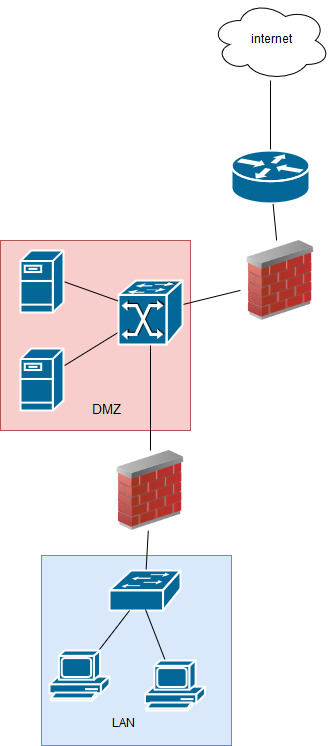
IAS utiliza los puertos 1812 y 1645 para la autenticación y los puertos 813 y 1646 para el arqueo.

Para la protección de borde de la red se utilizara un firewall de nueva generación (NGFW) .

Características de los NGFW:

* Detección y prevención de intrusiones (IPS): Protección contra amenazas de red examinando flujos de tráfico (basado en firmas y en comportamientos anómalos).
* Filtrado web: Protege bloqueando acceso a páginas inapropiadas y/o peligrosas.
* Anti-SPAM: Reduce el volumen de SPAM en el perímetro.
* Anti-Virus: Protección frente amenazas a nivel de contenidos en el perímetro.
* Amenazas Persistentes Avanzadas (APT): Protección frente a APTs mediante el uso de sandboxing (local o en la nube).
* Análisis tráfico encriptado (HTTPS)
* Acceso remoto SSL/VPN

Se colocará un firewall entre el router y los switches de la capa de distribución. Su función será filtrar el trafico proveniente de la red wan e internet. Además será el encargado de realizar la conexión vpn con el resto de “sucursales”



## 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.

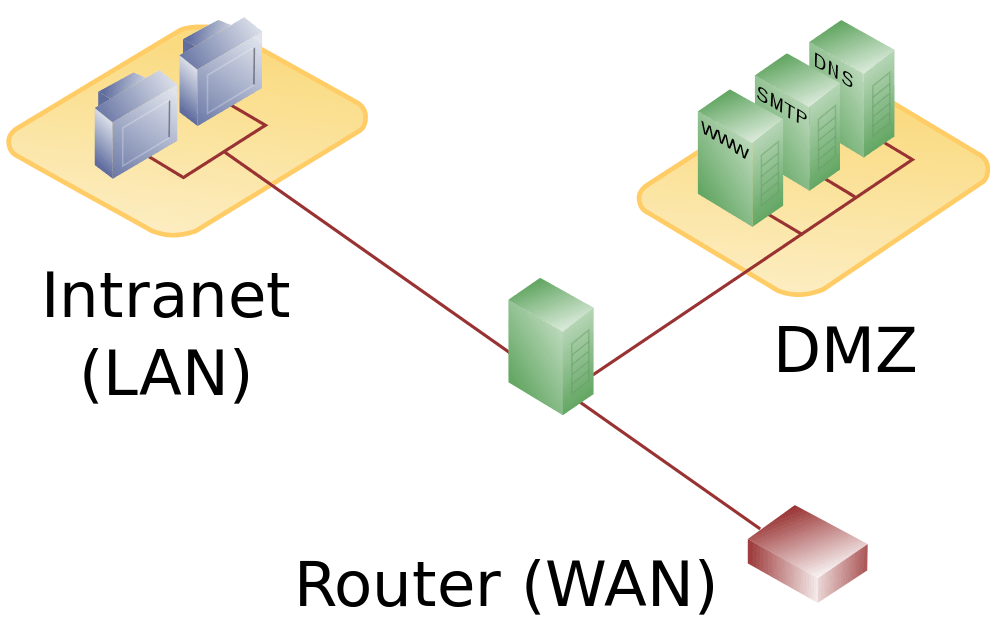
Es decir, colocamos en una red independiente los equipos que prestan un servicio y que deben ser accesibles desde Internet. De modo que aun estando dentro de la empresa, no están en la misma red que los usuarios. si uno de los equipos se ve comprometido, no afectará a la seguridad del resto de la compañía.

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 (un router con firewall) con terminales para tres conexiones de red separadas: una para Intranet, otra para Internet y otra para la DMZ.

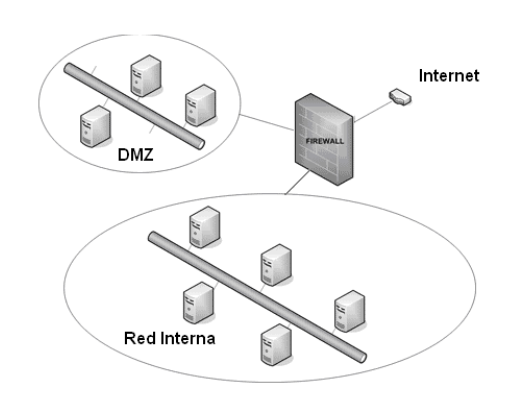


El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

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:

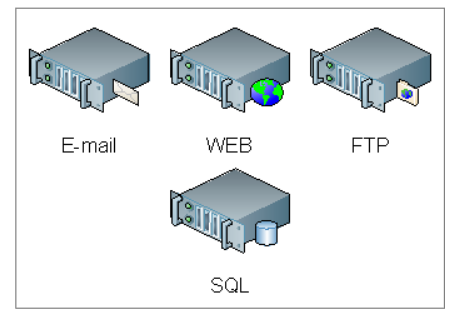
* Tráfico de la red externa hacia la DMZ autorizada.
* Tráfico de la red externa hacia la red interna prohibida.
* Tráfico de la red interna hacia la DMZ autorizada.
* Tráfico de la red interna hacia la red externa autorizada.
* Tráfico de la DMZ hacia la red interna prohibida.
* Tráfico de la DMZ hacia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



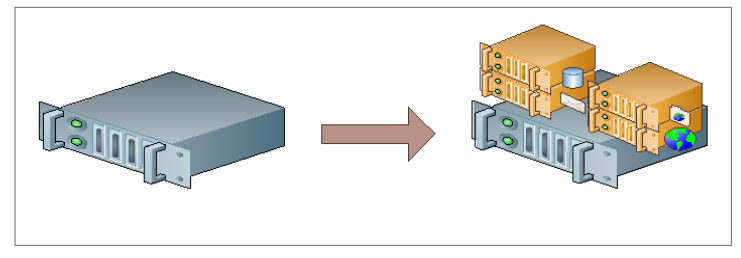
## POR QUÉ ES NECESARIO VIRTUALIZAR.

Virtualizar es una manera de crear independencia y disminuir complejidad en entornos donde se trabaja con múltiples aplicaciones y más aún si se trata de hardware, en este caso de servidores.

Comúnmente para cada servicio se dedicaba un equipo en particular, por lo consiguiente se infrautilizaba su capacidad.



Con una estructura de servidores virtuales es posible obtener los mismos servicios, pero en un solo equipo.



### Escenarios de virtualización

#### Consolidación de servidores

La virtualización permite consolidar las cargas de trabajo asignadas a un equipo servidor específico, en un número más reducido, así el mismo intensifica su uso. Esto implica ocupar menos espacio en el centro de cómputo y una reducción en el consumo de energía, con el mismo consumo eléctrico se pueden tener entre 10 ó 15 servidores virtuales por cada servidor físico.

#### Continuidad del negocio

Esta nueva tecnología proporciona la capacidad para la eficiencia de recuperación de desastres para reducir al mínimo el tiempo de inactividad. Debido a que los sistemas operativos y aplicaciones se conservan en archivos de datos, la virtualización ayuda a automatizar y racionalizar los procesos de backup, duplicación y movimiento de datos.

#### Delegaciones remotas

La virtualización contribuye a optimizar el uso de todos los recursos disponibles, independizando cada elemento en función de los otros y convirtiéndolos en servicios que se encuentran disponibles en forma inmediata.

#### Concepto de virtualización

La virtualización es la abstracción de los recursos de una computadora y su puesta en funcionamiento como máquina virtual en otra máquina física.

La virtualización se puede presentar como una aplicación o directamente un sistema operativo (hipervisor), donde se permite aislar los sistemas operativos virtualizados del sistema físico, proporcionándoles un hardware virtual uniforme. De este modo, la memoria RAM, las CPUs, los discos duros

y los dispositivos de red, pasan a ser recursos que se ofrecen a las Máquinas Virtuales para su uso

Un hipervisor o monitor de máquina virtual es una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos (sin modificar o modificados, en el caso de Paravirtualización) en una misma computadora. Una de sus funciones es aislar a los sistemas operativos del hardware real y controlar el acceso a dichos recursos.

La función del hypervisor es la de monitorear todas las peticiones de hardware del sistema operativo invitado y ejecutarlas en el hardware real.

#### Virtualización de hardware

Se llama también virtualización de plataforma y se refiere a la creación de máquinas virtuales que se comportan como máquinas reales con su propio sistema operativo, funcionando en una máquina anfitrión que carece de sistema operativo. La máquina anfitriona sólo ejecuta un software de virtualización para poder ejecutar las máquinas virtuales. Esta suele ser una opción utilizada cuando tenemos varios servidores, ya sean servidores de email, impresoras en red, ficheros, gestores de contenido, etc. y queremos hacerlos funcionar en una sola máquina.

#### Virtualización de sistema operativo

La virtualización del sistema operativo, hace referencia al uso de un software que permite al sistema de hardware ejecutar múltiples instancias de diferentes sistemas operativos de forma concurrente (simultánea), permitiendo, en una única computadora, ejecutar diferentes aplicaciones que requieren diferentes sistemas operativos. El software garantiza que los sistemas operativos no interfieran entre sí, ni a las aplicaciones.

#### Para-virtualización

En este caso la máquina anfitriona ejecuta un sistema operativo, y el software de virtualización interactúa con él. De este modo, independientemente de los sistemas operativos propios de cada máquina virtual, podremos utilizar la máquina anfitriona ya que posee su propio sistema operativo, ya sea personal o de servidor.

#### Virtualización de almacenamiento

Es la unión de múltiples dispositivos de almacenamiento conectados en red, de tal manera que parezcan una única unidad. Existe un amplio catálogo de software que nos permite hacer virtualización de almacenamiento.

#### Virtualización red

Consiste en poder unir en una red virtual varios elementos de red heterogéneos, ya sean hardware o software, conectados a distintas redes y dispersos topológicamente. Es decir, podemos tener varios elementos de red como computadoras, impresoras, servidores de ficheros, nuestra computadora personal en nuestra casa, etc. localizados en distintos puntos geográficos que, con sólo una conexión a internet, podemos agrupar formando una red virtual, con las ventajas administrativas que ello conlleva.

#### Virtualización de aplicaciones

Este tipo de virtualización divide la aplicación del sistema operativo, lo que reduce los conflictos entre aplicaciones, y simplifica las distribuciones y 30 actualizaciones de software. Se puede dar un entorno integrado de una aplicación con todos sus componentes, de manera que se ejecuten independientes de otras aplicaciones, permitiendo que en un mismo equipo se puedan ejecutar versiones diferentes de los componentes que serían incompatibles en un mismo sistema operativo.

#### Virtualización de servidores

Se denomina virtualización de servidores básicamente a agrupar diferentes aplicaciones y servicios dentro de un mismo hardware, de forma que los usuarios y el propio sistema los vean como máquinas independientes dedicadas. Para ello, el sistema operativo virtualizado debe ver el hardware de la máquina real como un conjunto normalizado de recursos independientemente de los componentes reales que lo formen.

Para virtualizar un sistema de servidores, los administradores deben, optimizar los recursos disponibles, incluyendo el número de los servidores físicos individuales, procesadores, y sistemas operativos, con el objetivo de producir una mejora tanto en la gestión como en el manejo de sistemas informáticos.

El administrador del sistema virtual utilizará un software para la división del servidor físico en entornos virtuales. Estos entornos se conocen técnicamente como servidores privados virtuales, en los cuales se administran características como particiones de unidades de almacenamiento, o emulaciones de sistemas operativos. Es decir que el administrador puede crear unidades virtuales de almacenamiento o aplicaciones virtuales para el uso de los clientes o usuarios finales

Una de las ventajas de la virtualización de servidores es que permite brindar protección contra las interrupciones de las actividades empresariales en caso de que se produzca un desastre natural, un corte de energía o error humano, ya que, una empresa con un servidor virtual de respaldo puede duplicarlo y almacenar una copia a nivel externo, a través de herramientas automatizadas las cuales permiten programar dichas copias según sea la necesidad.

La virtualización de servidores es importante para respaldar las iniciativas innovadoras de la empresa. Al implementar la virtualización de servidores, se contará con una mejor disposición para crear una infraestructura informática con mayor capacidad de respuesta que además de simple resulta más barata.

Además, la implementación que se realice se basará tanto en los conocimientos técnicos como sectoriales que ya están siendo implementados en otras partes del mundo.

#### VENTAJAS Y DESVENTAJAS DE LA VIRTUALIZACIÓN

Siempre que se desea llevar a cabo un proyecto utilizando una nueva tecnología es necesario tener en cuenta que ventajas no puede ofrecer esta tecnología y los inconvenientes que esta conlleva, para así poder tener claro a que posibles riesgos nos estamos enfrentando.

**Ventajas**

La virtualización reduce el consumo eléctrico y el dióxido de carbono emitido a la atmósfera al reducir el número de máquinas.

Reducción de costos de hardware, espacio físico y mano de obra.

Permite un aislamiento de las particularidades de los dispositivos, por lo que un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales.

Rápida incorporación de nuevos recursos para los servidores virtualizados: se trata de una tecnología escalable donde es fácil la incorporación de nuevas máquinas virtuales en una máquina anfitriona.

**Desventajas**

Necesidad de mayor cantidad de recursos hardware (memoria RAM, procesadores y disco).

Se pueden presentar problemas con los administradores de virtualización: ya que se necesita experiencia para gestionar adecuadamente la tecnología.

Dificultad en la configuración de servicios de Microsoft Windows (Exchange, SQL Server, Oracle, etc.).

Problemas de compatibilidad con los dispositivos Hardware virtualizados.

#### Diferencias entre virtualización de hardware y virtualización de software

Podemos decir que cuando nos referimos a la virtualización de hardware estamos haciendo referencia a una máquina anfitriona que no posee sistema operativo instalado, por lo que esta solamente puede funcionar con el sistema operativo de la máquina virtual.

En estas solo se pueden ejecutar y trabajar con los programas instalados en la máquina virtual y se emula el hardware de la misma para poder trabajar, en cambio, en la virtualización de software las maquinas anfitrionas poseen un sistema operativo propio lo cual les permite tener una lista de hardware certificado mucho más amplia, es decir que tiene una referencia, pues se basan en la información del sistema operativo de la maquina anfitriona, además que en este tipo de virtualización podemos trabajar con el sistema operativo de la maquina anfitriona y también con el de la máquina virtual.

#### VIRTUALIZACIÓN Y DATACENTER

Un Datacenter o centro de datos si lo traducimos literalmente es una instalación especializada para brindar facilidades desde hospedaje web de páginas webs estáticas hasta hospedaje de aplicaciones y diversos servicios de comunicaciones, como el nombre lo implica el propósito es el manejo de datos.

Un datacenter físico está compuesto por: switches, routers, racks, pach panel, organizadores y bandejas. Además de esto unidades de almacenamiento como lo son los servidores y equipos destinados para las aplicaciones dentro de este.

Un datacenter virtual contiene plantillas de VM para que pueda crear nuevas máquinas virtuales de forma rápida, o cargar las máquinas virtuales que ya se están ejecutando en el entorno interno. También puede crear aplicaciones virtuales (vApp) dentro de su centro de datos virtual, estas se usan cuando usted tiene una aplicación que requiere más de una máquina virtual.

Además, se tiene seguridad personalizada y / o la configuración de red, parámetros de inicio personalizados y desea que las aplicaciones se almacenan y aprovisionado de un catálogo. Además de esto puedes crear clúster y agregar host virtual para el manejo de tu infraestructura virtual.

#### Beneficios de la virtualización del centro de datos o Datacenter

A partir de un punto de vista de la arquitectura, con la virtualización, en esencia, se necesita menos hardware o hardware menos costoso para hacer el mismo trabajo. Se puede obtener 5 veces el rendimiento de una tercera parte del costo cuando se compara un sistema de gama media a un conjunto de servidores.

Si puedo poner 10 de esos servidores de bajo costo en un fondo de recursos virtualizados, tengo 5 a 10 veces el poder de los más poderosos de gama media del sistema en una tercera parte del costo.

Al virtualizar servidores, no solo puedo conseguir un ahorro de costos enormes, sino que también tengo una arquitectura con mejor disponibilidad y mantenimiento continúo. Si tengo una caída de servidor, esta no afecta a los otros, ya que se puede agregar máquinas virtuales para apoyar mi arquitectura.

Los beneficios de la virtualización de los centros de datos o Datacenter realmente son el mantenimiento y gestión, la reducción de los costos de adquisición de hardware, pues son menos partes en caso de mantenimiento, la disponibilidad de una mejor arquitectura, la seguridad y el rendimiento.

Todas estas son las razones por las que la virtualización se está convirtiendo en el estándar para la forma en que se crea el diseño de sus recursos de TI para el futuro.

### 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 | Primario | 10.10.0.1 | Virtual |
| GNCADII | Secundario | 10.10.0.15 | Virtual |

Cada uno con su contingencia:

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

|  |  |  |  |
| --- | --- | --- | --- |
| SERVIDOR |  | DIRECCION IP | TIPO |
| GNCAD2 | Primario | 10.10.0.1 | Virtual |
| GNCADII2 | Secundario | 10.10.0.15 | Virtual |

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 |

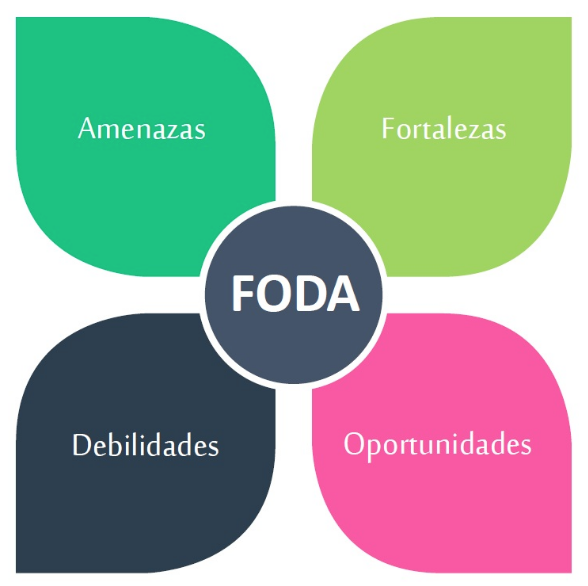
Configuración de los servidores secundarios, este se encuentra en el Datacenter de Antel

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

#### PLAN DE CONTINGENCIA

GNC cuenta con un Datacenter central en el cual están ubicados los servidores de la organización.

La infraestructura está divida en dos, donde están instalados los servidores operacionales y en caso de incidentes que les impida funcionar están los de contingencia que se alojan en otra ubicación, para garantizar que se encuentren operativos y accesibles estos se encuentran en el país. Ya que los tiempos de respuesta es menor.



## ¿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.