**PROYECTO DE INFRAESTRUCTURA**

**TERNERAS DE TAMBO**



GNC

Gestión de Nacimiento y Cría

**Integrantes:**

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

**Índice**

[WINDOWS SERVER 3](#_Toc529019844)

[Servidor de archivos 3](#_Toc529019845)

[Servidor de impresión 3](#_Toc529019846)

[Servidor de comunicaciones 3](#_Toc529019847)

[Servidor de correo electrónico. 3](#_Toc529019848)

[Servidor Web 3](#_Toc529019849)

[Servidor FTP 3](#_Toc529019850)

[Servidor proxy 3](#_Toc529019851)

[Controladores de dominio 3](#_Toc529019852)

[Servidores miembro 3](#_Toc529019853)

[Seguridad 4](#_Toc529019854)

[DNS o Domain Name System 4](#_Toc529019855)

[Directorio Activo 4](#_Toc529019856)

[Dominio 4](#_Toc529019857)

[Unidad Organizativa(OU). 4](#_Toc529019858)

[Grupos 4](#_Toc529019859)

[Objetos 5](#_Toc529019860)

[DHCP 5](#_Toc529019861)

[SERVICIOS A IMPLEMENTAR 6](#_Toc529019862)

[Tambos a Implementar. 6](#_Toc529019863)

[DESCRIPCIÓN Y EQUIPOS DE LA RED 7](#_Toc529019864)

[DEFINICIÓN DE CONTRASEÑA 9](#_Toc529019865)

[Servidor de archivos (FILE SERVER) 10](#_Toc529019866)

[Función de servidor de archivos: 10](#_Toc529019867)

[Servidor de IMPSRESIÓN (PRINT SERVER) 11](#_Toc529019868)

[DISEÑO DE LA SEGURIDAD FISICA 11](#_Toc529019869)

[AREAS SEGURAS 11](#_Toc529019870)

[Perímetro Físico 11](#_Toc529019871)

[Controles de acceso físico 12](#_Toc529019872)

[Protección de oficinas 12](#_Toc529019873)

[SEGURIDAD DE LOS EQUIPOS 12](#_Toc529019874)

[Suministros de Energía 12](#_Toc529019875)

[DISEÑO DE LA SEGURIDAD LOGICA 13](#_Toc529019876)

[DISEÑO DE LA RED 13](#_Toc529019877)

[Políticas de seguridad del hardware 13](#_Toc529019878)

[Seguridad física del equipo 14](#_Toc529019879)

[Mantenimiento de equipos 14](#_Toc529019880)

[Políticas de seguridad del software 14](#_Toc529019881)

[Políticas de seguridad para el control de acceso a los sistemas de información 14](#_Toc529019882)

[Acceso Físico 14](#_Toc529019883)

[Acceso a la información (archivos y documentos) 14](#_Toc529019884)

[Respaldos y Recuperación de archivos, aplicaciones y bases de datos 14](#_Toc529019885)

[Administración de usuarios 15](#_Toc529019886)

[Correo electrónico e Internet 15](#_Toc529019887)

[Políticas de seguridad para contingencia 15](#_Toc529019888)

[Concepto Seguridad Informática 15](#_Toc529019889)

[Amenazas Informáticas 15](#_Toc529019890)

[Ataques internos 16](#_Toc529019891)

[Ataques externos 16](#_Toc529019892)

[SEGURIDAD PERIMETRAL 16](#_Toc529019893)

## 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 desdedicho 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

(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**, 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.

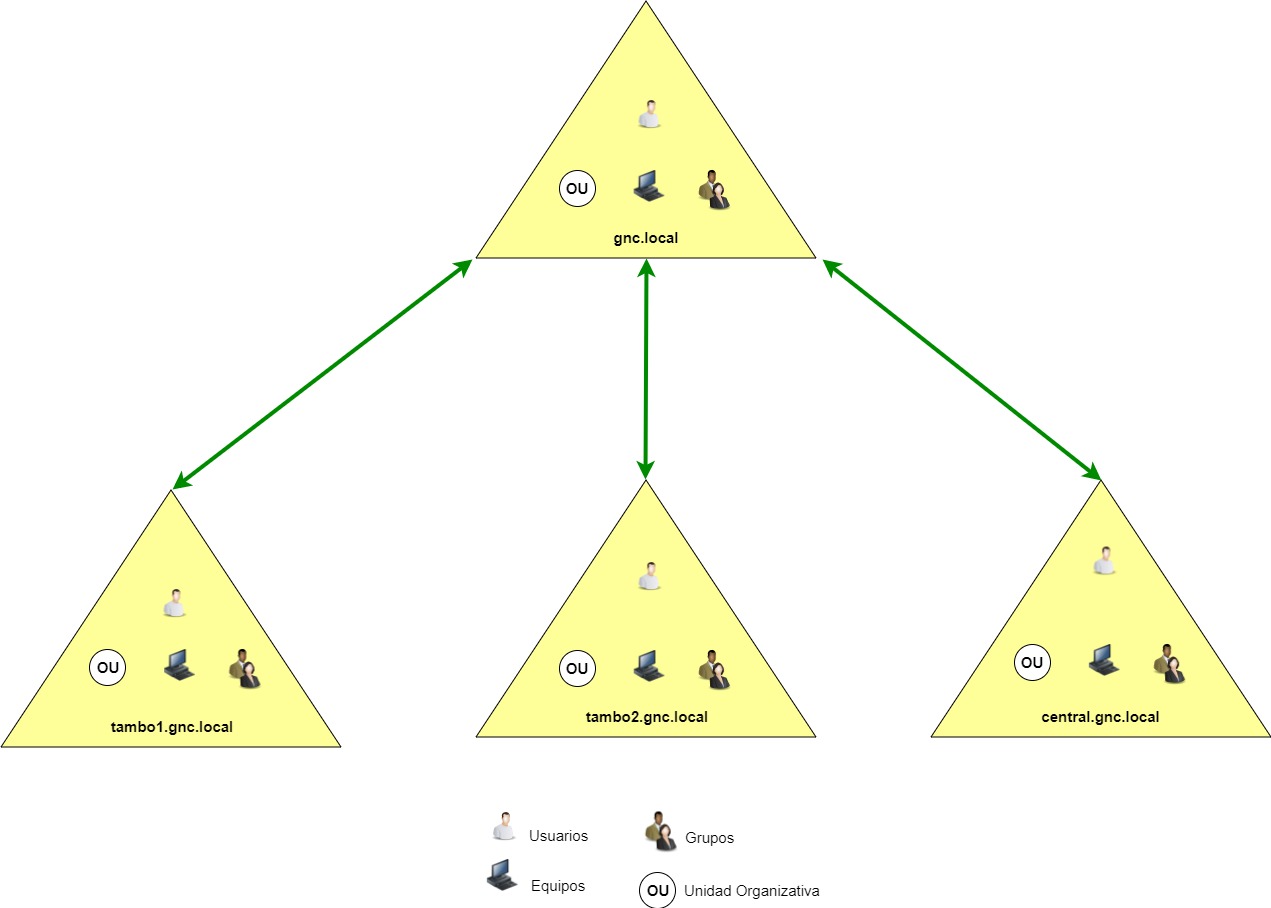
### Tambos a Implementar.

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

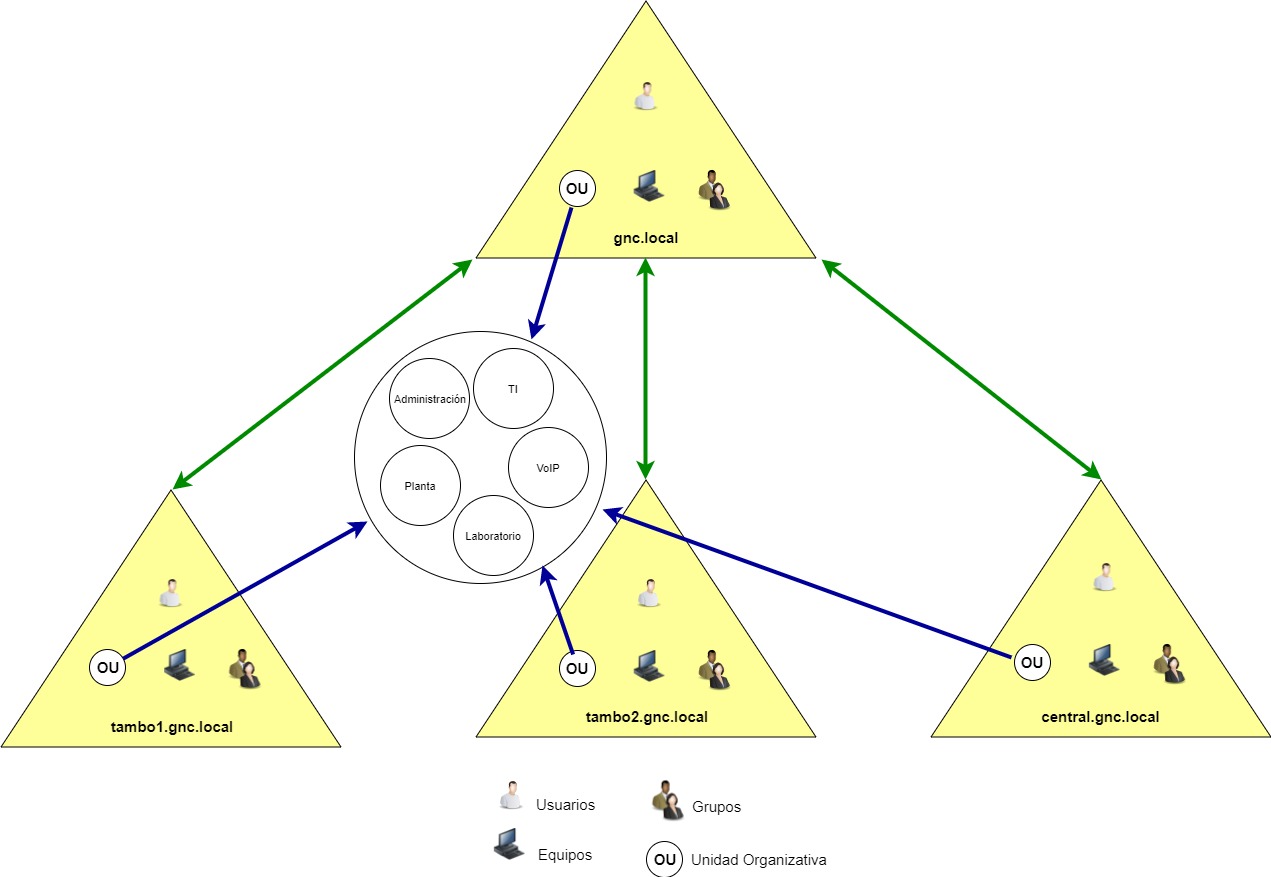
La estructura física de la organización está compuesta por un tambo principal y varias sucursales.

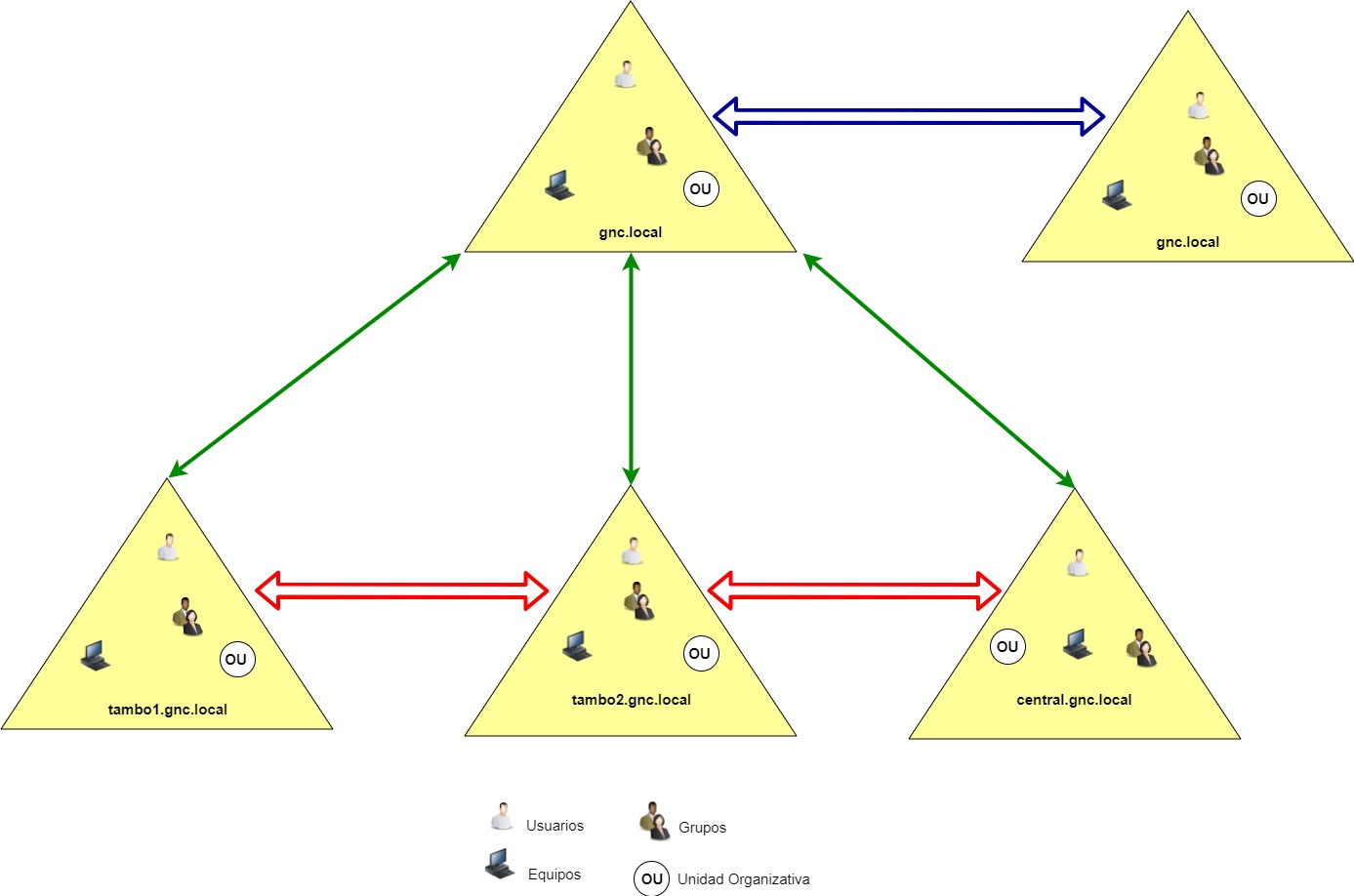
En el tambo principal o sede central están los servidores de la organización (o dominio raíz), además el subdominio **central.gnc.local**.

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



Esquema del Dominio gnc.local y sus subdomionios





### 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 |
| CENTRALAD | AD DC / DNS | 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 |
| CENTRALEMAIL | EMAIL | 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, conyuges, ...). 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. La lista siguiente muestra los tipos de información que debería evitar cuando esté creando una contraseña:

***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.

### 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.

Debido 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.

De debe aplicar políticas sobre 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

Se contar 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 Información implementará políticas para el manejo de computadores móviles o portátiles donde 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.

## 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

Tecnologías de la Información 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

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

TI será el encargado de la actualización de software y de los parches de seguridad periódicamente.

## 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.

Se deberá responsabilizar al personal de contrato sobre el manejo de información a través de sus contratos.

### 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.

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 y no sea interrumpido 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.

Administración de las IPs públicas y privadas.

Monitoreo de la red y si encontrara alguna actividad sospechosa ocasionado por un computador personal, lo desconectará de la red hasta solucionar el problema.

### 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 podrá cambiar su contraseña que será única e intransferible, es decir, queda prohibido que el usuario comparta su contraseña a los compañeros.

Vida útil de la clave.

Eliminar o bloquear 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.

### 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 tiene

n 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 colocara 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”