PROYECTO Final

TERNERAS DE TAMBO

Tecnicatura en tecnologías de la información

GNC

Gestión de Nacimiento y Cría

Integrantes:

Emiliano Silva

Samuel Rodríguez

Agustín Rodríguez

Sebastián Mena

Contenido

[**Nombre del grupo, e Integrantes**](#_ootcwrc8b3nr) **3**

[Metodología de Trabajo:](#_92up95fde7sm) 3

[Pautas de trabajo](#_12tu75wk9qn) 3

[Organización de la forma de trabajo](#_pwqt0fq6t1x1) 4

[Herramientas:](#_v5tcsrkcdkor) 4

[**Diagrama de red (físico)**](#_30j0zll) **7**

[**Diagrama de red (lógico)**](#_t6lz3f5yrvse) **8**

[**Especificación técnicas de los equipos**](#_sf4vamp04fw2) **9**

[DataCenter](#_9vrq7aftsp05) 9

[Routers](#_wnehxw4h6fr1) 9

[Firewall](#_xbvoya71qrwm) 9

[Switches](#_7i465i6unpz8) 10

[Cableado](#_qf9bf5rxb8q6) 10

[Cableado fibra óptica.](#_j37vsy295ay3) 11

[Servidores](#_e62pqpext4b5) 12

[**Equipos de Administración, Soporte IT, Planta, Laboratorio**](#_6j3asinr5j5h) **12**

[Administración](#_ub7dmsw3a8jj) 13

[Soporte IT](#_q64h24n0rli9) 13

[Planta](#_42hdkchovlqx) 14

[Laboratorio](#_blr43j2aanf5) 14

[**Esquema con tolerancia a Fallos**](#_vkqgyj1o1zam) **15**

[Prevención de Fallos en los Data Center](#_efu9velca1ae) 15

[**Planos y esquemas**](#_60tz6742fo9o) **18**

[**Plano de interconexión**](#_2et92p0) **18**

[**Esquema CDA**](#_ul1939acdk33) **19**

[Estructura de IP de los tambos (VPN)](#_sntczghjzme) 23

[Intercambio de datos financieros seguro de cada departamento](#_ye708fneehfu) 25

[de administración](#_7n99sly3izn) 25

[Auditoría de Ministerio de Economía y Finanzas](#_hd3nqmetrx45) 25

### Presentación del caso

Este proyecto se enfoca en una Empresa de gran porte con alcance y distribución nacional, conformada por varias sucursales (tambos) distribuidos estratégicamente en todo el país.

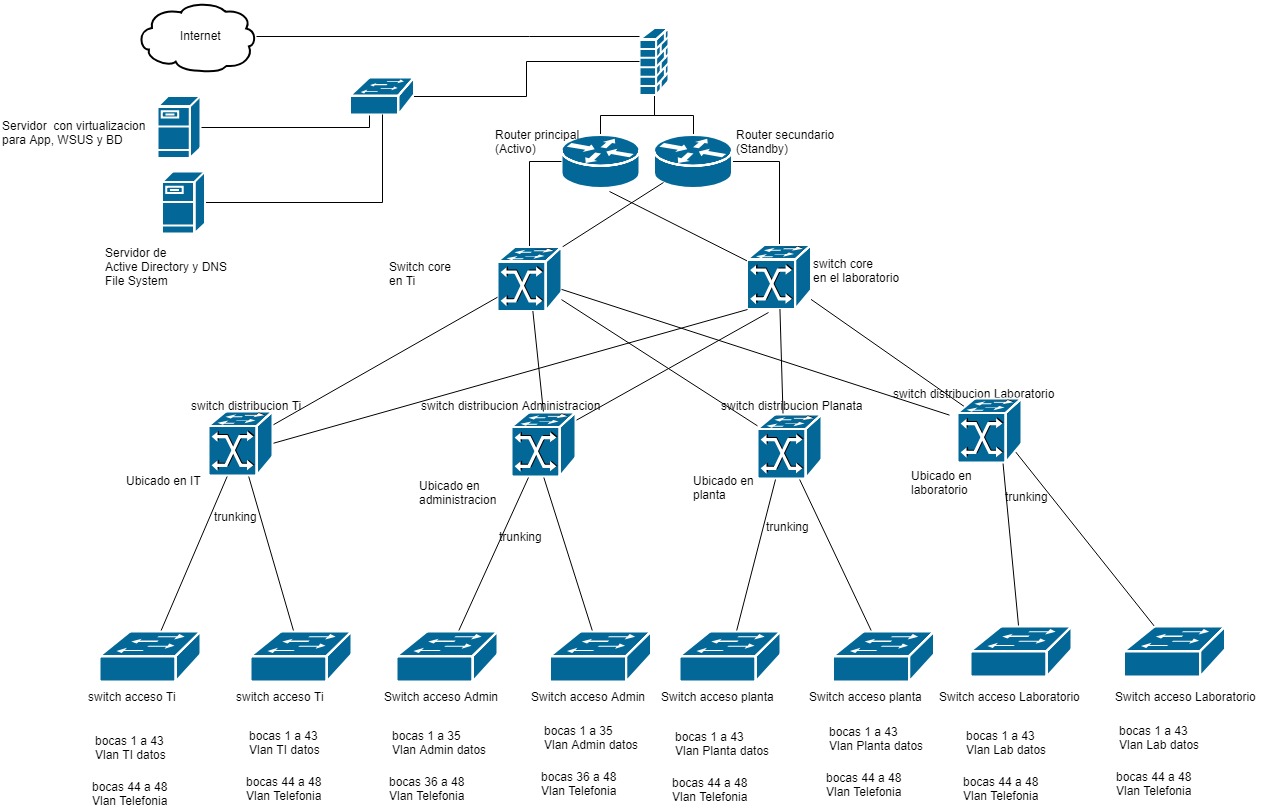
Un tambo requiere la instalación de una infraestructura, en la que sus servidores deban estar funcionales 24/7 por lo que deben ser tolerantes a fallos, deben ser eficientes y se debe contemplar la ecuación calidad/precio. El tambo cuenta con 4 departamentos.

Tomaremos cada uno de estos tambos de forma independiente para nuestro proyecto, todos ellos sumados conforman nuestra Empresa. Consideraremos cada uno de estos tambos como pequeñas empresas para su representación informática, los cuales están compuesto por diferentes departamentos o secciones, a saber: Administración, Planta, Laboratorio e IT.

Los tambos están interconectados entre sí para el intercambio de datos sensibles, contemplando exigencias y normativas Gubernamentales.

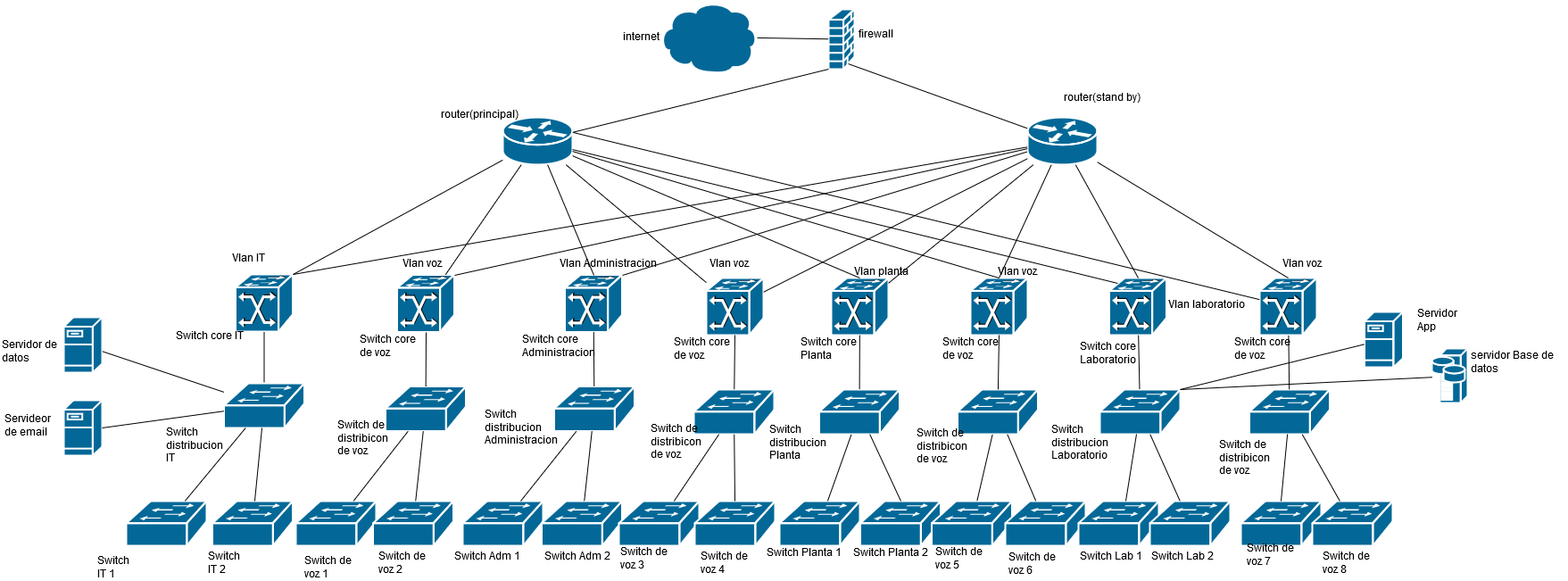
Como suele ocurrir en Empresas de esta envergadura es de vital importancia la información a proteger, en nuestro caso son los datos alojados en las instalaciones en forma de: bases de datos, sistemas de control lechero (software específico), información financiera, datos de los funcionarios, etc.

### Diagrama de red (físico)

[para mejor calidad de imagen](https://drive.google.com/open?id=11uwTigjuZf8bXkGFre8Q1-drVKGRj12W)

### Diagrama de red (lógico)

[para mejor calidad de imagen](https://drive.google.com/open?id=1QDnfM9vk9aCSl3yJD14XOpIVsgrINbJ8)



### Especificaciones técnicas de los equipos

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| Router Mikrotik (RB3011UiAS-RM) | 1 |
| Fortinet 500D | 1 |
| Switch Gestionable L2 JetStream de 12 puertos SFP | 2 |
| Switch Gestionable L2 T2600G-18TS JetStream de 16 Puertos con 2 Ranuras SFP (TL-SG3216) | 2 |
| Tp-Link Switch JetStream Gestionable Gigabit L2 de 48 Puertos con 4 ranuras SFP T2600G-52TS | 1 |
| System x3550 M5 Rack Server (Archivos – Mail) | 1 |
| System x3650 M5 Rack Server (Servidor APP – Base de Datos) | 1 |
| Cable UTP Cat-5e | \* |
| UPS BackUP | 1 |
| Generador | 1 |

## DataCenter

\*: A tratar con el cliente

# **Routers**

Los routers se elegirán de arquitectura modular para adaptarlos a nuestros requerimientos. El modelo de router seleccionado será el Router Mikrotik (RB3011UiAS-RM) con conexiones Ethernet Gigabit cuyo precio aproximado de mercado ronda los 320 dólares.

# **Firewall**

Un firewall de hardware es una unidad que se conecta entre la red y el dispositivo de conexión a Internet, brindando seguridad en nuestra conexión con la nube.

**Switches**

Características que deben tener los Switches propuestos para llevar a cabo la instalación.

- Apilables y modulares.

- Gestionables.

- Con funcionalidades VLAN en base a Access Control List.

- Velocidad de puertos seleccionables 10/100/1000 Mbps

- Capacidad de conexión por fibra.

Para Datacenter se usará Switch capa 3 con 4 conexiones de fibra óptica, para los departamentos (Datacenter/ (Administración, Planta, Laboratorio)) y Switch capa 2 con 2 conexiones de SFT. Estos equipos soportan VLAN, DCHP, tráfico Gigabits.

- Se deberán usar Switch del mismo tipo (caracteristicas, modelo), de forma de disponer de al menos uno de reserva para el caso de avería, y que este pueda usarse en sustitución de cualquiera de ellos.

Un IDF (Intermediate Distribution Facility) es el habitáculo de comunicaciones donde residen los equipos de comunicación, así como los armarios de racks de comunicaciones. En este caso los IDF contendrán un armario rack que albergará los switch de cada planta.

Cableado horizontal: mediante este cableado se interconectará cada uno de los host con los IDFs (Intermediate Distribution Facility). El cableado horizontal conectará cada una de las rosetas de los puestos de trabajo con los paneles de parcheo (patch pannels) de cada uno de los IDF por planta.

- Cableado vertical: el cableado vertical conectará los IDF situados en cada planta.

# **Cableado**

Se utilizarán dos tipos de cableado. Por un lado, el que une las estaciones de trabajo a su Switch correspondiente, que será del tipo UTP Cat-5e y Cat-6e con sus conexiones RJ45, para conectar los terminales a las rosetas.

El cableado vertical será de fibra óptica. Para conectar los IDF’s con el MDF se utilizará fibra óptica monomodo.

Los estándares que se acostumbran a utilizar en el cableado vertical son 100 BASE-FX (Fast Ethernet con fibra óptica) y 1000 BASE-FX (Gigabit Ethernet con fibra óptica). Por lo tanto, todos los racks deberán tener conectores en el panel de conexión tanto de fibra óptica como de cable RJ-45 para cubrir todas las necesidades de todo el edificio.

Los enlaces entre las diferentes plantas se realizarán con fibra óptica de 1 Gbps (Gigabit Ethernet), que permitirá suplir todas las necesidades de tráfico del sistema a largo plazo.

Los cables Cat-5e permiten a una red operar a velocidades cercanas al gigabit, aunque técnicamente no están certificados para garantizar estas velocidades. En nuestro caso se usarán los de Cat-5e para conectar los equipos de usuarios a la red.

Los cables Cat-6e garantizan al usuario velocidades de gigabit y también permiten transmisiones de datos de hasta 10 gigabits por segundo. El uso en el Datacenter garantizara que no se pierda velocidad de tráfico a los entre los dispositivos y departamentos conectados a este.

# **Cableado fibra óptica.**

Fibra óptica necesaria para comunicar el Datacenter con la planta, 2000 metros y con el Laboratorio, 3000 metros.

*Las razones por las cuales se elige instalar fibra óptica en lugar de cable UTP (servicios de voz y datos)*

• Ancho de banda. La tasa de transmisión en bits/segundo es mucho mayor con un cable de fibra óptica que con uno de cobre.

• No es susceptible de interferencia electromagnética. Esto significa que los campos electromagnéticos externos no se acoplan al cable de fibra.

• Los cables de fibra óptica pueden transmitir a mayores distancias sin que la señal se atenúe o se distorsione a un grado tal que la información no pueda recuperarse.

• Ofrece mayor seguridad (debido a que el cable no puede ser fácilmente intervenido o monitoreado.

Dado que las distancias óptimas para los cables UTP es 100 metros, y distancia entre las distintas plantas de 300, 2000 y 3000 metros, es inviable el uso de cable UTP.

La forma de tender el cableado entre los edificios sería con canalizaciones subterráneas.

**Racks**

Los racks necesarios para los IDF’s y MDF serán de 22 U, para colocación de Switches y paneles de parcheo. Se debe tener en cuenta la reserva de espacio para posibles ampliaciones, así como para cada Switch la reserva de una unidad para su panel de parcheo correspondiente.

**Virtualización**

La virtualización de servidores abstrae (aísla) el software de servidor del hardware por invitado/host, lo que facilita que varios servidores virtuales se ejecuten en un dispositivo físico.

**Definición de virtualización de servidores**

La virtualización de servidores es una arquitectura de software que permite que más de un sistema operativo de servidor se ejecute como invitado en un host de servidor físico específico. Al abstraer (aislar) el software de servidor de la máquina física de esta forma, el servidor se convierte en una "máquina virtual," separado de la superficie física, si bien el servidor "cree" que se está ejecutando exclusivamente en los recursos de memoria y de procesamiento. Realmente se está ejecutando en una imitación virtual del hardware del servidor.

**¿Por qué elegir la virtualización de servidores?**

La virtualización de servidores permite un uso más eficiente de los recursos de TI que antes. Antes de la virtualización de servidores, era común tener hardware infrautilizado y sobreutilizado en el mismo centro.

### Servidores

# **Servidor 1**

En este primer System x3550 M5 Rack Server se montarán los servidores de: archivos, Active directory del dominio principal y active directory del subdominio de ese tambo, siempre usando la virtualización. Para este servidor se usará un equipo con las siguientes características: dos procesadores de la serie Intel® Xeon® E5-2600 v3 con hasta 18 núcleos cada uno, cambio en caliente de Fuente, y HDD.

# **Servidor 2**

En este segundo System x3650 M5 Rack Server se montarán todos los servidores de Base de Datos, Aplicación y Wsus.

Para este servidor se usará un equipo con las siguientes características: almacenamiento Raid 1 para obtener velocidad de procesamiento de datos; dos procesadores de la serie Intel® Xeon® E5-2600 v3 con hasta 18 núcleos cada uno, componentes de intercambio en caliente (Fuentes de alimentación, módulos de ventilador y unidades HDD/SSD).

Hipervisor y hipervisor nativo

El hipervisor dirige el concepto de virtualización al permitir que la máquina física (en este caso un servidor) opere múltiples máquinas virtuales como invitados para ayudar a maximizar el uso efectivo de los recursos informáticos, como la memoria, el ancho de banda de la red y los ciclos de la CPU.[[1]](#footnote-1)

El hipervisor *nativo*, *unhosted* o *bare metal* (*sobre el metal desnudo*), es un tipo de hipervisor que se ejecuta directamente sobre el hardware, para ofrecer la funcionalidad descrita de permitir el uso de distintos sistemas operativos a la vez.[[2]](#footnote-2)

Para este proyecto se utilizara el hipervisor nativo que ofrece VMware, con su producto VMware Vsphere hypervisor (ESXI). Se adquirirá este software en un kit que incluye productos que facilitaran la administración de las máquinas virtuales, así como la implementación de la seguridad endpoint de las VM (Virtual Machines).

En cada servidor se instalara Vsphere Vshield que viene en el kit, lo que permitirá centralizar la seguridad endpoint de las VM que estén en el mismo servidor.

A cada máquina virtual se le instalaran la VMware Tools que permitirá mejorar el rendimiento de las VM.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tambo Central | | | | |
| Servidor 1 | | | | |
| Máquina virtual | **Procesador** | **Espacio en Disco** | **SO** | **Servicio** |
| 1 | 5 núcleos | 150 GB | Windows Server 2008 R2 | Active Directory/DNS Raíz |
| 2 | 5 núcleos | 1TB | Windows Server 2008 R2 | File Sysyem |
| 3 | 5 núcleos | 100GB | Windows Server 2008R2 | Active Directory/DNS Subdominio |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tambo Central | | | | |
| Servidor 2 | | | | |
| Máquina virtual | **Procesador** | **Espacio en Disco** | **SO** | **Servicio** |
| 1 | 5 núcleos | 750 GB | Windows Server 2008 R2 | Servidor BD |
| 2 | 8 núcleos | 750GB | Windows Server 2008 R2 | Servidor de App |
| 3 | 5 núcleos | 500 GB | Windows Server 2008R2 | Servidor WSUS |

### Equipos de Administración, Soporte IT, Planta, Laboratorio

Punto De Acceso Wifi Mimo 3x3, 450 clientes, 165 metros proveerá a los usuarios conexión sin problemas desde cualquier parte, este equipo es dual band (5 y 2.4 Mhz), la cantidad de conexión es mayor a 250 equipos. Los usuarios de estos departamentos usaron los siguientes equipos:

Desktop: Equipos con 4 GB de memoria RAM, 1 TB HDD, los procesadores de estos equipos de escritorio van a ser Core i3 o Core i5.

Notebook: 1 TB de HDD, 8 GB de memoria RAM, procesador Core i5.

# **Administración**

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| Tp-Link Switch Administrable L2 de 48-Puertos de 10/100Mbps + 4 Puertos Gigabit JetStreamTL-SL3452 | 2 |
| Punto De Acceso Wifi Mimo 3x3, 450 Clientes, 165 Metros | 2 |
| ThinkCentre M710 SFF (Intel) PC Core I3 | \* |
| ThinkCentre M710 SFF (Intel) PC Core I5 | \* |
| Ideapad 320 (15”, Intel) Notebook Core I5 | \* |
| Cable UTP Cat.5 | \* |

\*: A tratar con el cliente

# **Soporte IT**

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| Tp-Link Switch Administrable L2 de 48-Puertos de 10/100Mbps + 4 Puertos Gigabit JetStreamTL-SL3452 | 2 |
| Punto De Acceso Wifi Mimo 3x3, 450 Clientes, 165 Metros | 2 |
| ThinkCentre M710 SFF (Intel) PC Core I3 | \* |
| ThinkCentre M710 SFF (Intel) PC Core I5 | \* |
| Ideapad 320 (15”, Intel) Notebook Core I5 | \* |
| Cable UTP Cat.5 | \* |

\*: A tratar con el cliente

# **Planta**

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| Tp-Link Switch Administrable L2 de 48-Puertos de 10/100Mbps + 4 Puertos Gigabit JetStreamTL-SL3452 | 2 |
| Punto De Acceso Wifi Mimo 3x3, 450 Clientes, 165 Metros | 2 |
| ThinkCentre M710 SFF (Intel) PC Core I3 | \* |
| ThinkCentre M710 SFF (Intel) PC Core I5 | \* |
| Ideapad 320 (15”, Intel) Notebook Core I5 | \* |
| Cable UTP Cat.5 | \* |

\*: A tratar con el cliente

**Laboratorio**

|  |  |
| --- | --- |
| **Equipo** | **Cantidad** |
| Tp-Link Switch Administrable L2 de 48-Puertos de 10/100Mbps + 4 Puertos Gigabit JetStreamTL-SL3452 | 1 |
| Punto De Acceso Wifi Mimo 3x3, 450 Clientes, 165 Metros | 2 |
| ThinkCentre M710 SFF (Intel) PC Core I3 | \* |
| ThinkCentre M710 SFF (Intel) PC Core I5 | \* |
| Ideapad 320 (15”, Intel) Notebook Core I5 | \* |
| Cable UTP Cat.5 | \* |

\*: A tratar con el cliente

### Esquema con tolerancia a Fallos

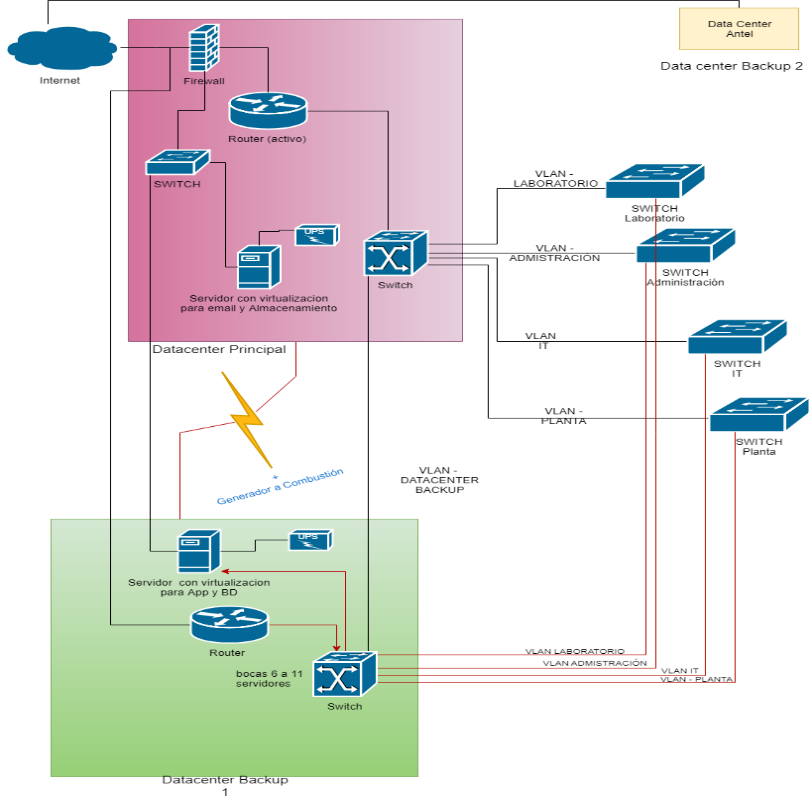
Con el fin de estar operativos 24/7 se cuenta con baterías que permiten que ante cortes de energía provenientes de la red eléctrica, el data center deje de estar operativo, estas dan un margen de tiempo que el sistema de suministro de energía de emergencia alimente de energía a los equipos.

Todos los servidores instalados en los Data Centers cuentan con sistemas Redundante de almacenamiento (Raid 5 y Raid 1), al tener un Datacenter de Backup la información estará disponible 24/7 los 365 días.

Las instalaciones cuentan con un Datacenter Principal ubicado en el departamento de Ti, en caso de falla total de este ya sea por incendio, o cualquier otro motivo que impida que este brinde el servicio a los usuarios, está otro Datacenter que tiene la misma información que el central. En condiciones normales actuará como Backup. Su ubicación física será en el Datacenter de Antel. Además se cuenta con un segundo servidor en el laboratorio, se elige esta ubicación que implica menos costos de instalación por encontrarse en el centro de la estructura física, tiene conexión directa a administración, planta y el propio laboratorio. Los costos que implica dicha instalación son los de los equipos de comunicación (Router, Switch de enlace, servidores).

En el Datacenter central estará ubicado un servidor con virtualización de Active directory/DNS (raíz), Active Directory (subdominio) y Almacenamiento, mientras que en el datacenter secundario se encontrará otro servidor con virtualización de Aplicación, Base de datos y Wsus.

Cada servidor es capaz de asumir la carga del otro servidor, es decir que el primer servidor también podría virtualizar lo que está en el servidor dos y viceversa. Esto permite proporcionar la disponibilidad 24/7 dado a que, si hay una falla con el servidor uno, se levantaría un back up en el servidor 2 y a la inversa.



[para mejor calidad de imagen](https://drive.google.com/open?id=18j_XBLBKuMtzaOIASbtqSwF1fgOK2iZ-)

# **Prevención de Fallos en los Data Center [[3]](#footnote-3)**

Los puntos básicos que deben considerarse para que un Data Center sea confiable:

A: Energía siempre disponible: UPS, generadores, baterías y Switches estáticos

B: Control del ambiente: Temperatura y humedad, filtración y flujo de aire

C: Seguridad: Protección contra incendios, inundaciones e intrusión

D: Monitoreo y control: Alarmas, redundancia, administración de energía.

A: Operar sin interrupciones es una necesidad vital en los centros de datos. De ahí que sea fundamental contar con grupos electrógenos para enfrentar un eventual corte de energía. Ante una falla en la red eléctrica estos equipos inician su funcionamiento entregando carga al sistema y permitiendo períodos extensos de autonomía eléctrica.

Otros equipos relevantes son los sistemas de UPS, que asumen la carga de los equipos mientras los grupos electrógenos completan su ciclo para suministrar energía, evitando -según indica el ejecutivo de Telefónica- los cortes de energía durante los cambios y regulando el voltaje, entre otras ventajas.

Expertos van más allá todavía, y aseguran que las UPS son el corazón del subsistema eléctrico dentro de un Data Center, porque permiten la continuidad operativa de los sistemas, filtran los mayores problemas eléctricos y enlazan la energía hasta el encendido del grupo generador.

B: El ambiente para de los Datacenter de contar con un control de temperatura, humedad, ventilación. Los equipos de comunicación levantan temperatura y para mantener la temperatura controlada para un funcionamiento óptimo se usarán aire acondicionado que mantendrá la sala a temperatura constante.

**Temperatura:** la temperatura debe oscilar entre 18ºC y 21ºC.

**Humedad:** debe oscilar entre el 40% y el 60%.

**Ventilación:** se debe contar con sistema que permita la recirculación de aire.

**Espacio Físico**

El espacio físico debe de estar distribuido de manera tal que se pueda maximizar su utilización. Todas las áreas deben ser funcionales y deben de ubicarse salidas de emergencia, áreas de circulación, áreas de profesionales de soporte, etc. La visibilidad dentro del centro de datos debe ser total.

# **Sistema de Aire Acondicionado**

Debe diseñarse un sistema de acondicionamiento de precisión y ecológico, con la mejor tecnología disponible y dentro de los estándares actuales.

Debe poseer control de temperatura y humedad dentro del Data Center.

# **Sistema de Cableado**

El cableado debe realizarse de acuerdo a las normas establecidas, incluyendo materiales y elementos para el correcto funcionamiento y distribución del cableado dentro del Data Center.

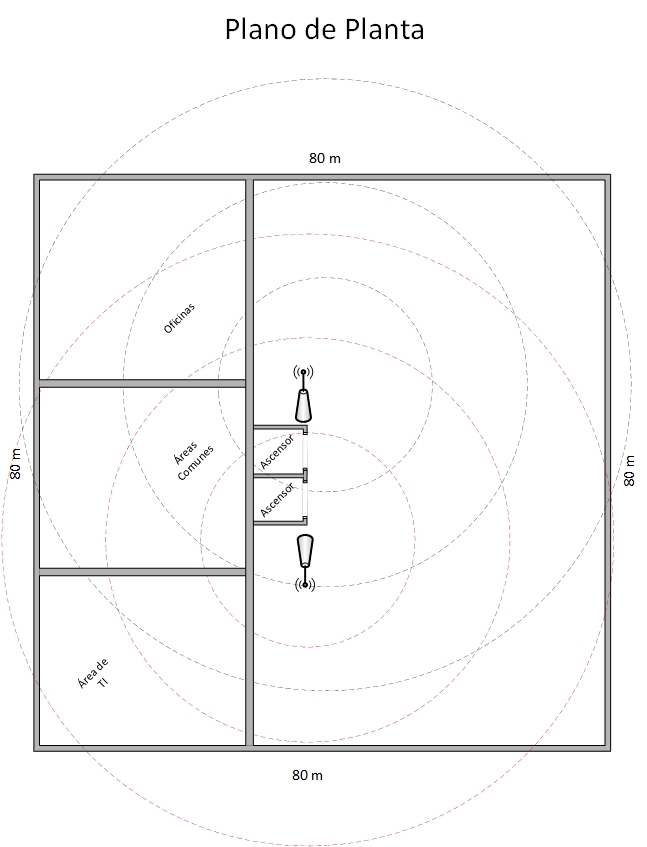
**Gabinetes**

Los gabinetes deben cumplir con las normas y especificaciones establecidas para soluciones de Data Center. Deben estar diseñados para soportar todos y cada uno de los equipos que se requieren, como así también los altos pesos que cada uno de ellos posee.

### Planos y esquemas



### Plano de Planta



### Esquema CDA

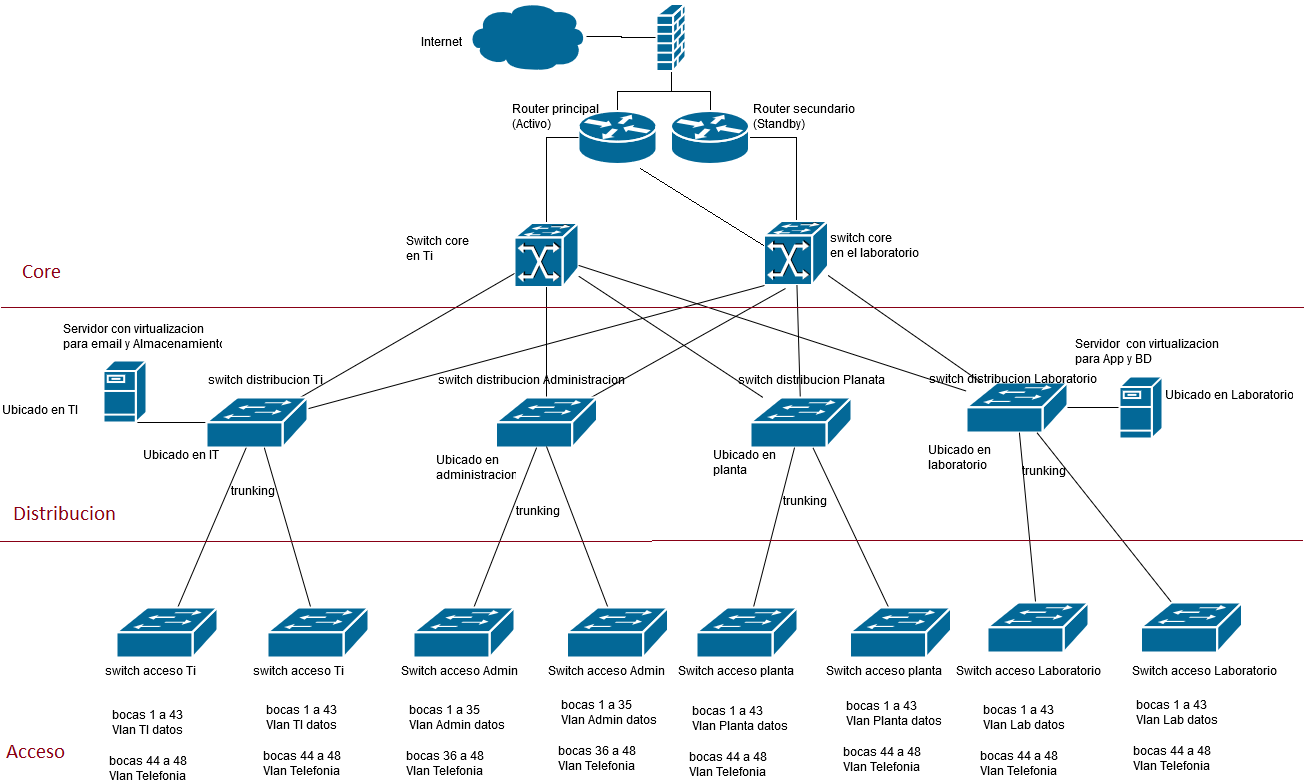
# **Esquema del Core Distribución y Acceso.**

La capa core está conformado por un Firewall Fortinet 500D / FortiGate 500D la función será de Firewall y servicios de VPN con 8 puertos RJ45 y 8 puertos SPF. Un Router MIkrotik RB3011UiAS-RM con diez puertos Gigabit, divididos en dos grupos de switch, un slot SFP.

El nexo entre el Core y Distribución se realiza por un Switch Gestionable L2 JetStream de 12 puertos SFP Gigabit y 4 Puertos, se distribuye los datos y voz por medio de Fibra.

La capa distribución se realiza por un Switch Gestionable Gigabit L2 JetStream de 16 Puertos con 2 Ranuras SFP, llegando por fibra tanto los datos como Voz.

La capa de acceso está gestionada por uno o varios switch Administrable L2 de 48-Puertos de 10/100Mbps + 4 Puertos Gigabit estos equipos proveerán de servicios a PC y access Point.

****

[para mejor calidad de imagen](https://drive.google.com/open?id=1O5cMvm89ORkgTph-sUG5rSha7Z2iW6SR)

### Vlan’s

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

### IPs Servidores y firewall

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NOMBRE | SERVICIOS | IP | DNS | Puerta de enlace |
| CENTRALAD | AD DC / DNS | 10.10.21.11 | 10.10.21.11 | 10.10.21.1 |
| CENTALFS | FILE SERVER / PRINTER SERVER | 10.10.21.12 | 10.10.21.11 | 10.10.21.11 |
| CENTALBD | BASE DE DATOS | 10.10.21.13 | 10.10.21.11 | 10.10.21.11 |
| CENTRALAPP | APLICACIONES | 10.10.21.14 | 10.10.21.11 | 10.10.21.11 |
| CENTRALWSUS | PARCHEO | 10.10.21.15 | 10.10.21.11 | 10.10.21.11 |
| FIREWAL | FIREWALL | 10.10.21.16 | 10.10.21.11 | 10.10.21.11 |

### Enrutamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DISPOSITIVO | DIRECCION IP | MASCARA DE SUBRED | GATEWAY PREDETERMINADO | BOCA |
| Router 1 | 10.10.21.1 | 255.255.254.0 | No aplica |  |
| Router 2 | 10.10.21.2 | 255.255.254.0 | No aplica |  |
| Switch 1 | 10.10.21.3 | 255.255.254.0 | No aplica | 1 |
| Switch 2 | 10.10.21.4 | 255.255.254.0 | No aplica | 2 |
| Switch 3 | 10.10.21.5 | 255.255.254.0 | No aplica | 3 |
| Switch 4 | 10.10.21.6 | 255.255.254.0 | No aplica | 4 |

### Servicios VPN

Para interconectar los distintos tambos distribuidos en todo el País por ello se deberán prever los mecanismos

necesarios para comunicar las diferentes sedes con la sede principal.

En esta fase se debería comunicar cada uno de los tambos con los servidores de aplicaciones, base de datos, mail, archivos, etc y la intranet de la empresa principal.

Para ello se necesita que el sistema esté preparado para comunicar las diversas sedes a la sede principal, de forma remota.

Para realizar este cometido, se plantea como solución el uso de las redes virtuales o VPN. Una red privada virtual VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública como internet. Los paquetes de datos de la red privada viajarán por un túnel definido en la red pública. De esta forma se permitirá que la computadora de nuestra red envíe y reciba datos sobre redes públicas como si fuera una red privada con toda funcionalidad, seguridad y políticas de gestión de este tipo de redes.

# **Aplicación de la VPN a la red:**

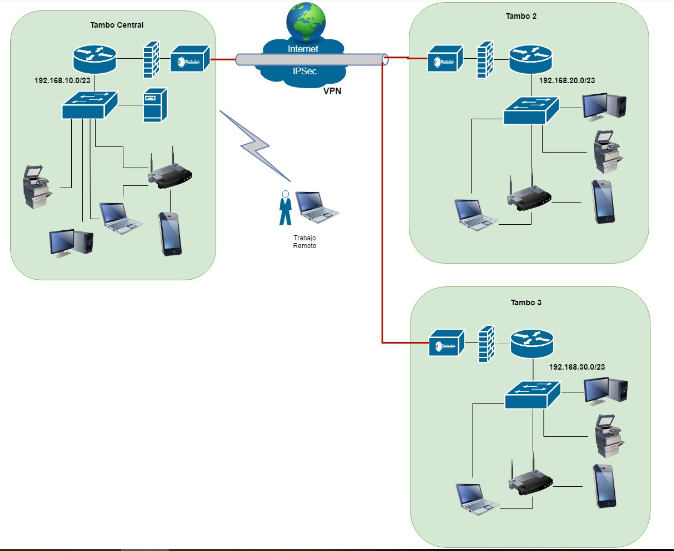
Para conectar la sede principal con las demás sucursales de los tambos mediante VPN, se utilizará un router/firewall con capacidad de gestión y creación de túneles VPN, que facilitará la tarea de conexión y enlace.

Las líneas dedicadas de acceso a Internet para empresas proporcionan enlaces simétricos de alta velocidad con garantía de disponibilidad y ancho de banda, por lo que se convierten en soluciones óptimas para el acceso a aplicaciones empresariales, voz sobre IP, Redes Privadas Virtuales (VPN), Multi-Videoconferencia o Acceso a Internet de elevada criticidad.

Se usará IPSec túnel LAN to LAN (IP to IP) una VPN punto a punto. El cifrado a utilizar será el aes, el método de autenticación de integridad será SHA-256 y autentificación de claves precompartidas. Se deberá habilitar el puerto 51 con protocolo IP y el puerto 500 con protocolo UDP.

### Estructura de IP de los tambos (VPN)

Para el tambo central (Datacenter) las IP van a ser 192.168.10.0 a 192.168.19.255, para las sucursales el tercer octeto va aumentar de a 10 por cada sucursal, tambo 2: 192.168.20.0, tambo 3: 192.168.130.0, tambo 4: 192.168.40.0.

****

### Intercambio de datos financieros seguro de cada departamento de administración

GNC cuenta con varios tambos distribuidos en todo el país, para que la gestión de tambos sea en tiempo real existe un Datacenter que concentra toda la información de los tambos del Grupo GNC. Este Datacenter Posee Conectividad 24/7 los 365 días de alta velocidad de procesamiento de información, los servicios que provee son E-mail, software del tambo, base de datos, archivos. Mediante Virtual Private Network (**VPN**) los tambos que no están en el predio de Datacenter o tambo Central se van a conectar de forma segura. VPN brinda Confidencialidad, Integridad, Disponibilidad que se transportan a través de esta red. Los Datos financieros de todos los tambos estarán almacenados el Datacenter, esto garantiza que la información sea fiable, esté disponible cuando se la necesite.

Los datos financieros serán procesados por el sistema de Gestión de Nacimiento y Cría (GNC) y almacenados en base de datos Oracle.

Los técnicos y empleados autorizados podrán acceder a todo el sistema desde cualquier lugar como si estuviesen en la oficina.

### Auditoría de Ministerio de Economía y Finanzas

Se configura un directorio de archivos para que técnicos del MEF puedan acceder 24/7 a toda la información financiera del grupo de tambos. Esta información estará centralizada en el tambo central, toda la información de los ambos está almacenada en un único lugar físico. Una vez al día la información financiera de los tambos será volcada a un directorio de forma automática por el sistema del tambo. Para que los técnicos del MEF puedan acceder se creará un acceso a usuarios que el MEF mediante un usuario y contraseña. Este Acceso se hará mediante VPN IP Sec.

.

1. https://www.networkworld.es/m2m/que-es-un-hipervisor [↑](#footnote-ref-1)
2. https://es.wikipedia.org/wiki/Hipervisor [↑](#footnote-ref-2)
3. <https://www.mundohvacr.com.mx/2009/04/acondicionamiento-en-data-center/>

   https://iesbidaju.wordpress.com/2016/05/27/data-center-y-mini-data-center/ [↑](#footnote-ref-3)