AUDITORÍA DE LA PLATAFORMA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DE LA AGENCIA NACIONAL DE INFRAESTRUCTURA – ANI

Octubre 2013

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

Este informe es el resultado de la auditoría de la plataforma tecnológica y el sistema actual de información con el que cuenta **La Agencia Nacional de Infraestructura (ANI)**, presenta un diagnóstico detallado y caracterización adecuada con el fin de poder establecer las recomendaciones y las acciones necesarias para salvaguardar la información y mejorar la gestión de activos.

El presente documento comprende los ámbitos LAN, WLAN, WAN, ToIP Seguridad Perimetral y TI como verticales contemplados en el análisis de situación actual y evaluación de posibilidades de mejora. Las mejoras o recomendaciones se basan en el rol y la criticidad dentro del flujo de negocio y expectativa de crecimiento general de la ANI.

La Agencia se encuentra en estos momentos en el "Desarrollo de un sistema de información y un sistema de gestión que permita a los clientes internos y externos contar con la información real sobre el estado y los aspectos relevantes de los proyectos APP y de la institución.", esto significa que mediante el uso de las Tecnologías de la Información - TI, se soportan todas las actividades de la Agencia convirtiendo la Gestión TI en uno de los pilares sobre los que se soporta la operación total de la entidad.

El informe brinda información detallada de la situación actual de TI, analiza los diferentes hallazgos y sustentándose en las mejores prácticas brinda recomendaciones para el mejoramiento de toda la infraestructura además de plantear un "camino a seguir" y la infraestructura tecnológica a la cual apuntar para cumplir con las expectativas de la entidad en lo que respecta a gestión, control, alta disponibilidad, tolerancia a fallos y respaldo de la información.

2. SITUACION ACTUAL

2.1 Red

2.1.1 Red LAN

La red LAN del cliente está diseñada en una topología tipo estrella, compuesta en su totalidad por equipos Juniper, switches de acceso EX-4200, switches core EX-4550.

Se cuentan con 3 cuartos de equipos ubicados en los pisos 2, 6 y 7.

- En el piso 2 se cuenta con una cascada de 3 switches de acceso Juniper EX-4200, también se cuenta con una cascada de 2 switches core Juniper EX-4550.
- En el piso 6 se cuenta con una cascada de 5 switches de acceso Juniper EX-4200.
- En el piso 7 se cuenta con una cascada de 4 switches de acceso Juniper EX-4200.

De cada cascada de switches de acceso se cuentan con dos conexiones en fibra óptica hacia el switch core de 10Gbps, donde el protocolo STP (Spanning Tree Protocol) se encuentra bloqueando uno de los puertos para evitar un loop sobre la red.

En el switch core se encuentran conectados todos los servidores, además del enlace MPLS a la red Ravec (2Mbps) y el enlace de Internet (20Mbps).

2.1.2 Red Wireless

La red wireless del cliente está compuesta en su totalidad por equipos Juniper, un controlador inalámbrico WLC8R y 9 Access Point WLA532E distribuidos de la siguiente manera:

- En el piso 2 se encuentran conectados y configurados 4 Access Points y el controlador inalámbrico.
- En el piso 6 se encuentran conectados y configurados 2 Access Points.
- En el piso 7 se encuentran conectados y configurados 3 Access Points.

2.1.3 Red WAN

A nivel WAN el cliente cuenta con una conexión a la red MPLS de Ravec de 2Mbps y una conexión a internet de 20Mbps, ambas conexiones se encuentran físicamente conectadas al switch core.

A continuación se presenta un diagrama de red actual de la red LAN y WLAN:

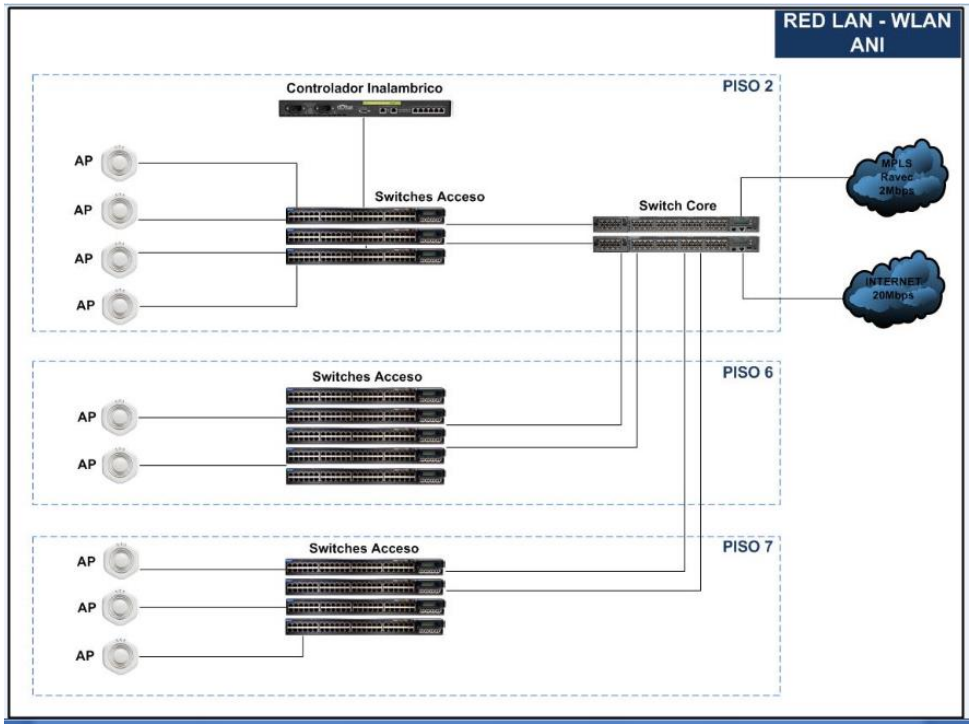

Figura 1 Topología Red LAN WAN

2.2 Telefonía IP - ToIP

El servicio de telefonía IP es suministrado mediante una solución Elastix (Asterix) sin redundancia de procesamiento de llamadas para un número de extensiones efectivo inferior a 50 extensiones.
El servicio de telefonía tiene especial relevancia en las áreas de contacto con la ciudadanía.

2.2.1 Plataforma

Se cuenta con un servidor CentOS release 5.7 sobre el cual se aloja Elastix 2.3.0.

```
[root@pbxani /]# uname -a
Linux pbxani.ani.gov.co 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:22:04 EDT 2011 x86_64 x86_
64 x86_64 GNU/Linux
[root@pbxani /]#
```

Las condiciones actuales de demanda del servicio se prestan sin congestión con los recursos actuales.

Se resumen las características de la PBX a continuación.

Procesamiento de Llamadas	1 Servidor
Extensiones	124 Configuradas 109 Activas en CDRs Julio – Agosto 2013
Conexión PSTN (ETB)	60 Canales SIP Trunk Remoto ETB SIP Server 200.75.51.208
Conexión Lync	30 Canales SIP trunk Remoto Lync Server 192.168.30.21

Tabla 1 Características PBX IP

2.2.2 Topología

La topología como el servicio mismo es bastante simple. A continuación se ilustra la solución y las interacciones principales.

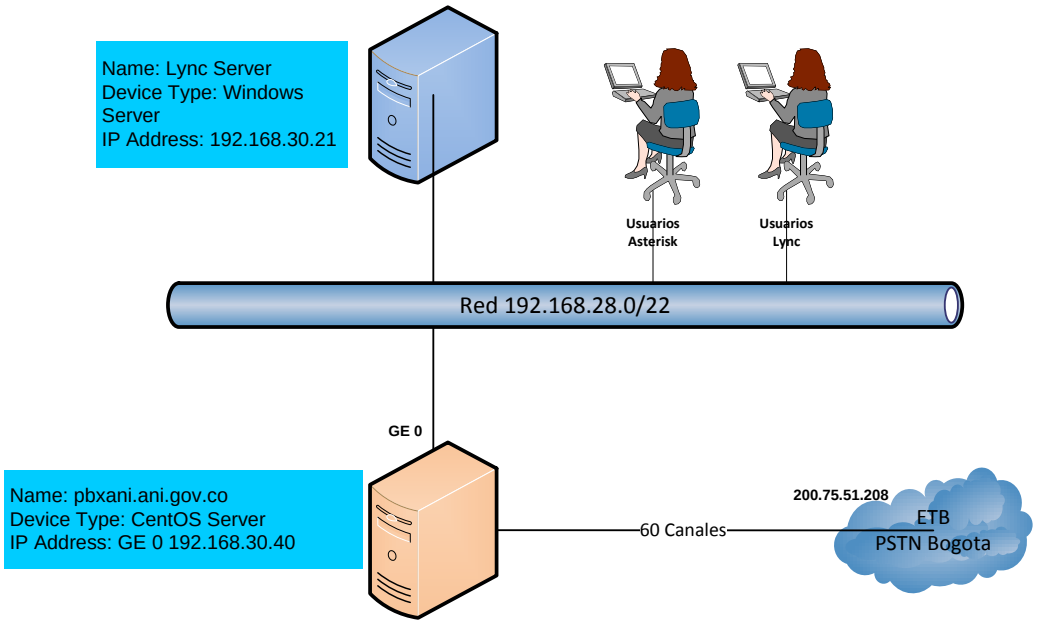

Figura 2 Topología ToIP

2.3 Seguridad Perimetral

El servicio de seguridad perimetral en la red de ANI se presta mediante un firewall basado en Linux CentOS en el feature conocido como IP Tables.
La topología de red en que se encuentra implementado el firewall la permite controlar el tráfico entre los siguientes espacios de direccionamiento:

1. Internet
2. Servidores ANI
3. Red Interna ANI (Este se encuentra enrutado por el switch core de ANI). Dentro de estos se referencian los siguientes:
    a. Red Funcionarios (cableada, WiFi y Teléfonos IP)
    b. Red Wireless Visitantes
    c. Red Gestión Cámaras y Puertas Electrónicas
4. RAVEC. Red de Alta Velocidad del Estado Colombiano

Como resultado de la topología de implementación el firewall es responsable de las traslaciones hacia desde Internet y RAVEC para el apropiado enrutamiento sobre estas redes. Adicionalmente controla el flujo de información desde/hacia la red Interna.
También como resultado de la topología, es imposible controlar el tráfico entre las redes de Funcionarios y Visitantes, ya sea redes cableadas o WiFi.
A continuación se presenta la topología lógica vista desde la perspectiva del firewall y el enrutamiento asociado a este.

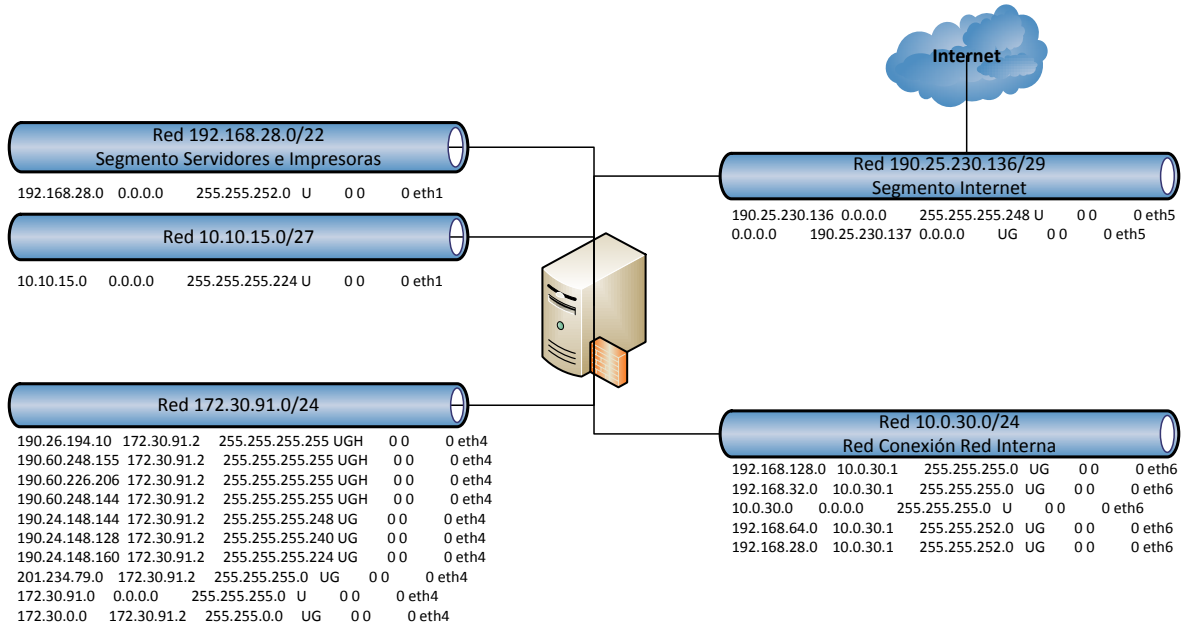

Figura 3 Topología Seguridad Perimetral

2.4 Hardware de servidores

2.4.1 C7000

El chasis HP C7000 es el corazón de la infraestructura tecnológica, allí se aloja casi la totalidad de servidores de la entidad. En estos momentos se encuentra lleno al 40%; es decir, su capacidad de crecimiento está para más del doble con lo que cuenta actualmente La Agencia. En la Figura 1 se aprecia la distribución de dispositivos vistos desde el frente y desde atrás del chasis.

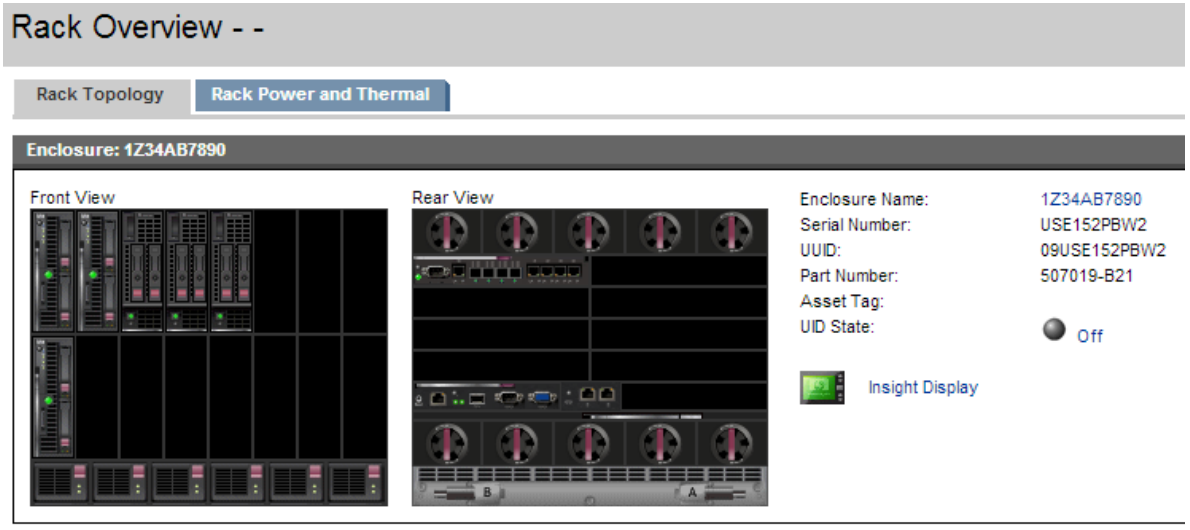

Figura 4 Chasis HP C7000

Cuenta con seis servidores tipo Blade de media altura dispuestos en las bahías 1, 2, 3, 4, 5 y 9; dejando el resto de bahías (10) libres para crecimiento futuro. Seis fuentes de alimentación y diez turbinas de ventilación en configuración redundante, minimizan los riesgos de interrupción del servicio por daño de fuentes o ventiladores además de asegurar el crecimiento futuro a carga completa.

Una de las partes importantes para la gestión de sistemas TI es el firmware de cada subsistema. A continuación se detallan todos los componentes involucrados en la solución y las respectivas versiones de firmware presentes en cada uno de ellos.

Bay	Model	Manufacturer	Serial Number	Part Number	Spare Part Number	Firmware Version
1	BladeSystem c7000 DDR2 Onboard Administrator with KVM	HP	OB18BP3854	456204-B21	503826-001	3.70 Oct 01 2012

Tabla 2 C7000 Firmware Information

Complementan al chasis el sistema de administración remota ILO y un Ethernet Blade Switch sin redundancia. La Tabla 2 muestra las versiones de firmware y la actualización disponible para el ILO, display y turbinas que componen en sistema C7000.

Device Model	Current Firmware Version	Available Firmware Version
BladeSystem c7000 Onboard Administrator Tray	1.7	1.7
BladeSystem c7000 Insight Display	2.5.3	2.5.3
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4
Active Cool 200 Fan	2.9.4	2.9.4

Tabla 3 C7000 Component Firmware Information

La Tabla 3 muestra la información de firmware de los blades para ROMs, iLO y Power Management Controllers.

Bay	Device Model	Firmware Component	Current Version
1	**ProLiant BL460c G7**	System ROM	I27 01/29/2011
		iLO3	iLO3 1.20 Mar 14 2011
		Power Management Controller	1.6
2	**ProLiant BL460c G7**	System ROM	I27 05/05/2011
		iLO3	iLO3 1.15 Oct 22 2010
		Power Management Controller	1.6
3	**ProLiant BL460c Gen8**	System ROM	I31 08/20/2012
		iLO4	iLO4 1.13 Nov 08 2012
		Power Management Controller	3.0
4	**ProLiant BL460c Gen8**	System ROM	I31 08/20/2012

		iLO4	1.13 Nov 08 2012
		Power Management Controller	3.0
5	**ProLiant BL460c Gen8**	System ROM	I31 08/20/2012
		iLO4	1.13 Nov 08 2012
		Power Management Controller	3.0
6	**ProLiant BL460c G7**	System ROM	I27 01/29/2011
		iLO3	iLO3 1.20 Mar 14 2011
		Power Management Controller	1.6

Tabla 4 C7000 Blades Firmware

La información de firmware del Ethernet Blade Switch no pudo ser recolectada.

Bay	Device Model	Firmware Version
1	GbE2c Layer 2/3 Ethernet Blade Switch	Not Available

Tabla 5 Ethernet Blade Switch Firmware

Para la gestión de activos es importante contar con un inventario actualizado de servidores y los subsistemas asociados, las tablas siguientes resumen localización, modelo, número de serie y número de parte. Esto también agiliza el proceso de solicitud de garantías al tener consolidado en un solo sitio datos requeridos por el fabricante.

Part	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
Enclosure	BladeSystem c7000 Enclosure G2	HP	USE152PBW2	507019-B21	N/A
Enclosure Midplane	N/A	HP	N/A	N/A	519345-001
Onboard Administrator Tray	BladeSystem c7000 Onboard Administrator Tray	HP	OJ18BK3140	N/A	519346-001
Power Input Module	HP AC Module, Three Phase	HP	N/A	N/A	413495-001

Tabla 6 Enclosure FRU Information

Bay Number	Model	Manufacturer	Serial Number	Part Number	System Board Spare Part Number
1	ProLiant BL460c G7	HP	MXQ108061P	637391-B21	605659-001
2	ProLiant BL460c G7	HP	MXQ108061W	637391-B21	605659-001
3	ProLiant BL460c Gen8	HP	MXQ249005J	666159-B21	704709-001
4	ProLiant BL460c Gen8	HP	MXQ249005N	666159-B21	704709-001
5	ProLiant BL460c Gen8	HP	MXQ249005C	666159-B21	704709-001
9	ProLiant BL460c G7	HP	MXQ1090NVD	637391-B21	605659-001

Tabla 7 Blade FRU Information

Bay	Mezz Slot	Model	Manufacturer	Serial Number	PCA Serial Number	Part Number	Spare Part Number
3	FLB 1	HP FlexFabric 10Gb 2-port 554FLB Adapter	HP	CN7244V00Y	WD2ABR0129	647586-B21	649940-001
4	FLB 1	HP FlexFabric 10Gb 2-port 554FLB Adapter	HP	CN7244V00R	WD2ABR1526	647586-B21	649940-001
5	FLB 1	HP FlexFabric 10Gb 2-port 554FLB Adapter	HP	CN7244V00T	WD2ABR1655	647586-B21	649940-001

Tabla 8 Blade Mezzanine FRU Information

La Tabla anterior nos muestra que no todos los blades tienen instalador adaptador de fibra, esto es un limitante a la hora de incluir todos los servidores en una solución tipo SAN.

Bay Number	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
1	GbE2c Layer 2/3 Ethernet Blade Switch	HP	MY32075UXY	438030-B21	438475-001

Tabla 9 Interconnect FRU Information

Bay Number	Model	Part Number	Spare Part Number
1	Active Cool 200 Fan	412140-B21	413996-001
2	Active Cool 200 Fan	412140-B21	413996-001
3	Active Cool 200 Fan	412140-B21	413996-001
4	Active Cool 200 Fan	412140-B21	413996-001
5	Active Cool 200 Fan	412140-B21	413996-001
6	Active Cool 200 Fan	412140-B21	413996-001
7	Active Cool 200 Fan	412140-B21	413996-001
8	Active Cool 200 Fan	412140-B21	413996-001
9	Active Cool 200 Fan	412140-B21	413996-001
10	Active Cool 200 Fan	412140-B21	413996-001

Tabla 10 Fan FRU Information

Bay Number	Model	Part Number	Serial Number	Spare Part Number
1	HP 2400W HE PSU	499253-B21	5AGUD0AHL1R434	500242-001
2	HP 2400W HE PSU	499253-B21	5AGUD0AHL1R432	500242-001
3	HP 2400W HE PSU	499253-B21	5AGUD0AHL1R433	500242-001
4	HP 2400W HE PSU	499253-B21	5AGUD0AHL1R431	500242-001
5	HP 2400W HE PSU	499253-B21	5AGUD0AHL1R42U	500242-001
6	HP 2400W HE PSU	499253-B21	5AGUD0AHL1R42X	500242-001

Tabla 11 Power Supply FRU Information

Model	Spare Part Number	Manufacturer
BladeSystem c7000 Insight Display	441203-001	HP

Tabla 12 Insight Display FRU Information

2.4.2 Blades

Como se indicó anteriormente, el sistema C7000 cuenta con seis servidores tipo Blade, tres BL 460c G7 y tres BL 460 Gen8. En estos servidores se ha virtualizado casi la totalidad de la plataforma de infraestructura de **La Agencia**. La tabla siguiente resume la configuración de procesamiento y memoria de los servidores y su hostname.

Bay	Model	Hostname	CPU	Memoria
1	BL460c G7	VIRANI6	Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Not Present	36 GB
2	BL460c G7	VIRANI1	Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Not Present	6 GB
3	BL460c Gen8	VIRANI2	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (8 Cores) CPU2 Not Present	32 GB
4	BL460c Gen8	VIRANI3	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (8 Cores) CPU2 Not Present	32 GB
5	BL460c Gen8	VIRANI4	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (8 Cores) CPU2 Not Present	32 GB
9	BL460c G7	VIRTUALANI2	Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Not Present	36 GB

Tabla 13 Blades CPU y Memoria

2.4.3 Servidor VIRANI5 (Stand-alone)

Adicional al chasis C7000 **La Agencia** cuenta con un servidor ProLiant DL 380 G7 con Windows 2012 Datacenter con el rol de Hyper-V instalado. Este servidor cuenta con doble procesador de 6 núcleos cada uno.

Model	Hostname	CPU	Memoria
DL380 G7	VIRANI5	CPU1 Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores)	30 GB

Tabla 14 Stand-alone server

Este servidor cuenta con dos arreglos de discos, el primero de 840 GB en RAID1 y el segundo de 4.1TB en RAID5. Sobre estos se encuentran alojadas las máquinas FWINCO, ORFEO, ORFEOP, SVEXH2 y SVEXCH03.

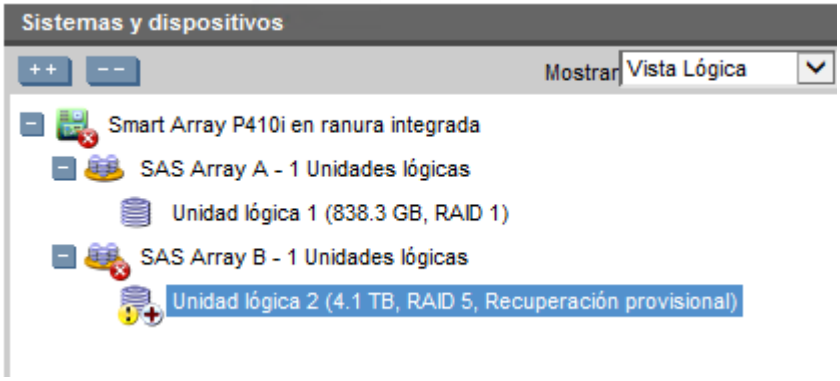

Figura 5 VIRANI5 Discos

Se recomienda revisar el error de arreglo de discos que informa la controladora.

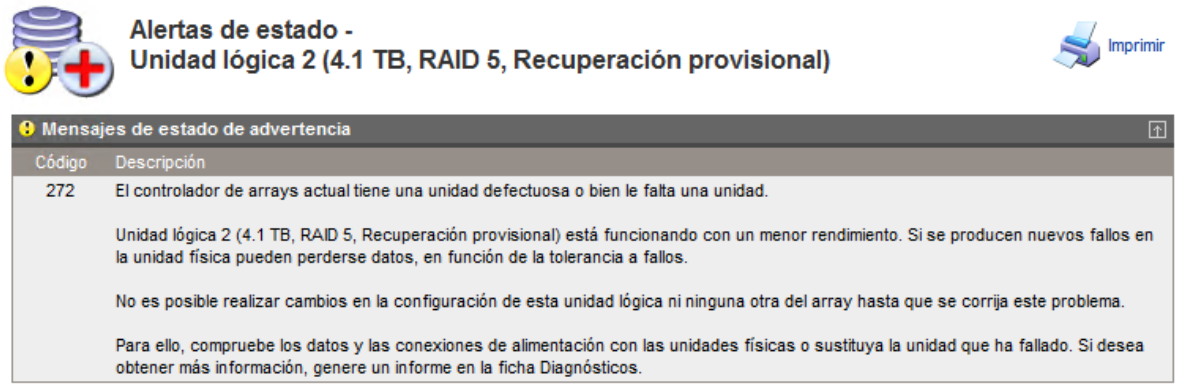

Figura 6 Error controladora

Error 272. El controlador de arrays actual tiene una unidad defectuosa o bien le falta una unidad.

Unidad lógica 2 (4.1 TB, RAID 5, Recuperación provisional) está funcionando con un menor rendimiento. Si se producen nuevos fallos en la unidad física pueden perderse datos, en función de la tolerancia a fallos.

No es posible realizar cambios en la configuración de esta unidad lógica ni ninguna otra del array hasta que se corrija este problema.

Para ello, compruebe los datos y las conexiones de alimentación con las unidades físicas o sustituya la unidad que ha fallado. Si desea obtener más información, genere un informe en la ficha Diagnósticos.

2.5 Infraestructura Tecnológica

2.5.1 Virtualización

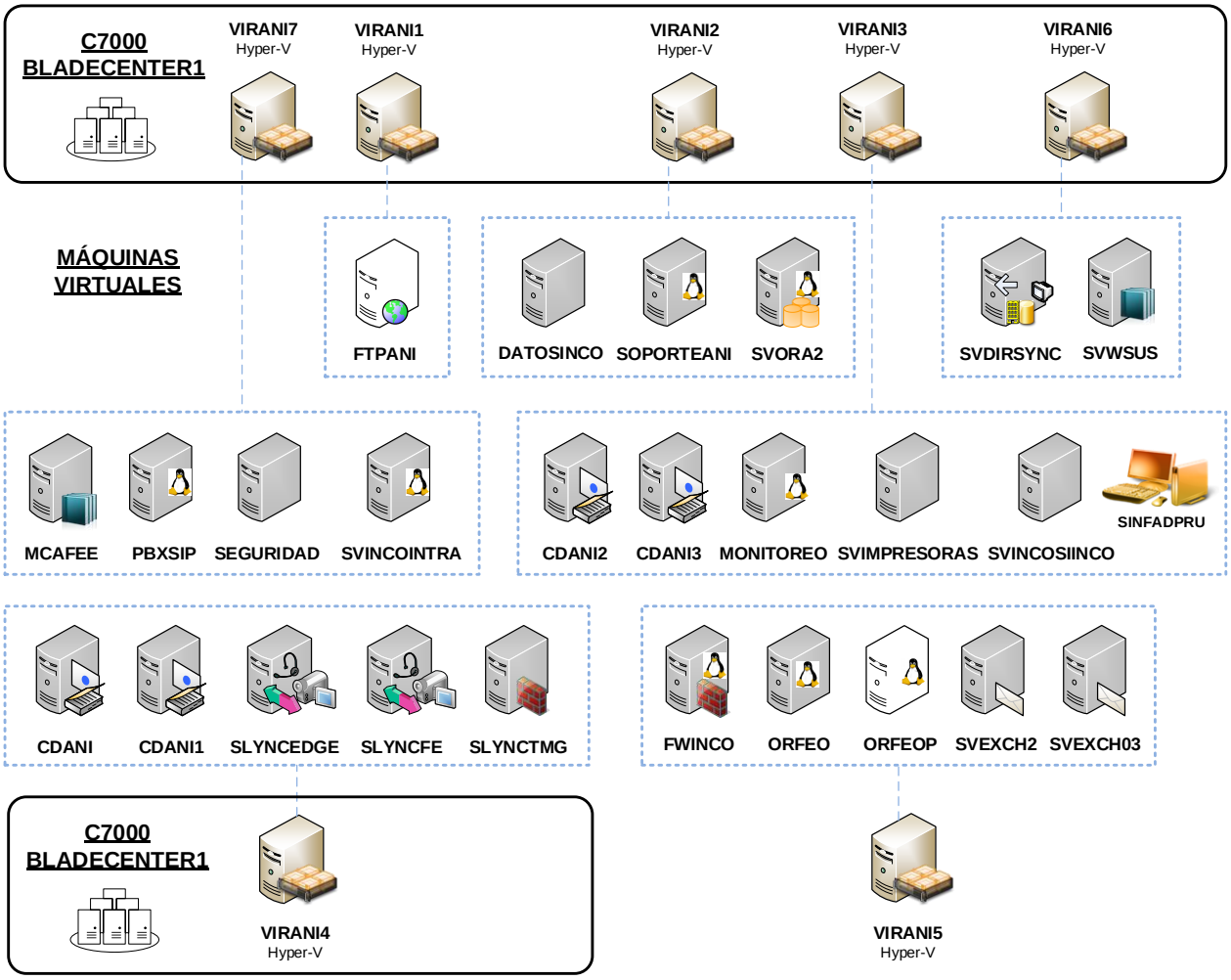

Figura 7 Infraestructura Actual

La figura 2 muestra la plataforma de virtualización existente en **La Agencia** y la distribución de máquinas virtuales sobre los nodos reales. En el C7000 se alojan seis blades todos con el servicio de Hyper-V configurado, en la gráfica son las de nombre **VIRANIX**. Adicional hay un servidor real fuera del *enclosure* **VIRANI5** también con el servicio de Hyper-V instalado. Las máquinas en tono gris son virtuales y las blancas son las que se encuentran apagadas. Adicional a éstas existe una máquina virtual Windows XP.

Todas las máquinas virtuales corren en el almacenamiento directo de los servidores.

2.5.2 Almacenamiento

La Agencia en estos momentos no cuenta con un tipo de almacenamiento SAN. Todo se maneja en discos locales de servidores y los respaldos en discos externos.

2.5.3 Directorio Activo

La Agencia cuenta con un bosque de un dominio **inco.local**, nivel de funcionalidad Windows 2008 R2. Consta de cuatro controladoras de dominio con los roles de FSMO localizados en CDANI1, la funcionalidad del dominio también es Windows 2008 R2

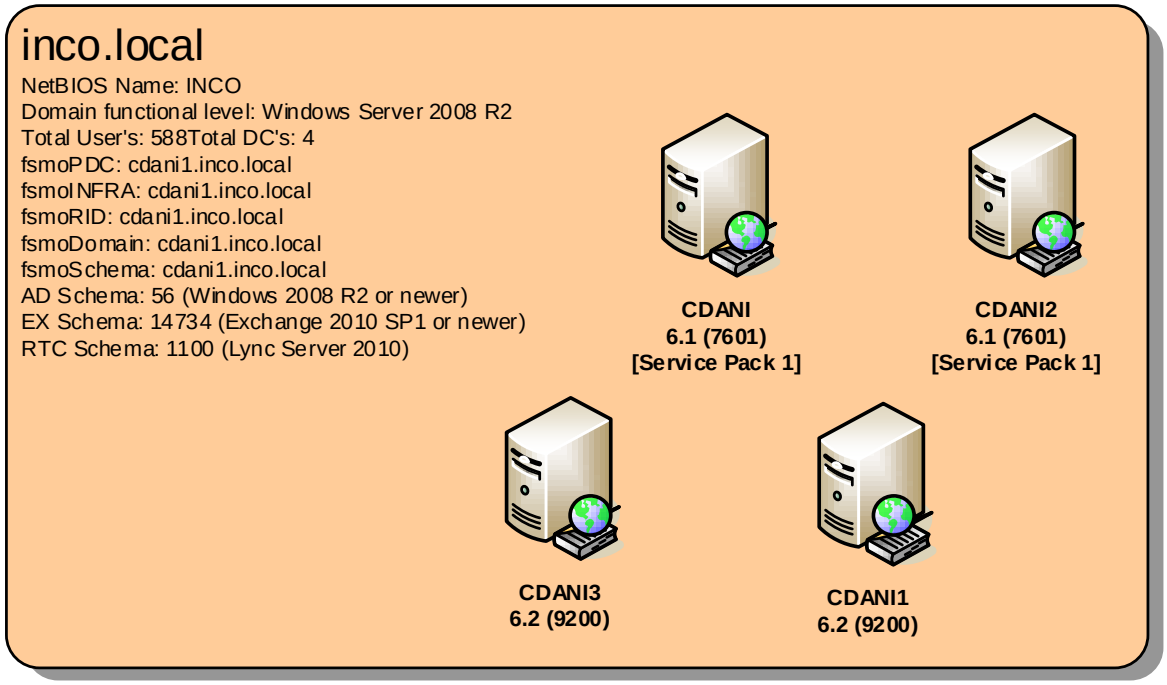

Figura 8 Bosque inco.local

El dominio inco.local no tiene relaciones de confianza con ningún otro dominio, no tiene definidos sufijos UPN.

2.5.3.1 Site Topology

El dominio **inco.local** tiene un solo *site* llamado **Nombre-predeterminado-primer-sitio** que es el nombre puesto por defecto en la creación del directorio activo. Este *site* contiene la cuatro controladoras en replicación como muestra la Figura 3, toda las controladoras de dominio son Global Catalog Server.

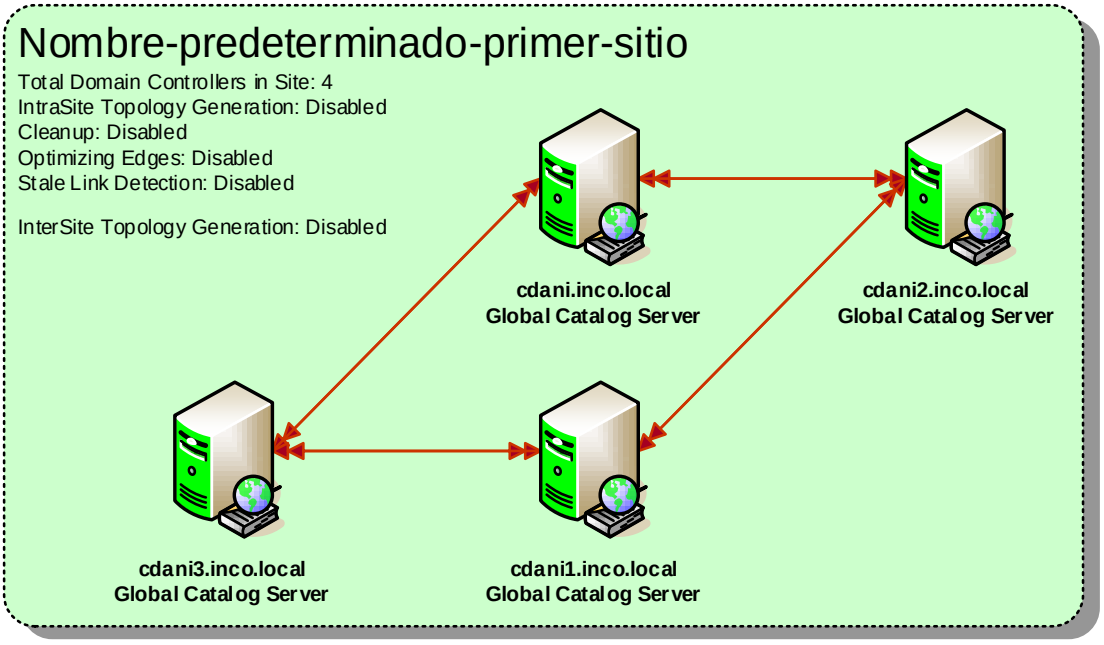

Figura 9 Site Topology

El *site* no tiene definidas subredes IP.

2.5.3.2 Organizational Units

El dominio **inco.local** presenta una estructura básica de unidades organizacionales donde solo se ha definido un OU **ANI** y dentro de esta siete OUs hijas sin usuarios. Adicional tiene unas OUs llamadas **Sin Politicas, Retirados**, **Servidores** y **Sistemas**. En la OU **ANI** están casi la totalidad de usuarios y computadores del dominio.

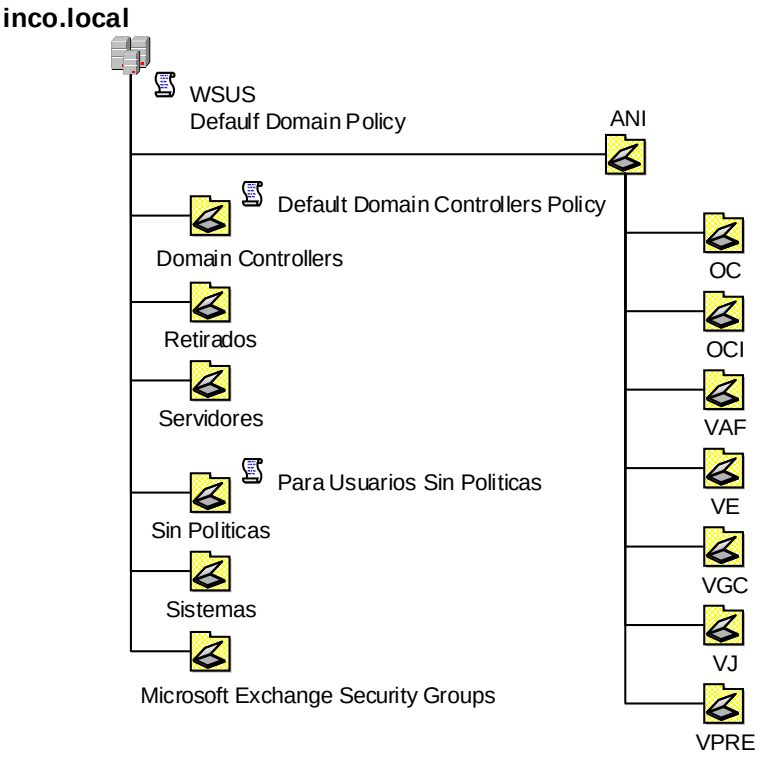

Figura 10 OUs

2.5.4 Exchange

La organización cuenta con dos servidores de Exchange 2010 SP1. En estos momentos se encuentra con una configuración híbrida para suavizar la migración a Office 365.

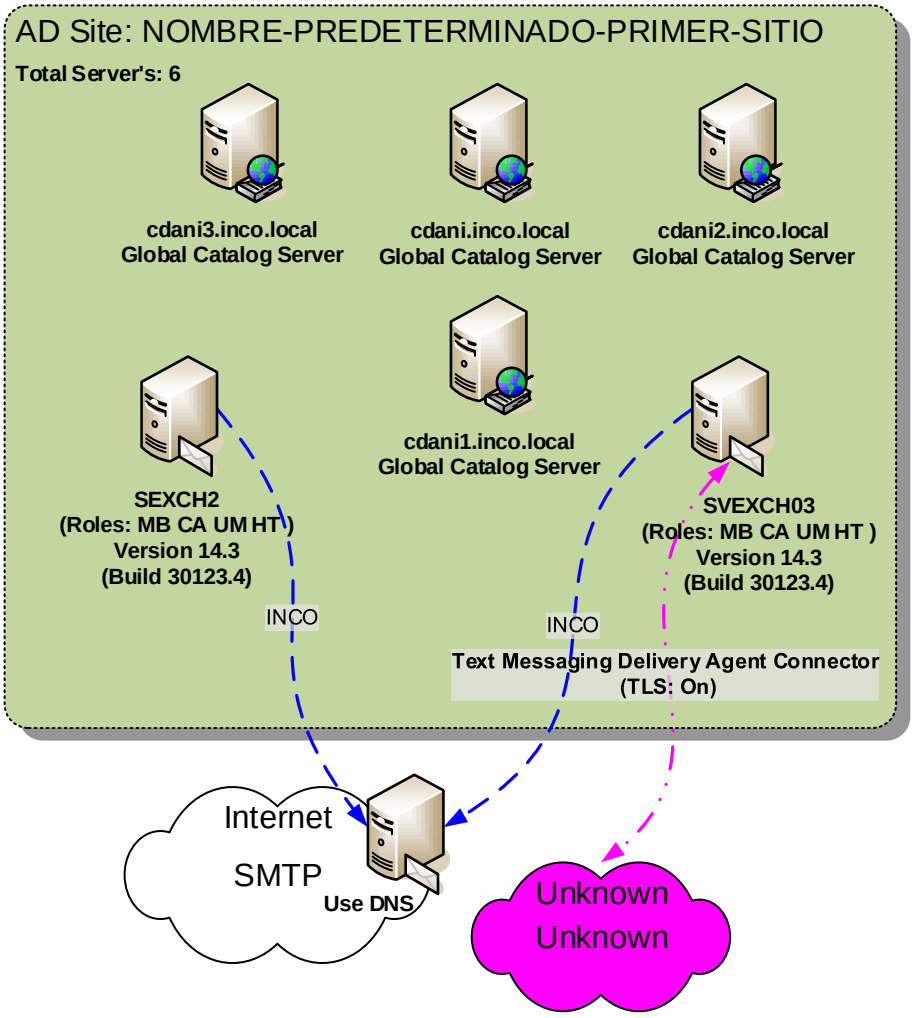

Figura 11 Exchange

2.5.5 Lync

La topología de Lync Server se compone de tres servidores: **SLYNCTMG** para publicar el servicio en Internet, SLYNCEDGE para la comunicación al exterior y **SLYNCFE** para el acceso a los clientes corporativos.

3. ANÁLISIS Y RECOMENDACIONES

3.1 Red

En visita realizada a la Agencia Nacional de Infraestructura (ANI) el cliente informa que en ocasiones algunos equipos de usuario (PCs de Escritorio, Equipos Portátiles) que se conectan a la red LAN y WLAN presentan conectividad limitada o nula.

Se realiza una revisión en sitio en conjunto con el cliente donde se observa lo siguiente:

- El servicio DHCP se encuentra configurado directamente en el switch core.
- Los pool DHCP que se tienen configurados son los siguientes:

  192.168.64.0/22 Red Wireless Funcionarios, Red Cableada Funcionarios, Red Teléfonos IP
  192.168.128.0/24 Red Wireless Visitantes
  192.168.30.0/24 Red Servidores e Impresoras
  192.168.32.0/24 Red Gestión Cámaras y Puertas Electrónicas
  10.0.30.0/24 Red Conexión Internet
  10.1.1.0/24 Red Gestión Equipos de Red

- Del segmento de red 192.168.64.0/22 (Red Wireless Funcionarios, Red Cableada Funcionarios, Red Teléfonos IP), solo se están anunciando las direcciones IP 192.168.64.1 a la 192.168.66.255 en el servidor DHCP, el pool de direcciones IP 192.168.67.0 a la 192.168.67.254 no está siendo anunciado por el servidor DHCP, cuando se presenta conectividad limitada o nula en algún equipo de usuario final, el cliente tiene que configurar una dirección IP de forma estática en el equipo del usuario, normalmente la asignación se realiza del pool de direcciones IP que no está siendo anunciado por el servidor DHCP, de esta manera el problema queda solucionado.

- Según información del cliente la concurrencia máxima de usuarios que se pudiera presentar en cada uno de los segmentos de red seria:

  Funcionarios Red Cableada 400 Usuarios
  Funcionarios Red Wireless 1000 Usuarios
  Visitantes Red Wireless 150 Usuarios
  Servidores Segmento /24 no presentaría ningún inconveniente
  Impresoras 20 Impresoras
  Teléfonos IP 30 Teléfonos IP

- El cliente informa que en el piso 2 se encuentra conectado un HUB a la red el cual realiza la conexión de 3 impresoras.

- La conexión a la red wireless de funcionarios se realiza por medio de una clave fija por medio del sistema WPA2-PSK.

- La conexión a la red wireless de visitantes se realiza por medio de una clave fija por medio del sistema WPA2-PSK.

- No se sabe la ubicación exacta de cada AP.

3.1.1 Conclusiones

Según la información suministrada por el cliente y el levantamiento realizado en sitio con acompañamiento de los ingenieros que se encargan de administrar la red LAN y WLAN de la Agencia Nacional de Infraestructura (ANI) se logró observar:

- A nivel físico se cuenta con un buen diseño de red, donde se cuenta con doble enlace físico entre cada switch de acceso y el switch core, cada enlace físico es de 10Gbps.

- Todos los switches de acceso se encuentran conectados y configurados en stack, igualmente se observó que el stack en todos los casos se encuentra cerrado.

- Se cuenta con redundancia física en el switch core, donde se tienen dos switches conectados y configurados en stack.

- En referencia a la cobertura de la red inalámbrica no se puede realizar ningún diagnostico ya que el cliente no tiene los diagramas de radiación de la red inalámbrica.

- A nivel lógico se observan algunas anomalías que se serán descritas más a detalle en el ítem de recomendaciones.

3.1.2 Recomendaciones

- Implementar una estandarización de nombres de todos los equipos de red. Con esto se puede llevar un mejor control de la red, además de una mejor administración de la red.
  Por ejemplo:

Switch Core	SW_CORE
Switches de Acceso	SW_ACCESO_PISO_X
Controlador Inalámbrico	CONTROLADOR_INALAMBRICO
Access Points	AP_X_PISO_X_SALA_DE_REUNIONES

- Realizar la implementación de una herramienta de monitoreo de red, con esto se podrá tener un mejor control sobre la red, ser proactivo ante cualquier incidente que se pueda presentar, llevar un control y estadísticas de consumos de anchos de banda (BW), cargas de cpu, memoria, perdida de paquetes, colisiones, errores en interfaces, entre otras.

3.1.2.1 Red LAN

- Realizar la configuración del servicio DHCP en un servidor dedicado para este servicio y eliminar esta configuración del switch core, este tipo de configuraciones no es recomendable realizarlas en switches a menos de que sea una asignación muy pequeña de direcciones IP.

- Configurar las impresoras en un segmento de red exclusivo para impresoras, no realizar la asignación de direcciones IP a las impresoras en el mismo segmento de red de los servidores.

- Realizar una mejor asignación de segmentos de red para ser configurados a los diferentes usuarios y equipos de la red. Según las necesidades expuestas por el cliente se recomienda crear y asignar los segmentos de red de la siguiente manera.

Funcionarios Red Cableada	/23
Red Teléfonos IP	/24
Red Servidores	/24
Red Cámaras y Puertas Electrónicas	/24
Red Impresoras	/24
Red Gestión Equipos de Red	/24
Funcionarios Red Wireless	/22
Red Wireless Visitantes	/24
Red Conexión Internet	/29
Red Conexión Ravec	/29

NOTA: Esta recomendación se realiza según requerimientos del cliente por sesiones concurrentes que se presentaría en cada uno de los segmentos de red descritos en el ítem #4.

- Realizar la desinstalación del Hub conectado en el piso 2, y realizar la conexión de cada impresora directamente al switch de acceso de ese piso.

- Realizar la configuración del protocolo LACP (Link Aggregation Control Protocol) entre cada switch de acceso de cada piso y el switch core, con esto se lograra duplicar el ancho de banda de 10Gbps a 20Gbps sobre los enlaces troncales entre pisos, además de tener una conmutación de forma inmediata si alguno de estos enlaces presente algún inconveniente, el cual no será perceptible para los usuarios finales.

- Definir el switch core como el root switch del protocolo STP (Spanning Tree Protocol).

- Configurar todos los puertos que no sean puertos troncales como edge ports y todos los puertos troncales como no-edge ports, para de esta manera evitar que se presenten cambios topológicos continuos en la estructura del protocolo STP (Spanning Tree Protocol).

- Sobre los enlaces troncales tagear únicamente las vlan que por allí se necesiten, con esto se lograra que las tormentas de broadcast sean mucho menores y el performance sobre la red mejore de manera considerable.

3.1.2.2 Red Wireless

- Realizar la integración del controlador inalámbrico con el Directorio Activo, para de esta manera implementar que la autenticación de los usuarios de la Agencia Nacional de Infraestructura (ANI) se realice por medio de autenticación contra el AD.

- Realizar la autenticación de los usuarios visitantes a la red inalámbrica por medio del portal captive.

- Colocar la ubicación exacta de cada Access Point en los planos de los pisos 2, 6 y 7 en el controlador inalámbrico para de esta manera observar el diagrama de radiación y cobertura de cada Access Point, con esto se podrá observar la cobertura total de la red inalámbrica, la cantidad de equipos que se conectan a cada Access Points y la velocidad de transmisión de cada uno de ellos.

- Realizar la conexión del controlador inalámbrico directamente al switch core.

NOTA: Tener muy presente que si la concurrencia máxima de usuarios que se conectaran a la red inalámbrica es la indicada en el ítem # 4, se tendría que

realizar la instalación de más Access Points, ya que con la cantidad de Access Points actuales no se podría cubrir esa demanda.
Según el datasheet del controlador inalámbrico WLC8R, la cantidad máxima de Access Points que este equipo puede administrar es de 12, por tal motivo muy posiblemente se tendría que realizar el cambio del controlador inalámbrico.

3.2 Telefonía IP - ToIP

Dentro de las características actuales de la implementación se tienen los siguientes aspectos relevantes:

- Espacio de direccionamiento compartido por clientes de telefonía, clientes de datos y servidores.

- La PBX presenta que el procesamiento de CPU y uso de memoria no alcanzan el 10%. De igual manera el espacio en disco no llega al 5% de ocupación

- Se observa la siguiente distribución de llamadas entrantes y salientes con respecto a las interconexiones Lync y PSTN-ETB

	Periodo	Entrantes	Salientes
ETB	Mes	15.692 (55%)	13.097 (45%)
ETB	Trimestre	47.246 (55%)	38.091 (45%)
ETB	Semestre	82.296 (54%)	71.336 (46%)
Lync	Mes	446 (83%)	94 (17%)
Lync	Trimestre	1.399 (70%)	586 (30%)
Lync	Semestre	3.287 (50%)	3.258 (50%)

Tabla 15 Volumen de llamadas PSTN y Lync

Con lo anterior se establece una relación 50/50 para las llamadas contra la PSTN-ETB y una relación creciente 70/30 contra Lync. Esta medición deberá hacerse más fuerte en lync en la medida que se masifique el servicio como es la visión de ANI.

- En cuanto a la concurrencia de llamadas hacia/desde la PSTN se encontró que los canales actuales (60) son suficientes. De hecho se realizó un ajuste menor pues solo se estaban considerando 30 canales para la salida de llamadas. Esto no ha afectado la experiencia de los usuarios por cuanto las llamadas concurrentes no llegan a ser más de 30.

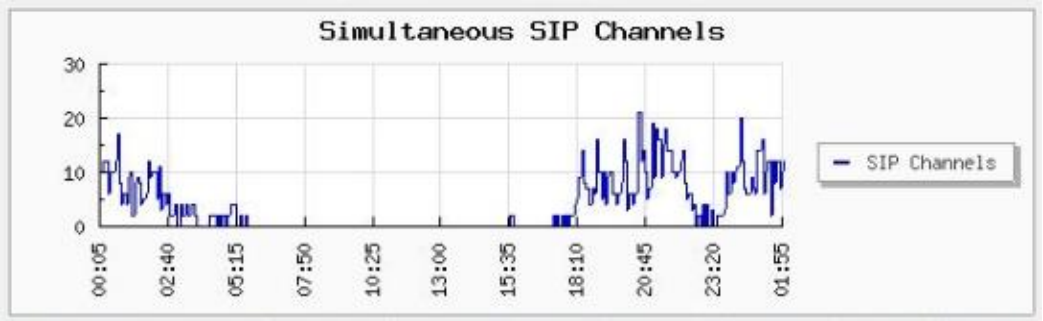

Figura 12 Concurrencia de Llamadas SIP

- Se manifiesta de parte de los usuarios la incapacidad de enviar FAX mediante el sistema en la actualidad.

3.2.1 Conclusiones

Según la información suministrada por el cliente y el levantamiento realizado en sitio con acompañamiento de los ingenieros que se encargan de administrar el servicio de ToIP de la Agencia Nacional de Infraestructura (ANI) se logró observar:

- La redundancia de procesamiento de llamadas recae en la configuración de los servidores blade.

- La plataforma instalada cubre y provee los servicios básicos de telefonía (a excepción de la salida de FAX) requeridos por ANI.

- La perspectiva de ANI y su integración con los productos Microsoft tiende a reemplazar/migrar la totalidad de los servicios prestados por elastix hacia lync.

3.2.2 Recomendaciones

- La plataforma actual está sobre dimensionada en cualidades de procesamiento. Se hace pertinente una depuración de las configuraciones de usuarios-extensiones y otras parametrizaciones que no tienen uso efectivo en la solución actual

- Mientras la solución de telefonía sea prestada por Elastix se debe asegurar que la plataforma de cómputo en los servidores blade, brinde las condiciones de alta disponibilidad para garantizar la continuidad del servicio. Se deben ejecutar los simulacros de falla que depuren los procedimientos y acciones de contingencia.

- El espacio de direccionamiento IP debe ser segmentado adecuadamente para la implementación de estrategias de seguridad y diagnóstico de fallos estándar.

- Es de interés para la organización como ente público, utilizar el auto attendant en conjunto con el IVR y un manejo de colas de llamadas en las llamadas entrantes, para la divulgación de mensajes al público en general. Con esto se logrará que los usuarios se informen durante los tiempos de espera mientras sus llamadas son atendidas.

- La única carencia de servicio actual (servicio de FAX) debe depurarse y de preferencia ser integrada con el correo electrónico. Según la revisión realizada, bastaría con realizar depuración de la configuración y validación de módulos para el funcionamiento básico de Fax. La integración con el correo electrónico tiene otras variables que pueden dar mayor complejidad a la puesta en marcha del servicio.

3.3 Seguridad Perimetral

La revisión detallada de las políticas implementadas destaca el uso de SPI en el control de tráfico, lo cual garantiza que las políticas verifican el estado de las conexiones más allá que solo los servicios de capa 4 y direcciones de capa3.
Las condiciones de desempeño del firewall son óptimas. No se tienen problemas con el procesamiento y/o consumo de memoria en las condiciones actuales.

3.3.1 Conclusiones

Del análisis de la información en Seguridad Perimetral de la Agencia Nacional de Infraestructura (ANI) se logró observar:

- Las características de alta disponibilidad recaen sobre la plataforma de cómputo (blade) pues no se cuenta con un cluster para el servicio de seguridad perimetral

- En la topología actual el firewall controla adecuadamente los flujos de tráfico que tiene a su alcance (Internet, RAVEC, Red Interna, Servidores)

- El crecimiento en ancho de banda hacia el segmento de servidores puede ser una limitante, debido a la arquitectura de los servidores blade y del switch core.

- No se cuenta en la actualidad con servicios de IPS, filtrado de contenido, control Anti-X y servicios de VPN (IPSEC o SSL) dentro de la capa de seguridad perimetral.

3.3.2 Recomendaciones

- Implementar el concepto de clúster o Alta Disponibilidad en el servicio de seguridad perimetral, eliminando puntos únicos de falla para este servicio. Clave por cuanto esta capa controla la interacción con el mundo vía Internet y RAVEC.

- Implementar una solución que permita el control de navegación y/o acceso a los recursos con políticas de control de tráfico autenticadas en integración contra el directorio activo de ANI

- Integrar servicios de seguridad con una solución UTM que permitirá brindar dentro de la capa de seguridad perimetral entre otros, los siguientes servicios/características:
  - Firewall y VPN
  - Intrusion Prevention System (IPS)
  - Antimalware/Antivirus/Antispyware
  - Application Control
  - Web Filtering
  - Antispam

- Integrar una herramienta de reportes y análisis de logs para la plataforma de seguridad perimetral que facilite el análisis de logs por parte del administrador para así tomar decisiones efectivas ante los retos que supone el aseguramiento de los recursos de red de ANI.

3.4 Hardware de servidores

Como pilar de toda la infraestructura tecnológica es recomendable hacer una gestión proactiva del *enclosure* C7000 dentro de las tareas a realizar están:

- Cambiar el nombre del chasis C7000 por un nombre amigable y acorde a un estándar definido.

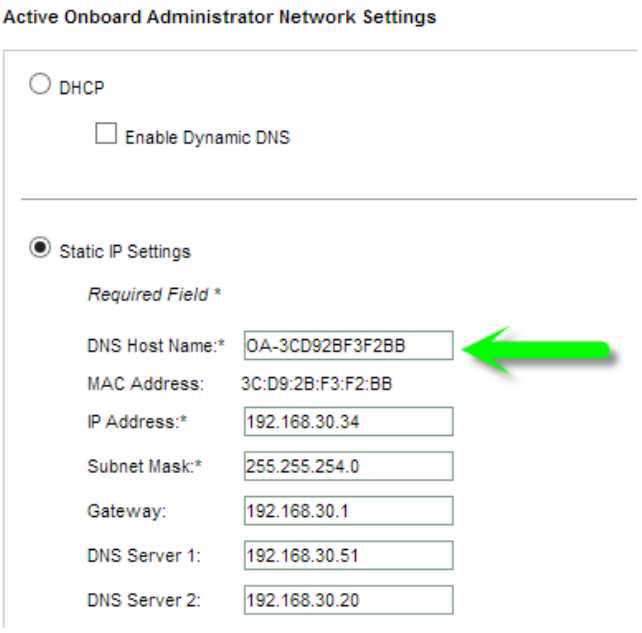

Figura 13 C7000 IP Settings

- Configurar parámetros de monitoreo como envío de mail de alerta.

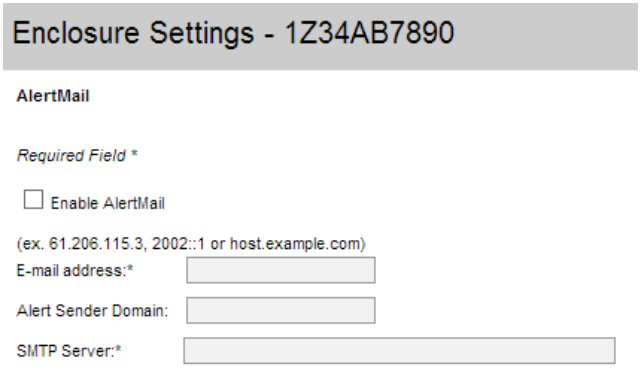

Figura 14 C7000 AlertMail

- Definir una entidad de sincronización de tiempo para la entidad y configurar los parámetros de NTP en el C7000.

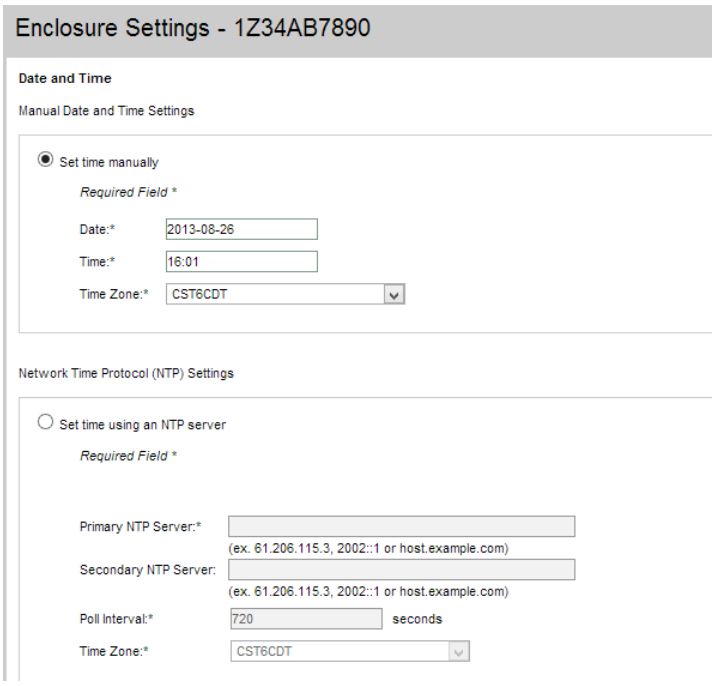

Figura 15 C7000 NTP Settings

- Un hito importante en seguridad es restringir los protocolos de gestión del *enclosure,* actualmente están habilitados todos los protocolos de administración haciendo bastante vulnerable el chasis y por consiguiente toda la plataforma. Se recomienda dejar solo administración HTTPS y en la pestaña "Trusted Hosts"; habilitar "IP address access restriction" y especificar únicamente las direcciones desde donde se va a poder gestionar el C7000.

Figura 16 C7000 Protocol Restrictions

- Asignar nombres de host a las iLOs de los blades basándose en el estándar definido y asignar direcciones IP contiguas en un rango

determinado, por ejemplo para las iLOs desde la 192.168.0.1 hasta la 192.168.0.20, suponiendo que el C7000 se ocupara total a futuro. Esto garantiza la fácil gestión y recordación de las IPs involucradas en la administración.

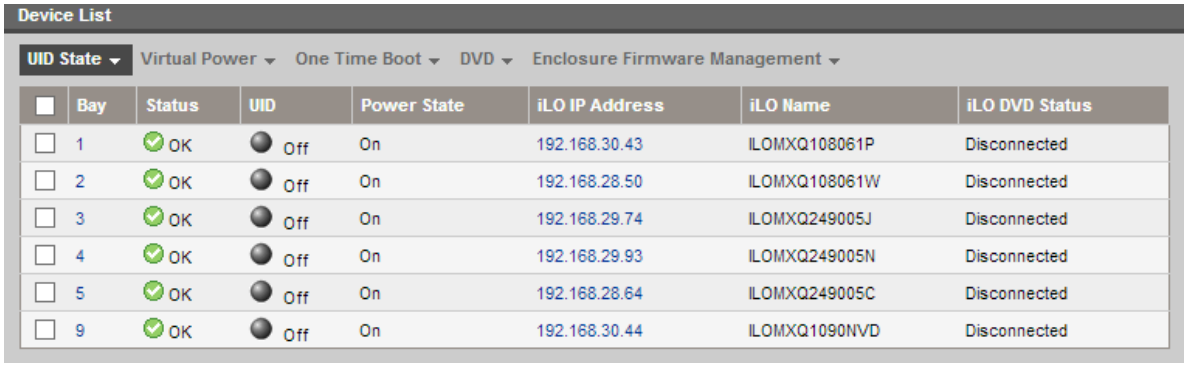

Figura 17 C7000 iLOs

- Actualizar el firmware del C7000 que se encuentra en la penúltima versión, se puede descargar de acá: http://goo.gl/Am2kIZ

- Los blades tienen firmware bastante desactualizado, se recomienda averiguar cuales son las últimas versiones y aplicarlas.

- En estos momentos en C7000 no tiene redundancia a nivel de LAN Switch convirtiendo este dispositivo en un punto único de falla, en caso de falla de este switch, todo el *enclosure* incluyendo los servidores blades dentro de este quedarían aislados de la red. Es muy importante adquirir otro LAN Switch y configurarlos en alta disponibilidad.

- Se observó que solo los blades de las bahías 3, 4 y 5 poseen HP FlexFabric, este dispositivo es el que le da acceso a una solución tipo SAN con tecnología de *fiber channel,* adicional cada blade solo cuenta con un puerto de conexión. Para sistemas con alta tolerancia a fallos se recomiendan dos puertos por servidor blade, es decir se requieren otros tres HP FlexFabric para los que ya poseen este puerto y seis más para los blades ubicados en las bahías 1, 2 y 9 que no cuentan con este dispositivo.

- Es importante para la gestión y agilidad en garantías, contar con los números y fechas de vencimiento y de los contratos de mantenimiento HP Care Pack. Mantener las suscripciones al día y renovar contratos, así se estará cubierto en caso de calamidad.

3.5 Crecimiento horizontal y vertical

En la Tabla 13 se evidencia que todos los servidores blade pueden crecer verticalmente tanto en memoria como en procesador. Todos aceptan un segundo procesador incrementando el poder de cómputo sin gastos adicionales y todos son expandibles en memoria, los BL460 G7 soportan hasta 384 GB de RAM y los BL460c Gen8 hasta 512 GB de RAM, incrementando el poder de virtualización de forma aritmética.

Bay	Model	Hostname	CPU	Memoria
1	BL460c G7	VIRANI6	Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Not Present	36 GB
2	BL460c G7	VIRANI1	Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Not Present	6 GB
3	BL460c Gen8	VIRANI2	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (8 Cores) CPU2 Not Present	32 GB
4	BL460c Gen8	VIRANI3	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (8 Cores) CPU2 Not Present	32 GB
5	BL460c Gen8	VIRANI4	Intel(R) Xeon(R) CPU E5-2650 0 @ 2.00GHz (8 Cores) CPU2 Not Present	32 GB
9	BL460c G7	VIRTUALANI2	Intel(R) Xeon(R) CPU E5649 @ 2.53GHz (6 Cores) CPU2 Not Present	36 GB

Tabla 16 Procesamiento y Memoria

El servidor **VIRANI1** tiene muy poca memoria (6GB) subutilizando el poder de la máquina, esta es una de las primeras candidatas para aumentar memoria con lo cual se puede mejorar el alojamiento de máquinas virtuales.

El C7000 soporta aún otros 10 blades de media altura o 5 de altura completa, esto da una capacidad de crecimiento horizontal de un poco más del doble de lo que se tiene actualmente. Se puede ir adquiriendo gradualmente, si se requiere, servidores con una inversión mínima no comparable con la inicial. El C7000 ya está configurado a nivel de fuentes de poder y ventilación para soportar carga completa.

3.6 Virtualización

En el modelo actual de virtualización con el que cuenta **La Agencia** en caso de fallas un nodo, las máquinas virtuales que corren sobre este quedarían deshabilitadas. Una buena práctica es implementar Hyper-V en clúster o Live Migration y llevar las máquinas virtuales críticas a esta configuración. Bajo este tipo de tecnología muchos de los servicios de infraestructura quedan con alta disponibilidad.

Más adelante se diagrama como sería la infraestructura propuesta considerando los cambios y recomendaciones sugeridos en este documento.

3.7 Almacenamiento

Es sumamente importante adquirir una solución de almacenamiento tipo SAN. Es recomendable alojar los archivos de máquinas virtuales en el sistema de almacenamiento de alto rendimiento SAN destinado para esto, esto incrementa el rendimiento y asegura la alta disponibilidad de los datos. Los discos que alojan las VMs se recomienda sean RAID5.

De la mano de una solución de almacenamiento va una de respaldo. Es necesario generar políticas de backup y contar con una solución de respaldo confiable y automática para asegurar la calidad y confiabilidad de los datos respaldados.

3.8 Gestión y Monitoreo

3.9 Diseño de Directorio Activo

El Directorio Activo es uno de los pilares básicos de la infraestructura tecnológica, la gestión adecuada de este repercute en la calidad de los servicios, se identificaron varias tareas a realizar para el mejoramiento de la estructura actual de dominio.

3.9.1 Cambiar nombre del dominio

Mediante el Decreto Ley 4165 del 3 de noviembre de 2011, se modificó la naturaleza jurídica y la denominación del Instituto Nacional de Concesiones- INCO por el de Agencia Nacional de Infraestructura – ANI. El dominio actual se llama **inco.local**, es recomendable por identidad corporativa cambiar el nombre de dominio por ejemplo a **ani.local**. Este procedimiento es bastante sensible y requiere evaluación por parte del área de infraestructura considerando el impacto versus el requerimiento.

3.9.2 Actualizar las controladoras a Windows 2012

Es recomendable actualizar todas las controladoras de dominio a Windows 2012 y subir la funcionalidad del bosque y de dominio para aprovechar las nuevas funcionalidades del sistema operativo.

3.9.3 Redistribuir los roles de FSMO

En estos momentos todos los roles de FSMO se encuentran en la controladora **CDANI1**, existen mejores prácticas en la distribución de estos roles en las diferentes controladoras, por ejemplo, PDC emulator no debería estar en la misma máquina del RID Master. El siguiente enlace amplia el tema http://oreilly.com/pub/a/windows/2004/06/15/fsmo.html

3.9.4 Gestión de Active Directory Sites and Services

El site de directorio activo tienen el nombre por defecto, es recomendable ponerle un nombre acorde al sitio que está manejando.

También definirle subredes al sitio, esto va de la mano del nuevo esquema de segmentación de red propuesto en la parte de recomendaciones IP ubicado en este mismo documento.

3.9.5 Controladoras de dominio

El dominio cuenta con cuatro controladoras para un dominio de un solo *site* y solo 500 usuarios con dos controladoras para redundancia es suficiente. Se recomienda evaluar la necesidad de tener cuatro controladoras y si es mejor por gestión solo tener dos.

También es recomendable dejar al menos una controladora de dominio real y en este caso solo se requerirá una controladora adicional virtual para tolerancia a fallos.

3.9.6 Esquema de nombres

Definir un esquema de nombres consistente y estándar a través de toda la organización, agiliza la gestión y creación de nuevos recursos en el directorio activo. Se recomienda crear políticas para definir lo siguiente:

- Convención de nombre de dominio
- Convención de nombre para servidores
- Convención para estaciones de trabajo
- Convención para los nombres de las cuentas de usuario
- Convención para los nombres de las cuentas de correo

3.9.7 Estructura del árbol del directorio activo

El uso fundamental de las unidades organizacionales (OUs) es organizar de forma lógica los objetos de un dominio, pudiendo además utilizarse para delegar la administración de sus objetos a otros usuarios distintos del administrador del

dominio y personalizar el comportamiento de los usuarios y/o equipos mediante la aplicación de directivas específicas a la unidad.

Se recomiendan las siguientes actividades para organizar el árbol de OUs y mejorar la gestión de equipos y usuarios del dominio.

- Definir un diseño de directorio activo OUs
- Estructura unidad organizacional Funcional
- OUs de Temporales y Contratistas
- OUs específicas para equipos clientes

3.9.8 Rangos de direcciones

Este ítem va de la mano con la segmentación de red propuesto en este mismo documento. Es recomendable definir rangos de direcciones dentro de las mismas subredes y asignar estos a clases de dispositivos. Por ejemplo, de la 192.168.0.1 hasta la 192.168.0.20 para las interfaces de red de administración iLOs de los blades. De la 192.168.0.21 a la 192.168.0.60 para servidores, así dependiendo de la clase de dispositivos estos quedaran con IPs contiguas y organizadas.

3.9.9 DHCP como servicio de Windows e integrado

El servicio de DHCP es prestado por uno de los *switches core*, se recomienda implementar el servicio de Microsoft DHCP en uno de los servidores, con esto se obtiene tolerancia a fallos, mejor gestión de direcciones e integración con el directorio activo y DNS.

3.9.10 Esquema de DNS

Al servicio de DNS hay que realizarle varias tareas, inicialmente limpiar registros obsoletos. También eliminar los servidores de DNS de la pestaña de replicación.

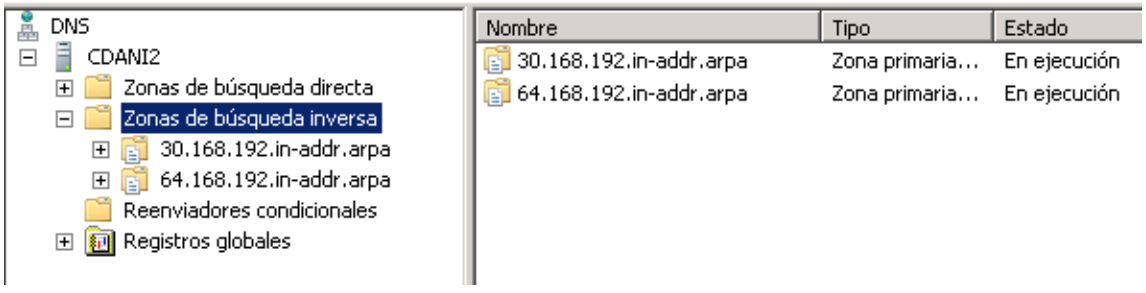

Figura 18 DNS Zonas de búsqueda inversa

Incluir en las zonas de búsqueda inversa las subredes que salgan de la segmentación de IP.

3.9.11 Registros de Usuarios y equipos obsoletos

Dentro de las labores de mantenimiento de directorio activo se encuentra el limpiar cuentas de usuarios y computadores periódicamente.

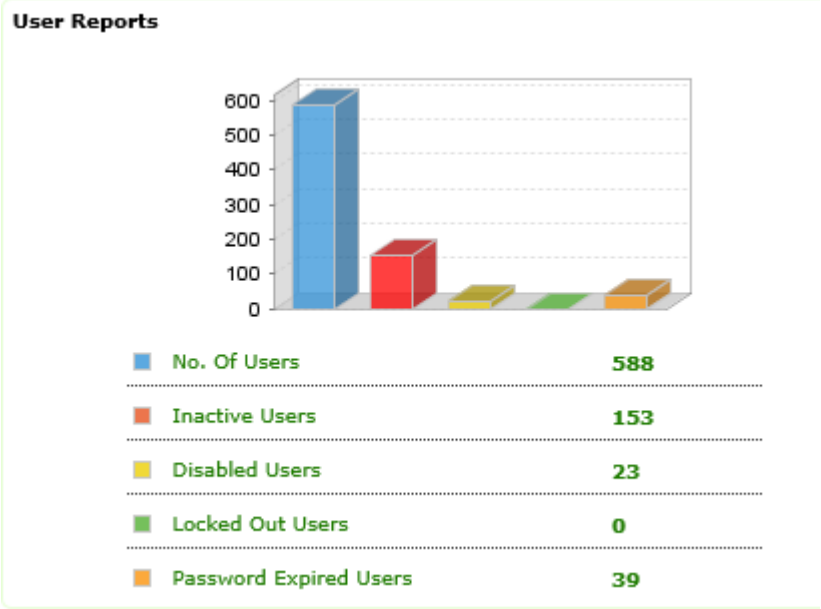

Figura 19 Reporte de usuarios

En la figura anterior se observa que existen 588 usuarios del domino de los cuales 153 están inactivos, 23 deshabilitados y 39 con el la clave vencida. Adjunto a este documento están anexos en formato Pdf y Excel reportes detallados del directorio activo para:

- Usuarios con cuenta expirada (clic)
- Todos los usuarios
- Usuarios deshabilitados
- Usuarios inactivos los últimos 90 días
- Usuarios con clave expirada
- Usuarios que nunca se han logueado

Es necesario revisar los reportes detallados de computadores y verificar cuales se pueden eliminar de Active Directory Users and Computers. En el reporte de computadores inactivos durante los últimos 90 días, existen una gran cantidad de equipos que no han ingresado a la red en este lapso de tiempo, estos pueden ser candidatos a elimina. Anexo encontraran estos reportes:

- Todos los computadores
- Computadores inactivos los últimos 90 días
- Computadores deshabilitados

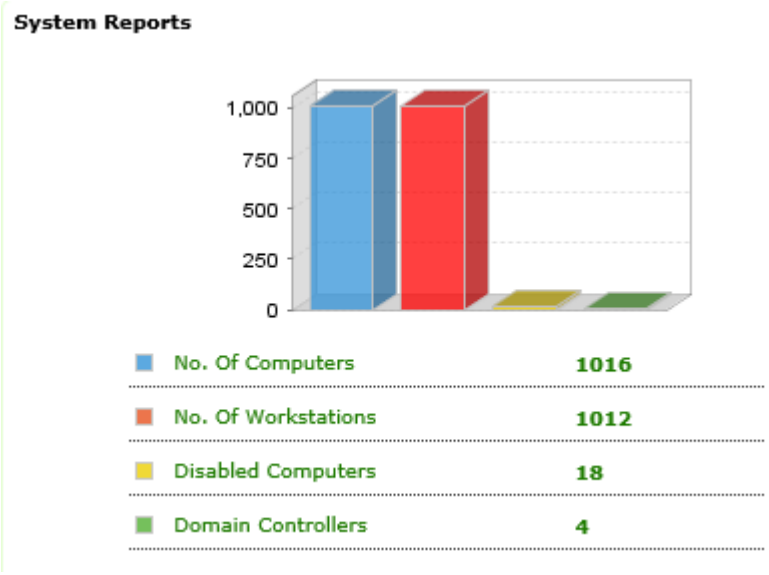

Figura 20 Reporte de computadores

De revisar también los grupos de usuarios existentes en el dominio, verificar cuales son necesarios y cuales no y gestionar la membresía de los mismos.

Se adjuntan los reportes de grupos:

- Grupos que no tienen miembros
- Grupos de Seguridad

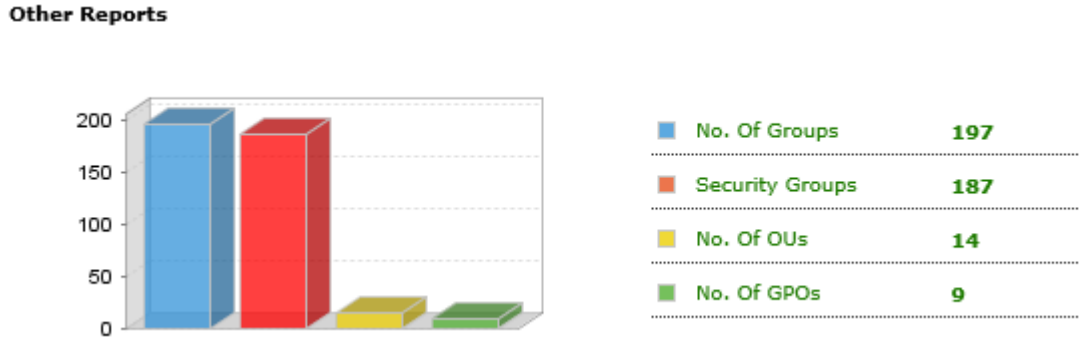

Figura 21 Grupos, OUs, GPOs

4. INFRAESTRUCTURA PROPUESTA

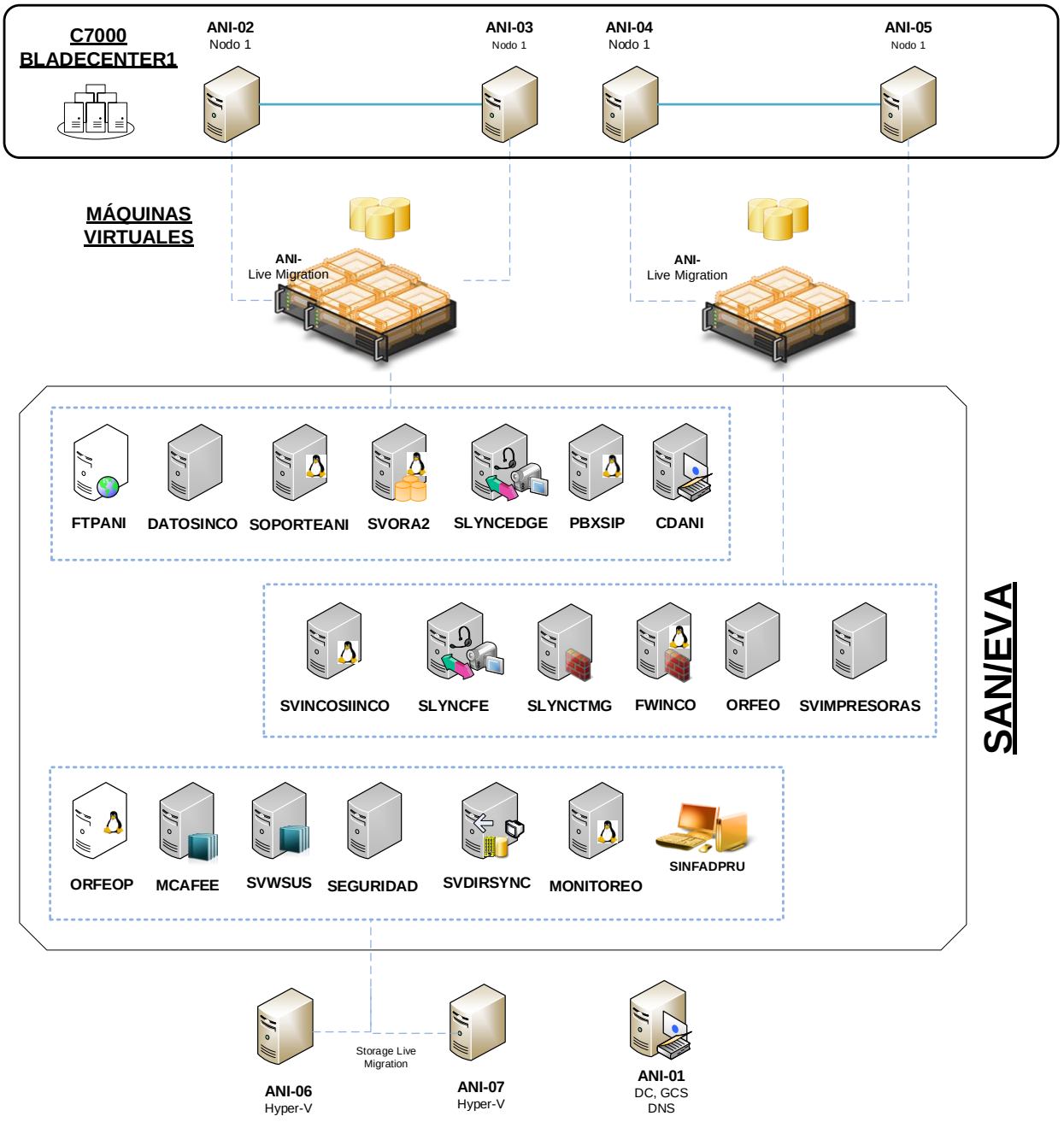

Figura 22 Infraestructura propuesta

Sustentados en las recomendaciones presentadas en este documento y considerando la adquisición de un sistema de almacenamiento tipo SAN se presenta esta infraestructura. Básicamente es implementar dos clúster de Hyper-

V, uno con los BL460c G7 y otro con los BL460 Gen8 y allí situar las máquinas virtuales más críticas del negocio. La configuración con Live Migration garantiza alta disponibilidad de los servidores allí alojados.

Con el BL460c G7 y el BL460 Gen8 restantes se puede armar un sistema de Storage Live Migration y tener agilidad en la gestión de la virtualización.

5. Base de datos Oracle

El objetivo principal es presentar un informe detallado el estado actual de la base de datos, de la Agencia Nacional de infraestructura, con el fin de poder establecer las recomendaciones y acciones necesarias para salvaguardar la información de La Agencia y mejorar el rendimiento de la base de datos. El alcance de las labores ejecutadas, se orientan al reconocimiento y el estado actual de la base de datos y establecer las recomendaciones:

- Arquitectura de la base de datos.
- Levantamiento de información de la base de datos.
- Tareas de Afinamiento total de la base de datos.

5.1 Diagnóstico y afinamiento de la base de datos Oracle 11g release 2

A continuación se realiza el levantamiento de información y posterior diagnóstico de la base de datos PROD, la cual corre sobre Oracle 11G Release 2.

5.1.1 Ficha técnica

La ficha técnica del levantamiento de información realizado es la siguiente:

Nombre Instancia	PROD
Archivo Salida	LEV_rod_30Ago2013.log
Fecha Ejecución	30/08/2013
Ejecutado Por	SYS

Tabla 17 Oracle Ficha Técnica

5.1.2 Características base de datos

Estas son las principales características de la base de datos PROD.

DB Name	PROD
Global Name	PROD
Host Name	Virani2

Archive Log Mode	Enable

Tabla 18 Oracle características

5.1.3 Registro de componentes

A continuación se muestra el registro de componentes para la base de datos PROD.

Component Name	User	Status	Version
JServer JAVA Virtual Machine	SYS	VALID	11.2.0.1.0
OLAP Analytic Workspace	SYS	INVALID	11.2.0.1.0
OLAP Catalog	OLAPSYS	INVALID	11.2.0.1.0
Oracle Application Express	APEX_030200	VALID	3.2.1.00.10
Oracle Database Catalog Views	SYS	VALID	11.2.0.1.0
Oracle Database Java Packages	SYS	VALID	11.2.0.1.0
Oracle Database Packages and Types	SYS	VALID	11.2.0.1.0
Oracle Enterprise Manager	SYSMAN	VALID	11.2.0.1.0
Oracle Expression Filter	EXFSYS	VALID	11.2.0.1.0
Oracle Multimedia	ORDSYS	VALID	11.2.0.1.0
Oracle OLAP API	SYS	INVALID	11.2.0.1.0
Oracle Rules Manager	EXFSYS	VALID	11.2.0.1.0
Oracle Text	CTXSYS	VALID	11.2.0.1.0
Oracle Workspace Manager	WMSYS	VALID	11.2.0.1.0
Oracle XDK	SYS	VALID	11.2.0.1.0
Oracle XML Database	XDB	VALID	11.2.0.1.0
OWB	OWBSYS	VALID	11.2.0.1.0
Spatial	MDSYS	VALID	11.2.0.1.0

Tabla 19 Oracle Registro de componentes

5.1.4 Modo de archivado de la base de datos

A continuación se mostrara el modo de archive en el cual está la base de datos. Es necesario tener el privilegio SYSDBA para ejecutar el comando "archive log list" satisfactoriamente.

Database log mode	Archive Mode
Automatic archival	Eneble
Archive destination	USE_DB_RECOVERY_FILE_DEST
Oldest online log sequence	327198155
Current log sequence	327028632
Created	31/DIC/2012 01:11:25 PM
LOCATION	/home/u01/app/oracle/flash_recovery_area/PROD/archivelog/

Tabla 20 Oracle modo de archivado

5.1.5 Archivos físicos de base de datos

Aquí se realiza una descripción de los archivos físicos que componen la base de datos. Se referencian entre otros, los data files, temp files, control files y redo log files.

Tablespace Name	File Name	Size (mb)	Autoext?
PROD	/home/u01/app/oracle/oradata/PROD	770	YES
	/datafile/o1_mf_sysaux_87xybsf0_.dbf	770	YES
SYSTEM	/home/u01/app/oracle/oradata/PROD/datafile/o1_mf_system_87xybsbj_.dbf	3640	YES
TOAD	/home/u01/app/oracle/oradata/PROD/datafile/TOAD01.dbf	100	YES
TS_ADMI_D	/home/u01/app/oracle/oradata/PROD/datafile/TSADMI01.dbf	180	YES
TS_ARANDA	/home/u01/app/oracle/oradata/PROD/datafile/TSARANDA01.dbf	300	YES
TS_DESARROLLO	/home/u01/app/oracle/oradata/PROD/datafile/TSDESARR01.dbf	100	YES
TS_DORFEO_DESA	/home/u01/app/oracle/oradata/PROD/datafile/TSDORFEDESA01.dbf	100	YES
TS_FINA_D	/home/u01/app/oracle/oradata/PROD/datafile/TSFINA01.dbf	560	YES
TS_NOMI_D	/home/u01/app/oracle/oradata/PROD/datafile/TSNOMI01.dbf	440	YES
TS_ORFEO	/home/u01/app/oracle/oradata/PROD/datafile/TS_ORFEO.dbf	180	YES
TS_SIINCOBD	/home/u01/app/oracle/oradata/PROD/datafile/TSSIINCOBD1.dbf	100	YES
TS_SINFAD	/home/u01/app/oracle/oradata/PROD/datafile/TSSINFA01.dbf	100	YES
TS_WEBSITE	/home/u01/app/oracle/oradata/PROD/datafile/TSWEB01.dbf	100	YES
TS_WINISIS	/home/u01/app/oracle/oradata/PROD/datafile/TSWINISIS01.dbf	100	YES
UNDOTBS1	/home/u01/app/oracle/oradata/PROD/datafile/o1_mf_undotbs1_87xybsd7_.dbf	585	YES
USERS	home/u01/app/oracle/oradata/PROD/datafile/o1_mf_users_87xybsb2_.dbf	5890	YES

Tabla 21 Oracle data files

Name
/home/u01/app/oracle/oradata/PROD/controlfile/control01.ctl
/home/u01/app/oracle/flash_recovery_area/PROD/controlfile/control02.ctl

Tabla 22 Oracle control files

Group	Members	Size (MB)	File Name
1	2	125	/home/u01/app/oracle/flash_recovery_area/PROD/onlinelog/redo01_m02.log
1	2	125	/home/u01/app/oracle/oradata/PROD/onlinelog/redo01_m01.log
2	2	125	/home/u01/app/oracle/flash_recovery_area/PROD/onlinelog/redo02_m02.log
2	2	125	/home/u01/app/oracle/oradata/PROD/onlinelog/redo02_m01.log
3	2	125	/home/u01/app/oracle/flash_recovery_area/PROD/onlinelog/redo03_m02.log
3	2	125	/home/u01/app/oracle/oradata/PROD/onlinelog/redo03_m01.log

Tabla 23 Oracle redo log files

5.1.6 Identificación de instancia

A continuación se muestran los parámetros de identificación de la instancia PROD.

Instance Name	PROD
Version	Oracle Database 11g Release 11.2.0.1.0 64 bit Production

5.1.7 Parámetros de memoria para instancia

A continuación se mostraran algunos de los parámetros más importantes que determinan el tamaño y funcionamiento de la instancia PROD.

Parameter Name	Value
db_16k_cache_size	0
db_2k_cache_size	0
db_32k_cache_size	0

db_4k_cache_size	0
db_8k_cache_size	0
db_block_buffers	0
db_block_size	8192
db_cache_size	0
db_keep_cache_size	0
db_recycle_cache_size	0
java_pool_size	0
Large_pool_size	0
log_buffer	43638784
pga_aggregate_target	0
sga_max_size	4429185024
sga_target	3355443200
shared_pool_reserved_size	107374182
shared_pool_size	0
sort_area_retained_size	0
sort_area_size	65536
workarea_size_policy	AUTO

Tabla 24 Parámetros de memoria

5.1.8 Administración de undo

A continuación se muestran los parametros de administración de undo.

Parameter Name	Value
undo_management	AUTO
undo_retention	900
undo_tablespace	UNDOTBS1

Tabla 25 Administración de undo

5.2 RECOMENDACIONES PARA BASE DE DATOS PROD.

Las recomendaciones se sugieren de acuerdo al levantamiento de información y la entrevista con el Ing. responsable de la Base de datos.

1. Descargar y aplicar el PatchSet y de seguridad de la base de datos y el Sistemas operativo.

2. Activar las estadísticas ya que se encuentran inactivas y con recopilación en cero segundos, con el fin de poder realizar los ajustes a los parámetros adecuados, ya que se encuentran los parámetros por default de la instalación, lo que significa que no se realiza un adecuado proceso de tunning de la base de datos, el cual es proceso continuo de administración.

3. Se evidenció que existe configurada una arquitectura de alta disponibilidad la cual está inactiva hace dos meses y en el levantamiento de información no se encontró el nodo principal y se encuentra activo el nodo de respaldo, lo que implica, que la licencia principal no se está utilizando, en el esquema planteado solo tienen que permanecer en funcionalidad dos de dos días. Es necesario poder determinar que pasó con la maquina principal y poder realizar la configuración adecuada, poner a funcionar el esquema de alta disponibilidad de dos nodos.

4. El esquema de backup identificado, se encontró que la base de datos se encuentra en modo ArchiveLog, lo que define un esquema de backup en línea, pero desde hace dos meses no se realiza un procesos de backup Full y almacenamiento de los archivo de Log, lo que pone en riesgo la información de la Agencia, ya que no se encuentra los grupos y archivos necesarios para la realización de la restauración de la base de datos. Es importante restablecer la configuración adecuada y la configuración de los backup, la realización de las copias de seguridad de acuerdo a las políticas establecidas. Las cuales se encuentran configuradas en el nodo principal de la arquitectura de alta disponibilidad, el cual está apagado.

5. Se observa que prácticamente la totalidad de la base de datos se encuentra ubicada en el disco /home/ Se recomienda distribuir la base de datos entre los discos en diferentes unidades.

6. Prácticamente todos los tablespaces de la base de datos se encuentran mezclados datos e índices a pesar de que hay tablespaces dedicados a

contener índices los cuales no están siendo utilizados. Se recomienda comenzar con el movimiento de estos objetos a los tablespaces correspondientes. Esta labor aún no se ha ejecutado debido a que no se encontró la ventana de tiempo adecuada para realizarlo, y requiere un tiempo prolongado de ejecución. Por lo tanto el siguiente mes de soporte se ejecutará esta labor.

7. Se refrescaron las estadísticas de base de datos para los usuarios

8. Se recreó la consola de OEM para la base de datos PROD, la cual estaba presentando problemas de caídas continuas.

9. Se observa que la memoria con la cual cuenta el servidor está mal distribuida para las necesidades del mismo. Se recomienda distribuir la memoria en los diferentes parámetros del servidor de forma urgente.

10. Se encontraron varios segmentos de la base de datos que necesitan mantenimiento.

11. Se encontraron varios segmentos de la base de datos que están muy fragmentados.

Anexo 1. PARÁMETROS DE INICIACIÓN DE LA BASE DE DATOS