# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL


## Facultad de Ingeniería en Electricidad y Computación

# "IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PARA REPOTENCIAR LA INFRAESTRUCTURA FÍSICA Y LÓGICA DE UNA ENTIDAD DE SERVICIOS."

**EXAMEN DE GRADO (COMPLEXIVO)**

**PREVIO A LA OBTENCIÓN DEL TÍTULO DE**
**MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA**

**Mario Pinos Guerra**
**Guayaquil – Ecuador**
**2016**

# AGRADECIMIENTO

Agradezco a Dios por la vida y la salud, necesarias para poder realizar el presente trabajo. A mis padres y a mis hermanas, familiares y amigos cercanos que siempre me animaron a seguir luchando y me brindaron su apoyo incondicional.

# DEDICATORIA

Dedico el presente trabajo a mis padres por apoyo incondicional a mis hermanas Marielita y Maribel por ser parte del impulso que llevo a terminar esta etapa de mi vida.

# TRIBUNAL DE SUSTENTACIÓN

MGS. LENÍN FREIRE

DIRECTOR DE LA MSIA

MGS.JUAN CARLOS GARCÍA

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

# RESUMEN

Para mejorar el servivio en una entidad se incrementa los puestos de trabajo, sin embargo si es un crecimiento no planificado, tiende a llevar al límite e incluso sobre pasar las capacidades lógicas de la entidad, lo que provoca lentitud en la red.

El presente trabajo toma como guía el estándar TIA-942(2007) [1] sobre diseño de infraestructuras de telecomunicaciones para Centros de Datos, donde se define las características que debe tener para ser encasillado en un nivel determinado y de la norma TIA-568A(1991) [7] que da la pauta de cómo debe realizarse de manera correcta la instalación de cableado estructurado.

El presente trabajo nos permite tomar como guía el estándar TIA-942(2007) [1] sobre diseño de infraestructuras de telecomunicaciones para Centro de Datos, donde se define las características que debe tener para ser encasillado en un nivel determinado y dela norma TIA-568A(1991) [7] que da la pauta de cómo debe realizarse de manera correcta la instalación de cableado estructurado.

Se analizará con una tabla comparativa la infraestructura antes y después de la implementación del proyecto.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

El desarrollo del trabajo muestra los problemas de un crecimiento no planificado y de las medidas que se deben adoptar para repotenciar esta solución y alcanzar estándares de calidad, describiendo el ambiente en el cual se generaron nuevas áreas con sus respetivos puestos de trabajo.

Se tomó la decisión de implementar un estándar, que nos permita un óptimo funcionamiento y adicional a esto asegurarnos de mantener la disponibilidad e integridad de la información utilizando mecanismos para asegurar los datos.

Con lo descrito en el primer capítulo se podrá observar los antecedentes, el problema y la propuesta de soluciones, mientras que en el segundo capítulo encontraremos el marco teórico el levantamiento de la información y el diseño de la solución.

En el tercer capítulo se muestran la implementación y el desarrollo de la solución. Demostrándose que el seguimiento del crecimiento de la infraestructura de una entidad es primordial a la hora de tomar decisiones ya que estas tomadas a tiempo podrían genera un ahorro importante dentro de la organización.

# CAPÍTULO 1

# GENERALIDADES

## 1.1 ANTECEDENTES

Ante la evolución de la entidad creada en 1937 nace la necesidad de migrar e implementar nuevos parámetros de seguridad debido al crecimiento no planificado y descontrolado del mismo.

Se realizan varios estudios, diagnósticos y análisis para considerar la nueva infraestructura para convertir la misma en una infraestructura que garantice un buen servicio dentro de la entidad y que además sirva para ser utilizada por 15 años siempre y cuando su crecimiento sea de la forma planificada.

## 1.2 DESCRIPCIÓN DEL PROBLEMA

Luego de ciertos cambios gubernamentales la entidad de servicios modificó su estructura organizacional, por lo que nació la necesidad de repotenciar la infraestructura existente; tanto en la parte activa como en

la pasiva. Tomando en consideración los futuros requerimientos de la entidad para su correcto funcionamiento.

La última actualización realizada en el edificio consta en planos y se lo fecha en Abril del 2002; considerando que la parte pasiva, en cuanto a categoría del cableado estructurado era la mejor propuesta para la fecha de su implementación, (categoría-5E) y los servidores y equipos activos eran los adecuados para la infraestructura vigente y que ha tenido un crecimiento no planificado, provocado por el incremento de personal y readecuaciones de las áreas de trabajo.

El Centro de Datos está ubicado en el primer piso, se encuentra aislado por mampostería de oficina, la cual no brinda las seguridades pertinentes. Estas generan vulnerabilidad de la información que se almacena en sus servidores, lo que se podría calificar como ataques físicos. Además, su sistema de enfriamiento es un aire acondicionado de pared tipo cajón, el mismo que hace una mala distribución del frío en la habitación. Esta situación ha provocado que los equipos activos no se enfríen de la manera adecuada, generando a su vez una reducción del tiempo de vida y un umbral para posibles fallos. Sin considerar que la mala distribución del frío obliga al compresor del aire acondicionado a

trabajar más y esto se refleja también como un incremento de consumo energético, el Sistema de Alimentación Ininterrumpida (Uninterruptible Power Supply - UPS) carece de redundancia y no existe un sistema de registro y control de acceso al Centro de Datos, adicional no posee sistema de vigilancia, que generen un registro visual de las actividades realizadas dentro del área.

Los equipos activos existentes instalados son enrutadores HP, que funciona como servidor DHCP (Protocolo de Configuración dinámica de Usuarios) y cortafuegos. Adicional existen enlaces de Redes Virtuales Privadas (Virtual Private Network – VPN) con Quito, Cuenca y Guayaquil. Las configuraciones permiten conexiones de administración remota, para soporte desde exteriores, el programa no está actualizado y el flujo de información no estaría en capacidad de manejar el nuevo requerimiento.

La entidad cuenta con enlaces vigentes entre la ciudad de Guayaquil – Quito, Guayaquil – Cuenca, levantadas a través de enlaces dedicados con enrutadores HP, utilizando VPN, que a su vez eran utilizadas como un tipo de cortafuegos realizando una función, para el que no fue diseñado. Esto produce una vulnerabilidad por el tipo de encriptado de los enlaces y la velocidad de los mismos; por la cantidad de paquetes por

millón manejados. Los conmutadores instalados son marca HP y tienen dos Redes de Área Local Virtual (Virtual Local Área Network – VLAN) configuradas, la de administración y la plana que es por donde tiene acceso a los diversos servicios que ofrece la institución. La solución de servidores tiene instalados un repositorio y adicional varios servicios como el de correo electrónico y la base de digitalizaciones de los registros.

## 1.3 SOLUCIÓN PROPUESTA

Se propone repotenciar un Centro de Datos con las nuevas tecnologías de la información que incluyen:

Especificaciones Técnicas de la Entidad

1.-SEGURIDAD FÍSICA

- 12.5 m2 Obra Civil para CENTRO DE DATOS:
- Desmontaje y montaje de mampostería de madera y estructura metálica con divisiones.
- 12.5 m2 piso de acceso elevado en área de CENTRO DE DATOS
- 2 Equipos de precisión inteligentes de climatización serie 7 de 2.5 TON.

- Control de Acceso por tarjeta magnética.
- Sistema de Video Vigilancia

2.-ENERGÍA ELÉCTRICA

- Incluye todo lo necesario para la conexión del equipo existente de (8 KVA) y el nuevo a adquirir de (10 KVA) en redundancia con bypass por separado; además de las instalaciones eléctricas y luminarias necesarias dentro del CENTRO DE DATOS.
- EQUIPO DE RESPALDO DE ENERGÍA CON INDEPENDENCIA DE 30 min A CARGA COMPLETA

3.-SERVIDORES

- Se adquirirán 2 servidores nuevos para balancear carga de accesos y programas existentes en el único servidor Blade.

4.-RECONFIGURACIÓN E INSTALACIÓN DE PLATAFORMA TECNOLÓGICA

- El principal objetivo es balancear el consumo de recursos de los servidores y mantener una plataforma de información de alta disponibilidad.

Los Puntos de Voz y Datos serán en categoría 6A y debidamente certificados, incluyendo el cableado estructurado horizontal que estarán en los cuartos de distribución con los materiales, se utilizarán canaletas, cajas, tubos, conectores de tubos, cable de Usuario Final, etc.

Realizar visita insitu con el personal de TI, (Tecnología de la Información) para chequear requerimientos que serán necesarios para cubrir las nuevas necesidades de infraestructura de datos y servicios. Así mismo proponer la migración de los servicios alojados en servidores virtuales a servidores dedicados.

Se realizará el levantamiento de información técnica sobre la infraestructura pasiva y activa existente. Además de clasificar según los recursos y servicios del Centro de Datos; que NIVEL sería basándose en el estándar TIA-942 (2007) [1] y de esta manera proponer las medidas correctivas para llegar a NIVEL III.

Con el crecimiento del personal se generaron puntos de servicios que no contaban con las respectivas facilidades, por lo tanto mediante la

repotenciación se colocará más CT (Cuartos de Telecomunicaciones) y aumentar la cobertura de la red. Con esto se pretende cubrir la demanda existente en el mismo y de esta forma crear la plataforma física y evitar problemas futuros.

Se realizarán los cambios necesarios en el Centro de Datos basándose en el estándar TIA-942 (2007) [1] y de esta manera alcanzar un NIVEL III, lo que generaría un cambio en la estructura actual del Centro de Datos e incluiría colocar controles de acceso, protección contra incendios y la instalación de equipos nuevos. Cada uno con su respectiva redundancia para mejorar la respuesta, disponibilidad y seguridad de los servicios. Las capacidades de un Centro de Datos con NIVEL III le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupción en las operaciones de la misma.

Los recursos de los servidores se encuentran al máximo, por lo tanto se vió la necesidad de actualizar y migrar los servicios a unos servidores nuevos que cumplieran con los nuevos requerimientos establecidos, con el fin de mantener disponibilidad de servicios para las dos instituciones,

entre los servicios migrados se encuentran; intranet corporativa, correo electrónico, chat y un servidor proxy.

# CAPÍTULO 2

# METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

Tomando en cuenta la descripción del problema que enumera las principales necesidades de una institución, se busca solucionarlas usando una normativa que permita el funcionamiento de una manera óptima y adecuada.

## 2.1 NORMATIVA TIA-942

Desarrollado para dar los lineamientos en el diseño e implementación de Centros de Datos (Data Centers - DC), el estándar TIA-942(2007) [1] da las directrices para la instalación de infraestructuras dependiendo de las necesidades o del alcance del proyecto y basándose en su disponibilidad y su fiabilidad.

Según Grupo Cofitel (2014) [2] al diseñar los centros de datos conforme a la norma, se obtienen ventajas fundamentales, como son:

- Nomenclatura estándar.

- Funcionamiento a prueba de fallos.
- Aumento de la protección frente a agentes externos.
- Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad.

De acuerdo con él estándar TIA-942(2007) [1], la infraestructura de soporte de un Data Center estará compuesta por cuatro subsistemas:

- Telecomunicaciones: Cableado de armarios y horizontal, accesos redundantes, cuarto de entrada, área de distribución, backbone, elementos activos y alimentación redundantes, patch panels y latiguillos, documentación.
- Arquitectura: Selección de ubicación, tipo de construcción, protección ignífuga y requerimientos NFPA 75(Sistemas de protección contra el fuego para información), barreras de vapor, techos y pisos, áreas de oficina, salas de UPS y baterías, sala de generador, control de acceso, CCTV, NOC (Network Operations Center – Centro operativo).
- Sistema eléctrico: Número de accesos, puntos de fallo, cargas críticas, redundancia de UPS y topología de UPS, puesta a tierra, EPO (Emergency Power Off- sistemas de corte de emergencia) baterías, monitorización, generadores, sistemas de transferencia.

- Sistema mecánico: Climatización, presión positiva, tuberías y drenajes, CRACs y condensadores, control de HVAC (High Ventilating Air Conditionning), detección de incendios y sprinklers, extinción por agente limpio (NFPA 2001), detección por aspiración (ASD), detección de líquidos.

**El concepto de Nivel**

Según Grupo Cofitel (2014) [2] es una clasificación que hace referencia a la fiabilidad de un centro de datos. Tomando en referencia que mientras más grande es el Nivel, mayor es la disponibilidad y también mayor el costo de implementación y mantenimiento.

Tabla 1. Lista de disponibilidad según el Nivel

| TIER | % DISPONIBILIDAD | % PARADA | TIEMPO ANNUAL DE PARADA |
|---|---|---|---|
| TIER I | 99,67% | 0,33% | 28,82 HORAS |
| TIER II | 99,74% | 0,25% | 22,68 HORAS |
| TIER III | 99,98% | 0,02% | 1,57 HORAS |
| TIER IV | 100.00% | 0,01% | 52,56 MIN |

Fuente: Grupo Cofitel, 2014, recuperado 06/01/2016, http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/

### 2.1.1 CARACTERÍSTICAS DEL CABLEADO ESTRUCTURADO CATEGORÍA-6A

Según la Norma ANSI-TIA-568-C-2(2011) la Categoría–6A trata sobre cables de comunicación, con par trenzado de cobre y sus componentes. Además establece que la distancia horizontal ente puntos de datos es de máximo 90 metros y se reserva 10 metros para conexiones con usuarios finales y equipos activos. Dando una distancia máxima de 100 metros con una velocidad de transmisión de 10 Gigabits sobre conectores de cuatro pares de hilos trenzados a una frecuencia de 500 MHz para esta categoría.

Según Black Box Network Services (2010) [3] el cableado está diseñado para soportar aplicaciones de alta velocidad, en relación a la categoría 6 que fue diseñada para funcionar a una velocidad máxima de 1 Gigabits con una frecuencia de 250 MHz sobre cobre.

Por lo general, se suele reemplazar de 3 a 5 veces los equipos activos; en el ciclo de vida útil de un sistema de cableado estructurado que suele ser de 15 a 20 años. Por lo que el cableado instalado debe ser considerado para soportar al menos dos generaciones de equipos activos Ethernet.

## 2.2 PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD

Según Harris (2013) [4] los pilares en los que se fundamenta la seguridad son; disponibilidad, integridad y confidencialidad. Cada uno de estos pilares requiere un nivel o metodología diferente para su protección.

- **Disponibilidad:** Esta protección se encarga de asegurar el acceso en todo el tiempo a la data y recursos permitidos para cada usuario. Por lo tanto se deben ejecutar políticas o mecanismos tanto en la red interna y externa, para que ayude a evitar que afecte el desempeño del negocio. La infraestructura de Trabajo está compuesta por una parte física (Elementos Activos y Pasivos) y otra lógica (Sistemas Operativos, software, aplicaciones, etc…). El fallo o el ataque a alguno de estos elementos puede llevar al entorno a una pérdida de disponibilidad, por lo tanto se debe tener presente la vulnerabilidad del sistema en el que se está trabajando para tratar de mitigar y de esta manera evitar caer en un fallo de disponibilidad.

- **Integridad:** Esta Protección se encarga de evitar que la información provista por sistema se modificada por algún agente sin autorización. El perfecto trabajo entre Hardware y software, además de la correcta aplicación de mecanismos ayudan a que el flujo de datos lleguen a

su destino sin un cambio inesperado. Por lo tanto si alguna intrusión en el sistema fuese exitosa, por algún medio; ya sea virus, gusanos, etc,.. este se lo consideraría corrupto. Para evitar esto, se utilizaría Sistemas de Detección de Intrusos (IDS) o comparaciones de Hash.

- **Confidencialidad:** Esta protección se encarga de garantizar que la Data es transmitida con el respectivo encriptado y un estricto acceso a la información clasificada, para evitar divulgación no autorizada que podría generarse por atacantes, que usando técnicas como; ingeniería social, shoulder surfing, archivos que roban contraseñas o esquemas que rompen encripciones, para evitar esto se necesita capacitar al personal sobre métodos adecuados para la protección de la Data.

### 2.2.1 DEFINICIONES DE SEGURIDAD

Según Harris (2013) [4] es necesario aclarar las siguientes definiciones; vulnerabilidad, amenaza, riesgo y exposición. Debido a que a menudo suelen ser mal interpretadas o en el peor de los casos confundidas entre ellas.

- **Vulnerabilidad:** Es un punto débil dentro de un esquema o sistema que carece de alguna solución, para repáralo o

en el peor de los casos una solución incompleta o mal diseñada, que genera una nueva debilidad. Por ejemplo las aplicaciones sin parches, un puerto abierto en un servidor de seguridad, etc…

- **Amenaza:** Es el producto de explotar una vulnerabilidad que se encuentra en el sistema, que se considere peligrosa, como por ejemplo; un ente externo identifica una vulnerabilidad de la red y la explota para poder tener acceso a información privilegiada de esta manera violando la política de seguridad.

- **Riesgo:** Es la probabilidad de que una amenaza explote una vulnerabilidad. Por ejemplo si un servidor no tiene cerrado los puertos innecesarios, se corre un gran peligro de que exista una intrusión sobre todo, si no se implementa un IDS porque existiría la probabilidad de que dicho ataque pasara desapercibido.

- **Exposición:** Es la acción de ser vulnerable a una acción que puede generar pérdidas. Por ejemplo si una organización no mantiene una política sobre contraseñas laxas se puede exponer a que su información confidencial pueda ser vista por personal no autorizado.

Si bien es cierto la mayoría de los riesgos no se pueden eliminar completamente, pero si se pueden mitigar o reducir su daño con una contramedida que puede ser un software, un hardware o una política que reduzca la posibilidad de que la amenaza sea explotada. Por ejemplo un firewall, un IDS, un guardia de seguridad, un sistema de incendio, cifrado de información, etc….

El análisis de estos términos cubren los conceptos básicos de seguridad y se los debe de tener claros para evitar confundirse entre ellos.

## 2.3 LEVANTAMIENTO DE INFORMACIÓN DE LA INFRAESTRUCTURA PRESENTE TANTO EN SEGURIDAD FÍSICA COMO LÓGICA

A continuación se detalla la distribución que se recogió después de realizar una inspección insitu en la entidad, indicando la posición actual de los Cuartos de Telecomunicaciones (CT) y del Centro de Datos (CD), incluyendo la cantidad de puntos existentes en categoría 5-e y los enlaces de Fibra Óptica (F.O.) multimodo 62.5/125 de 4 hilos. Adicionalmente se pudo verificar, que en el CD, la única separación entre los equipos activos y la gente de sistemas era una mampara de oficina y tenían un UPS para abastecer al servidor Blade HP y a los equipos

activos. No existía ningún control de acceso salvo la cerradura de la puerta, además no había una bitácora de visita. El aire acondicionado que desempeñaba el papel de climatización de CD, no es adecuado para este fin.

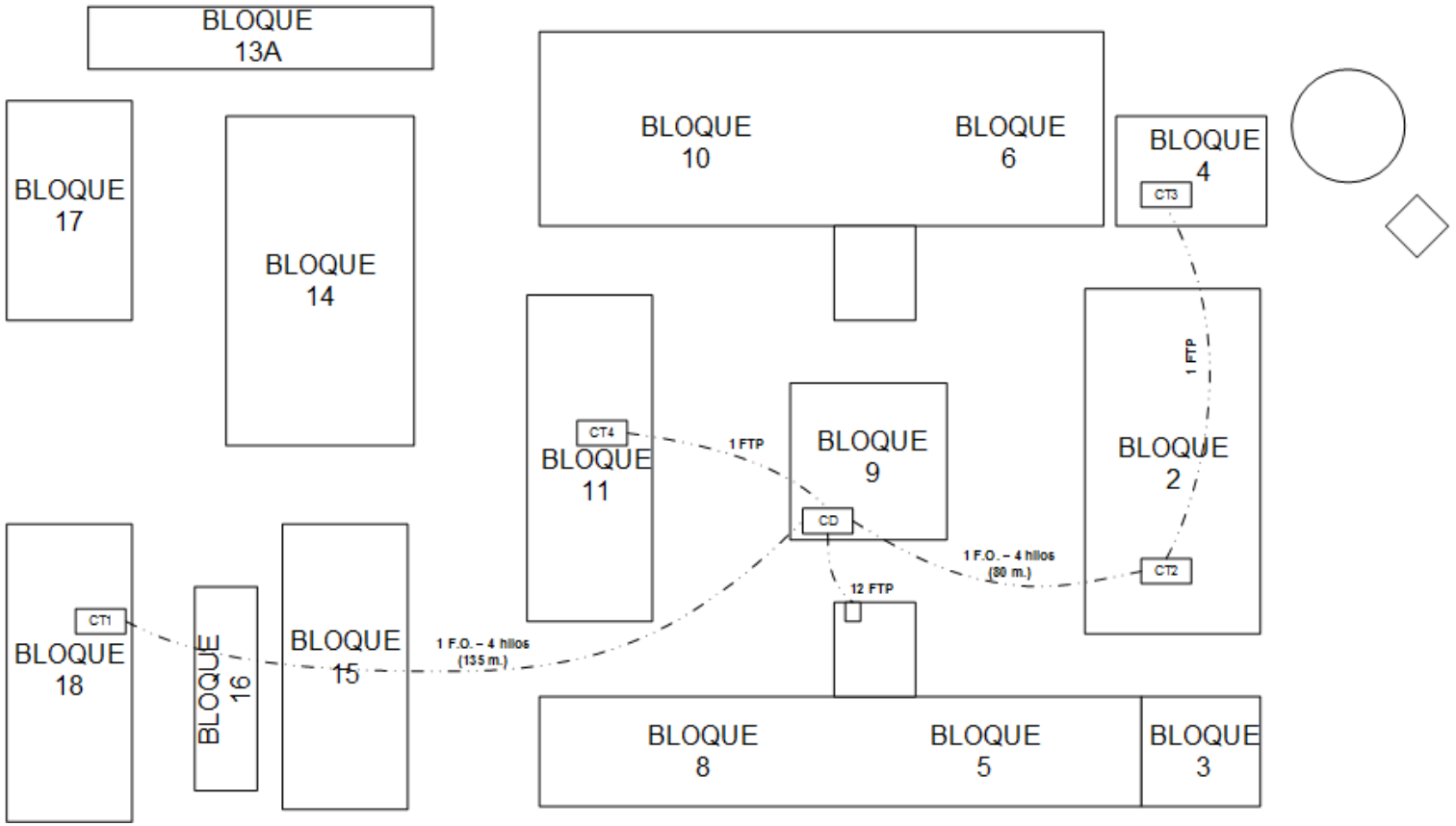


Figura 2.1. Diagrama de Conexiones de Edificios de la Entidad

Fuente: Mario Pinos Guerra (2016)

A continuación se detalla el número de puntos de Datos de cada distribuidor de cableado:

Tabla 2. Cantidad y Distribución de los puntos de Datos iniciales

| | |
|---|---|
| **1. Rack Centro de Datos** | |
| Ubicación: | Bloque 9 - 1er piso |
| Número de Puntos de Datos: | 112 |
| Enlaces de Cobre | 1 |
| Enlaces de Fibra: | 2 |
| **2. Rack CT1** | |
| Ubicación: | Bloque 18 - 2do piso |
| Número de Puntos de Datos: | 90 |
| Enlaces de Fibra: | 1 |
| **3. Rack CT2** | |
| Ubicación: | Bloque 2 - Planta Baja, Central Telefónica |
| Número de Puntos de Datos: | 80 |
| Enlaces de Fibra: | 1 |
| **4. Gabinete CT3** | |
| Ubicación: | Bloque 4 - Planta Baja |
| Número de Puntos de Datos: | 35 |
| Enlaces de UTP: | 1 |
| **5. Gabinete CT4** | |
| Ubicación: | Bloque 11 - 2do piso |
| Número de Puntos de Datos: | 25 |
| Enlaces de UTP: | 1 |

Fuente: Mario Pinos Guerra (2016)

Se adjunta un diagrama de red existente de la entidad.

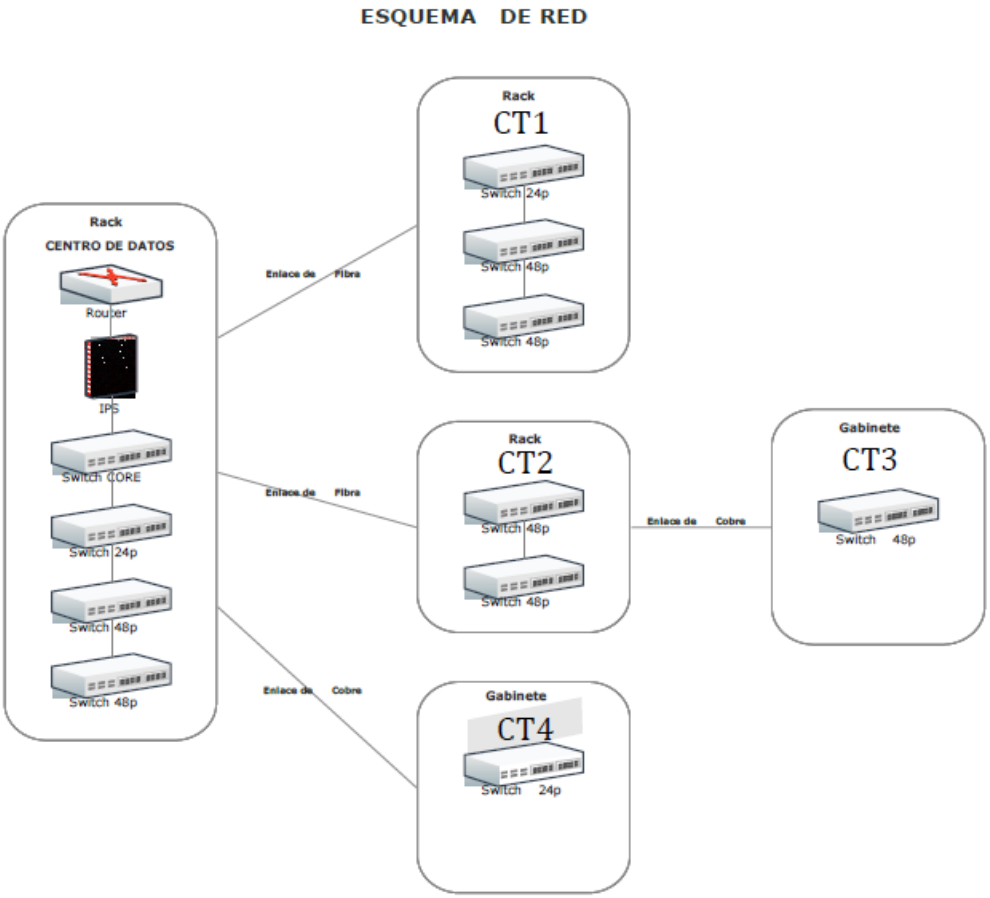


Figura 2.2. Esquema de Red antes de la Repotenciación de la infraestructura
Fuente: Mario Pinos Guerra (2016)

### 2.3.1 NIVELES PARA CENTRO DE DATOS

Según la norma TIA-942(2007) [1], los cuatro niveles corresponden a diferentes grados de disponibilidad, el cual se aplica a cada subsistema del centro de datos y a este se lo califica por el valor más bajo en niveles de sus subsistemas,

esto quiere decir que si todos los subsistemas son nivel cuatro y el subsistema eléctrico es nivel tres la calificación del centro de datos sería nivel tres, por el subsistema eléctrico.

A continuación se detalla brevemente las características de los cuatro niveles según Enrich (2007):

- **Nivel 1:** Centro de Datos Básico.

  Un Centro de Datos Nivel 1 puede ser susceptible a interrupciones de servicios. Debe tener sistemas de climatización y de distribución de energía eléctrica; no es necesario piso falso y debe tener UPS o un Generador eléctrico en cualquiera de los últimos dos casos, puede no haber redundancia. La carga crítica para este nivel siempre va a ser considerada como el 100% y debe estar fuera de servicio al menos una vez al año por mantenimiento preventivo o por reparaciones de sistemas defectuosos. La tasa de disponibilidad máxima del centro de datos es 99.671% anual.

- **Nivel 2:** Componentes Redundantes

  Cumple con las características de un Nivel 1, pero con la diferencia de que el centro de datos tiene piso falso y se

considera para el diseño del centro de datos todos los subsistemas más uno (N+1), lo que quiere decir, que existe al menos un duplicado por subsistemas del centro de datos. Por lo que la tasa de disponibilidad máxima del centro de datos en este Nivel es de 99.749% anual.

- **Nivel 3:** Mantenimiento Concurrente

  Al igual que los otros niveles hereda sus características con algunos cambios como por ejemplo; que este nivel permite hacer mantenimientos y pruebas sobre cualquier componente de la infraestructura, sin experimentar interrupciones en las operaciones. Adicional, se debe manejar doble línea de distribución de energía. Este Nivel aún es vulnerable a actividades no planificadas como fallos de la infraestructura, lo que coloca su tasa de disponibilidad máxima en 99.982% anual.

- **Nivel 4:** Tolerante a fallas

  En este Nivel se tiene la posibilidad de realizar mantenimientos e incluso existe la funcionalidad de tolerancia a fallas, lo que le permite a la infraestructura seguir operando sobre un evento crítico no planificado y

así no perder el servicio. Para esto es necesario dos líneas de distribución activas esto significa dos sistemas de UPS totalmente independientes con su redundancia respectiva (N+1). Lo que coloca la tasa de disponibilidad máxima de centro de datos en 99.995% anual.

### 2.3.2 NIVELES PARA SEGURIDAD DE LA INFORMACIÓN EN CENTRO DE DATOS.

Según Noordergraaf (2000) [5] la infraestructura debe ser diseñada en función de sus servicios y de la criticidad de la información, para esto lo separamos en Niveles para incrementar la seguridad junto a cada nivel, debe existir una única segmentación física. Los Niveles son:

1. Internet – Nivel de Servidor Web
2. Servidor Web – Nivel de Servidor de Aplicaciones
3. Nivel de Servidor de Aplicaciones – Nivel de Base de Datos
4. Nivel de ExtraNet – Nivel de Base de Datos
5. Nivel de Respaldos – Sistemas que manejan Respaldos

6. Nivel de Red de Área de almacenamientos (Storage Area Network - SAN) – Sistemas que utilicen SAN en su infraestructura.

7. Nivel de Administración – Todos los Servidores

La implementación de redes de trabajo separada y niveles proporcionan la habilidad de detectar intrusos durante un ataque por una brecha de seguridad.

Cada uno de los servicios y sistemas debe ser protegido debido a que cada uno tiene diferentes vulnerabilidades y deben ser consideradas en el momento de hacer un análisis de riesgos, para tomar la decisión adecuada.

Entre las medidas que se deben optar son Fortalecimiento de Servidores, Firewall bastion - host.

El fortalecimiento de servidores se obtiene modificando la configuración de fábrica de los sistemas operativos, debido a que hay funciones de seguridad que vienen deshabilitadas y mejoran la resistencia de los sistemas, para evitar accesos no autorizados.

Los Corta Fuegos son comunes, se pueden usar de manera efectiva en un entorno n-niveles, sino están bien dimensionado

la capacidad de estos pueden causar problemas y afectar negativamente la disponibilidad de la red, al convertirse en un embudo entre capas. Si se considera su uso también debe ser considerado en la redundancia, por lo que se debe analizar cuidadosamente su uso debido que si no se está seguro de sus beneficios en mejor no instalarlo.

Se recomienda manejar servidores dedicados para cada servicio, ya que de esta forma el firewall puede proveer el nivel necesario para prestar servicios a redes específicas; creando un conjunto de reglas simples y minimizar el impacto.

## 2.4 DISEÑO PARA AMPLIAR LA COBERTURA DE LA INFRAESTRUCTURA BASÁNDONOS EN LOS REQUERIMIENTOS ACTUALES CONSIDERANDO EL INCREMENTO DE PUESTOS DE TRABAJO.

Según la norma EIA/TIA 568-A (1991) [6] se considera los puntos más lejanos y se verifica si existe una distancia de recorrido horizontal, entre el punto de usuario final y el cuarto de telecomunicaciones que no sea mayor a 90 metros, dejando 10 metros para conexiones de usuario final y de equipos activos. Esta distancia va a permitir analizar la cobertura de un cuarto de rack, por lo tanto si se analiza sobre planos vamos a localizar las áreas a las que se tiene que dar servicio, por lo que se debe

considerar si la distancia es suficiente o si se coloca un rack adicional. Adicional a esto se debe considerar que la distancia menor al rack debe de ser de 15 m para evitar efectos de reflexión.

Partiendo de esta premisa se toma la decisión de colocar los rack según la cantidad de usuarios y en función de la distancia.

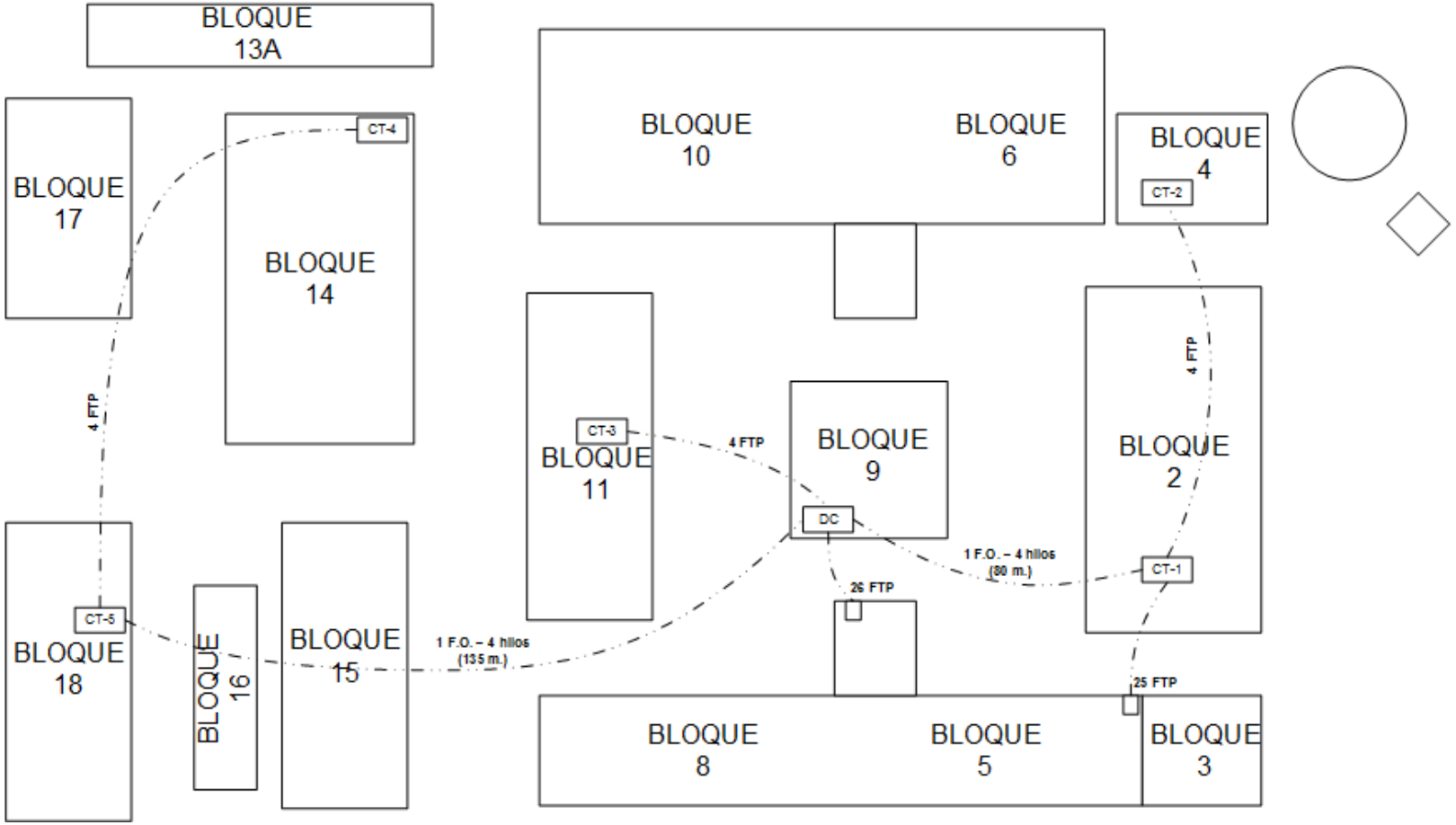


Figura 2.3. Diseño propuesto para repotenciación de Infraestructura
Fuente: Mario Pinos Guerra (2016)

La topología física de cableado a implementar es de tipo estrella y la cobertura máxima según estándar EIA/TIA 568-A (1991) [6] de un cuarto de comunicación es de un radio de máxima de 60m. A continuación se detalla el número de puntos de Datos de cada distribuidor según los requerimientos planteados en diseño:

Tabla 3. Cantidad y Distribución de los puntos de Datos después de Diseño

| **1. Rack Centro de Datos** | |
|---|---|
| Ubicación: | Bloque 9 - 1er piso |
| Número de Puntos de Datos: | 264 |
| Enlaces de UTP: | 30 |
| Enlaces de Fibra: | 2 |
| **2. Rack CT1** | |
| Ubicación: | Bloque 2 - Planta Baja, Central Telefónica |
| Número de Puntos de Datos: | 103 |
| Enlaces de UTP: | 29 |
| Enlaces de Fibra: | 1 |
| **3. Rack CT2** | |
| Ubicación: | Bloque 4 - Planta Baja |
| Número de Puntos de Datos: | 91 |
| Enlaces de UTP: | 4 |
| **4. Gabinete CT3** | |
| Ubicación: | Bloque 11 - 2do piso |
| Número de Puntos de Datos: | 53 |
| Enlaces de UTP: | 4 |
| **5. Gabinete CT4** | |
| Ubicación: | Bloque 14 - 2do piso |
| Número de Puntos de Datos: | 49 |
| Enlaces de UTP: | 4 |
| **6. Gabinete CT5** | |
| Ubicación: | Bloque 18 - 2do piso |
| Número de Puntos de Datos: | 90 |
| Enlaces de Fibra: | 1 |
| Enlaces de UTP: | 4 |

Fuente: Mario Pinos Guerra (2016)

## 2.5 DISEÑO DE LA INFRAESTRUCTURA DEL CENTRO DE DATOS BASÁNDONOS EN LA ACTUAL PARA LLEGAR A UN CENTRO DE DATOS NIVEL III.

Según Tyco Electronics Corporation (2010) [7]; la ubicación del Centro de Datos es muy importante para la infraestructura de telecomunicaciones. Debe colocarse en un lugar que se de fácil acceso para la canalización de las troncales además de evitar lugares que limiten el crecimiento de Centro de Datos como ascensores o que impida el ingreso de equipos grandes.

La estructura física de un Data Center incluye requerimientos específicos de diseño entre los que tenemos:

1. Tamaño del Centro de Datos
2. Seguridad
3. Piso Falso
4. Protección contra fuego
5. Control Ambiental
6. Iluminación
7. Alimentación de Tensión

8. Construcción Física
9. Protección contra el polvo
10. Puesta a Tierra
11. UPS

Por lo que se plantea la siguiente propuesta:

**OBRA CIVIL**

- 12.5 $m^2$ Obra Civil para Centro de Datos
- Desmontaje y montaje de mampostería de madera y estructura metálica con divisiones
- Elaboración de paredes de bloques enlucidas y pintadas en área de 2.50 m x 5 m
- Tumbado de yeso con aluminio.
- 2 Ventanas selladas con vidrio 10cm de 40cmx100cm, con película antirrobo
- 1 puerta de seguridad semiblindada brazo.

**PISO FALSO**

12.5 m2 piso de acceso elevado en área de Centro de Datos

- Paneles
- Paneles reforzados
- Rampa de acceso
- Ventosa
- Hermetización de pasos de cables para las consolas de iluminación
- Malla de alta frecuencia, instalación y aterrizaje
- Pintura antiestática

**ENFRIAMIENTO**

2 Equipos de precisión inteligentes de climatización serie 7 de 2.5 TON. Tipo Split Centro de Datos

2 Tarjetas de monitoreo remoto con panel M52

**UPS**

EQUIPO DE RESPALDO DE ENERGÍA CON INDEPENDENCIA DE 30 min A CARGA COMPLETA

- 1 UPS 10KVA CON RESPALDO DE BATERIAS 30 MINUTOS
- 1 GABINETE DE BATERIAS PARA INDEPENDENCIA DE 30 MINUTOS A CONSUMO DE CARGA COMPLETA

**ENERGÍA ELÉCTRICA**

Incluye todo lo necesario para la conexión del equipo existente de 8 KVA y el nuevo a adquirir de 10 KVA en redundancia con bypass por separado; además de las instalaciones eléctricas y luminarias necesarias dentro del DATA CENTER.

**SERVIDORES**

Se colocará 2 servidores nuevos para balancear carga de accesos y programas existentes en el único servidor Blade.

- 2 HP DL380p Gen8 E5-2650 HPM US Svr

**SEGURIDAD**

Se colocará seguridad Biométrica para restringir el acceso a personal no autorizado, adicional a esto se instalaran dos cámaras tipo domo con protección anti vandalismo.

**SISTEMA CONTRA INCENDIOS**

Bombonas de FM-200

## 2.6 DISEÑO DE LA REPOTENCIACIÓN DE LOS ENLACES VPN DEL INSTITUTO PARA CUBRIR VULNERABILIDADES.

El principal objetico es proteger de intrusiones y accesos no permitidos de las redes internas (LAN) así como la protección de datos en las 3 ciudades sedes principales de la entidad.

En los alcances previamente establecidos para este proceso de instalación se determinó la necesidad de migrar la configuración de enmascaramientos, permisos de acceso y túneles VPN de los equipos que anteriormente brindaban ese servicio al nuevo esquema de protección perimetral basada en equipos Cisco ASA 5520.

Los equipos Cisco ASA 5520 pueden ejecutar control de acceso en ambientes que manejen hasta un tráfico de 450 Mbps, permiten 750 sesiones vpn y pueden conectarse físicamente hasta 5 interfaces para brindar un soporte de hasta 150 Vlans.

## 2.7 REPOTENCIACIÓN DEL CABLEADO ESTRUCTURADO CONSIDERANDO LA COBERTURA DE LAS DOS INSTITUCIONES

### RESTRUCTURACIÓN DEL CENTRO DE DATOS (CD)

El Data Center o DC se localiza en el primer piso alto del Bloque 9 indicado en el plano de conexiones entre edificios el mismo que cubre el Bloque 9 y el Bloque 8 en un total de 55 puntos de datos cat-6A. Además se decidió colocar un rack adicional en el Data Center para diferenciar la infraestructura nueva de la antigua y se mantuvo la topología anterior en la que separaba los equipos activos en un rack y los pasivos en otra colocando de esta manera el firewall CISCO ASA-5520 en el Rack R3.

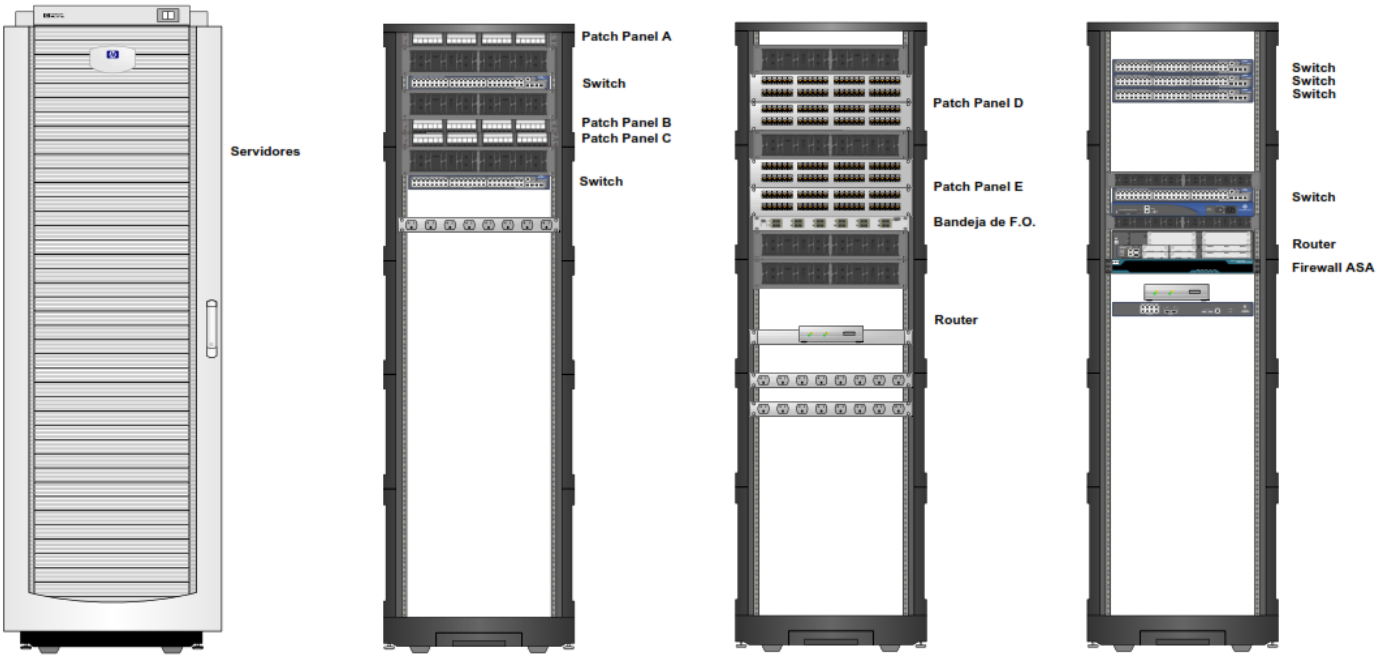


Figura 2.4. Diagrama de Rack de Centro de Datos

Fuente: Mario Pinos Guerra (2016)

## RACK CT1

El primer Rack se localiza en el Bloque 2 en el CT-1 indicado en el plano de conexiones entre edificios este rack cubre el Bloque 2, Bloque 3 y el Bloque 5 en total 103 puntos de datos cat-6A

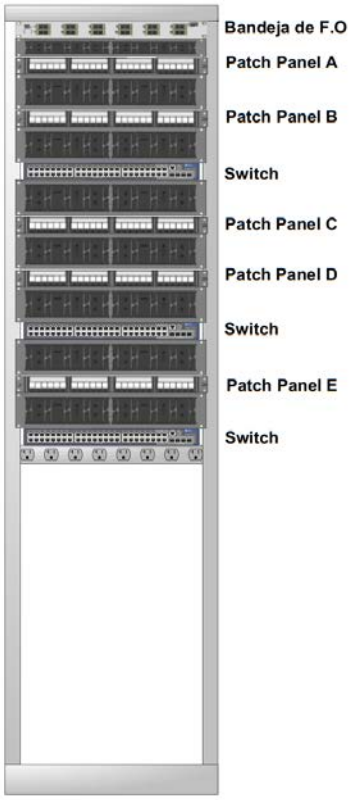


Figura 2.5. Diagrama de Rack de CT-1

Fuente: Mario Pinos Guerra (2016)

## RACK CT2

El Segundo y Tercer Rack se localiza en el Bloque 4 en el CT-2 indicado en el plano de conexiones entre edificios este rack cubre el Bloque 4, Bloque 6 y el Bloque 10 en total 91 puntos de datos cat-6A


Figura 2.6. Diagrama de Rack CT-2
Fuente: Mario Pinos Guerra (2016)

## RACK DE CT3

El Cuarto Rack se localiza en el primer piso alto del Bloque 11 en el CT-3 indicado en el plano de conexiones entre edificios este rack cubre el Bloque 11 en total 53 puntos de datos cat-6A.

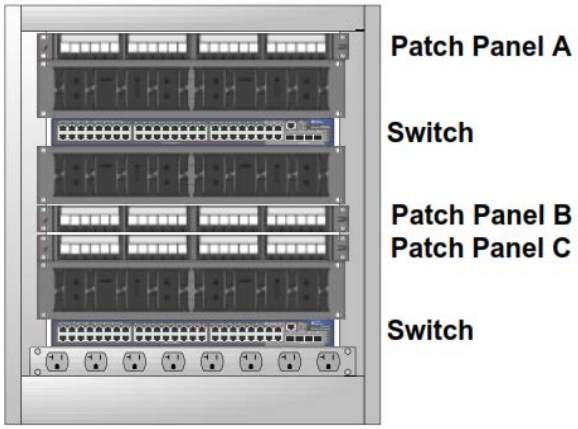


Figura 2.7. Diagrama de Rack CT-3
Fuente: Mario Pinos Guerra (2016)

**RACK CT4**

El Quinto Rack se localiza en el Segundo piso alto del Bloque 14 en el CT-4 indicado en el plano de conexiones entre edificios este rack cubre el Bloque 14 en total 49 puntos de datos cat-6A.

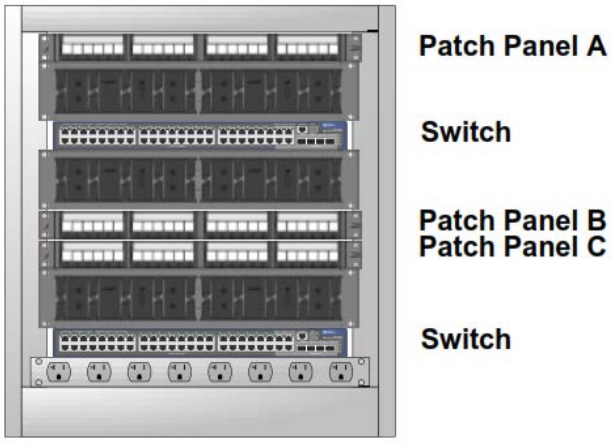


Figura 2.8. Diagrama de Rack CT-4
Fuente: Mario Pinos Guerra (2016)

## INFRAESTRUCTURA GENERAL DEL CABLEADO ESTRUCTURADO DE DATOS

El Cableado de Datos está compuesto por 351 puntos Categoría 6-A, el recorrido del Punto es; del Switch sale un Patch Cord Categoría 6-A, que luego de pasar por el organizador horizontal, llega a un puerto del Patch panel; que es donde sale el cable STP Categoría 6-A. El mismo que viaja por un electro canal, donde se distribuye por tuberías de 1” o ¾ hacia la parte superior de cada punto, hasta una caja de paso que anuncia la bajada del STP, por canaletas decorativas de diferentes mediadas hacia una caja rectangular empotrada o sobre puesta donde se coloca un faceplate de diferentes servicios conectado a un Jack Categoría 6-A del cual sale un Patch Cord Categoría 6-A, flexible que se unirá a la tarjeta de red de cualquier equipo que se desee conectar la LAN.

## 2.8 IMPLEMENTACIÓN DE LOS FIREWALL DE BORDE Y LEVANTAMIENTO DE SEGURIDADES EN LOS ENLACES VPN'S (GUAYAQUIL – QUITO) Y (GUAYAQUIL – CUENCA).

### Equipo Guayaquil:

Para minimizar el impacto de la migración de configuraciones al Cisco ASA y debido a la existencia de direcciones IP secundarias en la configuración inicial, fue necesario configurar dos interfaces para la red interna y una para la conexión de la red externa, el siguiente gráfico muestra al equipo y sus conexiones físicas.

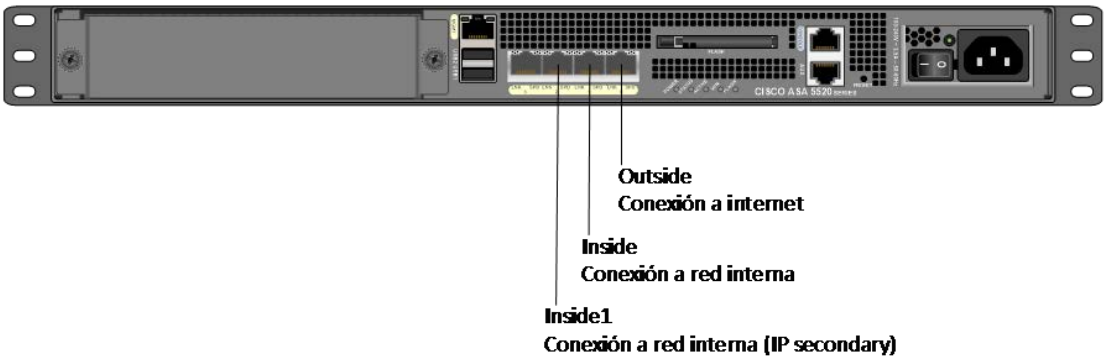


Figura 2.9. Conexión de Firewall de Guayaquil
Fuente: Mario Pinos (2016)

Todas las interfaces del equipo son Gigabit Ethernet y su nomenclatura corresponde al slot 0; Las direcciones IP asignadas a las interfaces son las siguientes;

Tabla 4. IP´s asignadas a interfaces en Firewall de Guayaquil

| Interface | Nomenclatura | Dirección IP |
|---|---|---|
| **outside** | Gi0/0 | 186.0.20.1/24 |
| **inside** | Gi0/1 | 172.10.200.1/24 |
| **inside1** | Gi0/2 | 172.72.94.252 |

Fuente: Mario Pinos Guerra (2016)

La ruta por defecto se encuentra en la interface outside y tiene como pasarela la dirección IP: 186.0.20.9. Además se configuró varias rutas dentro de la red interna, como lo muestra la tabla a continuación:

Tabla 5. Rutas internas en Firewall de Guayaquil

| Interface | Red destino | Mask destino | Puerta enlace |
|---|---|---|---|
| **inside1** | 10.10.0.0 | 255.255.0.0 | 10.72.92.254 |
| **inside1** | 10.10.100.0 | 255.255.255.0 | 10.72.94.254 |
| **inside1** | 10.20.0.0 | 255.255.0.0 | 10.72.94.253 |
| **inside1** | 10.72.95.0 | 255.255.255.0 | 10.72.94.254 |
| **inside1** | 10.72.96.0 | 255.255.255.0 | 10.72.94.254 |
| **inside1** | 172.16.0.0 | 255.255.0.0 | 10.72.94.254 |

Fuente: Mario Pinos Guerra (2016)

Para habilitar el acceso desde internet a un servicio ubicado en la red interna, es necesario que el equipo que realiza dicha función pueda acceder al internet con una dirección IP Pública. Así mismo que permita el tráfico en ambos sentidos, para esto se configuraron las siguientes reglas de enmascaramiento con las siguientes direcciones IP;

Tabla 6. Enrutamiento para Acceso a Internet en Firewall de Guayaquil

| Origen | | Destino | |
|---|---|---|---|
| **inside1** | 10.72.94.30 | **outside** | 186.10.10.4 |
| **inside1** | 10.72.94.31 | **outside** | 186.10.10.5 |
| **inside1** | 10.72.94.23 | **outside** | 186.10.10.6 |
| **inside1** | 10.72.94.43 | **outside** | 186.10.10.7 |
| **inside1** | 10.72.94.37 | **outside** | 186.10.10.8 |
| **inside1** | 10.72.94.65 | **outside** | 186.10.10.10 |
| **inside1** | 10.72.94.22 | **outside** | 186.10.10.11 |
| **inside1** | 10.72.94.47 | **outside** | 186.10.10.12 |
| **inside1** | 10.72.94.70 | **outside** | 186.10.10.13 |
| **inside1** | 10.72.94.39 | **outside** | 186.10.10.14 |

Fuente: Mario Pinos Guerra (2016)

Para cada dirección enmascarada se configuraron permisos para puertos tcp definidos, estos permisos se muestran en la siguiente tabla:

Tabla 7. Permisos de accesos a puertos por dirección IP en Firewall de Guayaquil

| IP Privada | Servicio | IP Publica | Servicio | Observaciones |
|---|---|---|---|---|
| **10.72.94.30** | | 186.10.10.4 | | Acceso Internet |
| **10.72.94.31** | 80,443,5432 | 186.10.10.5 | 80,443,5432 | |
| **10.72.94.37** | 25,110,587,143,465, 993,995 | 186.10.10.8 | 25,110,587,143,465,993, 995 | Correo Antiguo |
| **10.72.94.47** | 25,110,587,143,465, 993,995 | 186.10.10.12 | 25,110,587,143,465,993, 995 | Correo Nuevo |
| **10.72.94.65** | | 186.10.10.10 | | mstsc |
| **10.72.94.43** | 80,8080,443,3306 | 186.10.10.7 | 80,8080,443,3306 | Documents |
| **10.72.94.70** | 9090,9091,5222,5223, 5269,5275,7070,7443, 3478,3479,5229,22,21 | 186.10.10.13 | 9090,9091,5222,5223, 5269,5275,7070,7443, 3478,3479,5229,1021,21 | Acceso Internet |
| **10.72.94.22** | | 186.10.10.11 | | MIES - mstsc |
| **10.72.94.39** | 80,22,3306 | 186.10.10.6 | 80,1021,3306 | Varios |

Fuente: Mario Pinos Guerra (2016)

Para los equipos que no tengan la necesidad de brindar servicios en internet y únicamente necesiten consumir servicios de ella, se configuró un enmascaramiento dinámico basado en un grupo de acceso llamado srvInternetProxy, el cual accede a internet utilizando solamente una dirección IP pública: 186.10.10.2.

Las conexiones con las oficinas de Quito y Cuenca se establecen a través de enlaces VPN peer-to-peer; El tráfico es enviado hacia estos destinos a través de listas de acceso, los mismos lo clasifican y lo encapsulan en modo encriptado, Los túneles se registraron mediante la siguiente configuración:

Tabla 8. Configuración de Túneles Guayaquil-Quito, Guayaquil-Cuenca

| Ip Destino | Clave | Redes Origen | Redes Destino | Crypto |
|---|---|---|---|---|
| **186.0.30.6** | 5t4r3e2w1q | 10.10.0.0/16 ; 10.72.0.0/24 | 192.168.0.0/16 | ESP-3DES-SHA |
| **186.0.10.1** | 5t4r3e2w1q | 10.10.0.0/16 ; 10.72.0.0/24 | 10.30.0.0/16 | ESP-3DES-SHA |

Fuente: Mario Pinos Guerra (2016)

Estas configuraciones son aplicadas en forma inversa en los equipos destino.

La administración del equipo se la puede realizar desde cualquiera de las redes internas utilizando un navegador con la URL:

Desde la inside: https://172.10.200.1/.

Desde la inside1: https://172.72.94.252/

Las credenciales para acceso son; admin/admin. Se recomienda reemplazar el usuario y/o contraseña una vez entregado el proyecto.

**Equipo Quito:**

El equipo ubicado en la ciudad de Quito posee una configuración similar al equipo de Guayaquil, con la diferencia que en este equipo no se encuentran los enmascaramientos estáticos. La siguiente gráfica muestra las conexiones físicas del equipo:

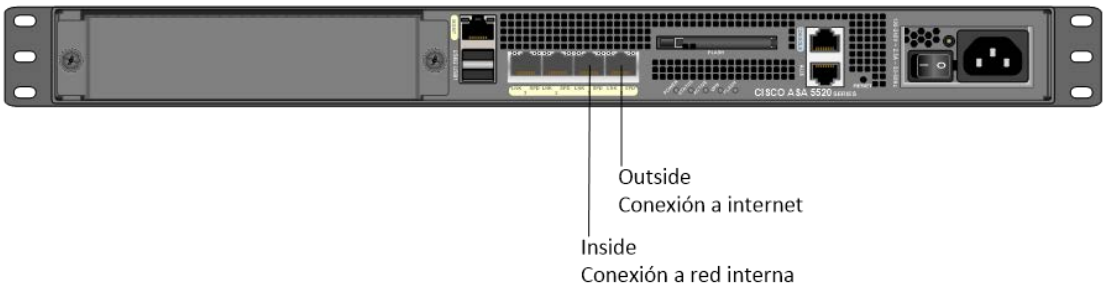


Figura 2.10. Conexiones de Firewall de Quito

Fuente: Mario Pinos Guerra (2016)

Las interfaces poseen la siguiente configuración:

Tabla 9. IP´s asignadas a interfaces en Firewall de Quito

| Nombre | Interface | IP | Mascara |
|---|---|---|---|
| **Outside** | GigabitEthernet0 | 186.0.30.6 | 255.255.255.248 |
| **Inside** | GigabitEthernet0 | 192.168.3.2 | 255.255.0.0 |

Fuente: Mario Pinos Guerra (2016)

El equipo posee únicamente una ruta por defecto que utiliza la puerta de enlace 186.0.30.5 a través de la interface outside.

Para el acceso a internet se habilitó un grupo de objetos que se enmascaran a través de la IP pública: 186.0.30.1; la administración del equipo se realiza de manera similar al de Guayaquil a través de las siguientes URL:

Red inside https://192.168.3.2/

Red Outside https://186.0.30.6 únicamente desde la IP pública: 186.10.10.2 que es la dirección IP para administración del equipo desde la oficina GYE.

**Equipo Cuenca:**

El equipo ubicado en la oficina de Cuenca al igual que el de Guayaquil, posee dos interfaces conectadas a la red Inside; debido a que el equipo que se reemplazó poseía una interface con una dirección IP secundaría.

El gráfico siguiente muestra la conexión física utilizada:

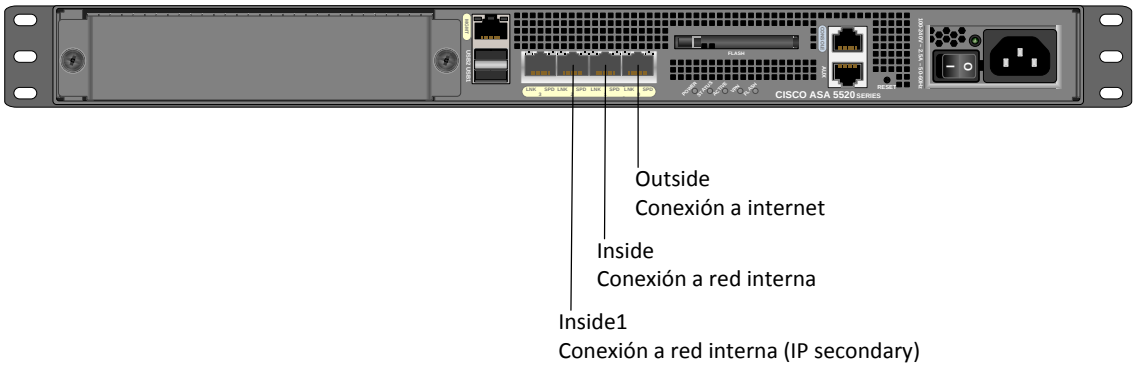


Figura 2.11. Conexiones de Firewall de Cuenca

Fuente: Mario Pinos Guerra (2016)

El direccionamiento IP de las interfaces se muestra a continuación:

Tabla 10. IP´s asignadas a interfaces en Firewall de Cuenca

| Nombre | Interface | IP | Máscara |
|---|---|---|---|
| **Outside** | GigabitEthernet0/0 | 186.0.10.1 | 255.255.255.248 |
| **inside1** | GigabitEthernet0/1 | 172.30.10.1 | 255.255.255.0 |
| **inside2** | GigabitEthernet0/2 | 192.168.0.1 | 255.255.255.0 |

Fuente: Mario Pinos Guerra (2016)

Esta oficina no posee servicios publicados a internet y únicamente mantiene un grupo de enmascaramiento dinámico para acceso a la web, con la dirección pública: 190.95.200.148.

El acceso administrativo es posible mediante las URL:

Desde la red inside1 a través de http://172.30.10.1/

En la red externa con la URL: http://186.0.10.1/ únicamente desde la oficina de GYE.

## 2.9 INSTALACIÓN Y MIGRACIÓN DE SERVICIOS EN SERVIDORES DEDICADOS-CENTOS.

**http://186.10.10.12/intranet**

Link para ingreso a la Intranet corporativa de la Entidad instalada en el servidor nuevo HP DL360p Gen8

Usuario admin password admin

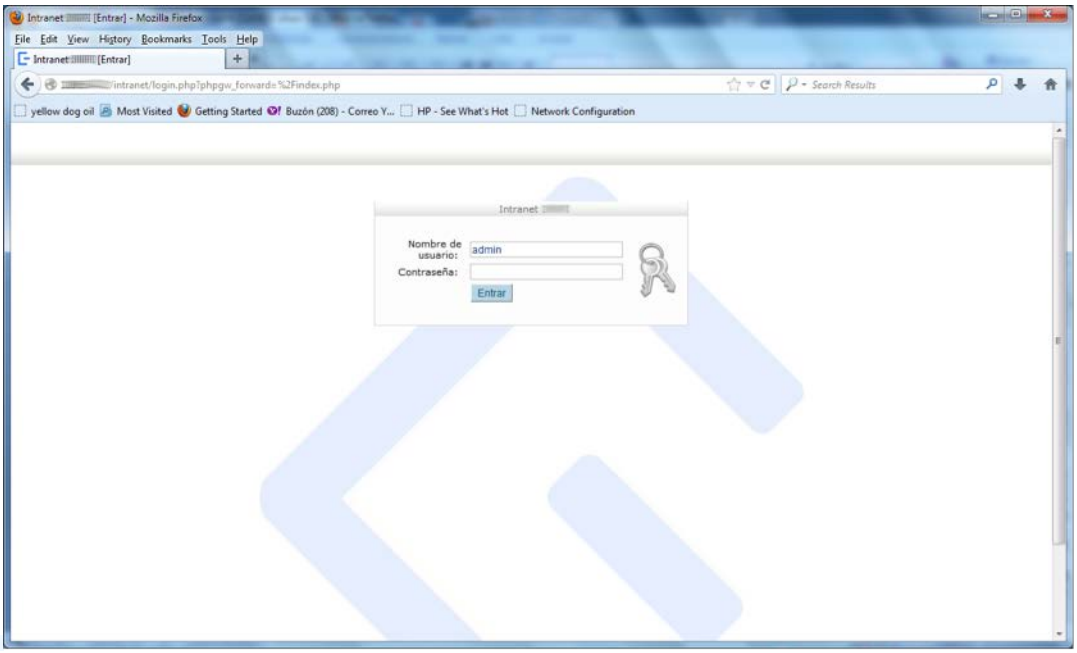


Figura 2.12. Portal de Ingreso a Intranet migrado

Fuente: Mario Pinos Guerra (2016)

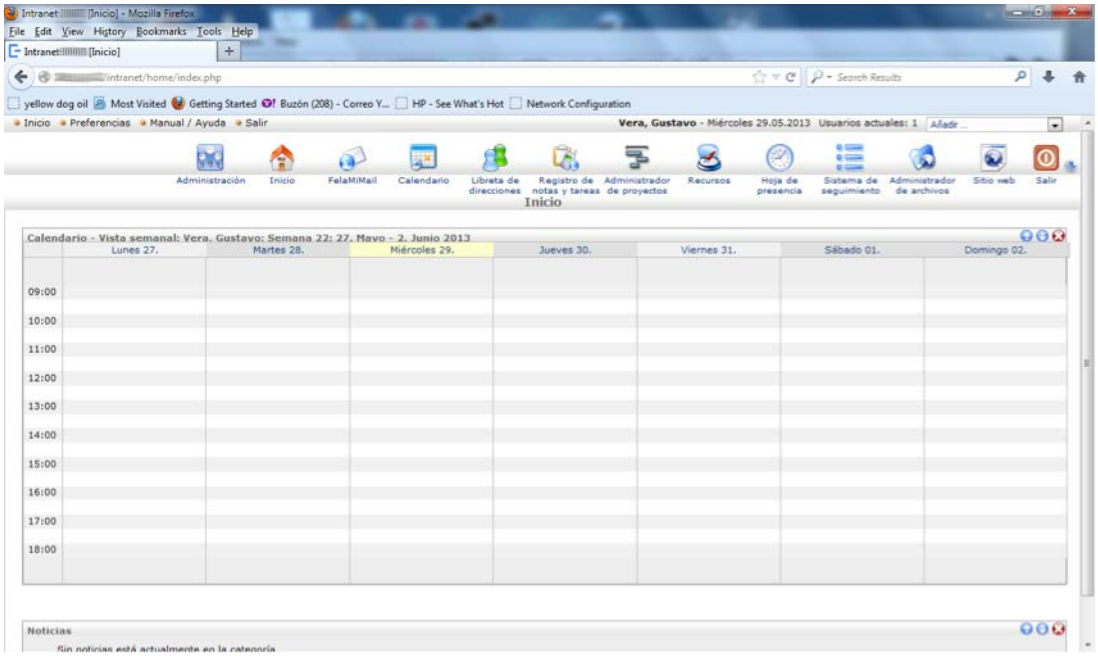


Figura 2.13. Portal de Intranet

Fuente: Mario Pinos Guerra (2016)

**http://mail.entidad.org/intranet**

Link para ingreso a la Intranet corporativa de la Entidad instalada en el servidor Virtualizado, donde está instalado el correo con el dominio entidad.org.

Esta instalación debido al tamaño del disco duro del servidor DL 360p, se la puede usar como un repositorio adicional de documentos o como una contingencia.

Usuario admin password admin

## Correo electrónico

Link para ingreso a la consola de administración del servidor de Correo

**https://186.10.10.12:10000/**

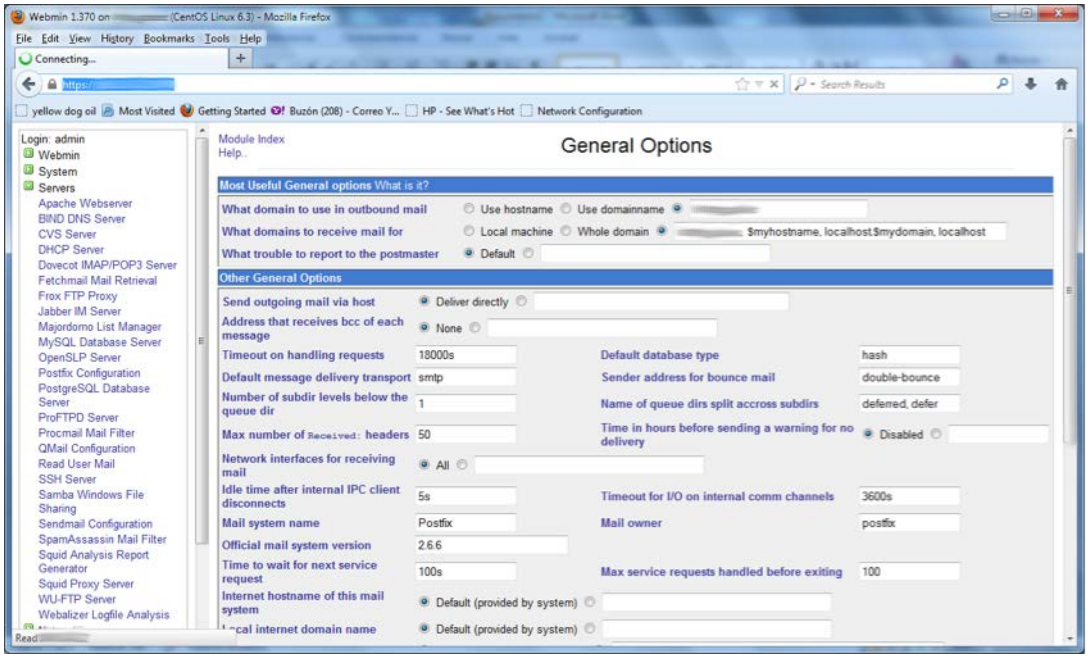


Figura 2.14. Consola de Administración de correo electrónico

Fuente: Mario Pinos Guerra (2016)

## Webmail Servidor de correo dominio

Link para ingreso al Webmail **http://186.10.10.12/correo.html**

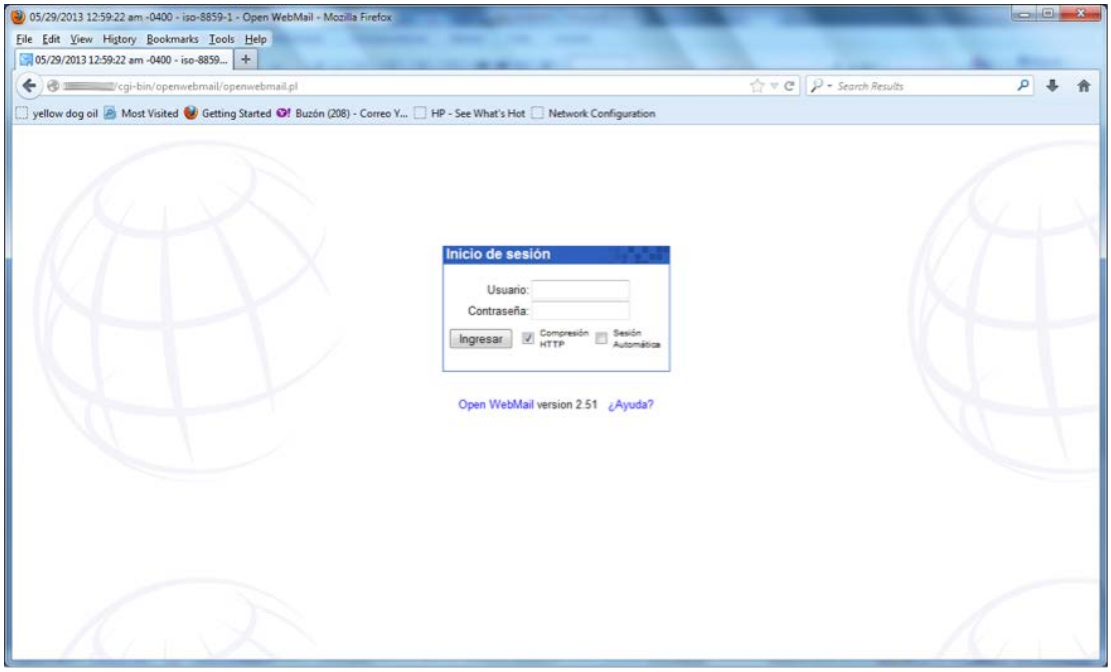


Figura 2.15. Enlace de acceso a Webmail

Fuente: Mario Pinos Guerra (2016)

## Prueba de envío de correo hacia un dominio externo desde el servidor

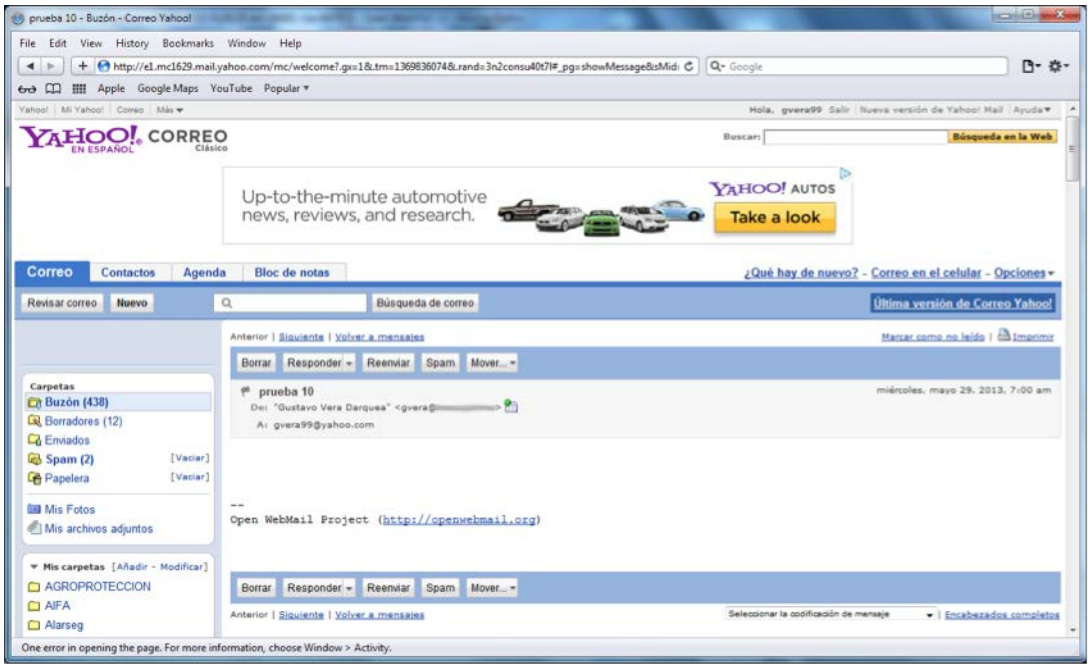


Figura 2.16. Prueba de envío de correo hacia dominio externo

Fuente: Mario Pinos Guerra (2016)

**Servidor de Chat OpenFire**

Link para ingreso a la consola de administración del servidor de Chat:

**http://186.10.10.13:9090/**

usuario: admin password: admin

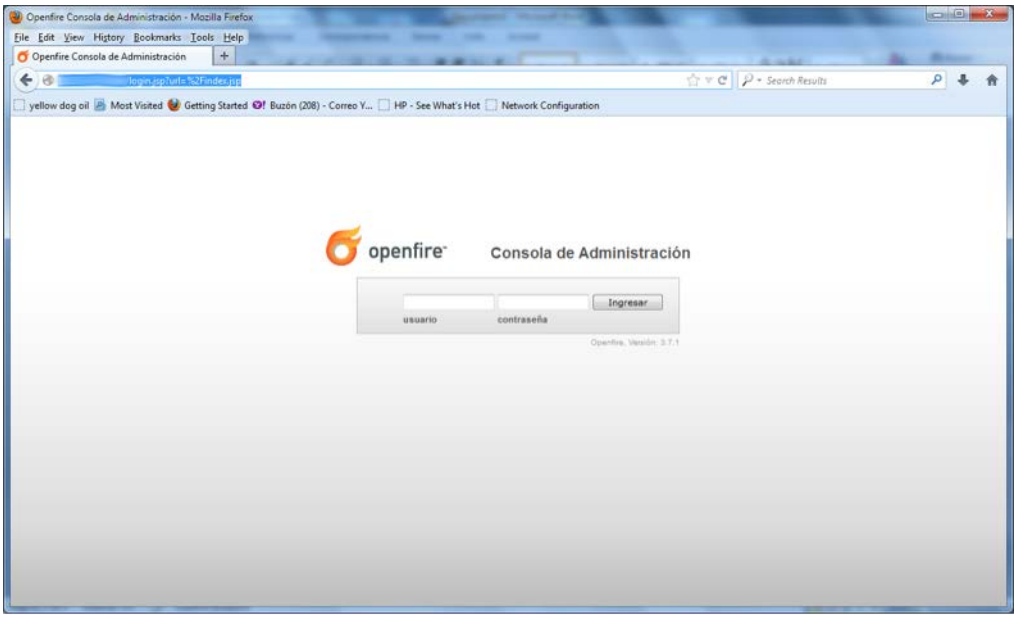


Figura 2.17. Ingres de la consola de administración del Servidor de Chat

Fuente: Mario Pinos Guerra (2016)

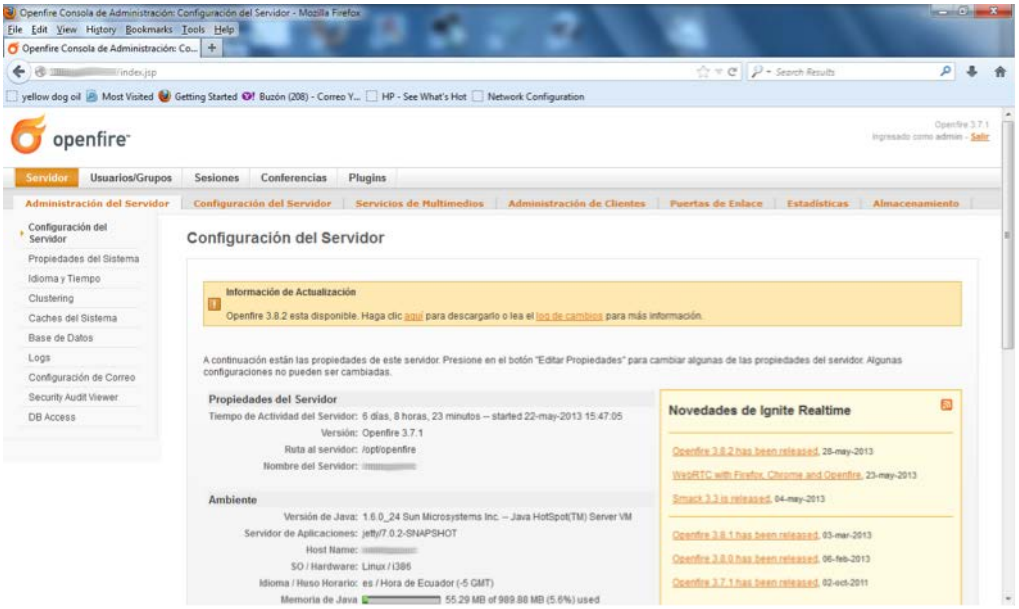


Figura 2.18. Consola de administración del servidor chat

Fuente: Mario Pinos Guerra (2016)

Link para acceso del cliente Spark para conexión al servidor desde un browser

**http://186.10.10.13/chat/**

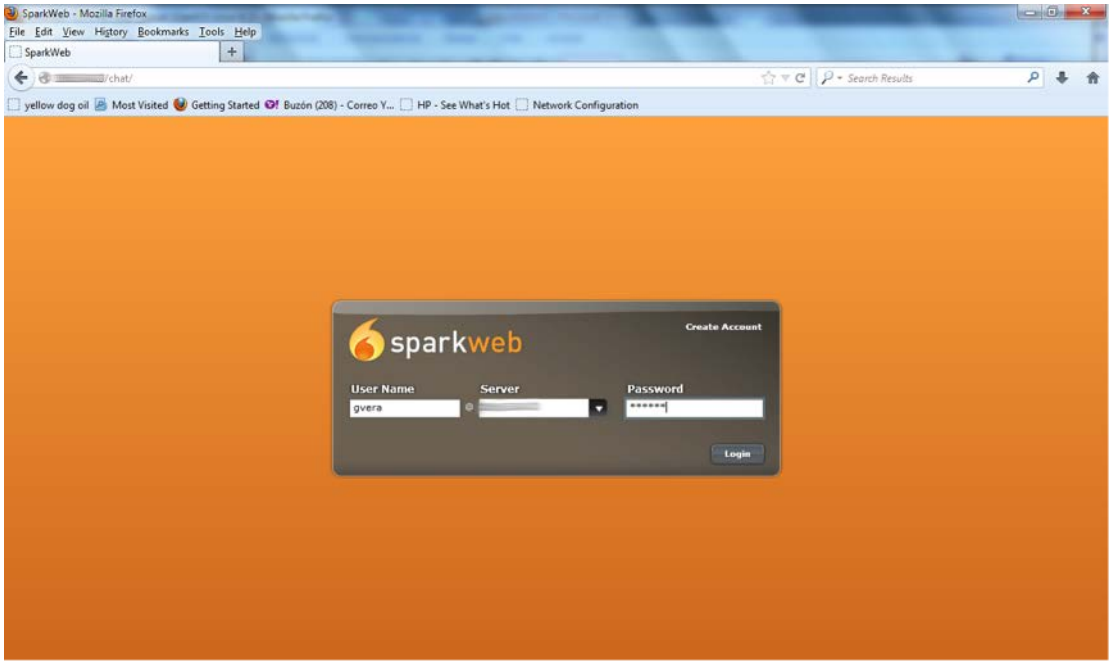


Figura 2.19. Portal de ingreso para clientes del servicio de chat

Fuente: Mario Pinos Guerra (2016)

Prueba de conexión al servidor Openfire a través del cliente web Sparkweb a la dirección 186.10.10.13

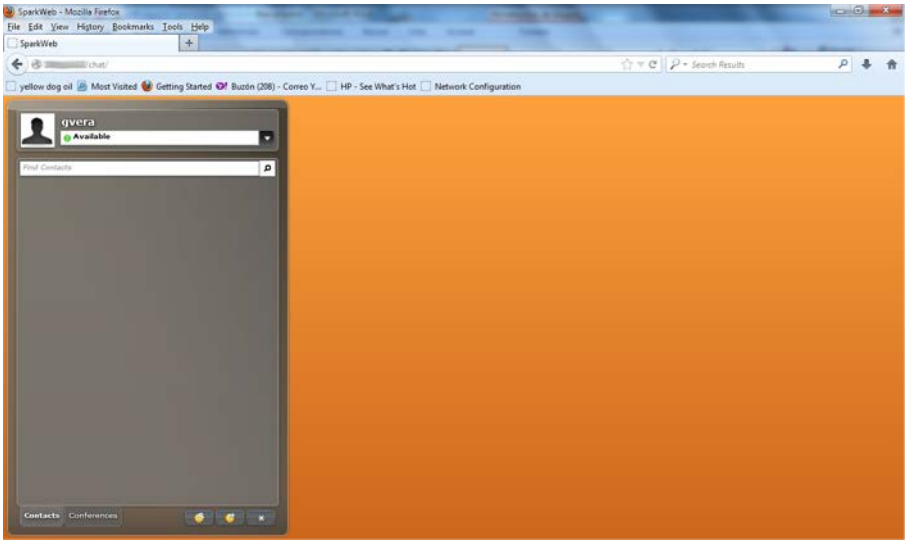


Figura 2.20. Prueba sobre cliente en entorno web del servicio de chat

Fuente: Mario Pinos Guerra (2016)

Prueba de conexión al servidor Openfire a traves del cliente Spark a la dirección 186.10.10.13 desde un PC con Windows 7

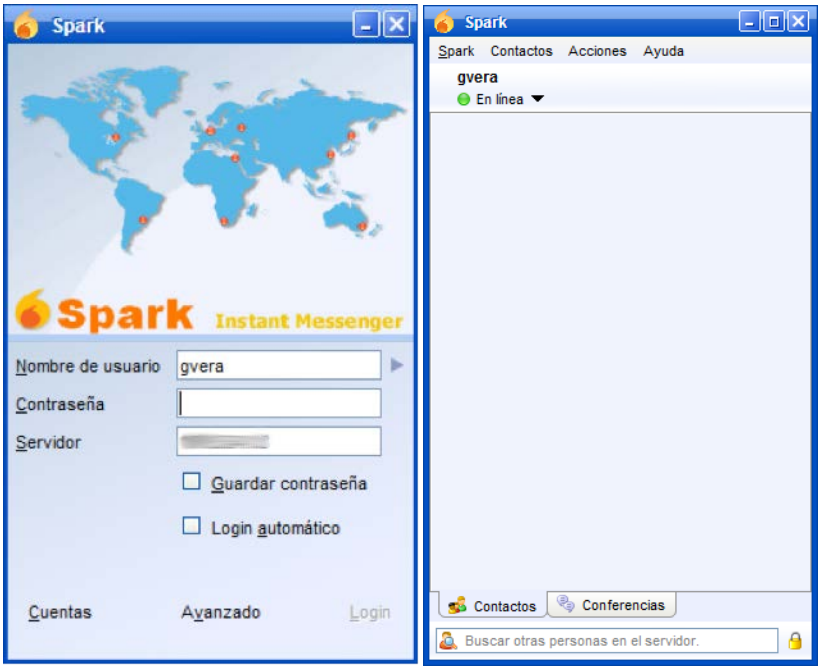


Figura 2.21. Prueba sobre cliente sobre plataforma Windows 7

Fuente: Mario Pinos Guerra (2016)

## OpenVPN

Las configuraciones del servidor VPN se encuentran en el servidor mail.entidad.org dentro de /etc/openvpn/keys, donde están ubicadas los certificados digitales para cada uno de los clientes remotos que se van a conectar al equipo a través del cliente OpenVPN.

Output conexión cliente OpenVpn desde sitio remoto exitosa

```
Wed May 29 12:53:59 2013 OpenVPN 2.2.1 Win32-MSVC++ [SSL] [LZO2] built on Jul  1 2011
Wed May 29 12:53:59 2013 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to call user-defined scripts or
executables
Wed May 29 12:53:59 2013 LZO compression initialized
Wed May 29 12:53:59 2013 Control Channel MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Wed May 29 12:53:59 2013 Socket Buffers: R=[8192->8192] S=[8192->8192]
Wed May 29 12:53:59 2013 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
Wed May 29 12:53:59 2013 Local Options hash (VER=V4): '41690919'
Wed May 29 12:53:59 2013 Expected Remote Options hash (VER=V4): '530fdded'
Wed May 29 12:53:59 2013 UDPv4 link local: [undef]
Wed May 29 12:53:59 2013 UDPv4 link remote: 186.10.10.8:1194
Wed May 29 12:54:01 2013 TLS: Initial packet from 186.10.10.8:1194, sid=74581607 12c7b480
Wed May 29 12:54:02 2013 VERIFY OK: depth=1,
/C=EC/ST=Guayas/L=Guayaquil/O=ENTIDAD/CN=ENTIDAD_CA/emailAddress=admin@entidad.org
Wed May 29 12:54:02 2013 VERIFY OK: nsCertType=SERVER
Wed May 29 12:54:02 2013 VERIFY OK: depth=0,
/C=EC/ST=Guayas/L=Guayaquil/O=ENTIDAD/CN=server/emailAddress=admin@entidad.org
Wed May 29 12:54:14 2013 Data Channel Encrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed May 29 12:54:14 2013 Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed May 29 12:54:14 2013 Data Channel Decrypt: Cipher 'BF-CBC' initialized with 128 bit key
Wed May 29 12:54:14 2013 Data Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Wed May 29 12:54:14 2013 Control Channel: TLSv1, cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 1024 bit RSA
Wed May 29 12:54:14 2013 [server] Peer Connection Initiated with 186.10.10.8:1194
Wed May 29 12:54:16 2013 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
Wed May 29 12:54:16 2013 PUSH: Received control message: 'PUSH_REPLY,route 10.72.94.0 255.255.0.0,dhcp-
option DNS 10.72.94.37,route 192.168.245.1,topology net30,ping 10,ping-restart 120,ifconfig 192.168.245.6
192.168.245.5'
Wed May 29 12:54:16 2013 OPTIONS IMPORT: timers and/or timeouts modified
Wed May 29 12:54:16 2013 OPTIONS IMPORT: --ifconfig/up options modified
Wed May 29 12:54:16 2013 OPTIONS IMPORT: route options modified
Wed May 29 12:54:16 2013 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Wed May 29 12:54:16 2013 ROUTE default_gateway=192.168.1.1
Wed May 29 12:54:16 2013 TAP-WIN32 device [{79322B77-B038-42B5-A88E-AE20B5933F23}] opened:
\\.\Global\{79322B77-B038-42B5-A88E-AE20B5933F23}.tap
Wed May 29 12:54:16 2013 TAP-Win32 Driver Version 9.8
Wed May 29 12:54:16 2013 TAP-Win32 MTU=1500
Wed May 29 12:54:16 2013 Notified TAP-Win32 driver to set a DHCP IP/netmask of 192.168.245.6/255.255.255.252
on interface {79322B77-B038-42B5-A88E-AE20B5933F23} [DHCP-serv: 192.168.245.5, lease-time: 31536000]
Wed May 29 12:54:16 2013 Successful ARP Flush on interface [11] {79322B77-B038-42B5-A88E-AE20B5933F23}
Wed May 29 12:54:22 2013 TEST ROUTES: 3/3 succeeded len=3 ret=1 a=0 u/d=up
Wed May 29 12:54:22 2013 C:\WINDOWS\system32\route.exe ADD 10.72.94.0 MASK 255.255.0.0 192.168.245.5
Wed May 29 12:54:22 2013 Warning: address 10.72.94.0 is not a network address in relation to netmask
255.255.0.0
Wed May 29 12:54:22 2013 ROUTE: route addition failed using CreateIpForwardEntry: The parameter is incorrect.
[status=87 if_index=11]
Wed May 29 12:54:22 2013 Route addition via IPAPI failed [adaptive]
Wed May 29 12:54:22 2013 Route addition fallback to route.exe
The route addition failed: The parameter is incorrect.
Wed May 29 12:54:22 2013 C:\WINDOWS\system32\route.exe ADD 10.72.94.0 MASK 255.255.0.0 192.168.245.5
Wed May 29 12:54:22 2013 Warning: address 10.72.94.0 is not a network address in relation to netmask
255.255.0.0
Wed May 29 12:54:22 2013 ROUTE: route addition failed using CreateIpForwardEntry: The parameter is incorrect.
[status=87 if_index=11]
Wed May 29 12:54:22 2013 Route addition via IPAPI failed [adaptive]
Wed May 29 12:54:22 2013 Route addition fallback to route.exe
The route addition failed: The parameter is incorrect.
Wed May 29 12:54:22 2013 C:\WINDOWS\system32\route.exe ADD 192.168.245.1 MASK 255.255.255.255
192.168.245.5
Wed May 29 12:54:22 2013 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=30 and
dwForwardType=4
Wed May 29 12:54:22 2013 Route addition via IPAPI succeeded [adaptive]
Wed May 29 12:54:22 2013 Initialization Sequence Completed
```

Figura 2.22. Conexión VPN exitosa
Fuente: Mario Pinos Guerra (2016)

**Proxy Server**

**https://186.10.10.13:10000**

Usuario: root password: 123456

# CAPÍTULO 3

# ANÁLISIS DE RESULTADOS

## 3.1 ANÁLISIS COMPARATIVO DE LOS RESULTADOS OBTENIDOS PRODUCTO DE LA REPOTENCIACIÓN DE LA INFRAESTRUCTURA.

Tabla 11. Tabla de Análisis de resultados obtenidos

| INFRAESTRUCTURA ANTERIOR | DESCRIPCIÓN | INFRAESTRUCTURA NUEVA | DESCRIPCIÓN |
|---|---|---|---|
| **Cableado Estructurado** | El cableado estructurado estaba diseñado para dar servicio a un máx. de 342 usuarios, el cuál al ser cat-5e permitía una velocidad máxima de conexión de 100 Mbps, los enlaces de cobre carecían de redundancias y eran categoría 5e mientras que los enlaces de F.O. eran multimodo de 62.5/125. | **Cableado Estructurado** | El cableado estructurado está diseñado para dar servicio a una máximo de 650 usuarios, este es categoría 6A el cual nos permite una velocidad de conexión máxima de 10 Gbps, los enlaces de cobre tienen redundancia (n+3) y también pertenecen a la misma categoría de los puntos finales, los enlaces de F.O. son multimodo de 4 hilos 50/125. |

| INFRAESTRUCTURA ANTERIOR | DESCRIPCIÓN | INFRAESTRUCTURA NUEVA | DESCRIPCIÓN |
|---|---|---|---|
| **Mampostería** | Las paredes del Centro de Datos eran de mampostería de madera y estructura metálica con divisiones y sin piso falso. | **Obra Civil** | Las paredes del Centro de Datos son de bloque enlucida y pintada en área de 12.5 $m^2$, tiene una puerta semiblindada y su techo es de Gypsum con malla electro soldada para evitar intrusiones, tiene una ventana sellada con vidrio antirrobo de 20mm (100cm x 80cm), su piso falso para el área de centro de datos tiene una rampa para facilitar ingreso de equipos activos. |
| **Sistema de Climatización** | El sistema de climatización consistía en un aire acondicionado de pared tipo cajón de 12000 btu. | **Sistema de Climatización** | La solución de climatización es de dos equipo de climatización serie 7 de 2.5 Ton. Tipo Split Data Center con tarjetas de monitoreo remoto M52. |
| **UPS** | El sistema de respaldo consistía en un equipo de 8KVA con una autonomía de carga media de 15 min y de autonomía a carga completa de 6min sin banco de baterías. | **UPS** | La solución incluye una UPS de 10 KVA con autonomía a media carga de 20 min y a carga completa de 7 min, adicional a esto un banco de baterías con una autonomía de 30 min para que el equipo nuevo funcione como master y el ya existente funcione como respaldo del sistema. |
| **Servidores** | El servidor instalado era una solución blade HP que cumplía la función de repositorio y que brindaba los servicios de correo electrónico en la entidad los mismos que estaban virtualizados. | **Servidores** | Se adicionó dos servidores HP DL380p Gen8 E5-2650 con el objetivo de balancear la carga de accesos y programas existentes en el servidor Blade por lo tanto se migró 1500 cuentas al nuevo servidor, se migro una parte del repositorio y se instaló un software de colaboración Intranet con chat interno, se migró el proxy server y se configuró un VPN server |

| INFRAESTRUCTURA ANTERIOR | DESCRIPCIÓN | INFRAESTRUCTURA NUEVA | DESCRIPCIÓN |
|---|---|---|---|
| **Seguridad – Acceso** | Existía una puerta de aluminio de oficina. | **Seguridad - Acceso** | Se instaló un panel lector de tarjetas y de seguridad biométrica para controlar una cerradura magnética de 1200 lb - 545 Kg de retención adicional de esto se instaló una solución de vigilancia con un NVR de 5 canales de las cuales una cámara esta en exterior y las otras cuatro distribuidas en las esquinas del centro de datos. |
| **Sistema de mitigación de incendios** | El sistema consistía en un extintor de polvo químico seco de 10Kg. | **Sistema de mitigación de incendios** | El sistema fue fortalecido con un sistema contra incendio con sensores de humo y estaciones manuales que disparan el FM-200 de la bombona. |
| **Enlaces VPN** | La solución instalada era de un grupo de Routers marca HP que cumplían la función de equipos de enlace por los que se levantaban los enlaces VPN para dar servicio a las otras dos sucursales que quedan en Quito y Cuenca respectivamente ambas reciben a través de los enlaces los servicios de Internet, correo, aplicaciones de la entidad, etc.., al no ser un equipo diseñado para hacer filtrado pero puede realizarlo sacrifica como resultado velocidad de conexión la que se incrementa en función del aumento de usuarios. | **Enlaces VPN** | Se migró la configuración de enmascaramientos, permisos de acceso y túneles VPN los equipos anteriormente brindaban ese servicio al nuevo esquema de protección perimetral basada en equipos Cisco ASA 5520 los mismos que pueden ejecutar control de acceso en ambientes que manejen hasta un tráfico de 450 Mbps, permiten 750 sesiones VPN y pueden conectarse físicamente hasta 5 interfaces para brindar un soporte de hasta 150 Vlans lo que me permite poder crecer de ser necesario sin mayor problema debido a las altas características del equipo. |

Fuente: Mario Pinos Guerra (2016)

# CONCLUSIONES Y RECOMENDACIONES

Después del desarrollo anterior se concluye lo siguiente:

1. Las políticas de seguridad aplicadas en los corta fuegos sean las más sencillas para evitar que el sistema se vuelva un cuellos de botella.

2. Para el fortalecimiento de los servidores es necesario detectar cuales son los puertos que se necesitan para que los servicios o aplicaciones se ejecuten de manera adecuada y cerrar el resto de puertos para prevenir fallos de seguridad.

3. Todos los subsistemas que funcionan dentro de un centro de datos tienen su respectiva vulnerabilidad, se les debe dar el tratamiento adecuado para ayudar a mitigar los posibles riesgos que se puedan generar por el agujero de seguridad de cada uno de ellos.

4. Concientizar al personal de la entidad para el uso de buenas prácticas con respecto a la seguridad de la información

# BIBLIOGRAFÍA

[1] Tyco Electronics Corporation, «Ubicación de espacios de telecomunicaiones,» *Diseño de Cableado de Redes,* pp. 3, 4, 5, 2010.

[2] Grupo Cofitel, «c3comunicaciones.es,» 14 Febrero 2014. [En línea]. Available: http://www.c3comunicaciones.es/data-center-el-estandar-tia-942/.

[3] S. Harris, All in one CISSP, Mc Graw Hill, 2013.

[4] G. G. Enrich, «El estándar TIA-942,» Julio 2007. [En línea]. Available: http://www.areadata.com.ar/pdf/El%20standard%20TIA%20942%20-vds-11-4.pdf.

[5] Black Box Network Services, «Blackbox.com,» 2010. [En línea]. Available: https://www.blackbox.com/resource/genpdf/white-papers/cat6a-futp-vs-utp.pdf.

[6] A. Noordergraaf, «Sun BluePrints - Building Secure N-Tier Environments,» Octubre 2000. [En línea]. Available: http://sun.com/blueprints.

[7] EIA/TIA 568-A, Julio 1991. [En línea]. Available: http://www.tiaonline.org/.