**TRABAJO ESPECIAL DE GRADO**

# DISEÑO DE PLATAFORMA DE SEGURIDAD EN CENTRO DE DATOS LA COLINA, CASO CORPORACIÓN DIGITEL

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Sánchez S., Celsa C.
para optar al título de
Ingeniero Electricista

Caracas, 2013

**TRABAJO ESPECIAL DE GRADO**

# DISEÑO DE PLATAFORMA DE SEGURIDAD EN CENTRO DE DATOS LA COLINA, CASO CORPORACIÓN DIGITEL

PROF. GUIA: Ing. CARLOS MORENO
TUTOR INDUSTRIAL: Ing. GISELLA LUCAR

Presentado ante la Ilustre
Universidad Central de Venezuela
por la Br. Sánchez Santana, Celsa Carolina
para optar al título de
Ingeniero Electricista

Caracas, 2013

# CONSTANCIA DE APROBACIÓN

Caracas, 07 de junio de 2013

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por la Bachiller Celsa C. Sánchez S., titulado:

**"DISEÑO DE PLATAFORMA DE SEGURIDAD EN CENTRO DE DATOS LA COLINA"**

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Luis Fernández
Jurado

Prof. Ricardo Santana
Jurado

Prof. Carlos Moreno
Prof. Guía

# DEDICATORIA

A mis abuelos, Aida Santana porque siempre serás mi fortaleza e inspiración y Ubencio Sánchez por tu amor incondicional durante el tiempo que dios me permitió compartir a tu lado.

# AGRADECIMIENTOS

A mi mamá Elsa Sánchez y a mi abuela Aida Santana, que durante toda mi carrera estuvieron a mi lado, brindándome todo su amor, apoyo, aliento y orientación, indudablemente sin ustedes este logro no hubiese sido posible.

A toda mi familia pero en especial a mi tío David Sánchez, por su amor, consejos y solidaridad, porque gracias a su apoyo logré superar adversidades y conseguir mis metas.

A Alice Barreto, que me brindó su amor incondicional de madre y su apoyo durante los últimos años de mi carrera. A Alvaro Teixeira, por su cariño y amor, por su apoyo y optimismo, por sus palabras de aliento en los momentos que más las necesité y porque hoy, este logro también es tuyo.

A mis amigos, Andreina Rodríguez, Doriana Hernández, Eduardo Paiva, María Marcano, María Arévalo y Ana Pineda, por estar a mi lado en todo momento a pesar de la distancia y porque para mí son mi segunda familia.

A la coordinación de redes de Corporación Digitel, por su colaboración en el desarrollo del presente proyecto de investigación, pero en especial a Gisella Lucar y Luzbella Gámez por su paciencia, enseñanzas, orientación, cariño y respeto.

A todos los profesores que contribuyeron en mi formación profesional, pero en especial a Carlos Moreno y María Auxiliadora.

Y por sobre todas las cosas a DIOS, gracias por un día más de inmensa felicidad.

**Sánchez S., Celsa C.**

# DISEÑO DE PLATAFORMA DE SEGURIDAD EN CENTRO DE DATOS LA COLINA

**Prof. Guia: Ing. Carlos Moreno. Tutor Industrial: Ing. Gisella Lucar. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: Corporación Digitel. Trabajo de Grado 2013. 141 h.**

**Palabras Claves:** Centro de datos; Cortafuego; Políticas de seguridad; Zonas de seguridad; Red interna.

**Resumen.** Se plantea un diseño de seguridad lógica en el centro de datos La Colina de Corporación Digitel, con el objetivo principal de brindar una capa de seguridad a los servidores que allí se encuentran, a través de reglas y políticas. Los mismos, serán divididos en tres zonas fundamentales denominadas “TRUST” (equipos con sistema operativo UNIX), “UNTRUST” (equipos con sistema operativo Microsoft) y “MIDDLEWARE” (equipos con sistemas operativos UNIX en su gran mayoría y Microsoft en algunos casos). Se necesitará la implementación de un equipo cortafuego dedicado exclusivamente a proteger la red interna del centro de datos y negar el acceso a usuarios que no cumplan con los protocolos de seguridad, se describirá el proceso que debe llevarse a cabo para implementar las políticas de seguridad propuestas y levantar una eficiente plataforma de seguridad.

# ÍNDICE GENERAL

# INDICE DE FIGURAS

# INDICE DE TABLAS

# ACRÓNIMOS

SMTP: Simple Mail Transfer Protocol, en español Protocolo para la transferencia simple de correo electrónico.

DNS: Domain Name System, en español Sistemas de nombres de dominio.

DMZ: Demilitarized Zone, en español Zona desmilitarizada.

SSH: Secure Shell, en español Intérprete de órdenes seguras.

POP3: Post Office Protocol, en español Protocolo de oficina de correo.

IMAP: Internet Messages Access Protocol, en español Protocolo de acceso de mensajes de internet.

FTP: File Trasnfer Protocol, en español Protocolo de transferencia de archivos.

TCP: Transmission Control Protocol, en español Protocolo de control de transmisión.

UDP: User Datagram Protocol, en español Protocolo de datagrama de usuario.

HTTP: Hypertext Transfer Protocol, en español Protocolo de transferencia de hipertexto.

HTTPs: Hypertext Transfer Protocol Secure, en español Protocolo seguro de transferencia de hipertexto.

UPS: Uninterruptible Power Supply, en español Sistema de alimentación ininterrumpida.

# INTRODUCCIÓN

La seguridad en las redes a nivel mundial se ha convertido en un tema de vital importancia debido a la gran cantidad de actividades maliciosas en el universo de internet. En el mundo actual, son raras las empresas que no necesitan el servicio de internet o conexión entre redes, en consecuencia las amenazas, ataques, gusanos, intrusiones, infecciones se reproducen a niveles inimaginables con el objetivo de obtener información clasificada, producir daños a los equipos o al sistema, sabotear el funcionamiento de una empresa, propinar amenazas, entre muchas otras.

El presente proyecto de investigación, cuyo objetivo es crear una plataforma de seguridad para el centro de datos La Colina de Corporación Digitel, aborda los aspectos esenciales a la hora de proteger la red de cualquier institución, a través de programas de concientización a los empleados, políticas rigurosas en cuanto a seguridad física y lógica, despliegue de tecnología como incorporación de equipos cortafuegos o firewalls a la red, entre muchos otros.

El desarrollo se dividirá en varias etapas de acuerdo a los objetivos específicos que se plantean lograr, la primera constituye un levantamiento de información de todo el funcionamiento de la empresa en cuanto a topologías, distribución de equipos, espacios físicos, accesos, entre otros, así como la documentación de los servidores objetivo de la problemática, aquellos que se necesitan proteger del mundo exterior, además de establecer el requerimiento de la empresa en cuanto a seguridad, definir sus expectativas, necesidades, problemas que afronta en la actualidad y recolectar toda la información organizada de acuerdo a sus criterios para ser analizada y continuar con las demás fases del proyecto.

En el segundo punto, el autor realiza una diversa documentación en torno a los aspectos más importantes de seguridad que tienen que ver con la problemática de la institución y que serán de gran ayuda, como documentación, a la hora de realizar el diseño d seguridad.

La tercera etapa, se caracteriza como el eje central del proyecto de investigación, en ella el autor plantea la propuesta de diseño cuyo objetivo será proteger en su totalidad los servidores alojados en el centro de datos La Colina. Y finalmente, en la última se documenta cómo debería darse el escenario de implementación una vez aprobada la propuesta de diseño.

A través del siguiente trabajo de investigación, se adquirirán nociones específicas sobre el mundo de seguridad, tanto física como lógica y se brindarán herramientas de gran utilidad a la hora de llevar a cabo cualquier diseño de proyectos.

# CAPÍTULO I

## 1. EL PROBLEMA

Digitel fue constituida formalmente en el año 1997, sin embargo no es sino hasta 1998 que entra en funcionamiento el primer Switch de Digitel en Caracas (Sartenejas) y se inician operaciones de pruebas en áreas rurales del Estado Aragua. A mediados de 1999, inicia el lanzamiento de telefonía móvil con planes en segundos y cierra el año con 15 mil usuarios. Desde sus inicios la empresa cuenta con una concesión por 20 años provista por el gobierno nacional, la cual le proporciona el derecho a ofrecer servicios de telefonía fija y móvil en los estados del centro del país (Miranda, Aragua Carabobo, Cojedes, Falcón, Guárico, Yaracuy y el Distrito Federal).

Una de las principales contribuciones de la compañía al proceso de apertura de las telecomunicaciones en Venezuela, ha sido la introducción de la tecnología GSM (Global System for Mobile Communication), lo que le ha permitido consolidar su presencia como operador de telefonía avanzada en el país. Con la tecnología GSM, los usuarios disfrutan las ventajas que ofrece el sistema de comunicaciones más seguro, el cual brinda privacidad y prevención de fraudes por clonación. Asimismo, en septiembre del año 2000, Digitel sacudió al mercado con la puesta en servicio de la mensajería de texto, lo cual obligó a las otras operadoras a ofrecer el servicio a sus clientes. Esta evolución no se detuvo y en noviembre de 2002 Digitel presentó al mercado venezolano la mensajería multimedia, con su servicio Exprésate, sobre la innovadora plataforma GPRS.

A finales del año 2000, Telecom Italia Mobile (TIM) adquirió la mayoría accionaria de DIGITEL, incrementando el crecimiento en las operaciones y el desarrollo tecnológico de ésta, a través de la experiencia acumulada de TIM en

varios países de Europa y Latinoamérica. En noviembre de 2002, Digitel inició el servicio de Roaming Internacional para los clientes prepago, diferenciando aún más su oferta de servicios.

En octubre de 2004, TIM se convierte en el único accionista y se implementa EDGE (Enhance Data GSM Evolution) como software que potencia la tecnología GPRS. En este mismo año DIGITEL se hace acreedor del Premio P&M a la mejor empresa de Telecomunicaciones del país.

En mayo del año 2006, con la aprobación de la Comisión Nacional de Telecomunicaciones (CONATEL), TIM vendió su participación en DIGITEL a Telvenco S.A., liderada por el Sr. Oswaldo Cisneros Fajardo, (actualmente con el 100% de las acciones de la compañía). Posteriormente, como parte del programa de expansión previsto por los nuevos accionistas, en junio de ese mismo año, DIGITEL adquirió los fondos de comercio de Infonet Redes de Información C.A., Digital Celular GSM C.A. y Digicel C.A., las cuales mantenían concesiones para proveer servicios de telefonía móvil en el occidente y oriente del país. De esta forma, durante el año 2006, DIGITEL completa la integración de las operaciones de estas empresas a su oferta de servicios, operando con cobertura nacional. Desde el mes de julio, se inició un proceso de expansión de la cobertura, que cerró el 2006, con más de 1.070 radio bases instaladas, 4 switches nuevos en las ciudades de Barquisimeto, Maracaibo, Táchira y Caracas; y un despliegue del 100% de la red GPRS/EDGE en el occidente del país que ofrece a los clientes soluciones de comunicación, datos, información y entretenimiento.

Posteriormente, a finales del año 2009, lanza el servicio de Banda Ancha Móvil BAM, red de 3era generación, ofreciendo altas velocidades de transmisión de datos. Así se convierte en la 1era operadora en Latinoamerica en desplegar esta

tecnología en la banda de los 900 Mhz, frecuencia reconocida por brindar un mayor alcance y mejor cobertura.

La red 3G llega a caracas y fortalece su presencia en el resto del país, con más de 350 mil clientes de esta tecnología y más de 6.5 millones de usuarios de telefonía al cierre del 2011. Digitel comienza el despliegue de su red de Fibra Óptica, fortalece su servicio de datos y ofrece soluciones corporativas. Anuncia el lanzamiento de la gama de equipos móviles Apple y fortalece su compromiso social con la consolidación de la alianza con Fe y Alegría.

El crecimiento de Digitel GSM ha sido sostenido y acelerado, contando en la actualidad con más de 6 (seis) millones de clientes. Desde sus inicios Digitel se ha caracterizado por innovadoras propuestas, que van desde: la instauración de un sistema de facturación en segundos, el lanzamiento del servicio de mensajería de texto que luego evolucionó a mensajería multimedia, la incorporación del servicio Oficina Móvil y el programa de lealtad Club Digitel hasta la evolución a la tecnología de 3era generación.

En vista del rápido crecimiento a nivel nacional, Corporación Digitel encuentra la necesidad de ampliar todas las plataformas de sus centros de datos, siendo imperativo crear nuevas infraestructuras en casos en los que el crecimiento no es posible debido a la ubicación, es por ello que surge el proyecto de creación del centro de datos La Colina, cuyo objetivo es migrar servicios alojados en el antiguo centro de datos Cubo Negro, ampliarlo y mejorarlo de acuerdo a las visiones y misiones que se tengan para con la empresa y el servicio a la sociedad venezolana.

## 1.1 Planteamiento del problema

Corporación Digitel planea realizar una serie de modificaciones en sus Centros de Datos debido al gran crecimiento en cuanto a clientes en los últimos años, estos cambios incluyen adquisición de equipos de enrutamiento y despliegue de plataformas de seguridad, punto que debe ser monitoreado constantemente debido a los ataques y fraudes electrónicos.

Uno de los Centros de Datos en gestión y del que se espera un sostenido crecimiento es el ubicado en la sede La Colina, originado por la necesidad de migrar muchos de los equipos que pertenecían al centro de datos Cubo Negro por problemas de ubicación y espacio; sobre este centro de datos no sólo reposa la necesidad de adquirir nuevos equipos sino el despliegue de una amplia plataforma que permita proteger y a la vez incluir sus dispositivos a la red actual.

Para la fecha en curso, Corporación Digitel no dispone de equipos de acceso (Enrutadores) ni de seguridad (Cortafuegos (Firewalls)) para realizar la integración de la sede La Colina a su red corporativa, debido a que los Enrutadores actualmente operativos se encuentran en calidad de préstamo, pues corresponden a otro proyecto de menor envergadura en la sede Torre La Castellana y por lo tanto no poseen capacidad para soportar el crecimiento estimado del Centro de Datos La Colina; asimismo, los equipos Cortafuegos (Firewalls) actualmente disponibles en el centro de datos, no disponen de una amplia plataforma de seguridad que se adapte al nuevo despliegue de tecnología, por lo tanto se diseñarán políticas de seguridad apropiadas que solucionen este inconveniente. Asimismo, Corporación Digitel se encuentra actualmente en negociaciones con proveedores para adquirir nuevos equipos Cortafuegos (Firewalls) en un futuro cercano, por lo que la nueva plataforma de seguridad debe diseñarse de tal manera que se adapte a esta nueva adquisición.

En base a lo antes planteado surgen las siguientes interrogantes: ¿la plataforma de seguridad diseñada será suficiente para proteger al centro de datos?, ¿se podrá diseñar todas las políticas y estructura de seguridad en el tiempo establecido? Ésta y otras interrogantes deberán ser analizadas en el desarrollo del proyecto.

## 1.2 Justificación

La seguridad es la principal defensa que puede tener una organización si desea conectarse a Internet, dado que expone su información privada y arquitectura de red a los intrusos de Internet. El Cortafuegos (o Firewalls en inglés) ofrece esta seguridad mediante: monitoreo y políticas de seguridad, determinando a qué servicios de la red se puede acceder y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no autorizados y en caso de un ataque generar alarmas de seguridad.

Asimismo, la solución al problema actual del centro de datos La Colina, contará con políticas de seguridad que permitirán un flujo seguro del tráfico, controlado según las necesidades de cada una de las plataformas del centro de datos, estas políticas permitirán filtrar el tráfico que se dirija a las plataformas internas del centro de datos admitiendo o denegando el mismo según las especificaciones de IP, Puertos, Protocolos que cada servidor maneje.

Los equipos de seguridad contarán con la redundancia pertinente mediante el uso de tecnologías de "*Failover*" (Enrutadores maestro-esclavo), sus conexiones físicas serán establecidas a la instancia externa y a cada una de las instancias internas configuradas en los Switches.

Las incursiones informáticas y saboteos electrónicos forman parte de la actual realidad y su crecimiento es paralelo a los avances tecnológicos, sin embargo, a causa de su existencia la prestación de un servicio no puede detenerse, las empresas deben establecer políticas entre su red privada e internet de tal manera de garantizar el servicio y no exponer sus recursos, estructura de red, equipos y demás información confidencial al resto del mundo.

## 1.3 Antecedentes del estudio

El diseño de políticas de seguridad es un tema ampliamente desarrollado en los últimos tiempos debido al gran peligro que enfrenta cualquier empresa al conectar sus redes a internet, por ende existen diferentes estudios enfocados en la forma de desarrollar este tipo de plataformas en centro de datos.

Se deberá planificar recursos anuales adicionales para el mejoramiento y/o actualización tecnológica del Centro de Datos, según el análisis de requerimiento de tecnologías realizado periódicamente basado en los siguientes aspectos: a) Infraestructura. Se deberá asegurar que la infraestructura que soporta el centro de datos sea la adecuada y cumpla con los requerimientos de seguridad para su buen funcionamiento, de ser necesario se deberá planificar la actualización de las instalaciones; b) Equipamiento. Se deberá garantizar que el equipamiento cumpla con las especificaciones de seguridad actuales, se podrán adquirir nuevos equipos según necesidad o requerimiento de acuerdo al análisis realizado por TICs; c) Actualización. Los equipos deberán estar actualizados de manera que garanticen la seguridad de datos. El personal de TI deberá monitorear por actualizaciones constantemente, se preverán recursos para la compra de sistemas, licencias y actualizaciones de seguridad para los equipos, además de sistemas de administración de ser necesarios y según análisis realizado. [1]

Es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras está vigente. Este ciclo de vida incluye un esfuerzo de investigación, la labor de escribirla, lograr que las directivas de la organización la acepten, conseguir que sea aprobada, lograr que sea diseminada a través de la empresa, concienciar a los usuarios de la importancia de la política, conseguir que la acaten, hacerle seguimiento, garantizar que esté actualizada y, finalmente, suprimirla cuando haya perdido vigencia. [2]

Asimismo, corporación Digitel ha desarrollado este tipo de plataformas en cada Centro de Datos activo actualmente (dos), es por ello que su personal goza de experiencia y está altamente calificado en el área.

## 1.4 Objetivos

### OBJETIVO GENERAL

DISEÑAR PLATAFORMA DE SEGURIDAD EN CENTRO DE DATOS LA COLINA, CASO CORPORACIÓN DIGITEL.

### OBJETIVOS ESPECÍFICOS

1. Levantar información de plataforma de servidores en producción en centro de datos.

2. Estudiar posibles políticas de seguridad para un centro de datos.

3. Diseñar políticas de seguridad para el centro de datos La Colina.

4. Documentar el proceso de implementación de las políticas de seguridad.

## 1.5 Alcance

El trabajo estará delimitado por la necesidad de brindar una capa de seguridad al Centro de Datos La Colina, el cual se encuentra operativo en estos momentos, a través del diseño de una plataforma de seguridad adecuada al crecimiento estipulado para él. Sin embargo, el enfoque específico estará alrededor de la seguridad lógica del mismo, en vista de que ya se ha realizado un despliegue de infraestructura en cuanto a seguridad física, no obstante, también se realizará un monitoreo de las mejores prácticas aplicas en este último punto de seguridad.

## 1.6 Metodología

**Fase 1. Estudio Documental**

En esta fase se deberá recopilar toda la información y documentación necesaria para llevar a cabo el estudio planteado, es imperativo establecer una base sólida de conceptos y teoría necesaria para comprender términos abstractos que podrán manejarse más adelante. Entre la información requerida se puede resaltar lo siguiente:

1. Documentación técnica sobre funcionamiento y estructura de Firewalls y políticas de seguridad intrínsecas a él. Para ello, se hará una revisión exhaustiva de libros y manuales disponibles en el departamento.
2. Revisión de recomendaciones dadas por la UIT sobre normas de seguridad. Esta información será recopilada a través de páginas WEB (En específico página oficial de la UIT).
3. Levantamiento de información sobre plataforma de internet de la red corporativa y su interconexión con el Centro de Datos La Colina.

Información que será suministrada a través de las bases de datos del departamento.

4. Levantamiento de información de plataforma de servidores en producción en centro de datos La Colina. Esta información es necesaria ya que a través de ella se delimitará el alcance del proyecto. Información que será suministrada por el departamento.

**Fase 2. Estudiar posibles políticas de seguridad para un centro de datos**

Mucho antes de siquiera pensar en el diseño de la plataforma y políticas de seguridad para el centro de datos La Colina, se debe realizar un amplio estudio sobre las posibles políticas que pueden ser aplicadas a un centro de datos genérico, de manera tal de adecuar posteriormente estas políticas a las especificaciones del caso en estudio.

**Fase 3. Diseño de políticas de seguridad para el centro de datos La Colina**

De acuerdo a las necesidades y requerimientos del centro de datos La Colina, sus políticas en cuanto a seguridad deberán ser muy específicas, por lo tanto se realizará un diseño de las mismas tomando en cuenta los posibles riesgos a los que se encuentra expuesto el centro de datos.

**Fase 4. Documentar el proceso de implementación de las políticas de seguridad**

Una vez realizado el diseño de las políticas de seguridad, el estudio debe incluir en detalle cómo debería darse el proceso de implementación, resaltando características de posibles equipos de seguridad a implementar y configuración de los mismos.

**Fase 5. Elaboración de informe final**

Finalmente, se elaborará un informe en el cual se especificarán todas las actividades realizadas en detalle, resultados obtenidos e información en general sobre el desarrollo del proyecto.

1.7 Herramientas y equipos a utilizar.

Se dispondrá de varios recursos como computadora personal con acceso a internet, guías y manuales disponibles en el departamento, acceso al centro de datos La Colina con asesoría técnica, acceso a información corporativa y red interna; Además de acceso a equipos de seguridad como Cortafuegos (Firewalls) y enrutadores, con asesoría técnica.

1.8 Análisis de Factibilidad

El proyecto tendrá su desarrollo en el departamento de Redes ubicado en el cubo negro y en el Centro de Datos con sede en La Colina. La tecnología necesaria para llevar a cabo el estudio está al alcance de la corporación, el tiempo dispuesto para el desarrollo del proyecto se ajusta a las semanas disponibles, asimismo, este tipo de plataformas de seguridad ya ha sido ejecutada en otros centros de datos de Digitel, por lo tanto el personal técnico posee experiencia previa en él.

# CAPITULO II

## 2. MARCO TEÓRICO

En alineación con el objetivo del proyecto se realizará una documentación teórica de los aspectos de mayor impacto a lo largo de la investigación como infraestructura de centros de datos, tipos de centros de datos, organismos nacionales e internacionales de regulación para centros de datos, normas de seguridad de la información, equipos de protección cortafuego o firewall, entre otros.

### 2.1 Centros de Datos

Un centro de datos o centro de procesamiento de datos, es un edificio o porción de un edificio cuya función principal es alojar un ambiente para computadoras y sus áreas de soporte, puede ocupar un cuarto de un edificio o un edificio entero. El propósito del centro de datos es alojar los activos de datos (ya sean equipos montados en racks o gabinetes y su sistema de cableado estructurado para interconectarlos), en un entorno que satisface sus necesidades por potencia, telecomunicaciones, redundancia y seguridad. Los centros de datos son divididos según la clase de servicio que proveen, existen dos (2) categorías principales: a) Dominio privado, empresarial o corporativo; b) dominio público, de internet o de Hosting.

Centro de datos privado: es manejado por el departamento de tecnología de la información (TI) de la propia organización, provee funciones de almacenamiento, aplicaciones, Web-hosting y funciones de negocios que toda empresa necesita.

Centro de datos de Hosting: sirve a una variedad de clientes y es poseído por un proveedor de servicios que se encarga de vender servicios de datos de internet (como Web-hosting o VPN) a varios clientes.

Es importante para todo diseño de centro de datos, conservar el correcto funcionamiento de los equipos, aún bajo las peores circunstancias, por lo tanto todo centro de datos es construido bajo ciertas premisas de infraestructura de soporte e ingeniería, entre ellas se puede mencionar el suministro de energía eléctrica y respaldo, controles de enfriamiento y ambientales, sistemas de detección de fuego y humo, seguridad física, conectividad a redes externas, Centro de Operaciones de Red o NOC por sus siglas en inglés Network Operations Center, cableado y puesta a tierra, entre muchos otros.

Principios del diseño de la infraestructura de un centro de datos

Al momento de diseñar un centro de datos se deben considerar ciertos aspectos, con el objetivo de optimizar todas sus funciones y procesamiento de red, entre ellos se puede mencionar:

- ✓ Ahorro de espacio: maximizar los recursos de espacio es un aspecto crítico del diseño de un centro de datos
- ✓ Confiabilidad: diseños redundantes, a prueba de fallas y de máximo tiempo de actividad y operación.
- ✓ De fácil administración: la infraestructura es diseña no sólo para proveer un servicio altamente confiable sino flexible, de fácil recuperación ante desastres.

El proceso de diseño, recomendado por normas internacionales establece varias premisas a la hora de evaluar la implementación de un centro de datos, entre ellas se incluye: estimación de necesidades a máxima capacidad para todo el equipamiento, anticipación de crecimiento futuro, proveer todos los requerimientos a arquitectos e ingenieros, crear un plano del piso de equipamiento y diseñar el sistema de cableado de telecomunicaciones.

Niveles de un centro de datos

Los niveles son relacionados con la disponibilidad del centro de datos, las clasificaciones por niveles fueron definidos originalmente por The Uptime Institute, el cual abordaba las diferentes clasificaciones de los sistemas crítico. [3]

1) Nivel 1 – Básico: no posee ningún componente redundante, puede no tener un piso levantado, es susceptible a discontinuidades a partir de actividades planificadas y no planificadas, se calcula en 28.8 horas de parada anual.

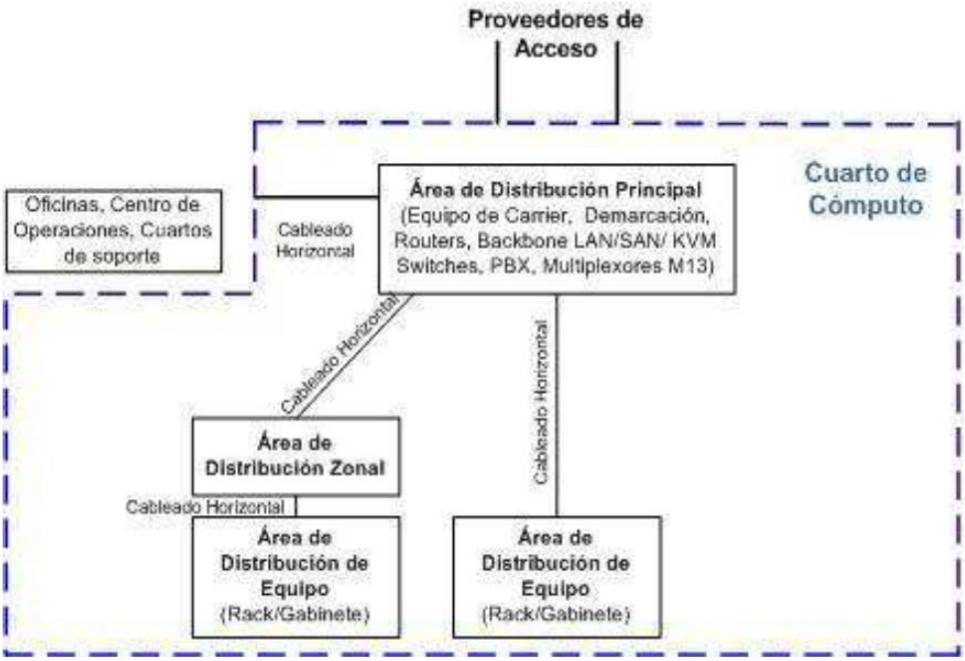



Figura 1 Ejemplo de topología de centro de datos Básico

Fuente: Norma ANSI/TIA/EIA-942

2) Nivel 2 – Componentes redundantes: posee componentes redundantes, trayecto único para potencia y distribución de enfriamiento, piso levantado, ligeramente menos susceptible a discontinuidades que el Nivel 1, 22 horas de parada anual.

3) Nivel 3 – Concurrente: posee componentes redundantes, múltiples trayectos de potencia y distribución de enfriamiento, deja margen para cualquier actividad planificada de la infraestructura del sitio sin perturbar la operación del computador, 1,6 horas de parada anual.

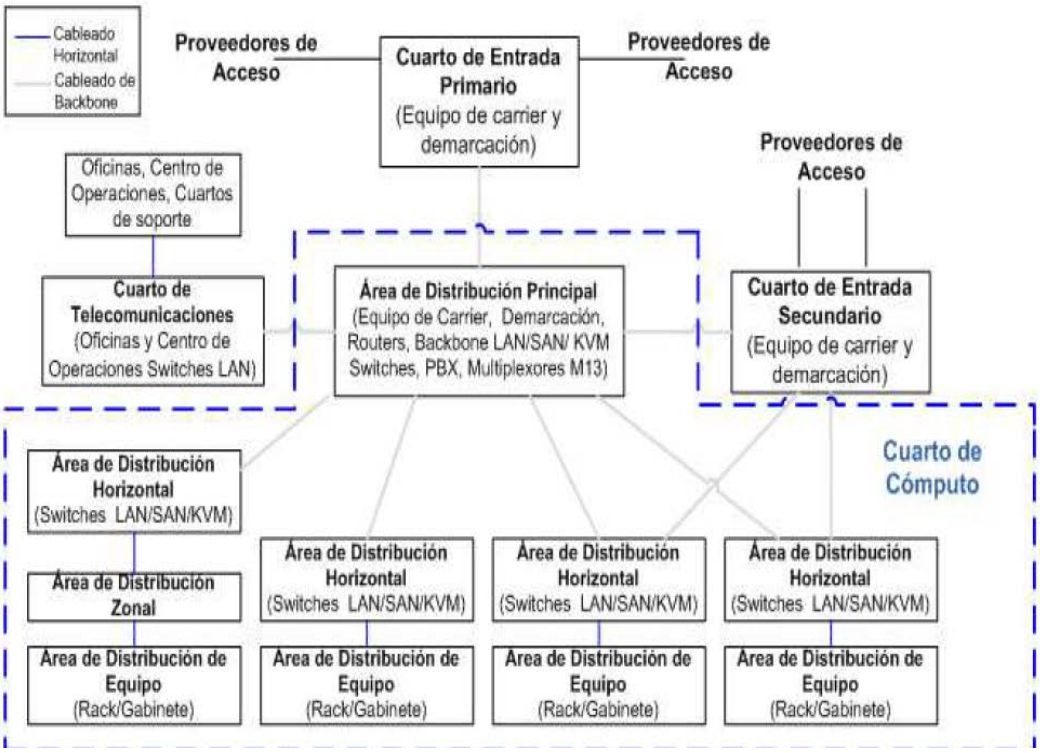



Figura 2 Ejemplo de topología de centro de datos Concurrente

Fuente: Norma ANSI/TIA/EIA-942

4) Nivel 4 – Tolerante a fallas: Posee componentes redundantes, múltiples trayectos de potencia y distribución de enfriamiento, todo hardware de computadora posee entradas duales de potencia, podría sostener al menos un peor caso, falla no planificada o evento, con ningún impacto de carga crítico, 0,4 horas de parada anual.

Espacios de Telecomunicaciones

Según la norma ANSI/TIA-942 los espacios para soportar los equipos de telecomunicaciones y cableado son los siguientes:

1) Cuarto de entrada (ER): punto de delimitación del proveedor de acceso, puede ser localizado dentro o fuera del cuarto de computadoras, está definido por la interface entre el cableado del centro de datos y el cableado inter – edificio.

2) Cuarto de telecomunicaciones (TR): espacio dedicado a la oficina y operaciones del centro de datos, suele ser la ubicación del centro de operaciones de red.

3) Área de distribución Principal (MDA): es el espacio central donde el punto de distribución para el sistema de cableado estructurado en el centro de datos está localizado.

4) Área de distribución horizontal (HDA): suele ser la localización típica de los Switches LAN, SAN y KVM que soportan los equipos finales, generalmente hay varios HDA.

5) Cross – connect horizontal (HC): es un gran campo de conexión que distribuye cables “horizontales” hacia los equipos

6) Área de distribución de zona (ZDA): es el punto de interconexión opcional dentro del cableado horizontal, se encuentra localizado entre el HDA y el EDA.

7) Área de distribución de equipos (EDA): son espacios asignados para los equipos finales, incluyendo sistemas de computadoras, equipos de comunicaciones y servidores.

Además de la distribución de espacios de telecomunicaciones, es importante resaltar el concepto de pasillos fríos y calientes en la distribución de equipos de un centro de datos: los gabinetes o racks deberán ser arreglados en un patrón alternante, cuyas partes delanteras se enfrente unas con otras en una fila para crear pasillos “calientes” y “fríos”. Asimismo, se reservará un mínimo de un metro de espacio delantero para la instalación de equipos y un mínimo de 0.6 metros de espacio trasero para acceso de servicio.

Sistema de cableado del centro de datos

Los medios de cableado mayormente reconocidos en el mundo son el par trenzado de 100 ohm, la fibra óptica multimodo (MM) y monomodo (SM), el cable coaxial de 75 ohm, además de las terminaciones tradicionales de campo y las configuraciones perterminadas.

Según la norma ANSI/TIA-942 los componentes de la arquitectura de un sistema de cableado son: el cableado horizontal, el cableado de bacbone, el cross-connect, el main cross-connect y el horizontal corss-connect.

## 2.2 Consideraciones de normas para el diseño de un centro de datos

Existen diversos organismos a nivel mundial que se encargan de estandarizar todos los procesos de diseño de centros de datos y de establecer las mejores prácticas en cuanto a energización, cableado, distribución de espacios, entre otros; es importante estar al tanto de todas estas normativas en el campo de centro de datos ya que pueden ser de gran utilidad a la hora de abordar el proceso de investigación del proyecto.

### 2.2.1 COVENIN (Comisión Venezolana de Normas Industriales)

Es el organismo de regulaciones técnicas a nivel nacional, respecto a actividades que tengan relación con el sector eléctrico como proyectos, instalaciones y servicios, cumplimiento de estándares de calidad, seguridad, eficiencia y protección del medio ambiente, entre otros. Establece los requisitos mínimos para la elaboración de procedimientos, materiales, productos, actividades y demás aspectos que cada una de sus normas rige, es el encargado de velar por la normalización bajo lineamientos de alta excelencia en el país.

Código Eléctrico Nacional: Norma 200 de COVENIN

*Esta norma venezolana establece los requisitos que deben cumplir las instalaciones eléctricas para la salvaguarda, validez e intención de estas, a saber son: a) Salvaguarda. El propósito de este Código es la salvaguarda real de las personas y propiedades de los peligros que implica el uso de la electricidad; b) Validez. Este Código contiene disposiciones que se consideran necesarias para la seguridad.* [4]

### 2.2.2 ISO (Organización Internacional para la Normalización)

Organización internacional reconocida por su amplia selección de estándares internacionales, y desarrollo del famoso modelo en capas llamado OSI. Gracias a la división de capas en este estándar, es posible detectar con mayor rapidez qué punto de la red presenta fallas, a través de cuáles protocolos puede ser gestionado y a qué aplicaciones pertenece. Este mecanismo es de suma importancia a la hora de elaborar políticas de seguridad e identificar a qué capa pertenece cada elemento.

Norma ISO-IEC 27002

La Comisión Electrotécnica Internacional (IEC) y la organización Internacional para la normalización, forman el sistema especializado para la estandarización mundial. Los organismos internacionales miembros de ISO e IEC participan en el desarrollo de Estándares Internacionales a través de los comités establecidos por la organización respectiva para lidiar con áreas particulares de la actividad técnica. Esta norma es un estándar para los sistemas de gestión de seguridad informática.

### 2.2.3 ANSI (Instituto Nacional Americano de Normalización)

Organización que aprueba los estándares nacionales de Estados Unidos y colabora en el desarrollo de estándares internacionales en relación con comunicaciones y redes. Es miembro de la IEC (Comisión Electrotécnica Internacional) y la Organización Internacional para la Normalización.

Norma ANSI/EIA/TIA 942

Es un estándar que especifica los requerimientos mínimos para la infraestructura de telecomunicaciones de centros de datos y cuartos de computadoras. [5]

### 2.2.4 IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

Instituto que desempeña actividades técnicas educacionales y profesionales que promueven la teoría y la práctica de la electrotecnia para el desarrollo profesional de sus miembros. Además, fomenta avances científicos y tecnológicos, que se transforman en productos prácticos y seguros.

Norma 518-1982 IEEE

Guía para la instalación de equipos eléctricos para minimizar la entrada de ruido. [6]

Norma 142-1991 IEEE

Práctica recomendada para poner a tierra los sistemas de energía industriales y comerciales. [7]

## 2.3 Premisas de seguridad del Cortafuegos o Firewall

El Cortafuegos o Firewall es un sistema de seguridad de redes en el que se protege una máquina o subred de servicios que desde el exterior puedan suponer una amenaza a su seguridad, es decir, proporcionan un aislamiento entre dos o más redes con el objetivo de evitar tráfico no deseado. Un cortafuego actúa generalmente como un filtro, examinando cada uno de los paquetes de información en base a ciertas bien definidas. Sólo bajo una política de seguridad decide qué paquetes puede aceptar, modificar o bloquear. La ubicación del Cortafuego en la red generalmente depende del tipo de topología física que adopte la empresa, aunque la más común es de tipo jerárquica.

Topologías de red

1) Tipo Bus: topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos.

2) Tipo Anillo: topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente

estación. En este tipo de red la comunicación se da por el paso de un token o testigo.

3) Tipo Estrella: las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información.

4) Tipo Malla: es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos.

5) Tipo Jerárquica: es una topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos.

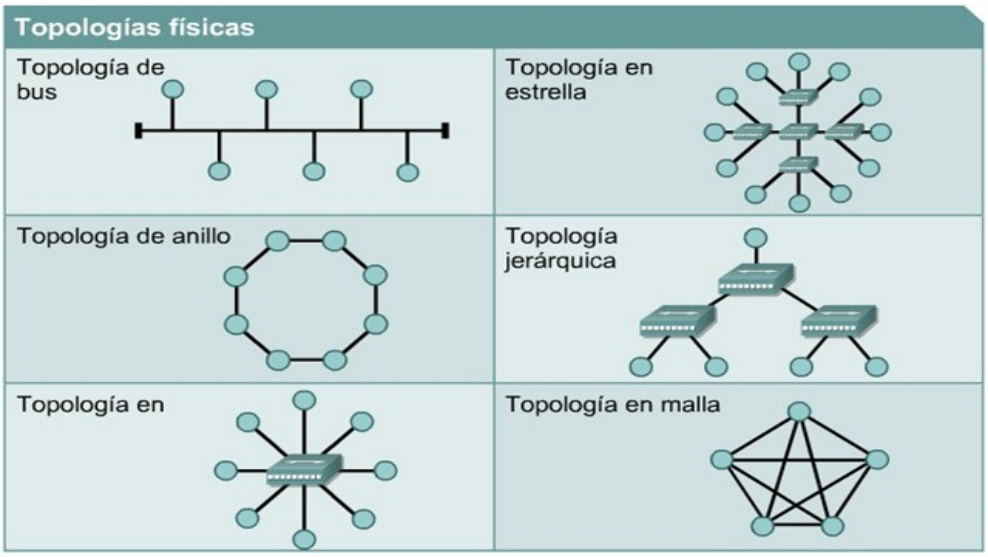



Figura 3 Topologías Físicas

Fuente:

http://lh4.ggpht.com/_zYDYxKevmcw/SoccWCDUN5I/AAAAAAAAAWw/QINMP0D3YUo/s1600-h/Topologiasfisicasciscoccna15.jpg

Consulta: 20/04/2013

Políticas de diseño en un Cortafuego o Firewall

Las políticas de accesos en un Firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso.

Restricciones de un Cortafuego o Firewall

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1) Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina Trusted (validados). Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.

2) Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

Beneficios de un Cortafuego o Firewall

Además de brindar una capa de protección a la red, el Cortafuego es ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque o intrusiones, el administrador será el responsable de la revisión. Asimismo, desde el punto de vista de llevar estadísticas del ancho de banda consumido en la red, es idóneo, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Limitaciones de un Cortafuego o Firewall

Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si existe un error en cuanto al diseño de las reglas o políticas de seguridad dentro de él, el tráfico no deseo puede transitar hacía la red interna.

## 2.4 Metodología PPDIOO

Este modelo o metodología elaborado por el fabricante internacional CISCO SYSTEMS, se ha convertido en una guía para todas aquellas pequeñas y grandes empresas que desean llevar a cabo el diseño de un proyecto. Como sus siglas en inglés lo indican (Phases Prepare, Plan, Design, Implement, Operate and Optimize), lleva el proceso de implementación de un proyecto a seis fases que forman un ciclo en constante revisión.

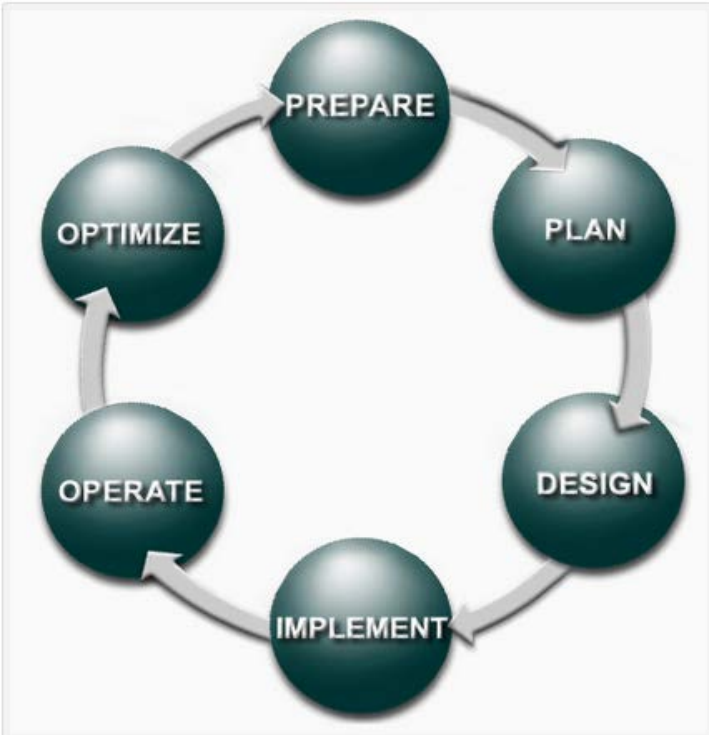



Figura 4 Diseño PPDIOO

Fuente: http://wmagliano.wordpress.com/2008/09/27/diseno-de-redes-capitulo-1-ppdioo/

Consulta: 20/04/2013

1) Fase de preparación: se lleva a cabo un proceso de descubrimiento para comprender mejor las necesidades de negocio, los requisitos de alto nivel, y los desafíos. Este esfuerzo incluye una serie de entrevistas con el personal de apoyo para elaborar y proponer una solución viable, equilibrar las necesidades de la competencia, entender el negocio y entorno técnico.

2) Fase de planeación: se refina la estrategia preliminar desarrollada durante la fase de preparación para establecer los requisitos y la funcionalidad necesaria para la prueba de uso y la validación de las pruebas, pero todavía no para las pruebas específicas de alto nivel,

3) Fase de diseño: En la fase de diseño, el equipo del proyecto desarrolla y presenta el diseño de bajo nivel que con el tiempo se pondrá en práctica.

4) Fase de Implementación: El plan de proyecto es seguido durante esta fase. Cada paso en la implementación debe incluir una descripción y guía de puesta en producción, detallando tiempo estimado para implementar, pasos para volver a la configuración antigua en caso de falla e información de referencia adicional.

5) Fase Operativa: Esta fase mantiene el estado de la red día a día. Esto incluye administración y monitoreo de los componentes de la red, administración de actualizaciones, administración de performance, e identificación y corrección de errores de red. Esta fase es la prueba final de diseño.

6) Fase de Optimización: Esta fase envuelve una administración pro-activa, identificando y resolviendo cuestiones antes que afecten a la red. Se puede crear una modificación al diseño si demasiados problemas aparecen, para mejorar cuestiones de performance o resolver cuestiones de aplicaciones.

Esta metodología fue de gran ayuda a la hora de abordar el aspecto del diseño de la plataforma de seguridad del centro de datos La Colina.

# CAPITULO III

## 3. MARCO METODOLÓGICO

### 3.1 Consideraciones Generales

En toda investigación se hace necesario establecer de manera sistemática y organizada los procedimientos a través de los cuales se alcanzará el objetivo propuesto inicialmente; asimismo, se deben plantear el conjunto de operaciones técnicas llevadas a cabo en el despliegue de la investigación y en el proceso de obtención de los datos para finalmente delimitar la investigación, en función a responder las interrogantes planteadas en un principio.

Es por lo antes expuesto que, el Marco Metodológico, de la presente investigación donde se propone diseñar una solución para brindar una capa de seguridad al centro de datos “La Colina”, está referido al conjunto de procedimientos lógicos y tecno-operacionales implícitos en todo proceso de investigación, que no constituyen fórmulas rígidas sino que forman parte de un razonamiento, derivado del análisis y conclusiones de orden teórico.

En consecuencia, en este apartado se introducirán los distintos procedimientos de orden tecno-operacional más indicados para recopilar la información, sintetizar el contenido de la misma, analizar los datos más importantes y finalmente acertar con el propósito del estudio. Es imprescindible cumplir todos los objetivos planteados al inicio de la investigación, a medida que se avanza en el desarrollo de la misma, debido a que ellos ayudan a identificar el tipo de estudio y su diseño de investigación, que en este caso, se trata de una investigación proyectiva, así como el universo o población estudiada, las técnicas e instrumentos que se emplearán en la recolección de los datos, la presentación de

los mismos y el análisis e interpretación de los resultados que permitirán definir el diseño que más se adapta a las características y necesidades arrojadas en el estudio.

## 3.2 Tipo de investigación

De acuerdo a las características de los objetivos planteados con anterioridad, el presente trabajo queda tipificado como una "Investigación Proyectiva" debido a que, a partir de un proceso de indagación, propone soluciones a una situación determinada; este tipo de investigación se caracteriza principalmente por proponer alternativas de cambio que no necesariamente deben ser ejecutadas. Según la norma de la UPEL, en esta categoría entran los "Proyectos Factibles" definidos de la siguiente manera: "El Proyecto Factible consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales; puede referirse a la formulación de políticas, programas, tecnologías, métodos o procesos. El proyecto debe tener apoyo en una investigación de tipo documental, de campo o un diseño que incluya ambas modalidades." [8]

Asimismo, el término "proyectivo" hace referencia a proyecto pero en cuanto a propuesta, a la cual puede llegarse mediante diferentes enfoques, métodos y técnicas; Puede realizarse una planificación desde el presente hacia el futuro (perspectiva) o por el contrario, puede trasladarse el proyecto a un momento determinado en el futuro, diseñarlo y luego realizar en el presente una serie de pasos para obtener la meta del futuro (prospectiva).

Finalmente es importante destacar que de manera general, los proyectos factibles comprenden varias etapas de ejecución: a) Diagnóstico del problema

planteado y fundamentación teórica de la propuesta; b) Detalle del procedimiento metodológico con las actividades respectivas y recursos agotados para su ejecución; c) Conclusiones sobre la viabilidad del proyecto, ejecución de la propuesta y evaluación tanto del proceso como de los resultados.

## 3.3 Diseño de la investigación

Luego de establecer el tipo de investigación, se plantea la necesidad de definir o delimitar el diseño, que será útil para desarrollar el plan estratégico de trabajo a seguir en la investigación y el proceso de recolección, análisis e interpretación de resultados. En tal sentido, una definición acertada de Alvira Martín, plantea lo siguiente: "Un diseño de investigación se define como el plan global de investigación que integra de un modo coherente y adecuadamente correcto técnicas de recogida de datos a utilizar, análisis previstos y objetivos…" [9]

Atendiendo a los objetivos del trabajo y a las características del mismo, el proyecto obedece a un diseño de campo, toda vez que los datos se recogen de manera directa de la realidad en su ambiente natural, a través de encuestas, entrevistas y observando en primera persona las actividades de interés o relevantes al proyecto; es decir, el objeto de estudio de la investigación, sirve como fuente de información para el investigador.

Los diseños de campo pueden clasificarse a su vez en experimentales y no experimentales, de acuerdo a su profundidad y extensión; el caso que nos ocupa (proyectos factibles) es identificado como no experimental debido a que los hechos en estudio se observan tal como se manifiestan, sin ningún tipo de manipulación intencional a las variables de estudio.

## 3.4 Población o universo de estudio

Queda entendido por población, según Angel Alcaide en su libro Estadística Aplicada a las Ciencias Sociales, como "…cualquier conjunto de elementos de los que se quiere conocer o investigar alguna o algunas de sus características" [10].

En el caso que nos ocupa, referido al Diseño de la plataforma de seguridad del centro de datos "La Colina", el universo del estudio esta constituido por todos aquellos servidores a los que se le quiera brindar una capa de seguridad y proteger de cualquier ataque interno o fuera de la red; esta población se encuentra dividida en tres grandes grupos llamados: Microsoft, Middleware y Unix; También forman parte del universo o población, los equipos de protección o cortafuegos, debido a que a través de ellos se protegerán los servidores mencionados en la primera instancia, por lo tanto es necesario estudiar sus características y alcance a la hora de diseñar la propuesta.

## 3.5 Instrumentos de recolección de información

Una vez delimitado el tipo de investigación (Proyectiva), diseño (de Campo) y población o universo de estudio, otro aspecto de importante relevancia es la definición de los métodos, técnicas e instrumentos de recolección de datos que se llevan a cabo a lo largo de todo el proyecto.

A razón de que la búsqueda de información, observación de los acontecimientos y recolección de datos en general son reunidos y utilizados por el autor de forma directa de su ambiente natural, la fuente de información es clasificada como "primaria", identificada como: "Aquellos que se dedican a la

observación de la realidad, y exigen respuestas directas de los sujetos estudiados; donde se interroga a las personas en entrevistas orales o por escrito…" [11].

Dada la naturaleza del proyecto de investigación, es necesario aplicar diferentes técnicas de recolección de datos para el momento teórico y para el metodológico, así como la elaboración y presentación del trabajo escrito, debido a que cada uno de ellos posee características particulares que obligan al autor a realizar un análisis detallado de acuerdo al momento en el que se encuentre. En la primera etapa, constituida principalmente por la investigación teórica, análisis de fuentes documentales y estudio de servidores en producción en el centro de datos en estudio, la técnica utilizada es llamada "observación documental", definida básicamente como aquella que enfoca su observación en diversas fuentes documentales existentes; es explicada por Mirían Balestrini como "…es un área básica, donde se ha de coincidir, independientemente del tipo de investigación que se realice y de la implicación que ésta tenga con una rama de conocimiento específica" [12]. En segundo lugar, y en referencia al desarrollo del proyecto de acuerdo a los objetivos, se debe aplicar la observación directa con la implementación de encuestas, entrevistas, visitas técnicas y la observación mecánica con la ayuda de artefactos tecnológicos (cámaras de fotografías y video grabadoras). Finalmente, se aplican otras técnicas referentes al diseño de la solución necesitada, como diagramas de análisis, flujo gramas, ingeniería de diseño, entre otros.

## 3.6 Metodología

De manera tal de dar continuidad al proceso metodológico del trabajo de aplicación profesional, referido al Diseño de plataforma de seguridad del centro de datos La Colina, se describen a continuación las actividades realizadas en cada etapa de la investigación, de acuerdo a los objetivos específicos descritos inicialmente.

### 3.6.1 Fase 1: Estudio Documental

Inicialmente se recolectó toda la información teórica respecto a normas a seguir en un Centro de Datos, equipos de seguridad, recomendaciones de seguridad, diseños en un Centro de Datos, definiciones de interés, entre muchos otros, para lo cual se consultaron datos teóricos en libros, Internet y en documentos de la corporación; Asimismo, se realizó un levantamiento de información de la plataforma de servidores en producción en el centro de datos La Colina (activos en ese momento y pendientes por migrar en un futuro cercano), para ello, fue necesario consultar información documentada en los archivos de la corporación y realizar entrevistas al personal del departamento de UNIX y MICROSOFT.

Para todo lo comentado en el párrafo anterior, el autor utilizó los siguientes materiales: computadora, impresora, documentos de la corporación, material de oficina y grabadora.

### 3.6.2 Fase 2: Estudiar posibles políticas de seguridad para un centro de datos

Luego de realizar todo el levantamiento de información preliminar, se continuó con la indagación pero con un enfoque más específico, de manera de responder a la siguiente interrogante ¿Qué políticas de seguridad son implementadas generalmente en un Centro de Datos?; Para dar respuesta a la interrogante, el autor realizó varias entrevistas al personal de sistemas, basándose en su experiencia y experticia en proyectos pasados, de similar envergadura; Aunado a ello, se buscó información en diferentes páginas Web y en libros de fácil alcance.

Los materiales necesarios para el desarrollo de esta fase estuvieron comprendidos en computadora con acceso a Internet, grabadora, materiales de oficina e impresora.

### 3.6.3 Fase 3: Diseño de políticas de seguridad para el centro de datos La Colina

Al momento de establecer un diseño, es importante tomar en cuenta las recomendaciones de los grandes fabricantes de la industria de Internet como lo son HUAWEI, JUNIPER y CISCO SYSTEM; en cuanto a éste último, existe una metodología llamada PPDIOO que detalla de manera específica, a través de seis pasos (Preparar, Planear, Diseñar, Implementar, Operar y Optimizar) cómo debería ejecutarse un proyecto y su respectivo ciclo de vida. Para esta etapa, el autor usó la metodología antes mencionada como referencia en ciertos aspectos del proceso de diseño.

De manera de establecer, en un principio, un orden coherente de las actividades a realizar, se inició con la indagación de las necesidades y carencias de la Corporación en cuanto a seguridad en el centro de datos La Colina (información recolectada a través de entrevistas y reuniones con los supervisores de sistemas e implementación de proyectos de la empresa); Este proceso constituyó la fase de preparación del diseño, documentada en la metodología PPDIOO como sigue a continuación: “En la fase de preparación del ciclo de vida de la red, una empresa establece los requerimientos de negocio y la visión tecnológica correspondiente. La empresa desarrolla una estrategia tecnológica e identifica las tecnologías que pueden soportar sus planes de crecimiento de mejor manera.” [13]. Los datos recolectados a este nivel, se enfocaron en la profundidad del servicio de seguridad necesitado, las tecnologías soportadas según la arquitectura planeada a desplegar en el centro de datos y la protección a plataformas, equipos, servidores e información en general contra ataques internos y externos.

Debido a que el proyecto contempla la adquisición de equipos de seguridad para construir la plataforma de protección adecuada, el personal especializado recomendó en diversas ocasiones que, al momento de analizar el tipo de equipos de mejor adaptación a las características y requerimientos del centro de datos, se hacía imperativo considerar las marcas ya operativas y desplegadas en toda la red, por razones de compatibilidad, organización y minimización de errores técnicos.

La siguiente fase, corresponde al plan a ejecutar una vez reunida toda la información necesaria, el cual no sólo contempla las actividades a realizar de manera sistemática y organizada para lograr el diseño, sino que incluye tareas para administrar los riesgos, problemas y responsabilidades que se puedan afrontar a la hora de implementar cambios en la red. Según la metodología PPDIOO, la seguridad es un tema de suma importancia a desarrollar "Para planear la seguridad de la red, la empresa evalúa su sistema, redes e información contra intrusos, así como también evalúa la red para detectar la factibilidad de que redes externas y no confiables obtengan acceso a redes y sistemas internos y confiables." [14].

Finalmente, de acuerdo a la estructura y fases previas, se desarrolló un diseño del sistema en general donde se detalló específicamente las soluciones atadas a los requerimientos y que de alguna u otra forma, satisfacen la carencia en cuanto a seguridad del centro de datos; fueron creadas aplicaciones a la medida de las solicitudes de manera de permitir la integración con la infraestructura de red existente. A medida que se avanzaba en el cuerpo del diseño, era consultado con el personal encargado, para así corregir errores, anexar sugerencias y aumentar el nivel de protección de acuerdo a la propuesta.

Los materiales necesarios para el diseño del proyecto fueron los siguientes: computadora con acceso a Internet, material de oficina, grabadora, impresora, cámara fotográfica, libros y documentos de la empresa.

### 3.6.4 Fase 4: Documentar el proceso de implementación de políticas de seguridad

Además de afinar los criterios de diseño en diversas reuniones con el personal de la empresa, se realizó una documentación de cómo debería darse el proceso de implementación de las políticas de seguridad y la plataforma de protección en general. Este proceso fue divido en varias etapas, para no afectar en lo posible las actividades normales de la corporación y dar continuidad a los servicios ofrecidos. Para el cumplimiento de este objetivo, el autor recolectó información de trabajos de gran envergadura realizados con anterioridad en el departamento.

Para finalizar con esta fase, se realizaron varias visitas técnicas al centro de datos La Colina con asesoría profesional, se tomó un conjunto de fotografías del lugar y se realizaron constantes reuniones con el personal especializado para aclarar detalles en cuanto al proceso de implementación.

# CAPITULO IV

## RESULTADOS Y ANÁLISIS

### 4.1 Levantamiento de información

En todo proyecto de investigación se hace necesario realizar un estudio general de las condiciones actuales que afronta la empresa y el despliegue de tecnología que se ha realizado en el área de estudio, de manera tal de establecer un punto de partida e identificar cuáles aspectos necesitan ser reforzados como valor agregado del diseño a ser planteado y cuáles deberían ser incorporados desde sus inicios.

En virtud de lo antes expuesto, el autor realizó una exhaustiva indagación sobre aspectos referentes a la situación real de la empresa, su topología actual y futura con la implementación final del centro de datos “La Colina”, el impacto de esta implementación para la red corporativa, identificar el nivel de ejecución de aspectos como la infraestructura, despliegue de tecnologías, servicios, plataformas migradas y establecidas en el centro de datos en referencia, hasta el momento de la recolección de información, así como otras actividades necesarias para comprender en su totalidad la estructura de la red, obtener información vital para el diseño y finalmente identificar las herramientas de las cuales se puede disponer.

### 4.1.1 Estructura de La Red Corporativa

La plataforma de Red Corporativa es la base fundamental de la empresa debido a que permite la interconexión y acceso a todos los servicios de red (conectividad interna y a sedes remotas, aplicaciones y servicios como correo, impresión, carpetas compartidas, acceso a Internet, entre otros) mediante una arquitectura compuesta principalmente por routers, conmutadores (switches) y cortafuegos (firewalls).

La red Corporativa de Digitel está constituida por un modelo de tres (3) capas identificadas como *NUCLEO, DISTRIBUCIÓN* y *ACCESO*, cada capa posee funcionalidades diferentes, sin embargo su división debe verse más como una separación lógica que física, es decir, un solo equipo puede realizar funciones de más de una capa a la vez.

En la capa *NUCLEO* o *CORE* se encuentran los equipos con mayor capacidad ya que en ella se gestiona el tráfico de todos los nodos de la siguiente capa de manera veloz y confiable; en caso de presentarse alguna falla en esta etapa, la afectación es general hacia todos los servicios, por lo tanto es importante una gran tolerancia a fallas; en esta plataforma se encuentran los equipos de borde de la corporación. Está constituida principalmente por el centro de datos *Universidad Simon Bolívar (USB)* y el centro de datos *Cubo Negro (CBN)* los cuales cuentan con múltiples enlaces de interconexión (alta redundancia) para asegurar el servicio en caso de que alguno de ellos llegase a fallar. En la siguiente gráfica se puede observar un ejemplo de interconexión lógica entre dos centros de datos, generalmente uno posee mayor capacidad que el otro y gestiona gran parte del tráfico.

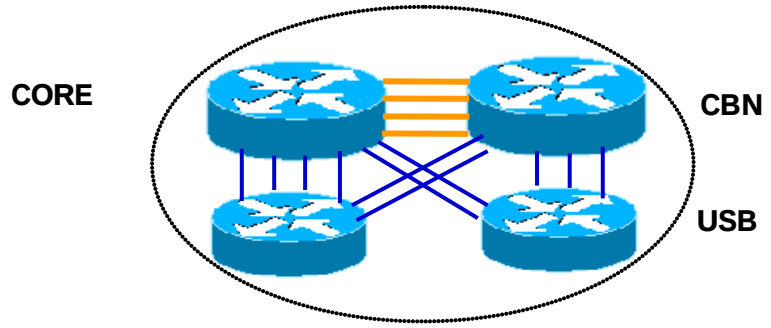



Figura 5 Ejemplo de interconexión de centros de datos
Fuente: Departamento de Sistemas de Corporación Digitel

La siguiente capa, *DISTRIBUCION*, se encarga de enrutar el tráfico proveniente de la capa de acceso y de determinar qué paquetes deben ser enviados al núcleo y cuáles no, esta capa comprende los nodos de cada región a lo largo del país y su interconexión con los puntos de acceso en la capa inferior.

La última capa, *ACCESO*, está constituida principalmente por los centros de atención y las oficinas regionales de la empresa, se encarga básicamente de la conmutación de paquetes entre ellos y controla el acceso de los usuarios a la red. En la siguiente figura se puede apreciar la estructura detallada de la empresa incluyendo los dos centros de datos que conforman el Núcleo de la topología, los diferentes POP de cada región respectiva que conforman la capa de Distribución y los puntos de acceso con las oficinas regionales y centros de atención correspondientes a la última capa de la topología.

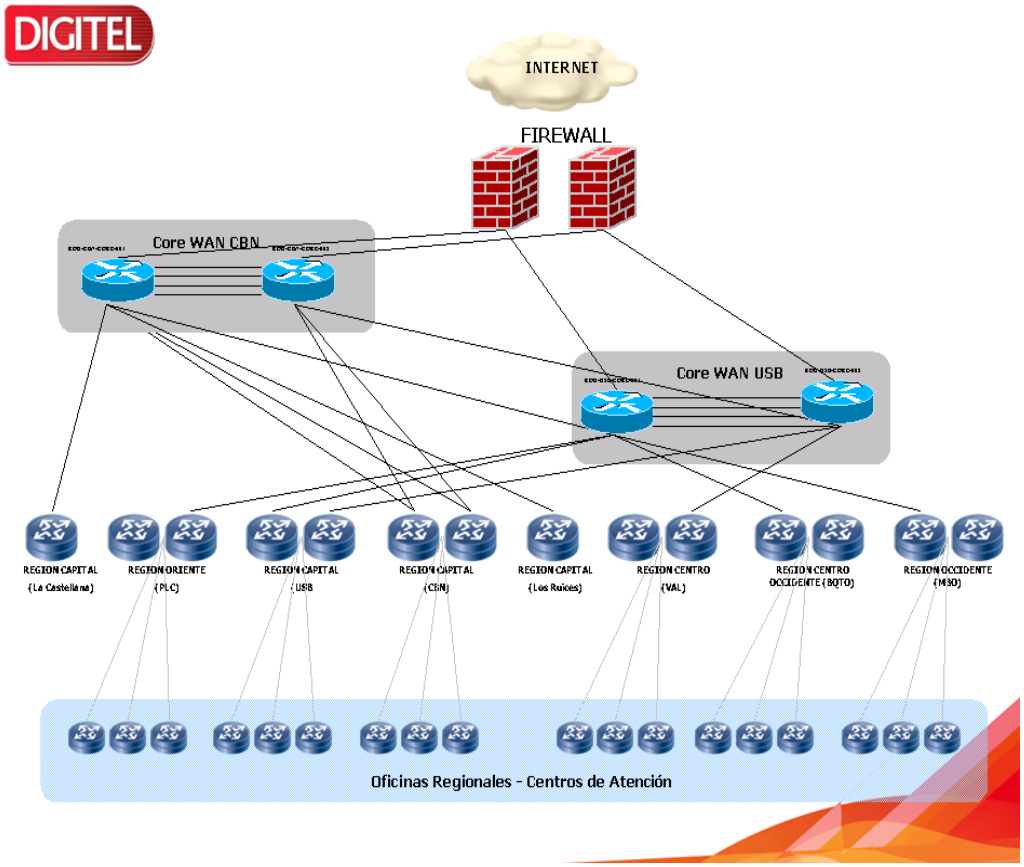



Figura 6 Actual distribución de la Red Corporativa

Fuente: Departamento de Sistemas de Corporación Digitel

En la figura 6 se puede apreciar en lo más alto de la estructura, dos Firewall o Corta fuegos perimetrales, que se encargan de proteger a toda la corporación de múltiples ataques provenientes de la nube o Internet.

Dentro de la capa de distribución, cada región está constituida por dos routers (a excepción de “Región Capital La Castellana” y “Región Capital Los Ruices”), cada pareja de routers posee interconexiones, que no son observadas en la figura 6 pero existen lógicamente de manera tal de asegurar una ruta al momento de fallar uno de los enlaces y garantizar la continuidad del servicio.

De acuerdo a la estructura de la Red Corporativa, la capa *NUCLEO* o *CORE* está comprendida por los centros de datos *Cubo Negro (CBN)* y *Universidad Simón Bolívar (USB)*, en un futuro cercano estará constituida además, por el centro de datos *La Colina*, ya que la sustitución de éste último por *Cubo Negro*, no es inmediata y convivirán los tres centros de datos durante un período de tiempo. La estructura diseñada por el departamento de sistemas para la interconexión de los tres centros de datos es la siguiente:

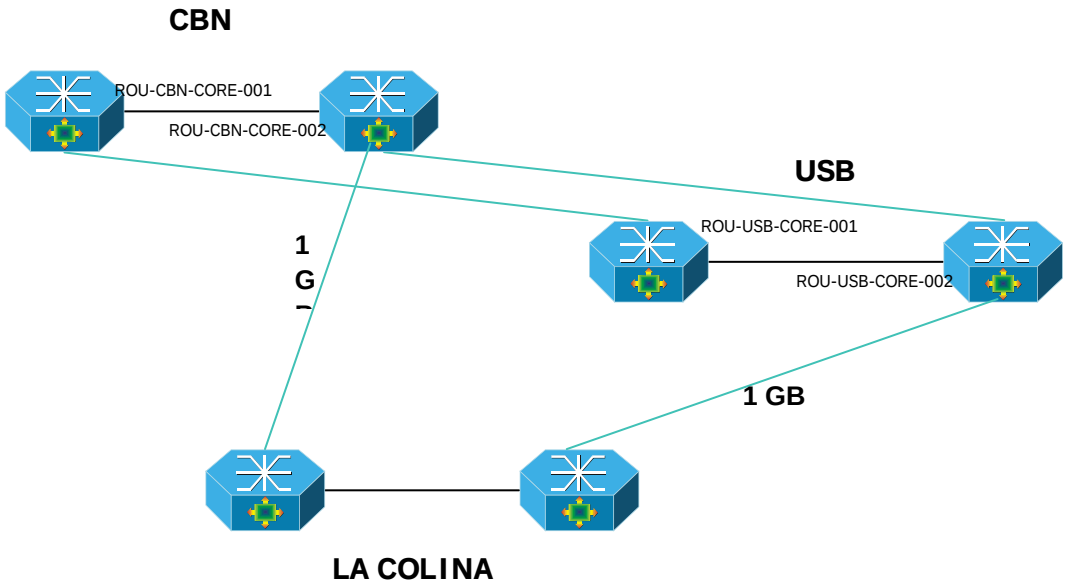



Figura 7 Interconexión de tres centros de datos
Fuente: Departamento de Sistemas de Corporación Digitel

Todos los centros de datos en el gráfico, poseen al menos una ruta por defecto y una de respaldo en caso de fallas en el enlace, además de interconexiones entre ellos y alta capacidad para gestionar una gran cantidad de tráfico. Los enlaces contra *La Colina* son los de mayor capacidad (1 Gbps), ya que se estima que una vez operativo será la cabecera en cuanto a gestión. Asimismo, cuando el centro de datos *Cubo Negro* sea desincorporado por completo, los enlaces redundantes serán únicamente entre *Universidad Simón Bolívar* y *La Colina*.

### 4.1.2 Estructura del centro de datos La Colina

Como consecuencia del impacto e importancia de la implementación del centro de datos en la corporación, debido a que pasaría a formar parte de la capa *Core* de la misma, su estructura obedece a un sistema organizado, seguro y con características muy similares a la división en capas de la topología de red de la empresa.

En primera instancia el centro de datos estará interconectado a la red corporativa a través de dos enlaces de 1Gbps, uno con el centro de datos *Universidad Simon Bolivar* y otro con *Cubo Negro* (como se detalló en la figura 7), estas conexiones, junto con los routers de borde de cada nodo, formaran la red de área amplia (WAN).

Los enlaces de la interconexión de la red WAN llegarán a dos routers de borde ubicados en la primera etapa de la topología de red de *La Colina*; el siguiente peldaño se constituirá por dos switch y dos firewall a través de enlaces de alta capacidad (10Gbps) y tendrá el nombre de capa *Core*; la ubicación lógica de los firewall en esta topología no fue definida por el personal de sistemas, por lo tanto en la imagen número 8 se colocan al mismo nivel que los equipos switch pero sin ningún tipo de conexión con el sistema hasta que el diseño quede definido por completo. Finalmente, la última capa de la topología es llamada *Acceso* y en ella estarán alojados todos los servidores que forman parte de la población del presente estudio, además de varios switch que permitirán la interconexión entre cada uno de ellos. Es importante señalar que, la capa *Core* y la capa de *Acceso* conforman la red de área local (LAN) del centro de datos *La Colina*.

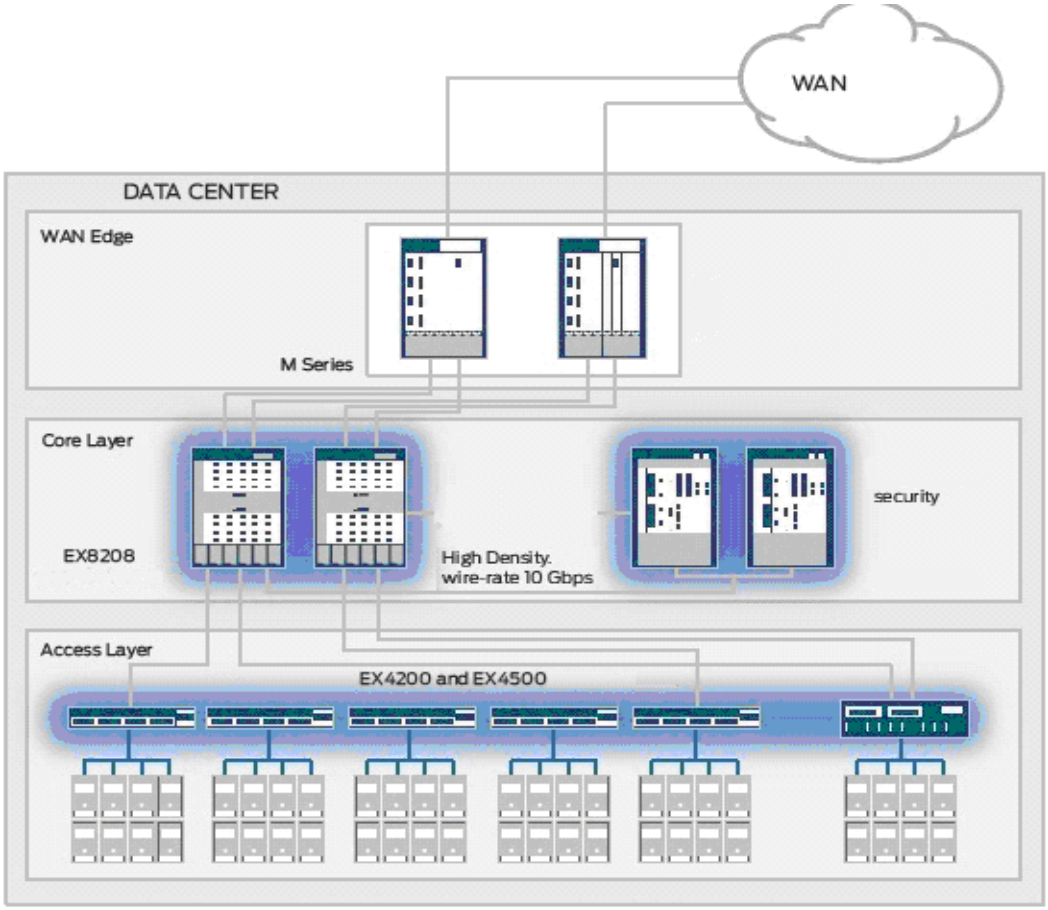



Figura 8 Topología del centro de datos *La Colina*
Fuente: Departamento de Sistemas de Corporación Digitel

Como se puede observar en la figura 8, muchos de los equipos están identificados con un número serial o código que corresponden a la marca Juniper, seleccionada por la empresa como solución para sus routers y switch; es por ello que, en relación a mantener la armonía y organización en la topología el departamento de sistemas sugirió que los equipos firewall incluidos en el diseño de la plataforma de seguridad pertenezcan también a esta marca y se lleve a cabo el desarrollo del proyecto tomando en cuenta las virtudes y capacidades que pudiesen aportar los mismos a las soluciones propuestas.

Los equipos actualmente desplegados en la topología de red del centro de datos La Colina, detallados en la figura 8, pueden ser observados en la siguiente

tabla con una breve descripción respecto a su funcionalidad en la estructura. Es importante aclarar que, no se incluye al firewall o cortafuegos en la tabla 1 debido a que éste se encuentra en la fase de diseño y no ha sido implementado, a diferencia de los demás equipos que sí se encuentran actualmente instalados.

Tabla 1 Equipos de la topología de red *La Colina*

| | |
|---|---|
| Router Wan MX 480: Router de borde con alta capacidad de enrutamiento de tráfico, ubicado en la primera etapa de |  |
| Switch Core Lan EX8208: Switch de la capa *Core* y red LAN de la topología del centro de datos; posee una plataforma modular con gran densidad de puertos y escalabilidad. |  |
| Equipo EX XRE200: Máquina de enrutamiento externa agregada a equipos Switch y Firewall, para formar una estructura denomina Virtual Chasis. |  |
| Switch Acceso EX4200: Switch de la capa de acceso con capacidad de Virtual Chasis. |  |

En la tabla 1 se hace referencia a una tecnología denomina *Virtual Chasis*, la cual consiste en unir dos equipos Switch o Firewall, provistos con puertos indicados para tal fin, y ser trabajados lógicamente como un solo equipo, de tal

manera de ahorrar trabajo en gestión y aumentar la capacidad de enlaces en un solo equipo virtual.

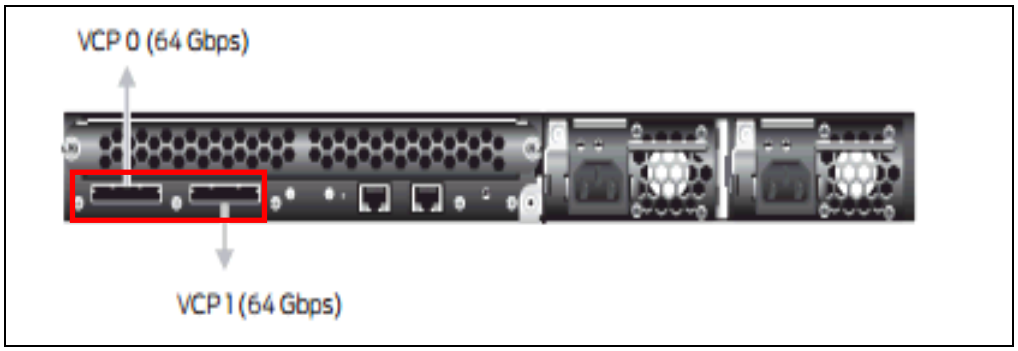



Figura 9 Puertos de Virtual Chasis en un equipo Switch EX4200
Fuente: http://www.juniper.net/techpubs/en_US/junos/topics/concept/virtual-chassis-ex4200-overview.html
Consulta: 20/01/2013

Debe señalarse que aunque los equipos sean trabajados lógicamente como uno solo, no implica que la capacidad aumente al doble, uno de los equipos sigue tomando el control como maestro y el otro se conserva como respaldo o backup en caso de que el primario falle. En la topología del centro de datos se aplicará esta tecnología en los equipos Switch de la capa *Core* y *Acceso*.

### 4.1.3 Infraestructura del centro de datos *La Colina*

El centro de datos *La Colina* se encuentra ubicado, en la avenida la salle, colina Los Caobos al lado de la Quinta Miss Venezuela; el acceso es realizado a través de carro particular y el ingreso a las instalaciones es limitado. Su infraestructura se encuentra en sus fases terminales, restando el acabado del área de oficinas e iluminación en el último piso.

En la figura 10 se expone una vista superior del primer piso, lugar donde estará ubicada la sala de equipos, los cuartos de terceros y las oficinas de monitoreo; el interior del edificio tendrá una expansión de 14x24 metros cuadrados aproximadamente y tres pisos compuestos por planta baja, piso 1 (detallado en el plano por ser el referente al área del centro de datos) y piso 2 de oficinas; los equipos se mantendrán a una temperatura adecuada para su correcto funcionamiento a través de aires acondicionados y estarán dispuestos de tal manera que se formen pasillos “calientes” y “fríos”, como se indica en el plano de la siguiente página, con el fin de proporcionar una refrigeración más precisa y eficiente, reduciendo al mismo tiempo el consumo energético; la salida de los equipos de refrigeración se concentra en los pasillos fríos, donde los equipos toman en su parte frontal el aire y lo expulsan hacia el pasillo en el que se ubican las salidas traseras de los equipos (pasillo caliente).

En el plano se detalla el cuarto de equipos con cinco filas de servidores, los primeros cuatros Racks de la fila “D” son identificados como “Switch Redes”, de manera de establecer que esa será la ubicación para los equipos de la topología (Routers MX480, Switch 8208, Switch EX4200 y Firewall). La sala contigua al cuarto de equipos, será habilitada para diseñar un cuarto de terceros, una sala de monitoreo y una sala mucho más pequeña con servidores de “Storage” y Racks disponibles.

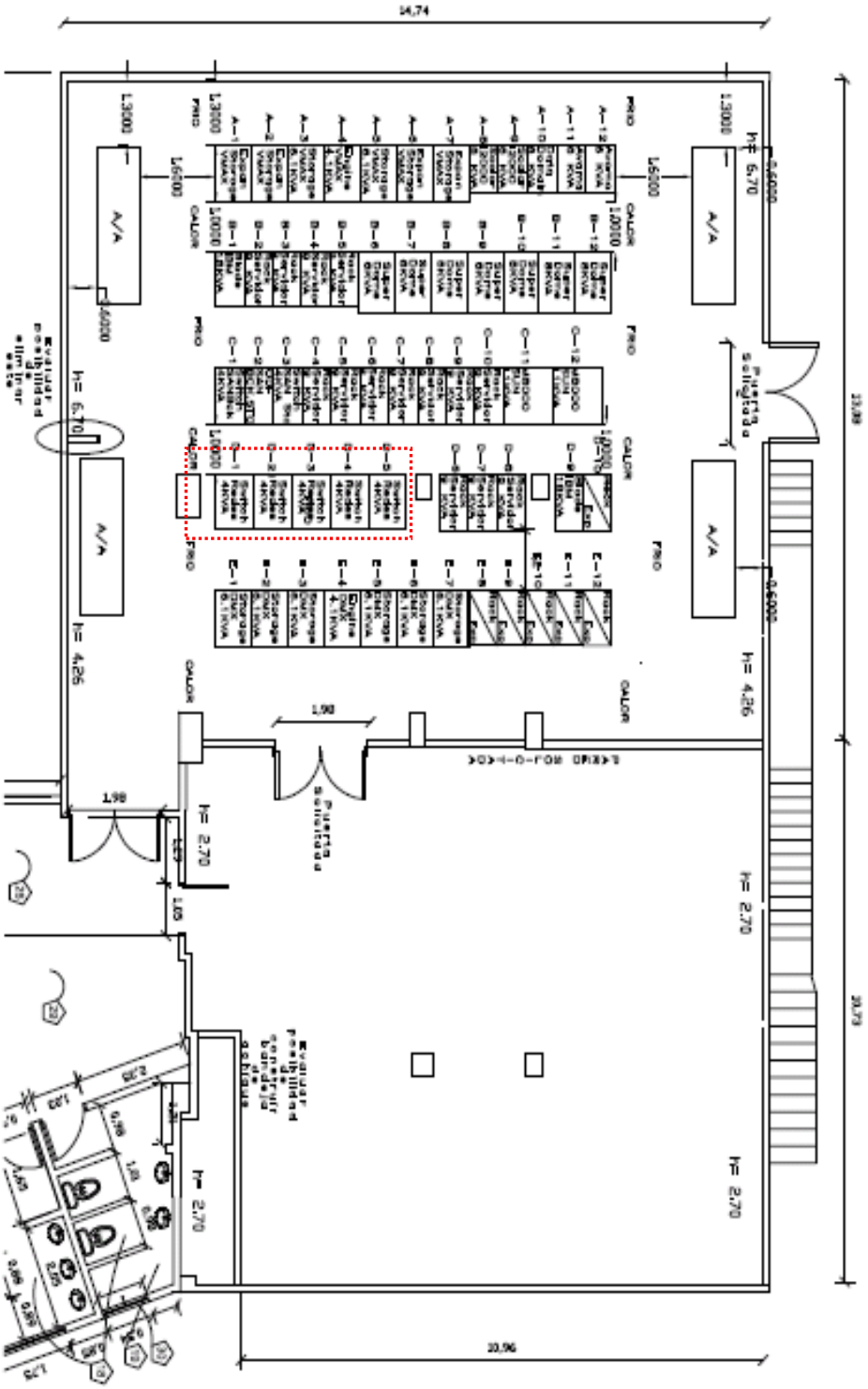


Figura 10 Plano Planta Nivel Piso 1 Centro de Datos La Colina

Fuente: Departamento de Sistemas

Además de la distribución de equipos y espacios dentro de la infraestructura física, otro aspecto de relevante importancia es el referente a la energización de los equipos y el cableado de los mismos.

La distribución de cableado en el Centro de Datos en lo que respecta a las conexiones está basada en un diseño propuesto por distintas zonas según el tipo de servicio o sistema operativo a instalar, respetando las normas de cableado horizontal y vertical según sea el caso. La solución escogida por la corporación es llamada “Fiber Runner” o Canal de Fibra Óptica. En cuanto a energización se realizó un dimensionamiento de las cargas que soportará el centro de datos, tomando en cuenta un futuro crecimiento, además de disponibilidad de recursos alternativos como baterías para los UPS y plantas de emergencia.

### 4.1.4 Requerimiento de la empresa en cuanto a seguridad

Para realizar el diseño de plataforma de seguridad del centro de datos *La Colina*, en primera instancia fue necesario conocer el requerimiento general de la empresa en cuanto a sus necesidades, debilidades y preocupaciones respecto a la actual estructura.

Luego de reuniones y entrevistas con el personal de redes, se pudo establecer que la necesidad principal de la empresa en cuanto a seguridad en el centro de datos *La Colina*, encuentra sus principios en la protección de los servicios y/o servidores alojados en las plataformas Microsoft y Unix, debido a que actualmente el acceso a ellos no se ve limitado por políticas o reglas de seguridad y son desarrollados en el mismo ambiente. En consecuencia a ello, el riesgo a ataques internos es elevado, por lo tanto el departamento de sistemas

expuso la necesidad de separar ambas plataformas y delimitar el acceso de una hacía otra.

A pesar de que el nivel de seguridad solicitado no hace referencia a un firewall perimetral, ya que la empresa dispone de un equipo para tal fin que se encarga de proteger a la red completa contra ataques externos, si expone la importancia de respaldar la plataforma a través de un cortafuegos que permita proteger las áreas, servicios, aplicaciones y/o servidores delimitando de qué forma se acceden a ellas, quiénes gozan de permisos de control y monitoreo, separar los ambientes de desarrollo y producción de cada plataforma y brindar protección contra ataques en caso de que algún intruso logre derribar la protección del firewall perimetral.

Finalmente en concordancia con la información recolectada, las divisiones solicitadas por la empresa para proteger las distintas plataformas serán las siguientes:

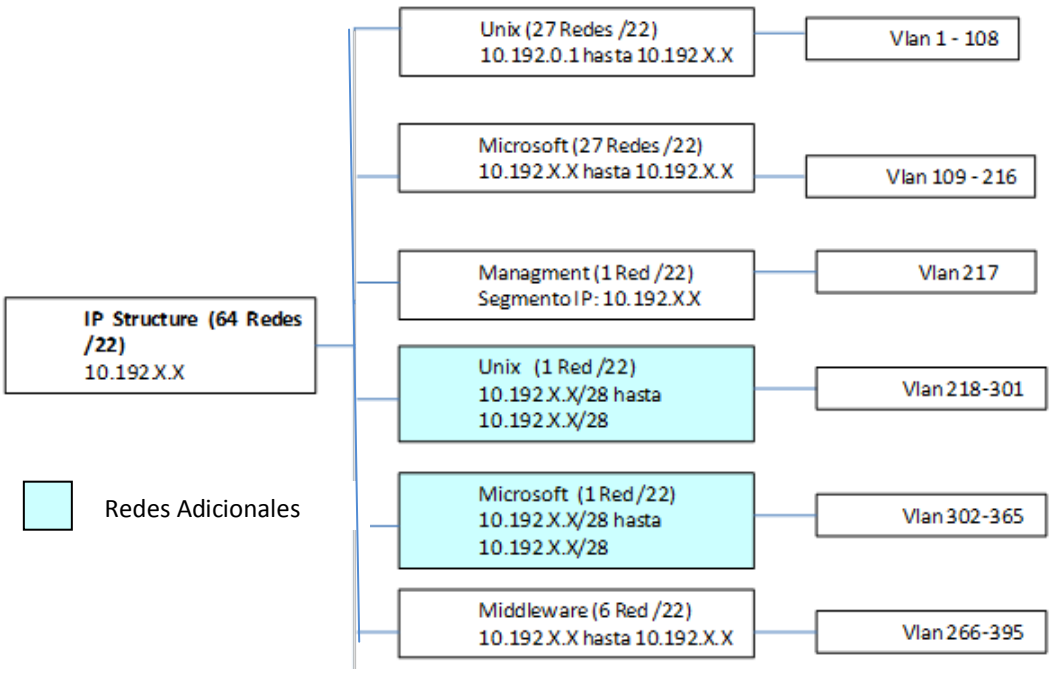
a) Zona Trust: integrada por todos los servidores pertenecientes a la plataforma Unix; es identificada como una zona de confianza debido a que el desarrollo de ataques contra este sistema operativo es pobre y más complejos que otros como Microsoft. A pesar de estar en una zona etiquetada como “segura” en ella se aplican de igual forma todas las políticas y reglas del centro de datos.

b) Zona Untrust: definida por todos los servidores pertenecientes a la plataforma Microsoft; la etiqueta de zona insegura proviene de la gran cantidad de ataques desarrollados contra este sistema operativo y por ende de su vulnerabilidad contra intrusos y amenazas. El acceso de esta zona hacia la zona de confianza será regulado severamente.

c) Zona Middleware: cuando se realiza una petición a una aplicación y la respuesta a ella depende de dos servicios diferentes, es necesario un software que gestione la información entre ambas aplicaciones y de una respuesta acertada, este software es llamado Middleware y todos los servidores que lo gestionan serán ubicados en una zona diferente, de manera de asegurar el flujo de información sin que la zona segura penetre a la insegura o viceversa.

Asimismo, la empresa decidió ubicar a cada plataforma en segmentos IP distintos, de manera tal de identificar fácilmente la ubicación de un paquete de acuerdo a su IP y filtrar a través de grandes segmentos el tráfico cursante y no individualmente. A continuación se muestra un esquema con la asignación de segmentos IP a cada departamento.

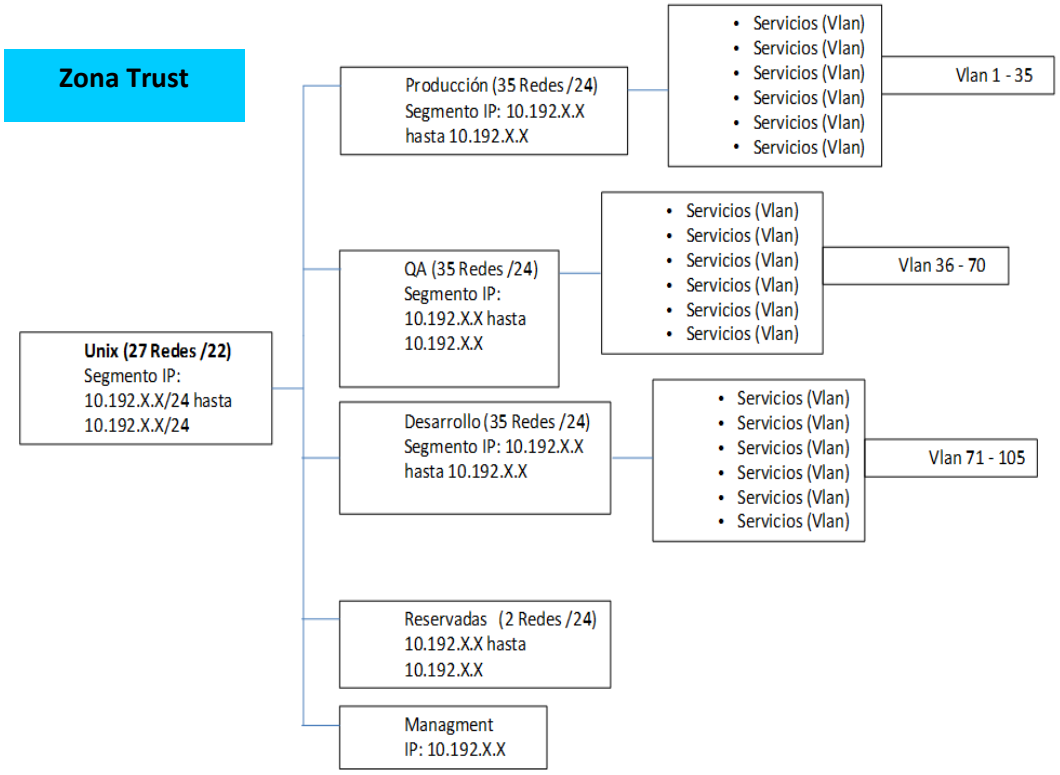
Tabla 2 Asignación de segmentos IP a cada departamento
Fuente: Departamento de Sistemas de Corporación Digitel



Las zonas en color azul, se refieren a redes adicionales en caso de implementaciones no previstas inicialmente por el departamento. A su vez cada zona divide sus segmentos en: Producción, Desarrollo y Q/A con el propósito de realizar pruebas en cada servicio y/o aplicación mucho antes de la puesta en producción. En los siguientes esquemas se detalla la división de cada plataforma en varios ambientes de acuerdo a lo indicado anteriormente.

Tabla 3 Distribución de segmento IP en plataforma Segura o Trust

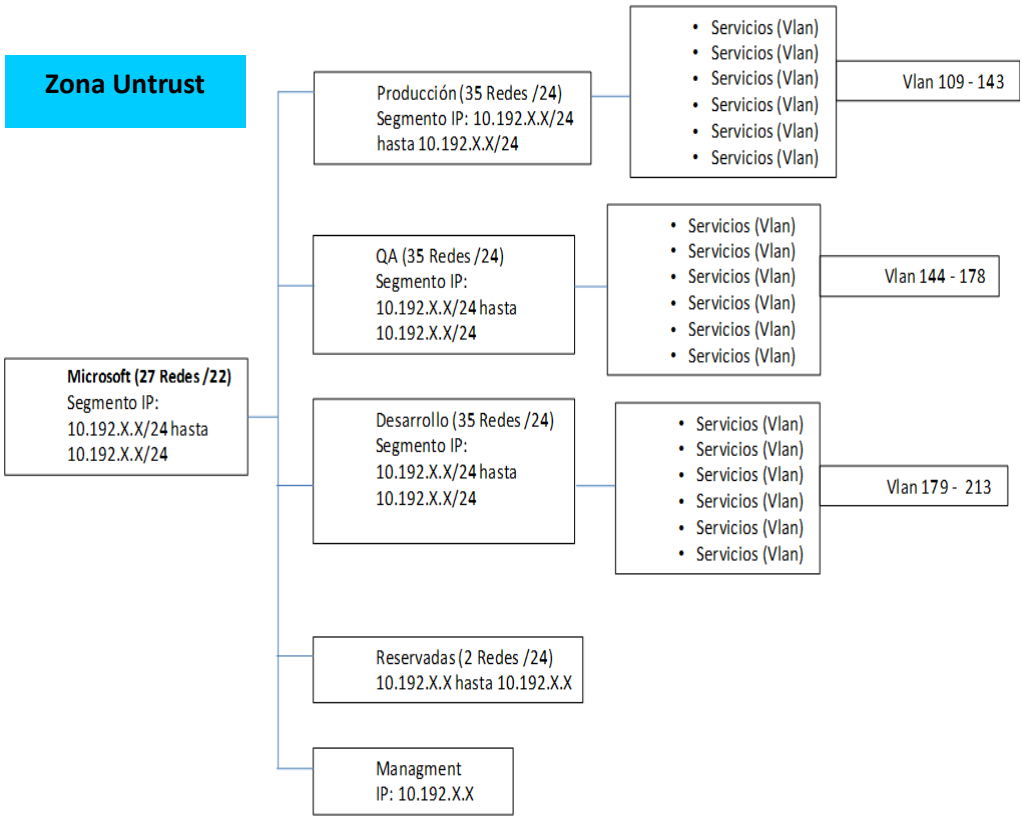
Fuente: Departamento de Sistemas de Corporación Digitel




El área identificada como Q/A es aquella donde se realizan constantes pruebas a un servicio o aplicación de manera de comprobar su calidad, en el área de desarrollo se realizan cambios cuando se detecta una falla o defecto en la sección anterior; finalmente, cuando se superan todas las pruebas exitosamente la aplicación es puesta en producción y se cumple el ciclo completo.

Tabla 4 Distribución de segmento IP en plataforma Insegura o Untrust

Fuente: Departamento de Sistemas de Corporación Digitel

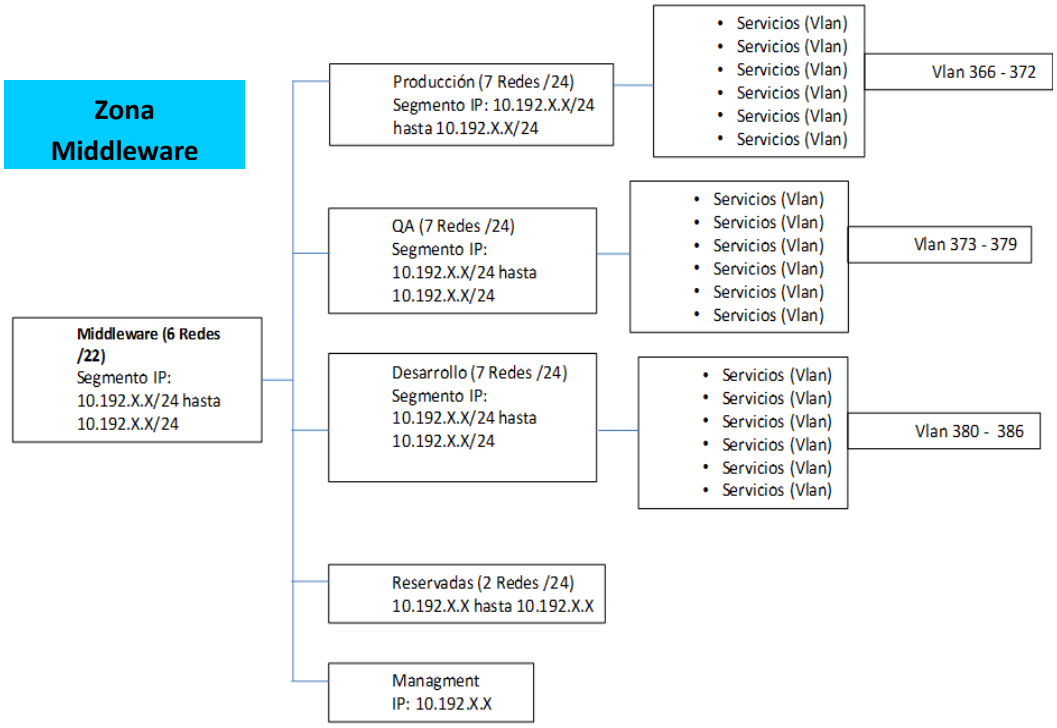



Tanto la zona segura como la insegura poseen 27 Redes segmentadas en barras 22 (/22) que a su vez se dividen en 35 redes de segmento barra veinticuatro (/24) para producción, 35 para Q/A, 35 para Desarrollo, 2 reservadas y una de gestión o Management.

En el caso de la zona Middleware y por tratarse de la zona más pequeña de ambas (sólo 6 redes barra 22), la segmentación se realizó de la siguiente manera: 7 redes barra 24 por cada ambiente de producción, Q/A y desarrollo, dos redes barra 24 reservadas y una red barra 24 para gestión o Management.

Tabla 5 Distribución de segmento IP en plataforma Middleware

Fuente: Departamento de Sistemas de Corporación Digitel



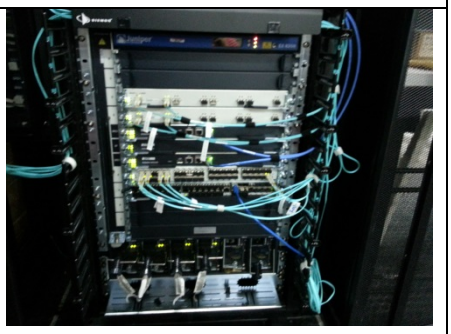

Al observar el desglose por segmentos de direcciones IP, es notable que la migración debe darse bajo un proceso organizado y en un periodo de tiempo considerable, en relación a lo cual la empresa solicitó la protección de los servidores (en producción) ubicados hasta ese momento en el centro de datos, bajo una propuesta que permitiría expansión a medida que el resto de los servidores sea migrado.

### 4.1.5 Servidores en producción en centro de datos La Colina

Una vez identificada la necesidad de la empresa, el siguiente paso constituyó el levantamiento de información de todos los equipos y servidores que se encontraban desplegados en el centro de datos *La Colina*.

En concordancia a lo antes expuesto, la primera inspección se realizó en base a cuáles equipos de la topología del centro de datos se habían instalados hasta ese momento y cuáles se encontraban actualmente gestionando peticiones, la respuesta a esta interrogante se detalla en la siguiente tabla:

Tabla 6 Equipos instalados en el centro de datos *La Colina*
Fuente: Fotografías recolectadas por el autor

| Equipo | Modelo | Cantidad | Marca | Foto |
|---|---|---|---|---|
| Router | MX-480 | 2 | Juniper |  |
| Switch | EX-8208 | 2 | Juniper |  |
| Routing Engine | EX-XRE200 | 2 | Juniper |  |
| Switch | EX-4200 | 20 | Juniper |  |

Las fotos anexas en la tabla 6 fueron recolectadas por el autor en las instalaciones del centro de datos *La Colina*, excepto la referente al equipo EX – 4200, que al formar parte de la capa de acceso y necesitar cercanía con los servidores a los que será conectado, su ubicación física no es igual a los demás equipos de la topología.

El siguiente paso se caracterizó por continuas entrevistas con el personal de los departamentos Unix, Microsoft y la coordinación de servidores de aplicación, con el fin de recolectar toda la información de los servidores correspondientes a cada plataforma, ya migrados al centro de datos *La Colina*. Es importante aclarar que todo el universo de servidores no fue migrado en una sola etapa, la migración será realizada en varios niveles, sin embargo se requiere proteger los servidores de la primera etapa de migración y establecer las políticas de seguridad a la hora de migrar el resto del universo.

La información se recolectó en función del nombre de VLAN, segmento asociado a ella, direcciones IP de cada segmento, servidor asociado a cada dirección IP y nombre de las aplicaciones por servidor.

La IP cuya último número del octeto es diez (10), corresponde al Gateway de la VLAN asociada, el pool de direcciones IP desglosadas junto a cada segmento IP, hace referencia sólo a las direcciones IP de los servidores actualmente en producción en el centro de datos *La Colina* y no a la totalidad de sus direcciones

Todos los datos detallados anteriormente, fueron organizados en tablas, de acuerdo a cada zona (Trust, Untrust y Middleware), y son presentados en las siguientes páginas.

Tabla 7 Servidores en producción en el centro de datos *La Colina*. **Zona Trust**

Fuente: Departamento Unix de Corporación Digitel

| Nombre VLAN | Segmento IP | Direcciones IP | Servicio |
|---|---|---|---|
| **MONITOREO_CONTROL_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Aplicaciones varias (Remedy, Rmedy Mid Tier, Factura Digital) Multipath |
| | | X.X.X.X | Aplicaciones varias (Remedy, Rmedy Mid Tier, Factura Digital) |
| | | X.X.X.X | CMD |
| | | X.X.X.X | CMD (Multipath) |
| | | X.X.X.X | Remedy Servicio Mid Tier |
| | | X.X.X.X | Remedy |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) Multipath |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) Multipath |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) |
| | | X.X.X.X | Aplicación TMART |
| **ALMACENAMIETNO_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | Legato respaldo Colina |
| | | X.X.X.X | Catalogo RMAN La Colina (Prueba 2) |
| | | X.X.X.X | Catalogo RMAN La Colina (Prueba 1) |
| | | X.X.X.X | Catalogo RMAN La Colina (Servicio) |
| | | X.X.X.X | Data Domain |
| | | X.X.X.X | Data Domain |
| | | X.X.X.X | Data Domain |
| | | X.X.X.X | Data Domain |
| **BCK_MONITOREO_CONTROL_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Aplicaciones varias (Remedy, Rmedy Mid Tier, Factura Digital) Backup |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) Backup |
| | | X.X.X.X | CMD (Backup) |
| | | X.X.X.X | Aplicación TMART (Backup) |
| | | X.X.X.X | Remedy Servicio Mid Tier (Backup) |
| | | X.X.X.X | Remedy (Backup) |
| | | X.X.X.X | Nodo 1 Aplication Server Factura Digital (Backup) |
| | | X.X.X.X | Nodo 2 de Factura Digital (Backup) |
| | | X.X.X.X | Factura Digital (Backup) |
| | | X.X.X.X | SAP Historico |
| **BCK_ALMACENAMIENTO_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Legato respaldo Colina (Backup) |
| **SEGURIDAD_ELECTRONICA** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |

| | | | |
|---|---|---|---|
| | | X.X.X.X | No hay servicios alojados en este servidor |
| **GESTION_SERVICIOS_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Zona Global (Prueba 1) |
| | | X.X.X.X | Zona Global (Prueba 2) |
| | | X.X.X.X | Zona Global (Servicio) |
| | | X.X.X.X | DNS La Colina |
| | | X.X.X.X | Repositorio OPCSW |
| | | X.X.X.X | SMTP La Colina |
| **OTRAS_BD_TRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Base de Datos RGR (Prueba 1) |
| | | X.X.X.X | Base de Datos RGR (Prueba 2) |
| | | X.X.X.X | Base de Datos RGR (Servicio) |
| | | X.X.X.X | Base de datos unica de clientes (Multipath) |
| | | X.X.X.X | Base de datos unica de clientes (Multipath) |
| | | X.X.X.X | Base de datos unica de clientes |
| | | X.X.X.X | Base de datos unica de clientes (VIP Nodo Cluster) |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 (Multipath) |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 (Multipath) |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 (VIP Nodo cluster) |
| | | X.X.X.X | Base de datos unica de clientes (Round Robin) |
| | | X.X.X.X | Base de datos unica de clientes (Round Robin) |
| | | X.X.X.X | Base de datos unica de clientes (Round Robin) |
| | | X.X.X.X | Billing History |
| | | X.X.X.X | Billing History (Multipath) |
| | | X.X.X.X | Billing History (Multipath) |
| | | X.X.X.X | Billing History (VIP Nodo Cluster) |
| | | X.X.X.X | Billing History |
| | | X.X.X.X | Billing History (Multipath) |
| | | X.X.X.X | Billing History (Multipath) |
| | | X.X.X.X | Billing History (VIP Nodo Cluster) |
| | | X.X.X.X | Billing History - Base de datos (Round Robin) |
| | | X.X.X.X | Billing History - Base de datos (Round Robin) |
| | | X.X.X.X | Billing History - Base de datos (Round Robin) |
| | | X.X.X.X | TT Whare House - Base de datos (Prueba 1) |
| | | X.X.X.X | TT Whare House - Base de datos (Prueba 2) |
| | | X.X.X.X | TT Whare House - Base de datos (Servicio) |
| | | X.X.X.X | Repositorio de archivos planos Providencia (Prueba 1) |
| | | X.X.X.X | Repositorio de archivos planos - Providencia (Prueba 2) |
| | | X.X.X.X | Repositorio de archivos planos - Providencia (Servicio) |
| | | X.X.X.X | Zona Global (IVR, CL House, SARA) Prueba 1 |
| | | X.X.X.X | Zona Global (IVR, CL House, SARA) Prueba 2 |
| | | X.X.X.X | Zona Global (IVR, CL House, SARA) Servicio |
| | | X.X.X.X | CL House (Prueba 1) |
| | | X.X.X.X | CL House (Prueba 2) |

| | | | |
|---|---|---|---|
| | | X.X.X.X | CL House (Servicio) |
| | | X.X.X.X | Base de datos consolidada (SARA) |
| | | X.X.X.X | Base de datos consolidada (SARA) Prueba 1 |
| | | X.X.X.X | Base de datos consolidada (SARA) Prueba 2 |
| | | X.X.X.X | ROAMI |
| | | X.X.X.X | ROAMI (Prueba 1) |
| | | X.X.X.X | ROAMI (Prueba 2) |
| **BCK_OTRAS_BD_TRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Base de datos RGR (Backup) |
| | | X.X.X.X | Base de datos unica de clientes (Backup) |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 (Backup) |
| | | X.X.X.X | Billing History (Backup) |
| | | X.X.X.X | Billing History (Backup) |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | Repositorio de providencia (Backup) |
| | | X.X.X.X | Zona Global (IVR, CL House, SARA) Backup |
| | | X.X.X.X | CL House (Backup) |
| | | X.X.X.X | SARA (Backup) |
| | | X.X.X.X | ROAMI (Backup) |
| **BCK_GESTION_ TRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| **CLUSTER_BDUC_TRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Base de datos unica de clientes (Interconnect Cluster) |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 (Interconnect Cluster) |
| | | X.X.X.X | Base de datos unica de clientes (Interconnect Cluster) |
| | | X.X.X.X | Base de datos unica de clinetes oracle 2 (Interconnect Cluster) |
| **PLATSAP_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Zona Global (App. Servers SAP) Prueba 1 |
| | | X.X.X.X | Zona Global (App. Servers SAP) Prueba 2 |
| | | X.X.X.X | Zona Global (App. Servers SAP) Servicio |
| | | X.X.X.X | App. SAP 1 |
| | | X.X.X.X | App. SAP 2 |
| | | X.X.X.X | Zona Global (App. Servers SAP) Prueba 1 |
| | | X.X.X.X | Zona Global (App. Servers SAP) Prueba 2 |
| | | X.X.X.X | Zona Global (App. Servers SAP) Servicio |
| | | X.X.X.X | App. SAP 3 |
| | | X.X.X.X | App. SAP 4 |
| | | X.X.X.X | Zona Global (2 servidores de BI - Moscoso y 1 servidor SAP) |
| | | X.X.X.X | Servicio Inteligencia de negocios (BI) |
| | | X.X.X.X | Servicio Inteligencia de negocios (BI) |
| | | X.X.X.X | Solution Manager SAP |
| | | X.X.X.X | Zona Global providencia (App. Providencia y Base de datos Providencia) |
| | | X.X.X.X | Base de datos providencia |
| | | X.X.X.X | Solution Manager SAP Prueba 1 |
| | | X.X.X.X | Solution Manager SAP Prueba 2 |

| | | | |
|---|---|---|---|
| | | X.X.X.X | App. Server Providencia |
| | | X.X.X.X | Zona Global providencia<br>(App. Providencia y Base de datos Providencia) Prueba 1 |
| | | X.X.X.X | Zona Global providencia<br>(App. Providencia y Base de datos Providencia) Prueba 2 |
| | | X.X.X.X | Base de datos providencia Prueba 1 |
| | | X.X.X.X | Base de datos providencia Prueba 2 |
| | | X.X.X.X | App. Server Providencia Prueba 1 |
| | | X.X.X.X | App. Server Providencia Prueba 2 |
| | | X.X.X.X | Zona Global providencia<br>(App. Providencia y Base de datos Providencia) |
| | | X.X.X.X | Zona Global providencia<br>(App. Providencia y Base de datos Providencia) Prueba 1 |
| | | X.X.X.X | Zona Global providencia<br>(App. Providencia y Base de datos Providencia) Prueba 2 |
| | | X.X.X.X | RBI / ISAP (Prueba 1) |
| | | X.X.X.X | RBI / ISAP (Prueba 2) |
| | | X.X.X.X | Inteligencia de negocios (BI) Prueba 1 |
| | | X.X.X.X | Inteligencia de negocios (BI) Prueba 2 |
| | | X.X.X.X | Inteligencia de negocios (BI) Prueba 1 |
| | | X.X.X.X | Inteligencia de negocios (BI) Prueba 2 |
| | | X.X.X.X | Cluster Rack Oracle ATC |
| | | X.X.X.X | Cluster Rack Oracle ATC Prueba 1 |
| | | X.X.X.X | Cluster Rack Oracle ATC Prueba 2 |
| | | X.X.X.X | SAP |
| | | X.X.X.X | SAP Prueba 1 |
| | | X.X.X.X | SAP Prueba 2 |
| **DEV_ENVIRO_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Zona Global desarrollo (REMEDY, MID TIER) Prueba 1 |
| | | X.X.X.X | Zona Global desarrollo (REMEDY, MID TIER) Prueba 2 |
| | | X.X.X.X | Zona Global desarrollo (REMEDY, MID TIER) Servicio |
| | | X.X.X.X | Aplicaciones varias (Mediacion, Data W.) Multipath |
| | | X.X.X.X | Mediacion |
| | | X.X.X.X | Mediacion |
| | | X.X.X.X | Mediacion |
| | | X.X.X.X | Data W. |
| | | X.X.X.X | REMEDY |
| | | X.X.X.X | MID TIER |
| | | X.X.X.X | REMEDY |
| **PLATPROV_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Aprovisionamiento |
| | | X.X.X.X | Aprovisionamiento Prueba 1 |
| | | X.X.X.X | Aprovisionamiento Prueba 2 |
| **PREVENCION_CONTROL_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | IP de prueba |
| | | X.X.X.X | IP de prueba |
| **BCK_ PLATPROV_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |

| | | | |
|---|---|---|---|
| | | X.X.X.X | Backup Aprovisionamiento |
| **BCK_ PLATSAP_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Sap Aplication Server 1 y 2 |
| | | X.X.X.X | Sap Aplication Server 1 |
| | | X.X.X.X | Sap Aplication Server 2 |
| | | X.X.X.X | Sap Aplication Server 3 y 4 |
| | | X.X.X.X | Sap Aplication Server 3 |
| | | X.X.X.X | Sap Aplication Server 4 |
| | | X.X.X.X | SAP Solution Manager Backup |
| | | X.X.X.X | Interligencia de negocios Backup |
| | | X.X.X.X | Zona global (RBI / ISAP) Backup |
| | | X.X.X.X | Interligencia de negocios Backup |
| | | X.X.X.X | Zona global<br>(App. Providencia y Base de datos Providencia) Backup |
| | | X.X.X.X | Base de datos providencia Backup |
| | | X.X.X.X | App. Server Backup |
| | | X.X.X.X | Zona global<br>(App. Providencia y Base de datos Providencia) Backup |
| | | X.X.X.X | Zona Global Cluster ATC |
| | | X.X.X.X | SAP Backup |
| **ATCMV_TRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | IVR Prueba 1 |
| | | X.X.X.X | IVR Prueba 2 |
| | | X.X.X.X | IVR Servicio |
| | | X.X.X.X | Cluster ATC Nodo 2 |
| | | X.X.X.X | Cluster ATC Nodo 2 Prueba 1 |
| | | X.X.X.X | Cluster ATC Nodo 2 Prueba 2 |
| | | X.X.X.X | Base de datos ATC |
| | | X.X.X.X | Base de datos ATC Prueba 1 |
| | | X.X.X.X | Base de datos ATC Prueba 2 |
| | | X.X.X.X | Base de datos ATC |
| | | X.X.X.X | Base de datos ATC Prueba 1 |
| | | X.X.X.X | Base de datos ATC Prueba 2 |
| | | X.X.X.X | Zona Global L Domain |
| | | X.X.X.X | Zona Global L Domain Prueba 1 |
| | | X.X.X.X | Zona Global L Domain Prueba 2 |
| **BCK_ATCMV_TRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | IVR Backup |
| | | X.X.X.X | Zona Global L Domain Backup |
| | | X.X.X.X | Base de datos ATC Nodo 1 Backup |
| | | X.X.X.X | Base de datos ATC Nodo 2 Backup |
| | | X.X.X.X | Zona Global L Domain Backup |

Tabla 8 Servidores en producción en el centro de datos *La Colina*.

**Zona Middleware**

Fuente: Departamento Unix y Coordinación de Servidores de Aplicación de Corporación Digitel

| Nombre VLAN | Segmento IP | Direcciones IP | Servicio |
|---|---|---|---|
| **MIDDLE_PROD_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Factura Digital (Multipath) |
| | | X.X.X.X | Factura Digital |
| | | X.X.X.X | Aplicaciones varias (Remedy, Rmedy Mid Tier, Factura Digital) Multipath |
| | | X.X.X.X | Aplicaciones varias (Remedy, Rmedy Mid Tier, Factura Digital) Multipath |
| | | X.X.X.X | Nodo 2 de Factura Digital |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) Multipath |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) Multipath |
| | | X.X.X.X | Nodo 1 Aplication Server Factura Digital |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | Balanceador F5 Flotante |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware (Multipath) |
| | | X.X.X.X | Middleware (Multipath) |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | SMS Sender nodo 1 Interno |
| | | X.X.X.X | SMS Sender nodo 1 Interno (Multipath) |
| | | X.X.X.X | SMS Sender nodo 1 Interno (Multipath) |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware (Multipath) |
| | | X.X.X.X | Middleware (Multipath) |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Sap Aplication Server 1 y 2 |
| | | X.X.X.X | Sap Aplication Server 1 y 2 (Multipath) |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Sap Aplication Server 3 y 4 |
| | | X.X.X.X | Sap Aplication Server 3 y 4 (Multipath) |
| | | X.X.X.X | Middleware |
| | | X.X.X.X | Aplicaciones varias (TMART,SAP Historico, Factura Digital) |
| | | X.X.X.X | Aplicaciones varias (Remedy, Rmedy Mid Tier, Factura Digital) |

| | | | |
|---|---|---|---|
| | | X.X.X.X | Sap Historico |
| | | X.X.X.X | Sap Aplication Server 3 |
| | | X.X.X.X | Web Logic Base de datos unica de clientes |
| **BCK_MIDDLE_PROD_TRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | Middleware (Backup) |
| | | X.X.X.X | SMS Sender nodo 1 Interno (Backup) |
| | | X.X.X.X | SMS Sender nodo 1 Interno (Backup) |
| | | X.X.X.X | Web logic Froname ATC Postpago - Prepago y Club de lealtad (Backup) |
| | | X.X.X.X | Bus SAP - Bus 412 Postpago - Bus consolidado (Backup) |
| | | X.X.X.X | Bus 412 - VP Prepago - Bus 412 ECM LM Prepago (Backup) |
| | | X.X.X.X | Encuestas BAM - Trivia - Enc. GOH - Promociones Agentes Aut. (Backup) |
| | | X.X.X.X | Web logic base de datos unica de clientes (Backup) |

La gran mayoría de los servidores ubicados en el centro de datos La Colina, que pertenecen a esta zona (Middleware) trabajan bajo el sistema operativo UNIX.

Tabla 9 Servidores en producción en el centro de datos *La Colina*.

**Zona Untrust**

Fuente: Departamento Microsoft de Corporación Digitel

| Nombre VLAN | Segmento IP | Direcciones IP | Servicio |
|---|---|---|---|
| **MONITOREO_CONTROL_UNTRUST** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Apl. TMART |
| **ALMACENAMIIENTO_UNTRUS** | **10.192.X.X/24** | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | Consola Control Center EMC |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |

| | | | |
|---|---|---|---|
| | | X.X.X.X | Gateway EMC |
| **MICROSOFT_UNTRUST_PRODUCCION** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Domain Controller |
| | | X.X.X.X | BES 10(App Blackberry) |
| | | X.X.X.X | App Virtualización |
| | | X.X.X.X | Aplicación SIMCARDS |
| | | X.X.X.X | App Autana |
| | | X.X.X.X | BES (App Blackberry) |
| | | X.X.X.X | Gestion IP |
| | | X.X.X.X | Software Reportes BO |
| | | X.X.X.X | Plan de numeracion Nac |
| | | X.X.X.X | App. Autocad |
| | | X.X.X.X | Consola PCM (sap) |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | App solarwins |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| **UMARKET1_UNTRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |

| | | | |
|---|---|---|---|
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| **UMARKET2_UNTRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| **UMARKET3_UNTRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| | | X.X.X.X | Recargas Electronicas |
| **UMARKET4_UNTRUST_PROD** | **10.192.X.X/24** | X.X.X.X | Gateway Recargas Electronicas |
| **PREVENCION_CONTROL_UNTRUST** | **10.192.X.X/24** | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | SEGURIDAD |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |
| | | X.X.X.X | |

| | | | |
|---|---|---|---|
| **Servicios_plataformas_microsoft** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Windows Update SUS |
| | | X.X.X.X | Próxy Desarrollo |
| | | X.X.X.X | DNS Externo |
| **Servicios_plataformas_correo** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Correo - DAG digitelcorp.com.ve |
| | | X.X.X.X | Correo - DAG digitelcorp.com.ve |
| | | X.X.X.X | Correo - DAG digitelcorp.com.ve |
| | | X.X.X.X | Exchange 2010 Dominio Digitel |
| | | X.X.X.X | Exchange 2010 Dominio Digitel |
| | | X.X.X.X | Correo - DAG digitelcorp.com.ve |
| | | X.X.X.X | Correo - DAG digitelcorp.com.ve |
| | | X.X.X.X | Correo - DAG digitelcorp.com.ve |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| **BCK_ Servicios_plataformas_correo** | **10.192.X.X/24** | X.X.X.X | Gateway |
| **Ambiente_Desarrollo_virtual** | **10.192.X.X/24** | X.X.X.X | Hyper-V (Virtualizacion) |
| | | X.X.X.X | Nodo Hyper-V (Virtualizacion) |
| | | X.X.X.X | Nodo Hyper-V (Virtualizacion) |
| | | X.X.X.X | Hyper-V (Virtualizacion) |
| | | X.X.X.X | Hyper-V (Virtualizacion) |
| | | X.X.X.X | Hyper-V (Virtualizacion) |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| | | X.X.X.X | No hay servicios alojados en este servidor |
| **Laboratorio** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Laboratorio Microsoft |
| | | X.X.X.X | Laboratorio SQL |
| **Serv_Agent_Aut_produccion** | **10.192.X.X/24** | X.X.X.X | Gateway |
| | | X.X.X.X | Domain Controller Digitelaccc |
| | | X.X.X.X | Exchange 2010 Dominio Digitelaccc |
| | | X.X.X.X | Exchange 2010 Dominio Digitelaccc |
| | | X.X.X.X | Correo |
| | | X.X.X.X | Correo |
| | | X.X.X.X | No hay servicios alojados en este servidor |

## 4.2 Estudio de políticas de seguridad en un centro de datos

Existen diversos documentos en la red de Internet, tesis e informes de investigación donde se detalla en base a normas y experiencia, el proceso que debe llevarse a cabo para brindar total seguridad a un centro de datos o cómputo, en base a ellos se establecerá de forma general un esquema con las políticas de seguridad mayoritariamente empleadas en el mundo actual y que deben ser referencia a la hora de desarrollar la propuesta en cuanto a seguridad.

Inicialmente, se recomienda por muchos expertos en el tema que las políticas de seguridad a ser implementadas en un centro de datos, tomen un enfoque de acuerdo a los distintos niveles de protección que se pretenden desarrollar: Físicos, Lógicos, Humanos y la interacción que existen entre ellos.

Según Benson Cristopher en su libro *Estrategias de Seguridad*, todo plan de seguridad debe incluir tanto una estrategia Proactiva como una Reactiva: *"**La Estrategia Proactiva** (proteger y proceder) o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia."* [15]. Asimismo, *"**La Estrategia Reactiva** (perseguir y procesar) o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia Proactiva…"* [16].

Además de lo antes expuesto, existen dos posturas que toda plataforma de seguridad implementa de acuerdo a sus objetivos; la primera hace referencia a la premisa de que todo lo que no se permite será denegado o prohibido (regla negar todo); la segunda indica que todo lo que no es prohibido explícitamente será

permitido (regla permitir todo). De acuerdo a cuál fundamento sea elegido, dependerá la naturaleza de las políticas de seguridad a ser implementadas.

Por otra parte, todo estratega de seguridad debe responder tres preguntas básicas cuando se enfrenta a la necesidad de proteger una plataforma; estas interrogantes pueden ser apreciadas en el siguiente ciclo de vida.


Figura 11 Esquema de estrategias de seguridad

Fuente: Seguridad en redes informáticas. Autor Luis Miguel Díaz Vizcaino

http://www.it.uc3m.es/~lmiguel/Firewall_www/SEGURIDAD-to-Web.htm

### 4.2.1 Elementos a proteger en un centro de datos

Toda necesidad de seguridad parte del principio básico y esencial de proteger los elementos que forman parte de la plataforma de una empresa, estos elementos son divididos según su naturaleza, pueden ser de índole Físico o Lógico.

Los elementos físicos dentro de la plataforma de una empresa, son todos aquellos equipos que forman parte de la topología y tienen su ubicación en un espacio determinado del centro de datos, como routers, switch, firewall, servidores, aires acondicionados, fuentes de alimentación eléctrica, entre otros; por ello, es de suma importancia restringir el acceso a las áreas donde son ubicados de manera tal de reducir al máximo robos, daños maliciosos y cualquier otra acción perjudicial contra su estado y condición física.

Por otra parte, los elementos lógicos que toda corporación desea proteger pueden dividirse, a su vez, en datos, programas y hardware; Los datos de una empresa se exponen diariamente a actos perjudiciales como robo de información confidencial, destrucción y desaparición de investigaciones y proyectos o modificación de datos, los cuales equivalen de manera similar a resultados nefastos y de gran atraso para la empresa. Asimismo, los programas también deben ser protegidos por la principal razón de que a través de ellos se puede acceder a los datos; finalmente, el hardware es una herramienta tan vulnerable como las dos mencionadas anteriormente, debido a que un usuario malintencionado puede utilizar una máquina que no es suya para perpetrar ataques y permanecer en el anonimato.

De manera similar y no menos importante, otro elemento que debe ser protegido es la imagen, a razón de que una empresa que ha sido atacada o

utilizada para atacar a terceros, produce alta desconfianza entre la colectividad y una apariencia de desidia que no la favorece en ningún caso.

### 4.2.2 Amenazas contra centro de datos

Las amenazas que afronta constantemente un centro de datos pueden ser divididas en dos categorías, las que pertenecen al campo de las redes y software informáticos, llamadas también amenazas digitales, y las que se refieren a la infraestructura física denominadas amenazas físicas.

Dentro de las amenazas físicas, se pueden mencionar: temperatura de los aires acondicionados en la sala, Racks y equipos, debido a que niveles superiores a los especificados o cambios drásticos en la temperatura, pueden ocasionar problemas en los equipos o reducción de su vida útil; asociada a la temperatura se encuentra la humedad relativa en la sala de quipos y Racks, que puede producir puntos de acumulación de electricidad estática lo que deriva en fallas en los equipos; las filtraciones de líquidos forman parte de las posibles amenazas porque pueden producir daños en el piso, cableado y equipos; asimismo, se debe considerar el factor humano y el acceso de personal a las distintas áreas de acuerdo a su nivel de importancia, una deficiente política al respecto puede llevar a robo de los equipos o sabotaje, así como daños involuntarios; otra posible amenaza es referente a incendio de equipos eléctricos o materiales, daños causados por humo y consecuencias de los mismos dentro de las instalaciones del centro de datos; finalmente, se debe tomar en cuenta los contaminantes peligrosos como químicos, hidrogeno de las baterías o partículas de polvo, que puedan quedar suspendidos en el aire y producir obstrucción de filtros/ventiladores, falta de confiabilidad en los UPS y fallas en general por la emanación de hidrogeno.

En concordancia con lo antes expuesto, las amenazas digitales pueden resultar iguales o más peligrosas que las amenazas físicas, porque en muchas ocasiones pueden pasar desapercibidas; las principales amenazas digitales están constituidas por hackers, crackers, virus, cuellos de botella en las redes y cualquier otro ataque accidental o malicioso a la red de seguridad o a la transmisión de datos. A continuación se anexa una imagen donde se puede apreciar la diferencia entre amenazas físicas y digitales:


Figura 12 Amenazas a los centros de datos

Fuente:

http://www.fasor.com.sv/whitepapers/whitepapers/Monitoreo/Como_monitorear_amenazas_fisicas_en_centro_de_datos.pdf

Consulta: 19/02/2013

Sin embargo, los ataques más conocidos en el mundo de redes y sistemas de seguridad son los siguientes: Trashing (Cartoneo) ocurre cuando un atacante se hace de una llave para entrar al sistema; ataques de monitoreo, cuya finalidad es observar a la víctima y su sistema para establecer sus vulnerabilidades y emprender futuros ataques, se encuentra divido en cuatro tipos: Shoulder Surfing,

Decoy (señuelos), Scanning (Búsqueda) y Snooping-Downloading; ataques de autenticación cuyo objetivo es engañar al sistema de la víctima para ingresar al mismo, el más conocido de este tipo de ataque es el spoofing-looping; Denial of Service (DoS) o denegación de servicio, consiste en saturar los recursos de la víctima para inhabilitar los servicios que brinda, este tipo de ataque se puede presentar en dos formas: Jamming o Flooding y Conection Floyd; otro ataque conocido es el de modificación o daño y se puede dar como Tampering o Data Diddling y Borrado de Huellas.

Asimismo, existen muchos servicios en la red cuyas debilidades son explotadas diariamente, a continuación se detallan lo más usados de éstos y los riesgos que se corren al utilizarlos:

Correo: es quizás uno de los servicios más usados en la red, su principal riesgo consiste en la difusión de gusanos por toda la red. A nivel de protocolo puede dividirse en POP3 (que corre en el puerto 110), IMAP, muy parecido al POP3 y utilizado para correo entrante y SMTP utilizado comúnmente para el correo saliente.

FTP: es usado para transferir archivos entre usuarios y su principal problema radica en el hecho de que se pueden transmitir archivos malignos sin el conocimiento del autor. Generalmente se usa a través del puerto 21 para comandos y 20 para datos (en modo activo)

Telnet: a través de este servicio se puede controlar remotamente un equipo, en modo consola por medio del puerto TCP 23. Su principal problema radica en que no utiliza encriptación. En su lugar es mucho mejor utilizar SSH que corre en el puerto TCP 22 y utiliza encriptación para proteger la información.

HTTP: es el servicio más usado en el mundo de Internet y paradójicamente no provee por si mismo ningún tipo de autenticación ni de encriptación, generalmente utiliza el puerto TCP 80 y su principal función es la transmisión y ejecución de programas a través del navegador de Internet.

DNS: este servicio se encarga de transformar nombres en direcciones IP y viceversa. Su principal debilidad es contra ataques de tipo Buffer Overflow y negación de servicio.

Otros servicios: según Luis Miguel Díaz Vizcaino es de suma importancia conocer como funciona cualquier servicio a la hora de habilitarlo, en su artículo "Seguridad Informática" presentado ante la Universidad Carlos III de Madrid, indica que "*En cualquier caso es conveniente testear la seguridad de un programa antes de permitir que se instale en la red y comprometa la seguridad de esta. Por otro lado, el servicio debe abrir un único puerto, para minimizar el riesgo, y en caso de que pueda abrir gran cantidad de ellos, se debe fijar estáticamente a un único puerto.*"[17]

### 4.2.3 Políticas para proteger un centro de datos

La seguridad de la red corporativa y su infraestructura asociada, dependen de los conocimientos que se tengan sobre sus vulnerabilidades y las medidas de protección desplegadas en toda su plataforma; estos conocimientos no impedirán que se realicen ataques a su estructura pero sí reducirá notablemente el riesgo de que alguno de ellos logré causar daños a la empresa. En la actualidad, los ataques a pequeñas y grandes empresas son más frecuentes y es necesario contar con un

esquema de seguridad que logre protegerla y asegure el correcto funcionamiento en toda su estructura.

Como se mencionó con anterioridad, existen dos tipos de amenazas contra un centro de datos: Físicas y Lógicas, por ello las políticas de seguridad se agruparán de acuerdo al tipo de amenaza que representan, a continuación el detalle.

Políticas para la seguridad física

La seguridad física identifica las amenazas y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización, por ello es de suma importancia tomar en cuenta los riesgos a los que se encuentra expuesto diariamente el centro de datos, para así implementar, de acuerdo al área y necesidades, los sistemas que aseguren el buen funcionamiento de los equipos, por ejemplo los sistemas UPS son capaces de monitorear la calidad de la energía e integridad de las baterías, las unidades de enfriamiento monitorean las temperaturas de entrada y salida así como el estado de los filtros y los sistemas de extinción de incendios monitorean la presencia de humo o exceso de calor.

Además, se debe realizar seguimiento periódicamente a los cuartos de telecomunicaciones, con el objetivo de identificar el estado de los equipos y las condiciones ambientales del mismo, de manera de poder aplicar los correctivos necesarios a tiempo. A continuación, se expone un resumen de las recomendaciones generales, en cuanto a políticas de seguridad física que toda empresa debe implementar para proteger su plataforma.

- ✓ **Control de acceso físico a áreas seguras**

1) El perímetro de seguridad debe ser claramente definido.
2) Los salones de los centros de cómputo deben estar equipados con puertas antimotines, resistentes al fuego y a cualquier intento de entrada forzosa.
3) Los espacios donde se ubiquen los equipos de procesamiento o almacenamiento, deben ser protegidos de accesos no autorizados, utilizando técnicas de autenticación, monitoreo y registro de entradas y salidas.
4) Se deben establecer diferentes categorías de personal de acuerdo al acceso permitido: A) Personal que labore diariamente en las áreas seguras. B) Personal que requiera acceso periódico. C) Otros que requieran acceder muy rara vez.
5) Separación física de cuartos de terceros con espacios de telecomunicaciones propios, a fin de evitar que personas externas a la empresa ingresen a los cuartos de telecomunicaciones.
6) Todos los visitantes deben ingresar con un acompañante durante toda su estadía en el centro de datos y deben poseer una identificación a la vista.
7) No se debe permitir el acceso con videograbadoras, cámaras de fotografías, ni equipos de hardware especial.
8) Todas las salidas de emergencia deben tener alarmas sonoras y cierre automático.

- ✓ **Seguridad de los equipos**

1) Se debe contar con un sistema de enfriamiento, control de temperatura y humedad en los cuartos de telecomunicaciones. Implementación de pasillos fríos y calientes.

2) En todo centro de procesamiento deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio.
3) Se deben tener extintores de incendios debidamente probados y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.
4) No se debe permitir el ingreso de material explosivo a las instalaciones.
5) Las salas de procesamiento de la información deben estar ubicadas en pisos a una altura superior al nivel de la calle a fin de evitar inundaciones.
6) Las cañerías deben poseer válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre flujos.
7) Los cables de potencia deben estar separados de los de comunicaciones.
8) El cableado de la red debe ser protegido de interferencias usando canaletas que lo aseguren.
9) No se permite fumar, ni consumir ningún tipo de alimento o bebida en las áreas donde se ubiquen los equipos de procesamiento.
10) Protección de equipos contra fallas de potencia u otras anomalías eléctricas: correcto uso de UPS (Uninterruptable power suply), los cuales deben garantizar suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones; Se deben poseer interruptores eléctricos adicionales y el generador debe ser regularmente probado.
11) Todas las puertas de los estantes y gabinetes de equipos ubicados en el centro de cómputo deben permanecer cerrados con llave, a menos que un técnico especializado esté realizando reparaciones o mantenimiento.

- ✓ **Mantenimiento de los equipos**

1) Se debe realizar mantenimiento sobre los equipos de acuerdo a las recomendaciones del fabricante y ser realizado únicamente por personal autorizado.

- ✓ **Escritorios y pantallas limpias**

1) Papeles y medios de información deben ser asegurados en armarios especiales, cuando sea necesario, especialmente en horas no laborables.
2) Información confidencial debe ser asegurada en bóvedas preferiblemente.
3) Las impresoras y fotocopiadoras deben estar protegidas de uso no autorizado.

- ✓ **Bitácora de eventos**

1) Finalmente se recomienda llevar una bitácora de cuartos de telecomunicaciones con el fin de identificar constantemente el estado de los equipos y las condiciones ambientales. Asimismo, es importante llevar un inventario de los activos del centro de datos.

Esta información fue recolectada de varias guías de fabricantes y grandes empresas a través de Internet, las fuentes son debidamente identificadas en la bibliografía del presente trabajo.

Políticas para la seguridad lógica

Luego de establecer los principios de la seguridad física básica de una empresa o establecimiento, lo siguiente es controlar el acceso digital desde y hacia la red de la organización, que en la mayoría de los casos se logra controlando los puntos de acceso con el mundo exterior. Una de las muchas formas de controlar el acceso de una zona a otra se logra con un dispositivo firewall o cortafuegos, debido a que puede controlar estrictamente qué se autoriza a pasar de un lado al otro, la elección del tipo de firewall depende de ciertos factores, como los niveles de tráfico, los servicios que requieran protección y la complejidad de las reglas que se necesitan implementar.

A través de un dispositivo firewall se puede bloquear el tráfico de red dirigido a ciertos destinos, este proceso puede realizarse tanto por direcciones IP como por puertos de servicios específicos de la red, por ejemplo, una empresa que desee brindar acceso a su servidor Web puede limitar todo el tráfico al puerto 80 (puerto HTTP estándar), en la mayoría de los casos las restricciones son aplicadas al tráfico que se origina en lado no confiable de la red. No obstante, el problema de la mayoría de las empresas radica en el hecho de enfrentar la realidad de permitir el acceso a los servicios públicos que ésta ofrece, como servidor de correo electrónico, servidor DNS, la Web, el FTP, entre otros, y conservar al mismo tiempo una seguridad rigurosa en su red. En la mayoría de los casos, el método utilizado para resolver este inconveniente se basa en la creación de una zona desmilitarizada o DMZ, ubicada entre el firewall perimetral y el firewall que protege la red interna de la empresa, en la siguiente imagen se puede observar con mayor claridad esta definición.

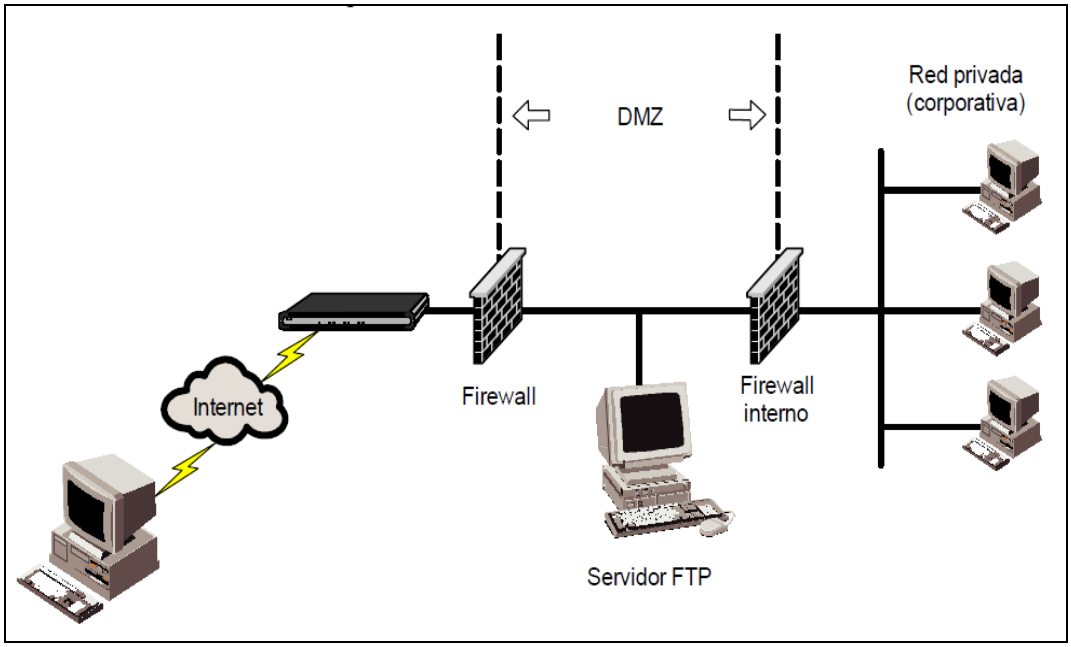



Figura 13 Firewalls duales con DMZ

Fuente: Christopher Leidigh, Principios fundamentales de la seguridad de las redes

Además de la implementación de un firewall para establecer la seguridad de la red corporativa, las organizaciones pueden definir unos ámbitos básicos o esenciales en donde empezar a implementar políticas de seguridad; entre los más comunes encontramos: seguridad de la red, seguridad de los usuarios y seguridad de los datos; a ello también se le debe sumar todos los aspectos referentes a las auditorias de seguridad y los compromisos legales. Estos elementos constituyen el último eslabón de una plataforma solida de seguridad en cualquier empresa y centro de datos, a continuación se enumeraran las políticas de seguridad que constituyen cada ámbito.

- ✓ **Seguridad de la red:** configuración de los sistemas operativos, acceso lógico y remoto, autenticación, Internet, disciplina operativa, gestión de cambios, desarrollo de aplicaciones.

1) Supervisar la configuración de los sistemas operativos, los sistemas que no posean los parches adecuados de software o que estén contaminados con virus, deben ser desconectados de la red.
2) Implementar equipos de protección como firewalls o cortafuegos en los puntos de tránsito de la red pública o privada.
3) Configurar en los equipos métodos de autenticación seguros, para administración vía Web HTTPS o vía consola SSH.
4) Todas las conexiones entre las redes internas de la institución e Internet, deben incluir un cortafuego autorizado y los controles de acceso correspondientes.
5) Todos los accesos a interneT utilizando computadores de las oficinas de la empresa deben ser enrutados a través del cortafuego.
6) La institución debe monitorear el tráfico en Internet sin bloquear ni filtrar los sitios visitados por los trabajadores, ni censurar las transmisiones enviadas o recibidas.

7) Los diseñadores y desarrolladores de los sistemas de la empresa deben restringir la utilización de las interfaces de redes y protocolos externos y utilizar aquellos expresamente autorizados.
8) Debe existir un proceso formal para el manejo de problemas, de tal modo que éstos puedan quedar registrados para minimizar su incidencia y evitar que ocurran de nuevo.
9) Los parámetros de configuración y de instalación de todos los servidores incorporados a la red de la empresa deben ajustarse a la normativa y políticas de seguridad interna especificadas.
10) La gerencia debe diseñar sus redes de comunicaciones de manera tal que no exista un solo punto central de falla que pudiera causar la no disponibilidad de los servicios de la red.
11) Los servidores públicos en Internet se deben ubicar en subredes, aparte de las redes internas de la institución, y a las cuales se haya restringido el paso del público mediante enrutadores o cortafuegos.

- ✓ **Seguridad de los usuarios:** composición de claves, seguridad en estaciones de trabajo, formación y creación de conciencia.

1) Cualquier sistema pequeño que maneje información bien sea crítica o sensible, debe utilizar una versión mantenida adecuadamente de un sistema de control de acceso basado en contraseñas (creación de contraseñas alfanuméricas y cambio de las mismas cada tres meses).
2) Los usuarios no deben implantar conexiones Telnet en los computadores de la empresa utilizando contraseñas fijas tradicionales en internet.
3) Los trabajadores no deben descargar software de ningún sistema externo a la empresa a menos que posea la autorización del administrador.
4) La empresa debe monitorear rutinariamente los computadores personales conectados a sus redes para detectar virus.
5) Todos los computadores de los usuarios conectados a internet deben tener activo un sistema de detección de intrusiones autorizado por el departamento.

6) Todos los computadores personales y estaciones de trabajo con acceso a internet, deben tener sus propios cortafuegos instalados y continuamente activos.
7) Se debe instruir al personal sobre la importancia de la seguridad de la información y resguardo de contraseñas, claves y privilegios de usuarios intransferibles.

- ✓ **Seguridad de los datos:** criptografía, clasificación, privilegios, copias de seguridad y recuperación, antivirus, plan de contingencia.

1) Debe estar instalado y habilitado un software antivirus en todos los cortafuegos de la institución, los servidores FTP, los servidores de correo, los servidores de la intranet y las máquinas de escritorio.
2) Se debe respaldar mensualmente toda la información en los sistemas informáticos de la institución. Toda la información sensible debe estar cifrada a la hora de realizar el respaldo.
3) Todos los archivos respaldados deben ser recuperables para su posterior revisión por parte de los administradores.
4) Toda la información considerada sensible, de fácil acceso a través de medios públicos, debe ser ligeramente modificada con el objetivo de esconder su real naturaleza de alta integridad.
5) Todos los sistemas conectados a Internet utilizados con fines productivos, deben usar diariamente herramientas para evaluar la integridad de los archivos y comparar las firmas digitales de los archivos críticos con las firmas digitales mantenidas en un sistema desconectado.
6) Los trabajadores que han sido autorizados para ver la información clasificada con un cierto nivel de sensibilidad, pueden acceder sólo a la información de ese nivel o a la de menor nivel de sensibilidad.
7) Debe elaborarse un plan de contingencia en caso de fallas o intrusiones.

- ✓ **Auditoria de seguridad:** incluye todos los análisis de riesgos, revisiones periódicas, visitas técnicas, monitoreo y auditoria.

- ✓ **Aspectos legales:** contratos y acuerdos comerciales, leyes y reglamentación gubernamental.

El cumplimiento de todas las políticas antes mencionadas (físicas y lógicas), reduce notablemente el riesgo de ataques e intrusiones a la red corporativa de cualquier empresa.

## 4.3 Diseño de políticas de seguridad para el centro de datos La Colina

Las políticas de seguridad bien planificadas dentro de una empresa, incrementan la seguridad de la red corporativa de forma significativa, ayudando a reducir los huecos obvios en el sistema y permitiendo la resolución de problemas más complejos. Como se ha indicado en el desarrollo del trabajo de investigación, el tema de seguridad debe ser atacado bajo dos ángulos bien diferenciados: seguridad física y seguridad lógica; a pesar de que el alcance del actual proyecto se limite a la parte lógica o digital, se realizó un seguimiento de las condiciones de seguridad físicas en el centro de datos en cuestión, con el objetivo de verificar las buenas prácticas implementadas y realizar recomendaciones sobre las deficiencias que puedan presentar, para ser corregidas mucho antes de su puesta en servicio por completo.

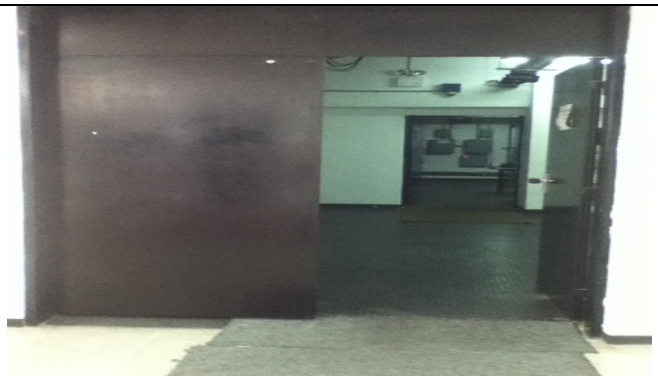
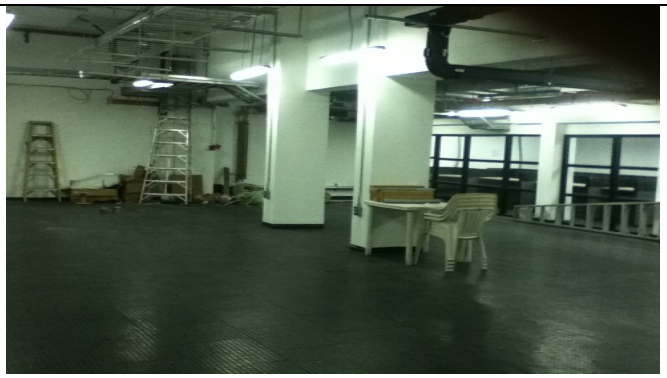
### 4.3.1 Aspectos de seguridad física en el centro de datos La Colina

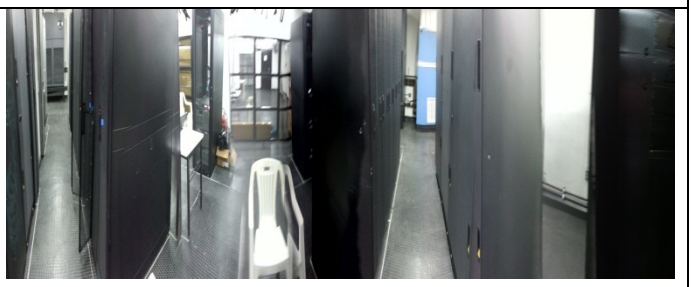
Para la evaluación de este aspecto, se partió de las recomendaciones en cuanto a políticas de seguridad física del apartado anterior y se realizó un análisis en general de las condiciones del centro de datos, de manera de especificar la normativa a seguir según las condiciones y necesidades particulares de la empresa

y su centro de datos. A través de diferentes recorridos a las instalaciones y por medio de entrevistas con el personal de supervisión del área, se logró recolectar la información necesaria.

- ✓ **Políticas de control de acceso:** el área de equipos de telecomunicaciones se encuentra explícitamente definido, las puertas que dan acceso al centro de datos son de material resistente y antimotines, el acceso a los diferentes espacios es limitado a través de un sistema automatizado que verifica el nivel de acceso otorgado a cada empleado según su carnet, los cuartos de terceros se encuentran físicamente separados del cuarto de telecomunicaciones de la empresa, no posee salidas de emergencias en los laterales (sólo dispone de una única salida al exterior del edificio para los tres pisos) ni cámaras de seguridad.

Tabla 10 Espacios en el centro de datos La Colina
Fuente: fotografías recolectadas por el autor

| | |
|---|---|
| Puerta exterior que da acceso al cuarto de telecomunicaciones en general (compuesto de tres espacios diferenciados) |  |
| Espacio aún en construcción, separa el cuarto de equipos y el espacio de monitoreo y cuarto de terceros. |  |

| | |
|---|---|
| Cuarto de terceros (puerta marrón) y espacio para equipos y personal de monitoreo. |  |
| Puerta de acceso al cuarto de equipos. A la derecha, indicado por el área en color rojo, se encuentra el sistema de acceso a través de carnet. |  |
| Vista Panorámica del cuarto de equipos del centro de datos La Colina |  |

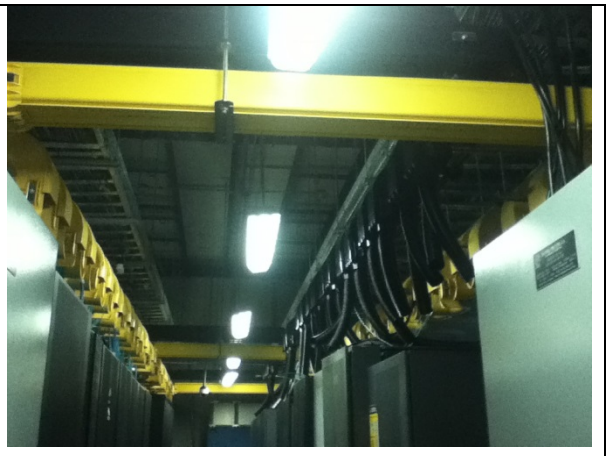
La única salida del cuarto de telecomunicaciones es la puerta principal indicada en la primera fotografía; luego para salir de las instalaciones sólo existen unas escaleras que dan con el exterior del edificio.

- ✓ **Políticas de seguridad de los equipos:** el centro de datos La Colina cuenta con sistemas de enfriamiento de alta potencia y distribución de pasillos fríos y calientes, posee detectores de calor y humo en el cuarto de equipos y extintores de incendio en cada espacio, el cuarto de telecomunicaciones se encuentra en el primer piso del edificio a una elevación considerable de la calle de manera tal de disminuir el riesgo contra inundaciones y daño por agua en los equipos, los cables de potencia están separados de los cables de comunicaciones por medio de canaletas diferentes, además del suministro

eléctrico regular cuenta con sistemas UPS en caso de fallas en la electricidad, todos los racks de equipos se encuentran cerrados con llaves de seguridad.

Tabla 11 Equipos del centro de datos La Colina
Fuente: fotografías recolectadas por el autor

| | |
|---|---|
| Sistema de control de humedad ubicado en las paredes laterales del cuarto de equipos. |  |
| Sistemas de enfriamiento ubicados en las paredes laterales del cuarto de equipos, al lado de los sistemas de control de humedad. |  |
| Tableros eléctricos tipo CCB 454 AB 400. 208/120 Vac, 60 Hz y 25 KA Icc (rms). 3 Fases, 5 Hilos. |  |

| | |
|---|---|
| Cables de comunicaciones y de potencia divididos a través de las canaletas. |  |
| Sistema contra incendio ubicado a la entrada del cuarto de telecomunicaciones. Estos sistemas se encuentran distribuidos en todos los espacios del centro de datos. |  |
| Como se puede observar en la fotografía de la fachada del edificio, el primer piso se encuentra elevado a una altura considerable del piso, evitando posibles daños por agua en los equipos. |  |
| Todos los racks donde se encuentran los equipos se encuentran asegurados con llaves tanto en su parte frontal como posterior. |  |

En cuanto a seguridad de los equipos, el centro de datos La Colina se encuentra en excelentes condiciones y preparado ante cualquier eventualidad. Respecto a las demás políticas de seguridad, que se refieren a actividades preventivas y de mantenimiento, se realizará un resumen en el apartado de recomendaciones.

### 4.3.2 Aspectos de seguridad lógica en el centro de datos La Colina

El centro de datos La Colina no cuenta, en la actualidad, con una plataforma lógica de seguridad, siendo su única protección el firewall perimetral de la red corporativa en general, es por ello que el autor elaboró una propuesta de diseño que pretende satisfacer las necesidades de la empresa y proteger todos los servidores alojados en el centro de datos La Colina.

Esta propuesta contempla tanto la ubicación de los equipos firewalls o cortafuegos dentro de la topología, según recomendaciones y mejores prácticas, como la aplicación de distintas zonas de seguridad, segmentación IP, filtrado de tráfico por el equipo, herramientas de control de acceso, protección contra ataques e intrusiones y finalmente elaboración de políticas de seguridad y recomendaciones.

### 4.3.3 Propuesta de diseño de plataforma de seguridad

El objetivo principal de la propuesta, es diseñar una plataforma que proteja los servidores que actualmente se encuentran en el centro de datos La Colina y elaborar una serie de recomendaciones a seguir a la hora de migrar nuevos servidores y personal de oficina.

En cuanto al equipo encargado de proteger la red interna, la empresa seleccionó dos Firewalls o Cortafuegos marca Juniper, modelo SRX 3600; de acuerdo a las características del mismo se realizará el dimensionamiento de la plataforma, por lo tanto es necesario analizar sus especificaciones técnicas y alcance.

Especificaciones técnicas del equipo Firewall SRX 3600

El chasis del equipo SRX3600 mide 22,2 cm de alto, 44,5 cm de ancho, y 64,8 cm de profundidad (desde la parte frontal a la parte posterior del chasis). Se instala en bastidores estándar de telecomunicaciones de estructura abierta de 800 mm (o mayor) gabinetes cerrados. En su configuración básica el peso total es de 33 Kg, y con todas las tarjetas de red agregadas el peso máximo es de 52.6 Kg.

Se encuentra divido en varios módulos y su expansión depende de los servicios requeridos por el cliente, pueden ser agregados módulos de puertos para tener más conexiones o tarjetas de red de procesamiento para mejor su gestión.

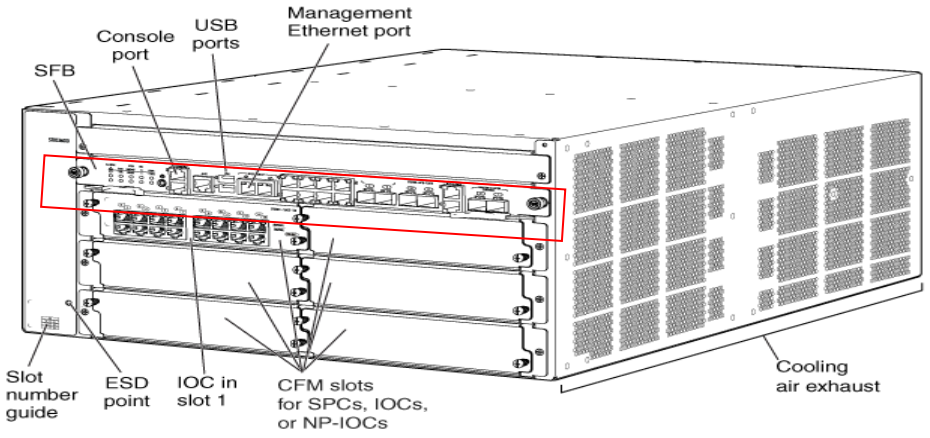



Figura 14 Vista frontal del equipo SRX3600

Fuente: http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/concept/chassis-srx3600.html

El módulo seleccionado en color rojo es llamado SFB por sus siglas en inglés Switch Fabric Board y es el corazón de la arquitectura de servicios dinámicos, su propósito es permitir a todos los módulos enviar tráfico a través de un gran ancho de banda. Está compuesto por dos (2) puertos de consola, uno (1) auxiliar, dos (2) puertos USB, dos (2) puertos de gestión Ethernet, ocho (8) puertos de cobre Gigabit Ethernet con velocidades de transmisión de datos entre 10/100/1000 Mbps y conexión con cables RJ-45, cuatro (4) puertos de fibra Gigabit Ethernet y conexión con transceptores SFP y XFP, dos (2) puertos de sincronismo y dos (2) puertos de control chasis clúster que proporcionan redundancia de red al agrupar dos dispositivos de la misma clase. En el lateral derecho se encuentra una serie de ranuras de ventilación. Los módulos debajo de la tarjeta SFB principal, van enumerados del Slot 1 al Slot 6 y pueden ser sustituidos por tarjetas de red de tipo SPC, IOC o NP-IOC, en el primer Slot fue agregada una tarjeta IOC como ejemplo.

Las tarjetas SPC o Service Processing Card, son consideradas el cerebro del sistema y se encargan de procesar todos los servicios disponibles en el equipo; El módulo NPC o Network Processing Card distribuye todo el tráfico de entrada y salida hacia las tarjetas SPCc y IOCs para garantizar el máximo rendimiento de procesamiento y flexibilidad, además aplica calidad de servicio e impone protecciones contra ataques de denegación de servicio, para que el sistema funcione apropiadamente se requiere un mínimo de una (1) tarjeta NPC y una (1) tarjeta SPC. El módulo IOC por sus siglas en inglés Input/Output card equipa al sistema con un conjunto de puertos ya sea de cobre o fibra óptica, generalmente incluye 16 interfaces Gigabit Ethernet (conexiones de cobre o fibra) o 20 interfaces Gigabit Ethernet (2 x 10 puertos XFP Gigabit Ethernet). Asimismo, la tarjeta NP-IOC es una fusión de los módulos IOC y NPC, sin embargo está dimensionada para aplicaciones de baja latencia, su característica relevante radica en el hecho de que todo el tráfico es gestionado por ella misma y no necesita del procesamiento de la tarjeta NPC. En los módulos de la parte frontal sólo pueden agregarse tarjetas de tipo SPC, IOC o NP-IOC.

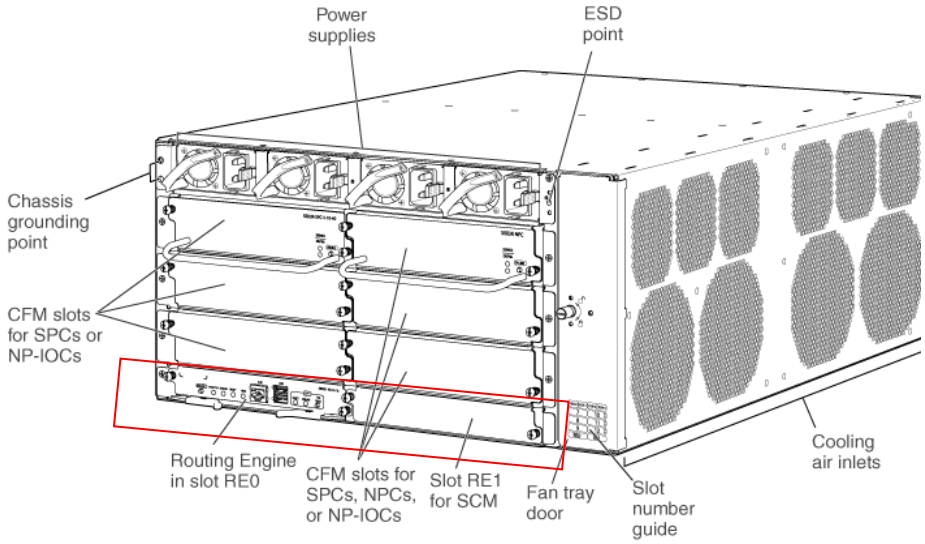



Figura 15 Vista posterior del equipo SRX3600

Fuente: http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/concept/chassis-srx3600.html

En la parte posterior del equipo, se ubican cuatro (4) módulos de alimentación eléctrica para garantizar alta redundancia en el suministro, pueden ser AC o DC de acuerdo a las facilidades de la empresa, también se detallan cuatro módulos para tarjetas de red de tipo SPC o NP-IOC en los Slots 7 al 9 y tarjetas SPC, NPC o NP-IOC de los Slots 10 al 12. El área seleccionada en color rojo es destinada para la ubicación de las tarjetas Route Engine (RE), mejor conocida como el sistema nervioso central de la arquitectura, es el plano de control del chasis, proporciona una gestión global y comunicación desde y para los administradores de sistemas, así como calcula las tablas de enrutamiento del tráfico de red. A la derecha de los módulos de tarjetas de red se encuentra la bandeja de ventilación (fan tray) y en el lateral derecho del equipo la entrada de ventilación de aire frío. En la siguiente tabla se muestran las características generales del equipo.

Tabla 12 Descripción general del SRX3600

Fuente: http://www.juniper.net/us/en/products-services/security/srx-series/srx3600/#specs

Consulta: 18/02/2013

| | |
|---|---|
| Versión de software Junos | Junos 12.1X44 |
| Rendimiento máximo del equipo | 55 Gbps |
| Rendimiento VPN | 15 Gbps |
| Máximo de sesiones simultaneas | 2,25 / 6 millones |
| Nuevas sesiones / segundo | 270.000 |
| Máximo de políticas de seguridad | 40.000 |
| Máximo de usuarios soportados | Sin restricciones |
| Máximo de ranuras disponibles para IOC | 6 |
| Máximo de ranuras disponibles para NP-IOC | 11 |
| Máximo de ranuras disponibles para NPC | 3 |
| Máximo de ranuras disponibles para SPC | 7 |
| Opciones de interfaz LAN | 16x1/10/100/1000 Mbps conector RJ-45. 16x1 Gigabit Ethernet conector SFP. 2x10 Gigabit Ethernet conector XFP. |
| Soporte de alta disponibilidad | Activo / Activo ; Activo / Pasivo a través de Chassis Cluster |
| Dimensión (LxAxP) | 44,5 x 22,2 x 64,8 cm |
| Peso | Chasis: 19,8 Kg, configuración completa: 52,6 Kg |
| Fuente de alimentación (AC) | 100 a 240 Vac |
| Consumo de energía máxima | 1750W (AC) |
| Detección de ataques de red | Sí |
| Protección DoS y DDoS | Sí |
| Protección para la fragmentación de paquetes TCP | Sí |
| Ataque de mitigación de fuerza bruta | Sí |
| Protección cokie SYN | Sí |
| Zonas basadas en Spoofing IP | Sí |

| | |
|---|---|
| Protección de paquetes con formato incorrecto | Sí |
| Inspección de estado GPRS | Sí |
| Protocolo con estado de firmas | Sí |
| Mecanismos de detección de ataques | Sí |
| Inspección de tráfico SSL encriptado | Sí |
| Protección contra troyanos | Sí |
| Protección contra Spyware | Sí |
| Otra protección contra malware | Sí |
| Número aproximado de ataques cubiertos | 6000 |
| Protección de reconocimiento | Sí |

Una vez caracterizado el equipo de gestión y protección, el siguiente paso constituye la organización de las zonas de seguridad para la protección de todos los servidores en producción.

Organización de zonas en el centro de datos La Colina

En base al requerimiento de la empresa, fundamentado en la protección de los servidores ubicados en el centro de datos, cada uno de ellos fue agrupado en tres zonas bien diferenciadas: Trust, Untrust y Middleware.

La zona trust estará compuesta por servidores de bases de datos, servidores de aplicaciones como TM-ART, Remedy, SAP, Factura Digital entre otras, equipos con servicios de monitoreo y control como la herramienta Patrol y servidores de gestión. Cada uno de ellos será supervisado por el departamento encargado, pertenecerán a un segmento IP (con su VLAN asociada) y necesitarán la activación de los puertos y protocolos asociados a cada uno de ellos; toda esta información fue recolectada con varias coordinaciones de la empresa y puede apreciarse un resumen en la siguiente tabla, que muestra los servidores que actualmente se encuentra alojados en el centro de datos La Colina:

Tabla 13 Descripción Zona TRUST

Servidores ubicados actualmente en el centro de datos

| **ZONA TRUST** | | | | | |
|---|---|---|---|---|---|
| **Nombre de VLAN** | **Nro. VLAN** | **Segmento IP** | **Puertos de aplicaciones** | **Protocolo** | **Dpto. Encargado** |
| Monitoreo_Control | 2 | 10.192.1.0/24 | Desde el 1024 al 65535 | TCP/UDP | Monitoreo y Control-App |
| Almacenamiento | 3 | 10.192.2.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| Bck_Monitoreo_Control | 4 | 10.192.3.0/24 | Desde 1520 al 1530; 3181, 2059, 1828 | TCP/UDP | Base de datos |
| Back_Almacenamiento | 5 | 10.192.4.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| Gestion_Servicios | 7 | 10.192.6.0/24 | 53, 25 y desde 1520 al 1530 | TCP/UDP | Gestión de Servicios |
| Otras_BD_Producción | 8 | 10.192.7.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| Bck_Otras_BD_Produc | 9 | 10.192.8.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| Cluster_BDUC_Produc | 11 | 10.192.10.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| PlatSap | 13 | 10.192.12.0/24 | Desde el 1024 al 65535 | TCP/UDP | SAP |
| Dev_Enviro | 14 | 10.192.13.0/24 | Desde el 1024 al 65535 | TCP/UDP | Enviro |
| PlatAprov | 15 | 10.192.14.0/24 | Desde el 1024 al 65535 | TCP/UDP | Aprovisionamiento |
| Previsión_Control | 19 | 10.192.18.0/24 | Desde el 1024 al 65535 | TCP/UDP | Monitoreo y Control |
| Bck_PlatProv | 20 | 10.192.19.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| Bck_PlatSap | 21 | 10.192.20.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| ATCMV_Prod | 23 | 10.192.22.0/24 | Desde el 1024 al 65535 | TCP/UDP | ATCMV |
| Bck_ATCMV_Prod | 24 | 10.192.23.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |

Esta información será utilizada a la hora de elaborar las políticas de seguridad en el cortafuego o firewall, debido a que el tráfico será filtrado a través de segmentos IP, VLAN, puertos y protocolos. Esta zona no tendrá acceso, bajo ninguna circunstancia a la zona Untrust, las peticiones enviadas a esta última serán redirigidas a la zona Middleware, quien se encargará de buscar la información pertinente y dar una respuesta.

Asimismo, la zona Middleware contiene servidores de aplicaciones Web, servicios y bases de datos. La mayoría de las consultadas realizadas a éstos equipos son producto de aplicaciones web que pasan a través de un gestor llamado BlueCoat y son redirigidas a dos balanceadores de carga llamados F5 que se encargan de distribuir las peticiones bajo la premisa Round Robin (se reparten peticiones a todos los servidores por igual).

Tabla 14 Descripción Zona Middleware

Servidores ubicados actualmente en el centro de datos

| ZONA MIDDLEWARE | | | | | |
|---|---|---|---|---|---|
| **Nombre de VLAN** | **Nro. VLAN** | **Segmento IP** | **Puertos de aplicaciones** | **Protocolo** | **Dpto. Encargado** |
| Middle_Prod_Trust | 368 | 10.192.230.0/24 | Desde el 1024 al 65535 | TCP/UDP | Servicios y Aplicaciones |
| Back_Middle_Prod_Trust | 369 | 10.192.231.0/24 | Desde el 1024 al 65535 | TCP/UDP | Servicios y Aplicaciones |

El departamento encargado de la gestión de esta zona, informó que a razón de que constantemente se crean aplicativos de gestión (para comunicación entre dos o varias aplicaciones) y se migran nuevos servicios, la selección de puertos representa una problemática, debido a que constantemente se necesitaría habilitar nuevos puertos y el protocolo para la aprobación de esta petición demoraría cierta cantidad de tiempo, lo que retrasaría el trabajo del departamento y produciría un aspecto negativo para el área de creatividad y desarrollo. En consecuencia, el autor plantea realizar el filtrado de puertos (desde el 7000 hasta el 8000 para HTTP y desde el 9000 hasta el 10000 para HTTPs) sólo para las peticiones provenientes del mundo exterior (Internet); para las solicitudes y gestiones dentro de la empresa no existiría filtrado en cuanto a puertos, sólo a direcciones IP. Es importante aclarar que, esta zona también actuará como intermediario entre la plataforma Trust y Untrust a razón de que ellas no tendrán permiso de acceder una a la otra en ningún sentido, por lo tanto las peticiones de esta índole serán gestionadas por la zona Middleware.

Finalmente, la zona Untrust estará constituida por servidores de bases de datos, servidores de correo electrónico y DNS, equipos gestionados por el departamento de seguridad y servidores de aplicaciones como AUTANA y Recargas Electrónicas. El resumen puede ser observado en la siguiente tabla.

Tabla 15 Descripción Zona Untrust

Servidores ubicados actualmente en el centro de datos

| ZONA UNTRUST | | | | | |
|---|---|---|---|---|---|
| **Nombre de VLAN** | **Nro. VLAN** | **Segmento IP** | **Puertos de aplicaciones** | **Protocolo** | **Dpto. Encargado** |
| Monitoreo_Control | 110 | 10.192.109.0/24 | 19121, 19122, 19124 hasta 19126 | TCP/UDP | Monitoreo y control – App. |
| Almacenamiento | 111 | 10.192.110.0/24 | Desde 1520 al 1530 | TCP/UDP | Base de datos |
| Microsoft_Prod | 112 | 10.192.111.0/24 | Desde el 1024 al 65535 | TCP/UDP | Microsoft |
| Umarket1_Prod | 114 | 10.192.113.0/24 | Desde el 1024 al 65535 | TCP/UDP | Recargas Electronicas |
| Umarket2_Prod | 115 | 10.192.114.0/24 | Desde el 1024 al 65536 | TCP/UDP | Recargas Electronicas |
| Umarket3_Prod | 116 | 10.192.115.0/24 | Desde el 1024 al 65536 | TCP/UDP | Recargas Electronicas |
| Umarket4_Prod | 117 | 10.192.116.0/24 | Desde el 1024 al 65536 | TCP/UDP | Recargas Electronicas |
| Prevención_Control | 121 | 10.192.120.0/24 | Desde el 1024 al 65536 | TCP/UDP | Seguridad |
| Servicios_Plat_Microsoft | 122 | 10.192.121.0/24 | 25,135, 88, 53, 135, 389, 50636 (sólo TCP), 80(solo TCP), 443 (Solo TCP) | TCP/UDP | Microsoft |
| Servicios_Plat_Correo | 124 | 10.192.123.0/24 | 25 y 587 | TCP | Microsoft |
| Ambiente_desarrollo_virtual | 128 | 10.192.127.0/24 | Desde el 1024 al 65536 | TCP/UDP | Desarrollo Virtual |
| Laboratorio | 140 | 10.192.139.0/24 | Desde el 1024 al 65536 | TCP/UDP | Microsoft |
| Serv_Agent_Aut_produccion | 142 | 10.192.141.0/24 | 25, 587, 80, desde 1520 a 1530 | TCP/UDP | Autana |

La mayoría de los servicios brindados en esta plataforma serán de correo electrónico y DNS. Esta zona no podrá acceder bajo, ninguna circunstancia a la zona Trust, y las peticiones que hacía ella realice serán en primera instancia verificadas minuciosamente frente a los controles de seguridad y luego re direccionadas a la zona Middleware que se encargará de buscar la información solicitada y arrojar una respuesta pertinente.

Asimismo, el autor propone la creación de una cuarta zona llamada Externa que se encontrará definida por el mundo exterior fuera del centro de datos pero dentro de la empresa, es decir por todos aquellos segmentos IP de todos los departamentos de la corporación. El objetivo de la creación de ésta zona es básicamente, facilitar la implementación de las políticas de seguridad cuando llegue una petición externa al centro de datos.

Por otra parte, continuando con las recomendaciones y mejores prácticas, y en función de la organización de zonas en el centro de datos, el autor plantea que se realice una separación física de servidores de cada plataforma, ubicando por ejemplo los equipos de la zona trust en la fila A de racks (Figura 4.1.6), los pertenecientes a la zona middleware en la fila B de racks y los servidores de la zona untrust en la fila C de racks, asimismo, la ubicación del equipo cortafuego o firewall debería realizarse siguiendo la topología jerárquica del centro de datos y de la red corporativa en general.

Como se indicó en apartados anteriores, el router de borde del centro de datos La colina formará un anillo junto con los routers de los demás centros de datos, cuando un paquete con una IP perteneciente al segmento de su red LAN transite por ese anillo, el router se encargará de direccionarlo al equipo al que va dirigida la petición dentro de su red, en la actualidad este direccionamiento va directamente al Switch EX8208 quien se encarga de enviar el paquete a la VLAN respectiva. En vista de este comportamiento la mejor ubicación del cortafuego o firewall sería entre el Router de borde y el Swicht EX8208, de manera tal de ahorrar procesamiento en éste último si la petición no cumple con los requerimientos de seguridad.

Los dos equipos cortafuegos adquiridos por la empresa trabajarían en modo Activo / Pasivo, en caso de alguna eventualidad o avería en el equipo principal, el segundo asumiría todo el tráfico y por lo tanto se aseguraría la continuidad del servicio. En la siguiente imagen se puede apreciar la topología final luego de la incorporación del cortafuego o firewall a la red.

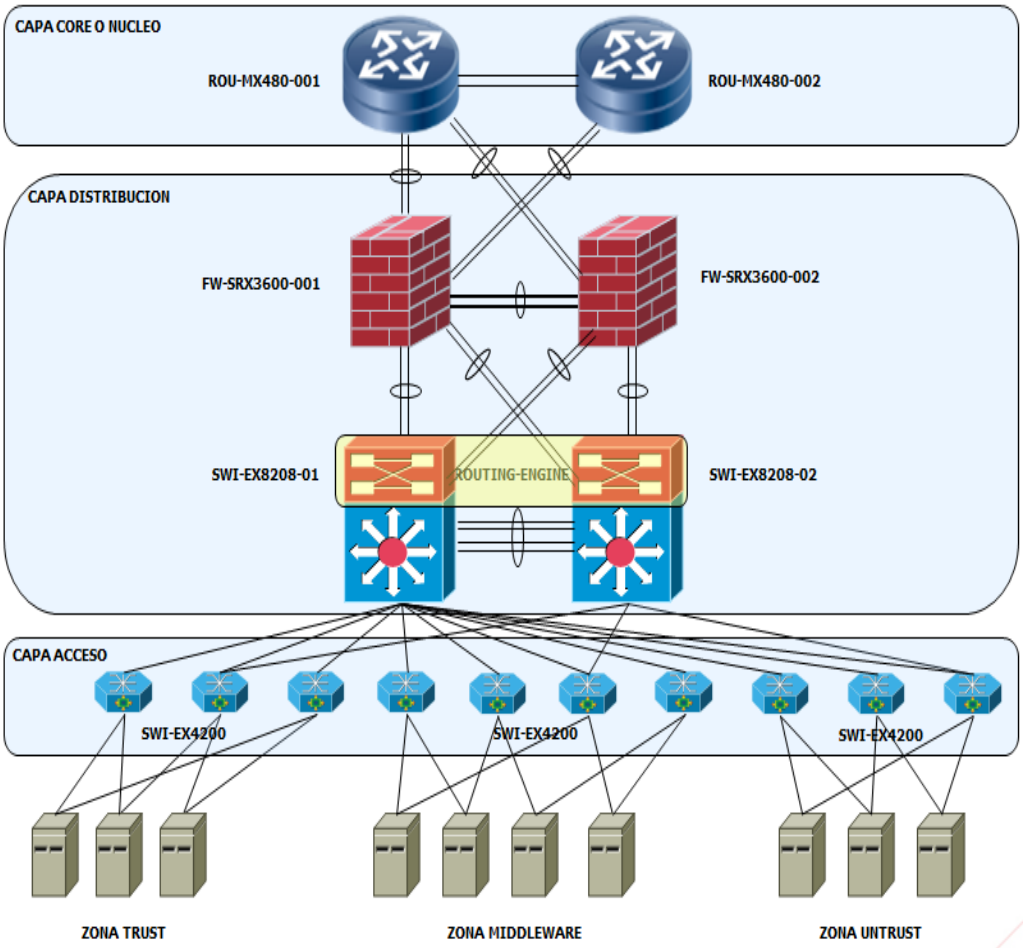



Figura 16 Topología propuesta con equipo cortafuego incorporado en La Colina

Como puede observarse en la imagen anterior, se deberían establecer diversos enlaces de redundancia y de gestión interna entre los equipos, se recomienda la agregación de tarjetas SPC y NPC en su mayoría, de manera de llevar la capacidad de procesamiento del equipo a un nivel de excelencia, sin menospreciar la capacidad de puertos necesarios para realizar todas las interconexiones.

De acuerdo a las observaciones indicadas en este apartado, el autor elaboró una serie de políticas que constituirán el alma de la plataforma de seguridad del

centro de datos La Colina y que deberán ser implementadas para el buen funcionamiento de la plataforma.

Políticas de seguridad

**Política 1. Ubicación del Cortafuego o Firewall**

Comentario: el equipo de protección será ubicado en la capa de distribución de la red LAN del centro de datos La Colina, como se puede apreciar en la figura 16, entre el Router MX480 y el Switch EX8208, de manera de filtrar las peticiones realizadas al router y reducir procesamiento en el switch.

**Política 2. Ubicación de servidores en el centro de datos La Colina**

Comentario: cada grupo de servidores será ubicado en una fila de racks diferente de acuerdo a la zona a la que pertenezcan, los pertenecientes a la zona Trust en la fila A, los pertenecientes a la zona Middleware en la fila B y los que pertenezcan a la zona Untrust en la fila C.

**Política 3. Declaración de zonas en Cortafuego o Firewall**

Comentario: Cada zona de seguridad será declarada en el equipo de protección como TRUST, UNTRUST y MIDDLEWARE. La zona trust tendrá asignado el segmento de red que iría desde la IP 10.192.0.1/24 hasta la 10.192.107.1/24 y VLAN desde la 1 hasta la 108. La zona untrust tendrá asignado el segmento de red que irá desde la IP 10.192.108.1/24 hasta la 10.192.215.1/24 y VLAN desde la 109 a la 216. La zona middleware se le asignará el segmento de red que irá desde la IP 10.192.228.1/24 hasta la 10.192.251/24 y VLAN desde la 266 hasta la 395. Finalmente, la zona Externa estará constituida por todo el segmento IP perteneciente a la corporación 10.21.0.0/16.

Nota: el segmento IP 10.192.220.1/22 perteneciente a la plataforma Trust y el segmento 10.192.224.1/22 perteneciente a la plataforma Untrust no son declarados en el equipo de protección hasta que la empresa defina el uso de esas IP.

**Política 4. Gestión o Management**

Comentario: Se definirá un segmento de red en el equipo de protección destinado únicamente a gestión y monitoreo, su direccionamiento IP será 10.192.216.1/22 y VLAN 216. Cada zona de seguridad tendrá una dirección IP destinada a un servidor de gestión o management, cada uno de ellos se comunicará con el servidor central de monitoreo que será ubicado en la VLAN 216 y se encargará de verificar que los servicios de cada zona funcionen correctamente, en caso contrario deberá notificarlo.

**Política 5. Acceso de administradores por departamento**

Comentario: cada zona permitirá el acceso vía remota al administrador del departamento encargado del segmento, es decir, por cada VLAN se permitirá el acceso desde la IP de un administrador en particular. Por lo tanto, en cada segmento de red se debe declarar qué IP tiene acceso vía remota y qué nivel de gestión posee (sólo lectura, monitoreo o modificación).

**Política 6**. **Acceso a la Zona Trust**

Comentario: el tráfico proveniente de la zona untrust no será permitido bajo ninguna circunstancia hacía esta zona. Todas las peticiones hacía esta zona serán reguladas de acuerdo al segmento IP al que se dirijan, debido a que cada VLAN tendrá permisos diferentes en cuanto a puertos de aplicación, es decir, en referencia a la tabla 13, un paquete que se dirija a la VLAN número 8 sólo será escuchado por los puertos 1520 hasta 1530 (UDP7TCP), si la petición no es de ésta índole, el paquete será rechazado, así sucederá con los demás segmentos. Dentro de la red interna del centro de datos, sólo la zona middleware tendrá permiso de acceso hacía la zona trust, respetando las reglas de direccionamiento antes planteadas, es decir, el tráfico proveniente de cualquier otro segmento IP será redirigido a la zona middleware y ella se encargará de gestionar la petición. El tráfico proveniente de la red externa al centro de datos, que se dirija a la zona trust, deberá respetar las reglas de direccionamiento y puertos de aplicación, en caso de cumplirlas tendrá acceso directo a la zona trust, en caso contrario el

paquete será rechazado. Una vez establecida la conexión y comprobados los requerimientos de seguridad, no se realizará nuevamente la revisión en cuanto a cumplimiento de reglas sino que se permitirá el tráfico hasta que la sesión finalice, con el objetivo de ahorrar procesamiento al cortafuego.

**Política 7. Acceso a la Zona Untrust**

Comentario: el tráfico proveniente de la zona trust no será permitido hacía esta zona. Todas las peticiones hacía la zona untrust serán reguladas de acuerdo al segmento IP al que se dirijan, debido a que cada VLAN tendrá permisos diferentes en cuanto a puertos de aplicación (al igual que en el caso de la zona trust), es decir, en referencia a la tabla 15, un paquete que se dirija a la VLAN número 124 sólo será escuchado por los puertos 25 y 587 (TCP), si la petición no es de ésta índole, el paquete será rechazado, así sucederá con los demás segmentos. Asimismo, dentro de la red interna del centro de datos, sólo la zona middleware tendrá permiso de acceso hacía la zona untrust, respetando las reglas de direccionamiento antes planteadas, por lo tanto, un paquete proveniente de cualquier otro segmento de red será re direccionado a la zona middleware. El tráfico proveniente de la zona externa al centro de datos, que se dirija a la zona untrust, deberá respetar las reglas de direccionamiento y puertos de aplicación, en caso de cumplirlas tendrá acceso directo a la zona untrust, en caso contrario el paquete será rechazado. Una vez establecida la conexión y comprobados los requerimientos de seguridad, no se realizará nuevamente la revisión en cuanto a cumplimiento de reglas sino que se permitirá el tráfico hasta que la sesión finalice.

**Política 8. Acceso a la Zona Middleware**

Comentario: cuando exista una petición de la zona trust a la untrust o viceversa, el paquete será re direccionado a la plataforma middleware y ella será la que se encargará de buscar la información en cada zona (porque será la única con permiso de acceso en ambas zonas), y de devolver una respuesta, funcionará muy parecido a un proxy para ambas plataformas. Cuando exista una petición de los servidores de gestión o management, también será la zona middleware la que se encargará de buscar la información pertinente y dar una respuesta. En cuanto al

tráfico y peticiones de la red externa al centro de datos, se realizarán dos divisiones: a) Peticiones provenientes de la IP del bluecoat, se permitirán sólo los paquetes cuyo destino sea algún segmento IP de la zona middleware y serán escuchados sólo por los puertos desde el 7000 al 8000 para HTTP y desde el 9000 al 10000 para HTTPs; b) Peticiones provenientes de segmentos IP del departamento de sistemas, en vista de la constante innovación y creación en cuanto a aplicaciones de gestión para la plataforma middleware, no se limitará ningún puerto de aplicación para el tráfico proveniente de éste segmento, sólo se verificará que la IP origen pertenezca al departamento de sistemas y que se dirija a una IP de la zona middleware. Una vez establecida la conexión y comprobados los requerimientos de seguridad, no se realizará nuevamente la revisión en cuanto a cumplimiento de reglas sino que se permitirá el tráfico hasta que la sesión finalice. Finalmente, cuando la zona middleware necesite acceder a algún servicio de las plataformas trust y untrust, se realizará la verificación en cuanto al cumplimiento de las políticas y reglas de cada zona y se permitirá el acceso.

**Politica 9. Todo lo que no sea explícitamente permitido, será rechazado.**

**Política 10. Tarjetas modulares del cortafuego**

Comentario: se deberán adquirir tarjetas del tipo SPC y NPC para aumentar el procesamiento del equipo de seguridad.

**Política 11. Prevención y detección de ataques**

Comentario: el equipo de protección debe contar con mecanismos de prevención y detección de ataques.

**Política 12. Prevención y detección de intrusiones**

Comentario: el equipo de protección debe contar con mecanismos de prevención y detección de intrusiones.

## 4.4 Documentación del proceso de implementación de las políticas de seguridad

El proceso de implementación de las políticas de seguridad debería darse en el correcto orden en el que fueron presentadas, debido a que las políticas desorganizadas pueden opacar el efecto de unas sobre otras. A continuación se presenta, cronológicamente, la forma en la cual debería llevarse a cabo el proceso de implementación de cada política.

### 4.4.1 Implementación de Política 1

Una vez seleccionada la ubicación lógica del equipo de protección, se debe identificar su ubicación física en los racks donde estarán todos los equipos de la topología, la cual debe tomar en cuenta las conexiones físicas que necesita el equipo contra el Router MX480 y el Swicht 8208. Para satisfacer la premisa de alta redundancia, se propone implementar dos conexiones con cada Router (una conexión para el pasivo y otra para el activo) y dos conexiones con cada switch (una conexión para el pasivo y otra para el activo), además de las conexiones entre los dos cortafuegos (realizadas a través de los puertos 0 y 1 dedicados para tal fin y llamados Control Chassis Cluster). Para las conexiones contra los switchs se propone utilizar los cuatro puertos ópticos de la tarjeta SFP (ge-0/0/8 al ge0/0/11) que soportarán el constante tráfico manejado a través de ellos. Para las conexiones contra los routers se propone utilizar cuatro de los ocho puertos de cobre (ge-0/0/0 hasta ge-0/0/3) con conectores RJ-45 de 1Gbps de capacidad.

### 4.4.2 Implementación de Política 2

La ubicación de los servidores de cada zona debería distribuirse a lo largo de los racks y de acuerdo a las filas mencionadas en la política. A: zona Trust, B:

zona middleware y C: zona untrust. En la siguiente imagen se selecciona en color rojo la ubicación de cada zona según el plano del centro de datos.

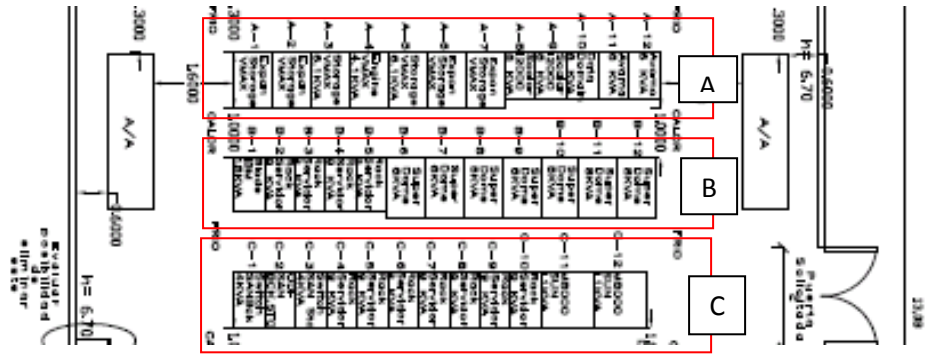



Figura 17 Distribución de servidores en el centro de datos La Colina

Fuente: Departamento de redes de Corporación Digitel

### 4.4.3 Implementación de Política 3

Para realizar la declaración de zonas en el cortafuego o firewall se recomienda la utilización de la guía *Junos Software, Security Configuration Guide* elaborada por la empresa Juniper y que detalla cada paso en la declaración e implementación de zonas y políticas de seguridad. A continuación, el autor expone un ejemplo de implementación para la declaración de las diferentes zonas de seguridad:

a) Primer paso: se declara la interfaz por la cual transitará el tráfico de todo el segmento de red.

*user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.21.0.0/16*
*user@host#set interfaces ge-0/0/8 unit 0 family inet address 10.192.0.0/24*

La primera interfaz corresponde con una de las conexiones hacia el Router MX480 con su respectivo segmento de red externo, la segunda interfaz

corresponde con una de las conexiones hacia el cortafuego o firewall y su segmento de la red interna completo. Se recomienda que se declaren todas las interfaces disponibles de manera de cumplir con la premisa de redundancia y balancear el tráfico.

b) Segundo paso: se declaran las zonas asociadas a cada interfaz

*user@host# set security zones security-zone **Externa** interfaces ge-0/0/0.0*
*user@host# set security zones security-zone **Trust** interfaces ge-0/0/8.1*
*user@host# set security zones security-zone **Middleware** interfaces ge-0/0/8.2*
*user@host# set security zones security-zone **Untrust** interfaces ge-0/0/8.3*

La interfaz de la red interna, declarada en el primer paso, será dividida en tres (3) sub interfaces para realizar la separación de cada zona.

c) Tercer paso: se configuran los segmentos IP de acuerdo a las zonas

*user@host# set security zones security-zone **Externa** address-book address **Red_Ext 10.21.0.12/16***

El primer segmento declarado será el de la zona Externa y se corresponderá con la piscina de direcciones IP asignada a la coordinación de redes de la empresa. Los demás segmentos serán divididos de acuerdo a la zona interna a la que pertenezcan.

Zona Trust

*user@host# set security zones security-zone **Trust** address-book address **Monitoreo_Control_trust 10.192.1.0/24***
*user@host# set security zones security-zone **Trust** address-book address **Almacenamiento_trust 10.192.2.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Bck_Monitoreo_Control 10.192.3.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Bck_Almacenamiento 10.192.4.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Gestion_Servicios 10.192.6.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Otras_BD_Produc 10.192.7.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Bck_Otras_BD_Produc 10.192.8.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Cluster_BDUC_Produc 10.192.10.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Plat_Sap 10.192.12.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Dev_Enviro 10.192.13.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Plat_Aprov 10.192.14.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Previsión_Control 10.192.18.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Bck_Plat_Prov 10.192.19.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Bck_Plat_Sap 10.192.20.0/24***

*user@host# set security zones security-zone **Trust** address-book address **ATCMV_Prod 10.192.22.0/24***

*user@host# set security zones security-zone **Trust** address-book address **Bck_ATCMV_Prod 10.192.22.0/24***

## Zona Middleware

*user@host# set security zones security-zone **Middleware** address-book address **Middle_Prod_Trust 10.192.230.0/24***

*user@host# set security zones security-zone **Middleware** address-book address **Bck_Middle_Prod_Trust 10.192.231.0/24***

Zona Untrust

*user@host# set security zones security-zone **Untrust** address-book address **Monitoreo_Control_Unt 10.192.109.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Almacenamiento_Unt 10.192.110.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Microsoft_Prod 10.192.111.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Unmarket1_Prod 10.192.113.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Unmarket2_Prod 10.192.114.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Unmarket3_Prod 10.192.115.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Unmarket4_Prod 10.192.116.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Prevención_Control 10.192.120.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Servicios_Plat_Microsoft 10.192.121.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Servicios_Plat_Correo 10.192.123.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Ambiente_desarrollo_virtual 10.192.127.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Laboratorio 10.192.139.0/24***

*user@host# set security zones security-zone **Untrust** address-book address **Serv_Agent_Aut_prod 10.192.141.0/24***

### 4.4.4 Implementación de Política 4

El servidor central de management será ubicado en el segmento IP 10.192.216.1/24, tendrá comunicación únicamente con los servidores de gestión de cada instancia o zona de seguridad y se permitir únicamente tráfico de gestión y monitoreo.

### 4.4.5 Implementación de Política 5

Esta política establece que el administrador de cada departamento tendrá acceso para monitorear y gestionar sus equipos, por lo tanto se debe identificar la IP del administrador de cada instancia y permitir tráfico desde una dirección de red particular y hacía otra muy específica.

a) Primer paso: se declara la interfaz asociadas a la red externa

*user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.21.0.0/30*

b) Segundo paso: se declara la zona asociada a la interfaz.

*user@host# set security zones security-zone **Externa** interfaces ge-0/0/0.0*

c) Tercer paso: se configuran los segmentos IP que dividirán a la zona. Se desarrollará el ejemplo en base a permisos sólo para tres administradores: administrador de Base de Datos zona Trust (segmento IP de Almacenamiento), administrador de Servicios y aplicaciones zona Middleware (segmento IP de Middle_ProduTtrust) y administrador de Microsoft zona Untrust (segmento IP de Microsoft_Prod), en la siguiente tabla se puede ver el detalle de cada uno.

Tabla 16 Ejemplo con administradores de red de cada zona

| Zona | Nombre de VLAN | N° VLAN | Segmento IP | Dpto. Encargado |
|---|---|---|---|---|
| TRUST | Almacenamiento | 3 | 10.192.2.0/24 | Base de Datos |
| MIDDLEWARE | Middle_Prod_Trust | 368 | 10.192.230.0/24 | Servicios y Aplicaciones |
| UNTRUST | Microsoft_Prod | 112 | 10.192.111.0/24 | Microsoft |

*user@host# set security zones security-zone **Externa** address-book address **Admin_BD_Trust 10.21.0.0/30***

*user@host# set security zones security-zone **Externa** address-book address **Admin_Serv_Apli_Midlleware 10.21.0.4/30***

*user@host# set security zones security-zone **Externa** address-book address **Admin_Microsoft_Untrust 10.21.0.8/30***

*user@host# set security zones security-zone **Externa** address-book address **Red_Ext 10.21.0.12/16***

d) Cuarto paso: se crean las políticas de permisos para cada zona

*user@host# set security policies from-zone **Externa** to-zone **Trust** Admin_BD_Trust Almacenamiento_Trust SSH permit*

*user@host# set security policies from-zone **Externa** to-zone **Trust** Admin_BD_Trust Almacenamiento_Trust Telnet permit*

*user@host# set security policies from-zone **Externa** to-zone **Middleware** Admin_Serv_Apli_Middleware Middle_Prod_Trust SSH permit*

*user@host# set security policies from-zone **Externa** to-zone **Middleware** Admin_Serv_Apli_Middleware Middle_Prod_Trust Telnet permit*

*user@host# set security policies from-zone **Externa** to-zone **Untrust** Admin_Microsoft_Untrust Microsoft_Prod SSH permit*

*user@host# set security policies from-zone **Externa** to-zone **Untrust** Admin_Microsoft_Untrust Microsoft_Prod Telnet permit*

De esta manera, los permisos para los administradores de cada departamento pueden ser otorgados.

### 4.5.6 Implementación de Política 6

La política seis, hace referencia a todas las reglas de acceso hacía la zona trust. A continuación, se describirán los paso que se deberían seguir a la hora de implementar la política y permisos.

a) Primer paso: se creará un set de aplicaciones, que no es otra cosa que agrupar un gran número de puertos de aplicaciones bajo un mismo nombre. Esto ahorrará gestión a la hora de regular el tráfico por puertos de aplicaciones.

*user@host# set applications application-set **Base_Datos** application 1520*
*user@host# set applications application-set **Base_Datos** application 1521*

Hasta llegar al puerto 1530 que conformaría el set de aplicaciones llamado Base de datos. El siguiente set de aplicaciones es llamado Backup Base de Datos.

*user@host# set applications application-set **Bck_Base_Datos** application 3181*
*user@host# set applications application-set **Bkc_Base_Datos** application 2059*
*user@host# set applications application-set **Bkc_Base_Datos** application 1828*
*user@host# set applications application-set **Bck_Base_Datos** application 1520*
*user@host# set applications application-set **Bck_Base_Datos** application 1521*
*user@host# set applications application-set **Bck_Base_Datos** application 1522*
*user@host# set applications application-set **Bck_Base_Datos** application 1523*
*user@host# set applications application-set **Bck_Base_Datos** application 1524*
*user@host# set applications application-set **Bck_Base_Datos** application 1525*
*user@host# set applications application-set **Bck_Base_Datos** application 1526*
*user@host# set applications application-set **Bck_Base_Datos** application 1527*
*user@host# set applications application-set **Bck_Base_Datos** application 1528*
*user@host# set applications application-set **Bck_Base_Datos** application 1529*
*user@host# set applications application-set **Bck_Base_Datos** application 1530*

De esta manera puede agruparse un conjunto de puertos de aplicaciones que se quieran aplicar posteriormente a una regla o política de seguridad.

b) Segundo paso: estará constituido por la implementación de las políticas de regulación de tráfico de la zona Externa a la zona Trust. De acuerdo al segmento de red al que la zona externa desee ir, diferentes puertos de aplicación serán permitidos o no; se realizarán tres ejemplos, uno con el

control de puertos del set de aplicaciones Base de Datos, otro con el set de aplicaciones Backup Base de Datos y otro sin ninguna restricción en cuanto a puertos de aplicación.

*user@host# set security policies from-zone **externa** to-zone **trust** Red_Ext Almacenamiento_trust **Base_Datos** permit*
*user@host# set security policies from-zone **externa** to-zone **trust** Red_Ext Back_Monitoreo_Control **Bck_Base_Datos** permit*
*user@host# set security policies from-zone **externa** to-zone **trust** Red_Ext Plat_Sap any permit*

c) Tercer paso: estará constituido por la implementación de las políticas de regulación de tráfico de la zona Middleware a la zona Trust. Se plantearán dos ejemplos, uno respecto al tráfico desde cualquier segmento de la zona Middleware al segmento Monitoreo_Control_Trust de la zona Trust, y otro desde cualquier segmento de la zona Middleware hacía el segmento Almacenamiento_Trust de la zona Trust; este procedimiento deberá aplicarse con todos los segmentos de la plataforma Trust.

*user@host# set security policies from-zone **Middleware** to-zone **Trust** any Monitoreo_Control_Trust any permit*
*user@host# set security policies from-zone **Middleware** to-zone **Trust** any Almacenamiento_Trust Base_Datos permit*

d) Cuarto paso: finalmente, este último paso estará constituido por la regulación de tráfico de la zona Untrust a la zona Trust. No se permitirá bajo ningún aspecto el tráfico directamente de la zona Untrust a la Trust, la plataforma Middleware debe actuar como intermediario en ambas y recoger las peticiones necesarias de cada plataforma.

*user@host# set security policies from-zone **Untrust** to-zone **Trust** policy DenyIn match **[Dirección origen]** netTopLoopInt*
*user@host# set security policies from-zone **Untrust** to-zone **Trust** policy DenyIn match **[Dirección destino]** netBottomLoopInt*
*user@host# set security policies from-zone **Untrust** to-zone **Trust** policy DenyIn match application any*
*user@host# set security policies from-zone **Untrust** to-zone **Trust** policy DenyIn then deny*

Se debe negar el tráfico desde todas las IP de la zona Untrust hacía todas las IP de la zona Trust.

### 4.5.7 Implementación de política 7

La política siete, hace referencia a todas las reglas de acceso hacía la zona untrust. A continuación, se describirán los paso que se deberían seguir a la hora de implementar la política y permisos.

a) Primer paso: se creará un set de aplicaciones, que no es otra cosa que agrupar un gran número de puertos de aplicaciones bajo un mismo nombre. Esto ahorrará gestión a la hora de regular el tráfico por puertos de aplicaciones.

*user@host# set applications application-set **TM-ART** application 19120*
*user@host# set applications application-set **TM-ART** application 19122*
*user@host# set applications application-set **TM-ART** application 19124*
*user@host# set applications application-set **TM-ART** application 19125*
*user@host# set applications application-set **TM-ART** application 19126*

El conjunto de puertos son agrupados bajo el nombre de TM-ART. El set de aplicaciones mostrado a continuación fue documentado en el punto anterior, sin embargo para efectos de organización será introducido nuevamente:

*user@host# set applications application-set **Base_Datos** application 1520*
*user@host# set applications application-set **Base_Datos** application 1521*
*user@host# set applications application-set **Base_Datos** application 1522*
*user@host# set applications application-set **Base_Datos** application 1523*
*user@host# set applications application-set **Base_Datos** application 1524*
*user@host# set applications application-set **Base_Datos** application 1525*
*user@host# set applications application-set **Base_Datos** application 1526*
*user@host# set applications application-set **Base_Datos** application 1527*
*user@host# set applications application-set **Base_Datos** application 1528*
*user@host# set applications application-set **Base_Datos** application 1529*
*user@host# set applications application-set **Base_Datos** application 1530*

Este conjunto de puertos de aplicación serán llamados bajo el nombre de Base de Datos. El siguiente set de aplicaciones es denominado Micro y hace referencia a la mayoría de los puertos utilizados por el departamento de Microsoft y la zona Untrust.

*user@host# set applications application-set Micro application 25*
*user@host# set applications application-set Micro application 135*
*user@host# set applications application-set Micro application 88*
*user@host# set applications application-set Micro application 53*
*user@host# set applications application-set Micro application 135*
*user@host# set applications application-set Micro application 389*
*user@host# set applications application-set Micro application 50636 TCP*
*user@host# set applications application-set Micro application 80 TCP*
*user@host# set applications application-set Micro application 443 TCP*

b) Segundo paso: estará constituido por la implementación de las políticas de regulación de tráfico de la zona Externa a la zona Untrust. De acuerdo al segmento de red al que la zona externa desee ir, diferentes puertos de aplicación serán permitidos o no; se realizarán tres ejemplos, uno con el control de puertos del set de aplicaciones TM-ART, otro con el set de aplicaciones Base de Datos y otro con el set de aplicaciones Micro.

*user@host# set security policies from-zone **externa** to-zone un**trust** Red_Ext Monitoreo_Control_Unt **TM-ART** permit*
*user@host# set security policies from-zone **externa** to-zone **trust** Red_Ext Almacenamiento_Unt **Base_Datos** permit*
*user@host# set security policies from-zone **externa** to-zone **trust** Red_Ext Servicios_Plat_Microsoft **Micro** permit*

c) Tercer paso: estará constituido por la implementación de las políticas de regulación de tráfico de la zona Middleware a la zona Untrust. Se plantearán dos ejemplos, uno respecto al tráfico desde cualquier segmento de la zona Middleware al segmento Monitoreo_Control_Unt de la zona Untrust, y otro desde cualquier segmento de la zona Middleware hacía el segmento Almacenamiento_Unt de la zona Untrust; este procedimiento deberá aplicarse con todos los segmentos de la plataforma Untrust.

*user@host# set security policies from-zone **Middleware** to-zone **Untrust** any Monitoreo_Control_Unt **TM-ART** permit*
*user@host# set security policies from-zone **Middleware** to-zone **Untrust** any Almacenamiento_Unt **Base_Datos** permit*

d) Cuarto paso: finalmente, este último paso estará constituido por la regulación de tráfico de la zona Trust a la zona Untrust. No se permitirá bajo ningún aspecto el tráfico directamente de la zona Trust a la Untrust, la plataforma Middleware debe actuar como intermediario en ambas y recoger las peticiones necesarias de cada plataforma.

*user@host# set security policies from-zone **Trust** to-zone **Untrust** policy DenyIn match **[Dirección origen]** netTopLoopInt*
*user@host# set security policies from-zone **Trust** to-zone **Untrust** policy DenyIn match **[Dirección destino]** netBottomLoopInt*
*user@host# set security policies from-zone **Trust** to-zone **Untrust** policy DenyIn match application any*
*user@host# set security policies from-zone **Trust** to-zone **Untrust** policy DenyIn then deny*

### 4.5.8 Implementación de Política 8

La política ocho, hace referencia a todas las reglas de acceso hacía la zona Middleware. A continuación, se describirán los paso que se deberían seguir a la hora de implementar la política y permisos.

a) Primer paso: se creará un set de aplicaciones, que no es otra cosa que agrupar un gran número de puertos de aplicaciones bajo un mismo nombre. Los puertos de aplicaciones que se crearán irán del 7000 al 8000 y del 9000 al 10000.

*user@host# set applications application-set **Middle_Internet** application 7000*
*user@host# set applications application-set **Middle_Internet** application 7001*
*user@host# set applications application-set **Middle_Internet** application 7002*

Se seguirá el orden establecido hasta llegar al Puerto número 8000, luego se repetirá el mismo procedimiento del puerto 9000 hasta el 10000, con el mismo nombre de set de aplicaciones.

b) Segundo paso: estará constituido por la implementación de las políticas de regulación de tráfico de la zona Externa a la zona Middleware. De acuerdo al segmento de red desde el que se realicen las peticiones, existirá filtro en cuanto a puertos de aplicaciones o no. Si las peticiones provienen del segmento de red del equipo gestor llamado Bluecoat (llamaremos a su dirección IP x.x.x.x ya que por motivos de seguridad no fue suministrada por la empresa) se aplicará filtro por puertos de aplicación, sin embargo si la solicitud proviene de la red externa (coordinación de redes), se permitirán peticiones de cualquier índole de puertos de aplicación.

Se crea la zona para el BlueCoat

*user@host# set interfaces ge-0/0/0.1 unit 0 family inet address x.x.x.x/x*
*user@host# set security zones security-zone **BlueCoat** interfaces ge-0/0/0.1*

Se establecen las políticas para el tráfico proveniente del bluecoat

*user@host# set security policies from-zone **BlueCoat** to-zone **Middleware** Middle_Internet permit*

Se establecen las políticas para el tráfico proveniente de la red externa

*user@host# set security policies from-zone **externa** to-zone **Middleware** Red_Ext Middle_Prod_Trust any permit*

*user@host# set security policies from-zone **externa** to-zone **Middleware** Red_Ext Bck_Middle_Prod_Trust any permit*

c) Tercer paso: estará constituido por la implementación de las políticas de regulación de tráfico de la zona Untrust a la zona Middleware. Se plantearán dos ejemplos, de acuerdo a los dos segmentos IP de la plataforma Middleware actualmente en producción en el centro de datos La Colina.

*user@host# set security policies from-zone **Untrust** to-zone **Middleware** any Middle_Prod_Trust any permit*

*user@host# set security policies from-zone **Untrust** to-zone **Middleware** any Bck_Middle_Prod_Trust any permit*

d) Cuarto paso: este último paso estará constituido por la regulación de tráfico de la zona Trust a la zona Middleware. Se plantearán dos ejemplos, de acuerdo a los dos segmentos IP de la plataforma Middleware actualmente en producción en el centro de datos La Colina.

*user@host# set security policies from-zone **Trust** to-zone **Middleware** any Middle_Prod_Trust any permit*

*user@host# set security policies from-zone **Trust** to-zone **Middleware** any Bck_Middle_Prod_Trust any permit*

Para el tráfico de la zona trust a la untrust y viceversa, la plataforma Middleware debe actuar como gestor, ya que es el único con acceso a ambas, el flujo directo de tráfico de una hacía otra no estará permitido. La mayoría de estos

casos, se producen a través de gestores de aplicación en la capa de acceso de la plataforma middleware.

### 4.5.9 Implementación de Política 9

Al final de las declaraciones de las políticas en el cortafuego o firewall, se debe indicar la acción de rechazar, es decir, si el paquete no encuentra ninguna coincidencia con las reglas anteriores se rechaza.

### 4.5.10 Implementación de Política 10

Se recomienda implementar en el equipo de seguridad dos tarjetas SPC y dos NPC para aumentar la rapidez del procesamiento, una vez sean migrados los demás servicios, ésta cantidad debería aumentar.

### 4.5.11 Implementación de Política 11

El equipo de seguridad cuenta con herramientas de prevención y detección de ataques.

### 4.5.12 Implementación de Política 12

El equipo de seguridad cuenta con herramientas de prevención y detección de intrusiones.

# CONCLUSIONES

A pesar de que una plataforma no llega a ser totalmente segura, sus riesgos a ataques e intrusiones pueden ser minimizados, de tal manera de obtener una red de confianza o de fiabilidad. Toda vez que se quiera desplegar un proyecto de protección, deben responderse varias preguntas que ayudarán al diseñador a identificar los aspectos fundamentales de seguridad, algunas de ellas son ¿Qué se quiere proteger?, ¿De quién se necesita proteger? y ¿Cómo se puede proteger? la respuesta a estas preguntas permitirán identificar las vulnerabilidades, los tipos de amenazas y las técnicas que se pueden desplegar para proteger una red.

Luego de analizar la plataforma de red del centro de datos La Colina de Corporación Digitel, se puede comentar que cumple con los lineamientos básicos de un centro de datos concurrente, ya que se asegura disponibilidad de sus recursos ante fallas programadas, posee varios enlaces de redundancia, pisos flotantes y no se identifica un único punto que afecte globalmente al sistema, sin embargo no se encuentra diseñado para grandes desastres o fallas masivas ya que para tal fin se requiere una fortaleza mayor en su topología de red; asimismo, el centro de datos, una vez finalizado, cumplirá con la mayoría de los requerimientos de seguridad física, proporcionando buenos controles de seguridad de acceso, distribución idónea de los equipos de cómputo, elementos de detección de perturbaciones en el ambiente, entre otros, no obstante es importante puntualizar varias recomendaciones en las pocas deficiencias observadas.

En cuanto a la seguridad lógica, se plantearon una serie de políticas que buscan reducir al máximo los ataques de cualquier índole, intrusiones no deseadas e infecciones que puedan reproducirse con rapidez, sin embargo, como se mencionó al inicio, la seguridad absoluta es relativa y por ello se prefiere hablar en términos de fiabilidad o confiabilidad. Es importante someter a constantes revisiones las políticas planteadas en el proyecto de investigación, de manera de mejorar cada vez más su eficiencia y eficacia.

La elaboración de las políticas se realizó cumpliendo las necesidades específicas de la empresa y tomando en consideración los planteamientos de seguridad informática de trabajos de investigación anteriores, normas, artículos informativos, entre muchos otros, no obstante, el proceso de su elaboración y planteamiento sirve como base para la ejecución de reglas de seguridad en proyectos de diversas índoles que busquen el mismo objetivo general: proteger sus redes.

Por otra parte, cuando la red de una empresa es lo suficientemente grande, como un centro de datos, se debe contar con un equipo especial de seguridad que gestione la protección de su plataforma y asegure la confianza en sus conexiones, no obstante, cuando la red es sustancialmente pequeña basta con la aplicación de reglas de seguridad a sus computadores y concientización a los empleados sobre resguardo de contraseñas, utilización de software seguro, limitaciones de acceso a páginas Web no seguras y un conjunto de políticas en general que aseguran en gran medida la protección de su información.

Finalmente, es importante aclarar que se cumplieron todos los objetivos establecidos al inicio del proyecto y se superaron las expectativas en cuanto a aprendizaje.

# RECOMENDACIONES

Se realizaron una serie de recomendaciones en vista de la experiencia adquirida a lo largo del trabajo de investigación:

1) El centro de datos no cuenta con puertas y escaleras de emergencia en caso de cualquier imprevisto, por lo tanto se recomienda la implementación de éstas mucho antes de que la migración completa se realice.

2) Se recomienda Instalar cámaras de seguridad en todas las puertas de acceso para mantener un control del personal que ingresa a las instalaciones y evitar eventos como robo o hurto.

3) En cuanto a la ubicación de la DMZ, se sugiere que sea fuera de la red interna del centro de datos pero dentro de la red protegida por el firewall perimetral de la empresa, para permitir el acceso a los usuarios sin comprometer la seguridad interna.

4) Fomentar en el personal de la empresa la importancia de la no divulgación de contraseñas y claves personales.

5) Todas las computadoras deben tener un antivirus actualizado y herramientas de detección de ataques e intrusos.

6) Se debe respaldar mensualmente la información contenida en los sistemas informáticos.

7) Se debe elaborar un plan de contingencia en caso de fallas.

8) Se recomienda realizar auditorías de seguridad regularmente.

# REFERENCIAS BIBLIOGRÁFICAS


[1] POLITICA DE SEGURIDAD DATACENTER,
http://www.slideshare.net/jose_calero/politicas-de-seguridad-de-la-informacin-trabajo-grupal
Consulta: 30/10/2012.

[2] GUIA PARA LA ELABORACION DE POLITICAS DE SEGURIDAD,
http://api.ning.com/files/u2gdYg06meFYaRrQcaCxfptLmTGcy2B8wrTgigBnj7JnOKqK3ya3pQkNHSxKqyYB-dFWd0WaYHhFvTBKv9bkG8b921Boq3f*/guia_para_elaborar_politicas_v1_0.pdf
Consulta: 29/10/2012.

[3] Diseño y Cableado de un Centro de Datos,
http://in.unsaac.edu.pe/~mpenaloza/cursos/docs/Cableado%20de%20un%20Centro%20de%20Datosx6.pdf
Consulta: 17/12/2012.

[4] Norma venezolana COVENIN 200:1999 Código eléctrico Nacional.
http://www.sereinca.net/DOCUMENTOS/Codigo_Electrico_Nacional.pdf
Consultado: 20/04/2013.

[5] The Purpose of ANSI/TIA/EIA-942,
http://publicweb2.unimap.edu.my/~ict/v4/images/doc/ansi-tia-eia-942.pdf
Consultado: 21/01/2013.

[6] Introducción a la instalación de equipamiento eléctrico para minimizar ruido eléctrico de fuente externa en las entradas de controladores (extracto de IEEE 518-1982),http://materias.fi.uba.ar/6510/Clase%2012%20-Instalaci%F3n%20para%20minimizar%20ruido.pdf
Consulta: 21/01/2013.

[7] IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems,
http://hmin.tripod.com/als/ccs/docs/pdf/Greenbook.pdf
Consulta: 21/01/2013.

[8] FEDEUPEL, Manual de trabajos de Grado de Especialización y Maestría y Tesis Doctorales 4ta Edición (Libro); Caracas: Venezuela, 2006. pág. 21.

[9] Manuel Garcia Ferrando, Jesús Ibáñez y Francisco Alvira, El Análisis de la Realidad Social Métodos y técnicas de Investigación (Libro); España: Alvira Martín, 1986. pág. 67.

[10] Angel Alcaide Inchausti, Estadística Aplicada a las Ciencias Sociales (Libro); España, 1979, pág. 63.

[11] Mirian Balestrini Acuña, Como se Elabora el Proyecto de Investigación, Para los estudios formulativos o exploratorios, descriptivos, diagnósticos, evaluativos, formulación de hipótesis causales, experimentales y los proyectos factibles (Libro); Caracas: Venezuela, 2006. pág. 146.

[12] Mirian Balestrini, Procedimientos Técnicos de la Investigación Documental (Libro); Caracas: Venezuela, 1987. pág. XIX.

[13] Portal oficial CISCO. http://www.cisco.com/web/LA/productos/servicios/docs/LCS_White_Paper_Spanish.pdf
[Internet, Consulta 2013]

[14] Portal oficial CISCO. <http://www.cisco.com/web/LA/productos/servicios/docs/LCS_White_Paper_Spanish.pdf> [Internet, Consulta 2013]

[15] BENSON, Christopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft © Solutions. http://www.microsoft.com/latam/technet/articulos/200011 Consulta: 14/03/2013.

[16] BENSON, Christopher. Estrategias de Seguridad. Inobis Consulting Pty Ltd. Microsoft © Solutions. http://www.microsoft.com/latam/technet/articulos/200011 Consulta: 14/03/2013.

[17] Luis Miguel Díaz Vizcaino. Seguridad Informática. Universidad Carlos III de Madrid, Departamento de Ingeniería Telemática. http://www.it.uc3m.es/~lmiguel/Firewall_www/SEGURIDAD-to-Web.htm Consultado el 11 de Abril de 2013.

# BIBLIOGRAFÍA


- ✓ TESIS DIGITALES UNMSM, http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap6.PDF Consulta: 24/10/2012

- ✓ SEGURIDAD DE LA RED – NORMALIZACIÓN, http://www.itu.int/itunews/issue/2002/06/security-es.html Consulta: 22/10/2012.

- ✓ POLÍTICAS DE SEGURIDAD,
- ✓ http://auditoriasistemas.com/auditoria-informatica/politicas-de-seguridad/ Consulta: 23/10/2012

- ✓ FIREWALLS: POLÍTICAS DE SEGURIDAD EN RED, http://mundopc.net/firewalls-politicas-de-seguridad-en-red/ Consulta: 24/10/2012

- ✓ Bruzual, Z. (2008) Instructivo y modelo para realizar el anteproyecto de Trabajo de grado.

- ✓ Arias, F. (2006) Introducción a la metodología científica, Episteme, Quinta Edición.

- ✓ Chris DiMinico, Telecommunications Infraestructure Standard for Data Centers http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf Consulta 24/01/2013

- ✓ Metodología PPDIOO http://www.cisco.com/global/EMEA/IPNGN/ppdioo_implement.html#implement Consulta 20/04/2013

- ✓ Norma Venezolana Código Eléctrico Nacional, COVENIN 200:1999
  http://www.sereinca.net/DOCUMENTOS/Codigo_Electrico_Nacional.pdf
  Consulta: 30/11/2012

- ✓ Estándar Internacional ISO/IEC 17799. Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información. Segunda edición 2005-06-15.

- ✓ Seguridad en los equipos activos de la universidad Distrital
  http://www.udistrital.edu.co:8080/documents/11177/20084/Politicas+de+Seguridad+-+Comunicaciones.pdf
  Consulta: 21/01/2013

- ✓ Security Configuration Guide, Juniper Networks, Inc.
  https://www.juniper.net/techpubs/software/junos-security/junos-security10.0/junos-security-swconfig-security/junos-security-swconfig-security.pdf
  Consulta: 16/01/2013

- ✓ Política Seguridad Física SISTESEG, Bogotá Colombia
  http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf
  Conculta: 13/12/2012

- ✓ Políticas de seguridad Informática
  http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Politicas_de_seguridad_informtica.pdf
  Consulta: 13/12/2012

# GLOSARIO

**Ataque borrado de huellas:** el borrado de huellas es una de las tareas más importantes que debe realizar el intruso después de ingresar en un sistema, ya que, si se detecta su ingreso, el administrador buscará como conseguir "tapar el hueco" de seguridad, evitar ataques futuros e incluso rastrear al atacante. Las Huellas son todas las tareas que realizó el intruso en el sistema y por lo general son almacenadas en Logs (archivo que guarda la información de lo que se realiza en el sistema) por el sistema operativo.
Los archivos Logs son una de las principales herramientas (y el principal enemigo del atacante) con las que cuenta un administrador para conocer los detalles de las tareas realizadas en el sistema y la detección de intrusos.

**Ataque conection Floyd:** la mayoría de las empresas que brindan servicios de Internet tienen un límite máximo en el número de conexiones simultáneas. Una vez que se alcanza ese límite, no se admitirán conexiones nuevas. Así, por ejemplo, un servidor Web puede tener, por ejemplo, capacidad para atender a mil usuarios simultáneos. Si un atacante establece mil conexiones y no realiza ninguna petición sobre ellas, monopolizará la capacidad del servidor. Las conexiones van caducando por inactividad poco a poco, pero el atacante sólo necesita intentar nuevas conexiones, para mantener fuera de servicio el servidor.

**Ataque Decoy (señuelos):** los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas". Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta estudiar el archivo generado para conocer nombres de usuarios y claves.

**Ataque Jamming:** este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más pueda utilizarla. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP usando Spoofing y Looping. El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

**Ataque shoulder Surfing:** consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora. Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso.

**Ataque Scanning (Búsqueda):** el Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (escanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma. El Escaneo de puertos pertenece a la seguridad informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos. La idea básica es simple: llamar a un número y si el módem devuelve un mensaje de conectado, grabar el número. En otro caso, la computadora cuelga el teléfono y llama al siguiente número.

**Ataque Snooping-Downloading:** los ataques de esta categoría tienen el objetivo de obtener la información sin modificarla. Sin embargo los métodos son diferentes. Aquí, además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de correo electrónico y otra información guardada, realizando en la mayoría de los casos un downloading (copia de documentos) de esa información a su propia computadora, para luego hacer un análisis exhaustivo de la misma. El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software.

**Ataque Spoofing-looping:** spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping. Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él. El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, tiene la finalidad de "evaporar" la identificación y la ubicación del atacante. El camino tomado desde el origen hasta el destino puede tener muchas estaciones, que exceden obviamente los límites de un país.

**Ataque tampering:** esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aun así, si no hubo intenciones de "bajar" el sistema por parte del atacante, el Administrador posiblemente necesite darlo de

baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

**Cifrado:** el cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo. Use el cifrado cuando desee un alto nivel de protección de la información.

**Cracker:** el cracker, es considerado un "vandálico virtual". Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión.

**Criptografía:** la criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

**DMZ:** cuando ciertas máquinas de la red interna tienen que ser accesibles desde el exterior (servidor web, un servidor de mensajería, un servidor FTP público, etc.),

normalmente es necesario crear una nueva política para una nueva red, accesible tanto desde la red interna como desde el exterior, sin correr el riesgo de comprometer la seguridad de la empresa. Se habla entonces de una "zona desmilitarizada" (DMZ para DeMilitarized Zone) para designar esta zona aislada que aloja aplicaciones a disposición del público. La DMZ sirve como una zona intermedia entre la red a proteger y la red hostil.

**Failover:** configuración de equipos en red en la que un segundo equipo se hace cargo de las funciones del principal cuando éste se detiene o falla. De esta forma, el servicio no es interrumpido.

**Hacker:** un hacker es una persona que entra de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo. Los hackers han evolucionado de ser grupos clandestinos a ser comunidades con identidad bien definida. De acuerdo a los objetivos que un hacker tiene, y para identificar las ideas con las que comulgan, se clasifican principalmente en: hackers de sombrero negro, de sombrero gris, de sombrero blanco y script kiddie.

**Hackers de sombrero blanco:** se le llama hacker de sombrero blanco a aquel que penetra la seguridad de sistemas para encontrar puntos vulnerables. La clasificación proviene de la identificación de héroes en las películas antiguas del viejo oeste, que usaban típicamente sombreros blancos.

**Hackers de sombrero gris:** como el nombre sugiere, se le llama hacker de sombrero gris a aquel que es una combinación de sombrero blanco con sombrero

negro, dicho en otras palabras: que tiene ética ambigua. Pudiera tratarse de individuos que buscan vulnerabilidades en sistemas y redes, con el fin de luego ofrecer sus servicios para repararlas bajo contrato.

**Hackers de sombrero negro:** se le llama hacker de sombrero negro a aquel que penetra la seguridad de sistemas para obtener una ganancia personal o simplemente por malicia. La clasificación proviene de la identificación de villanos en las películas antiguas del vejo oeste, que usaban típicamente sombreros negros.

**Middleware:** es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, software, redes, hardware y/o sistemas operativos. Éste simplifica el trabajo de los programadores en la compleja tarea de generar las conexiones que son necesarias en los sistemas distribuidos.

**Perímetro de seguridad:** frontera física o lógica que define un dominio de seguridad o zona en la que se aplica una determinada política de seguridad o se ha implantado una determinada arquitectura de seguridad.

**Servidor DNS:** es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y vice-versa. Aunque Internet sólo funciona en base a direcciones IP, el DNS permite que los humanos usemos nombres de dominio que son bastante más simples de recordar (pero que también pueden causar muchos conflictos, puesto que los nombres son activos valiosos en algunos casos). El sistema de nombres de dominios en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallas. Aunque parece muy difícil lograr todos esos objetivos, la solución no es tan compleja en realidad. El punto central se basa en un árbol que define la jerarquía entre los dominios y los sub-dominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda. Por ejemplo, en

dcc.uchile.cl, el dominio más alto es cl. Para que exista una raíz del árbol, se puede ver como si existiera un punto al final del nombre: dcc.uchile.cl., y todos los dominios están bajo esa raíz (también llamada ``punto").

**Servidor SMTP:** es un estándar internacional utilizado para transferencia de correo electrónico (email) entre computadoras. Hoy en día es utilizado exclusivamente para el envío de correos, donde la información de cada servicio de usuario es almacenada en servidores acondicionados para tal fin.

**Script kiddies:** Se les denomina script kiddies a los hackers que usan programas escritos por otros para lograr acceder a redes de computadoras, y que tienen muy poco conocimiento sobre lo que está pasando internamente.