ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DEL DATA CENTER PARA CERT- ECUADOR

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

DAVID FERNANDO TORRES ZAMBRANO

davidf_torres@outlook.com

DIRECTOR: DR. LUIS ENRIQUE MAFLA GALLEGOS, PHD

enrique.mafla@epn.edu.ec

Quito, Diciembre 2013

DECLARACIÓN

Yo, David Fernando Torres Zambrano, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normativa institucional vigente.

David Fernando Torres Zambrano

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por David Fernando Torres Zambrano, bajo mi supervisión.

Dr. Enrique Mafla, PHD

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Agradezco a mi mamá Aida Zambrano y a mi papá David Torres, por darme siempre su apoyo y por guiarme para convertirme en el hombre que soy.

Agradezco a mi hermano José Torres, por su gran apoyo y compañía.

A mis amigos que siempre me apoyaron.

A los ingenieros y amigos de la Supertel, por su amistad y por su ayuda.

A mi director por su guía durante todo el proyecto.

A todos gracias de todo corazón.

David Torres Zambrano

DEDICATORIA

…A mis padres

…A mi hermano

CONTENIDO

DECLARACIÓN……II

CERTIFICACIÓN……..III

AGRADECIMIENTO……..IV

DEDICATORIA……V

CONTENIDO……VI

RESUMEN……..XIII

ÍNDICE GENERAL

CAPÍTULO 1: DEFINICIONES

1.1. DEFINICIÓN DEL PROYECTO 1

1.2. DEFINICIONES 1

1.3. METODOLOGÍA Y HERRAMIENTAS 7

1.3.1. Metodología 7

1.3.1.1. Análisis de requerimientos 7

1.3.1.2. Diseño 7

1.3.2. Herramientas 8

1.3.2.1. Norma TIA-942 8

1.3.2.2. Arquitectura SAFE 11

1.3.2.3. Recomendaciones Amparo 11

CAPÍTULO 2: ANÁLISIS

2.1. REQUERIMIENTOS FUNCIONALES 13

2.1.1. Alertas y advertencias.....13

2.1.2. Manejo de incidentes 15

2.1.3. Gestión de vulnerabilidades.....17

2.1.4. Anuncios 19

2.1.5. Desarrollo de herramientas de seguridad 20

2.1.6. Detección de intrusos.....22

2.1.7. Educación y entrenamiento 24

2.1.8. Aplicaciones por servicio del EcuCERT *25*
2.2. REQUERIMIENTOS DE CAPACIDAD 25
2.2.1. Perfiles de usuario *26*
2.2.1.1. Perfil de uso para el servicio alertas y advertencias 29
2.2.2. Usuarios por aplicación *34*
2.2.3. Clasificación de los servicios por el tipo de interacción con el usuario *35*
2.2.4. Velocidad de enlace *36*
2.2.5. Almacenamiento *37*
2.2.6. Características de CPU, RAM, y Red por aplicación *38*
2.2.7. Crecimiento de usuarios *39*
2.2.7.1. Proyección de usuarios de la red interna 40
2.2.7.2. Proyección de clientes 40
2.3. REQUERIMIENTOS DE CABLEADO ESTRUCTURADO 41
2.4. REQUERIMIENTOS DE SEGURIDAD 41

CAPÍTULO 3: DISEÑO

3.1. DISEÑO DE LA RED 43
3.1.1. Módulo central (core) *45*
3.1.2. Módulo centro de datos intranet *50*
3.1.2.1. Infraestructura de networking del centro de datos intranet 53
3.1.2.2. Servidores 59
3.1.2.3. Propuesta de diseño del módulo centro de datos intranet 63
3.1.3. Módulo perimetral a internet *64*
3.1.3.1. Zona desmilitarizada DMZ 64
3.1.3.2. Perímetro del proveedor de servicios 70
3.1.4. Módulo de campus *71*
3.1.4.1. Capas del módulo de campus 72
3.1.5. Módulo Honeynet *73*
3.1.6. Módulo red de pruebas *74*
3.1.7. Módulo de administración *75*
3.1.8. Propuesta de red para el EcuCERT *76*
3.1.8.1. Puntos de red actuales y crecimiento de usuarios 79
3.2. SELECCIÓN DE EQUIPOS 79
3.2.1. Selección del medio de transmisión *79*
3.2.2. Equipos necesarios para la red del EcuCert *81*
3.2.3. Cálculo de la Potencia total *92*
3.2.4. Cálculo y dimensionamiento del UPS *94*
3.3. DISEÑO DEL CENTRO DE DATOS 95
3.3.1. Infraestructura del sistema de cableado del centro de datos *97*

3.3.2. Topología del Centro de datos 98
3.3.2.1. Descripción de los elementos del centro de datos 99
3.4. SISTEMA DE CABLEADO DEL CENTRO DE DATOS 101
3.4.1. Cableado horizontal 101
3.4.2. Cableado backbone 102
3.4.3. Etiquetado 104
3.4.3.1. Identificación de los rack y gabinetes 104
3.5. CUARTO DE CÓMPUTO 107
3.5.1. Etiquetado de equipos servidores 107
3.5.2. Área de distribución principal 109
3.5.3. Área de distribución de equipos 111
3.5.4. Ubicación de los racks dentro del cuarto de cómputo 111
3.5.5. Cableado entre racks 114
3.5.6. Sistema de flujo de aire 115
3.5.7. Sistema contra incendios 119
3.5.8. Seguridad física del cuarto de cómputo 121
3.5.8.1. Sistema de video vigilancia IP 121
3.5.8.2. Sistema de control de acceso 122
3.5.9. Sistema de puesta a tierra y Generador eléctrico 123
3.5.9.1. Sistema de puesta a tierra 123
3.5.9.2. Generador eléctrico 124
3.6. LISTA FINAL DE MATERIALES, EQUIPOS Y PRESUPUESTO 126
3.6.1. Equipos de red y servidores (Equipos activos) 126
3.6.2. Accesorios (Equipo pasivo) 127
3.6.3. Equipos UPS 127
3.6.4. Sistema de video vigilancia 127
3.6.5. Generador eléctrico 128
3.6.6. Sistema de conexión a tierra 128
3.6.7. Sistema de control de acceso 128
3.6.8. Sistema de piso de acceso elevado 129
3.6.9. Instalación y mensualidad del enlace a internet 129
3.6.10. Sistema de detección y extinción de incendios 130
3.6.11. Sistema de climatización 131
3.6.12. Resumen total del presupuesto 131

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES 132
4.2. RECOMENDACIONES 133

BIBLIOGRAFÍA **134**

ÍNDICE DE TABLAS

TABLA 1.1: CARACTERÍSTICAS DE LOS DIFERENTES TIPOS DE CENTROS DE DATOS 6
TABLA 1.2: ÍTEMS POR SUBSISTEMA 9
TABLA 2.1: APLICACIONES NECESARIAS POR SERVICIO DEL ECUCERT 26
TABLA 2.2: PERFILES DE USUARIO 27
TABLA 2.3: CARACTERÍSTICAS DE CPU, RAM Y RED NECESARIOS POR ACTIVIDAD DEL ECUCERT 28
TABLA 2.4: USUARIO POR APLICACIÓN. 34
TABLA 2.5: CLASIFICACIÓN DEL TIPO DE SERVICIO 35
TABLA 2.6: CARACTERÍSTICAS PARA DIMENSIONAMIENTO DE EQUIPOS SERVIDORES 38
TABLA 2.7: USUARIOS ACTUALES Y CRECIMIENTO A FUTURO 40
TABLA 3.1: MITIGACIÓN DE AMENAZAS EN EL MÓDULO CORE 49
TABLA 3.2 : TABLA DE DIRECCIONAMIENTO IP DEL ECUCERT 60
TABLA 3.3: PERFILES DE USUARIOS EN SERVIDOR PROXY 61
TABLA 3.4: NÚMERO DE EQUIPOS NECESARIOS 81
TABLA 3.5: RESUMEN DE CARACTERÍSTICAS DE LOS EQUIPOS *ROUTERS* 82
TABLA 3.6: RESUMEN DE CARACTERÍSTICAS DEL SWITCH DE CORE 85
TABLA 3.7: RESUMEN DE CARACTERÍSTICAS DEL SWITCH DE ACCESO 87
TABLA 3.8: RESUMEN DE CARACTERÍSTICAS DEL FIREWALL 88
TABLA 3.9: VIRTUALIZACIÓN DE SERVIDORES POR SERVICIO 90
TABLA 3.10: CARACTERÍSTICAS DE SERVIDORES 91
TABLA 3.11: CARACTERÍSTICAS DE SERVIDORES DE RED DE PRUEBA Y HONEYNET 92
TABLA 3.12: POTENCIA TOTAL CONSUMIDA POR EQUIPOS DE NETWORKING 93
TABLA 3.13: ETIQUETADO DE EQUIPOS DE NETWORKING Y UNIDADES DE RACK POR EQUIPO 108
TABLA 3.14: ETIQUETADO DE SERVIDORES Y UNIDADES DE RACK POR SERVIDOR 111
TABLA 3.15: GUÍA TÉRMICA ASHRAE 2011 117
TABLA 3.16: CABLES PARA TBB Y/O BC 123
TABLA 3.17: LISTA DE PRECIOS DE EQUIPOS Y SERVIDORES 126
TABLA 3.18: PRECIOS DE ACCESORIOS (EQUIPOS PASIVOS) 127
TABLA 3.19: PRECIOS DE UPS 127
TABLA 3.20: PRECIOS DEL SISTEMA DE VIDEO VIGILANCIA 127
TABLA 3.21: PRECIO DEL GENERADOR ELÉCTRICO 128
TABLA 3.22: PRECIOS DEL SISTEMA DE PUESTA A TIERRA 128
TABLA 3.23: PRECIOS DEL SISTEMA DE CONTROL DE ACCESO 128

TABLA 3.24: PRECIO DEL SISTEMA DE PISO ELEVADO (TODOS SUS COMPONENTES) 129
TABLA 3.25: COSTO DE ENLACES DE INTERNET 129
TABLA 3.26: PRECIO DEL SISTEMA DE DETECCIÓN Y EXTINCIÓN DE FUEGO 130
TABLA 3.27: PRECIO DEL SISTEMA DE CLIMATIZACIÓN (HVAC) 131
TABLA 3.28: COSTO TOTAL PARA LA IMPLEMENTACIÓN DEL CENTRO DE DATOS 131

ÍNDICE DE FIGURAS

FIGURA 2.1: CASO DE USO ALERTAS Y ADVERTENCIAS 14
FIGURA 2.2: CASO DE USO MANEJO DE INCIDENTES 16
FIGURA 2.3: CASO DE USO GESTIÓN DE VULNERABILIDADES 18
FIGURA 2.4: CASO DE USO ANUNCIOS 19
FIGURA 2.5: CASO DE USO DE HONEYNET 20
FIGURA 2.6: CASO DE USO DESARROLLO DE HERRAMIENTAS DE SEGURIDAD 21
FIGURA 2.7: CASO DE USO DETECCIÓN DE INTRUSOS 23
FIGURA 2.8: CASO DE USO EDUCACIÓN Y ENTRENAMIENTO 24
FIGURA 3.1: DISEÑO DE RED DE ACUERDO A CISCO SAFE 46
FIGURA 3.2: MÓDULO DE CORE 47
FIGURA 3.3: BANNER DE LOS EQUIPOS 48
FIGURA 3.4: ESTRUCTURA DEL MÓDULO CENTRO DE DATOS INTRANET 53
FIGURA 3.5: FLUJO DE TRÁFICO DE MONITOREO 57
FIGURA 3.6: USO DE BEACON PARA DETECTAR ENLACES CAÍDOS 58
FIGURA 3.7: DISEÑO DEL MÓDULO CENTRO DE DATOS INTRANET 63
FIGURA 3.8: MÓDULO PERIMETRAL A INTERNET - DMZ 69
FIGURA 3.9: MÓDULO PERIMETRAL A INTERNET – PERÍMETRO DEL PROVEEDOR DE SERVICIOS. 71
FIGURA 3.10: MÓDULO HONEYNET 73
FIGURA 3.11: MÓDULO RED DE PRUEBAS VIRTUALES 74
FIGURA 3.12: PROPUESTA 1 - DISEÑO DE RED CON REDUNDANCIA TIER 2 77
FIGURA 3.13: PROPUESTA 2 – DISEÑO DE RED CON REDUNDANCIA TIER 1 78
FIGURA 3.14: TRIÁNGULO DE POTENCIAS 94
FIGURA 3.15: RELACIÓN DE ESPACIOS EN UN CENTRO DE DATOS 96
FIGURA 3.16: INFRAESTRUCTURA DEL SISTEMA DE CABLEADO DEL CENTRO DE DATOS 97
FIGURA 3.17: PROPUESTA DE DISEÑO DEL CENTRO DE DATOS DEL ECUCERT 98
FIGURA 3.18: TOPOLOGÍA DE CABLEADO DE *BACKBONE* 102
FIGURA 3.19: REDUNDANCIA EN EL CENTRO DE DATOS DEL ECUCERT 103
FIGURA 3.20: ALINEACIÓN DE RACK Y GABINETES 105
FIGURA 3.21: IDENTIFICACIÓN DE PATCH PANEL 105

FIGURA 3.22: IDENTIFICACIÓN DE LA CONEXIÓN ENTRE PATCH PANELS 106
FIGURA 3.23: EJEMPLO DE ETIQUETADO DE PATCH PANEL 107
FIGURA 3.24: UBICACIÓN DE EQUIPOS Y PATCH PANELS EN EL RACK 1 EN MDA 109
FIGURA 3.25: UBICACIÓN DE EQUIPOS Y PATCH PANEL DE CONEXIÓN RACK 2 Y 3 EN MDA 110
FIGURA 3.26: UBICACIÓN DE EQUIPOS Y PATCH PANEL RACK 04 EN EDA 112
FIGURA 3.27: DISTRIBUCIÓN DE EQUIPOS Y TAMAÑO DEL CUARTO DE CÓMPUTO 113
FIGURA 3.28: CABLEADO ENTRE RACKS VISTA FRONTAL (CABLES PATCH CORD) 114
FIGURA 3.29: CABLEADO ENTRE RACKS VISTA TRASERA 115
FIGURA 3.30: ALTURA DEL CENTRO DE DATOS Y FLUJO DE AIRE 116
FIGURA 3.31: SISTEMA DE EXTINCIÓN Y DETECCIÓN DE INCENDIOS 119
FIGURA 3.32: ESQUEMA DE SEGURIDAD FÍSICA DEL CENTRO DE DATOS 121
FIGURA 3.33: DIAGRAMA DE CONEXIÓN DEL SISTEMA DE ACCESO 122
FIGURA 3.34: SISTEMA DE PUESTA A TIERRA 124
FIGURA 3.35: ESQUEMA DE CONEXIÓN DEL GENERADOR 125

ÍNDICE DE ANEXOS

Anexo A: Resumen de historias de usuario de la consultoría del EcuCERT

Anexo B: Tabla completa de características para los servicios

Anexo C: Propuesta de enlace a internet corporativo del ISP Movistar redes de prueba

Anexo D: Propuesta de enlace a internet corporativo del ISP Movistar red principal

Anexo E: Data sheet routers

Anexo F: Data sheet switch de core

Anexo G: Data sheet switch acceso

Anexo H: Data sheet firewall IDS/IPS

Anexo I: Data sheet Aire acondicionado de precisión

Anexo J: Data sheet UPS

Anexo K: Cotización servidores

- Anexo K-1: Cotización servidores A
- Anexo K-2: Cotización servidores B y C
- Anexo K-3: Cotización servidores D
- Anexo K-4: Cotización servidores E y F

Anexo L: Proforma de presupuesto

Anexo L-1: Proforma presupuestos implementación centro de datos

Anexo L-2: Proforma de equipos

Anexo M: Data sheet servidores

Anexo N: Data sheet servidor VMWare Raid

RESUMEN

El presente proyecto trata sobre el diseño del centro de datos para el CERT de Ecuador (EcuCERT). Para llevar a cabo el proyecto se utilizó la metodología sistemática, la cual permite dividir el proyecto en dos partes principales: análisis de requerimientos y diseño. El análisis de requerimientos se desarrolla con base en historias de usuarios, las cuales se obtienen directamente de la información facilitada por la Supertel. Las historias de usuario permiten desarrollar casos de uso para cada servicio brindado por el EcuCERT. Con los casos de uso se determinan todos los involucrados en el proyecto, las aplicaciones que corren en la red y los diferentes perfiles de usuario. Esta información permite determinar los requerimientos de capacidad y seguridad necesarios.

El diseño del centro de datos utiliza los datos del análisis de requerimientos, y se divide en tres partes. La primera es el diseño de la red. El diseño de la red se basa en la arquitectura SAFE[1] de Cisco y en el manual básico de gestión de incidentes y seguridad informática de Amparo[2], LACNIC[3]. Se escogió la arquitectura SAFE de cisco debido a que la mayoría de equipos que se utilizarán en la red son de esa marca. SAFE además permite un desarrollo de red modular lo que facilita el crecimiento y la protección de la red. Se escogió el manual de Amparo sobre otras herramientas similares, ya que al ser desarrollado por la LACNIC es la más cercana a la realidad del EcuCERT. La segunda etapa es la elección de equipos, en esta se determinan los requerimientos de hardware de los equipos así como los requerimientos de potencia eléctrica, aire acondicionado (HVAC) y de espacio necesarios para alojar todos los equipos.

Finalmente en la tercera etapa del diseño se realiza el diseño del espacio del centro de datos. Este diseño se lo hace bajo el estándar EIA[4]/TIA[5]-942, que es el estándar actual para el diseño de centros de datos. Esta etapa incluye la determinación de la topología del centro de datos, la distribución de racks, el sistema de

---

[1] SAFE: Plan de seguridad para redes empresariales.
[2] Amparo: Proyecto de LACNIC para el fortalecimiento de la capacidad regional de atención de incidentes de seguridad en América Latina y el Caribe.
[3] LACNIC: Registro de direcciones de internet para América Latina y el Caribe
[4] EIA: Alianza de industrias electrónicas, por sus siglas en inglés.
[5] TIA: Asociación de industrias de telecomunicaciones, por sus siglas en inglés

cableado estructurado, el dimensionamiento del UPS y generador eléctrico, el sistema de aire acondicionado, las medidas de ancho, largo y alto necesarias para el cuarto de cómputo, el etiquetado y el sistema de detección y extinción de fuego.

Por último se presentan conclusiones y recomendaciones derivadas del desarrollo del proyecto.

CAPÍTULO 1

DEFINICIONES

En el presente capítulo se realiza la definición del problema, se propone la solución al mismo y se selecciona la metodología y herramientas para ser utilizadas. Primero se define el problema tomando en cuenta las necesidades de la Supertel y a continuación se propondrá una solución que satisfaga los problemas planteados. Posteriormente se presentan conceptos de seguridad informática y se definen varios términos relacionados con CERTs y centros de datos. Finalmente se explica la metodología sistemática y las herramientas utilizadas EIA/TIA-942, Cisco SAFE, y el manual de gestión de incidentes de Amparo, LACNIC.

1.1. DEFINICIÓN DEL PROYECTO [L1]

La Supertel se encuentra en proceso de desarrollo de un CERT (EcuCERT). El EcuCERT debe contar con una infraestructura de centro de datos directamente bajo su control, de acuerdo al proyecto Amparo de LACNIC. Además, el EcuCERT planea ampliar sus servicios e incrementar sus clientes en años posteriores, por lo que la infraestructura del centro de datos debe permitir y facilitar el crecimiento. Finalmente, al ser el EcuCERT el encargado de solucionar y/o brindar asesoría ante problemas de seguridad informáticos, sería perjudicial para su imagen que su propia red sufra caídas de servicio o intrusiones de manera reiterada.

Para los problemas mencionados anteriormente el centro de datos propuesto, gracias a la implementación de las recomendaciones SAFE de cisco, la norma EIA/TIA-942 y el manual de gestión de incidentes de amparo de LACNIC, permite mejorar la seguridad, facilita el crecimiento y la administración, y permite optimizar recursos como el espacio físico necesario.

1.2. DEFINICIONES

Seguridad de la información [L1] [L6] [W2]

Seguridad de la información es la práctica de la defensa de la información y los sistemas de información frente al acceso, uso, divulgación, alteración, modifica-

ción, lectura, inspección, registro o destrucción no autorizados. A fin de proporcionar: Integridad, que significa la protección contra la indebida modificación o destrucción de la información, e incluye el no repudio de la información y la autenticidad. Confidencialidad, que significa la preservación de las restricciones autorizadas en materia de acceso y divulgación, así como medios para la protección de la intimidad personal y la información de propiedad. Disponibilidad, que significa garantizar el acceso y uso oportuno y confiable de la información. Seguridad de la información es un término general que se puede utilizar independiente de la forma en que se encuentren los datos.

Seguridad informática [L1] [L6] [W2]

La seguridad informática es un área de la informática que se encarga de la protección de la información procesada, transmitida, almacenada o difundida por medio la TICs[6]. La seguridad informática es la aplicación de la seguridad de la información a las TICs.

Incidente informático [L1] [L6] [W2] [W6]

El US CERT[7] define un incidente informático como: "Cualquier violación de la política de seguridad explícita o implícita, que atente contra la confidencialidad, integridad y disponibilidad de la información y los recursos tecnológicos". Los incidentes de seguridad informática se pueden clasificar en cinco categorías:

a) Acceso no autorizado; es cuando un individuo obtiene acceso lógico o físico no autorizado a la red, sistema, aplicaciones, datos o a otro tipo de recurso.
b) Código malicioso; es la instalación de un software malicioso (por ejemplo: virus, gusanos, troyanos, o cualquier clase de código malicioso) que infecta el sistema operativo o aplicaciones.
c) Interrupción del servicio o denegación de servicio; es un ataque que impide o disminuye la funcionalidad normal de la red, sistema o aplicación al agotar sus recursos. Esta actividad incluye ser víctima o participar en ataques DoS.

[6] Tecnologías de la Información y Comunicación.
[7] Cert de los Estados Unidos de América

d) Escaneos, pruebas o intentos de obtener información de redes o servidores sin autorización; esta actividad incluye cualquiera que pretenda identificar o acceder a un equipo, puertos abiertos, protocolos, servicios o cualquier combinación, para su posterior explotación.
e) Mal uso de los recursos tecnológicos; es cuando una persona viola las políticas de uso aceptable de los equipos de TICs.

CERT [L1] [L6] [W2] [W5]

CERT son las siglas de "*Computer emergency response team*," que en español significa "Equipo de respuesta a emergencias informáticas." Un CERT constituye un equipo de expertos en informática que se encargan de resolver o prevenir incidentes informáticos, así como de brindar apoyo para lidiar con dichos problemas. CERT es lo mismo que Csirt. Csirt son las siglas de "*Computer Security Incident Response Team*"; debido a que el término CERT se encuentra patentado por la universidad de Carnegie Mellon de los Estados Unidos de Norteamérica, muchos equipos optan por el término Csirt.

El término CERT/CC hace referencia a un CERT que actúe como centro de coordinación principal en el país. Los demás CERTs existentes en el país deberán reportar los incidentes al CERT/CC. El CERT que desea implementar la Supertel es del tipo CERT/CC.

Funciones de un CERT [L1] [W2] [W5]

Las funciones de un CERT son las tareas u obligaciones que tiene su personal y están orientadas específicamente para la "Comunidad" de la que el CERT es responsable, es decir los clientes que reciben los servicios del CERT. Las funciones típicas de un CERT de acuerdo al manual de amparo LACNIC son:

a. Ayudar a sus clientes a prevenir y atenuar un incidente de seguridad informática.
b. Prestar asistencia a sus usuarios para recuperarse de las consecuencias de un incidente o incidentes de seguridad informática.
c. Ayudar a proteger la información de los clientes.

d. Ayudar a establecer políticas de seguridad.
e. Coordinar de forma centralizada la seguridad de la información.
f. Almacenar evidencias.

Servicios de un CERT [L1] [W2]

Los servicios de un CERT constituyen "el producto" que el CERT ofrece a sus clientes. Los servicios que ofrece un CERT pueden ser: reactivos o proactivos de acuerdo al manual de amparo[8], a continuación se define cada uno de estos servicios.

Servicios Reactivos [L1] [W2]

Servicios reactivos son los que se centran en el tratamiento de incidentes así como en la mitigación de daños. Están enfocados en atender peticiones de asistencia por parte de los clientes u otros CERTs o Csirts. Los servicios reactivos son servicios en tiempo real, generalmente involucran el monitoreo de la red de los clientes. Entre los servicios reactivos se tiene:

- Alertas y advertencias
- Tratamiento de incidentes
- Análisis de incidentes
- Apoyo a la respuesta de incidentes
- Coordinación de la respuesta de incidentes
- Respuesta a incidentes *in situ*
- Tratamiento de vulnerabilidades
- Análisis de la vulnerabilidad
- Respuesta a la vulnerabilidad
- Coordinación de la respuesta a la vulnerabilidad

No es necesario que un CERT ofrezca todos los servicios mencionados. Ofrecer todos los servicios requiere de una gran cantidad de recursos humanos, técnicos

[8] *Referencia a: 1 "Como crear un CSIRT paso a paso", Enisa - Amparo LACNIC "Lineamientos y Acciones Recomendadas para la Formulación de un Centro de Respuesta a incidentes de Seguridad Informática " – CSIRT Services, Carnegie Mellon*

y económicos de acuerdo a US-CERT[9], por lo general un CERT empieza con los 5 primeros de la lista mostrada anteriormente.

Servicios Proactivos [L1] [W2]

Servicios proactivos son los servicios encargados de mejorar la infraestructura y la seguridad, antes de que ocurra o sea detectado un incidente. Su objetivo es: evitar, reducir el impacto, y limitar el alcance de los incidentes informáticos. Los servicios proactivos ayudan a crear una cultura de seguridad en los clientes, y no son servicios en tiempo real. Los servicios proactivos son servicios que ofrece el CERT como apoyo a la tarea de respuesta a incidentes. Entre los servicios proactivos se tiene:

- Comunicados
- Observatorio de tecnología
- Evaluaciones o auditorias de la seguridad
- Configuración y mantenimiento de la seguridad
- Desarrollo de herramientas de seguridad
- Servicios de detección de intrusos
- Difusión de información relacionada con la seguridad

Al igual que con los servicios reactivos no es obligación que un CERT los brinde todos, el único indispensable para un CERT es el de comunicados; y a medida que el CERT crezca puede implementar más servicios.

Centro de datos [L1] [E1]

Un centro de datos es una estructura o parte de una estructura cuyo objetivo es albergar todos los sistemas de información de una empresa y sus componentes asociados. El propósito de un centro de datos es mantener en línea y siempre disponible para los usuarios todos los servicios de la red, esto se logra con la planeación, el orden y la aplicación de normas y estándares con las que se diseña un centro de datos. Un centro de datos ayuda y facilita: el crecimiento, seguimiento y solución de fallas, actualización y mantenimiento. Además ayuda a mejorar el rendimiento en ventilación y a optimizar el espacio.

[9] US-CERT: Cert de los Estados Unidos de Norteamérica.

Tipos de centro de datos [E1]

La norma TIA-942, clasifica a los centro de datos en cuatro grupos llamados “tiers” que van desde *tier* I, siendo este el más simple, hasta *tier* IV que es más complejo. El *tier* se refiere al porcentaje anual de presencia que alcanza el centro de datos, o lo que es lo mismo, al nivel de tolerancia a fallas de la infraestructura del centro de datos. Un mayor porcentaje de presencia significa que puede soportar un mayor número de eventos, ya sean planeados o imprevistos sin que se produzca una parada en su funcionamiento, lo que se conoce como disponibilidad. Para clasificar un centro de datos se considera cuatro subsistemas independientes:

- Arquitectónico
- De Telecomunicaciones
- Eléctrico, y
- Mecánico

Cada subsistema es clasificado de manera independiente dentro de una categoría (*tier*), y la clasificación global del centro de datos será igual a la del subsistema con el menor número de *tier*. La tabla 1.1 muestra un resumen de porcentaje de parada y disponibilidad de los diferentes tipos de centro de datos.

TIER	% Disponibilidad	% de parada	Tiempo de parada al año	Tiempo promedio de implementación[10]
Tier I	99.671	0.329	28.82 horas	3 meses
Tier II	99.741	0.251	22.68 horas	3 a 6 meses
Tier III	99.982	0.018	1.57 horas	15 a 20 meses
Tier IV	99.995	0.005	52.56 minutos; 0.4 horas	15 a 20 meses

Tabla 1.1: Características de los diferentes tipos de centros de datos [E1]

[10] Tiempo según *TE Connectivity, Ltd.* Suiza

1.3. METODOLOGÍA Y HERRAMIENTAS

1.3.1. METODOLOGÍA

Para la elaboración del presente proyecto se utilizará la metodología sistemática, la cual divide el proyecto en dos etapas: análisis de requerimientos y diseño. Esta metodología permite definir los pasos que se deben seguir en la elaboración de cada etapa.

1.3.1.1. Análisis de requerimientos

En esta etapa se elabora un análisis de los requisitos del EcuCERT para su centro de datos. En base a información facilitada por la Supertel se procede a determinar en primer lugar los requerimientos funcionales. Estos requerimientos son determinados mediante la elaboración de casos de uso para cada servicio del EcuCERT, y permiten determinar las aplicaciones o servicios que correrán en la red.

Posteriormente se determinan los requerimientos de capacidad necesarios para cada aplicación. Estos requerimientos se refieren a las capacidades de CPU[11], memoria RAM, disco duros, y velocidad de enlace. Para determinar estos requisitos se establecen perfiles de usuarios, usuarios por servicios, clasificación de los servicios por su interacción con el usuario, tiempos de respuesta y velocidades de enlace estimadas. Finalmente se determinan los requerimientos de disponibilidad y seguridad. Los requerimientos de disponibilidad se refieren al porcentaje anual en el que el servicio es asequible y están dados por el nivel de *tier*, y los requerimientos de seguridad ayudan a la hora de elegir que protocolos deben soportar los equipos.

1.3.1.2. Diseño

La etapa de diseño se basa en los requerimientos identificados en el “análisis de requerimientos”. El diseño se divide en tres partes: diseño de la red, selección de equipos y diseño del espacio del centro de datos. El diseño de la red se apoya en la arquitectura SAFE de Cisco. La selección de equipos se basa en los requeri-

[11] Unidad central de procesamiento por sus siglas en inglés. Es el procesador de la máquina.

mientos del capítulo 2 y en el diseño de la red. Finalmente el diseño del espacio del centro de datos se basa en la norma EIA/TIA-942.

1.3.2. HERRAMIENTAS

1.3.2.1. Norma TIA-942 [E1]

El estándar "*EIA/TIA-942 Telecommunication Infrastructure Standard for Data Centers*" de *Telecommunications Industry Association's*, especifica los requerimientos mínimos para la infraestructura de centros de datos. El propósito de este estándar es proporcionar los requisitos y directrices para el diseño e instalación de un centro de datos, con el fin de unificar criterios en el diseño de áreas de centro de datos y cuarto de cómputo.

Para lograr una mejor organización y facilitar la clasificación de un centro de datos, el estándar TIA-942 divide la infraestructura de un centro de datos en cuatro subsistemas: telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico; cada subsistema se encarga de una serie de ítems como los que se muestra en la Tabla 1.2.

El estándar TIA-942 se basa en una serie de especificaciones y lineamientos, que se deben seguir para clasificar los diferentes subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar. En su anexo G (informativo) establece cuatro niveles (*Tiers*) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99,995%. Los principales aspectos que debe considerar, de manera general todo centro de datos en su diseño son:

- Estándares basados en sistemas abiertos.
- Alto rendimiento y gran ancho de banda que incluya factores de crecimiento.
- Soporte para velocidades de transmisión de 10G o superiores.
- Soporte para *storage devices*[12].
- Soporte para convergencia con factor de crecimiento incorporado.
- Alta calidad, confiabilidad y escalabilidad.
- Redundancia.

[12] Dispositivos de almacenamiento como fibra channel, SCSI, NAS

- Alta capacidad y densidad.
- Flexibilidad y capacidad de expansión, que facilite los movimientos, cambios e incorporaciones de nuevos equipos.

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de rack	Selección del sitio	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Tipo de construcción	Puntos únicos de falla	Presión positiva
Cuarto de entrada	Protección ignifuga	Cargas criticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chillers
Backbone	Barrera de vapor	Topología de UPS	CRAC's y condensadores
Cableado horizontal	Techos y pisos	PDU's	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendios
Alimentación redundante	NOC	EPO (Emergency Power Off)	Sprinklers
Patch panels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV	*Switches* de trasferencia eléctrica	

Tabla 1.2: Ítems por subsistema [W7]

De esta forma se tiene que los cuatro niveles *tiers* que plantea el estándar se corresponden con cuatro niveles de disponibilidad. Las recomendaciones propuestas en este estándar son independientes del tamaño del centro de datos, por lo que se adaptan al centro de datos del EcuCERT. Actualmente es estándar TIA-942 cuenta con dos *addendums* publicados, TIA-942-1 y TIA-942-2.

TIA-942-1 (Addendum 1)

"Data center coaxial cabling specifications and application distances." Fue publicado en 2008. Provee especificaciones adicionales para conectores de cables coaxiales usados para circuitos T-3, E-1, y E-3. Además se permite distancias de cableado horizontal más largas para el uso de cable coaxial desde el Área de distribución principal (MDA).

TIA-942-2 (Addendum 2)

"*Additional guidelines for data centers*." Fue aprobado a finales del 2009, es la última revisión del estándar.[13] Proporciona nuevas directrices en una gran variedad de temas, el más importante es el de mejorar la eficiencia de la energía. Los principales cambios introducidos por este addendum son:

- Se especifica un rango más amplio de temperaturas y humedad en centro de datos basados en las directrices de la *American Society of Heating, Refrigeration and Air Conditioning Engineers* (ASHARE) publicados en 2008.
- Se especifica un nuevo protocolo con tres niveles de iluminación para reducir el uso de energía.
- Se añade la categoría 6A como medio soportado y se lo señala como el medio recomendado para par trenzado balanceado.
- Alta orientación a consultar con los fabricantes de equipos relacionados con las fuentes de radio (*wireless* LANs, teléfonos celulares, radios portátiles, etc.) en las salas de computadoras y sala de entrada.

[13] En el 2013 se aprobó la nueva revisión llamada TIA-942-A, la cual incluye los dos adendums ya mencionados junto con nuevos cambios principalmente en eficiencia energética.

- Guía referencial para actualizar de *Tiering* a un centro de datos.

1.3.2.2. Arquitectura SAFE [L5]

La arquitectura SAFE es una propuesta de Cisco Systems, Inc.[14] Se trata de una guía de mejores prácticas para el diseño e implementación de redes seguras. SAFE propone un diseño modular, con lo cual se limita el alcance de los ataques informáticos, se permite que cada módulo sea asegurado por separado y de acuerdo a su importancia, facilita la actualización de la infraestructura de red, la cual puede ser llevada a cabo solo en los módulos necesarios y presenta un diseño de red redundante. Los módulos que propone SAFE son:

- Módulo de *core*
- Módulo del centro de datos intranet
- Módulo perimetral a internet
- Módulo de campus
- Módulo de administración y monitoreo de red

1.3.2.3. Recomendaciones Amparo [L1]

La herramienta final para la elaboración del presente proyecto es el "*Manual básico de Gestión de incidentes y seguridad informática, 2012.*" El cual es un conjunto de mejores prácticas para la implementación y puesta en funcionamiento de CSIRTs realizado por el proyecto Amparo de la LACNIC[15]. Unos de los aspectos que considera dicho manual es la infraestructura de centro de datos y red, estableciendo diferentes modelos según la necesidad y tamaño del CSIRT a implementar. Se eligió esta herramienta sobre muchas otras parecidas, debido a que al ser desarrollada por LACNIC se adapta más a la realidad del EcuCERT.

---

[14] Cisco Systems es una empresa de los Estados Unidos de Norte América, que se dedica al diseño, fabricación y venta de equipos de networking.

[15] LACNIC, Latin American and Caribbean Internet Addresses Registry, es la encargada de administrar las direcciones IP versión 4 y 6, y otros recursos de red para la región

CAPÍTULO 2

ANÁLISIS

El desarrollo del presente proyecto considera el análisis de la situación actual y el análisis de requerimientos. El análisis de la situación actual se limita a la mención de la consultoría entregada por la Supertel, debido a que se trata de un proyecto nuevo, que todavía no cuenta con ninguna infraestructura que pueda ser objeto de un "análisis de situación actual." En la consultoría se define: el número estimado de usuarios, los servicios que brindará el EcuCERT y los procesos que involucran. La consultoría además incluye las historias de usuarios que fueron realizadas durante los talleres; se cuenta con una historia de usuario para cada servicio del EcuCERT.

El análisis de requerimientos incluye: requerimientos funcionales, de capacidad, y de seguridad. En el presente capítulo se lleva a cabo el análisis de requerimientos funcionales y de capacidad, además se mencionan los requerimientos de seguridad. El análisis de requerimientos funcionales se basa en la consultoría facilitada por la Supertel y en lo que se conoce como historias de usuario. A partir de esa información, se procede a la elaboración de diagramas de casos de uso, con los que se determinan los requerimientos funcionales. Los requerimientos funcionales permiten determinar las aplicaciones que correrán en la red. Para el caso de telefonía o red de voz, el EcuCERT utilizará la red actual de la Supertel, por lo que esta no se diseña en el presente proyecto.

Los requerimientos de capacidad se refieren a las capacidades de CPU, memoria RAM, disco duro, y velocidad de red. Los requerimientos de capacidad son determinados estableciendo: perfiles de usuarios, usuarios por servicio, la clasificación de los servicios por su interacción con el usuario, y velocidades de enlace. En base a esos parámetros se clasifica las capacidades de CPU, RAM y velocidad de enlace, para cada aplicación de la red del EcuCERT, dentro de una categoría que puede ser alta, media o baja. Estas categorías están en función del presupuesto con que cuenta el EcuCERT. Por último se tiene los requerimientos de seguridad, de los que solo se realizará una breve mención ya que requerirían de un análisis

completo de “evaluación y gestión de riesgos” utilizando metodologías como Octave[16], lo cual está fuera del alcance del presente proyecto.

2.1. REQUERIMIENTOS FUNCIONALES [S1]

Para establecer los requerimientos funcionales, se utilizó lo que en las metodologías de desarrollo de software se conoce como “historias de usuario”.[17] Las historias de usuario forman parte de la consultoría facilitada por la Dirección Especial de Investigación de la Supertel (ver anexo A). A partir de las historias de usuario se procedió a realizar los “casos de uso”[18]. Los casos de uso permiten determinar los actores que existen en el sistema y las diferentes interacciones entre ellos, así como las diferentes aplicaciones que deben correr en la red. A continuación se muestran los casos de uso por servicio del EcuCERT.

2.1.1. ALERTAS Y ADVERTENCIAS [L1] [L6] [W2] [W5]

El servicio de alertas y advertencias es un servicio reactivo, el cuál se refiere a enviar información que describa: un ataque por parte de un intruso, una vulnerabilidad, una alerta, un virus o un caso de engaño (ingeniería social), y proporcione una guía corta para lidiar con el problema resultante. Esta alerta o aviso es enviada como una reacción al problema que se presenta para notificar sobre el mismo y/o brindar una solución para proteger o recobrar los sistemas.[W2]

La figura 2.1 muestra el caso de uso del servicio Alertas y advertencias. El caso de uso de este servicio parte del sistema de monitoreo. El sistema de monitoreo es el encargado de recibir “*logs*” de los equipos de seguridad de los clientes como *firewalls* e IDS/IPS, y almacenarlos en el servidor local. Además el sistema de monitoreo analiza los *logs* recibidos en busca de patrones de ataques conocidos, y en caso de detectar un ataque activa una alarma para notificar al funcionario. El sistema también permite el posterior análisis de los *logs* y es utilizado en varios de los servicios del EcuCERT.

---

[16] Operational Critical Threat Asset and Vulnerability Evaluation, es una metodología del análisis de riesgo.
[17] Un ejemplo de este tipo de metodología es la XP, eXtreme Programming.
[18] Casos de uso es una descripción de las actividades que se deben llevar a cabo para realizar un proceso.

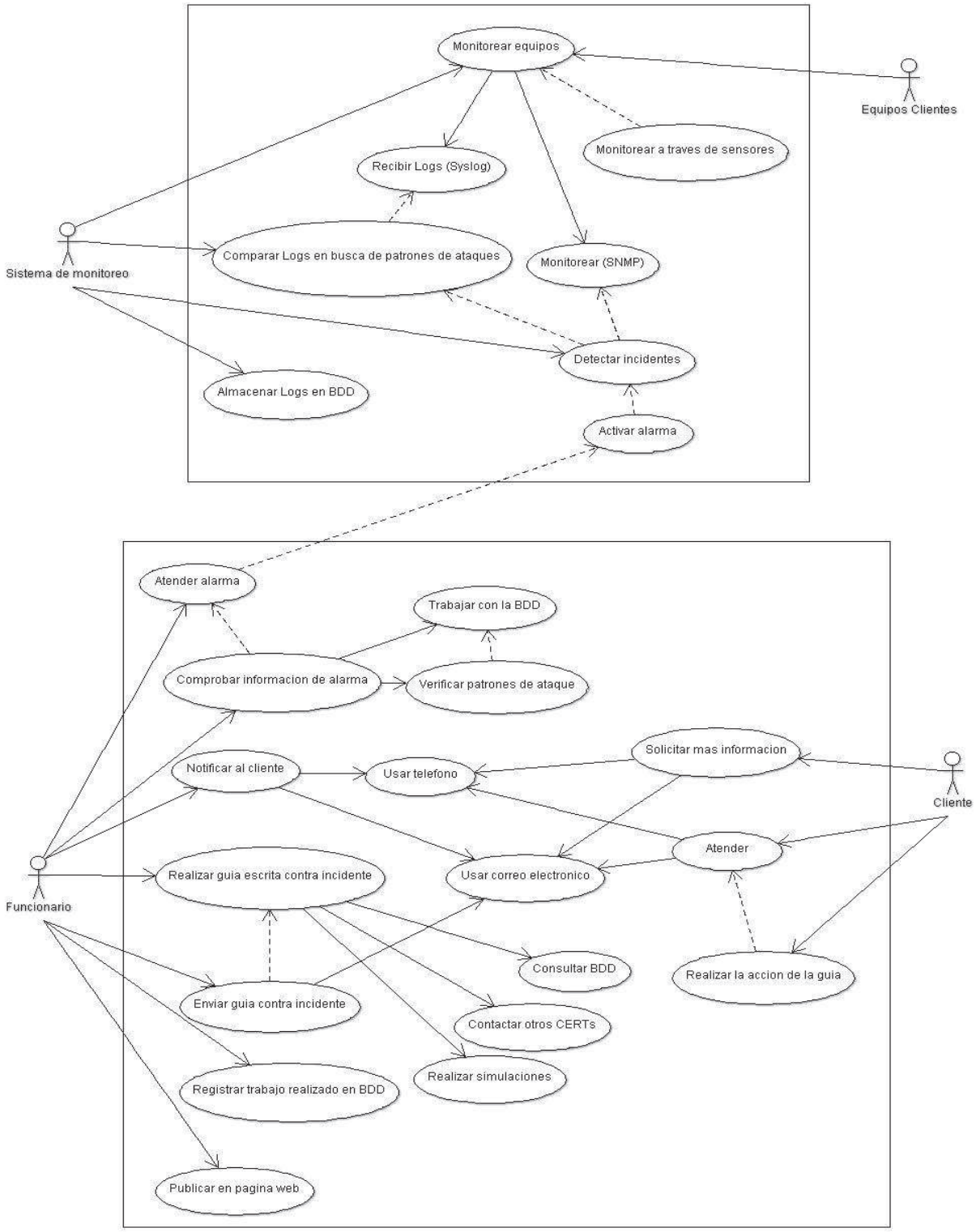

Figura 2.1: Caso de uso Alertas y advertencias

El sistema de monitoreo utilizará *logs* en formato “Syslog” que es un estándar libre para *logs* en el mercado. En algunos casos el sistema de monitoreo deberá contar con equipos sensores en las instalaciones del cliente, debiéndose realizar un es-

tudio para cada cliente en particular, lo que está fuera del alcance del presente proyecto. El proyecto actual únicamente dimensiona el servidor central que recibirá, procesará y almacenará los *logs* (ver capítulo 3).

En la segunda parte del caso de uso “alertas y advertencias” se tiene dos actores funcionario y cliente. El funcionario es alertado por el sistema de monitoreo, revisa los *logs* para confirmar la información, y se contacta con el cliente vía telefónica y/o correo electrónico. Además el funcionario debe realizar una guía que ayude al cliente a lidiar con el problema, para lo cual se vale de información de la base de datos, consulta a otros CERTs y/o realiza simulaciones. El funcionario puede publicar información en la página web, (si no se trata de información confidencial) sobre el ataque. Del diagrama de caso de uso se determina que las aplicaciones necesarias para este servicio son:

- Correo Electrónico.
- Página web.
- Sistema de monitoreo
- Base de datos
- Servidor de aplicaciones

2.1.2. MANEJO DE INCIDENTES [L1] [L6] [W2] [W5] [S1]

El manejo de incidentes es un servicio reactivo, el cual se refiere al tratamiento y proceso que se le da a un incidente una vez que es reportado al EcuCERT [W2]. Este proceso varía de acuerdo al CERT, para el caso del EcuCERT se tiene: Entrada y/o detección del incidente, registro, triage[19] (involucra clasificación y diagnóstico), resolución (análisis y respuesta) y cierre.[S1]

El servicio “Manejo de incidentes” es obligatorio para todo CERT o Csirt[L1]. En la figura 2.2 se puede observar el caso de uso de este servicio. El manejo de incidentes cuenta con tres actores, dos actores humanos: funcionario y cliente; y un sistema llamado sistema de monitoreo. El manejo de incidentes requiere que un

[19] Se refiere a clasificar “algo” para ser atendido de acuerdo a un diagnóstico con el fin de alcanzar un objetivo final. No existe un equivalente en español del termino *triage*, el más parecido es clasificación.

incidente sea detectado previamente. Para el caso del EcuCERT esto pude suceder de tres formas.

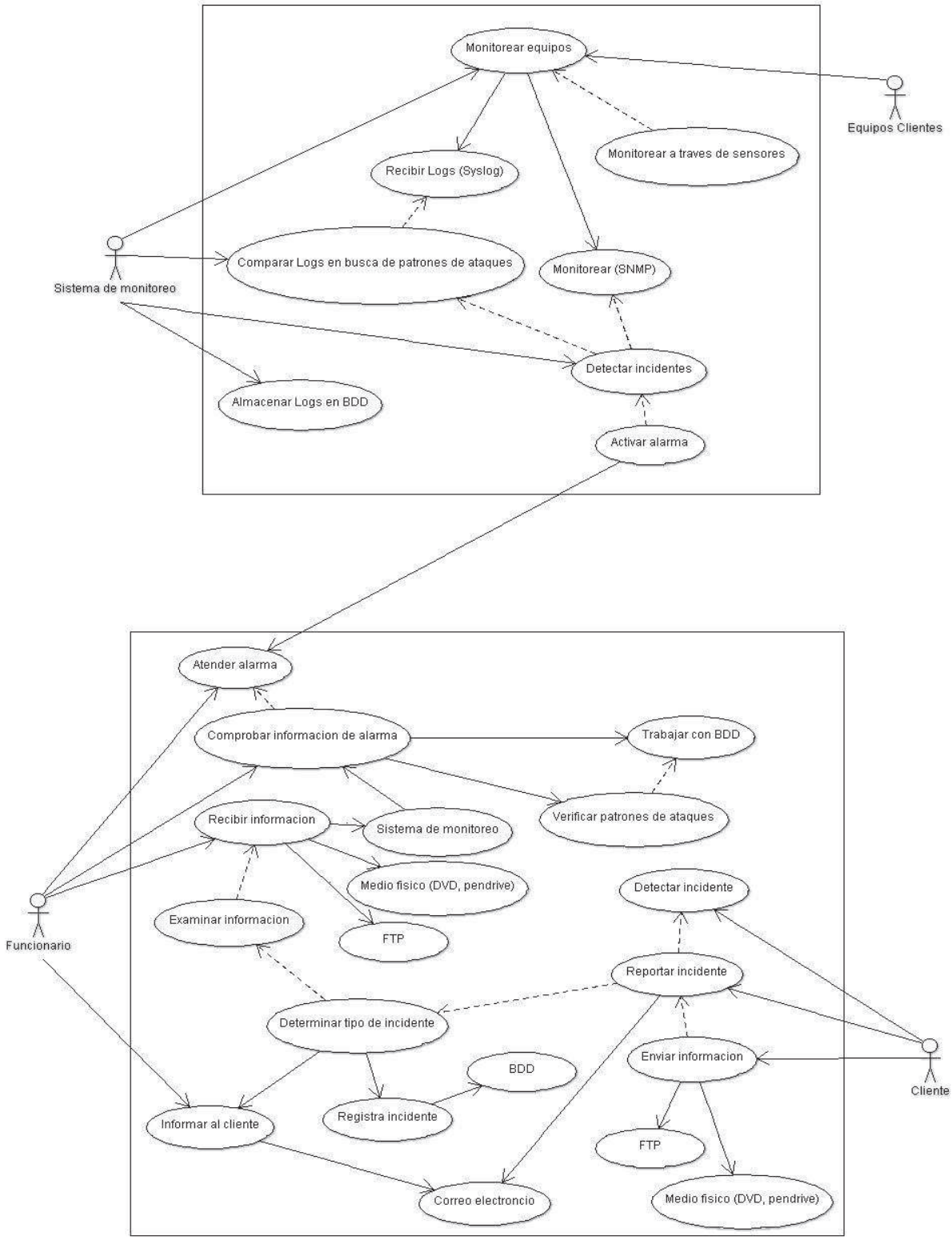

Figura 2.2: Caso de uso Manejo de incidentes

La primera, es cuando el sistema de monitoreo detecta un patrón que coincide con algún ataque conocido y lo reporta al funcionario activando su alarma. La segunda, es cuando el cliente detecta algún tipo de incidente y lo reporta al EcuCERT, en busca de ayuda para solucionarlo. Y la tercera, es cuando el funcionario del EcuCERT detecta un incidente al revisar la información que envía el cliente.

Una vez que un incidente es detectado, mediante cualquiera de las tres formas ya mencionadas, el funcionario del EcuCERT debe registrar el incidente, almacenar toda la información que se envió y/o recibió junto con el incidente, y contactar al cliente. La información debe ser almacenada por un periodo de seis a doce meses según los requerimientos de la Supertel. Del diagrama de casos de uso de la figura 2.2 se obtienen las aplicaciones necesarias para este servicio, las cuales son:

- Correo electrónico
- Servidor de monitoreo
- Servidor de base de datos
- Servidor de *storage*
- Servidor de aplicaciones
- Servidor ftp

2.1.3. GESTIÓN DE VULNERABILIDADES [L1] [L6] [W2] [W5]

La gestión de vulnerabilidades es un servicio reactivo que involucra el recibir información y reportes de vulnerabilidades de hardware y software. Con esta información se analiza la naturaleza, los mecanismos y efectos de estas vulnerabilidades, y se desarrollan estrategias de respuesta para detección y reparación de las mismas.[W2]

Como se aprecia en la figura 2.3 el caso de uso del servicio “Gestión de vulnerabilidades” involucra dos actores: funcionario y cliente. El funcionario del EcuCERT recibe la información enviada por el cliente para el análisis de vulnerabilidades; registra y almacena dicha información en el sistema y bases de datos. La información permanecerá almacenada por un periodo de seis a doce meses. El análisis de vulnerabilidades requerirá altas capacidades de procesamiento, según los estimados de la Supertel, ya que un solo caso puede tener varias decenas de *gi-*

gabytes de información. El contacto entre funcionario del EcuCERT con el Cliente, se dará por medio de correo electrónico. La transferencia de archivos se la podrá hacer de manera personal usando medios ópticos o magnéticos o haciendo uso del servidor *ftp*. De la descripción anterior se determina que las aplicaciones necesarias para este servicio son:

- Servidor de aplicaciones
- Servidor ftp
- Servidor de base de datos
- Servidor de *storage*
- Correo electrónico

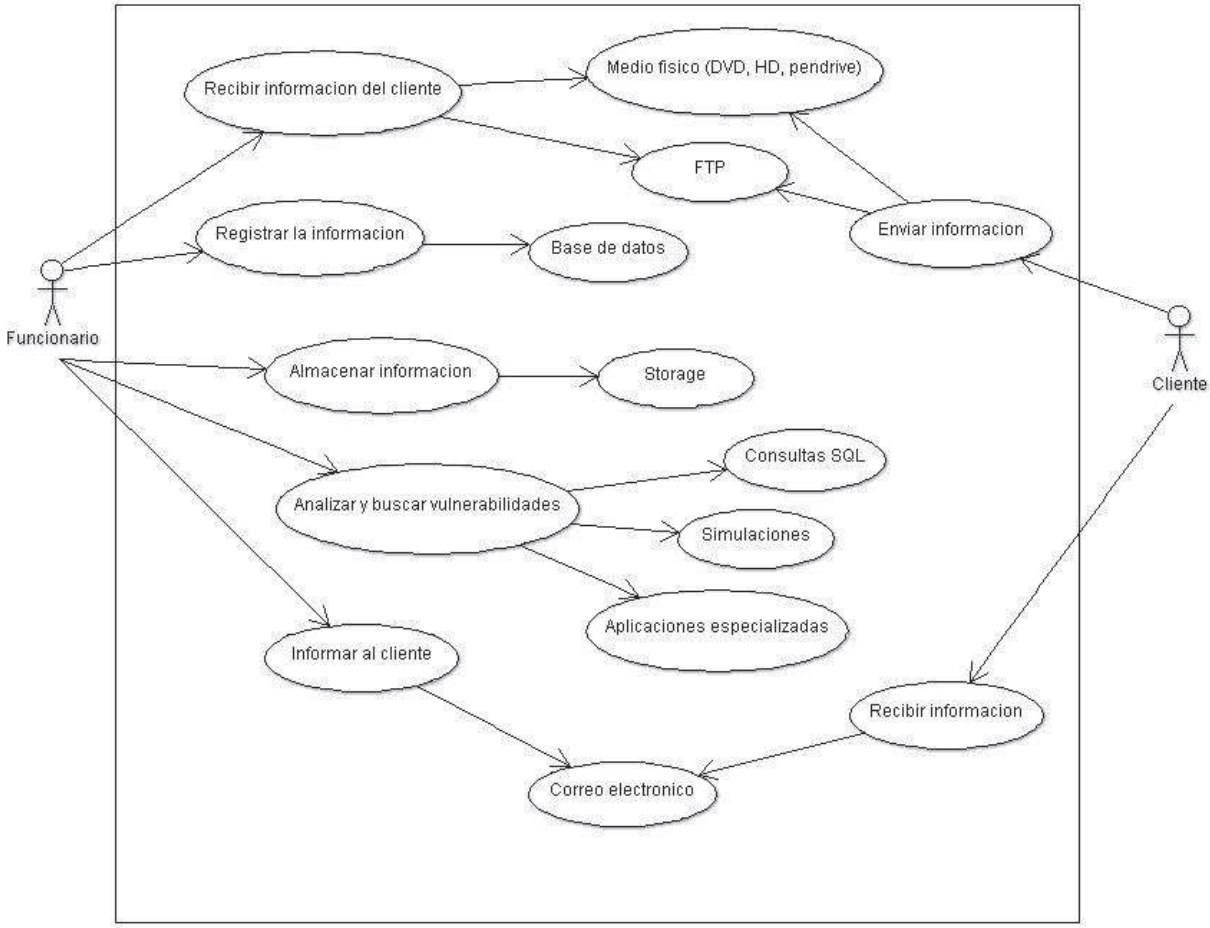

Figura 2.3: Caso de uso gestión de vulnerabilidades

2.1.4. ANUNCIOS [L1] [L6] [W2] [W5]

El servicio de “anuncios” es un servicio proactivo, se refiere a cualquier publicación que haga el EcuCERT como por ejemplo alertas de intrusos, alertas de vulnerabilidades, avisos de seguridad, etc. Estos anuncios informan a la comunidad acerca de nuevos desarrollos descubiertos. [W2]

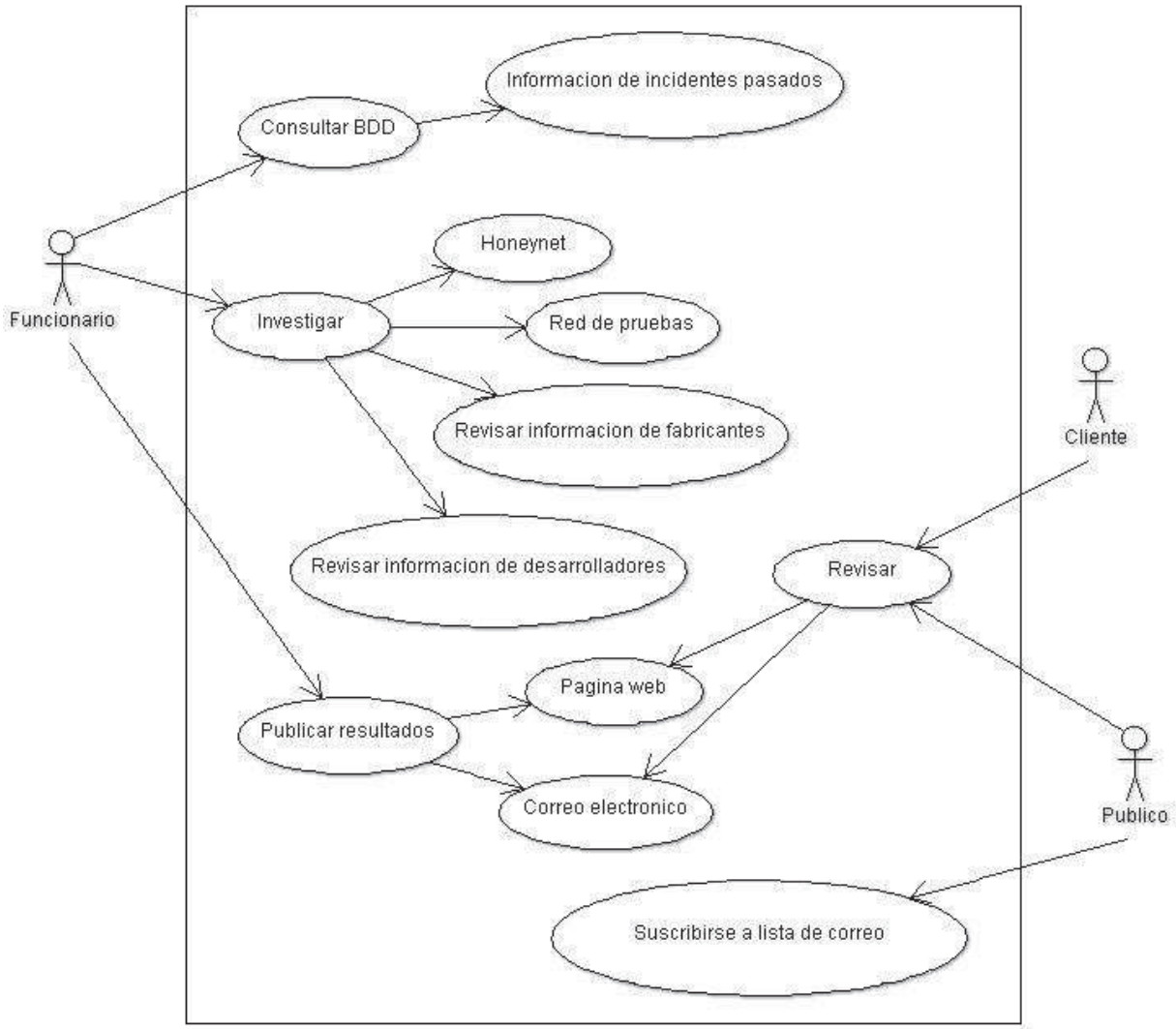

Figura 2.4: Caso de uso anuncios

La figura 2.4 muestra el diagrama de caso de uso del servicio “Anuncios”. El servicio de anuncios se trata de un servicio de carácter informativo, y de investigación. Cuenta con tres actores: el funcionario del EcuCERT, cliente y público en

general. Los anuncios serán vía web o correo electrónico. Las aplicaciones necesarias para este servicio son:

- Correo electrónico
- Servidor WEB
- Red de pruebas
- *Honeynet*
- Base de datos

En la figura 2.5 se puede apreciar el caso de uso de la *Honeynet. Honeynet* es una red trampa, diseñada especialmente para ser atacada y obtener información sobre los ataques. No se debe usar para ningún otro propósito, y debe ser independiente de la red del EcuCERT.

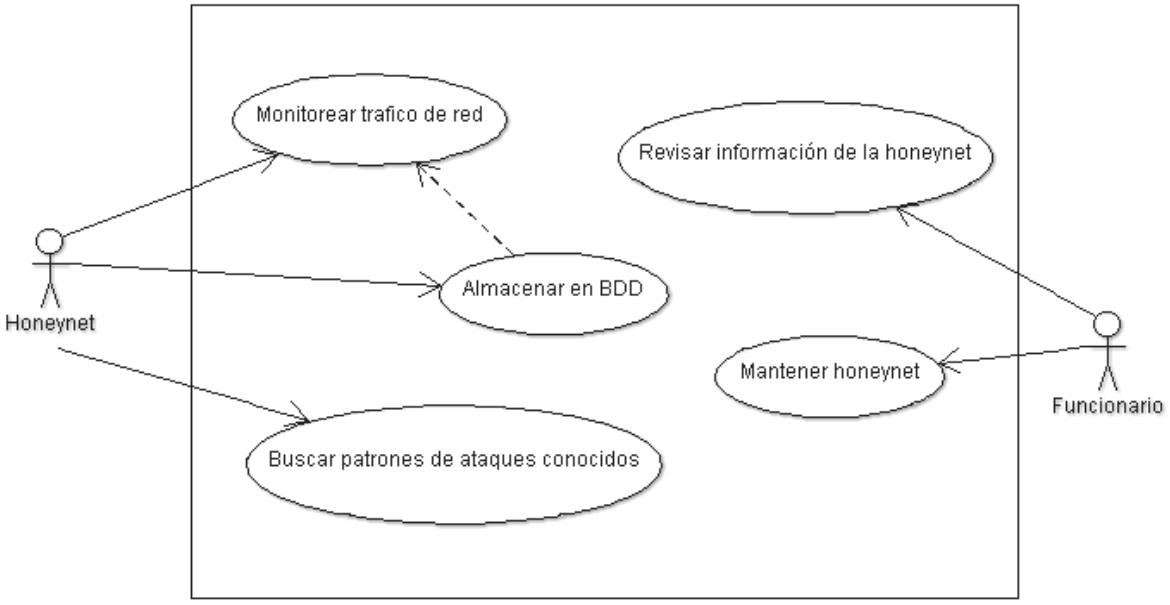

Figura 2.5: Caso de uso de Honeynet

2.1.5. DESARROLLO DE HERRAMIENTAS DE SEGURIDAD [L1] [L6] [W2] [W5]

El servicio de "desarrollo de herramientas de seguridad" es un servicio proactivo, se trata del desarrollo de herramientas para la comunidad del EcuCERT. Pueden ser parches de herramientas ya existentes o ser una herramienta completamente nueva.[W2]

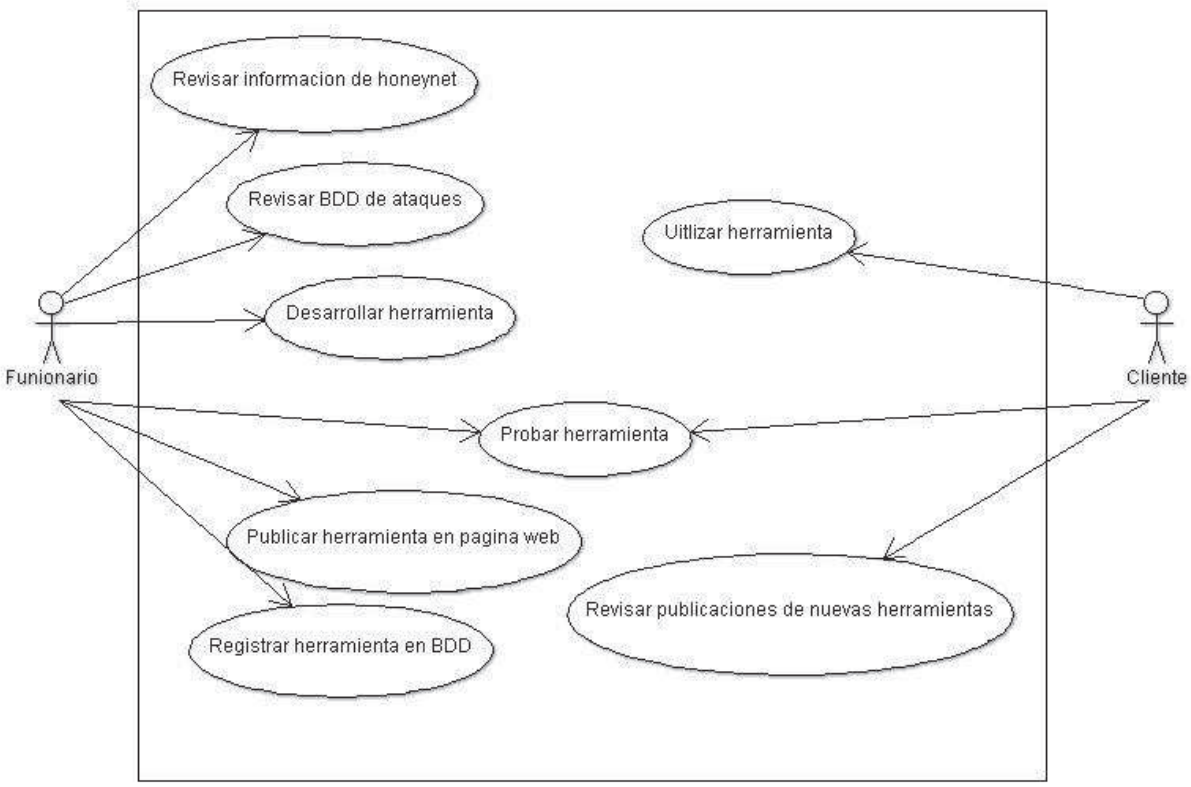

Figura 2.6: Caso de uso Desarrollo de herramientas de seguridad

En la figura 2.6 se observa el diagrama de caso de uso del servicio de "Desarrollo de herramientas de seguridad". Para este servicio se cuenta con cuatro actores:

- Funcionario.
- Cliente
- *Honeynet*
- Red de pruebas

La *honeynet*[20], actuará como un sistema que recopilará información, sobre atacantes, y la forma en que estos realizan sus ataques. El funcionario será el encargado de analizar la información de la *honeynet*; y junto con la información de otros ataques a clientes, y reportes de otros CERTs o Csirts, desarrollará herramientas

[20] Honeynet según Lance Spitzner, fundador del Proyecto Honeynet, es una red de honeypots de alta interacción, que simula una red de producción real, y que está especialmente diseñada para ser atacada y recabar así mucha información sobre posibles atacantes.

que ayuden a combatir, evitar o prevenir estos ataques. Todas las herramientas entrarán a un periodo de prueba, para lo cual se utilizará la red de pruebas con que contará el EcuCERT. Finalmente la herramienta será publicada en la página web o entregada directamente a los clientes de ser el caso. Además se almacenará la herramienta así como toda la información relativa a esta, como documentación, versiones previas, registro de la herramienta desarrollada en la base de datos, etc. Las aplicaciones o servidores necesarios para brindar este servicio son:

- Página web
- *Honeynet*
- Red de pruebas
- Servidor de aplicaciones
- Servidor de base de datos
- Servidor *storage*

2.1.6. DETECCIÓN DE INTRUSOS [L1] [L6] [W2] [W5]

El servicio de "Detección de intrusos" es un servicio proactivo. Los CERTs que realicen este servicio, revisan y analizan *logs* de diferentes equipos como *firewalls*, IDS, IPS y en caso de encontrar una amenaza inician una acción coordinada con el cliente para lidiar con la misma [W2].

El caso de uso del servicio de "Detección de intrusos" se observa en la figura 2.7. Como se puede apreciar los actores que intervienen en este servicio son: funcionario, y cliente. Este servicio funciona de dos maneras, en la primera el cliente entregará al funcionario del EcuCERT información correspondiente a *logs* de diferentes equipos de seguridad, usando para ello medios ópticos o magnéticos, o mediante transmisión ftp. En la segunda esta información es recopilada directamente por el sistema de monitoreo con que cuenta el EcuCERT. En cualquiera de los dos casos mencionados, cuando el funcionario reciba la información, esta será sometida a un análisis forense, dicho análisis se lo llevará a cabo en el laboratorio de análisis forense, el cual contará con sus propios equipos para el análisis y no es parte del diseño del centro de datos.

Figura 2.7: Caso de uso detección de intrusos

La infraestructura del centro de datos se utilizará para registrar en la base de datos todo lo que se hace, así como para almacenamiento por un periodo de 6 a 12 meses [S1] de toda la información con que se cuenta.

Las aplicaciones necesarias para este servicio son:

- Servidor de base de datos
- Servidor de *storage*
- Servidor ftp
- Servidor de monitoreo
- Servidor de aplicaciones

2.1.7. EDUCACIÓN Y ENTRENAMIENTO [L1] [L6] [W2] [W5]

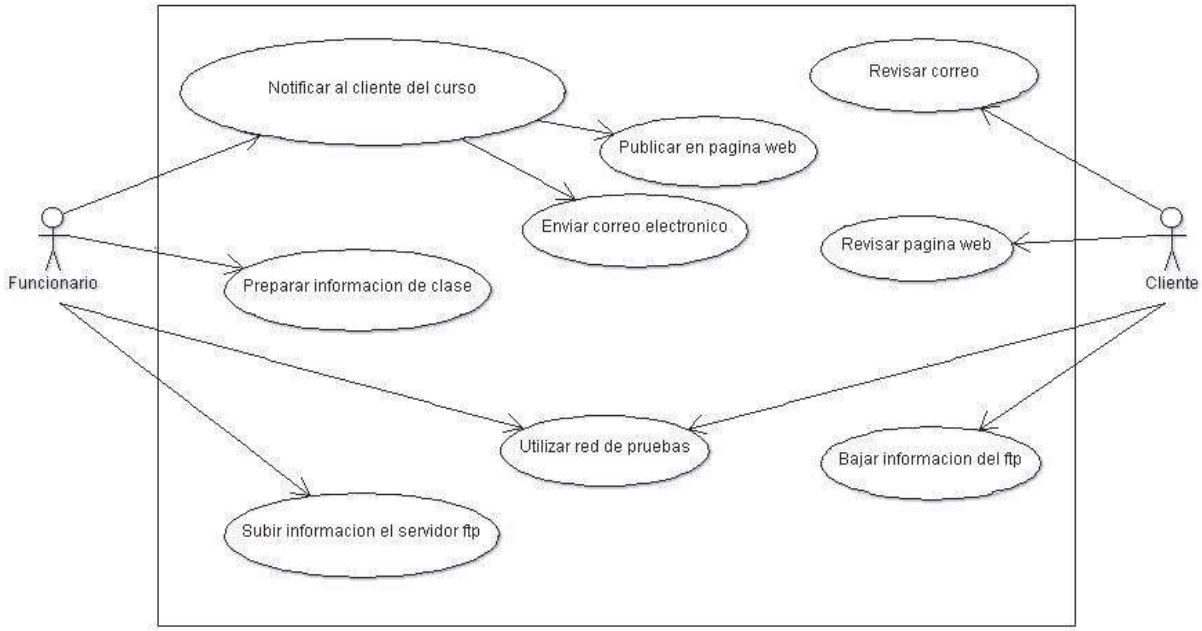

Figura 2.8: Caso de uso educación y entrenamiento

El servicio de "Educación y entrenamiento" provee a la comunidad del EcuCERT de material que ayude a mejorar su seguridad. Esta información puede incluir contenido de terceros tales como: otros equipos CERTs o Csirts, vendedores y expertos en seguridad. Para este servicio el EcuCERT puede ofrecer diferentes cursos de capacitación [W2]. La información publicada por el EcuCERT será:

- Información de contacto con el EcuCERT.
- Guías para comunicar un incidente a EcuCERT.
- Lista de alertas, advertencias, y otros anuncios.
- Documentación de las mejores y más actuales prácticas de seguridad.

- Políticas, procedimientos y *checklist* para mejorar la seguridad de la empresa.
- Estadísticas de las amenazas más comunes reportadas al EcuCERT.
- Guías generales de seguridad informática.

La figura 2.8 muestra el caso de uso del servicio “Educación y Entrenamiento”. Como se observa este servicio cuenta con dos actores, el funcionario y el cliente, que en este caso es un estudiante. El funcionario publicará en la página web, y hará uso del correo electrónico para promocionar el curso. Durante el curso se utilizará el servidor web que puede contar con un aula virtual, el servidor ftp será usado para descarga de archivos y material (de gran tamaño si se da el caso) y la red de pruebas para realizar diferentes actividades de entrenamiento. Para este servicio el EcuCERT, necesita: servidor web, servidor de correo, servidor ftp y red de pruebas, además se debe contar con aulas equipadas con 25 PCs, una para cada estudiante [S1].

2.1.8. APLICACIONES POR SERVICIO DEL ECUCERT

Como resultado de los requerimientos funcionales se obtuvo las aplicaciones que correrán en la red. En la tabla 2.1 se pueden apreciar los servicios del EcuCERT y la aplicación que necesita cada uno.

2.2. REQUERIMIENTOS DE CAPACIDAD

Los requerimientos de capacidad se refieren a las características de capacidad de procesador, memoria RAM, disco duro y velocidad de red necesarias para cada servicio del EcuCERT. El proceso que se utiliza es el siguiente:

a) Elaboración de perfiles de usuario, de acuerdo a la actividad o cargo que desempeñan en el EcuCERT.
b) Establecer las aplicaciones o servicios necesarios para cada perfil de usuario.
c) Clasificar las aplicaciones de la red por el tipo de interacción con el usuario.
d) Establecer niveles esperados de crecimiento.
e) Establecer los parámetros necesarios para el dimensionamiento del enlace a internet.

f) Clasificar los requerimientos de CPU, RAM, E/S en tres categorías: alta, media y baja.

	Reactivos			Proactivos			
	Alertas y advertencias	**Manejo de incidentes**	**Gestión de vulnerabilidades**	**Anuncios**	**Desarrollo de herramientas de seguridad**	**Detección de intrusos**	**Educación y entrenamiento**
Correo	Si	Si	Si	Si	Si	Si	Si
Web	Si	Si	Si	Si	Si	Si	Si
Aplicaciones	Si	Si	Si	Si	Si	Si	Si
Base de datos	Si	Si	Si	Si	Si	Si	Si
Storage	Si	Si	Si	Si	Si	Si	Si
FTP	Si	Si	Si	Si	Si		Si
Red de prueba (virtual)	Si	Si	Si	Si	Si	Si	Si
Honeynet	Si		Si	Si	Si	Si	Si
Servidor de monitoreo	Si					Si	

Tabla 2.1: Aplicaciones necesarias por servicio del EcuCERT

2.2.1. PERFILES DE USUARIO [S1]

Los perfiles de usuario están en función de la actividad que realizan, por lo se dividen en seis grupos principales: personal administrativo, personal técnico, clientes, visitantes del sitio web, estudiantes y equipos monitoreados. Los perfiles de usuarios, están basados en la consultoría entregada por la Supertel y en los diagramas de casos de uso del punto 2.1. En la tabla 2.2 se puede apreciar los diferentes perfiles de usuarios, su número estimado y su descripción.

Perfil de usuario	Usuario	N° usuarios[21]	Descripción
U1	Personal técnico	10	Es la persona que trabaja para el EcuCERT, y cuya herramienta de trabajo son los servidores con los que cuenta la red, el uso que hace de los servidores es muy alto. Aprovecha al máximo la capacidad de los servidores en horario 24/7.
U2	Personal administrativo	3	Son las personas encargadas de las tareas administrativas del EcuCERT. El uso que harán de los servidores es solo para tareas administrativas, pero de manera continua durante las horas de trabajo.
U3	Cliente	25	Es el personal de las empresas clientes del EcuCERT. Pueden hacer uso del servicio en horario 24/7.
U4	Visitante página web	100 (simultáneos máximo)	Es un usuario que accede a ciertos servicios disponibles para todo público como la página web. Puede ser en horario 24/7
U5	Estudiante de curso de capacitación	500[22] (25 simultáneos cursos)	Son las personas que acudirán a los cursos de capacitación que ofrezca el EcuCERT. Se les permitirá un perfil especial con acceso a ciertos servicios por un periodo de 6 a 12 meses[S1]
U6	Equipo monitoreado	100 (4 por cliente)	Se refiere a los equipos de networking y seguridad que el EcuCERT monitoreará. Se podrá monitorear un máximo de 4 equipos por cliente. Es el perfil de uso más alto, ya que estos equipos enviarán gran cantidad de datos de forma permanente.

Tabla 2.2: Perfiles de usuario [S1]

Para el dimensionamiento de los equipos se analiza cada función o tarea realizada por el "personal técnico" para cada uno de los servicios del EcuCERT. Se considera los protocolos que serían necesarios para cada una de dichas actividades, y se clasifican los componentes de CPU, RAM y red en una de tres categorías. Las categorías establecidas pueden ser:

[21] Estimado de usuarios de acuerdo a la Supertel
[22] Número de estudiantes promedio que se mantendrá en la base de datos del EcuCERT.

Servicio	Actividad realizada por el funcionario	*Seguridad			Parámetros	Clasificación	Protocolos utilizados
		C	I	D			
Sistema de monitoreo	Recibe logs y traps SNMP de clientes	Si	Si	Si	CPU	Alto	SSL (RSA, AES); Consultas SQL; decenas de gigas bytes de información; SNMPv3; varios equipos conectados al mismo tiempo
					RAM	Alto	
					RED	Alto	> 1 KB por segundo
	Compara y busca patrones	Si	Si	Si	CPU	Alto	SSL (RSA, AES); Consultas SQL; decenas de gigas bytes de información; SNMPv3; varios equipos conectados al mismo tiempo
					RAM	Alto	
					RED	Bajo	Busca en el servidor no ocupa la red
Alertas y advertencia	Comprueba información de alarma del sistema de monitoreo	Si	Si	Si	CPU	Alto	Consulta en BDD SQL varios gigas bytes; simulaciones
					RAM	Alto	Consulta en BDD SQL varios gigas bytes; simulaciones
					RED	Alto	Transmisión sobre la red de varios gigas bytes de información
	Informar al cliente	Si	Si	Si	CPU	Bajo	Correo seguro con PGP
					RAM	Bajo	Correo seguro con PGP
					RED	Medio	Correo seguro con PGP y archivos adjuntos.
	Realizar guía corta de incidente	Si	Si	Si	CPU	Alto	Consulta en BDD SQL varios gigas bytes; simulaciones
					RAM	Alto	Consulta en BDD SQL varios gigas bytes; simulaciones
					RED	Alto	Consulta en BDD SQL varios gigas bytes; simulaciones
	Enviar guía al cliente	Si	Si	Si	CPU	Bajo	Correo seguro con PGP
					RAM	Bajo	Correo seguro con PGP
					RED	Medio	Correo seguro con PGP y archivos adjuntos.

*C: Confidencialidad – I: Integridad – D: Disponibilidad

Tabla 2.3: Características de CPU, RAM y Red necesarios por actividad del EcuCERT

- Alta, cuando el usuario hace uso del servicio 24 horas del día, los 7 días de la semana (24/7), y lo ocupa en trabajos que requieren capacidad de procesamiento para varias decenas de *gigabytes* de datos. En esta categoría se utiliza protocolos que requieren de mucha memoria o CPU como protocolos de encriptación o consultas en bases de datos.
- Media, cuando la cantidad de información que se maneja es menor que en el caso anterior de varios *gigabytes* (pero sin llegar a la decena). En esta categoría se siguen ocupando protocolos de encriptación y consultas a bases de datos que consumen CPU y memoria RAM.
- Baja, es cuando la cantidad de información que se maneja es de pocos *megabytes* de tamaño.

A continuación se describe un ejemplo del análisis realizado para el servicio de "Alertas y advertencias", el cual incluye el sistema de monitoreo. En la tabla 2.3 se puede observar el resumen de las características para el servicio alertas y advertencias (la tabla completa se encuentra en el anexo B).

2.2.1.1. Perfil de uso para el servicio alertas y advertencias [L7] [W11] [W12]

2.2.1.1.1. Sistema de monitoreo

a) Recibir *logs* y *traps* SNMPv3

- <u>CPU: Alta</u>

Se necesita una capacidad de CPU "Alta", debido a que se trabaja con gran cantidad de datos. Se estima que el servidor de monitoreo reciba el equivalente de 1 KB de información por segundo por cada cliente. La información viajará por un canal seguro SSL[23] por lo cual se necesita de procesamiento para descifrar el tráfico, ya que SSL utilizará protocolos como RSA[24] para llaves públicas y AES[25] para el cifrado del tráfico.

Toda la información deberá ser almacenada en una base de datos SQL, por un periodo de mínimo 6 meses, y ser contrastada con los registros de ataques cono-

[23] SSL: Secure Socket Layer. Capa de conexión segura.
[24] RSA: Sistema criptográfico de clave pública.
[25] AES: Sistema de cifrado por bloques, para criptografía simétrica.

cidos. Además el servidor también receptará información del protocolo SNMPv3[26]. Todo el proceso mencionado consume mucho CPU, por lo cual la capacidad elegida es “Alta”.

- RAM: Alta

Como se menciona para el caso del CPU. Los protocolos que se utilizarán son SSL con RSA y AES, SNMPv3, y base de datos SQL. Estos protocolos demandan una “alta” capacidad de memoria RAM.

- Red: Alta

Debido al alto tráfico que manejará el servidor, se espera un mínimo de 1 KB por segundo por cada cliente; es necesario contar con una alta velocidad de enlace.

- Seguridad

- Confidencialidad: si
- Integridad: si
- Disponibilidad: si

Se necesitan los tres parámetros de seguridad mencionados en la metodología Octave. Debido a que se trata de información confidencial que puede ser utilizada en procesos judiciales, para resolver casos. Octave considera que el “no repudio” está incluido en la integridad

b) Comparación y búsqueda de patrones

- CPU: Alta

Una vez que la información es recibida debe ser almacenada en la base de datos SQL, y ser comparada con patrones de ataques conocidos para detectar incidentes, proceso que consume una alta capacidad de CPU.

- RAM: Alta

Para acelerar el proceso de trabajo con las base de datos, es preferible contar con grandes capacidades de memoria RAM.

[26] SNMPv3: Simple Network Management Protocol. Es un protocolo de capa de administración para el monitoreo de red.

- Red: Baja

Como la comparación de la información es local, no es necesaria una alta capacidad de red para esta actividad.

- Seguridad
- Confidencialidad: si
- Integridad: si
- Disponibilidad: si

Como se dijo anteriormente, es posible que esta información sea utilizada en procesos legales, por lo que debe garantizar estos tres parámetros durante todo el proceso.

2.2.1.1.2. Servicio alertas y advertencias

a) Comprobar la información de alarma

- CPU: Alta

Se escogió “alta”, ya que para esta actividad el funcionario del EcuCERT deberá consultar en la base de datos SQL, con el fin de comparar la información recibida con la de la base de ataques conocidos.

- RAM: Alta

De igual forma que para el procesador, el trabajar con base de datos SQL, requiere de gran cantidad de memoria RAM para agilitar el trabajo. Por lo que se escogió “Alta”

- Red: Alta

Debido que el funcionario accede a los servicios desde su computador personal, es necesario contar con una red de “Alta” velocidad para agilitar el trabajo.

- Seguridad
- Confidencialidad: si
- Integridad: si
- Disponibilidad: si

Se debe proporcionar todos los parámetros de seguridad en todo momento con el fin de mantener la cadena de custodia.

b) Informar al cliente

- CPU: Baja

El proceso de informar al cliente, implica el envío de correo electrónico seguro usando PGP desde la máquina del cliente, por lo que el servidor no necesita mayor procesamiento.

- RAM: Baja

Un servidor de correo con pocos usuarios como el del EcuCERT, no necesita demasiada RAM para funcionar.

- Red: Media

Debido a que el correo puede contener archivos adjuntos, es necesario contar con una velocidad de enlace de red “Media”, no es necesario alta ya que la mayoría de correo no contiene archivos adjuntos.

- Seguridad

- Confidencialidad: Si
- Integridad: Si
- Disponibilidad: Si

El proceso de informar al cliente requiere el uso de correo seguro con PGP, que garantice los parámetros de seguridad mencionados.

c) Realizar guía corta de incidente

- CPU: Alta

Se necesita de una capacidad de CPU alta, debido a que el usuario que realiza la guía, deberá realizar consultas en la base de datos y pruebas de simulación. Dichos procesos consumen mucho CPU.

- RAM: Alta

De igual forma que en CPU, los procesos de simulación y consulta en la base de datos, requieren de mucha RAM.

- Red: Alta

El acceder a los servicios para consultar información, y para realizar el trabajo desde el ordenador personal del funcionario hacia los servidores requiere de una "Alta" velocidad de red.

- Seguridad
- Confidencialidad: si
- Integridad: si
- Disponibilidad: si

De igual forma que para las actividades anteriores es necesario garantizar la seguridad para todo el proceso ya que de otra forma no tendría sentido.

d) Enviar guía al cliente

- CPU: Baja

El envío de la guía al cliente requiere del uso de un correo electrónico seguro con PGP. El cual no consume demasiados recursos de CPU por lo que se escogió bajo.

- RAM: Baja

Como ya se dijo un servidor de correo electrónico no consume mucho en lo referente a CPU o memoria RAM, por lo que se escogió bajo.

- Red: Media

El envío de la guía al cliente requiere de un correo con archivos adjuntos y para evitar congestión con otros usuarios, se decidió por una velocidad media.

- Seguridad
- Confidencialidad: Si
- Integridad: Si
- Disponibilidad: Si

Es necesario que el envío del correo electrónico sea con todas las seguridades del caso, por lo que se necesita un protocolo como PGP para confirmar la autenticidad del mismo.

2.2.2. USUARIOS POR APLICACIÓN [S1]

Servidores	Usuarios	Perfiles	Número de usuarios
Correo	- Funcionario del EcuCERT - Personal administrativo del EcuCERT	U1, U2	13
Web	- Todo, excepto equipos a ser monitoreados	U1, U2, U3, U4, U5	188
Aplicaciones	- Funcionario del EcuCERT - Personal administrativo del EcuCERT - Estudiantes del EcuCERT (curso actual)	U1, U2, U5	63
Base de datos	- Funcionario del EcuCERT - Personal administrativo del EcuCERT - Cliente – administrador de red - Estudiantes del EcuCERT	U1, U2, U3, U5	LAN: 63 Vía WEB: 88
Storage	- Funcionario del EcuCERT - Personal administrativo del EcuCERT - Estudiantes del EcuCERT (curso actual)	U1, U2, U5	63
FTP	- Todo, excepto equipos a ser monitoreados	U1, U2, U3,U4, U5	188
Red de pruebas	- Funcionario del EcuCERT - Estudiantes del EcuCERT (curso actual)	U1, U5	63
Honeynet	- Funcionario del EcuCERT - Estudiantes del EcuCERT	U1, U5	63
Servidor de monitoreo	- Funcionario del EcuCERT - Cliente – administrador de red - Equipos a ser monitoreados	U1, U3, U6	135

Tabla 2.4: Usuario por aplicación.

Con la información de la tabla 2.2 se procede a establecer los servicios o aplicaciones de la red que serán utilizadas por cada perfil de usuario. Establecer que usuario utilizará cada aplicación, ayuda para tener una idea del nivel de exigencia al que será sometida dicha aplicación, y a dimensionar los equipos que se deben adquirir para el centro de datos. En la tabla 2.4 se puede observar que perfil de usuario utiliza cada servicio de la red del EcuCERT.

2.2.3. CLASIFICACIÓN DE LOS SERVICIOS POR EL TIPO DE INTERACCIÓN CON EL USUARIO

Para establecer con mayor precisión los requerimientos de capacidad que se necesitan para los diferentes servicios, se procedió a clasificar a las aplicaciones que corren en la red de acuerdo al tipo de interacción con el usuario como se observa en la tabla 2.5. Cada servicio puede estar en una de las siguientes categorías:

Servidores	Tipo se servicio
Correo	Batch
Web	Interactivo
Aplicaciones	Interactivo
Base de datos	Batch & Interactivo
Storage	Batch & Interactivo
FTP	Batch & Interactivo
Red de prueba (virtual)	Interactivo
Honeynet	Batch
Servidor de monitoreo	Tiempo real & Batch

Tabla 2.5: Clasificación del tipo de servicio

- Batch, cuando se trata de aplicaciones que ejecutan procesos automáticos, sin la participación permanente del usuario.

- Interactivo, cuando el usuario trabaja permanentemente con el servicio.
- Tiempo real, cuando la aplicación debe presentar la información al usuario, lo más cercana posible al momento en que se generó el evento.

De esta clasificación se tiene que los servicios que mayor cantidad de recursos necesitan, son los del tipo "tiempo real" seguidos por los del tipo "Interactivo" y finalmente los que menor cantidad de recursos necesitan son los tipos "batch".

2.2.4. VELOCIDAD DE ENLACE [L2] [S2]

La velocidad de enlace (ancho de banda para el mercado), se refiere a la cantidad de información que puede fluir por un medio de transmisión en un determinado tiempo. Para el cálculo de la velocidad de enlace a internet se considera únicamente, al correo electrónico, al servidor web, al servidor ftp y al sistema de monitoreo, ya que son los únicos con salida a internet. Las demás aplicaciones de la red del EcuCERT corren en la LAN por lo que su velocidad de enlace es de 1000 Mbps. Los enlaces para la red de prueba y para la *Honeynet* son independientes y cada uno debe de ser de 2 Mbps por requerimiento de la Supertel. Además todos los equipos deben soportar el protocolo IPv6. En el capítulo 3 se realiza el cálculo para el dimensionamiento del enlace a internet. A continuación se muestran los requerimientos para las diferentes aplicaciones que corren en la red del EcuCERT obtenidos de las historias de usuarios.

Correo electrónico:

- Tamaño promedio de un correo electrónico: 2 MB
- Número promedio de correos recibidos y/o enviados por hora: 10
- Número estimado de usuarios simultáneos: 10
- 20 GB disponibles de almacenamiento para cada usuario

Web[27]*:*

- Usuarios simultáneos: 100
- Tiempo de refresco de página web[28]: 60 segundos
- Tamaño de la página: 2 MB

[27] De acuerdo a las estadísticas de la página actual de al Supertel entregado en la consultoría.
[28] Cada 60 segundos aproximadamente los usuarios hacen clic en un link de la página.

FTP:

- Transmisión de archivos de gran tamaño (decenas de *gigabytes*), sin límite en subida o bajada.
- Usuarios simultáneos: 1

Sistema de monitoreo:

- 1 KB por segundo de información por cada cliente
- Número estimado de clientes: 510
- Tiempo mínimo que debe almacenarse la información: 1 año

Base de datos

- Tamaño promedio de una consulta: 500 KB
- Número de consultas estimadas por hora: 30

2.2.5. ALMACENAMIENTO [S1]

Los requerimientos de almacenamiento necesarios para los diferentes servicios del EcuCERT fueron extraídos de la consultoría facilitada por la Supertel. Estos requerimientos son únicamente estimados ya que no se sabrá cuanto realmente se necesita hasta que el EcuCERT entre en operación.

Correo electrónico:

- 20 GB disponibles de almacenamiento para cada usuario

Servidor de almacenamiento (Storage) y Base de datos

- Número promedio de casos por mes: 10
- Cantidad de información promedio por caso: 20 GB

Aplicaciones

- No se tiene un requerimiento de almacenamiento específico para este servicio (Todavía no se sabe que aplicaciones implementará el EcuCERT en este servidor). Se establecerá un espacio de 500 GB con posibilidad de expansión.

FTP

- No se dispone de un requerimiento específico para este servicio (la consultoría facilitada por la Supertel habla de archivos de “gran tamaño”). Por este motivo se establece 1 TB para este servicio.

Servidor de Monitoreo

- Información promedio recibida: 1KB por segundo
- Tiempo que se almacena la información: 1 año

Para los servidores de dominio, DHCP, DNS, AAA, Proxy, Web y VPN la cantidad de espacio en disco necesaria no supera los 2 GB. Por ese motivo no se los consideran por separado

2.2.6. CARACTERÍSTICAS DE CPU, RAM, Y RED POR APLICACIÓN

Finalmente con la información de los pasos anteriores, se puede estimar las características de los componentes de CPU, RAM, y velocidad de enlace necesarias para cada servicio de la red. La tabla 2.6 muestra los parámetros necesarios para cada servicio que corre en la red del centro de datos del EcuCERT.

Servicio	CPU	RAM	Red	C	I	D (año)
Correo	Bajo	Medio	Medio	Si	Si	>99%
Web	Bajo	Alto	Alto	Si	Si	>99 %
Aplicaciones	Alto	Alto	Alto (LAN)	Si	Si	>99 %
Base de datos	Alto	Alto	Alto (LAN)	Si	Si	>99 %
Storage	Bajo	Medio	Alto (LAN)	Si	Si	>99 %
FTP	Bajo	Medio	Alto	Si	Si	>99 %
Red de prueba	Medio	Medio	Medio	Si	Si	>99 %
Honeynet	Medio	Medio	Medio	Si	Si	>99 %
Servidor de monitoreo	Alto	Alto	Alto	Si	Si	>99 %

C: Confidencialidad; I: Integridad; D: Disponibilidad (Anual)

Tabla 2.6: Características para dimensionamiento de equipos servidores[29]

[29] Los valores para la velocidad de red será establecida en el capítulo tres de acuerdo a la aplicación de que se trate.

Para explicar cómo se obtuvieron los valores de la tabla 2.6, se toma como ejemplo el servidor de correo electrónico. El servidor de correo electrónico es prácticamente utilizado por todos los servicios y perfiles del EcuCERT. El servidor de correo de acuerdo a la tabla 2.3 necesita una firma PGP en la mayoría de los caso, y puede incluir el envío de archivos adjuntos de alrededor de 10 MB. El correo electrónico es un servicio del tipo batch (no requiere de una entrega inmediata) por lo que su velocidad de enlace puede ser “Media”. La capacidad de CPU necesaria es “Baja”, ya que el servicio de correo no realiza mayor procesamiento. Como el servicio de correo es utilizado por varios perfiles de usuario, (no por todos) se requiere que el servidor atienda varias conexiones por lo que se necesita de una capacidad “Media” de RAM.

Los parámetros de alto, medio y bajo utilizados para el diseño en el capítulo 3 estarán en función del presupuesto de EcuCERT. De esta forma se tiene que un procesador de 2.7 GHz, 10 MB de Cache y seis núcleos con un precio promedio de 500 dólares es “alto”; uno de 2.3 GHz, 8 MB de Cache y 4 núcleos con un precio estimado de 300 dólares es “medio” y por debajo de eso es “bajo”. De igual forma para memoria RAM 16 GB DDR3, 1600 MHz con un precio promedio de 140 dólares es “alto”; 8 GB DDR3, 1600 MHz o 1333 MHz con un precio de 70 dólares es “medio” y por debajo de eso es “bajo”. Estos valores permiten que un mismo equipo físico (que posea uno de los CPU y memoria RAM mencionados) aloje varios servicios mediante virtualización. También es necesario que todos los equipos permitan aumentar el número de procesadores y la capacidad de memoria RAM para crecimiento.

2.2.7. CRECIMIENTO DE USUARIOS [S1]

De acuerdo a los datos proporcionados por la Supertel se espera que en los próximos 3 a 5 años el EcuCERT incremente el número de personal en un 10%. En el mismo periodo de tiempo (3 a 5 años) el EcuCERT planea incrementar el número de servicios que ofrece a los clientes, de acuerdo a la demanda y/o solicitud por parte de los clientes. Este crecimiento (del 10%) puede verse incrementado, si el EcuCERT tiene éxito, o en caso contrario puede verse disminuido. Para el presente proyecto se tomará como referencia el valor de 10%. Para el caso de los clientes, se espera que en 5 años el número de ISPs conectados al EcuCERT

aumente también en un 10% además a los ISP se sumarían las instituciones públicas y ministerios lo que podría incrementar el número de clientes en hasta un 50%, de acuerdo a los estimados de la Supertel[30]. Los usuarios que utilizarán los servicios del centro de datos, y que por lo tanto necesitan puntos de red, se los puede apreciar en la tabla 2.7. Además se tiene una sala de reuniones que dispone de 6 puntos de red.

Usuarios	Número actual de host	% de Crecimiento en 5 años	Número de Host a futuro
Funcionarios del EcuCERT	10	10%	11
Personal administrativo del EcuCERT	3	10%	3
Estudiantes de cursos de Capacitación	25	---	25
Sala de reunión	6	---	6
Equipos de Monitoreo	4	---	4
Total	**48**		**49**

Tabla 2.7: Usuarios actuales y crecimiento a futuro [S1]

2.2.7.1. Proyección de usuarios de la red interna

En el punto 2.2.1, se puede apreciar el número de usuarios exclusivo de la red interna, el cual es de solo 13 personas (está formado por el personal técnico y administrativo, tabla 2.2). Un crecimiento del 10% significaría que en 3 años únicamente aumentará una persona. El EcuCERT también dispondrá de cursos de capacitación; si se espera que el número de estudiantes aumente en un 10%, esto significa que se tendrá un total de 550 alumnos por año. Añadiendo las impresoras conectadas a la red de datos se tiene un total de 16 puntos de red para los funcionarios y de 30 para los cursos de capacitación.

2.2.7.2. Proyección de clientes

La infraestructura del EcuCERT está pensada principalmente para dar servicio a clientes externos. Esto se debe a que los clientes del EcuCERT enviarán información a través del internet (como por ejemplo los logs de los equipos de seguridad)

[30] Consultoría Supertel 2011

para su análisis. Además se espera que varias personas accedan a la página web y/o formen parte de las listas de correos electrónicos a las que se enviará información relativa a seguridad informática. Si se cumplen las proyecciones de la Supertel, en 5 años el número de clientes puede pasar de 25 a 37 lo que incrementaría en número de equipos monitoreados de 100 a 148.

2.3. REQUERIMIENTOS DE CABLEADO ESTRUCTURADO [E1] [E2]

El centro de datos de la Supertel debe cumplir con estándares internacionales en todos los aspectos que sean posibles, lo que incluye al sistema de cableado. El sistema de cableado estructurado es uno de los sistemas principales que conforman la red, ya que de él dependen todo el sistema de red del EcuCERT. La Supertel en sus requerimientos establece que el sistema de cableado estructurado del centro de datos debe cumplir con la norma EIA/TIA-942 que es la que regula los centros de datos, y con la norma EIA/TIA-568-C [E2] que constituye la más actual de las normas TIA/EIA en lo referente a cableado estructurado. Con el seguimiento de las normas mencionadas se espera que el sistema de cableado tenga una vida útil promedio de 10 a 15 años.

2.4. REQUERIMIENTOS DE SEGURIDAD [S1]

Los requerimientos de seguridad del centro de datos si bien salen del alcance del presente proyecto de titulación, serán establecidos de manera general. Un análisis completo que identifique los activos más importantes, los riesgos a los que están expuestos y establezcan métodos y/o medidas para proteger dichos activos en base a una metodología, como por ejemplo Octave[31], debe ser llevado a cabo para garantizar la correcta protección de los recursos y activos del EcuCERT (como se dijo un análisis de este tipo sale del alcance del presente proyecto).

De acuerdo a la Supertel, el EcuCERT (y por consiguiente su centro de datos), debe garantizar la integridad, confidencialidad y disponibilidad de su información según sea el caso. En la tabla 2.3 y con mayor detalle en el anexo B, se puede apreciar como la mayoría de los servicios brindados por el EcuCERT deben contar con estos tres parámetros. Esto se debe a que casi la totalidad de la informa-

[31] Operationally Critical Threat, Asset, and Vulnerability Evaluation

ción que manejará el EcuCERT es de carácter confidencial. La información es suministrada de parte de los clientes al EcuCERT esperando que éste le dé un trato adecuado. Además al ser el EcuCERT una empresa dedicada a la seguridad informática, resultaría muy bochornoso que sea víctima de frecuentes ataques y caídas de sistema. Si llegara a suceder algo como eso, podría verse afectado directamente las funciones del EcuCERT su credibilidad y su autoridad. Por todo lo dicho, es fundamental que todos los equipos, así como la infraestructura de red cuenten con las seguridades necesarias. En el material entregado por parte de la Supertel se establece como medidas mínimas de seguridad las siguientes:

- Implementar medidas de seguridad física (sistemas antiincendios, video vigilancia, protecciones eléctricas contra apagones y sobretensiones, sistemas de control de accesos, etc.)
- Codificar la información
- Utilizar contraseñas difíciles de averiguar
- Monitorear y vigilar permanente de la red
- Utilizar redes perimetrales de seguridad, o DMZ.
- Utilizar tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para protección de software, etc.
- Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.
- Controlar el acceso a la información por medio de permisos centralizados y mantenidos
- Mantener copias de seguridad de la información utilizando sistemas RAID
- Restringir el acceso a personal no autorizado
- Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan y controlar que modifican.
- Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.
- Actualizar constantemente las contraseñas de acceso.

CAPÍTULO 3

DISEÑO

En el presente capítulo se desarrolla el diseño de la red, la selección de equipos y el diseño del espacio del centro de datos. Además el capítulo incluye el diseño de los componentes necesarios para HVAC[32], protección eléctrica y protección contra incendios. El diseño de la red está basado en la propuesta SAFE de Cisco [L5], en el "Manual básico de gestión de incidentes de seguridad informática" de LACNIC [L1], en la norma EIA/TIA 942 [E1] y en los requerimientos del capítulo anterior.

El diseño de la red se divide en: módulo *core*, módulo de centro de datos intranet, módulo perimetral a internet, módulo de campus, módulo *honeynet*, módulo de red de pruebas y módulo de administración de red. Se diseña cada módulo por separado y al final se presentan dos propuestas de red que integren todos los módulos mencionados. La propuesta número uno incluye redundancia y la propuesta número dos no incluye redundancia. La selección de equipos se basa en los requerimientos del capítulo anterior, así como en el diseño de la red. Se utilizarán equipos Cisco para *networking*, por requerimiento de la Supertel. La descripción de los equipos incluye, el cálculo de la potencia total y el dimensionamiento del UPS.

Finalmente se tiene el diseño del espacio del centro de datos. El diseño del espacio del centro de datos, incluye el diseño del cuarto de cómputo, la ubicación de racks y gabinetes, el sistema de cableado estructurado del cuarto de cómputo y cuarto de operaciones, el sistema de HVAC, y el diagrama de la propuesta final para el centro de datos con las medidas de altura, ancho y largo. Además se incluye el dimensionamiento del generador eléctrico y el sistema de extinción de fuego. El diseño no incluye el cableado estructurado de todas las áreas del EcuCERT, debido a que la Supertel todavía no cuenta con los planos definitivos del nuevo edificio, por lo que se desconoce la distribución final de las áreas.

3.1. DISEÑO DE LA RED [L1] [L2] [L5] [E1]

El diseño de la red se basa en los requerimientos establecidos en el capítulo 2. Así como en el "Manual básico de gestión de incidentes de seguridad informática

[32] HVAC: sistema de climatización del centro de datos.

de la LACNIC," conjuntamente con la arquitectura SAFE de Cisco. Para el diseño de la red se presentarán dos propuesta: La primera propuesta de red incluye redundancia N+1 (lo necesario más uno) con la que se tiene un nivel de disponibilidad cercano a 99.741% o *Tier* 2. La segunda no incluye redundancia y permite una disponibilidad cercana al 99.671% o *Tier* 1.

Como punto de partida para el diseño se consideran las aplicaciones que correrán en la red, las cuales fueron determinadas en el capítulo 2. A éstas se añaden varios servicios, necesarios para mejorar el funcionamiento y administración de la red. Así tenemos que las aplicaciones que correrán en la red del EcuCERT son:

1. Correo electrónico
2. Página web
3. FTP
4. Servidor de aplicaciones
5. Base de datos
6. Almacenamiento
7. Red de prueba
8. *Honeynet*
9. Servidor de monitoreo
10. Servidor de dominio
11. DHCP
12. DNS
13. Servidor proxy
14. VPN
15. Servidor SNMP
16. Servidor NTP
17. Servidor de *logs* local

La red del EcuCERT se basa en el diseño propuesto por SAFE de Cisco. En la figura 3.1 se aprecia la propuesta de SAFE (con todos sus módulos) así como la red que será implementada para el EcuCERT. SAFE divide a la red en varios módulos, de los cuales el EcuCERT implementará: Administración, campus, centro de datos, *core*, internet *edge y teleworker,* ver figura 3.1 (no se implementan los demás módulos de SAFE ya que el EcuCERT no cuenta con dichas áreas, sin

embargo éstas pueden ser implementadas en etapas posteriores de ser necesario). Adicionalmente se implementarán los módulos *Honeynet* y red de pruebas. La arquitectura modular propuesta presenta las siguientes ventajas:

1. Permite y facilita el crecimiento a futuro, así como la posterior incorporación de los módulos que no se implementaron en una primera etapa.
2. Permite la actualización y mantenimiento de cada módulo por separado, lo que reduce los costos.
3. Permite administrar y proteger cada módulo de manera independiente lo que facilita su administración.

3.1.1. MÓDULO CENTRAL (CORE) [L2] [L5]

El objetivo del módulo central o *core* es el de permitir escalabilidad y confiabilidad. La función del módulo de *core* es enrutar y conmutar todo el tráfico entre las diferentes redes que forman la red del EcuCERT.[L5]

Las amenazas más comunes que enfrenta el módulo de *core* de acuerdo a cisco son:

- Ataques de DoS[33] y DDoS
- Accesos no autorizados
- *Sniffing, man-in-the-middle* (MITM)

El módulo de *core* del EcuCERT está diseñado de tal forma que combata las amenazas mencionadas, para lo cual se sigue la configuración descrita a continuación. Se implementará redundancia de equipos, por lo que el módulo de *core* estará formado por dos *switches* de capa 3 (ver figura 3.2). Se utilizan *switches* de capa tres debido a que se maneja VLANs, y se necesita de enrutamiento entre ellas.

Para evitar la formación de lazos por redundancia se utilizará el protocolo *Spanning Tree* (STP). Los puertos que se utilicen en ambos *switches* (puertos del 1 al 6) estarán configurados como "*trunk".* Se tendrá una VLAN llamada "*management*"; esta VLAN será utilizada para la administración de los equipos.

[33] DoS y DDoS son ataques de denegación de servicios por sus siglas en inglés, causa que un servicio o recurso sea inaccesible mediante la sobrecarga o consumo de recursos.

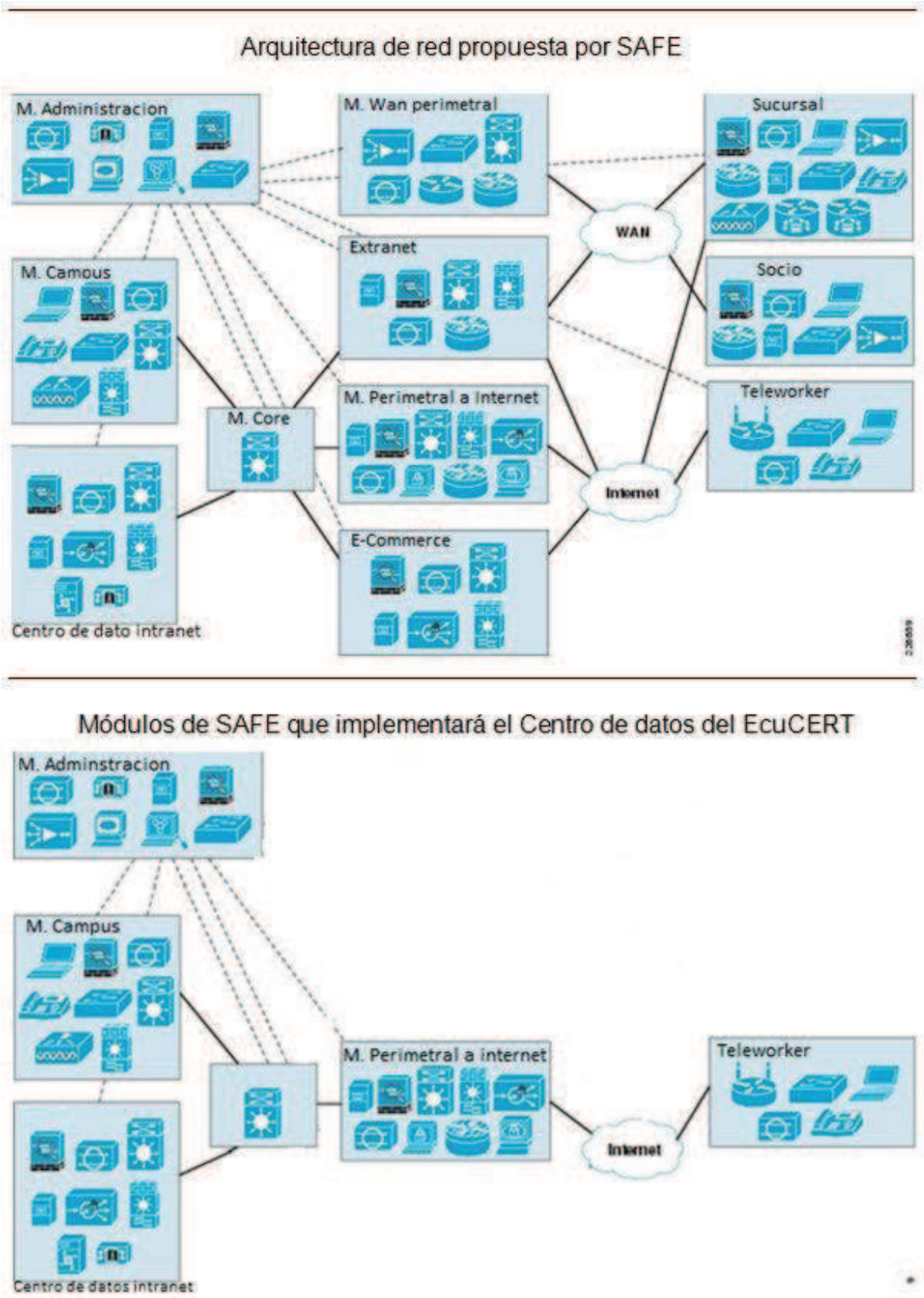

Figura 3.1: Diseño de Red de acuerdo a Cisco SAFE [L5]

Los puertos que no estén siendo utilizados deberán estar desactivados y pertenecer a otra VLAN, la cual no debe ser utilizada. El puerto 7 estará conectado a un IDS/IPS, por lo que deberá estar configurado como *mirror* de los demás puertos, este puerto utilizará la VLAN llamada "monitoreo". Además por seguridad, se debe cambiar la VLAN nativa que viene configurada por defecto (en los equipos Cisco es la VLAN 1).

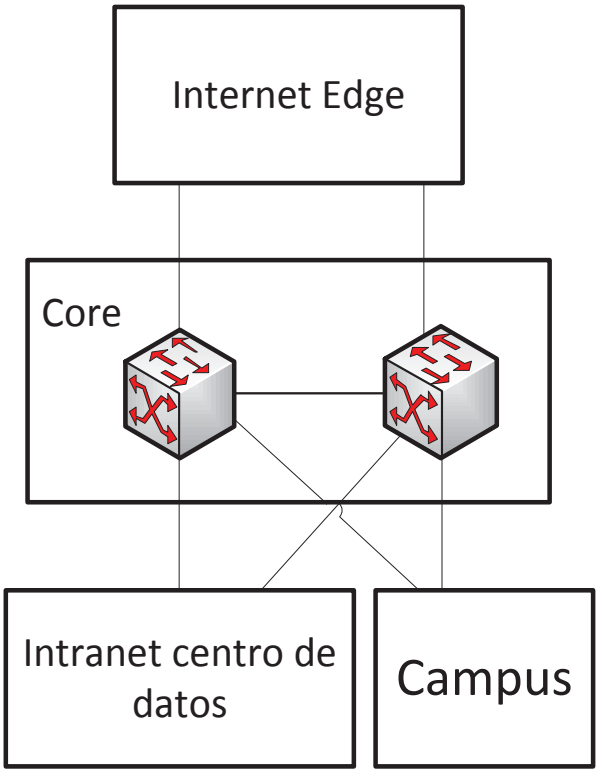

Figura 3.2: Módulo de core [L5]

Para la protección de los puertos que están siendo utilizados, se utilizará *port-security* y se restringirá el número de direcciones MAC que puede aprender cada puerto a una única dirección. Como acción ante una violación se debe utilizar una opción que descarte el trafico[34] cuyo origen es desconocido, registre el evento en syslog, envíe una *trap* SNMP, e incremente el contador de violaciones.

Para el control de acceso se utilizará un sistema de "AAA" con la base remota (y una base local en cada equipo como respaldo) el servidor de AAA utilizará TA-

[34] En equipos Cisco se utiliza la opción *restrict* de la siguiente forma: "*switchport port-security violation restrict*"

CACS+. Las contraseñas de acceso de estos usuarios deben cumplir las siguientes reglas:

- Ser de mínimo 8 caracteres
- Incluir símbolos, letras y números
- No usar palabras de diccionarios

```
                    ##################
                     # W A R N I N G #
                    ##################

#########################################################################

#                   TELEFONICA - ECUADOR                                #

#         UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.             #
                You must have explicit permission from EcuCERT
#                 to access or configure this device.                   #
                All activities performed on this device are logged.
#                                                                       #
#########################################################################
```

Figura 3.3: Banner de los Equipos[35]

Todas las contraseñas deben ser encriptadas. La autenticación mediante AAA deberá ser habilitada tanto para consola como para acceso remoto. Para ambos casos se fijará un tiempo de 5 minutos para desconectar una sesión inactiva, además se bloqueará los intentos de conexión a un usuario durante 60 minutos si se intenta conectarse sin éxito 3 veces o más en un periodo de 2 minutos (estos parámetros pueden ser cambiados de acuerdo con los registros de monitoreo de la red, una vez ésta se encuentre en funcionamiento). Adicionalmente se debe habilitar el registro de intentos de autenticación.

Para acceso remoto se utilizará SSH y se deshabilitará los demás tipos de acceso como *telnet* y HTTP. Para configurar SSH se utilizará una llave genérica para todos los servicios, especificando una encriptación de 1024 bit; y se establecerá el dominio como "ecucert.gob.ec". Las líneas "*vty*" deben estar configuradas para permitir únicamente el acceso vía SSH y un máximo de 2 sesiones simultáneas.

En todos los equipos se deben deshabilitar los servicios que no se utilizan (los cuales varían dependiendo del fabricante). Para los equipos se debe establecer un "*banner*" de inicio de sesión de acuerdo al departamento legal, de tal forma que

[35] Banner sugerido por Telefónica Ecuador a sus clientes corporativos.

todos los que ingresen al equipo estén advertidos de las implicaciones legales, ver figura 3.3. Se habilitarán los servicios de syslog y SNMP v3 para que envíen la información hacia el servidor. El nivel de mensajes de *syslogs* que se enviarán será fijado en *warning*, lo que implica que se envían mensajes de: *warning, error, critical, alert, y emergency* (no se envían mensajes del tipo *informational y debug*). Finalmente se sincronizará a los equipos con el servidor NTP del EcuCERT. La configuración de seguridad mencionada para el módulo de *core* será aplicada a todos los equipos de *networking* de la red del EcuCERT para los diferentes módulos citados en este capítulo.

Amenazas mitigadas en el módulo central

En la tabla 3.1 se puede apreciar las amenazas que de acuerdo a SAFE, se evitan gracias al módulo de *core*.

	DoS en infraestructura	**DDoS en infraestructura**	**Acceso no autorizado**	**Intrusiones**	**Routing Protocol Attacks**	**Botnets**	**Visibility**	**Control**
Topología y sistema redundante	Si	Si			Si	Si		Si
Deshabilitar servicios innecesarios	Si	Si	Si	Si			Si	Si
Políticas de password fuertes			Si	Si				Si
AAA[36]			Si	Si			Si	Si
SSH			Si	Si				Si
SNMP autenticado			Si	Si			Si	Si
Sesiones ACLs	Si	Si	Si	Si			Si	Si
Autenticación entre *routers* vecinos	Si		Si	Si	Si			Si
CoPP[37]	Si	Si	Si	Si	Si	Si		Si
Net Flow syslog							Si	

Tabla 3.1: Mitigación de amenazas en el módulo core [L5]

[36] Autorización, autenticación y contabilización por sus siglas en inglés.
[37] Servicio que puede ser configurado en los equipos cisco, Control plane policing implementa QoS

3.1.2. MÓDULO CENTRO DE DATOS INTRANET [L2] [L5] [W8] [W9]

El módulo centro de datos intranet es donde se ubican los equipos servidores de las diferentes aplicaciones para uso exclusivo del EcuCERT. Este módulo no es accesible directamente desde internet por el público en general. Las ventajas de la implementación del centro de datos intranet como un módulo aparte de acuerdo a SAFE son: (1) Posibilidad y flexibilidad de crecimiento; (2) Prevención contra intrusiones, ataques DoS, filtraciones de datos y fraude; (3) Disponibilidad, confidencialidad e integridad de los datos del usuario; (4) Segmentación y protección de servidores y aplicaciones.

A continuación se analiza, para la red del EcuCERT, cada una de las ventajas mencionadas para el diseño modular, y se las compara con un diseño de red no modular.

1. Posibilidad y flexibilidad de crecimiento

En el punto 2.2.6 del capítulo dos se estableció que el EcuCERT puede aumentar su número de clientes hasta en un 50% en 5 años y el número de funcionarios en un 10%, por este motivo es necesario contar con una infraestructura que permita y facilite el crecimiento. La arquitectura modular de SAFE propuesta permite que de ser necesarios se aumente el número de servidores y/o el de equipos de *networking*. Si se requiere de más puertos de acceso para estos servidores, solo se debe aumentar la capa de acceso del módulo que sea necesario, dejando intacta las demás capas (*core* y distribución) y los demás módulos. Del mismo modo si lo que se desea aumentar son servicios, solo se deben modificar las políticas de acceso y tráfico en la capa de distribución. Esto permite una gran flexibilidad para el crecimiento en comparación con una infraestructura no modular.

En una estructura no modular si bien los costos son menores, (ya que se necesitan menos equipos de *networking*) el incremento del número de usuarios o servicios requiere de muchos cambios en la infraestructura física, lo que contradice la norma TIA942 en la que se basa este proyecto. Además se tendría que modificar las políticas de control de acceso y tráfico en varios equipos lo que demoraría el trabajo y aumentaría la posibilidad que se cometa algún tipo de error.

2. Prevención contra intrusiones, ataques DoS, filtraciones de datos y fraude

En el punto 2.2.9 del capítulo dos se establece que el EcuCERT manejará información confidencial (la cual debe ser protegida). Además al tratarse de una institución dedicada a la seguridad informática, tiene que servir de ejemplo a otras instituciones, por lo que sus servicios deben estar disponibles la mayor cantidad de tiempo posible. La arquitectura modular de SAFE separa al red en módulos, (DMZ, servidores intranet, campus, etc.) esto permite un mejor control de quien o que se conecta y a que módulo o servicios puede acceder. El contar con un mejor control de la red ayuda a prevenir intrusiones, filtraciones de datos y fraude.

Para controlar los servicios a los que un usuario, aplicación o equipo tendrá acceso, se deben colocar ACL en los equipos de la capa de distribución (*switches* de *core* para el caso del EcuCERT[38]) que permitan el flujo solo de los protocolos autorizados y nieguen el resto. Además se debe contar con ACL que eliminen paquetes mal formados y bloqueen los paquetes ICMP para direcciones no autorizadas (direcciones diferentes a la de la red de administración). Esto permitiría proteger contra ataque DoS como ICMP *Flood, SMURF.*[39]. Las ACL para prevenir ataques de DoS en el caso del EcuCERT deben estar colocadas en los *routers* de acceso del ISP, y en los *switches* de *core*, para proteger de ataques internos. De igual forma, si no se cuenta con una arquitectura modular no importaría si se tratase de un ataque interno o externo, ya que en cualquiera de los dos podría provocar el colapso de toda la red.

3. Disponibilidad, confidencialidad e integridad de datos del usuario

Este punto es muy parecido al anterior, ya que en ambos casos se trata de proteger la información que maneja el EcuCERT usando un diseño modular. La mayor diferencia radica en que las ACL incluyen también el manejo de políticas de acceso, para controlar quienes pueden acceder a un servicio y que protocolos pueden circular por la red. Además, se contará con servidores de AAA para un control más detallado (ver sección 3.1.2.2). Una red modular facilita la prestación de dis-

[38] Los funcionalidades de las capas de *core* y distribución se encuentran agrupadas en los *switches* de *core* para el caso del EcuCERT.
[39] *Smurf* es una ataque DoS que amplifica considerablemente los efectos de una ataque ICMP *flood*

ponibilidad, confidencialidad e integridad ya que permite proteger cada módulo de manera general. Al contrario una arquitectura no modular, donde toda la red es parte de un mismo dominio de *broadcast*, debe contar con políticas para cada servicio específico lo que facilita la ocurrencia de errores.

4. Segmentación y protección de servidores y aplicaciones

En el punto 2.2.9 se establece como un requerimiento la protección de servidores y aplicaciones. La segmentación si bien no es un requerimiento, ayuda como medida de seguridad al impedir que usuarios que se encuentran en un segmento, acedan a otro. Un diseño no modular obviamente no posee segmentación por lo que todos sus usuarios y servidores se encuentran en el mismo dominio de *broadcast*, lo que dificulta la protección. El diseño modular de SAFE permite proteger cada módulo por separado y de acuerdo a la necesidad de cada uno. Además cuando se tienen varios servidores virtuales en un mismo equipo físico, es necesario controlar el tráfico que puede existir entre ellos (este tipo de tráfico no abandona el servidor físico, por lo que no circula por la red). Para controlar este tráfico es necesaria la implementación de *switches* virtuales. Los *switches* virtuales trabajan de manera similar que si se tratase de *switches* físicos permitiendo segmentar en dominios de colisión la conexión individual de cada servidor virtual. Además permiten la implementación de puertos *mirrors* para monitorear el tráfico entre servidores virtuales. Para el caso del EcuCERT el módulo centro de datos intranet será uno de los más protegidos ya que en él se almacena la información. Las medidas de protección son las mismas que se dijeron en los puntos anteriores.

De lo anterior se puede concluir que el diseño propuesto por SAFE si bien resulta más costoso, cumple con los requerimientos del capítulo dos para el centro de datos del EcuCERT. Además el diseño de SAFE ayuda a garantizar y facilitar el cumplimiento de los aspectos claves que todo centro de datos debe tener en cuenta: aislamiento, aplicación de políticas y visibilidad. La descripción dada en los puntos anteriores se ajusta también a los demás módulos de la red del EcuCERT, por lo que no será repetida nuevamente cuando se hable de ellos. A continuación se procede al diseño del *networking* y servidores.

3.1.2.1. Infraestructura de networking del centro de datos intranet [L2] [L5] [E1]

El centro de datos intranet se basa en la propuesta SAFE de Cisco para su diseño lógico. De acuerdo a dicha propuesta, estará constituido por las capas de: *Core*, agregación, servicios, acceso y acceso virtual, como se observa en la figura 3.4. La implementación del centro de datos intranet bajo este esquema, permite y facilita el crecimiento del centro de datos[40]. Debido a que se diseña un centro de datos *TIER* II es necesario contar con un nivel de redundancia N+1 es decir, que todos los elementos tenga un respaldo (esto es aplicable para todo el equipo del centro de datos). A continuación se presenta el diseño de cada una de las capas mencionadas.

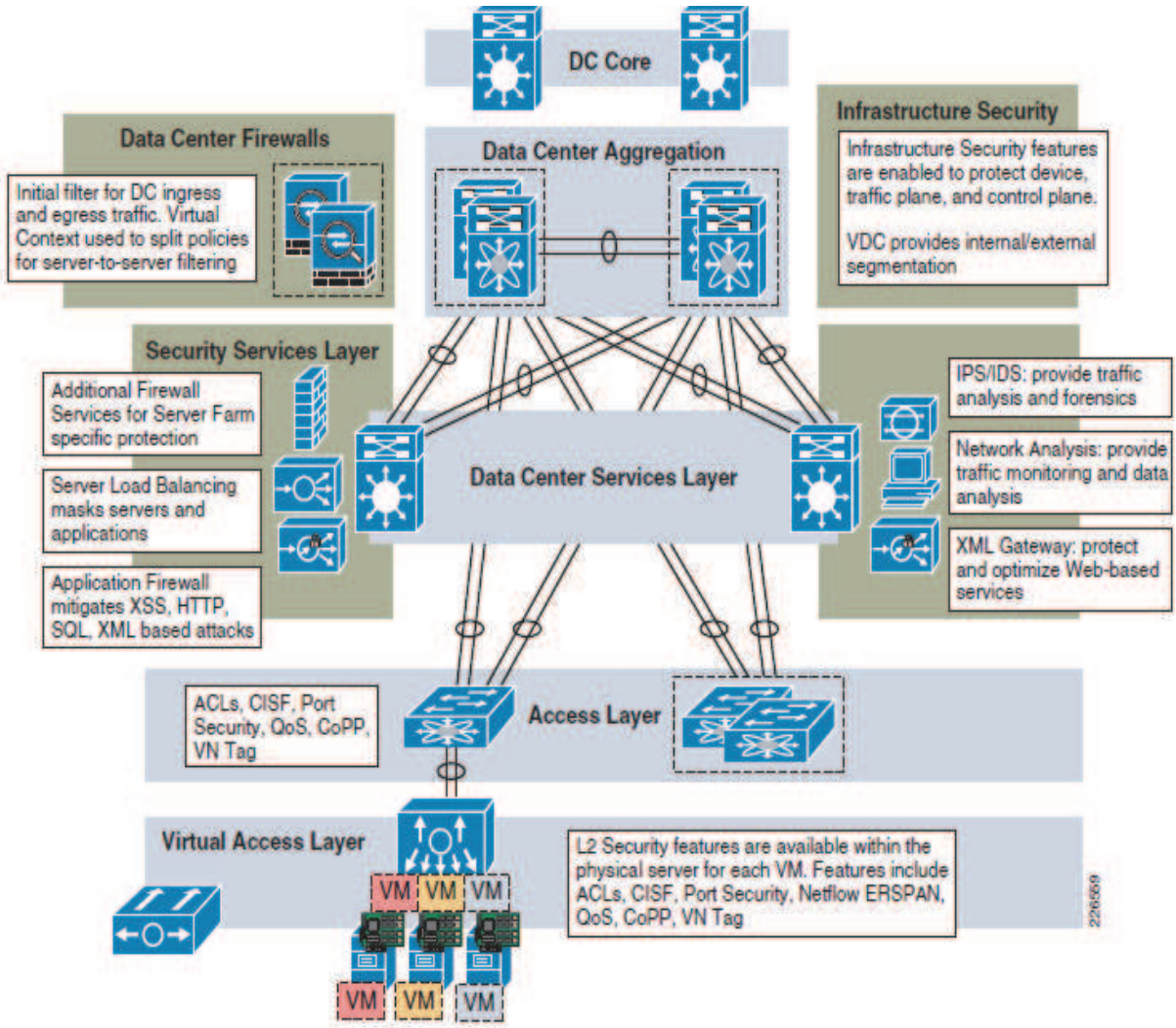

Figura 3.4: Estructura del módulo centro de datos intranet [L5]

[40] De acuerdo a OSI se ha demostrado que los modelos en capas son los más escalables.

3.1.2.1.1. Capa de core del centro de datos intranet [L1][L2][L5][E1]

La capa de *core* es la encargada de proveer conectividad de capa 3 entre el centro de datos intranet y la red del campus. Como la capa de *core* es por la que atraviesa todo el tráfico del centro de datos intranet; y al ser un requerimiento el diseño de un centro de datos *Tier* 2 (N+1); se debe contar con redundancia para que el servicio no se vea interrumpido y tener puertos *gigabit Ethernet*. Para tener una visibilidad completa de lo que sucede, debe permitir la implementación de SNMPv3 y Syslog (ver módulo de administración de red). Para el manejo y autenticación de usuarios los equipos deben seguir las consideraciones hechas para el módulo de *core*. Además deben soportar IPv6 para cumplir con el requerimiento de la Supertel.

Los *switches* de la capa de *core* deben trabajar en capa 2 y 3 del modelo OSI. Para la capa 3 deben permitir los protocolos de enrutamiento EIGRP, OSPF y *static IP Routing* (para IPv4 e IPv6). Se utilizará OSPF[41] (OSPFv3 es la versión que soporta IPv6 definida en el RFC 2740) ya que es un protocolo abierto[42] definido en el RFC 1583, a diferencia de EIGRP que es propietario de Cisco (si bien EIGRP en equipos Cisco presenta una convergencia más rápida que OSPF). OSPF es un protocolo de estado de enlace, lo que le permite crear una topología exacta de la red (lo que le da ventaja sobre protocolos como RIP, que es del tipo vector distancia) y buscar la ruta más corta en función del ancho de banda[43]. OSPF presenta una convergencia más rápida que IS-IS, y que RIP si bien su implementación es más compleja que ambos. En lo relativo a crecimiento y escalabilidad OSPF es más escalable que RIP. OSPF permite configurar autenticación MD5 para aceptar nuevas rutas o avisos de estado de enlace solo de *routers* cuya autenticidad sea comprobada. OSPF no utiliza TCP o UDP ya que tiene definido su propio paquete IP (protocolo IP 89), por lo que los *firewall* y ACL deben estar configurados para permitir el paso de dicho protocolo. Debido a la redundancia que se implementa en la red del EcuCERT es necesario configurar el balanceo de carga de OSPF

---

[41] OSPF es un protocolo de *Gateway* interior (IGP) es usado dentro de sistemas autónomos (AS) y utiliza el algoritmo de Dijkstra que es un algoritmo para determinar el camino más corto dado un vértice de origen al resto de vértices.

[42] Se refiere a que no está patentado por ninguna compañía

[43] Ancho de banda comercial se refiere a velocidad de enlace; para OSPF el costo de una ruta es 10^8/(AB[bps])

para que ambos *router* funcionen al mismo tiempo. Para manejar los *router* redundantes se usará HSRP[44], de tal forma que si uno de los *router* falla el otro se haga responsable de todo el tráfico.

Para capa dos se deben tener los protocolos 802.1d (*Spannig tree*), 802.1s (*Multiple Spanning Tree*), 802.1w (*RapidSpannig Tree*), 802.1Q (VLAN), 802.1p para implementar calidad de servicio (QoS) mediante lo que se conoce como CoS. Debe tener 802.1x para control de acceso basado en puerto, ACLs y *port security* que es una funcionabilidad para implementar medidas de seguridad en los puertos. Como medidas de seguridad se filtrarán las rutas que se pueden propagar. Para el caso del EcuCERT esta función estará concentrada en el módulo de *Core* de la red principal, y será desempeñada por los *switches* de capa tres.

3.1.2.1.2. Capa de Agregación [L1][L2][L5][E1]

La capa de agregación es la encargada de aislar la red del centro de datos intranet de la red del campus. En esta capa se ubican los *firewalls* encargados de controlar el tráfico que entra y sale de la red del centro de datos. Los equipos de esta capa deben permitir la implementación de al menos 10 contextos de seguridad para los diferentes perfiles de usuario que se tienen en el capítulo 2. Debe trabajar con IPSec, SSL VPN, deben soportar VLANs y permitir la implementación de ACLs. Su función principal es realizar un NAT entre la red del centro de datos intranet y la red externa. Para monitoreo deben contar con syslog, SNMPv3, NTP (todos los equipos deben contar con estos protocolos para monitoreo). Para el caso del EcuCERT se cuenta con dos *firewall* para llevar a cabo esta tarea. Todo el tráfico que entre y salga del centro de datos intranet pasa por estos *firewalls*. Si bien es posible concentrar todas las funciones de esta capa en los equipos del módulo de *core* (para disminuir los costos) no es recomendable sobrecargar de muchas funciones a la capa de *core* ya que esto puede conducir a errores y la capa de *core* es por donde atraviesa todo el tráfico del EcuCERT.

Los *firewall* que se ubican en esta capa deben permitir al momento de su implementación los siguientes protocolos y sus respectivos puertos[45]:

---

[44] HSRP es un protocolo propietario de Cisco que permite el despliegue de *routers* tolerantes a fallos en una red.

- DHCP: 67, 68 (UDP)
- DNS: 53 (TCP, UDP)
- Proxy: 3128 (TCP)
- SNMP: 161, 162 (TCP, UDP)
- NTP: 123 (TCP)
- Syslog: 514 (UDP)
- SQL: 3306 (TCP)
- Kerberos: 88 (TCP)
- LDAP: 389 (TCP, UDP)
- TACACS+: 49 (TCP)
- NFS: 2049 (TCP)
- SAMBA: 137, 138, 139, 445 (TCP, UDP)
- SSH: 22 (TCP)

Una vez la red se encuentre en funcionamiento se debe monitorear para establecer que otros protocolos son necesarios.

3.1.2.1.3. Capa de Servicios [L1][L2][I5][E1]

La capa de servicios es la capa donde se ubican los IDS, IPS, *firewalls* de aplicación web (WAF) y demás equipos de monitoreo. Constituye una capa adicional que permite la expansión de los servicios de monitoreo y seguridad sin que se requiera un rediseño de la red. Para el caso del EcuCERT, todas las funcionalidades de esta capa serán realizadas por los *firewalls* de la capa de agregación, los cuales estarán configurados para trabajar como *firewalls*, IPS y WAF.

La configuración como IPS o *inline mode,* si bien consume más recursos que la configuración como IDS o *promiscuous mode* [6], proporciona una protección en tiempo real deteniendo los ataques conocidos antes de que alcancen su objetivo. Para el tráfico entre servidores virtuales se configurará un puerto *mirror* en el *switch* virtual de tal forma que todo el tráfico pueda ser monitoreado.

---

[45] No se consideran puertos para el servidor de aplicaciones ya que todavía no se sabe que aplicaciones utilizará el EcuCERT y que puertos utilizarán dichas aplicaciones.

3.1.2.1.4. Capa de Acceso [L1][L2][L5][E1]

Es la encargada de proporcionar conectividad de capa 2 a los servidores. Su función es incrementar la densidad de puertos con los que se cuenta para la granja de servidores. En esta capa es imprescindible el uso de VLANs, para segmentar el tráfico de los servidores así como de ACLs para impedir flujos de tráfico no deseados. Se utilizarán *switches* de capa 2. Los *switches* deben cumplir los protocolos de capa dos mencionados para la capa de *core* del centro de datos intranet. Los *switches* de la capa de acceso del módulo centro de datos intranet contarán con un puerto *mirror* conectado al IDS (esto con el fin de monitorear el tráfico de los servidores virtuales).

3.1.2.1.5. Capa de acceso virtual [L5][W8][W9][W10]

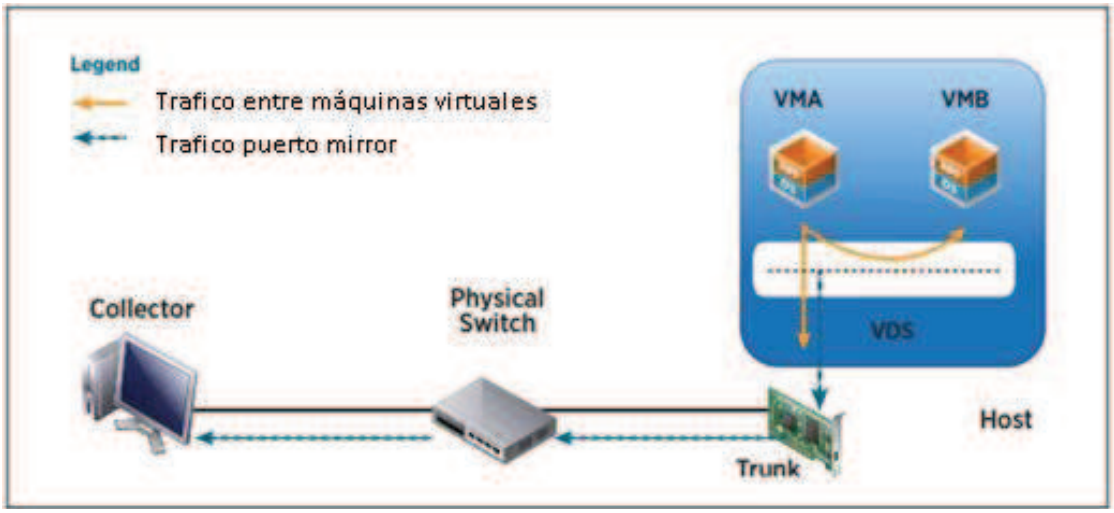

Figura 3.5: Flujo de tráfico de monitoreo [W8]

La capa de acceso virtual reside en los servidores físicos que implementan el software de virtualización. Debido a que con el uso de tecnologías de virtualización puede existir tráfico entre servidores virtuales, que se encuentren en una misma máquina física. Este tráfico no tendría que abandonar la máquina física en cuestión; es decir no circularía por la red física, lo que a su vez impediría que sea monitoreado y/o controlado por las políticas existentes de la red. Para lidiar con este tipo de problemas se utilizará un software de virtualización de servidores que permiten la implementación de *switches* virtuales (como VMWare vSphere). Los *switches* virtuales permiten la implementación de puertos *mirrors* lo que permite reenviar el tráfico para que sea analizado por el IDS (ver figura 3.5).

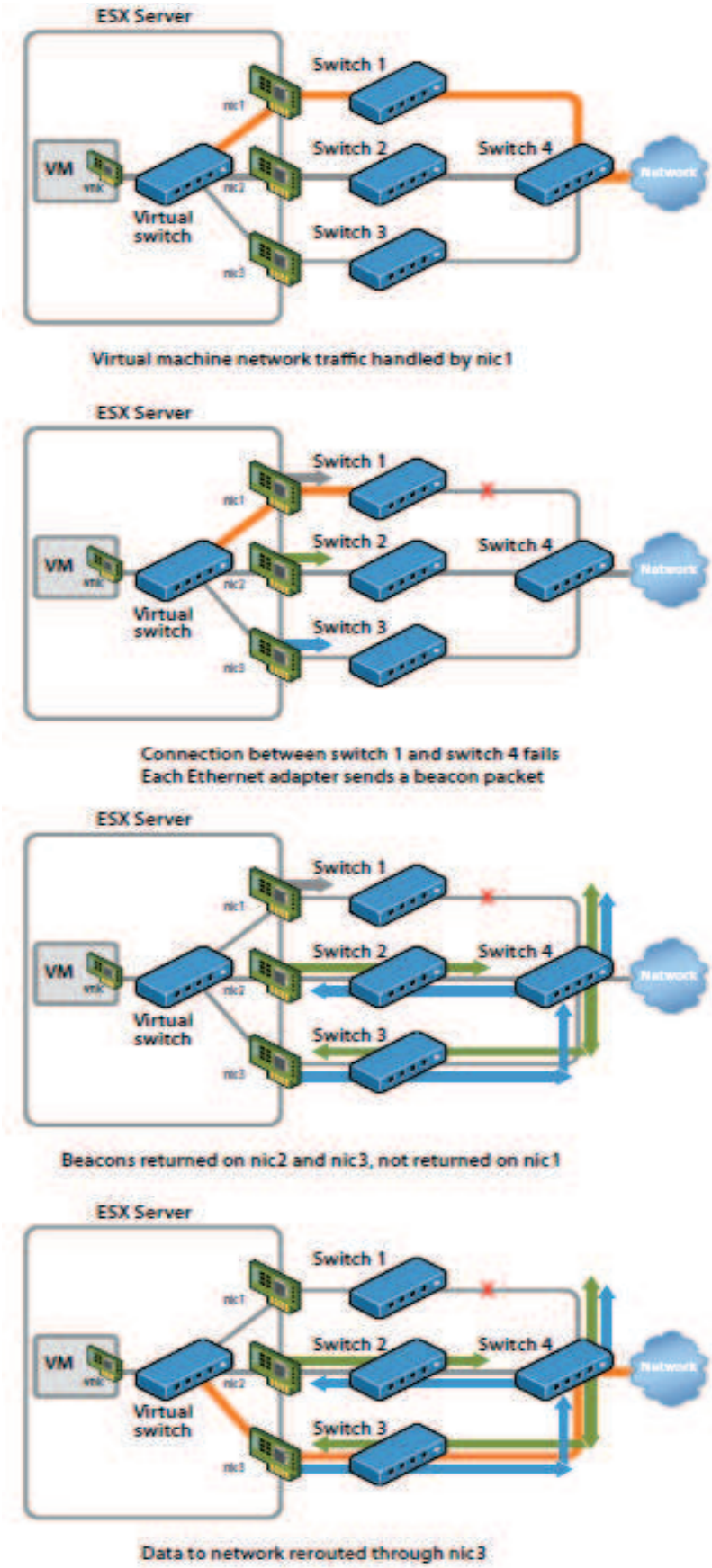

Figura 3.6: Uso de beacon para detectar enlaces caídos [W8]

Además los *switches* virtuales permiten implementar las políticas de seguridad de la red física de tal forma que no se pierda el control de la red. El software que se utilizará es VMware vSphere versión 5[46], ya que este es el software con que cuenta actualmente la Supertel en el laboratorio de redes IP. La configuración de adaptador virtual que se utilizará para las máquinas virtuales será *e1000*[47], ya que es la recomendada para arquitecturas de 64 bits (*vlance* es para arquitectura de 32 bits). Se elige la configuración *e1000,* ya que *vmxnet* necesita que el sistema "*guest*" tenga instalado los *vmware tools* (para evitar posibles incompatibilidades con los sistemas), y; *vswif* y vmknic son solo para el servicios de consola ESX server.

La interfaz física del equipo estará conectada directamente a un puerto *trunk* del switch físico y virtualmente asignada a un puerto *uplink*[48] del switch virtual. El switch virtual tendrá configuradas dos VLANs, una para administración y otra para el resto de datos. La configuración de las VLANs será en modo *virtual switch tagging* VST, en este modo se crea un *Port group* en el switch virtual para cada VLAN que se tenga (el switch virtual es el encargado añadir o quitar las etiquetas de VLANs). Además cada servidor contará con dos interfaces de red por motivos de disponibilidad. Ambas interfaces estarán conectadas a la red física mediante un puerto *trunk* del switch. En la red virtual se configurará las interfaces para que trabajen una a la vez, y cuando falle la conexión de la primera, esta sea inmediatamente sustituida por la segunda (ver figura 3.6) para lo que se utilizará la configuración *Beacon Probing* de VMware vSphere 5.

3.1.2.2.Servidores [L1][L7][W4]

Los servidores necesarios para el uso interno del EcuCERT son:

- Servidor DHCP
- Servidor DNS
- Servidor dominio
- Servidor proxy

---

[46] La versión 5 de VMware vSphere es la última versión disponible de vSphere
[47] *E1000* simula a un adaptador tipo *intel E1000 Ethernet*
[48] Es el nombre del puerto del *virtual switch* que se conecta a la interfaz física del servidor. Puede funcionar como puerto *mirror*.

- Servidor de aplicaciones
- Servidor de base de datos
- Servidor de *storage*
- Servidor de monitoreo

a) Servidor de dominio, DHCP y DNS

Servidor DHCP.- es el encargado de entregar la información de configuración IP, lo que incluye, dirección IP, mascara de subred, *Gateway*, y DNS. El servidor DHCP será montado sobre Linux Centos 6.6. El servidor DHCP atenderá a todas las subredes del EcuCERT. La configuración de direcciones IP que se utilizará se puede apreciar en la tabla 3.2 y está basada en los requerimientos del capítulo 2. Los equipos servidores contarán con IPs fijas al igual que las impresoras. Los usuarios VPN recibirán una del mismo servidor VPN. Ver direccionamiento IP.

Equipos	Subred	Primera Dirección	Ultima dirección	Broadcast	Máscara
Personal técni-co	172.16.0.0	172.16.0.1	172.16.0.254	172.16.0.255	255.255.255.0
Personal Administrativo	172.16.1.0	172.16.1.1	172.16.1.254	172.16.1.255	255.255.255.0
Red de administración	172.16.2.0	172.16.2.1	172.16.2.254	172.16.2.255	255.255.255.0
Red de Servidores	172.16.3.0	172.16.3.1	172.16.3.254	172.16.3.255	255.255.255.0
DMZ	172.16.4.0	172.16.4.1	172.16.4.254	172.16.4.255	255.255.255.0
VPN Túnel	10.1.1.0	10.1.1.1	10.1.1.30	10.1.1.31	255.255.255.224
Usuarios VPN	172.16.6.32	172.16.6.33	172.16.6.62	172.16.6.63	255.255.255.224

Tabla 3.2 : Tabla de direccionamiento IP del EcuCERT

Servidor DNS.- se encarga de traducir las direcciones IP a nombres que sean más fácilmente recordados por las personas. El servidor DNS será implementado en Linux Centos 6 utilizando el software BIND. Además se instalar *bind-chroot,* para enjaular al directorio raíz del servidor BIND, con lo cual el *path* donde se ubicarán los archivos de configuración será: */var/named/chroot/etc.* Como se dijo anterior-mente el dominio será *ecucert.gob.ec*, el cual contendrá el subdominio *mail*, nece-

sario para correo electrónico. El servicio de DNS será del tipo caché y recursivo, es decir que cualquier dirección que no la pueda resolver a un nombre la enviara a un servidor DNS externo previamente configurado. Cuando el servidor DNS externo envié su respuesta, esta se almacena para posteriores consultas. Los servidores DNS externos serán proporcionados por el ISP Telefónica.

Servidor de dominio.- se encarga de la administración de los equipos conectado a la red, mediante la centralización de información y políticas de los usuarios. Para el servidor de dominio se utilizará LDAPv3[49] junto con SAMBA[50]. El dominio principal será *ecucert.gob.ec*

Por políticas del gobierno central de Ecuador, todas las instituciones públicas deben procurar migrar a software libre. Por esta razón los servidores de dominio, DNS y DHCP serán implementados sobre un sistema Linux Centos 6.6 que es la versión más actual al momento de la realización del presente proyecto.

b) Servidor proxy

El servidor proxy es el encargado de controlar el acceso a páginas web de los usuarios de la intranet. El servidor proxy al igual que los servidores mencionados en el punto anterior será implementado sobre Linux Centos 6.6 y se utilizará el software *Squid*. El servidor proxy implementará su control de acceso mediante lo que se conoce como listas blancas, es decir se especifica únicamente los sitios web permitidos.

Grupo	Sitios permitidos
Funcionario del EcuCERT	Sin restricción
Personal administrativo	Dominios *.gob.ec y *.gov
Estudiante de curso de capacitación	Variable, (depende del curso)

Tabla 3.3: Perfiles de usuarios en servidor proxy

De acuerdo a los diagramas de casos de uso del capítulo dos, el personal técnico del EcuCERT, deberá investigar sobre diferentes temas de seguridad, por lo que

[49] LDAP: Protocolo ligero de acceso a directorio por sus siglas en inglés
[50] Samba: es una implementación libre del protocolo de archivos compartidos de Microsoft Windows

necesitan acceder a internet sin restricciones. El servidor proxy será implementado de acuerdo a la tabla 3.3.

c) Servidor de aplicaciones

El servidor de aplicaciones se refiere a las diferentes aplicaciones que utilizará el EcuCERT internamente para diferentes propósitos. Es decir éstas aplicaciones correrán exclusivamente en la LAN y podrán ser aplicaciones WEB, java, etc.

d) Servidor de Base de datos

El servidor de base de datos estará montado sobre Linux Centos 6, y utilizará MySQL 5.6; que es la última versión disponible en el mercado a la fecha en que se desarrolló el presente proyecto. Para el cálculo del tráfico del servidor de base de datos por motivos de consultas se estima, (de acuerdo a los datos proporcionados por la Supertel, ver capítulo 2) que el tamaño de una consulta es de 500 Kbyte y un usuario promedio realiza aproximadamente 30 consultas por hora, con lo que se tiene:

$$Trafico\ de\ BDD_{x\ usuario} = \frac{500\ KB}{1\ consulta} * \frac{30\ Consultas}{1\ hora} * \frac{1\ hora}{3600\ seg} * \frac{8\ bits}{1\ Byte} = 33.3Kbps$$

Como los datos serán almacenados en el servidor de *storage*, y se interactuará con éste a través del servidor de base de datos. El servidor de base de datos y *storage* pueden encontrarse en la misma máquina.

e) Servidor de almacenamiento

Conocido como servidor de *storage*, es donde se guarda o almacena la información de todos los casos con los que trabaja el EcuCERT. Es accesible únicamente desde la intranet del EcuCERT. Uno de los requerimientos para este servidor es que dicha información se encuentre disponible por un periodo de al menos 1 año. La conexión del servidor de *storage* está dispuesta como red NAS. En este tipo de conexión si bien la información viaja por el mismo canal que el del resto de la información, (a diferencia de una red SAN que tiene su propio segmento *Ether-*

net) resulta mucho más barato que la tecnología SAN. Por dicho motivo se recomienda que en una primera etapa el EcuCERT comience con una configuración NAS. Para calcular la capacidad de almacenamiento, se considera un promedio de 10 casos por mes, y cada caso con unos 20 GB de promedio de información (de acuerdo a los requerimientos del capítulo 2) con lo que se tiene:

$$Capacidad\ disco = \frac{10casos}{1mes} * \frac{20GB}{1caso} * \frac{12meses}{1año} * \frac{1TB}{1024GB} = 2.34TB/año$$

Por lo tanto la capacidad mínima de disco necesaria es de 2.34 TB por lo que se recomienda 3TB.

3.1.2.3.Propuesta de diseño del módulo centro de datos intranet

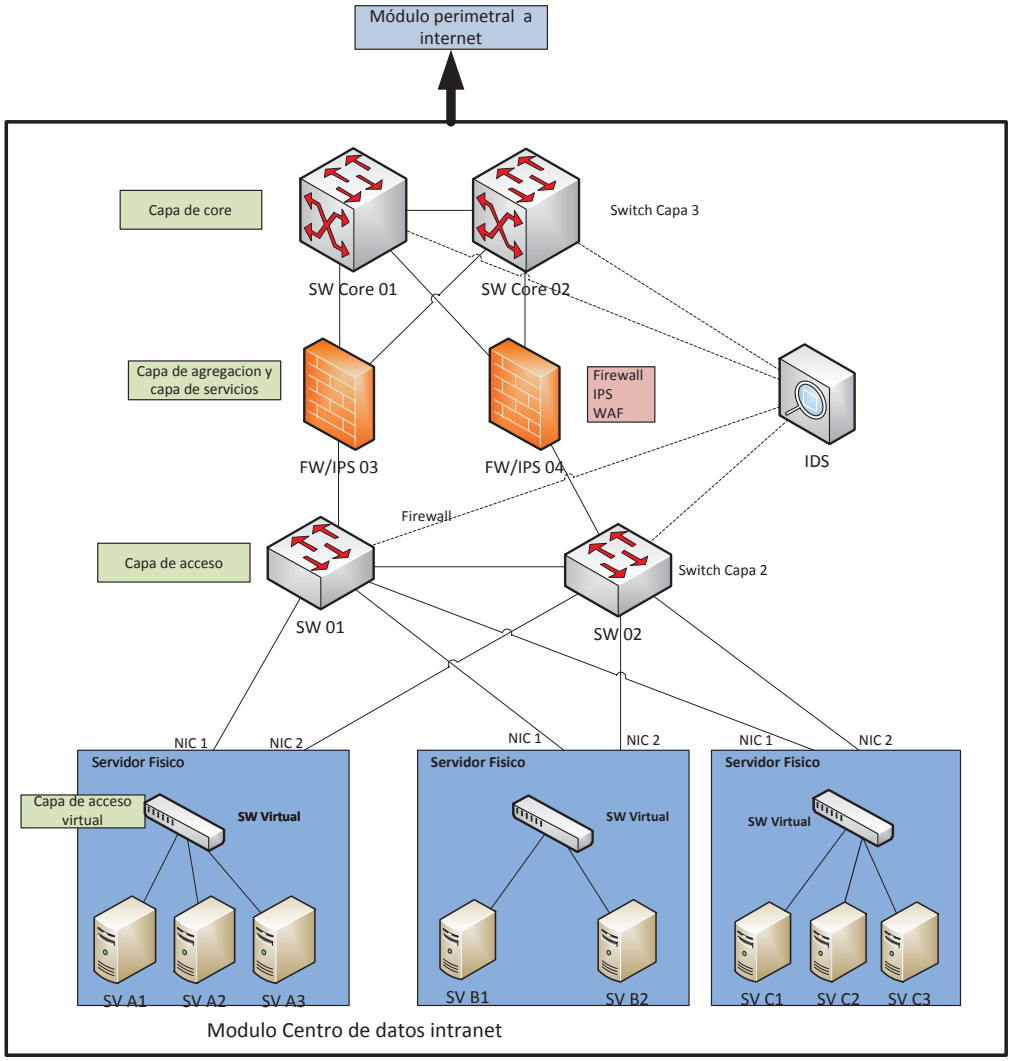

Figura 3.7: Diseño del módulo centro de datos intranet

Para el diseño del módulo de datos intranet, se utilizará servidores con doble tarjeta de red, de tal forma que cada tarjeta se conecte a un switch de capa dos. Cada servidor contará con un arreglo “raid 1” de discos. Se eligió raid 1 debido a que los costos son menores ya que requiere de menos discos, sin embargo se espera cambiar a raid 5 en un futuro, ya que este es más económico a largo plazo. La figura 3.7 muestra el esquema del módulo de centro de datos intranet.

3.1.3. MÓDULO PERIMETRAL A INTERNET [L1] [L5] [E1] [W8] [W9]

El módulo perimetral a internet constituye la parte de la infraestructura de red que se comunica directamente con internet, además actúa como el *gateway* de la empresa hacia el internet. Al ser éste el módulo que se conecta directamente a internet, se ve expuesto a un gran número de ataques de todo tipo. En el módulo perimetral a internet se ubican la zona desmilitarizada (DMZ), el acceso a internet y el acceso remoto VPN[51]. La implementación del módulo perimetral a internet como un módulo aparte de acuerdo a SAFE proporciona los siguiente beneficios[52].

- Disponibilidad de servicio y capacidad de recuperación a desastres.
- Prevención contra intrusiones, ataques DoS, filtraciones de datos y fraude
- Garantizar disponibilidad, confidencialidad e integridad en los datos del usuario
- Protección de aplicaciones y servicios

Esta sección se enfoca en el diseño del módulo perimetral a internet, para lo cual se divide dicho módulo en 2 bloques funcionales: Zona desmilitarizada DMZ que contendrá el servidor VPN y el acceso a internet.

3.1.3.1.Zona desmilitarizada DMZ

La zona desmilitarizada es una porción de red entre una red interna (por lo general segura) y una red externa (generalmente el internet). En la DMZ es donde se ubican servidores a los que resulta necesario acceder desde el exterior (prestan servicios a clientes externos a la red) [L5]. Para el caso del EcuCERT de acuerdo al punto 2.1.8 del capítulo dos, la zona desmilitarizada albergará los servicios de:

---

[51] Red privada virtual por sus siglas en inglés, tecnología de red que permite la extensión de una red privada sobre una red pública como por ejemplo internet.
[52] Ver explicación del punto 3.1.2 Módulo centro de datos intranet

- Email (correo electrónico)
- WEB
- FTP
- VPN
- Servidor de monitoreo para ISPs.

A continuación se describe la infraestructura de *networking* y los servidores necesarios para la DMZ.

3.1.3.1.1. Infraestructura de networking de la DMZ [L5]

La infraestructura de *networking* necesaria para la DMZ está constituida lógicamente por una capa de acceso, la cual se conecta directamente a los *firewall*, los que a su vez se conectan a los *routers* de los ISPs. Los *firewall* son los encargados de manejar y controlar todo el tráfico que ingrese a la red del EcuCERT, para redirigirlo a la interfaz de la DMZ o de la red interna. Como todo el tráfico atraviesa estos *firewalls* es necesario contar con redundancia (N+1) para garantizar la operatividad de la red por lo que cada *firewall* deberá contar con mínimo 5 interfaces de red *gigabit ethernet* (para poder conectarse con la DMZ, el módulo de *core* y con los equipos de los ISP). Los *firewalls* serán los encargados de almacenar las direcciones IPs externas que accedan a la DMZ, así como de realizar la conexión de los clientes externos a los servidores de la DMZ. Es necesario que los *firewalls* puedan trabajar como "*web application firewall WAF*" de tal forma que protejan de ataques en sesiones HTTP como inyecciones SQL, o *"Cross-site Scripting*[53] *XSS".* Los *firewalls* deberán soportar VLANs, SSL VPN, IPSec, ACLs, NTP, Syslog, SNMPv3, IPv6, IPv4. Los *firewalls* estarán configurados para trabajar como IPS de igual forma que los *firewalls* del módulo centro de datos intranet (ver punto 3.1.2.1.3).

Los puertos que se debe abrir en los *firewalls* son:

- Email: SMTP 25 (TCP) - POP3: 110 (TCP) - IMAP: 143 (TCP) - POP3 sobre SSL: 995 (TCP) – IMAP sobre SSL: 993 (TCP)
- Web: 80, 8080 (TCP)

[53] Consiste en la inyección de script maliciosos en el código de la página.

- FTP: 21 (TCP)
- SFTP: 22 (TCP)
- VPN: 9001 (TCP, UDP)
- Monitoreo: XXX[54] (TCP, UDP)

Los *switches* de la capa de acceso deben contar con las configuraciones y protocolos mencionados en la capa de acceso del módulo centro de datos intranet. Como se utilizará VMWare vSphere versión 5 para virtualización, es necesario implementar *switches* virtuales para la capa de acceso virtual (ver punto 3.1.2.1.5). Los *switches* virtuales envían el tráfico de los servidores virtuales hacia el IDS encargados de controlar dicho tráfico.

3.1.3.1.2. Servidores

A continuación se describen los servidores y se dimensiona la velocidad de enlace necesaria para el servicio de internet.

a) Servicio de correo electrónico

El servidor de correo electrónico será montado sobre Linux Centos 6.6 y se utilizará *Postfix.* Además se utilizará *dovecot* como sistema de entrega de correo. El dominio del correo electrónico será *mail.ecucert.gob.ec*. La manera en que *postfix* trabaja requiere que todos los usuarios del correo sean también usuarios del sistema operativo, por motivos de seguridad estos usuarios no deben poder loguearse en el sistema por lo que deben ser creados usando el comando:

- *useradd –s /sbin/nologin [*username*]*
- *paswd [*username*] [password]*

Para el servicio de correo electrónico se dispondrá un espacio de almacenamiento de 20 GB para cada usuario (ver punto 2.2.5). De esta forma el usuario puede almacenar por un periodo de tiempo prolongado la información de sus correos electrónicos. Con esto se tiene que para los 113 usuarios de correo electrónico, se necesita 2260 *Gigabyte*s de almacenamiento o 2.26 *Terabytes*, por lo que se recomienda 3 TB de disco.

[54] El servidor de monitoreo será el encargado de recibir los *LOGS* provenientes de los ISPs, pero todavía no se establece que puerto se utilizará.

Para determinar los requerimientos de ancho de banda, se debe considerar el tamaño de los correos electrónicos y el número promedio de correos que se envían. Para el tamaño se considera correos de 10 *Megabytes*, que incluye archivos adjuntos, y un promedio de 10 correos por hora, (ver punto 2.2.4).

$$Trafico\ de\ correo_{x\ usuario} = \frac{2048\ KB}{1\ Correo} * \frac{10\ Correos}{1\ hora} * \frac{1\ hora}{3600\ seg} * \frac{8\ bits}{1\ Byte}$$
$$= 45.51\ Kbps$$

Para el tráfico de correo total se tiene que se cuenta con 113 usuarios, se espera una carga de máximo 10 usuarios simultáneos.

$$Trafico\ de\ correo_{Total} = \frac{45.51\ Kbps}{1\ usuario} * 10\ usuarios\ simultaneos = 455.1\ Kbps$$

b) Servicio de página web

El servidor Web será implementado sobre Linux Centos 6.6, y se utilizará el servidor web *Apache.* Además se instalará el módulo *mod_ssl*, para implementar SSL cuando sea necesario. Para el cálculo del ancho de banda necesario para el servidor web, se toma en consideración un estimado de 100 usuarios simultáneos, con un tiempo de refresco de aproximadamente 60 segundos. Es decir que cada minuto el usuario realizará algún tipo de interacción con la página web. Como tamaño promedio de la página web se tiene 2 MB, que es el tamaño actual de la página web de la Supertel (ver punto 2.2.5). A partir de estos datos se puede calcular el ancho de banda necesario para el servidor de la página web, de la siguiente forma:

$$AB = \frac{\mathrm{T}\ [KB]}{\mathrm{t}\ [seg]} * \frac{8bits}{1Byte} * \#\ usuario\ simultaneos$$

Dónde:

T: tamaño de la página web en kilobytes

t: tiempo promedio en el que un usuario interactúa con la página web y por lo tanto ésta se vuelve a cargar.

$$AB = \frac{2048\ KB}{60\ seg} * \frac{8bits}{1Byte} * 100\ usuarios = 27306.6\ Kbps$$

$$AB\ = 27306.6\ Kbps * \frac{1\ Mbps}{1024\ Kbps} = 26.6\ Mbps$$

c) Servidor ftp

El servidor ftp será montado sobre un Linux Centos 6.6 y se utilizará el software llamado *vsftpd*[55], de igual forma que para el servidor de correo los usuarios del servidor ftp deben ser usuarios del sistema, y por seguridad no deben poder loguearse al mismo. El EcuCERT utilizará este servicio para la transmisión de grandes volúmenes de información, como por ejemplo los *logs* de equipos enviados por los clientes para que sean analizados por EcuCERT (en esos casos se utilizará un servidor SFTP para garantizar la seguridad). Como se observa en la tabla 2.8 el ftp no en un servicio de gran demanda en el EcuCERT, por lo que la velocidad de enlace recomendada para el mismo será de 10 Mbps. Debido a que este servidor almacenará gran cantidad de información por largos periodos de tiempo, deberá contar con gran capacidad de almacenamiento se establece un estimado de 1 TB de disco (ver punto 2.2.5).

d) Servidor de monitoreo

$$Trafico\ de\ monitoreo_{total} = \frac{1KB}{1\ seg} * \frac{8bits}{1Byte} * \frac{1Mbit}{1024Kbits} * 510usuarios = 4.1Mbps$$

[55] Vsftpd: muy seguro ftp por sus siglas en inglés.

El servidor de monitoreo, se encargará de recibir *logs* de los equipos de seguridad de los clientes, para lo cual se utilizará *syslog,* ya que es el estándar libre más utilizado en *logs*. El servidor de monitoreo se implementará en una segunda etapa del EcuCERT. Para calcular el tráfico que circulará por el servidor de monitoreo se toma lo requerimientos del punto 2.2.4 del capítulo dos.

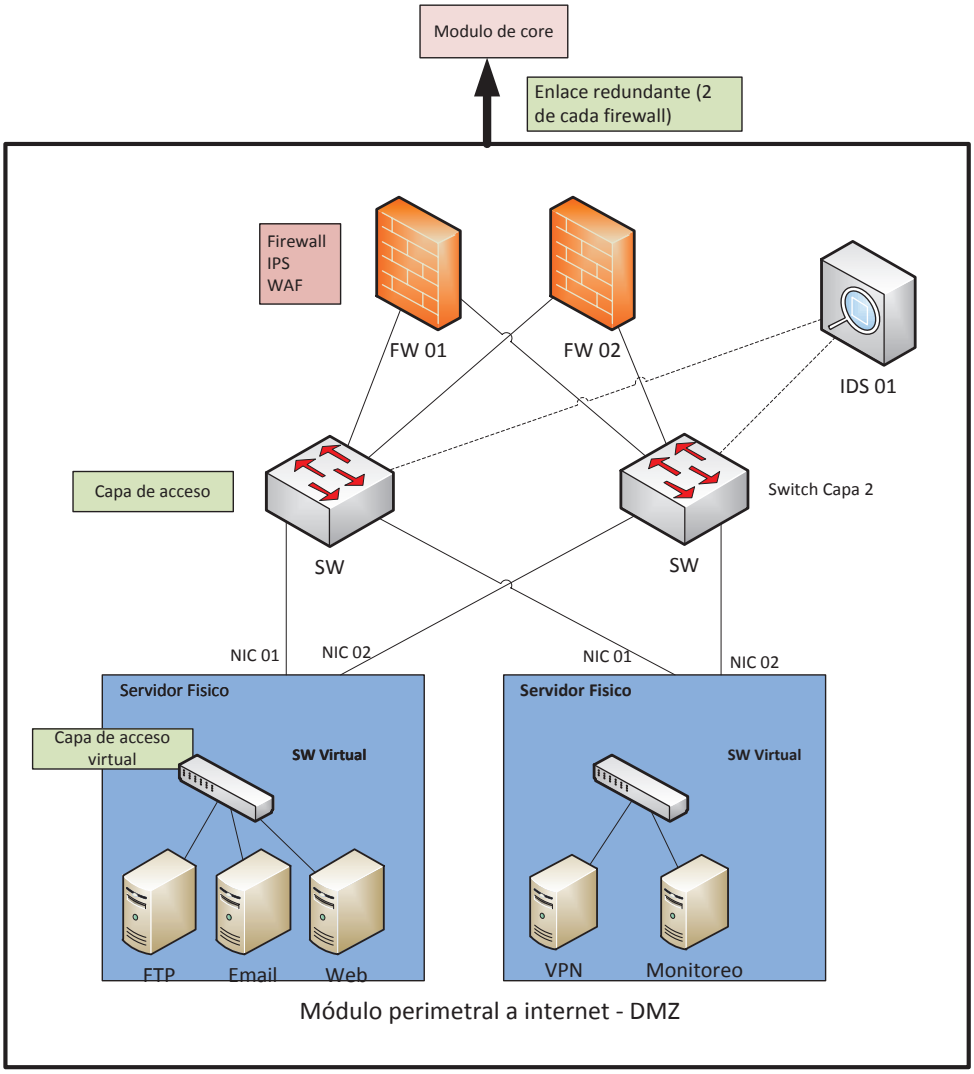

Figura 3.8: Módulo perimetral a internet - DMZ

Como es un requerimiento de la Supertel, que los archivos permanezcan almacenados en el servidor de monitoreo por un periodo de un año, para la capacidad de disco duro, se tiene:

$$Capacidad\ disco_{minima} = \frac{1KB}{1seg} * 510users * \frac{86400seg}{1dia} * \frac{365dias}{1año} * \frac{1TB}{2^{30}KB}$$
$$= 14.97TB/año$$

La capacidad mínima necesaria para el disco duro sería de 15 TB, por lo que se recomienda un tamaño de disco de 17 TB, para considerar un crecimiento del 10%.

e) Servidor VPN

Red privada virtual por sus siglas en inglés, es una tecnología de red que permite la extensión de una red privada sobre una red pública como el internet. El uso de VPN permite enlazar dos o más redes simulando una única red privada. El Ecu-CERT utilizará OpenVPN para permitir el acceso a sus empleados a través de internet. Para mayor seguridad el acceso será controlado mediante certificados digitales. Para permitir un correcto desempeño de "*telework*[56]", se le asignará un acceso de 1 Mbps a cada usuario VPN, que son los funcionarios del EcuCERT. Es decir se necesita de 10 Mbps de ancho de banda para VPN.

3.1.3.1.3. Diseño de la zona desmilitarizada

Para el caso del EcuCERT, la zona desmilitarizada se encuentra ubicada detrás de un *firewall* (dos considerando redundancia), el cual se encuentra conectado al *router* del ISP. Como se aprecia en la figura 3.8 todos los servidores se conectan a un *switch* capa 2 y éste a su vez se conecta al *firewall*. El *firewall* posee una conexión hacia el *switch* de capa 3 del módulo central.

3.1.3.2.Perímetro del proveedor de servicios [L1][L5]

El perímetro del proveedor de servicios constituye la parte del módulo perimetral a internet que se conecta directamente a internet por medio del equipo del ISP.[57] Para el caso del EcuCERT estos equipos serán *routers* arrendados por el provee-

[56] Se refiera a los funcionarios que acceden vía internet a la red del EcuCERT para realizar su trabajo, como si estuvieran físicamente en las instalaciones del EcuCERT.
[57] Proveedor de servicio de internet por sus siglas en inglés.

dor de servicios, lo que se conoce como DTU.[58] Los *routers* estarán conectados a un *firewall* propiedad del EcuCERT (como se observa en la figura 3.9). Los *routers* tendrán configurado BGP, ya que es el protocolo usado para intercambio de información de enrutamiento entre sistemas autónomos. BGP garantiza la elección de rutas libres de bucles, además permite utilizar MD5 para autenticación entre *routers* vecinos, lo que ayuda a prevenir que un intruso modifique la tabla de enrutamiento. Para la red interna se utilizará OSPF como se mencionó en el punto 3.1.2.1.

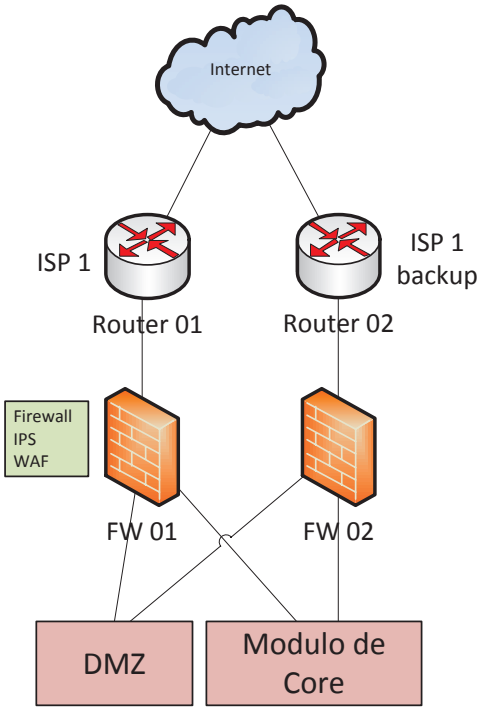

Figura 3.9: Módulo perimetral a internet – perímetro del proveedor de servicios.

3.1.4. MÓDULO DE CAMPUS [L1] [L2] [L5]

El módulo de campus es el encargado de proveer la conexión de red de los usuarios y equipos terminales. El módulo de campus se conecta al módulo *core* directamente. El módulo de campus se basa en la propuesta SAFE de Cisco para su diseño lógico. De acuerdo a dicha propuesta, el módulo de campus se constituye por las capas de: *Core*, distribución y acceso. Para el caso del EcuCERT las funciones de la capa de *core* (del módulo de acceso) serán realizadas por el *core*

[58] Unidad terminal de dato por sus siglas en inglés

general de la red. Esto se debe a que el número de usuarios que integran el módulo de acceso es relativamente pequeño, por lo que no se necesita de un "*Campus services*[59]", como se menciona en SAFE. A continuación se presenta el diseño para las capas de distribución y acceso.

3.1.4.1.Capas del módulo de campus

3.1.4.1.1. Capa de distribución del módulo de campus

La función de la capa de distribución es actuar como un control entre la capa de acceso y la capa de *core*. Es necesario que esta capa implemente redundancia para evitar caídas o pérdidas del servicio. La redundancia debe ser tanto a nivel de equipos como de enlaces. Si existen IDS o IPS exclusivos para el módulo de acceso, éstos deben ser colocados en esta capa. La configuración y protocolos que deben cumplir los equipos de esta capa son los mismos que los mencionados para la capa de *core* del centro de datos intranet (ver punto 3.1.2.1.1).

3.1.4.1.2. Capa de acceso del módulo de campus

La capa de acceso provee el punto de demarcación entre la infraestructura de red y el equipo final. Constituye la primera línea de defensa contra ataques generados por equipos conectados a la red. Los equipos de la capa de acceso deben seguir la siguiente configuración:

- Bloquear el acceso a puertos que no estén siendo utilizados y restringir los puertos utilizados solo a lo necesario.
- Presentar una notificación legal
- Permitir el acceso utilizando servidores de AAA
- Registra los *logs* para los eventos de acceso
- Deshabilitar servicios innecesarios.
- Implementar un servidor NTP
- Monitorear el tráfico en las interfaces para generar estadísticas de uso.
- Monitorear el estado del sistema (memoria, CPU, y procesos)

[59] *Campus services* constituye un área dentro del módulo de acceso que alberga servicios necesarios para el módulo de acceso, como por ejemplo servidor DNS, DHCP, etc

- Implementar ACLs para bloquear el acceso a usuarios no autorizados, y limitar el acceso de los usuarios autorizados únicamente a los que necesitan.
- Implementar *IP Sourced Guard* para evitar ataques de *IP spoofing.*[60]
- Utilizar *Spanning Tree Protoco,* implementar *Rapid Per-Vlan Spanning Tree*
- Habilitar *Port Security* en los puertos de acceso
- No usar la VLAN 1
- Definir un número máximo de direcciones MAC por puerto[61].

3.1.5. MÓDULO HONEYNET [L1] [W14]

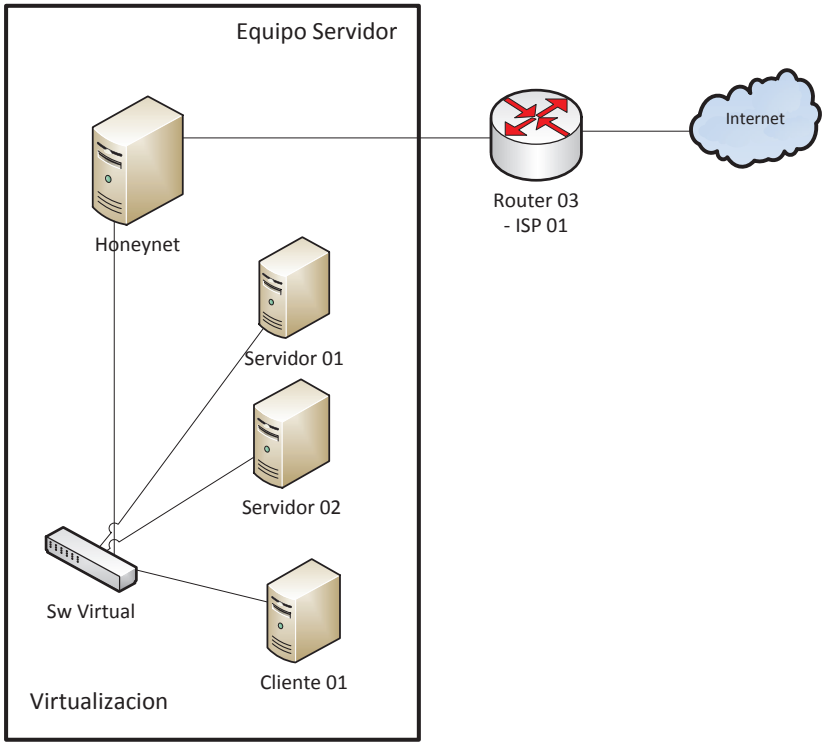

Figura 3.10: Módulo Honeynet

Uno de los requerimientos mencionados en el capítulo dos fue la implementación de un módulo adicional llamado *Honeynet*. La *Honeynet* se trata de una red trampa, con la que contará el EcuCERT para examinar patrones de ataques. La *honeynet* no debe ser utilizada por ningún miembro de EcuCERT, de tal forma que todo el tráfico que se encuentre en la misma pueda ser considerado como intrusivo. Es indispensable que tenga un acceso a internet independiente, por lo que contará con un enlace de 2 *Megabits* para su uso exclusivo. Para disminuir costos

[60] Es un ataque de suplantación de IP
[61] Debe ser fijado de acuerdo a las policías del EcuCERT y al SGSI interno.

se utilizará virtualización. Se necesita de un disco duro de 500 GB el cual se repartirá entre los diferentes honeypot. En la figura 3.10 se puede observar el módulo de la *honeynet*. Se utilizará el sistema *Honeywall*, el cual está basado en Linux y pertenece al proyecto *Honeynet*.[62]

3.1.6. MÓDULO RED DE PRUEBAS [L5]

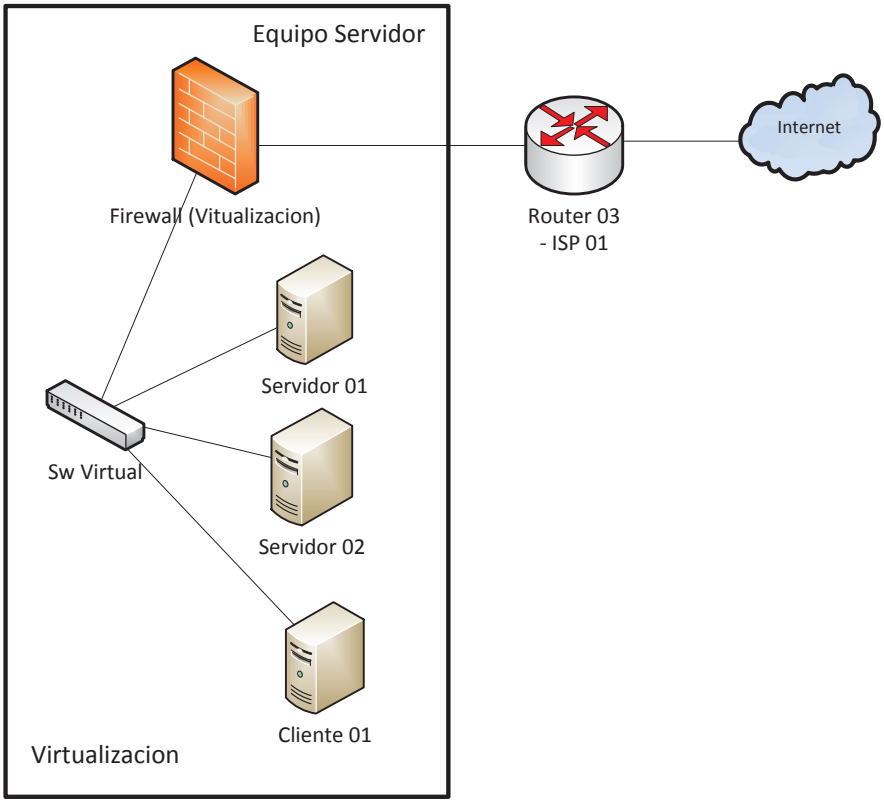

Figura 3.11: Módulo red de pruebas virtuales

El módulo de pruebas es otro de los requerimientos hechos por la Supertel. Como su nombre lo dice es la red que se utilizará exclusivamente para pruebas, por lo cual debe tener un acceso independiente de internet, se utilizará un enlace de 2 *Megabits* de velocidad. Para disminuir costos, esta red será simulada mediante virtualización en un solo servidor. Para la virtualización de la misma se necesita un disco duro de 500 GB, el cual se repartiría entre las diferentes máquinas virtuales de prueba. Para simular el *firewall* se podrá utilizar una distribución Linux como ClearOS, Smoothwall, etc.

[62] https://projects.honeynet.org/honeywall/

3.1.7. MÓDULO DE ADMINISTRACIÓN [L5]

El diseño propuesto considera una infraestructura para monitoreo y administración de la red. La función principal de este módulo es el facilitar la administración de todos los equipos y host de la red. Esto permite generar estrategias de seguridad y administración. Además provee de los siguientes elementos necesarios en la red:

- Acceso y configuración de equipos
- Control de acceso mediante autenticación, autorización y contabilización de equipos, dispositivos y usuarios.
- Equipos de sincronización de tiempo (NTP)
- Monitores para recolección de eventos, análisis y correlación de los mismos.
    - IDS/IPS
    - Servidor de *logs* (*Syslogs*)
    - Servidor SNMP
    - Servidor de AAA

a) Servidores de Logs, SNMP, NTP

Para el servicio de recolección de *logs*, se utilizará el formato *syslogs*, se recopilarán *logs* de los equipos de seguridad, *networking* y servidores. Para el equipo de sincronización de tiempo se utilizará un servidor NTP[63] sobre el sistema operativo Linux. El servidor NTP será el encargado de la sincronización del tiempo a todas las máquinas, servidores y equipos de *networking* de la red. A su vez este equipo obtendrá la hora del Instituto Oceanográfico de la Armada del Ecuador (Inocar) que es el servidor NTP oficial del Ecuador.

- Para la configuración de syslog se deben seguir las siguientes recomendaciones: Habilitar *timestamps* para mensajes de *debugging* y *logging*.
- Establecer la severidad de los mensajes que serán enviados a *logs*.
- Establecer la IP del servidor de syslog.

[63] NTP: *Network Time Protocol*

- Habilitar el buffer local para que reciba mensajes de *logging*. Esto evita la pérdida de mensajes en caso de falla en la comunicación con el servidor de syslog.

b) IDS / IPS

Los IDS, sistema de detección de intrusos por sus siglas en inglés. El IDS se encarga de detectar accesos no autorizados a la red. IPS, sistema de prevención de intrusos. El IPS se encarga de ejercer un control de acceso a los recursos de la red, de manera similar a un *firewall* pero enfocado en el tráfico y no en direcciones IP o puertos. Para el EcuCERT tanto el IDS como el IPS se encuentran integrados en los firewalls. El EcuCERT contará un IDS el cual será utilizado para monitorear el tráfico principalmente de los servidores virtuales utilizando puertos *mirrors* en los *switches* de acceso del módulo centro de datos intranet. Los demás *firewalls*, (los de acceso a la red y los del módulo de centro de datos) también desempeñaran la función de IPS además de la de *firewall.*

c) Servidor de AAA

Servidor de AAA se encarga de la autenticación, contabilidad y autorización de los usuarios. Para este servicio se implementará un servidor TACACS+ junto con Kerberos 5. El servidor TACACS+ será utilizado para los equipos de *networking* (*routers*, *switches* y *firewalls*), y para la autenticación y autorización de servidores y usuarios se utilizará un servidor *Kerberos* junto con LDAP. Ambos servicios estarán implementados sobre un servidor Linux Centos 6.6.

3.1.8. PROPUESTA DE RED PARA EL ECUCERT

De los puntos anteriores se puede determinar la propuesta final de diseño de la red del EcuCERT. La velocidad de enlace necesario para la conexión hacia internet, considerando todos los servicios y añadiendo un aproximado de 10 Mbps, para la navegación de los funcionarios del EcuCERT, es de 60 Mbps. Y dos enlaces independientes de 2 Mbps cada uno. Se tiene dos propuestas, correspondientes a la norma EIA/TIA 942. La primera representa un *TIER* 2, lo que implica una configuración N+1, es decir lo necesario más uno. Y la segunda propuesta es un *TIER* 1, la cual no considera redundancia.

Propuesta 1 – Red de infraestructura Tier 2

Características:

- Disponibilidad cercana a 99.741 %
- Horas de para al año: 22.68 horas

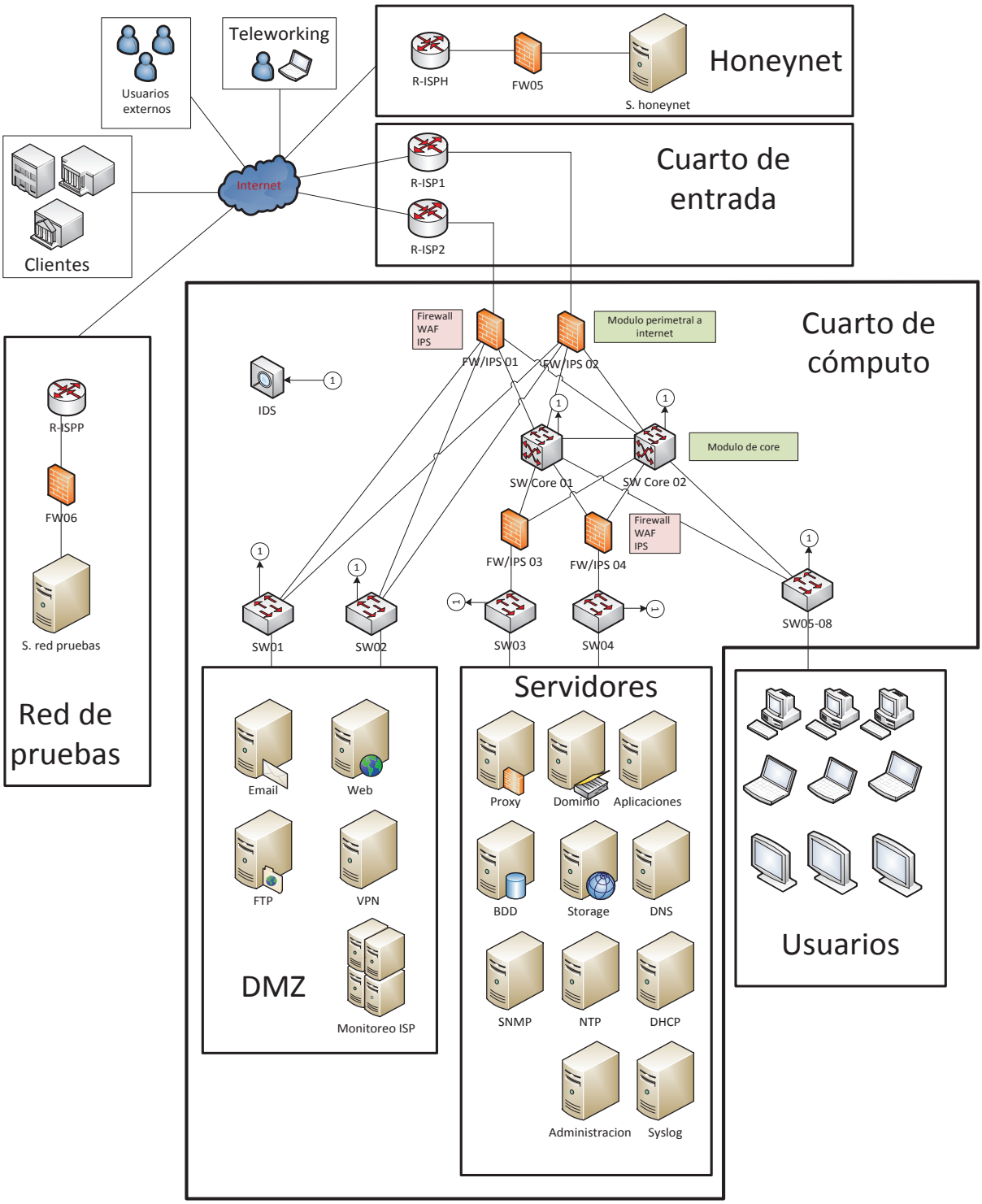

Figura 3.12: Propuesta 1 - diseño de red con redundancia Tier 2

Propuesta 2 – Red de infraestructura Tier 1

Características:

- Disponibilidad cercana a: 99.671%
- Horas de parada al año: 28.82 horas

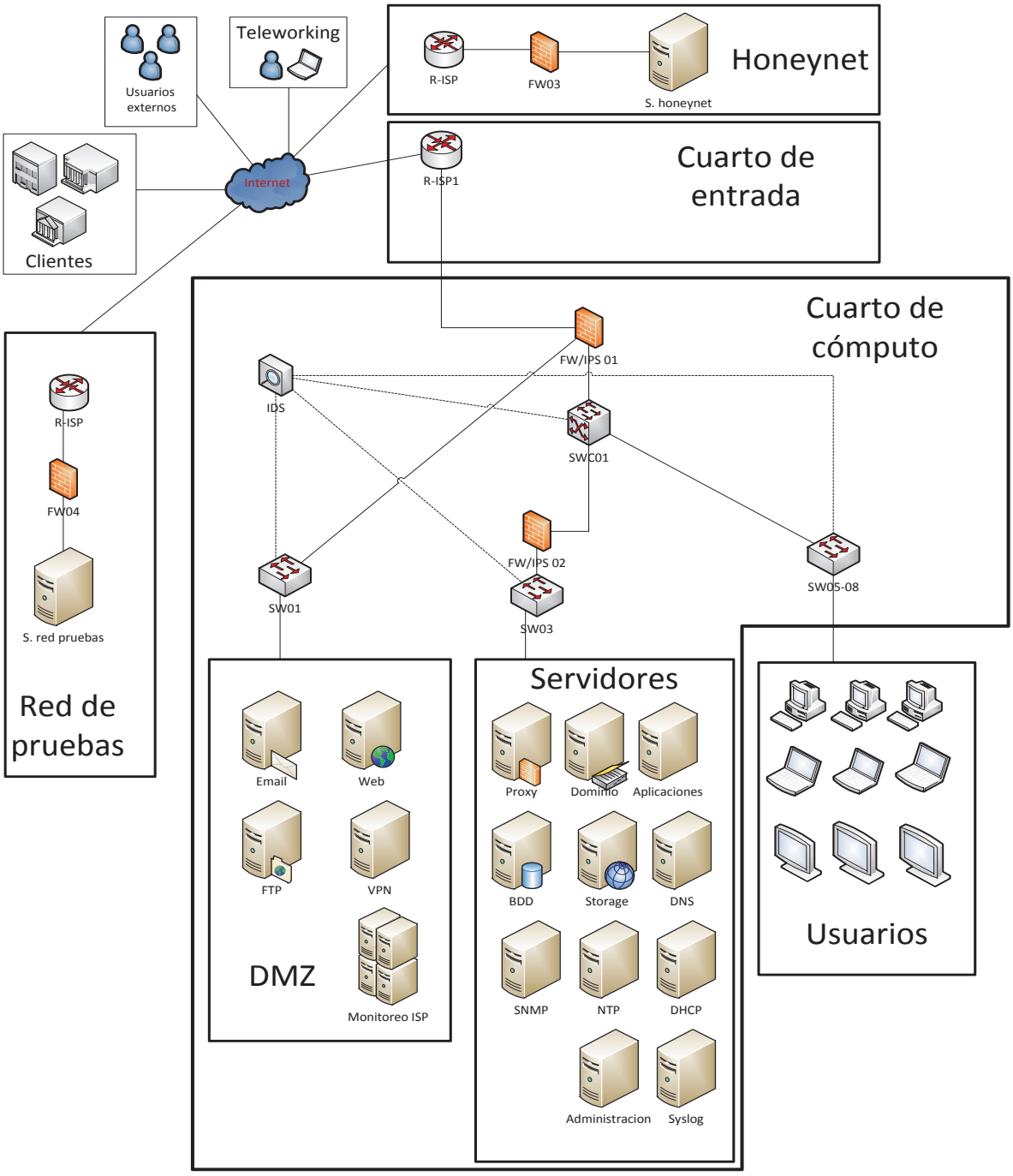

Figura 3.13: Propuesta 2 – diseño de red con redundancia Tier 1

3.1.8.1.Puntos de red actuales y crecimiento de usuarios

El centro de datos del EcuCERT está enfocado principalmente a clientes externos, que accederán a los servicios a través del internet. El crecimiento se centra en mayor medida en ampliar la capacidad del centro de datos para estos clientes, antes que en los puntos de red internos. Según estimados de la Supertel, se espera que en 5 años el número de clientes aumente hasta un 50% (ver punto 2.2.6). Para satisfacer esa demanda se necesita de espacio físico que permita ubicar nuevos equipos. Adicionalmente a los puntos de red listados en la tabla 2.7, se necesitan 4 puntos de red para equipos de visualización del monitoreo del centro de datos, lo que en total daría 44 puntos de red actuales y 49 considerando el crecimiento del 10% indicado en el punto 2.2.6 crecimiento. El diseño no considera puntos de voz, ya que la infraestructura necesaria para este servicio será incluida en la red LAN de la Supertel.

3.2. SELECCIÓN DE EQUIPOS

En ésta sección se determinan los equipos necesarios para la red de EcuCERT y el medio de trasmisión que se utilizará. Los equipos son seleccionados de acuerdo a los requerimientos del capítulo 2 y a la sección 3.1 del presente capitulo. Como se observó en el punto 3.1, se tiene dos propuestas de red: la primera con redundancia N+1 y la segunda sin redundancia. Para la selección de equipos se debe tener en cuenta la ley vigente en el Ecuador para empresas públicas, la cual impide que se mencionen marcas específicas en los pliegos de compras públicas. Por ese motivo el presente proyecto mencionará las características y/o protocolos que deben cumplir los equipos que se necesitan. Sin embargo como parte del presente proyecto de titulación se tiene que elaborar un presupuesto referencial[64], para esto se utilizarán proformas de equipos Cisco y DELL.

3.2.1. SELECCIÓN DEL MEDIO DE TRANSMISIÓN [L3] [E1] [E2]

En el punto 2.2.8 se tiene que uno de los requerimientos para el cableado del centro de datos es el cumplimiento de los estándares TIA/EIA-942 Addendum 2 y

[64] Requerimiento establecido en el plan de titulación

TIA/EIA-568-C. Ambas normas recomiendan el uso de los siguientes medios de transmisión:

- UTP de 100 ohm 6A
- Fibra óptica multimodo 50/125 micrones
- Fibra óptica monomodo

De los tres medios mencionados, la fibra óptica (monomodo y multimodo) es para distancias de *backbone*[65] mayores a 100 metros, como el centro de datos no supera esa distancia no es necesario el uso de fibra (el cual incrementaría el costo del centro de datos). Se utilizará cable UTP categoría 6A (que es la categoría recomendada por ambas normas) tanto para el cableado horizontal como para el cableado de *backbone*. Si bien ambas normas contemplan el uso de cable UTP categoría 5e y categoría 6, éstas limitarían las velocidades de transmisión que puede alcanzar el centro de datos, y debido a la gran cantidad de información que almacenará el centro de datos se necesita de un medio de transmisión que permita grandes velocidades ya que el esquema de red utilizado será del tipo NAS. Por último el uso de medios de transmisión más lentos como UTP categorías 5e y categoría 6 si bien puede no constituir un problema al principio (ya que se desconoce la velocidad de red exacta que necesitará el EcuCERT), complicaría el crecimiento a futuro, dado que cambiar o actualizar el cableado estructurado es un proceso muy complicado y costoso (por lo que ambas normas recomiendan diseñar un sistema de cableado que dure mínimo 10 años). La categoría 7 se descarta, ya que todavía no ha sido aceptada oficialmente por la TIA/EIA al momento de la elaboración de este proyecto. El cable UTP categoría 6A presenta las siguientes características.

- Permite una velocidad de transmisión de 10 Gbps con un ancho de banda de 500 MHz, en distancias de hasta 100 metros, superando al cable UTP categoría 6 que solo permite 250 MHz de ancho de banda y 1 Gbps de velocidad de transmisión. Esta velocidad alarga la vida útil del cableado estructurado.

[65] *Backbone*: se refiere al *backbone* en un centro de datos, el cual se explica en puntos posteriores

- El cable UTP categoría 6A posee un mayor trenzado entre pares que sus predecesores, por lo que presenta mayor tolerancia a fenómenos como la diafonía e interferencia electromagnética.
- Su implementación es más barata que la de la fibra óptica y su manejo es más sencillo.

3.2.2. EQUIPOS NECESARIOS PARA LA RED DEL ECUCERT

Establecido el número de usuarios y el crecimiento de la red del EcuCERT determinados en el capítulo 2 y conociendo el medio de transmisión que se utilizará, se puede pasar a la selección de equipos. En la figura 3.12 se puede apreciar el esquema de red propuesto como resultado del diseño de red detallado en el punto 3.1. A continuación se procederá a listar las características que deben cumplir los equipos de dicho diseño, en base a lo establecido en el punto 3.1. En la tabla 3.4 se puede observar la lista de equipos necesarios para la toda la infraestructura de red propuesta.

Equipo	**Unidades**	
	Sin redundancia	**Con redundancia**
Router	1	2
Switch de core	1	2
Firewall – IPS	2	4
IPS/IDS	1	1
Switch	3 x 24 pts usuarios 2 x 12 pts servidores	3 x 24 pts usuarios 4 x 12 pts servidores
Router (*honeynet* y pruebas)	1 *honeynet* 1 red pruebas	----- -----
Servidores	24 servicios 1 *honeynet* 1 red de pruebas	24 servicios 1 honeynet 1 red de pruebas

Tabla 3.4: Número de equipos necesarios

a. Router Principal, router honeynet y router de red de pruebas

El centro de datos necesita 4 *routers* para la propuesta 1, en la figura 3.12 se pueden apreciar los *routers* R-ISP1 y R-ISP2 para la red principal, y R-ISPH y R-ISPP para las redes *honeynet* y de pruebas respectivamente. Estos equipos pueden ser arrendados al proveedor de servicio de internet que se contrate o pueden ser adquiridos de manera permanente. De acuerdo al punto 3.1.3.2 se necesita que el router cuente con mínimo 2 interfaces *Ethernet* 10/100 y que posea slots de expansión HWIC para permitir el crecimiento a futuro (posibilidad de aumentar el número de interfaces).

Tipo de equipo	Router Administrable
Tipo de montaje	Montable en rack 19”
Puertos	2 x 10/100 Ethernet Ports
Protocolo de administración remota	SNMPv3 SNMPv2, Telnet, SSH, Syslogs
Protocolos de ruteo	RIP-1, RIP-2, IPv4, IPv6 y static routes, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP)
Métodos de autenticación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Características	HSRP (Hot Standby Router Protocol) o VRRP (Virtual Router Redundancy Pro-toco), Access Control List (ACL), Quality of Service (QoS).
Voltaje de entrada AC	100 - 240 [VAC]
Flujo de aire	Back and sides to front
Temperatura de funcionamiento para ambientes de	5 a 40 °C
Humedad relativa de ambiente	5 a 95 %

Tabla 3.5: Resumen de características de los equipos *routers*

Como requerimiento adicional dado por la Supertel, todos los equipos deben soportar el protocolo IPv6 además de IPV4. El *router* debe permiter la implementación de QoS, ya que el “tráfico de monitoreo” proveniente de los ISP debe tener

prioridad sobre otro tipo de tráfico[66]. Los protocolos necesarios son listados a continuación[67]: IPv4, IPv6 y *static routes* por requerimiento interno de la Supertel, *Open Shortest Path First* (OSPF) para la comunicación interna entre los *router* y *switches* capa 3, *Border Gateway Protocol* (BGP) para la comunicación con el proveedor de servicio ISP, IPSec para seguridad en capa 3, posibilidad de implementar subinterfaces, manejo de VLANs, y finalmente para administración se necesitan los protocolos SNMP v3, *Syslogs,* y SSH.

Las características físicas[68] que deben cumplir los *router* son:

- Voltaje de entrada AC (rango): 100 - 240 [VAC][69]
- Montable rack de 19 pulgadas: Si
- Flujo de aire: *Back and sides to front*
- Temperatura de funcionamiento para ambientes de: 5 a 40 °C

Humedad relativa del ambiente: 5 a 95 %

b. Switch de core

La propuesta 1 del centro de datos requiere de dos *switches* de *core* SW *Core* 01 y SW *Core* 02, ver figura 3.12. Como se estableció en los puntos 3.1.1 y 3.1.2 estos serán *switches* de capa 3 del modelo OSI, encargados de conmutar y enrutar todo el tráfico del centro de datos y de la red en general. Aunque físicamente se trata de un solo equipo (con redundancia dos), lógicamente estos equipos agruparán las funciones de módulo de *core* de toda la red, de la capa de *core* del módulo centro de datos intranet, y de la capa de distribución para el módulo de campus. A continuación se describen los protocolos necesarios para cada una de sus funciones.

- Módulo de *core* de toda la red del EcuCERT

Para el módulo de *core* de la red, los *switches* trabajan como equipos de capa dos del modelo OSI, conmutando todo el tráfico entre los diferentes módulos de la red

[66] Se debe realizar un análisis completo de trafico una vez la red se encuentre operativa.
[67] Ver punto 3.2.3.2 para un mayor detalle del diseño del módulo perimetral a Internet
[68] Los valores son una referencia de lo que se tiene en Quito, Ecuador. Si cumple con rangos más amplios de temperatura y humedad puede considerarse como una ventaja en el concurso público.
[69] Voltajes típicos en una red eléctrica

ver punto 3.1.1. Los estándares que debe cumplir para ésta capa son: IEEE 802.3 (*Ethernet*), IEEE 802.3u (*FastEthernet* 100 Mbps), IEEE 802.3ab (*Gigabit Ethernet* sobre UTP). Como se necesita de redundancia tanto de equipos como de enlaces para alcanzar la disponibilidad de un *TIER* 2, se requiere administrar dicha redundancia para lo que se usa *Spannig tree* y sus variaciones: IEEE 802.1D (*Spannig Tree*), IEEE 802.1w (*Rapid Spanning Tree*), IEEE 802.1s (*Multiple Spanning Tree*). Como el EcuCERT cuenta con diferentes perfiles (ver punto 2.2.1) y cada perfil está en una VLAN diferente (para seguridad y administración), se necesita que los equipos soporten IEEE 802.1Q (VLAN). Para el manejo de los diferentes tipos de tráfico (monitoreo, administración, *storage*, aplicaciones, etc.) se necesita IEEE 802.1p (Prioridad de tráfico) para asignar prioridades de tráfico. Para asegurar físicamente el acceso a los puertos de los equipos se necesita IEEE 802.1x (Control de acceso basado en puertos). Finalmente se necesita IEEE 802.1ax (anteriormente llamado 802.3ad) para agregación de enlace, con lo que se espera satisfacer la tendencia de incremento de velocidades de transmisión.

- Capa de *core* del módulo centro de datos intranet

En el módulo centro de datos intranet los *switches* están ubicados lógicamente en la capa de *core* y trabajan en capa 2 y 3 del modelo OSI. Para este módulo los equipos deben soportar todos los protocolos del punto anterior (para funciones de capa 2) añadidos los listados a continuación (ver punto 3.1.2). OSPF para el enrutamiento de la intranet del EcuCERT. *Static IP Routing,* IPv4, IPv6 por requerimiento de la Supertel.

Para manejo de enlaces redundantes de capa 3 (necesarios para garantizar la disponibilidad de un *tier* 2) se necesita los protocolos HSRP[70] (*Hot Standby Router Protocol*) o VRRP (*Virtual Router Redundancy Protoco*). Debido a que estos equipos trabajan en varios módulos es necesaria la aplicación de políticas para permitir o negar flujos de tráficos, por lo que se necesita de *Access Control List* (ACL). Para calidad de servicio, cuando se realicen video conferencias, o para el tráfico de *storage* y/o mantenimiento, es necesario que los equipos manejen *Quality of Service* (QoS).

[70] HSRP es un protocolo privado de Cisco que permite el despliegue de *routers* redundantes; VRRP es su equivalente no propietario definido en el RFC 3768

- Capa de distribución para el módulo de campus

En el módulo de campus los *switches* realizarán las funciones correspondientes a la capa de distribución ver punto (3.1.4.1). Los protocolos y estándares necesarios para ésta función son los mismos que para los puntos anteriores.

Tipo de equipo	Switch Administrable, apilable 12 puertos L3
Tipo de montaje	Montable en rack 19”
Puertos	24 x 10/100/1000 Ethernet Ports
Power over Ethernet (PoE)	No
Protocolo de administración remota	SNMPv3 SNMPv2, Telnet, SSH, Syslogs
Protocolos de ruteo	RIP-1, RIP-2, EIGRP, static IP routing, RIPng
Métodos de autenticación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Características	Layer 3 switching, Layer 2 switching, OSPF Static IP Routing, IPv4, IPv6, HSRP (Hot Standby Router Protocol) o VRRP (Virtual Router Redundancy Protoco), Access Control List (ACL), Quality of Service (QoS).
Estándares	IEEE 802.1D (Spannig Tree); IEEE 802.1w (Rapid Spanning Tree); IEEE 802.1s (Multiple Spanning Tree); IEEE 802.1Q (VLAN); IEEE 802.1p (Prioridad de tráfico); IEEE 802.1x (Control de acceso basado en puertos); IEEE 802.1ax (anteriormente llamado 802.3ad) para agregación de enlace; IEEE 802.3 (Ethernet); IEEE 802.3u (FastEthernet 100 Mbps); IEEE 802.3ab (Gigabit Ethernet sobre UTP).
Backplane	24 Gbps
Voltaje de entrada AC	100 - 240 [VAC]
Flujo de aire	Back and sides to front
Temperatura de funcionamiento	5 a 40 °C
Humedad relativa de ambiente	5 a 95 %

Tabla 3.6: Resumen de características del switch de core

Adicionalmente, se recomienda que tenga mínimo 12 puertos *Ethernet* 10/100/1000. Los *switches* deben ser apilables[71]. Además deben soportar los protocolos SNMP versión 3, syslog, SSH, Kerberos, Radius, Tacacas+ y FTP. La velocidad de conmutación (*backplane*) del switch de *core* debe ser de mínimo 24 Gbps (en caso de que se adquiera un *router* de 24 puertos el *backplane* debe ser de 48 Gbps). El cálculo del *backplane* (para todos los equipos donde se necesite) está de acuerdo a la siguiente fórmula:

$$Backplane_{FullDuplex} = \#\ ptos * Velocidad\ de\ puerto * 2$$

Las características físicas que debe cumplir son:

- Voltaje de entrada AC (rango): 100 - 240 [VAC][72]
- Montable rack de 19 pulgadas: Si
- Flujo de aire: *Back and sides to front*
- Temperatura de funcionamiento para ambientes de: 5 a 40 °C
- Humedad relativa: 5 a 95 %

c. Switch de acceso

La propuesta 1 del centro de datos requiere de 5 *switches* de acceso, para los módulos de centro de datos intranet, DMZ, y campus. Como se estableció en los puntos 3.1.2.1, 3.1.3.1 y 3.1.4.1 estos serán *switches* de capa 2 del modelo OSI, encargados de la conexión con los equipos finales (servidores, PCs, impresoras, etc.). Para capa dos los protocolos y/o estándares que se deben cumplir son: IEEE 802.1x (Control de acceso basado en puertos). Para la conexión se necesita IEEE 802.3 (*Ethernet*), IEEE 802.3u (*FastEthernet* 100 Mbps), IEEE 802.3x (Full Duplex), IEEE 802.3z (*Gigabit Ethernet*) IEEE 802.3ab (*Gigabit Ethernet* sobre UTP) ya que los equipos de los clientes actualmente vienen con tarjetas de red *gigabit*. Para gestionar los enlaces redundantes se utilizarán los protocolos 802.1d (*Spanning tree*), IEEE 802.1w (*Rapid Spanning Tree*) debido a que por motivos de disponibilidad se necesita que exista redundancia de enlaces.

---

[71] Se refiere a la tecnología que permite conectar varios *switches* para que trabajen como uno solo.
[72] Voltajes típicos en una red eléctrica

Tipo de equipo	Switch Administrable, apilable 24 puertos L2
Tipo de montaje	Montable en rack 19”
Puertos	24 x 10/100/1000 Ethernet Ports
Power over Ethernet (PoE)	No
Protocolo de administración remota	SNMPv3 SNMPv2, Telnet, SSH, Syslogs
Métodos de autenticación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Estándares	IEEE 802.1x (Control de acceso basado en puertos), IEEE 802.3 (Ethernet), IEEE 802.3u (FastEthernet 100 Mbps), IEEE 802.3x (Full Duplex), IEEE 802.3z (Gigabit Ethernet) IEEE 802.3ab (Gigabit Ethernet sobre UTP) 802.1d (Spanning tree), IEEE 802.1w (Rapid Spanning Tree), IEEE 8021.1Q (VLAN) y QoS (Calidad de servicio), IEEE 802.1p (Prioridad de tráfico).
Backplane	6.8 Gbps
Voltaje de entrada AC	100 - 240 [VAC]
Flujo de aire	Back and sides to front
Temperatura de funcionamiento	5 a 40 °C
Humedad relativa de ambiente	5 a 95 %

Tabla 3.7: Resumen de características del switch de acceso

Para la segmentación de la red se utiliza IEEE 8021.1Q (VLAN) y QoS (Calidad de servicio) para la calidad de servicio junto con IEEE 802.1p (Prioridad de tráfico). Adicionalmente, se requiere que tenga mínimo 24 puertos *Ethernet* 10/100/1000 y una velocidad de *backplane* de mínimo 10 Gbps. Además deben soportar los protocolos SNMP versión 3, syslog, SSH, Kerberos, Radius, Tacacs+, y FTP.

Las características físicas que debe cumplir son:

- Voltaje de entrada AC: 100 - 240 [VAC][73]
- Montable rack de 19 pulgadas: Si
- Flujo de aire: *Back and sides to front*
- Temperatura de funcionamiento para ambientes de: 5 a 40 °C
- Humedad relativa: 5 a 95 %

d. Firewall-IPS e IDS

El EcuCERT necesita de 4 *firewalls* para la propuesta 1 (ver figura 3.12), que trabajen como *firewalls* y como IPS (ver puntos 3.1.2.1 y 3.1.3.2). Además se necesita de un equipo que trabaje como IDS (ver punto 3.1.7). Los firewall-IPS deben tener un *backplane* de 8.2 Gbps, debe soportar IPSec y permitir mínimo 10 contextos de seguridad (para cumplir con los perfiles de usuario existentes en la red del EcuCERT).

Tipo de equipo	Firewall-IPS Administrable
Tipo de montaje	Montable en rack 19”
Puertos	4 x 10/100/1000 Ethernet 1 x 10/100 Ethernet
Protocolo de administración remota	SNMPv3 SNMPv2, Telnet, SSH, Syslogs
Métodos de autenticación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Firewall backplane	8.5 Gbps
Contextos de seguridad	10 (minimo)
Protocolos	VLANs, IPSec, WAF
Voltaje de entrada AC	100 - 240 [VAC]
Flujo de aire	Back and sides to front
Temperatura de funcionamiento	5 a 40 °C
Humedad relativa de ambiente	5 a 95 %

Tabla 3.8: Resumen de características del firewall

[73] Voltajes típicos en una red eléctrica

El equipo debe contar con balanceo de carga para gestión de enlaces redundantes, ya que cada *firewall* tendrá una conexión hacia cada uno de los *switches* de *core* y *switches* de la DMZ (ver figura 3.12). Debe poder funcionar como WAF para proteger de ataques como inyecciones SQL, o *cross site scripting XSS*. Debe tener 4 interfaces *Ethernet* 10/100/1000 y 1 interfaz *Ethernet* 10/100. El IDS debe tener el mismo *throughput* pero únicamente dos interfaces *Ethernet* 10/100/1000.

Las características físicas que deben cumplir los equipos son:

- Voltaje de entrada AC: 100 - 240 [VAC][74]
- Montable rack de 19 pulgadas: Si
- Flujo de aire: *Back and sides to front*
- Temperatura de funcionamiento para ambientes de: 5 a 40 °C
- Humedad relativa: 5 a 95 %

e. Equipos servidores

A continuación se presenta la elección de equipos servidores para la red. Por requerimientos de la Supertel se necesita que los servidores de la *honeynet* y de la red de pruebas sean completamente independientes, tanto del resto de la red como entre ellos. Por este motivo estos 2 servidores no serán agrupados con ningún otro servicio de la red. Los servidores restantes utilizarán virtualización para contener varios servidores en un solo equipo físico y pueden agrupar varios servicios dentro de un mismo servidor virtual. La agrupación de dichos servicios será en base a la tabla 2.6 del capítulo 2, en dicha tabla se aprecian las necesidades de hardware para cada uno de los servicios de la red del EcuCERT. La tabla 3.9 muestra la agrupación que se realiza en los servidores. Si bien de acuerdo a la norma TIA-942 todos los servidores deberían tener su duplicado (*TIER* II, N+1), en la práctica esto encarecería demasiado el proyecto, por los que los servidores (en una primera etapa) únicamente implementarán redundancia en disco duros (RAID 1), fuente de poder, y tarjeta de red.

Para la virtualización se utilizará VMware vSphere, que es una plataforma de la compañía VMware, ya que es el software que dispone la Supertel actualmente en

[74] Voltajes típicos en una red eléctrica

el “Laboratorio de redes IP de la Dirección Nacional de Investigación Especial”. De acuerdo a su página web VMware vSphere permite correr más de 100 máquinas virtuales, una administración centralizada de las mismas y posibilidad de crecimiento.

Servidores físicos	**Servidores virtuales**	**Servicios por servidor virtual**
Servidor físico A	Servidor virtual A1	Servidor de dominio DHCP DNS Servidor AAA
	Servidor virtual A2	Servidor proxy
	Servidor virtual A3	Servidor SNMP Servidor NTP Servidor de LOGs (internos)
Servidor fisco B (DMZ)	Servidor virtual B1	VPN
	Servidor virtual B2	Correo electrónico Servidor web FTP
Servidor físico C	Servidor virtual C1	Servidor BDD
	Servidor virtual C2	Servidor de aplicaciones
	Servidor virtual C3	Servidor de almacenamiento
Servidor físico D	Servidor virtual D3	Servidor de monitoreo de logs
Servidor físico E	(estimado de 5 máquinas virtuales)	Honeynet
Servidor físico F	(estimado de 5 máquinas virtuales)	Red de pruebas

Tabla 3.9: Virtualización de servidores por servicio

El sistema operativo que se instalará en cada máquina virtual será Centos 6.6 por ser la última versión estable al momento del desarrollo de este proyecto. Los requerimientos mínimos de hardware para este sistema son:

- CPU: Intel Pentium I/II/III/IV/Celeron/Xeon, AMD K6/II/III, AMD Duron, Athlon/XP/MP
- RAM: 128 MB mínimo; 512 MB recomendado
- Espacio en disco: 1.2 GB mínimo; 2.2 GB recomendado

La agrupación de servidores hecha en la tabla 3.9, logra que los equipos A, B, C y D presente capacidades de hardware similares (de acuerdo a la tabla 2.6). Sin embargo como se dijo en capítulos anteriores es imposible conocer con exactitud la capacidad necesaria de CPU, memoria RAM, y tamaño de disco duro necesario.

Procesador	2.40 GHz; núcleos 4 ; cache 10 Megabytes
Sockets procesador	2, Uno instalado
Factor de forma	Rack de 19 pulgadas. 6 UR máximo
Opciones de virtualización	VMware® vSphere ESX™ and ESXi™, Citrix XenServer
Memoria	16 GB DDR3 1600 MHz >20 DIMM slots, actualizable hasta mínimo 256 GB
Controlador Raid	RAID 1, RAID 5
Storage interno	7.2K RPM; SAS 6 Gbps; 3.5 in o 2.5 In Hot-plug Hard Drive Servidor A: 3 TB disponibles almacenamiento Servidor B: 4 TB disponibles almacenamiento Servidor C: 3 TB disponibles almacenamiento Servidor D: 15 TB disponibles almacenamiento Todas deben permitir ampliación a 32 TB disponibles para almacenamiento
Adaptador de red	2 x 1Gb RJ45 2 x 10Gb SFP
Alimentación eléctrica	Dual, Hot-plug, Redundant Power Supply (1+1), 750W
DVD ROM	DVD ROM, SATA, Interno

Tabla 3.10: Características de servidores

Las capacidades mostradas en la tabla 3.10 son estimaciones, por lo que se recomienda un monitoreo constante de la red y equipos servidores (cuando la red se encuentre en operación) para determinar si tienen que ser aumentadas (los servidores elegidos deber permitir crecimiento). De igual forma que en los equipos de *networking*, no se pueden mencionar marcas de equipos para la publicación de pliegos públicos.

La configuración para los servidores que funcionarán como *honeynet* y como red de pruebas varía para disminuir los costos, como se aprecia en la tabla 3.11.

Procesador	1.80GHz, 10MB Cache
Sockets procesador	2, Uno instalado
Factor de forma	Rack de 19 pulgadas, maximo 4 UR
Opciones de virtualización	VMware® vSphere® ESX™ and ESXi™
Memoria	8GB DDR3, 1333 MHz >20 DIMM slots, actualizable hasta mínimo 256 GB
Controlador Raid	RAID 1, RAID5
Storage interno	7.2K RPM; SAS 6 Gbps; 3.5 in o 2.5 In Hot-plug Hard Drive 1 TB disponibles almacenamiento Debe permitir ampliación a 16 TB disponibles para almacenamiento
Adaptador de red	2 x 1Gb RJ45
Alimentación eléctrica	Dual, Hot-plug, Redundant Power Supply (1+1), 400W
DVD ROM	DVD ROM, SATA, Interno

Tabla 3.11: Características de servidores de red de prueba y honeynet

Al ser la información algo primordial para el EcuCERT, se decidió utilizar en todos los servidores RAID 1. Las otras opciones de RAID encarecen los precios y no se considera una opción necesaria ya que al tratarse de un centro de datos *TIER* 2 la norma TIA 942, dice lo necesario más uno. Sin embargo debido a que RAID 5 es más eficiente (relación costo – espacio disponible de almacenamiento), los servidores deben soportar este tipo de RAID para una posible migración de ser necesario.

3.2.3. CÁLCULO DE LA POTENCIA TOTAL [L4]

Para calcular la potencia total es necesario conocer cuánto consume cada equipo del centro de datos. Realizar la suma de las potencias, obtener el total en vatios [W] y aumentar el 10 % de crecimiento. Al valor obtenido se debe añadir los equipos de los 10 usuarios que trabajan en el EcuCERT. Estableciendo un promedio de 700 W por PC[75] de cada usuario, se tiene que se necesitan 7000 W. Adicionalmente se tendrá 4 monitores LCD para monitoreo del centro de datos, con un

[75] El valor de 700 W por PC es un valor relativamente alto que nos permite un margen de error amplio a la hora de dimensionar el UPS

estimado de 170 W por televisor, se tiene una potencia de 680 W**.** Debido a que uno de los objetivos del presente proyecto es la elaboración de un presupuesto referencial, y que para el dimensionamiento del UPS que se necesita conocer exactamente que equipos se colocarán, se procede a seleccionar las marcas de los equipos de *networking* y servidores. Estos equipos cumplirán los protocolos y estándares del punto 3.2.2 y servirán únicamente como ejemplo para los puntos posteriores del trabajo.

Equipo	**Unidades**	**Potencia por unidad***	**Potencia total**
Router	2	320 W	640 W
Router (honeynet, pruebas)	2	80 W	160 W
Switches de core	2	99 W	198 W
Switches de acceso	8	39 W	312 W
Firewall	4	190 W	750 W
IDS/IPS	1	190 W	190 W
Servidores A, B, C, D	4	750 W	3000 W
Servidores E, F	2	495 W	990 W
Total			**6240 W**

*Valores tomados de los *datasheet* de cada equipo seleccionado

Tabla 3.12: Potencia total consumida por equipos de networking

En la tabla 3.12 se puede apreciar la potencia en vatios de cada uno de los equipos seleccionados, así como la potencia necesaria para el centro de datos al cual es de 6240 W solo para equipos de *networking* y servidores. Con un crecimiento esperado del 10 % se tiene que la potencia necesaria es: 6864 W. Sumando los resultados anteriores (7000 W de las PC, 680 W de monitores, y 6864 W equipos de *networking*) se tiene que la potencia necesaria para el centro de datos es de **14544 W.** No se consideran las 25 PCs para los laboratorios de los cursos de capacitación debido a que éstas estarán conectadas al UPS de la Supertel directamente.

3.2.4. CÁLCULO Y DIMENSIONAMIENTO DEL UPS [L4]

Con la potencia total obtenida se procede al cálculo del UPS. Para el cálculo se considera un factor de potencia de 0.9[76], para obtener la potencia aparente. La potencia aparente se mide en Volta-Amperios [VA], que es la unidad en la que por lo general se comercializan los UPS. A continuación se muestran el cálculo de dicha potencia, en base al triángulo de potencia de la figura 3.14.

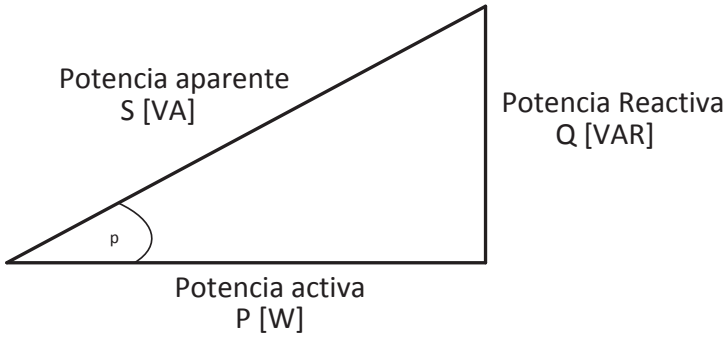

Figura 3.14: Triángulo de potencias

$$\cos(\rho) = \frac{P[W]}{S[VA]}$$

$$S[VA] = \frac{14544}{0.9} \cong 16160\ [VA]$$

Del cálculo anterior se tiene que se necesita un UPS de mínimo 16 KVA. Ya que los *16160 VA* sería en el caso en que todos los equipos se encuentren al 100 % de su capacidad, cosa poco probable. En cada rack se instalará una regleta con 7 tomas para los diferentes equipos. Los 16 KVA son únicamente para equipos de TI, el UPS para los sistemas de refrigeración es independiente. Como se trata de un centro de datos *Tier* II se deben adquirir 2 UPS, también se puede optar por

[76] APC Electric by Schneider Electric 2013

UPS que poseen componentes redundantes dentro de un solo case. Las características que debe cumplir[77] el UPS son:

- Capacidad en volta amperios: 16 KVA
- Capacidad en vatios: 11.2 KW
- Voltaje de entrada: 110 – 276 VAC
- Factor de potencia: >0.98
- Frecuencia de entrada: 40 - 70 Hz
- Tiempo de autonomía (carga completa): 20 min con posibilidad de expansión
- Componentes redundantes
- Voltaje de salida: 208/120 o 240/120
- Frecuencia de salida: 60 Hz
- Disipación de calor: < 4500 BTU
- Monitoreo: SNMP/RS232

3.3. DISEÑO DEL CENTRO DE DATOS [E1]

El diseño del centro de datos se refiere a los diferentes espacios físicos que conforman el centro de datos. El presente proyecto toma como referencia las áreas o espacios propuestos por la norma EIA/TIA 942. La figura 3.15 muestra la relación de espacios entre el centro de datos y otras áreas del edificio, en la figura 3.15 se pueden observar las siguientes áreas:

a) Fuera del centro de datos se encuentra localizado el equipo DTU del proveedor de servicios.
b) Dentro del centro de datos se encuentra:
   - Cuarto de entrada
   - Cuarto eléctrico y mecánico
   - Oficinas del personal de soporte del centro de datos
   - Oficinas y centro de operaciones
   - Cuarto de telecomunicaciones

[77] Cada uno de los UPS que se adquiera debe poder soportar el total de la carga es decir los 16 KVA

- Cuarto de cómputo
- Bodega y punto de carga

De acuerdo a la norma TIA 942, no es obligación que un centro de datos implemente todos los espacios mencionados, ni que todos sean ubicados en ambientes separados como indica la figura 3.15, pero es recomendado que así sea para mejorar la administración de los mismos, especialmente en centros de datos de gran tamaño. De los espacios mencionados este proyecto se enfoca principalmente en el cuarto de cómputo, cuarto de entrada y cuarto de telecomunicaciones. No se cuenta con un cuarto de equipos eléctricos, ya que estos serán ubicados dentro del cuarto de cómputo (de acuerdo con la norma TIA 942). Para los ambientes donde se ubica el personal del EcuCERT (oficinas del personal y centro de operaciones), se recomienda un área adyacente al centro de datos y con espacio suficiente para los puestos de trabajo y para que todos los empleados puedan desplazarse libremente.

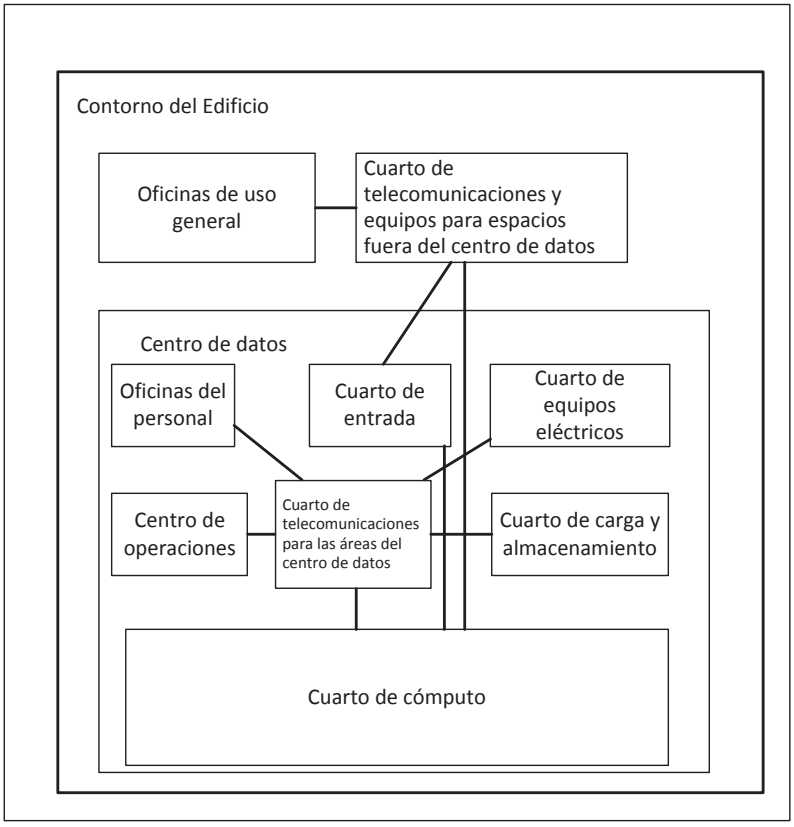

Figura 3.15: Relación de espacios en un centro de datos [E1]

3.3.1. INFRAESTRUCTURA DEL SISTEMA DE CABLEADO DEL CENTRO DE DATOS [E1]

De acuerdo a la norma EIA/TIA 942, los elementos del sistema de cableado que compone el centro de datos son:

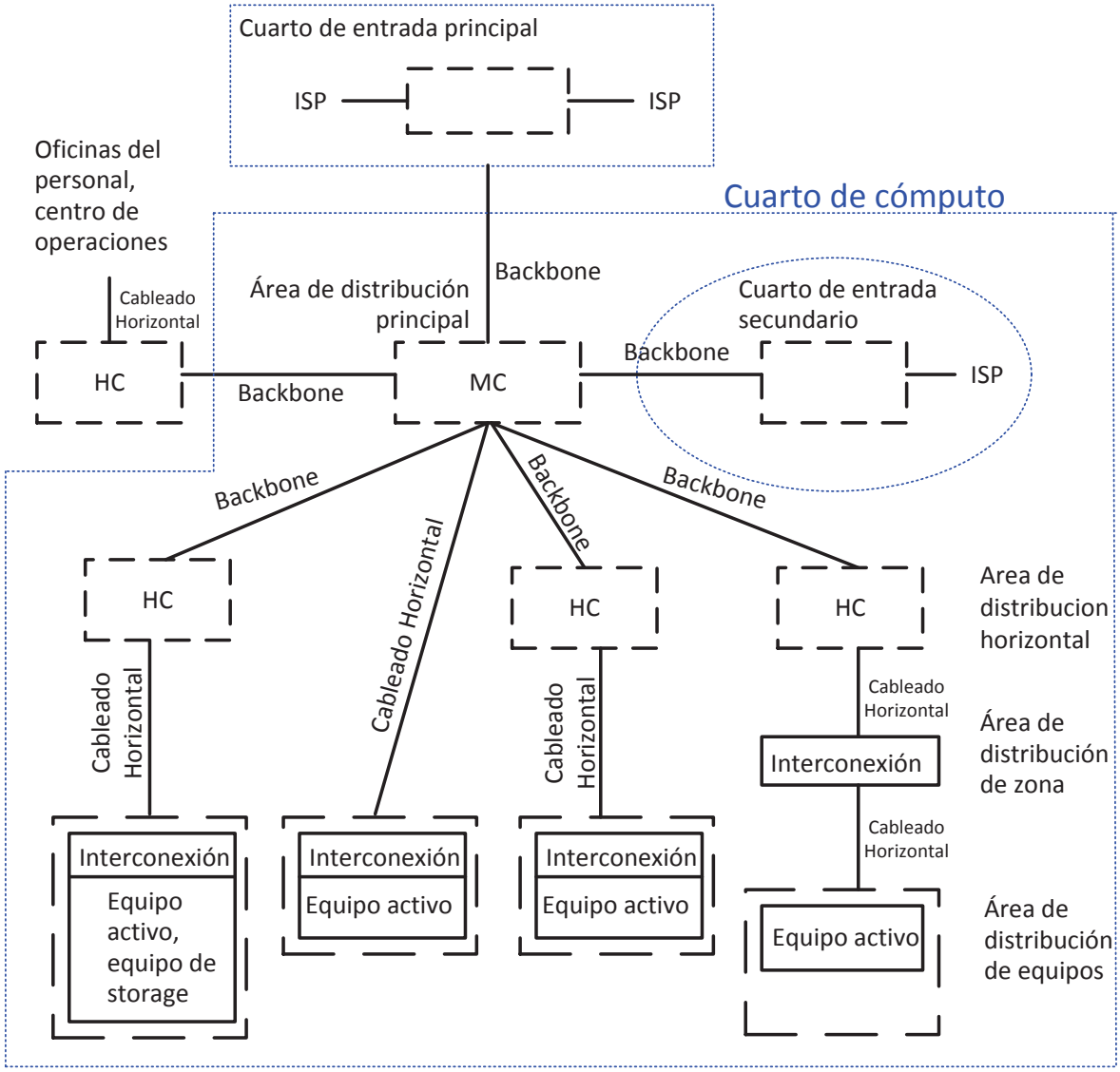

Figura 3.16: Infraestructura del sistema de cableado del centro de datos[E1]

- Cableado horizontal
- Cableado principal (*backbone*)

- Conexión cruzada en el cuarto de entrada o en el área de distribución principal
- Conexión cruzada principal (MC) en el área de distribución principal
- Conexión cruzada horizontal (HC) en el cuarto de telecomunicaciones, área de distribución horizontal, o áreas de distribución principal.
- Punto de consolidación en el área de distribución de zona
- Puntos de red o tomas en el área de distribución de equipos

La figura 3.16 muestra los diferentes elementos descritos y permite observar la topología de un centro de datos, así como la relación existente entre los diferentes elementos que conforman el mismo.

3.3.2. TOPOLOGÍA DEL CENTRO DE DATOS [E1]

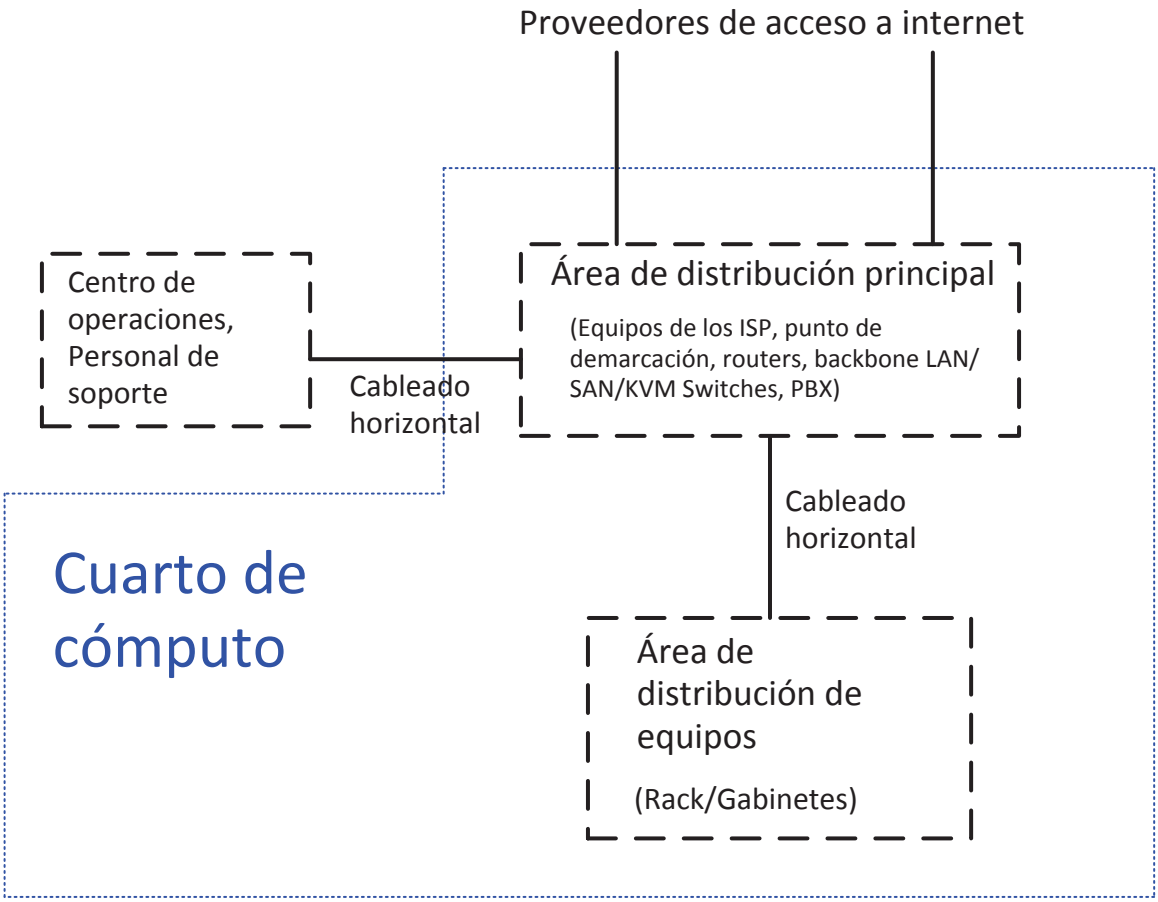

Figura 3.17: Propuesta de diseño del centro de datos del EcuCERT [E1]

La norma TIA 942 presenta una propuesta de diseño para centros de datos pequeños como es el caso del EcuCERT. La figura 3.17 muestra el diseño propuesto para el centro de datos del EcuCERT. Los espacios o áreas típicas que conforman un centro de datos de acuerdo a la norma TIA 942, son: cuarto de entrada, área de distribución principal (MDA), área de distribución horizontal (HDA), área de distribución de zona (ZDA), y área de distribución de equipos (EDA). Para el caso puntual del diseño del EcuCERT el área de distribución principal agrupa la conexión cruzada principal y la conexión cruzada horizontal, situación que contempla la norma TIA-942 para centro de datos pequeños.

3.3.2.1.Descripción de los elementos del centro de datos [E1]

3.3.2.1.1. Cuarto de entrada

El cuarto de entrada es el espacio que sirve como punto de conexión entre el cableado del centro de datos (cableado interno del EcuCERT) y la red del proveedor de servicios, es decir constituye el punto de demarcación.[78] En ésta área se ubican los equipos de los ISP. Es recomendable que se encuentre fuera del cuarto de cómputo para mayor seguridad. En caso de que esto no sea posible deberá estar ubicado adyacente o incluso combinado con el área de distribución principal, como es el caso del EcuCERT. El cuarto de entrada es donde se ubican los equipos del módulo perimetral a internet, específicamente el perímetro del proveedor de servicios.

3.3.2.1.2. Cuarto de cómputo

El cuarto de cómputo es el espacio diseñado con el único propósito de alojar equipo y cableado relacionado directamente con la infraestructura de red del EcuCERT. Como se observa en la figura 3.17 el cuarto de cómputo contiene al área de distribución principal, al área de distribución horizontal, al área de distribución de zonas y al área de distribución de equipos. Las características físicas de ubicación del cuarto de cómputo, acceso, arquitectura, ambiente, cableado eléctrico, protección contra fuego, ubicación de racks/gabinetes, ubicación de equipos en el rack/gabinete, distancia entre racks, anchos de pasillos y ventilación

[78] El punto de demarcación representa el límite de la responsabilidad del proveedor de servicios. En ese punto el cableado externo se une al cableado interno del edificio.

de gabinetes seguirán las recomendaciones establecidas por la norma TIA 942 y pueden observarse en las figuras 3.27 y 3.30.

3.3.2.1.3. Área de distribución principal

El área de distribución principal alberga la conexión cruzada principal (MC) para el sistema de cableado estructurado. Para el diseño propuesto también alberga la conexión cruzada horizontal y el cuarto de entrada. Está localizada dentro del cuarto de cómputo. En centro de datos muy grandes puede estar en un cuarto dedicado. Todo centro de datos debe tener por lo menos un área de distribución principal. La norma TIA-942 especifica racks separados para los cables de fibra, UTP[79] y coaxial. El área de distribución principal puede atender una o más áreas de distribución horizontal, o áreas de distribución de equipo dentro del cuarto de cómputo y uno o más cuartos de telecomunicaciones fuera del cuarto de cómputo. En esta área se encuentran los *routers* de *core*, los *switches* de *core*, *switches* de SAN[80] y PBX[81]. Esta área será donde se ubiquen los equipos del módulo de *core*.

3.3.2.1.4. Área de distribución horizontal

En el área de distribución horizontal se ubican las conexiones cruzadas horizontales (HC), y el punto de distribución para el cableado hacia las áreas de distribución de los equipos. Está localizada dentro del cuarto de cómputo pero puede ubicarse en un cuarto dedicado para mejorar la seguridad. Para el caso del EcuCERT, esta área se encuentra integrada en el área de distribución principal. En esta área se ubican los *switches* LAN, *switches* KVM[82], *switches* SAN. Esta área contiene los equipos de los módulos de campus y los *switches* de acceso de los módulos del centro de datos intranet y de la DMZ.

3.3.2.1.5. Área de distribución de zonas

El área de distribución de zonas es el área para los equipos que van a suelo y no pueden aceptar paneles de parcheo (patch panel), por ejemplo servidores tipo torre. El centro de datos del EcuCERT, no cuenta con esta área.

---

[79] Par trenzado sin blindaje por sus siglas en inglés. Es un tipo de cable usado como medio de trasmisión para conexiones de red.
[80] Red de área de almacenamiento por sus siglas en inglés
[81] PBX, es una central telefónica privada conectada directamente a la red de telefonía pública.
[82] Teclado/video/mouse, por sus siglas en inglés

3.3.2.1.6. Áreas de distribución de equipos

El área de distribución de equipos es el área donde se ubican los gabinetes y racks de los servidores. La norma TIA 942 especifica que los gabinetes y racks se deben colocar en una configuración *"hot aisle/cold aisle",* pasillo caliente/pasillo frío. En puntos posteriores se verá a mayor detalle el diseño para ventilaciones.

3.3.2.1.7. Cuarto de operaciones

El cuarto de operaciones es el espacio donde se ubicará el personal encargado de monitorear el centro de datos. Para el caso del EcuCERT este espacio contendrá a todo el equipo del personal técnico. Estará ubicado adyacente al cuarto de cómputo.

3.4. SISTEMA DE CABLEADO DEL CENTRO DE DATOS

Como se dijo en el punto 3.2.1 se utilizará cable UTP categoría 6A para el sistema de cableado. El sistema de cableado debe ser pensado como un ambiente multi-producto y multi-vendedor, de tal manera que no sea dependiente de un solo fabricante. A continuación se describen los diferentes componentes del sistema de cableado.

3.4.1. CABLEADO HORIZONTAL [E1]

El cableado horizontal es la porción de cableado que se extiende desde la zona de distribución de equipos hasta la conexión cruzada horizontal (HC), en el área de distribución horizontal; o hasta la conexión cruzada principal (MC), en el área de distribución principal. Las figuras 3.15 y 3.16 muestran los diferentes tipos de cableado existentes en el centro de datos. El cableado horizontal incluye los cables, los terminales mecánicos, patch cords[83] o jumpers[84] y puede incluir puntos de consolidación en el área de distribución de equipos. Para el cableado horizontal se utilizará una topología en estrella como dice la norma TIA 942. Las terminales de conexión en el área de distribución de equipos deben estar conectadas con la conexión cruzada horizontal o con la conexión cruzada principal. Se debe ase-

[83] Es un cable que se usa para conectar un dispositivo de red con otro
[84] Llamado también Puente, sirve para conectar dos terminales de manera temporal.

gurar que el cableado horizontal no contenga más de un punto de consolidación en el área de distribución de equipos.

La distancia que recorre el cableado horizontal no debe sobrepasar los 90 metros, independiente del medio de transmisión. La distancia total desde un equipo a otro (incluyendo el patch cord) no debe sobrepasar los 100 metros. La distancia máxima en un centro de datos sin incluir el área de distribución horizontal es de 300 metros para fibra, y 100 metros para cobre, en ambos casos incluyendo los patch cord. Para el caso del EcuCERT, se espera que las oficinas que atenderá el centro de datos se encuentren ubicadas en el mismo piso, razón por la cual no se necesita un cuarto adicional de telecomunicaciones o de equipos.

3.4.2. CABLEADO BACKBONE [E1]

El *backbone* es el cable entre el área de distribución principal y el área de distribución horizontal. El cableado de *backbone* puede incluir los cables, la conexión cruzada principal, conexión cruzada horizontal, patch cord y jumpers. El cableado de *backbone* debe permitir reconfiguraciones de red y crecimiento, y no debe verse alterado por estos. Para seguir la recomendación de la norma TIA 942 se utilizará una topología jerárquica en estrella como se observa en la figura 3.18. Sin embargo también se puede usar otros tipos de topología como anillo. En caso de que no exista el área de distribución horizontal como es el caso del EcuCERT, el cable que conecta el área de distribución de equipos con el área de distribución principal se lo considera cable horizontal. Para el caso del EcuCERT se eligió el cable UTP categoría 6 A 100 ohm, el cual está contemplado por la norma TIA-942 (la norma también contempla el uso de fibra óptica multimodo 62.5/125 micrones o 50/125 micrones, y fibra mono modo).

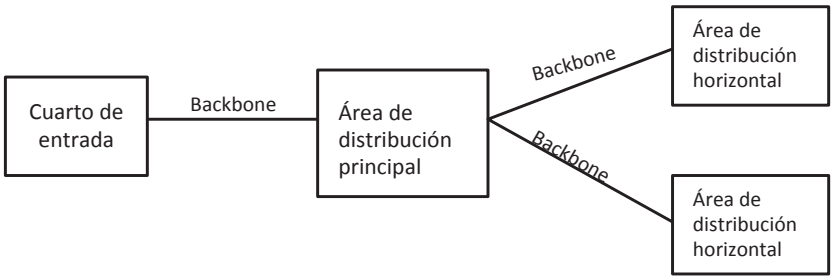

Figura 3.18: Topología de cableado de *backbone* [E1]

Las distancias del cableado de *backbone* dependen del medio que se utilice. Para el caso del cable UTP categoría 6A, la distancia máxima permitida es de 90 metros, lo que dejaría un margen de 10 metros para los patch cord a ambos extremos. El recorrido de cableado de un centro de datos sigue al norma ANSI/TIA-569-B. A continuación se muestran algunas consideraciones básicas para el diseño.

a) No se debe colocar el cable a través de espacios que sean accesible a al público en general, al menos que el cable se encuentre dentro de ductos o tubería cerradas.
b) Se debe colocar en bandejas separadas los cables de alimentación eléctrica y los cables de red.
c) Los cables de red colocados en el piso falso deben ir en bandejas.
d) Los cables de alimentación eléctrica pueden estar colocados directamente sobre el piso (no es necesario usar bandejas o escalerillas).

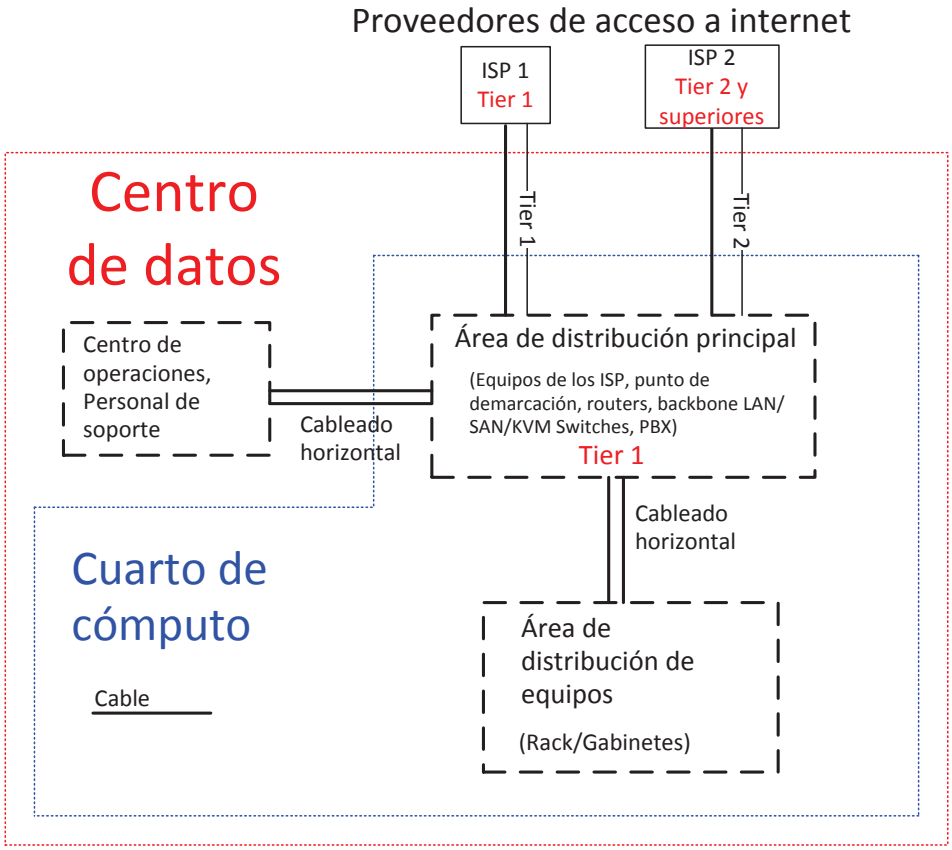

Figura 3.19: Redundancia en el centro de datos del EcuCERT [E1]

La norma TIA 942 también establece la redundancia que debe tener el sistema de cableado del centro de datos el cual está determinado por el "*Tier*" como se observa en la figura 3.19.

3.4.3. ETIQUETADO

El etiquetado es fundamental para la organización del cableado del centro de datos. La norma EIA/TIA-942 en su anexo B muestra información sobre ejemplos de etiquetado basados en la norma ANSI/TIA/EIA-606-B. La norma ANSI/TIA/EIA-606-B, establece cuatro clases de etiquetados, de acuerdo al tamaño de la estructura, así la clase uno es para centros de datos con un solo rack, la clase dos para instalaciones con varios racks en un solo edificio, la clase tres para instalaciones con varios edificios repartidos en un campus y la clase cuatro para instalaciones muy grandes que abarcan varios campus con varios edificios. La norma ANSI/TIA/EIA-606-B, obliga a que se tome como referencia para el etiquetado los distintos elementos que conforman el cableado estructurado como racks, patch panels y gabinetes. Para el etiquetado del EcuCERT, se utilizará la propuesta de la norma ANSI/TIA/EIA-606-B específicamente para la clase dos junto con la norma EIA/TIA-942.

3.4.3.1.Identificación de los rack y gabinetes

Para etiquetar los rack y gabinetes primero se debe etiquetar y numerar las baldosas del piso en un sistema de coordenadas "*x,y".* Hecho esto se procede a alinear cada rack o gabinete en su esquina frontal derecha con la esquina de una de las baldosa, como se observa en la figura 3.20. De esta forma el rack mostrado en la figura 3.20 sería conocido como rack *AJ05.*

Dónde:

AJ = la coordenada en "x"

05 = la coordenada en "y"

Para considerar una futura expansión, en la que el centro de datos del EcuCERT crezca a otros pisos del edificio se antepondrá un número que será el identificador del piso del edificio, quedando *01AJ05,* donde *"01"* sería el identificador del piso uno.

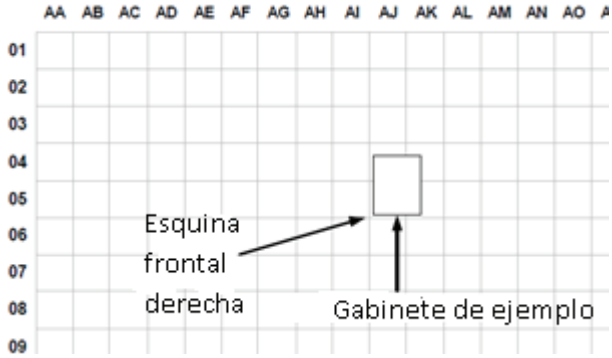

Figura 3.20: Alineación de rack y gabinetes [E1]

Para identificar los patch panel en un rack, la norma TIA-942 establece que se debe asignar una letra a cada patch panel empezando desde la parte superior. Y un número para identificar el puerto en el patch panel. De esta forma se tiene "*An";* donde *"A"* se refiere al patch panel *A* de la figura 3.21 y "*n"* sería el número de puerto en el patch panel *A.*

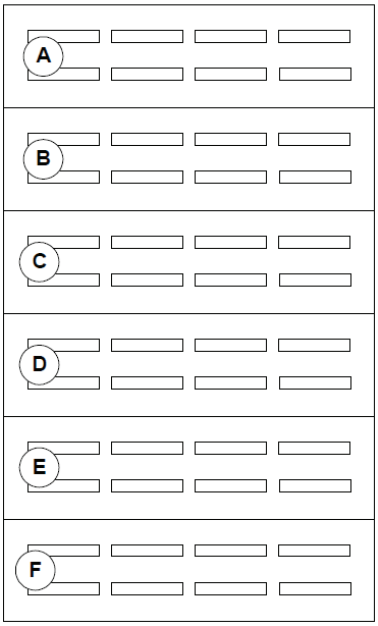

Figura 3.21: Identificación de patch panel [E1]

La norma TIA 942 también considera el etiquetado para identificar que patch panels están conectados entre sí. Esta etiqueta tiene que incluir hacia donde se están conectando, a que otro grupo de patch panel y en que rack. El etiquetado tiene que ser en la forma *p1 to p2,* donde *p1* es el rack cercano y *p2* es el rack lejano. Por ejemplo para identificar la conexión que se muestra en la figura 3.22 se tendría lo siguiente:

AJ05-A to AQ03-B Ports 01-24

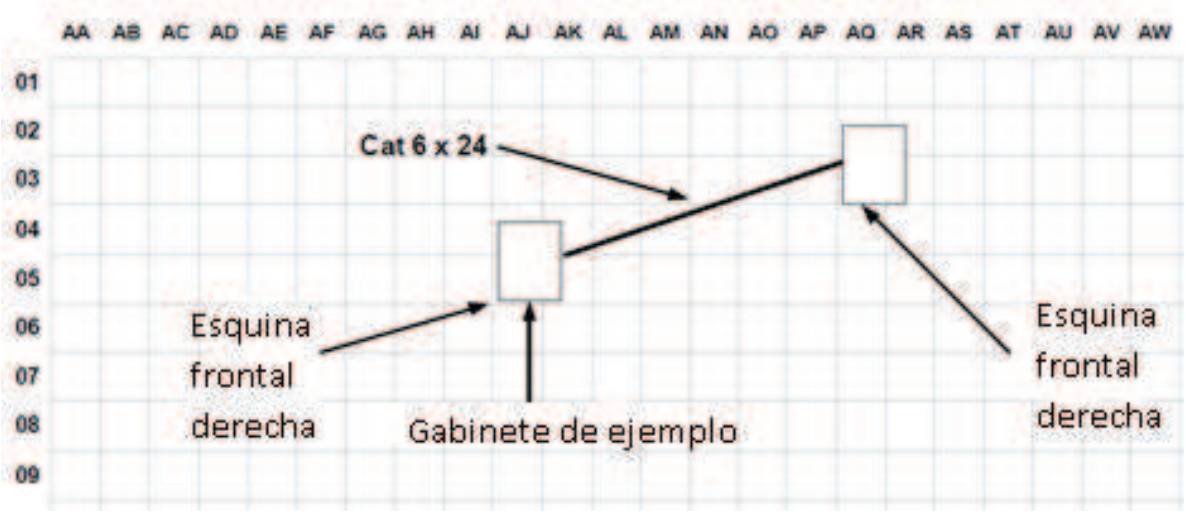

Figura 3.22: Identificación de la conexión entre patch panels [E1]

Dónde:
AJ05 = es el primer rack
A = es el patch panel A del rack AJ05
AQ03 = es el segundo rack del ejemplo
B = es el patch panel B del rack AQ03
Ports 01-24 indica que el patch panel AJ05-A interconecta como *mirror* sus 24 puertos con los puertos del patch panel AQ03-B.

La figura 3.23 muestra cómo quedaría el etiquetado del ejemplo ya colocado en el patch panel.

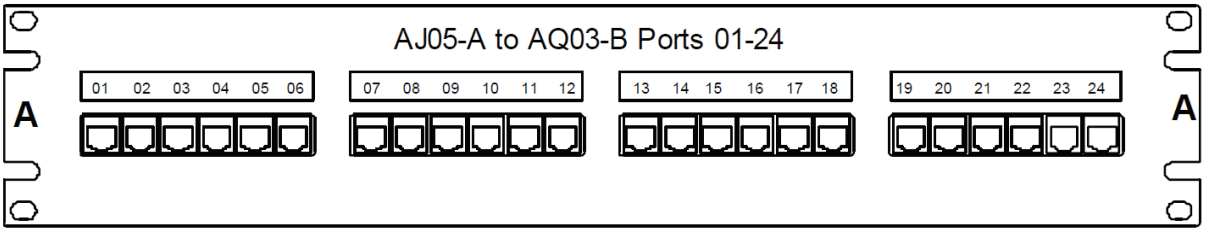

Figura 3.23: Ejemplo de etiquetado de patch panel [E1]

La norma TIA 942 también establece cómo debe ser el etiquetado de los cables y patch cord. Los cables deben ser etiquetados en ambos extremos. Se recomienda usar diferente color de cables para diferenciar entre aplicaciones. La norma TIA-942 recomienda el siguiente esquema de etiquetado:

p_{1n} *to* p_{2n}

Dónde:

p_{1n} = el rack más cercano y el puerto de conexión

p_{2n} = el rack más lejano y el puerto de conexión.

Por ejemplo para las figuras 3.22 y 3.23, el cable conectado en el primer puerto del rack *AJ05* llevaría la siguiente etiqueta: *AJ05-A01 to AQ03-B01;* y el mismo cable en el rack AQ03 llevaría la etiqueta: *AQ03-B01 to AJ05-A01.*

3.5. CUARTO DE CÓMPUTO

El cuarto de cómputo del centro de datos del EcuCERT estará formado por un área de distribución principal y un área de distribución de equipos. Esta será el área donde se encuentran todos los equipos del centro de datos.

3.5.1. ETIQUETADO DE EQUIPOS SERVIDORES

El diseño del EcuCERT propuesto incluye el etiquetado de los equipos de *networking* y servidores, de la siguiente manera.

RRC01

Dónde:

RR = es el tipo de equipo el cual puede ser:

RR: router

SW: switch

SR: servidor

FW: firewall

C = tipo de dispositivo el cual puede ser:

C: equipo de core

D: equipo de distribución

A: equipo de acceso

F: final

I: ISP

01 = el número de equipo en la red

Equipo	Unidades de RACK	Nomenclatura
Switch de core SW1	2	SWC01
Switch de core SW2	2	SWC02
Firewall FW1	1	FWA01
Firewall FW2	1	FWA02
Router del proveedor de servicios 1	2	RRI01
Router del proveedor de servicios 2	2	RRI02
Router del proveedor de servicios Honeynet	1	RRI03
Router del proveedor de servicio red de pruebas	1	RRI04
Firewall FW3	1	FWA01
Firewall FW4	1	FWA02
Switch de acceso 1	1	SWA01
Switch de acceso 2	1	SWA02
Switch de acceso 3	1	SWA03
Switch de acceso 4	1	SWA04
Switch de acceso 5	1	SWA05
Switch de acceso 6	1	SWA06
Switch de acceso 7	1	SWA07
TOTAL	**21**	

Tabla 3.13: Etiquetado de equipos de networking y unidades de rack por equipo

Como se puede observar en la tabla 3.13 se necesita de 21 UR disponibles solo para equipos (sin contar patch panel para interconexión de equipos y conexiones cruzadas). El diseño propuesto plantea la utilización de 3 racks para el área de distribución principal cada uno de 42 UR, lo que consideraría y permitiría crecimiento en el futuro.

3.5.2. ÁREA DE DISTRIBUCIÓN PRINCIPAL

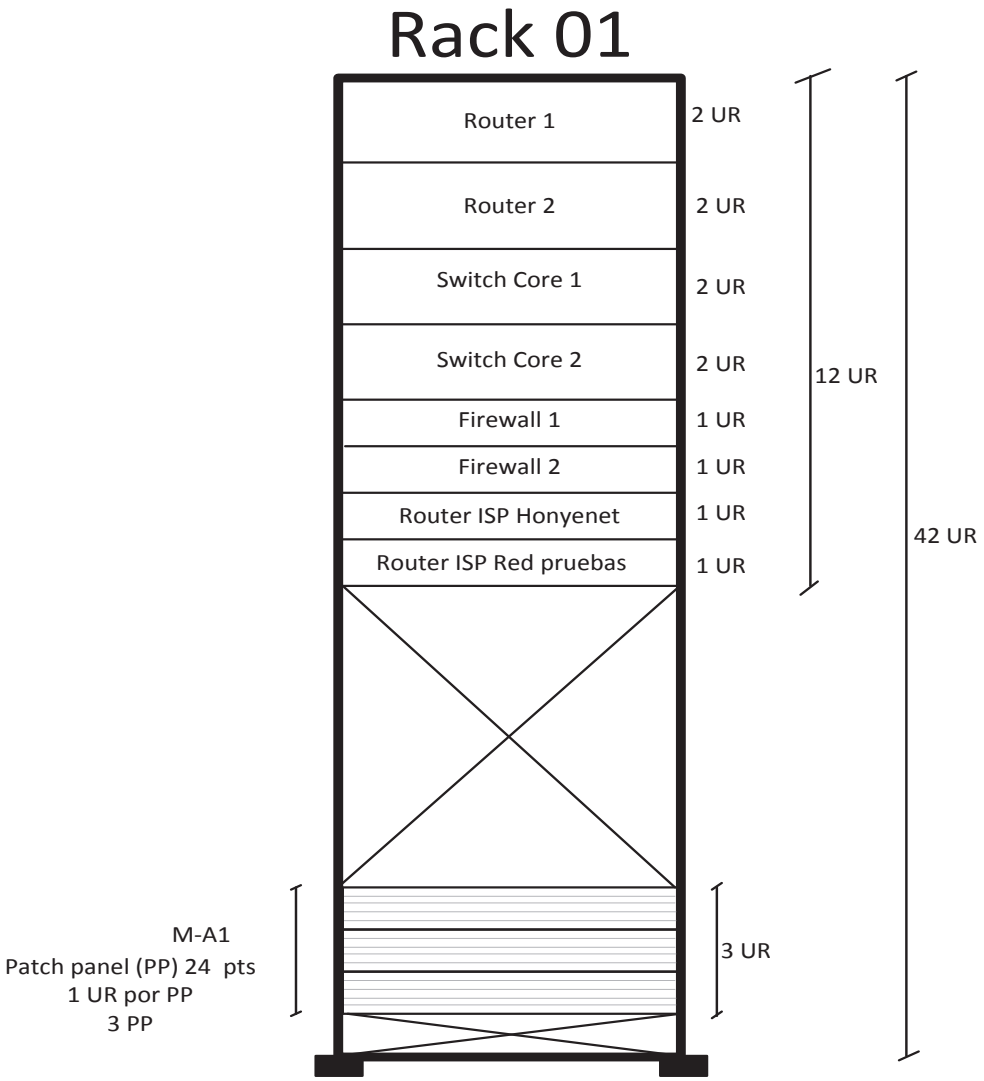

Figura 3.24: Ubicación de equipos y patch panels en el rack 1 en MDA

Para el caso del EcuCERT, el área de distribución principal incluye también el área de distribución horizontal y el cuarto de entrada. El área de distribución principal contiene los siguientes equipos:

- Switch de core SW1
- Switch de core SW2
- Firewall FW1
- Firewall FW2
- Router del proveedor de servicios 1
- Router del proveedor de servicios 2
- Router del proveedor de servicios *Honeynet*
- Router del proveedor de servicio red de pruebas.
- Firewall FW3
- Firewall FW4
- Switch de acceso 1 al 8

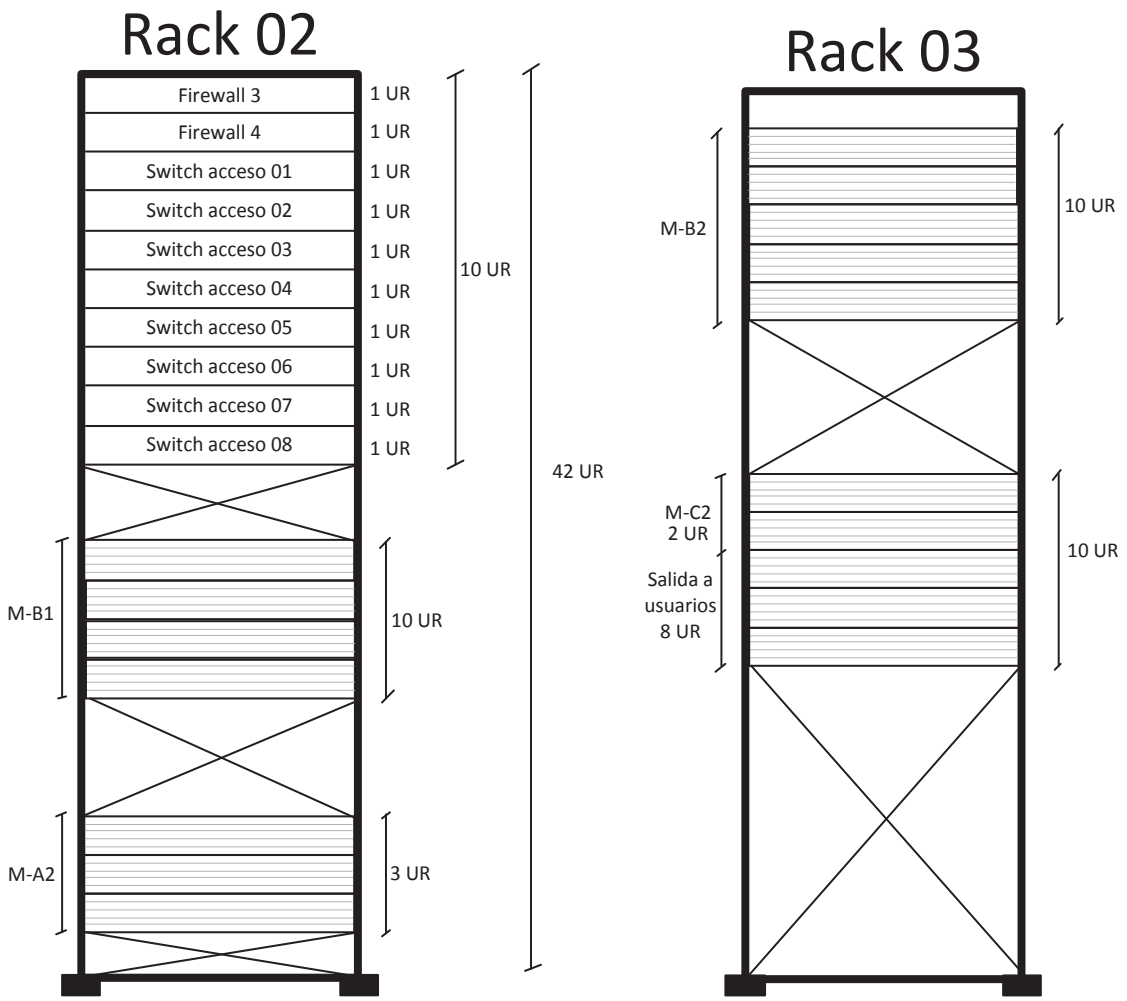

Figura 3.25: Ubicación de equipos y patch panel de conexión rack 2 y 3 en MDA

La tabla 3.13 detalla las unidades de rack necesarias para cada equipo, y el nombre o nomenclatura que se utilizará para referirse al mismo. Las figuras 3.23 y 3.24 muestran la ubicación física de los equipos dentro de los racks. Como se aprecia en ambas figuras los patch panel de los rack 1 y 2 son para realizar la interconexión entre los equipos ubicados en dichos rack. De esta forma se tiene que los patch panel en el rack 2 llamados M-A2, son un espejo (*mirror)* de los patch panel del rack 01, M-A1. El rack 3 cumple la función de conexión cruzada principal. En el rack 3 solo se ubican patch panel, no cuenta con equipos, al ser también el área de distribución horizontal es el punto al cual se conecta el *backbone* del edificio.

3.5.3. ÁREA DE DISTRIBUCIÓN DE EQUIPOS

Equipo	Unidades de RACK	Nomenclatura
Servidor 01	2 UR	SRF01
Servidor 02	2 UR	SRF02
Servidor 03	2 UR	SRF03
Servidor 04	2 UR	SRF04
Servidor 05	2 UR	SRF05
Servidor 06	2 UR	SRF06

Tabla 3.14: Etiquetado de servidores y unidades de rack por servidor

En el área de distribución de equipos se encuentra los servidores del EcuCERT. En la tabla 3.10 se puede apreciar la nomenclatura y las unidades de rack necesarias para cada servidor. La figura 3.26 muestra la ubicación dentro del rack de los servidores, y los patch panels necesarios para los mismos. De igual manera los patch panel del rack 4 “M-C1”, tiene su respectivo *mirror* en los patch panels del rack 3 “M-C2”.

3.5.4. UBICACIÓN DE LOS RACKS DENTRO DEL CUARTO DE CÓMPUTO

La figura 3.27 muestra el tamaño necesario para el cuarto de cómputo, y la distribución física de los rack dentro del mismo. Es preferible que el UPS y el tablero eléctrico de potencia estén ubicados en otra habitación. Sin embargo para el caso del EcuCERT, el UPS puede estar ubicado dentro del cuarto de cómputo ya que

su valor es mucho menor que los 100 KVA, que es lo máximo permitido por la norma TIA-942 para que esté dentro del cuarto de cómputo.

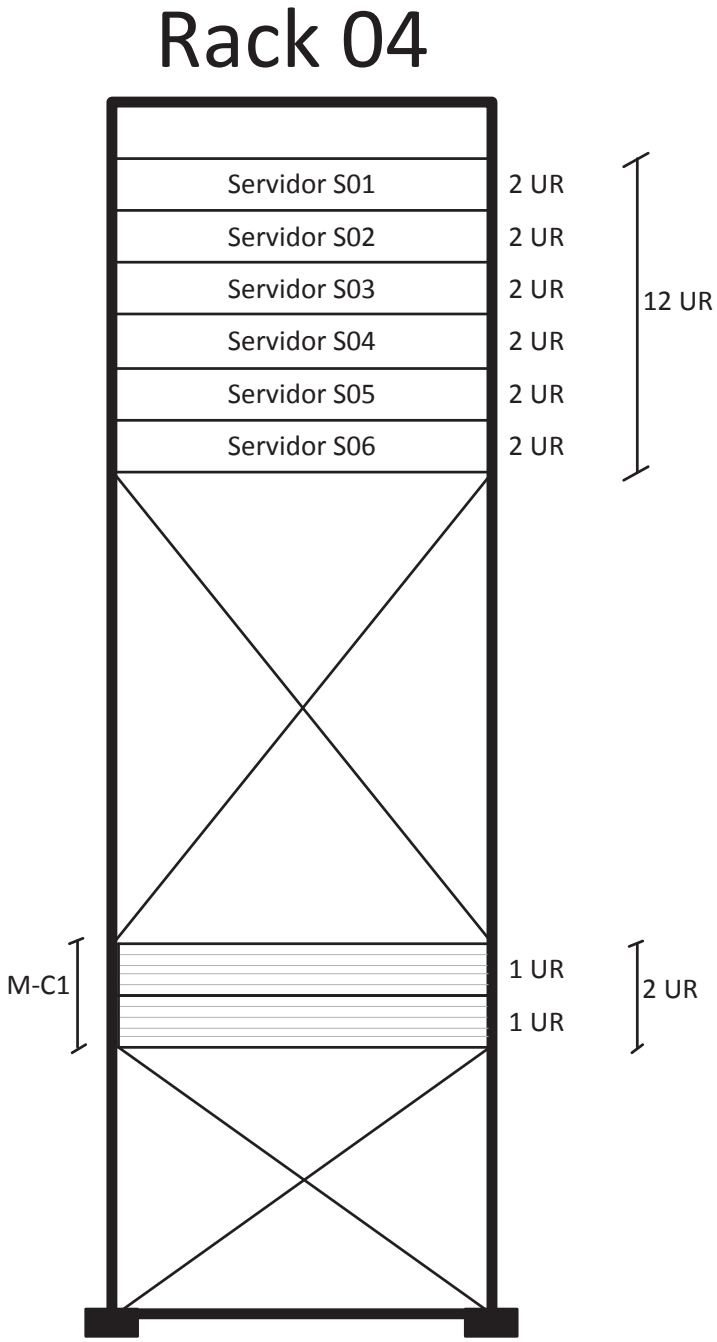

Figura 3.26: Ubicación de equipos y patch panel rack 04 en EDA

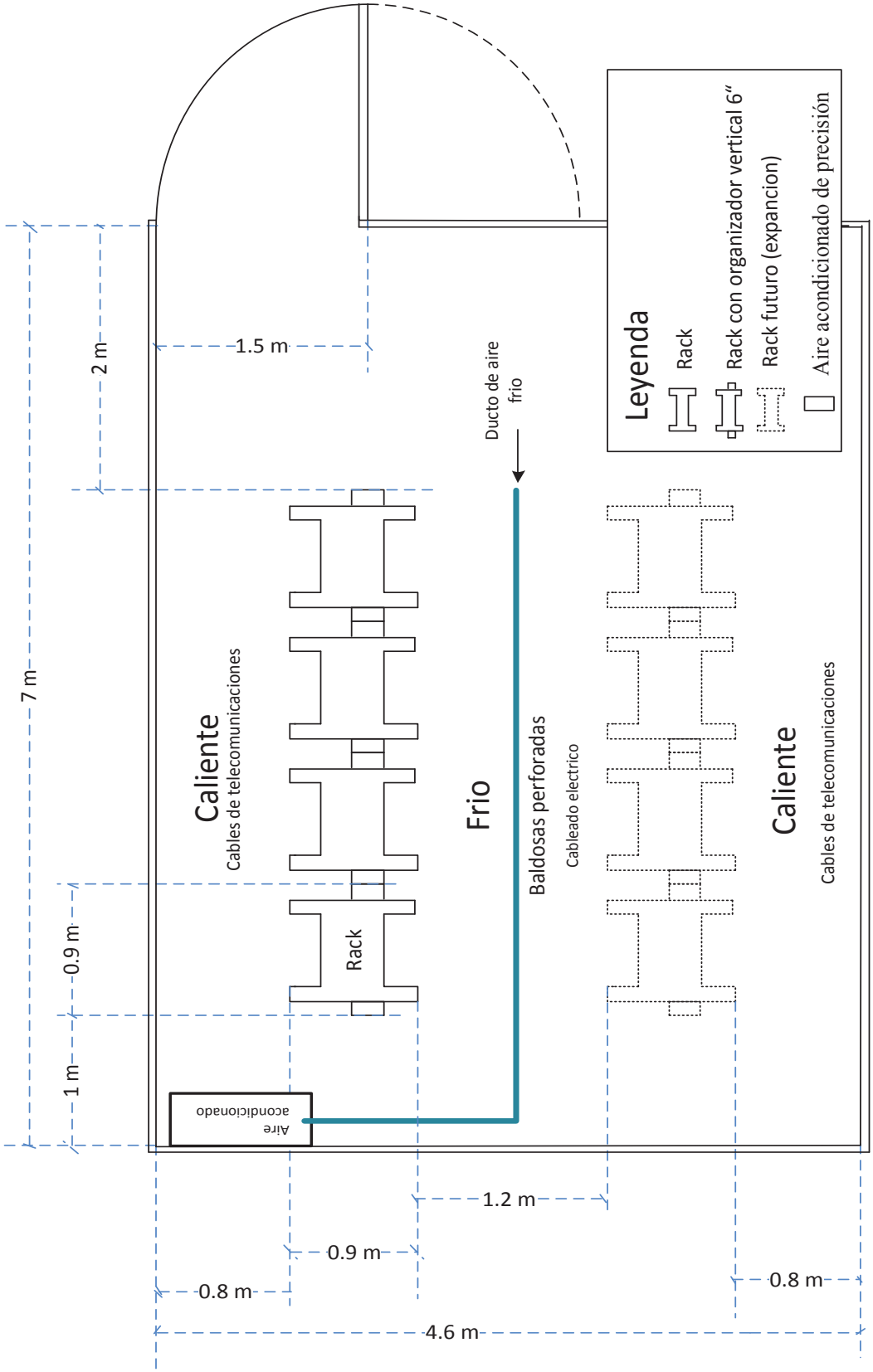

Figura 3.27: Distribución de equipos y tamaño del cuarto de cómputo

3.5.5. CABLEADO ENTRE RACKS [E1] [E2] [E3]

Las figuras 3.28 y 3.29 muestran el cableado en el rack y entre las dos áreas con que cuenta el centro de datos, el área de distribución principal y el área de distribución de equipos. Para garantizar el crecimiento y la rápida adición o remplazo de equipos se utiliza un sistema de conexión cruzada entre los racks, de tal forma que como se observa en la figura 3.28, por la parte frontal de los racks solo se utilizan patch cord entre equipos del mismo rack. Mientras que como se observa en la figura 3.29, entre racks se utiliza cables permanentes, los cuales se instalan solo una vez.

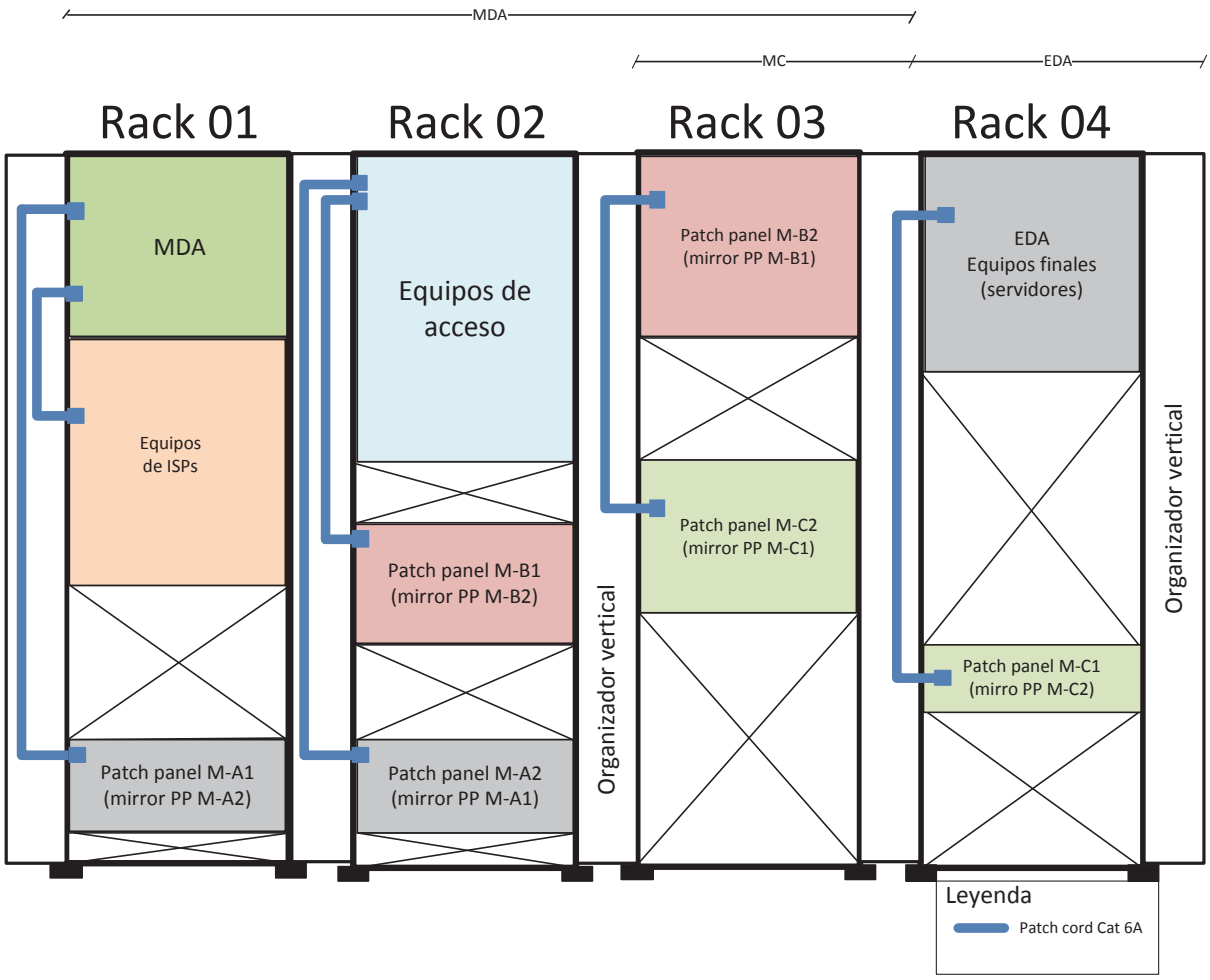

Figura 3.28: Cableado entre racks vista frontal (Cables patch cord)

Para una buena organización, el cableado perteneciente a conexiones en el mismo rack solo irá por los organizadores verticales de la izquierda del rack, mientras que los cables que conectan entre rack irán por el organizador vertical derecho y por el piso falso como se observa en las figura 3.28 y 3.29 respectivamente. Como el tamaño del cuarto de cómputo es de 7 x 4.6 m, y el royo de cable tiene 305 metros, solo es necesario un royo de cable UTP categoría 6A para el cableado entre racks.

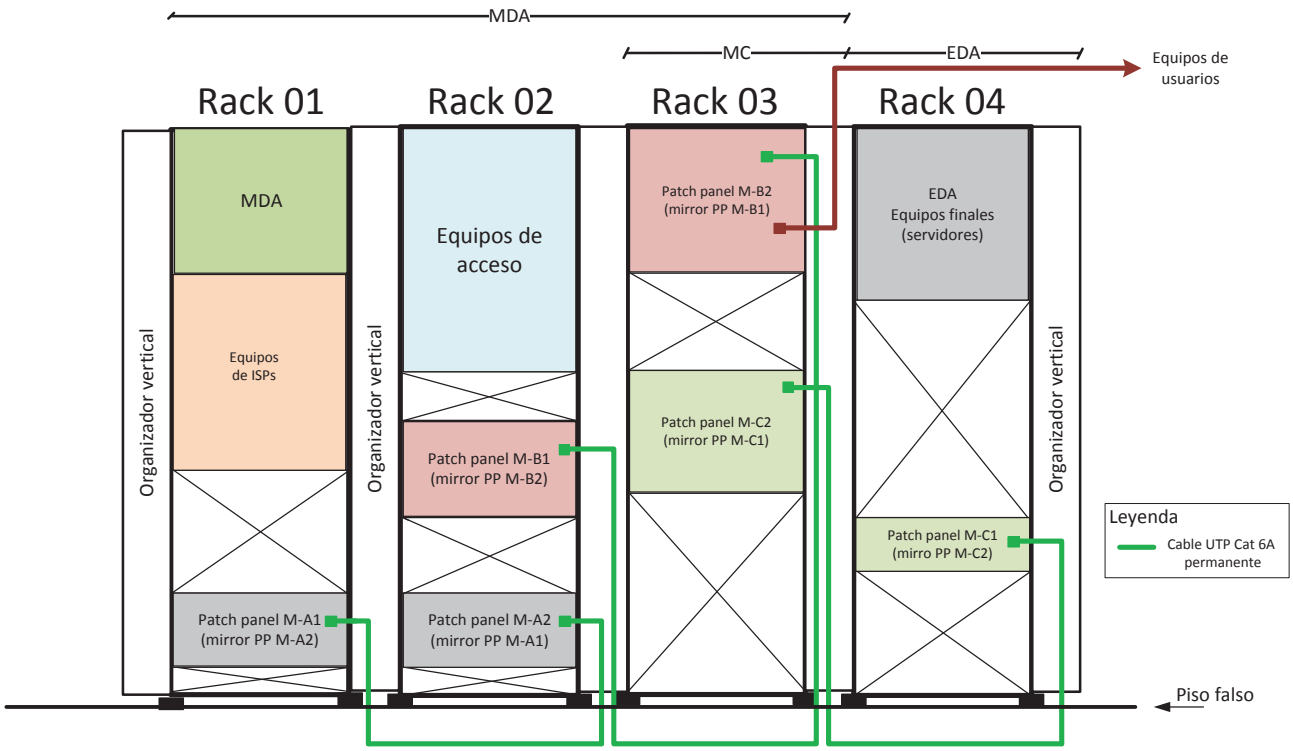

Figura 3.29: Cableado entre racks vista trasera

3.5.6. SISTEMA DE FLUJO DE AIRE [E1] [E5]

El sistema de HVAC debe seguir las directrices propuestas por ASHRAE[E5] TC 9.9[85], la cual establece los parámetros de humedad y temperatura dentro del cuarto de cómputo. En la tabla 3.15 se puede apreciar las clases de ambientes que

[85] American Society of Heating, Refrigerating and Air Conditioning Engineers DATA CENTER ESSENTIALS: GUIDANCE ON ENERGY-EFFICIENT DESIGN AND OPERATION

establece ASHRAE[E5]. El centro de datos del EcuCERT entra en la clase A1, por lo que sus rangos de temperatura y humedad relativa de acuerdo a ASHRAE son:

- Temperatura recomendada[86]: 18 a 27 °C
- Temperatura admisible: 15 a 32 °C
- Ámbito de humedad sin condensación recomendada: 5.5 C DP a 60% RH
- Ámbito de humedad sin condensación admisible: 20% a 80% RH
- Punto de rocío máximo: 17
- Elevación máxima en metros sobre el nivel del mar: 3050 m
- Velocidad máxima de cambio (°C/hr): 5/20

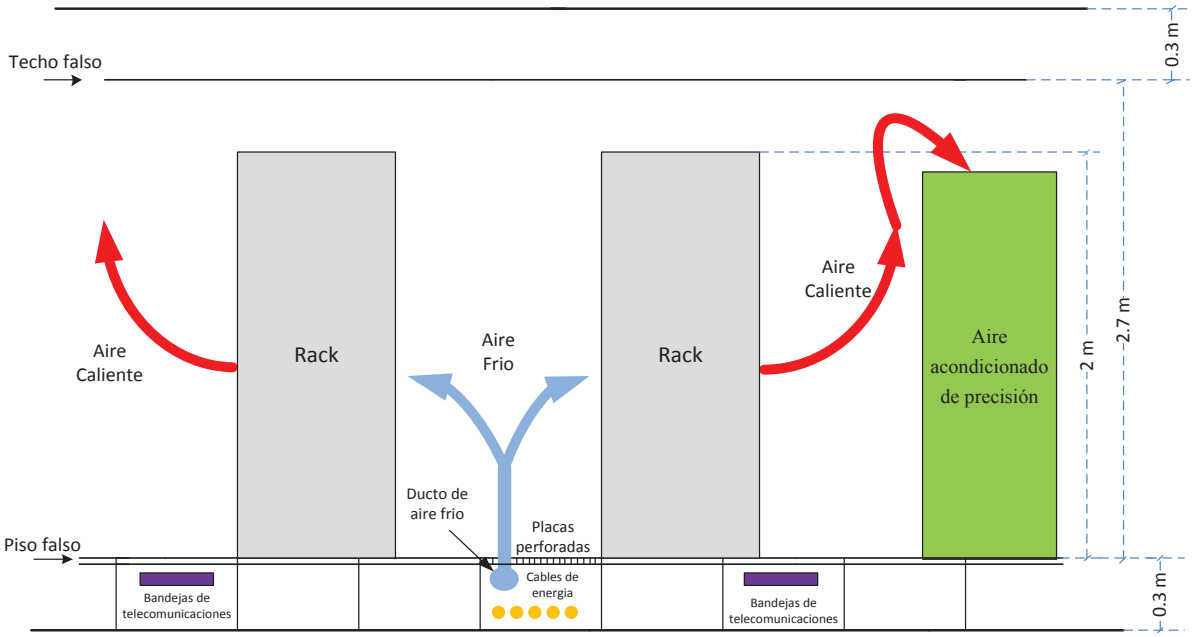

Figura 3.30: Altura del centro de datos y flujo de aire [E1]

En las figuras 3.27 y 3.30 se puede observar el sistema de HVAC con el que contará el centro de datos del EcuCERT, el cual está basado en la norma TIA 942 y en ASHRAE. Al seguir la propuesta de la norma TIA-942, se optimiza la refrigeración de los equipos al utilizar el flujo natural de aire, donde el aire caliente sube.

[86] La temperatura mostrada es para los pasillos fríos, los pasillos calientes pueden llegar a los 47 °C o incluso más altas

Clases	Aplicaciones	Equipos TI	Control ambiental
A1	Data center	Servidores de empresas, productos de almacenamiento	Estrechamente controlado
A2		Servidores de volumen, productos de almacenamiento, computadores personales y estaciones de trabajo	Estrechamente controlado
A3		Servidores de volumen, productos de almacenamiento, computadores personales y estaciones de trabajo	Estrechamente controlado
A4		Servidores de volumen, productos de almacenamiento, computadores personales y estaciones de trabajo	Estrechamente controlado
B	Oficinas, casas, etc	Computadores personales, estaciones de trabajo, laptops e impresoras	Mínimo control
C	Punto de ventas, industrias, fabricas, etc	Punto de venta de equipos, controladores robustos, computadores y PDAs	Sin control

Tabla 3.15: Guía térmica ASHRAE 2011 [E5]

De esta forma una tubería conduce el aire frío por debajo del centro de datos, por el mismo ducto donde se encuentra el cableado eléctrico. El aire frío sale a través de las baldosas perforadas correspondientes al pasillo frío, para ventilar los equipos. Los equipos expulsan aire caliente por la parte trasera de los rack el cual sube y es removido por el sistema de HVAC. Como se trata de un centro de datos, el aire acondicionado debe operar todos los días del año las 24 horas del día, por lo que se debe utilizar un sistema de aire redundante y especializado para centro de datos. Este tipo de sistema se conoce como aire acondicionado de precisión para centros de datos. Estos sistemas cuentan con microprocesadores que les permiten configurar parámetros muy exactos para control de temperatura y humedad relativa. Para el dimensionamiento del sistema de aire acondicionado se utiliza la siguiente relación: [L11] [L12]

$$KW = \frac{KBTU}{3.4122}$$

Dónde:

KW = es la potencia en kilowatts del equipo

KBTU[87] = unidades de calor en kilo BTU

Como se calculó anteriormente el valor de potencia total es de 6685 W, por lo que al aplicar la fórmula anterior se tiene que el valor en KBTU es de 22.8 KBTU. Solo para equipos de *networking*. En caso de que el UPS sea ubicado en el cuarto de cómputo, se tendrá 27 KBTU (ya que el UPS también emite calor). Debido a que en el mercado la mayoría de fabricantes utilizan la "tonelada"[88] como unidad para los equipos de ventilación, y 1 tonelada equivale a 12 KBTU, se tiene que el equipo necesario para el EcuCERT debe de ser de aproximadamente 2 toneladas (incluyendo también al sistema de iluminación).

Características para el sistema de HVAC

- Capacidad de enfriamiento: 2 toneladas
- Capacidad de remover humedad
- Posibilidad de expansión a 4 toneladas mínimo
- Voltaje: 120 V
- Monitoreo por SNMP

Como la norma TIA 942 recomienda que el UPS del sistema de ventilación sea independiente, es necesario adquirir un UPS específico para dicho fin (dos para redundancia), por lo que el equipo de HVAC debe incluir un UPS adecuado a sus características de potencia y además cumpla con lo siguiente:

- Montable en rack de 19 pulgadas
- Capacidad en volta amperios: la necesaria para el sistema de aire acondicionado
- Voltaje de entrada: 110 VAC

[87] Una BTU son las siglas de British termal unit; representa la cantidad de energía que se requiere para elevar en un grado Fahrenheit, la temperatura de una libra de agua en condiciones atmosféricas normales

[88] TRF, tonelada de refrigeración, unidad de medida utilizada principalmente en Estados Unidos para referirse a la capacidad de extracción de carga térmica.

- Factor de potencia: >0.98
- Frecuencia de entrada: 50 o 60 Hz
- Tiempo de autonomía (carga completa): 15 min
- Componentes redundantes: Si
- Voltaje de salida: 120 V
- Frecuencia de salida: 60 Hz
- Monitoreo: SNMP/RS232

3.5.7. SISTEMA CONTRA INCENDIOS [E1] [E6] [E7]

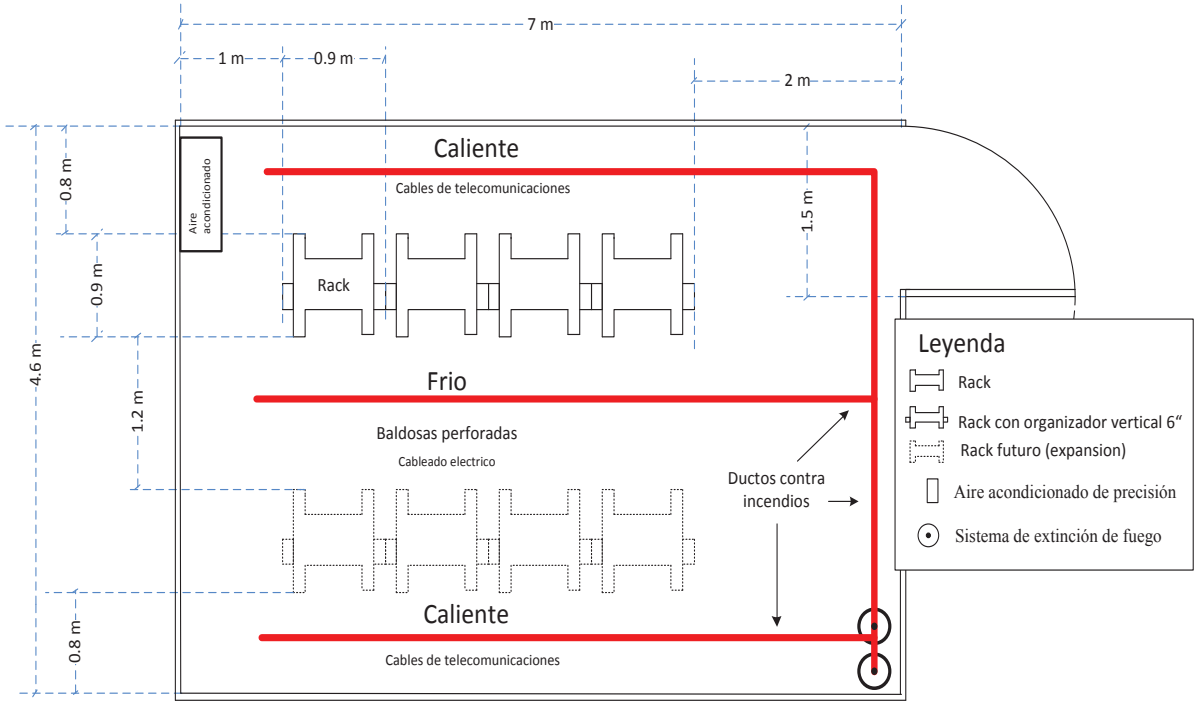

Figura 3.31: Sistema de extinción y detección de incendios

El sistema contra incendios debe seguir el estándar NFPA-75.[89] Para el sistema contra incendios se utilizará un sistema de extinción en base a agentes limpios, ya que no conducen electricidad y son más seguros para el medio ambiente y los humanos. Los agentes limpios son gases incoloros, inodoros, insípidos y no dejan

[89] Es un estándar de la National Fire Protection Association que establece los requisitos mínimos para la protección de equipo electrónico y/o de computación de los daños por fuego o sus efectos asociados.

residuos, remueven el calor, extinguen y evitan la propagación del fuego. La figura 3.31 muestra el diseño del sisma de extinción de fuego. Además se debe contar con un extintor de 10 lb FM-200 o Halotron colocado a la entrada del centro de datos.

Especificaciones del sistema

El sistema contra incendios se divide en dos partes: sistema de extinción y sistema de detección.

- Sistema de extinción

El sistema de extinción debe cumplir con las siguientes características:

- Utilizar un agente limpio (que no deje residuos como ECARO 25, HFC-227 o FM-200)
- Tiempo de extinción: menor a 10 segundos
- Incorpora un pulsador para desactivar la descarga del agente.
- Permitir una dispersión de 180 grados para cubrir una mayor área.
- Incorpora cilindro con kit de actuación automática.
- No ser conductor de electricidad
- No ser tóxico para las personas
- No afectar la capa de ozono

- Sistema de detección

El sistema de detección debe cumplir con los siguientes requerimientos:

- Detectores de detección activa[90]
- 4 detectores de humo a lo largo del centro de datos
- Panel LCD
- Leds indicadores de estado
- Proporcionar señales de alarma distintas para descarga, pre-descarga, o condiciones de supervisión.
- Compatible con SNMP

[90] Este tipo de detectores toman muestras del aire y la dirigen hacia el equipo detector donde las partículas de humo interfieren con un láser, generando una alarma temprana.

3.5.8. SEGURIDAD FÍSICA DEL CUARTO DE CÓMPUTO

La seguridad física del centro de datos de acuerdo a la norma TIA 942, requiere:

- Servicio de guardia las 24 horas del día los 7 días de la semana.
- Control y registro de acceso a las instalaciones del centro de datos.
- Sistema de video vigilancia.
- Puerta especializada.

3.5.8.1.Sistema de video vigilancia IP

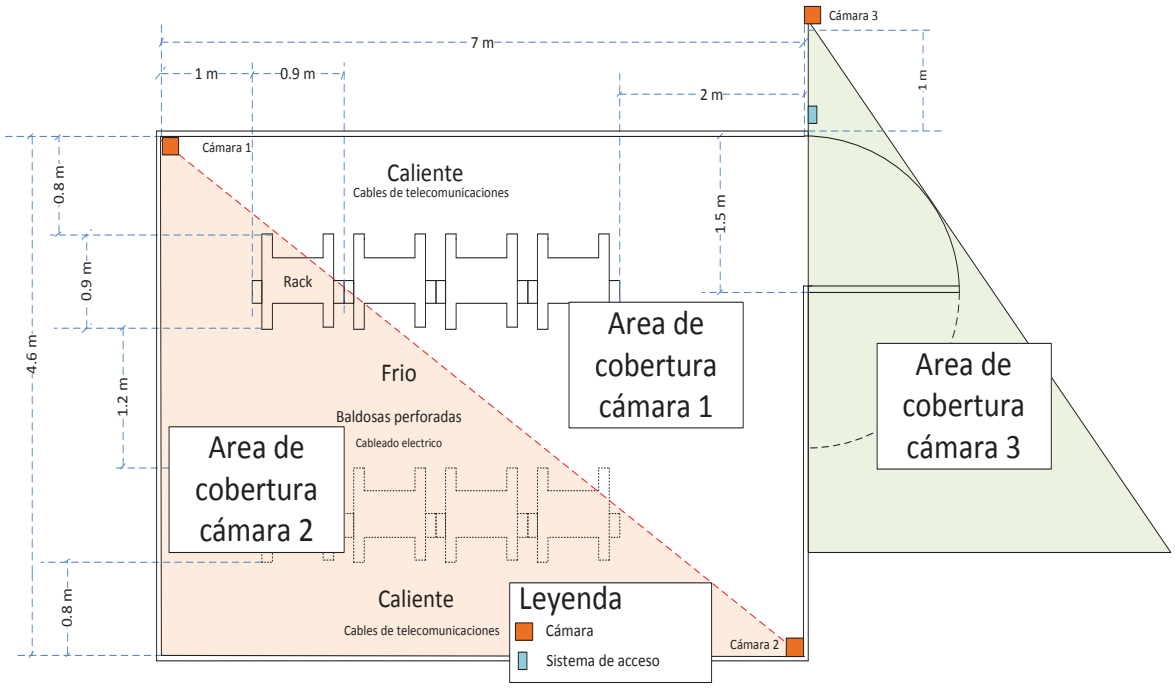

Figura 3.32: Esquema de seguridad física del centro de datos

Para el sistema de video vigilancia IP se utilizarán 3 cámaras IP El sistema de vigilancia tendrá una infraestructura de red independiente, cada cámara se conectará a un switch y este a su vez a un equipo servidor independiente del resto de equipos. Dos cámaras estarán colocadas en el interior del cuarto de cómputo, una en cada esquina de la diagonal del centro de datos (cada cámara debe tener un

ángulo de visión de 45 grados que asegure cubrir el total del área del cuarto de cómputo). Una tercera cámara se encontrará a la entrada del cuarto de cómputo (ver figura 3.32). El switch que se utilizará debe ser del tipo Power over *Ethernet* (PoE), administrable de mínimo 8 puertos. Las características mínimas del servidor que se utilizará son: 1.5 GHz, 4 GB RAM, 1 TB de disco en raid 1. El sistema operativo será Centos 6.6. El periodo que debe permanecer almacenada la información del sistema de video vigilancia no es tema del presente proyecto pero se recomienda 6 meses como mínimo. Es recomendable que el servidor de video vigilancia está ubicado en un cuarto diferente e independiente al del centro de datos.

3.5.8.2.Sistema de control de acceso

Para el sistema de control de acceso se recomienda el uso de un sistema de acceso biométrico mediante huella digital (también se puede utilizar un acceso por clave única para cada usuario). El uso de este sistema garantiza que todo acceso este debidamente registrado. Este tipo de sistema emplea cerradura magnética (por lo que se debe asegurar un flujo constante de corriente eléctrica), debe permitir la administración a través de la red IP, mediante un servidor central independiente de los del resto de la red, que al igual que en caso anterior es recomendable que no se encuentre dentro del cuarto de cómputo. El esquema de conexión para el sistema de acceso se puede apreciar en la figura 3.33.

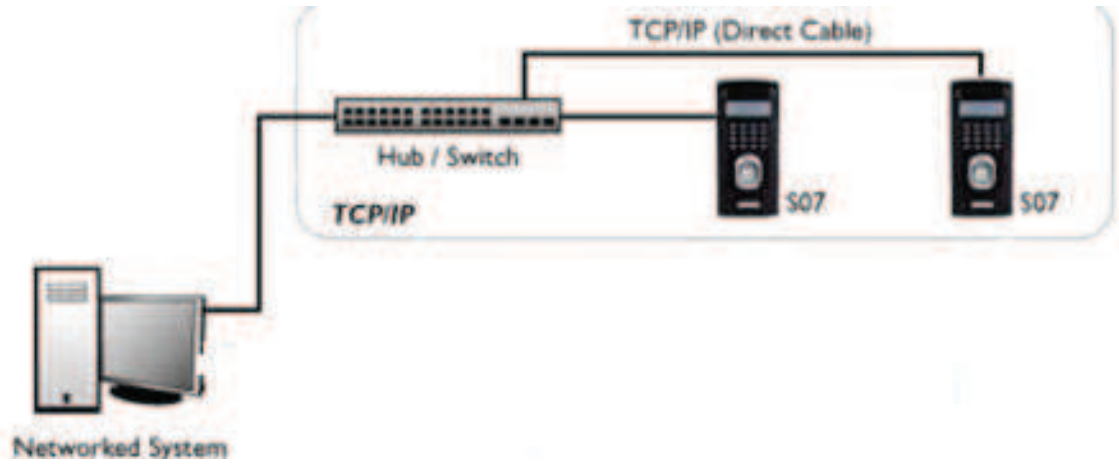

Figura 3.33: Diagrama de conexión del sistema de acceso

3.5.9. SISTEMA DE PUESTA A TIERRA Y GENERADOR ELÉCTRICO [E1] [E4]

3.5.9.1.Sistema de puesta a tierra [E6]

El sistema de puesta a tierra del centro de datos estará basado en las normas EIA/TIA-607[E4] y en la norma EIA/TIA-742, además se deberá cumplir con el estándar NFPA-70[91] [E6]. El propósito de la puesta a tierra es crear un camino de baja impedancia a tierra para descargas eléctricas, con el fin de proteger al usuario y a los equipos de dichas descargas. Al sistema de puesta a tierra se deben conectar todos los componentes metálicos que sean parte de la infraestructura del centro de datos. Todos los cables para puesta a tierra deberán ser de color verde.

Longitud de TBB y/o BC	Cable a utilizar número
0 – 13 m	1 AWG
13.1 – 16 m	1/0 AWG
16.1 – 20 m	2/0 AWG
20 o más m	3/0 AWG

Tabla 3.16: Cables para TBB y/o BC [E4]

El sistema de puesta a tierra estará formado por un cable número 2 AWG ubicado debajo del piso falso en el pasillo “Frío” con el resto del cableado eléctrico. Todos los rack del centro de datos estarán conectados a dicho conductor utilizando un cable número 6 AWG. Finalmente el cable número 2 AWG se conecta a la TGB[92] la cual estará ubicada en la pared entre los racks (ver figura 3.34). La TGB se conectará a la TMGB[93] mediante un conductor llamado TBB[94] cuyo calibre o número AWG está en función de la distancia que las separa, como se observa en la tabla 3.16 .La TMGB debe estar colocada lo más cerca posible a la tierra del edificio y conectada a esta mediante el BC cuyo número AWG depende de la distancia que las separa como se observa en la tabla 3.16. Los equipos ubicados en los rack

[91] Es un estándar de la *National Fire Protection Association* para la instalación segura de alambrado y equipos eléctricos, y es parte de la serie de normas para prevención de incendios.
[92] *Telecommunications Grounding Busbar* (Barra de tierra para telecomunicaciones) es una barra de cobre con perforaciones roscadas, debe ser de mínimo 6 mm de espesor y 50 mm de ancho.
[93] *Telecommunications Main Grounding Busbar* (Barra principal de tierra para telecomunicaciones) es una barra de cobre con perforaciones roscadas, debe ser de 6 mm de espesor por 100 mm de ancho.
[94] *Telecommunications Bonding Backbone* (*Backbone* de tierras)

conectarán sus chasis a tierra al lado derecho de los rack el cual contendrá la tira de conexiones a tierra (se debe considerar que las partes del rack donde se ubique el conector sean de metal puro).

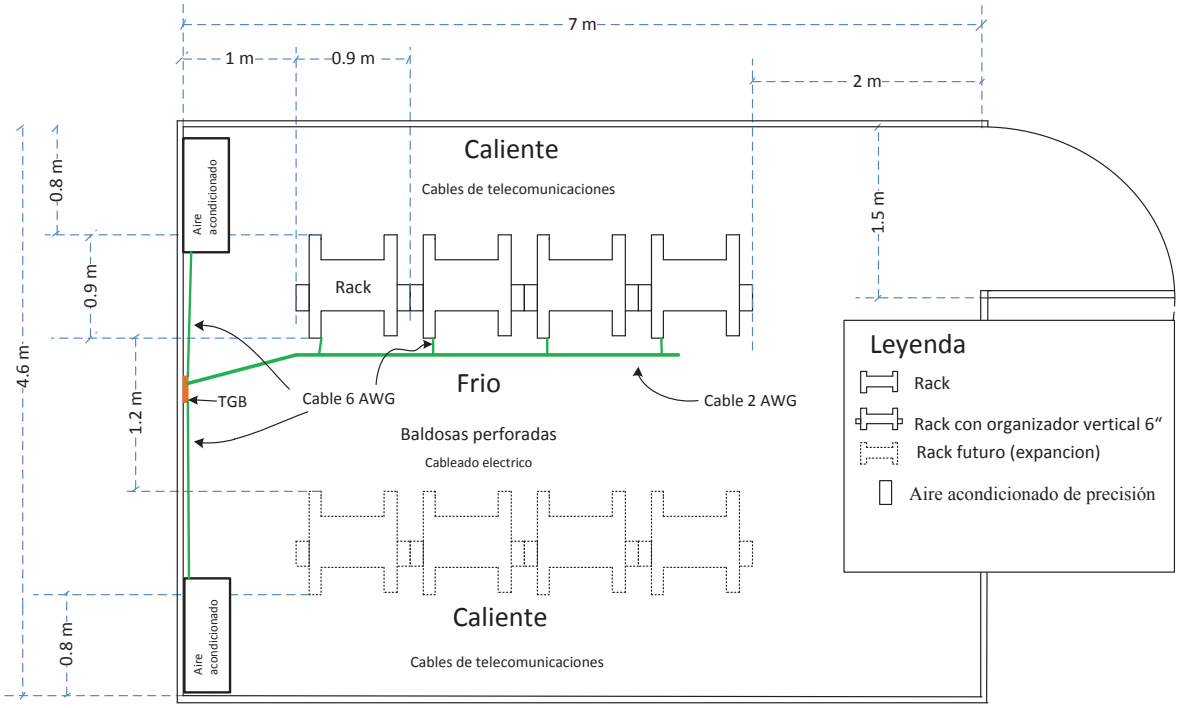

Figura 3.34: Sistema de puesta a tierra

3.5.9.2.Generador eléctrico

El generador del centro de datos del EcuCERT debe soportar todos los equipos. Para el cálculo del generador se deben sumar las potencias de todos los equipos en vatios y mediante la fórmula del punto 3.2.3.4 calcular la potencia en VA para un factor de potencia de 0.9. Para el ejemplo del cálculo del presupuesto para el centro de datos, la suma de todas las potencias es de 17.5 KW con un factor de potencia de 0.9 se tiene que el generador debe ser para 18.94 KVA lo más cercano disponible en el mercado es 20 KVA. Las características que debe cumplir el generador son:

- AC salida: 20 KVA

- AC salida de emergencia: 22 KVA
- AC voltaje de salida: 110-127/208-220 VAC
- AC frecuencia: 60 Hz
- Corriente: 55 A
- Tipo de motor: diesel
- Encendido: eléctrico (automático, programable mediante PLC)
- Batería: incluida
- Horas de operación al 75 % con tanque lleno: 8 hr

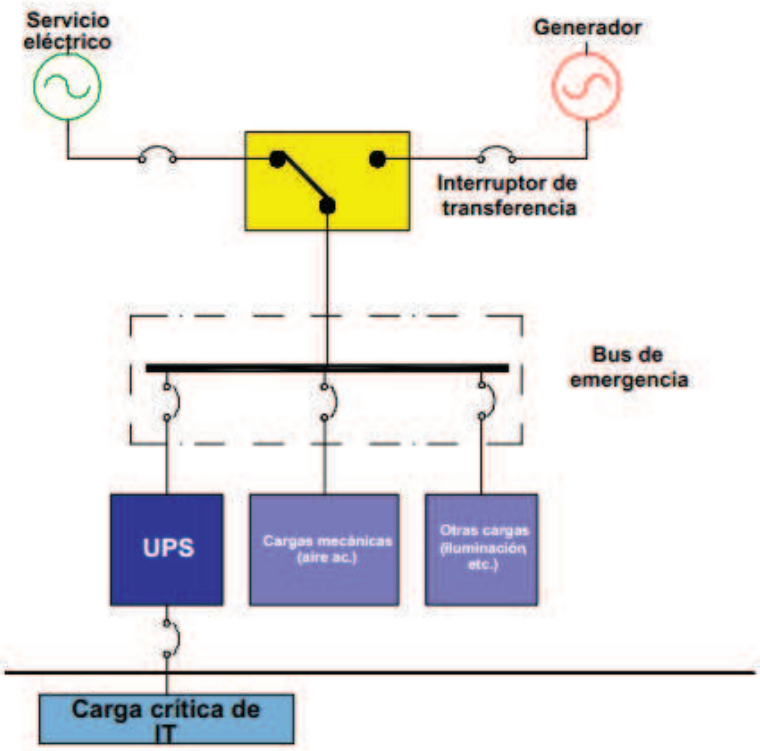

Figura 3.35: Esquema de conexión del generador [L4]

Debe incluir un tablero de transferencia automática con las siguientes características:

- Gabinete Metálico
- Luces piloto de emergencia y normal
- Voltímetro, Amperímetro y Frecuencímetro
- Contactores de emergencia y normal de 220 voltios
- Bases fusibles y fusibles
- Relays de 220 voltios

- Supervisor de voltaje 95-270 voltios
- Transformador de corriente y fuente
- Batería de 12 voltios dc
- PLC
- Corriente en función de la potencia del generador

El PLC debe permite ingresar a la base de datos para programar los tiempos de encendido y apagado del generador, ingreso y egreso de contactores con sus respectivos tiempos, programaciones semanales para encendido del generador los 7 días de la semana. El PLC además permite poder encender el generador a control remoto desde un computador, realizar transferencias y retransferencias exactas con tiempos determinados. La figura 3.35 muestra el esquema de conexión del generador y la red eléctrica del centro de datos.

3.6. LISTA FINAL DE MATERIALES, EQUIPOS Y PRESUPUESTO

Una vez establecido los elementos y equipos necesarios para la implementación del centro de datos, se procede a elaborar un presupuesto que sirva como referencia.

3.6.1. EQUIPOS DE RED Y SERVIDORES (EQUIPOS ACTIVOS)

Equipo y servidores	Modelo	Precio Unitario	Cantidad	Precio Total
Switch Core	Cisco catalyst 3450E-24-TD	$ 6350	2	$ 12700
Switch acceso	Cisco catalyst 2960S-24TD	$ 1200	8	$ 9600
Firewall IDS	Cisco asa 5520-AIP20	$ 6300	5	$ 31500
Servidores	DELL powerEdge R720	$ 6990	1	$ 6990
Servidores	DELL powerEdge R720	$ 8126	2	$ 16252
Servidores	DELL powerEdge R720	$ 10880	1	$ 10880
Servidores	DELL powerEdge R720	$ 4843	2	$ 9686
Total				**$ 97608**

Tabla 3.17: Lista de precios de equipos y servidores (Anexo L y K)

3.6.2. ACCESORIOS (EQUIPO PASIVO)

Elemento	Características	Precio Unitario	Cantidad	Precio Total
Patch Panel	24 pto, cat 6A, rack 19”	$ 80	38	$ 3040
Organizador vertical	42 UR, 6 pul-gadas	$ 100	5	$ 500
Patch cord	2 metros, cat 6A	$ 25	40	$ 1000
Patch cord	1 metros, cat 6A	$ 12	20	$ 240
Rack	42 UR; 19”	$ 573	4	$ 2292
Rollo de cable UTP	Categoría 6A	$ 185	1	$ 185
Regleta eléctrica	1 UR, 7 tomas, para rack 19”	$ 52.3	5	$ 261.5
Conectores RJ45		$ 0.25	50	$ 12.5
Total				**$ 7531**

Tabla 3.18: Precios de Accesorios (Equipos pasivos) (Anexo L)

3.6.3. EQUIPOS UPS

Equipo	Modelo	Precio Unitario	Cantidad	Precio Total
UPS 6 KVA	UPS Liebert GTX3 208/120 VAC 6 KVA	$ 5500	2	$ 11000
UPS 15 KVA con componentes redun-dantes	UPS Liebert NFINITY 12 a 20 KVA	$ 12800	1	$ 12800
Total				**$ 23800**

Tabla 3.19: Precios de UPS (Anexo L)

3.6.4. SISTEMA DE VIDEO VIGILANCIA

Equipo	Modelo	Cantidad	Precio uni-tario	Precio final
Cámara tipo domo PoE	E53	3	$ 521.57	$ 1564.7
Accesorio montaje pared	PMAX-0308	3	$ 87.84	$ 263.52
Switch 8 puertos PoE	ES-2108PWR	1	$ 567.7	$ 567.7
Laptop	--------	1	$ 1504	$ 1504
Instalación y mano de obra	--------	------	$ 1300	$ 1300
Total				**$ 5199.92**

Tabla 3.20: Precios del sistema de video vigilancia (Anexo L)

3.6.5. GENERADOR ELÉCTRICO

Descripción	Cantidad	Precio Total
Generador eléctrico y cabina insonora + instalación y montaje	1	$ 24691.20
Tablero de transferencia automática	1	$ 3878.4
Total		**$ 29769.6**

Tabla 3.21: Precio del generador eléctrico (Anexo L)

3.6.6. SISTEMA DE CONEXIÓN A TIERRA

Elemento	Característica	Cantidad	Precio unitario	Precio total
TMGB	Material cobre, 10 agujeros	1	$ 140	$ 140
TGB	Material cobre, 10 agujeros	1	$ 125.5	$ 125.5
Cable conductor	2 AWG, color verde	10 m	$ 4.5	$ 45
Cable conductor	6 AWG, color verde	5 m	$ 2.8	$ 14
Kits jumpers para equipos	10 AWG	21	$ 6	$ 126
Tira de conexiones para racks		4	$ 125.6	$ 502.4
Total				**$ 952.9**

Tabla 3.22: Precios del sistema de puesta a tierra (Anexo L)

3.6.7. SISTEMA DE CONTROL DE ACCESO

Descripción	Cantidad	Precio unitario	Precio Total
Sistema de control de acceso	1	$ 700	$ 700
Cerradura electromagnética	1	$ 140	$ 140
Instalación, accesorios y configuración	1	$ 300	$ 300
Total			**$ 1140**

Tabla 3.23: Precios del sistema de control de acceso (Anexo L)

3.6.8. SISTEMA DE PISO DE ACCESO ELEVADO

Descripción	Cantidad	Precio Unitario	Precio Total
Paneles	32.20 m^2	$ 195	$ 6279
Paneles perforados	12	$ 270	$ 3240
Rampa de acceso elevado	1	$ 760	$ 760
Ventosa	1	$ 31	$ 31
Hermetización de pasos de cable	24	$ 160	$ 3840
Instalación	32.20 m^2	$ 14	$ 450.8
Malla de alta Frecuencia	23.81m^2	$ 90	$ 2142.9
Aterrizaje de los pedestales	23.81 m^2	$ 5	$ 119.05
Instalación de la malla de alta frecuencia	23.81 m^2	$ 12	$ 285.72
Pintura antiestática	32.20 m^2	$ 24	$ 772.8
Escalerilla para cableado de datos e instalación	32.20 m^2	$ 150	$ 4830
Total			**$ 22751.27**

Tabla 3.24: Precio del sistema de piso elevado (todos sus componentes) (Anexo L)

3.6.9. INSTALACIÓN Y MENSUALIDAD DEL ENLACE A INTERNET

Descripción	Instalación	Mensualidad
Enlace 60 MB (centro de datos)	$560	$4383
Enlace de 2 MB (honeynet)	$560	$529
Enlace de 2 MB (Red de pruebas)	$560	$529
Total	**$1680**	**$5441***

*Precios no incluyen IVA

Tabla 3.25: Costo de enlaces de internet (Anexo C)

El nivel de disponibilidad ofrecido para el contrato de internet es de 99.6%, por lo que se debe contar con dos proveedores para garantizar un *TIER* II de 99.741%

3.6.10. SISTEMA DE DETECCIÓN Y EXTINCIÓN DE INCENDIOS

ÍTEM	Cantidad	Precio unitario	Precio Total
Sistema de detección - Panel de control con microprocesador y Display de 7 segmentos para fallas - Botón de descarga manual con llave de seguridad - Botón para abortar proceso de descarga de agente - Sistema de baterías para 12 horas de autonomía - 10 sensores de temperatura - 10 sensores láser	1	$ 9340.50	$ 9340.5
Sistema de extinción - Agente limpio ECARO 25 (HFC-125) - Tiempo de extinción menor a 10 segundos - Tobera de 180 grados	2	$ 3300	$ 6600
Sistema de gestión y monitoreo - Módulo electrónico para gestión y monitoreo - Módulo montable en rack - Tarjeta SNMP con puerto RJ45 para monitoreo - Modem GSM para envío de mensajes de texto - Puerto RS-232 - Monitoreo de 10 sensores de temperatura (ampliables)	1	$ 6059.5	$ 6059.5
Total			**$ 22000***

*Incluye instalación

Tabla 3.26: Precio del sistema de detección y extinción de fuego (Anexo L)

3.6.11. SISTEMA DE CLIMATIZACIÓN

ÍTEM	Modelo	Cantidad	Precio unitario	Precio Total
Aire acondicionado de precisión 2 *ton*	ClimateWorX serie 6, vertical Floor-Mount units	2	$ 10952,95	$ 21905.9
Ductos de ventilación aire frío	ClimateWorX – Floor mount	10 m	$ 9.40	$ 94
Instalación	NA	1	$ 2990	$ 2990
Total				**$ 24989.9***

Tabla 3.27: Precio del sistema de climatización (HVAC) (Anexo L)

3.6.12. RESUMEN TOTAL DEL PRESUPUESTO

Descripción	Valor
Generador de 20 KVA	$ 29769.6
Sistema de video seguridad	$ 5199.92
Sistema de control de acceso	$ 1140
Piso de acceso elevado	$ 22751.27
Sistema de detección y extinción de incendios	$ 22000
Sistema de climatización	$ 24989.9
Puesta a tierra	$ 952.9
Equipos networking y servidores	$ 97608
Accesorios de cableado	$ 7531
UPS	$ 23800
Instalación de internet	$ 1680
Total	**$ 237422.59**

Tabla 3.28: Costo total para la implementación del centro de datos

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- El centro de datos que se diseñó en el presente proyecto tiene un nivel de *Tier* II lo que implica una disponibilidad del 99.741% anual. Bajo este esquema se diseñó la infraestructura de red, el sistema de cableado, el sistema de HVAC, el sistema contra incendios y el sistema eléctrico de UPS. Además se presentaron pautas para el diseño arquitectónico y de iluminación. Todos los componentes del centro de datos presentan un nivel de redundancia N + 1 según lo establece la norma TIA-942 para un centro de datos *Tier* II.
- El diseño del sistema de red del EcuCERT permite la escalabilidad y flexibilidad para el crecimiento del centro de datos tanto a nivel físico como lógico. El crecimiento a nivel lógico se logra gracias a su arquitectura modular y de capas basada en SAFE de Cisco, y el crecimiento a nivel físico es gracias al diseño del sistema de cableado estructurado, el cual implementa un esquema de conexión cruzada basado en la norma TIA-942. Con el uso de estos dos esquemas, es fácil incrementar los servicios y la capacidad del centro de datos añadiendo nuevos equipos.
- El centro de datos se diseñó para cumplir con los aspectos claves de: aislamiento, aplicación de políticas y visibilidad. Estos tres aspectos se logran gracias al correcto uso de *firewalls,* de protocolos de enrutamiento, de ACLs y del módulo de administración. Aplicando las medidas mencionadas se logra separar lógicamente el centro de datos en áreas independientes y controlar quien puede acceder, así como quien está accediendo a un determinado servicio, equipo o aplicación sin importar que se trate de un equipo físico o virtual.

4.2. RECOMENDACIONES

- El presente proyecto basó su diseño en historias de usuario para dimensionar los equipos de *networking* y servidores. Se hizo de esta forma ya que actualmente no existe una infraestructura de red que pueda ser monitoreada y cuyos datos sirvan como punto de partida. Por dicho motivo se deben monitorear todos los equipos de la red ya en funcionamiento, y asegurarse que efectivamente satisfagan los requerimientos de esta.
- Los diseños presentados en este proyecto no constituyen una guía definitiva, que deba ser seguida estrictamente. Los diseños pueden estar sujetos a cambios al momento de su implementación. Se recomienda que se usen los mismos como una guía base para la implementación del centro de datos.
- Se debe tener en cuenta que si el EcuCERT desea obtener una certificación internacional *Tier* II para su centro de datos, tiene que asegurarse que los demás sistemas como el arquitectónico y el de iluminación (los cuales no son tema del presente proyecto de titulación) también cumplan con lo estipulado en la norma TIA-942.
- Si se desea diseñar un centro de datos *Tier* III o *Tier* IV se puede usar como punto de partida el diseño propuesto en el presente proyecto. El diseño que se realizó para este proyecto permite mejorar la infraestructura de red y el sistema de cableado para cumplir con los estándares más altos de un centro de datos *Tier* III o *Tier* IV.
- Para mejorar la seguridad del centro de datos, se debe realizar un análisis de riesgos. Para esto se debe aplicar alguna de las metodologías existentes como como por ejemplo Octave, a fin de establecer cuáles son los activos más valiosos del EcuCERT y cómo protegerlos.

BIBLIOGRAFÍA

Libros

[L1] AMPARO - LACNIC, “Manual básico de Gestión de incidentes y seguridad informática”, Montevideo, Uruguay, 2012

[L2] HIDALGO Pablo, "Folleto de Redes de Área Local", EPN, Ecuador, 2008

[L3] HIDALGO Pablo, "Folleto de Sistemas de Cableado Estructurado", EPN Ecuador, 2010

[L4] AVELAR V, “Cálculo del requisito total de potencia para los centros de datos”. Massachusetts, USA, 2010

[L5] CISCO, Systems Inc, “SAFE Reference Guide” San José, USA, 2010

[L6] NIST, “Special Publication 800-61 Computer Security Incident Handling Guide”, Maryland, USA, 2012

[L7] STALLINGS, William, "Cryptography and Network Security: Principles and Practice", 2nd Edition, USA, New Jersey, Prentice Hall, 1998

[L8] STALLINGS, W, “Comunicaciones y Redes de Computadores”, 6ta Edición, USA, Pearson Education, 2000

[L9] TANENBAUM, A, “Redes de Computadoras”, 4th Edición. USA, Prentice Hall, 2003

[L10] WEST-BROWN, Moira, “Handbook for Computer Security Incident Response Teams (Csirts), 2th Edition, USA, 2003

[L11] RUDOY, Wilian; CUBA, Joseph; AMERICAN SOCIETY OF HEATING, REFRIGERATING AND AIR-CONDITIONING ENGINEERS, Inc. (ASHARE). “Cooling and Heating Load Calculation” Atlanta, USA, 2011

[L12] KNOWLTON, Archer, “Standard handbook for electrical engineers”, 9th Edition. Mc Graw Hill Book Company, Inc. Tokio 1957

Estándares

[E1] ANSI/TIA-942, “Telecommunications Infrastructure Standard for Data Centers”

[E2] ANSI/TIA/EIA-568-C, “Generic Telecommunications Cabling for Customer Premises”

[E3] ANSI/TIA/EIA-606A, “Administration Standart for Telecommunications Infrastructure”

[E4] ANSI/EIA/TIA-607, “Grounding and Bonding Requirements for Telecommunications”

[E5] ASHRAE TC 9.9, “Thermal Guidelines for Data Processing Environments”

[E6] NFPA 70, “Standard for Electrical Safety in the Workplace”

[E7] NFPA 75, “Standard for the Protection of Information Technology Equipment”

[E8] ANSI/TIA-942, “Telecommunications Infrastructure Standard for Data Centers Addendum 2 – Additional Guidelines for Data Centers”

Internet

[W1] APC, Electric.APC Corporation, Revisado Febrero 5, 2013:
http://albinogoncalves.files.wordpress.com/2011/03/vavr-5tdtef_r0_ls.pdf

[W2] CERT, Carnegie Mellon, CERT, Revisado Abril, 2013:
http://www.cert.org/csirts/services.html#vhandling

[W3] Server Watch, Revisado Marzo 2013:
http://www.serverwatch.com/server-trends/the-7-best-servers-for-linux.html

[W4] TACACS. Revisado Febrero, 2013:
http://www.tacacs.net/

[W5] US CERT, Revisado Mayo, 2013:
http://www.us-cert.gov/government-users/reporting-requirements

[W6] USC, “Title 44 of the United States Code. Washington D. C”: USA. Goverment. http://www.law.cornell.edu/uscode/text/44

[W7] VentasDeSeguridad, Revisado Octubre, 2012 www.ventasdeseguridad.com

[W8] VMware Revisado, 2013: http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

[W9] VMWare, Revisado Abril 2013: http://www.vmware.com/es/products/datacenter-virtualization/vsphere/

[W10] VMWare, Revisado Abril, 2013: http://www.vmware.com/es/products/datacenter-virtualization/vsphere/

[W11] Wikipedia, http://es.wikipedia.org/wiki/Pretty_Good_Privacy

[W12] SNMP-LINK, Revisado Febrero, 2013: http://www.snmplink.org/

[W13] Panduit, "Structured Cabling Supplement", 2012, Revisado Mayo, 2013. http://faculty.ccri.edu/tonyrashid/Files/CCNA/Cisco%20Project/CCNA1_CS_1_en.pdf

[W14] Honeynet Project, Revisado Marzo, 2013 http://www.honeynet.org/aggregator

Proyectos de Titulación

[T1] NAVISOY Gustavo, ZAMBRANO Cesar, “Diseño de una red convergente para el edificio del gobierno del cantón Tulcán”, Quito, 2012

[T2] CALDERÓN Julio, SAMANIEGO Lara, “Diseño de la infraestructura segura para la red educativa metropolitana de quito”, Quito, 2010

Supertel

[S1] Superintendencia de Telecomunicaciones, “Consultoría EcuCERT”, Quito, 2012