ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS

Tesis de grado, previa a la obtención del título de Ingeniero en Sistemas e Informática

TEMA:

"Análisis, Evaluación y Propuesta de Optimización del funcionamiento del Data Center de la Escuela Politécnica del Ejército utilizando las Normas y Estándares Nacionales e Internacionales de Calidad**"**

AUTORES:

José David Barba Samaniego

Giovanny Alexander Viteri Arias

Sangolquí- Ecuador

Diciembre 2012

CERTIFICAN:

Que el informe de investigación realizado por los señores, José David Barba Samaniego y Giovanny Alexander Viteri Arias, egresados de la carrera de Ingeniería en Sistemas, cuyo tema es "Análisis, Evaluación y Propuesta de Optimización del funcionamiento del Data Center de la Escuela Politécnica del Ejército utilizando las Normas y Estándares Nacionales e Internacionales de Calidad", ha sido prolijamente analizado en su contenido y estructura; y, cumple con las exigencias técnicas, metodológicas y legales que establece la Escuela Politécnica del Ejército.

Por este motivo, autorizamos a los señores Barba Samaniego y Viteri Arias, la sustentación pública de los resultados de la investigación, previa a la obtención del título de Ingeniero en Sistemas e Informática

_____ _____

Ing. José Luis Torres — **DIRECTOR**

Ing. Carlos Caizaguano Ch. — **CODIRECTOR**

ESCUELA POLITECNICA DEL EJÉRCITO

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÀTICA

BARBA SAMANIEGO JOSÈ DAVID

VITERI ARIAS GIOVANNY ALEXANDER

Autorizamos a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la institución de la Tesis de Grado **"ANÁLISIS, EVALUACIÓN Y PROPUESTA DE OPTIMIZACIÓN DEL FUNCIONAMIENTO DEL DATA CENTER DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO UTILIZANDO LAS NORMAS Y ESTÁNDARES NACIONALES E INTERNACIONALES DE CALIDAD"** cuyo contenido, ideas y criterios es de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Diciembre 2012

_____

BARBA SAMANIEGO JOSÉ DAVID

_____

VITERI ARIAS GIOVANNY ALEXANDER

DEDICATORIA

Dedico el presente trabajo a mis padres Rosa Margarita Arias Buenaño y Luis Hernán Viteri Estévez, a mis hermanos Stephany y David, ya que sus valores, enseñanzas y consejos me ayudaron a nunca rendirme en los momentos difíciles.

Fueron mi fuente de inspiración a lo largo de mi vida personal y profesional, gracias a ellos he conseguido un objetivo más, el de terminar mi carrera universitaria.

Giovanny Alexander Viteri Arias

DEDICATORIA

A mi Madre Luisa, que siempre ha confiado en su hijo y aunque me grita yo se lo que hace para que sea una mejor persona, me ha enseñado valores para que no me pierda en el camino.

A mi padre Robert, le dedico este trabajo como muestra de mis ganas de superación, él ha sido de gran apoyo para la culminación del mismo.

A mi Abuelita Carmencita, por siempre acordarse de su nieto y ser un gran ejemplo.

A mi familia en general, por siempre ser un apoyo y por compartir gratos momentos a mi lado.

Y a todos los que se alegren y celebren este triunfo conmigo.

José David Barba Samaniego

AGRADECIMIENTO

Agradezco a mis padres, familiares y amigos quienes han sido de gran apoyo tanto en mi crecimiento personal como profesional. Un agradecimiento especial a los Ingenieros José Luis Torres y Carlos Caizaguano por haber sido un pilar fundamental en el desarrollo del presente trabajo no solo como guía sino dando todo su apoyo y a mi compañero de tesis José Barba.

Giovanny Alexander Viteri Arias

AGRADECIMIENTO

Agradezco a mis padres, por tener la confianza y la paciencia necesaria para apoyarme en todas las decisiones que he tomado en la vida, además apoyarme en el camino universitario.

Al Ing. Torres y Ing. Caizaguano, por la colaboración brindada a la largo del presente proyecto.

A mi compañero Giovanny Viteri, por ser una gran persona con la que se puede trabajar y también entablar una amistad.

A mis amigos en general, por las frases de apoyo a lo largo de mi vida.

José David Barba Samaniego

CERTIFICACIÓN DE AUTENTICIDAD DEL PRESENTE INFORME

Nosotros, José David Barba Samaniego y Giovanny Alexander Viteri Arias, autores del presente informe de investigación, certificamos que corresponde a nuestra autoría y autenticidad.

José David Barba Samaniego	**Giovanny Alexander Viteri Arias**

Introducción

El presente trabajo de investigación está orientado a fortalecer el funcionamiento del Data Center de la ESPE, mediante la aplicación de la metodología COBIT 4.1 para analizar sus políticas internas y la comparación de la infraestructura interna del mismo con las normas internacionales y nacionales de calidad.

El presente trabajo contempla el desarrollo de los siguientes capítulos:

En el Capítulo 1 se incluye el fundamento metodológico de la investigación. En términos generales se describen el planteamiento y justificación del problema a investigar, los objetivos que serán cumplidos a lo largo del trabajo y el alcance de mismo.

En el Capítulo 2 está contemplado todo el marco teórico, en el cuál se abordó temas estrictamente importantes como la definición de un Data Center; se ha incluido la manera recomendable de diseñar un Data Center. En esta parte fue indispensable describir la metodología; las normas y estándares internacionales y nacionales de calidad para el funcionamiento de un Data Center.

En el Capítulo 3 se muestra las mediciones y resultados necesarios para compararlos con los parámetros mínimos establecidos en las normas y estándares. Además se puede observar las deducciones luego de aplicar la metodología COBIT 4.1.

En el Capítulo 4 contiene las conclusiones y recomendaciones obtenidas al realizar el trabajo de investigación las cuales podrán ser de utilidad para la UTIC. Se presentan también los anexos necesarios para complementar la misma, como anexo destacado podemos nombrar el “Manual de Procedimientos” donde se detallan los pasos a seguir para realizar el análisis y evaluación del funcionamiento de la infraestructura del Data Center de la ESPE.

Tabla de contenido

Contenido Ilustraciones

CAPÍTULO 2

CAPÍTULO 3

Contenido Tablas

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 1

1 FUNDAMENTO METODOLÓGICO

1.1 Planteamiento del Problema

1.1.1 Contextualización del Problema

La Escuela Politécnica del Ejército, ESPE, es una institución de Educación Superior, con 90 años de experiencia en la formación de profesionales de excelencia, con capacidad de liderazgo y educación en valores.

El Consejo Nacional de Evaluación y Acreditación Universitaria, la ha ubicado en la categoría “A”, máxima calificación otorgada a las universidades ecuatorianas de calidad. Debido al crecimiento estudiantil que ha experimentado la Escuela Politécnica del Ejército y el auge de las nuevas tecnologías, se ha visto en la necesidad de actualizar e incrementar la capacidad de su Data Center para satisfacer de mejor manera las necesidades de la comunidad politécnica y mejorar su rendimiento operacional a todos sus usuarios.

Esta mejora institucional genera nuevas demandas de carácter técnico, como seguridad; oferta y demanda de más información; aumento en el consumo de energía eléctrica; más recursos humanos y demanda de servicios de los usuarios, lo cual exige que el Data Center funcione con los más altos estándares y normas de calidad

La carencia de disponibilidad del Data Center, dificulta el rendimiento de los usuarios internos y externos; la optimización de la productividad de la tecnología de la información, la disponibilidad de la información académica y administrativa como calificaciones, horarios y distribución horaria entre los docentes y estudiantes; demanda de matrículas, reingresos de estudiantes; principalización de carreras para quienes optan por una nueva carrera; records académicos; información de graduados y posgrados y más demandas de servicios académicos y administrativos concernientes a los estudiantes y docentes de la

institución en la sede central; de Latacunga y extensiones como “Héroes del Cenepa”; IASA I y IASA II; los 26 Centros de Apoyo de la sede principal de la Modalidad de Educación a Distancia en todos el país.

La problemática a investigar se evidencia en situaciones como: descargas electrostáticas que provocan fallas en la transmisión de datos entre equipos, provocando la pérdida de información valiosa para la institución; también puede existir un calentamiento de los equipos, que dificulte su funcionamiento y provoque daños a los elementos que forman el Data Center. La falta de seguridad física y lógica, puede llevar a que se cometan delitos informáticos alterando su buen funcionamiento y pérdida de información.

1.2 Justificación e Importancia

Si el Data Center es un eje fundamental en el desenvolvimiento normal de las actividades académicas de la ESPE, es necesario realizar un análisis y evaluación del funcionamiento del Data Center, que permitan identificar las dificultades específicas y asignar una serie de recomendaciones y directrices que salvaguarden los bienes de la institución, mediante el mantenimiento e integridad de los datos e información, indispensables para alcanzar los objetivos institucionales de manera eficaz y eficiente.

Además, es necesario identificar dificultades y riesgos para plantear medidas preventivas y correctivas, minimizando el impacto de los errores y su rectificación.

El Data Center es considerado un generador de valor especial para la ESPE, sus profesionales, estudiantes y más personas que forman parte de ella; por este motivo, es indispensable realizar un análisis que se fundamente en las normas internacionales TIA 942; ANSI/BICSI-002 (Mejores Prácticas para el diseño e implementación de un Data Center); ISO/IEC 24764 (Tecnología de la Información – Cableado Genérico para predios de Data Center); y, en la Norma Ecuatoriana de Construcción (NEC10).

Mediante el análisis se puede verificar el funcionamiento del sistema de energía eléctrica, para prevenir y controlar incendios e inundaciones como drenajes y extintores, vías de evacuación, puertas y pinturas ignifugas, aire acondicionado, UPS, pisos y techos falsos, alarmas, control de temperatura y humedad, cerraduras electromagnéticas, cámaras de seguridad, detectores de movimiento, tarjetas de identificación.

La importancia de la disponibilidad ininterrumpida del Data Center es esencial para la operación, desempeño y continuidad de actividades tecnológicas. Se debe garantizar su calidad de funcionamiento, mediante la tolerancia a fallas previsibles; todo esto es posible, mediante una evaluación del cumplimiento de normas nacionales e internacionales; y, de los reglamentos internos.

1.3 Objetivos

1.3.1 Objetivo General

Realizar una evaluación técnica de la infraestructura del Data Center de la Escuela Politécnica del Ejército, mediante actividades de observación y aplicación de herramientas de software, para garantizar el cumplimiento de las normas y estándares nacionales e internacionales de calidad, y reglamentos internos.

1.3.2 Objetivos específicos

- Determinar la situación actual del funcionamiento de los elementos, infraestructura; políticas y procedimientos del Data Center de la ESPE, considerados por la metodología COBIT 4.1.

- Analizar la pertinencia de los parámetros mínimos que constan en las normas nacionales e internacionales, en la utilización de los elementos y su aplicación en infraestructura del Data Center.

- Proponer recomendaciones de ser necesarias, para alcanzar los parámetros mínimos de las normas de calidad, en la optimización del funcionamiento del Data Center.

- Diseñar un Manual de procedimientos de análisis y evaluación, con el cual se pueda verificar los parámetros de funcionamiento del Data Center de la ESPE.

1.4 Alcance

Mediante la citada evaluación exploratoria se verificará el estado actual del Data Center de la ESPE, cuyo estudio permitirá un diagnóstico, conclusiones y recomendaciones, para el recurso de TI (Infraestructura), evaluado en los dominios: PO4 (Responsabilidades del personal frente al mantenimiento de la infraestructura del Data Center); PO9 (Reconoce los riesgos a los que está expuesta la infraestructura); AI3 (Mantenimiento y Disponibilidad de la Infraestructura); D2 (Determinar los Riesgos de los proveedores de servicios); DS4 (Recursos Críticos y Políticas de respaldo de información); DS5 (Prevención contra software malicioso); DS12 (Acceso Físico, protección contra factores ambientales, Administración Instalaciones Físicas); ME3 (Calificación de servicios de proveedores) y según la metodología COBIT 4.1.

Se determinará si el Data Center de la ESPE cumple con los requisitos mínimos, mediante evaluaciones y monitoreo de los activos, para concluir si puede ser considerado como TIER I o TIER II con las normas TIA 942; ANSI/BICSI-002, Mejores Prácticas para el diseño e implementación de un Data Center; ISO/IEC 24764 (Tecnología de la Información – Cableado Genérico para predios de Data Center); Uptime Institute TIERs; y, NEC-10 (Norma Ecuatoriana de Construcción).

CAPÍTULO 2

2 FUNDAMENTO TEÓRICO

2.1 Fundamentos de un Data Center

2.1.1 ¿Qué es un Data Center?

Es un “Centro de Datos” o “Centro de Proceso de Datos” (CPD), los cuales son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlos. Esta infraestructura informática, se ha creado para preservar y/o administrar información con seguridad, usando tecnología de punta.

Ahí se encuentran todos los recursos necesarios para el almacenamiento, gestión y procesamiento de información y ofrecer servicios de TI; es decir, infraestructura, equipos informáticos como racks, dispositivos de networking y almacenamiento, servidores (web, aplicaciones, base de datos) y áreas de soporte.

Es un activo muy importante y vulnerable en toda empresa, porque todos los recursos humanos inmersos, dependen de la información, necesaria para desarrollar su trabajo cotidiano, y garantizar de esta manera, los servicios informáticos que demandan las organizaciones empresariales y académicas.

2.1.2 Componentes de un Data Center

Un Data Center se compone de cuatro elementos principales:

Espacio blanco: Es un espacio libre dentro del Data Center, necesarios para poder reasignar alguna función en particular; por ejemplo, un área para equipos nuevos.

Infraestructura de apoyo: se refiere a los equipos y espacio necesarios para apoyar las funciones del Data Center como: transformadores, UPS, equipos de ventilación y aire acondicionado; panel de distribución de energía y equipos de transmisión remota**.**

Equipos de Soporte: como racks o bastidores, cableado estructurado, servidores, unidades de almacenamiento y equipos de red.

Operaciones: constituye el personal de operaciones o de soporte técnico, a quien asegura que los equipos y la infraestructura tengan el mantenimiento adecuado; estén mejorados y reparados.

2.2 Funciones de la Unidad de Tecnologías de la Información y Comunicación, con respaldo del Data Center.

- Cumplir y difundir con reglamentos y normas el correcto uso de los equipos informáticos.

- Prestar varios servicios informáticos a diferentes áreas de una empresa, por ejemplo: soporte técnico o help-desk; mantenimiento de equipos, servidor de aplicaciones e impresión.

- Almacenar datos para una mejor gestión de la información

- Desarrollo de aplicaciones y sistemas para beneficio de la empresa.

- Manejar el sistema informático central para garantizar su disponibilidad para los usuarios.

- Capacitar a los usuarios y al personal especializado acerca del uso adecuado de las aplicaciones y los equipos informáticos.

- Realizar el mantenimiento, actualización y limpieza de los equipos informáticos (soporte técnico).

- Supervisar las instalaciones de cableado y comunicaciones.

- Definir y ejecutar las necesidades de ampliación del cableado estructurado.

- Llevar un log o registro de fallos, problemas, soluciones, mantenimientos, actualizaciones, equipos, software instalado en los computadores y trabajos realizados.

- Realizar evaluaciones técnicas tanto de hardware como de software.

2.2.1 Recomendaciones para un Data Center eficiente:

- Tener un buen sistema de acondicionamiento para mantener una temperatura y humedad adecuada, para que los equipos electrónicos operen 24/7. Satisfactoriamente.

- Mantener el sistema de cableado; este debe estar siempre limpio y ordenado para evitar fallas en la transmisión de la información y de la energía eléctrica, ya que se utiliza tuberías y canaletas separadas; unas para el cableado estructurado y otras para el sistema eléctrico; también ayuda a mantener un buen flujo del aire. Estas medidas preventivas, facilitarán trabajos de mantenimiento posteriores.
- Disponer de un plan de seguridad, prevención, detección y extinción de incendios que salvaguarden la integridad de las personas y de la información, el activo más importante de la empresa.

- Debe contar con controles de acceso y puertas de seguridad, ya que solo personas autorizadas podrán ingresar al Data Center, así se evitará pérdida de información o daño en los sistemas y equipos.

- Conjuntamente con las anteriores recomendaciones, se debe disponer de un sistema de monitoreo y vigilancia (CCTV), para ver qué sucede dentro y fuera del Data Center y así prevenir percances.

- Contar con uno o más UPS con la finalidad de proveer energía eléctrica a los servidores, para que los servicios de informática tengan un alto grado

de disponibilidad. En el caso de corte del suministro eléctrico se requiere que funcionen normalmente o ininterrumpidamente.

2.2.2 ¿Qué es un Data Center Green?

Es un "Centro de Datos Verdes" que puede operar con el mínimo impacto en el medio ambiente, con la mayor eficiencia energética o con reducción máxima en el consumo de la electricidad.

2.3 Diseño de un Data Center

Al momento de considerar un diseño general de un Data Center se debe tomar en cuenta los siguientes parámetros:

- Espacio y diagrama de distribución.
- Cables a utilizar.
- Energía eléctrica.
- Refrigeración.

2.3.1 Espacio de Distribución

Se debe tener en cuenta una posible expansión futura del Data Center, ante la posibilidad de la adquisición de equipos nuevos; o al menos, garantizar que exista un área que se pueda anexar a él, de manera fácil y económica.

2.3.2 Diagrama de Distribución

A continuación se detallan algunas consideraciones para realizar una distribución aceptable y avalada por la norma internacional TIA-942:

- **Área de distribución de equipos:** Se considera la ubicación de los racks y gabinetes colocados en la configuración: "pasillo caliente/pasillo frío". Se tendrá una disipación eficaz del calor en los equipos.

- **Área de distribución horizontal:** En esta área se ubican las interconexiones horizontales. Es el punto de distribución de cableado para las áreas o él área de distribución de equipos. Esta área especifica un máximo de 2000 cables UTP de 4 pares o terminales coaxiales.

- **Área de distribución principal:** Es el punto central de conexión cruzada para el sistema de cableado estructurado de todo el Data Center. Se debe ubicar en la parte central para superar las distancias de cableado recomendadas.

- **Área de distribución de zona**: En esta área se concentra todo el cableado para los equipos que no aceptan paneles de cruzada.

- **Cuarto de Entrada**: Proveedores de ISP.

2.3.3 Administración de Cables

El sistema de cableado es genérico y permanente. Es un servicio flexible al que se pueden conectar nuevas aplicaciones o equipos. Si un Data Center es diseñado con esta mentalidad es factible hacer cualquier cambio o adición a futuro.

Racks y gabinetes: Deben brindar un amplio control de cables en dirección horizontal o vertical. Además de mantener organizado el cableado también elimina los obstáculos para mantener los equipos frescos. Estos equipos deben mantener y proteger los cables, asegurando que no excedan los límites del radio de curvatura o manejar la holgura del cable.

Sistema de tendido de cable: El tendido de cable debe usar el trayecto por debajo del piso falso para el cableado permanente; y, el trayecto por encima del piso, para el cableado temporal. Se deben separar los cables de cruzada y datos, de los de fibra, ya que la fibra es más frágil y puede sufrir daños.

Consideraciones Adicionales: Al instalar racks y el tendido de cable, se debe considerar lo siguiente:

- Los racks deben ser equipados con canales superiores de 3.5 pulgadas y 7 pulgadas inferiores para facilitar el tendido de cables.

- Instalar racks en las zonas principal y horizontal para un control unificado del cable.
- La fibra debe ser tendida en canales para evitar su deterioro.

2.3.4 Métodos de conexión

Existen tres tipos de conexión reconocidas:

Conexión Directa: Para un Data Center no es una opción adecuada ya que para movilizar equipos o realizar cambios internos, se tendría que localizar cables y moverlos con cuidado hacia la nueva ubicación, convirtiéndose en un gasto innecesario de recursos y de tiempo.

Interconexión: Se refiere a crear un ambiente amplio de trabajo, configurando una LAN, para que todos los usuarios puedan utilizar los servicios.

Conexión Cruzada: Es un sistema con el cual se pueden alcanzar bajos costos y un servicio muy confiable; todos los elementos de una red tienen conexiones de cable permanentes que se terminan una vez y no se vuelven a manejar nunca más. Algunas de las ventajas de esta conexión serían las siguientes:

- Reduce enormemente el tiempo de instalación de nuevos componentes como por ejemplo: agregar tarjetas, modernizar software y realizar mantenimiento.

- Las conexiones permanentes protegen los cables de las actividades y el desgaste cotidiano.

- Capacidad de aislar segmentos para reparar cualquier avería en la red, volviendo a tener un circuito mediante una reconexión.

- Se pueden realizar cambios muy rápidos en la red.
- Fácil activación de nuevos servicios con la ayuda de un cordón de cruzada.

2.3.5 Energía Eléctrica

Los Data Center deben garantizar un suministro de energía confiable. Entre los procedimientos que normalmente se lleva a cabo figuran:

- Suministro de Alimentación Interrumpible (UPS).

- Dos fuentes de alimentación provistas por dos empresas de servicio eléctrico.

- Generadores en el sitio.

- Circuitos múltiples.

2.3.6 Refrigeración:

Existe un método para favorecer la circulación de aire; es conocido como “pasillo caliente/pasillo frio”. Los racks se disponen en filas alternas de pasillos fríos y calientes. En el pasillo frío los racks se ponen frente a frente y en los pasillos calientes dorso contra dorso. Las placas perforadas en el piso falso de los pasillos fríos permiten que llegue aire frío al frente de los equipos. Lo que realiza el aire frío es envolver al equipo y ser expulsado por la parte trasera hacia al pasillo caliente. Como se muestra en la ilustración 2.1.

- Extender la altura del piso falso, esto permite aumentar la corriente de aire en un 50%.
- Usar racks abiertos en lugar de gabinetes.

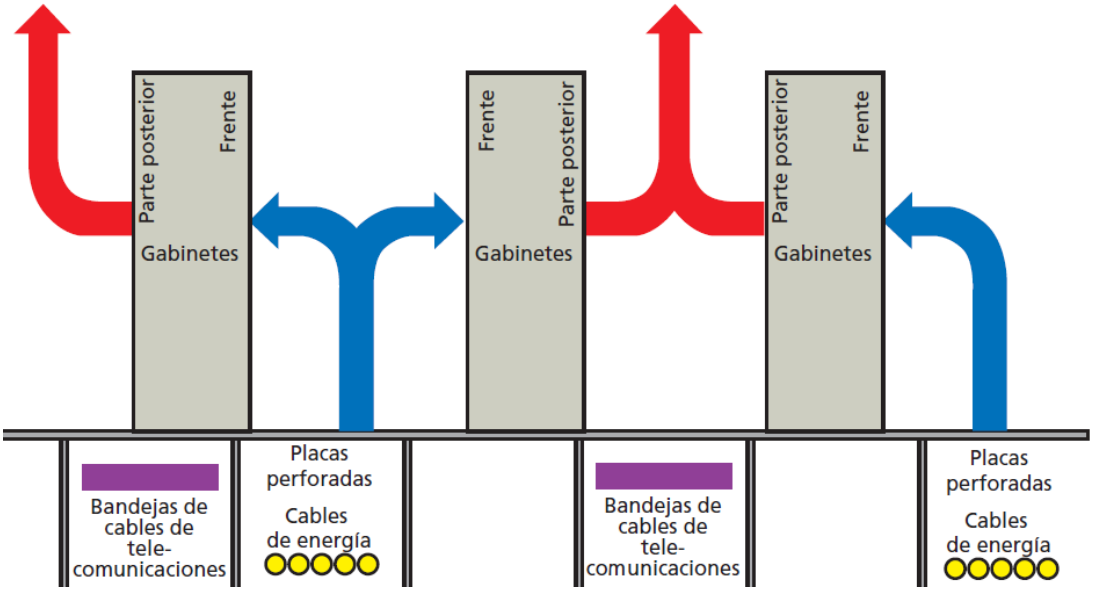


Ilustración 2.1 Configuración de los pasillos "Calientes y Fríos"

FUENTE: ADC Informe Técnico

2.4 Normativa

2.4.1 Estándar TIA 942

Este estándar se creó con la intención de unificar los criterios de diseño e implementación de los Data Center, añadiendo a estos la planificación de la instalación, el sistema de cableado estructurado y el diseño de la red.

Una planificación adecuada durante la implementación del Data Center es necesaria porque permitirá optimizar recursos económicos y resolver oportunamente errores y evitar costos, después de su instalación.

Los Data Center pueden beneficiarse de una buena infraestructura indispensable para apoyar el crecimiento y los cambios en los sistemas informáticos. TIA-942 presenta una topología de infraestructura para el acceso y la conexión de los respectivos elementos en el sistema de cableado; también especifica un sistema de telecomunicaciones y las instalaciones relacionadas con dicha función.

Criterios a considerar:

El estándar TIA-942 da dos categorías de criterios: de recomendaciones y de asesoramiento; estos se aplican en general a la protección, rendimiento, compatibilidad y administración de los requisitos mínimos aceptables que el estándar especifica.

Los criterios obligatorios son de asesoramiento y deben ser utilizados como recomienda este estándar, así mejorará el rendimiento general del sistema de cableado.

2.4.1.1 Unidades de Medida:

En la tabla 2.1 se muestra los acrónimos de las unidades de medida.

Tabla 2.1 Unidades de Medida

A	Amperio
°C	Grado Centígrado
°F	Grado Fahrenheit
Gb/s	Gigabit/segundo
Hz	Hertz
kb/s	Kilobit/segundo
kHz	Kilohercio
kVA	Kilo voltio amperio
kW	Kilovatio
Lbf	Libra-fuerza
MHz	Mega Hertz
µm	Micra

Fuente: TIA-942

2.4.1.2 Diseño de construcción de un Data Center

La información y recomendaciones al planificar el diseño de un Data Center, tienen el objetivo de permitir su efectiva implementación, mediante la identificación de las acciones apropiadas que deben adoptarse en cada paso del proceso.

Los pasos a seguir para el diseño del Data Center son:

- Estimación de equipos de telecomunicaciones, espacio, energía y refrigeración; seguridad, carga sobre el suelo, protección del sistema de tierra, protección eléctrica y demás requisitos de las instalaciones a realizar los arquitectos e ingenieros. Estas acciones son necesarias para obtener una capacidad total y una prolongada vida útil.

- Crear un plan de equipamiento para todas las áreas con las cuales contará el Data Center: vías de acceso, áreas principales de distribución, áreas horizontales de distribución, áreas de equipos para suministrar la energía, telecomunicaciones y ventilación en todas estas áreas.

- Diseño del cableado, basado en las necesidades de los equipos que van a operar en el Data Center.

- El lugar donde decida establecer el centro de datos es igual de importante que los datos que vaya a almacenar en él. En general, los centros de datos se ubican fuera y lejos de las sedes o sucursales de las compañías.

- Un centro de datos 'verde' es aquel que optimiza la eficiencia de la iluminación, refrigeración, disipación de calor, consumo de energía y la configuración de sistemas de hardware con el fin de minimizar el impacto medioambiental. Un centro 'verde' consume hasta un 80 por ciento menos de energía que las instalaciones construidas hace tan solo dos años.

Estos pasos se pueden utilizar para implementar un nuevo Data Center o ampliar uno ya construido. Como se muestra en la ilustración 2.2.

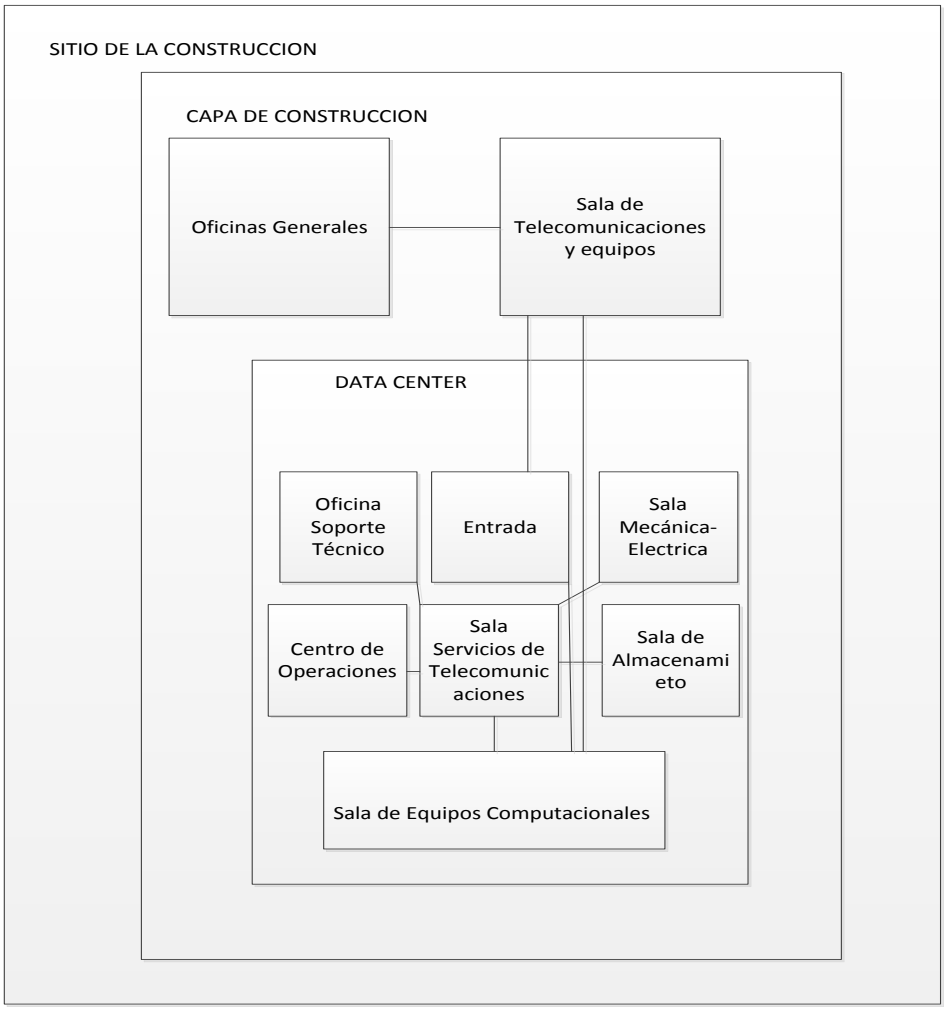


Ilustración 2.2 Construcción del Data Center

Fuente: TIA-942

2.4.1.3 Espacios para Telecomunicaciones:

El Data Center requiere de espacios dedicados para la infraestructura de telecomunicaciones. Como se muestra en la ilustración 2.3.

Elementos principales:

- Sala de entrada,
- Área principal de distribución (MDA).
- Área de distribución horizontal (HDA).
- Área de la zona de distribución (ZDA).
- Área de distribución de equipos (EDA).

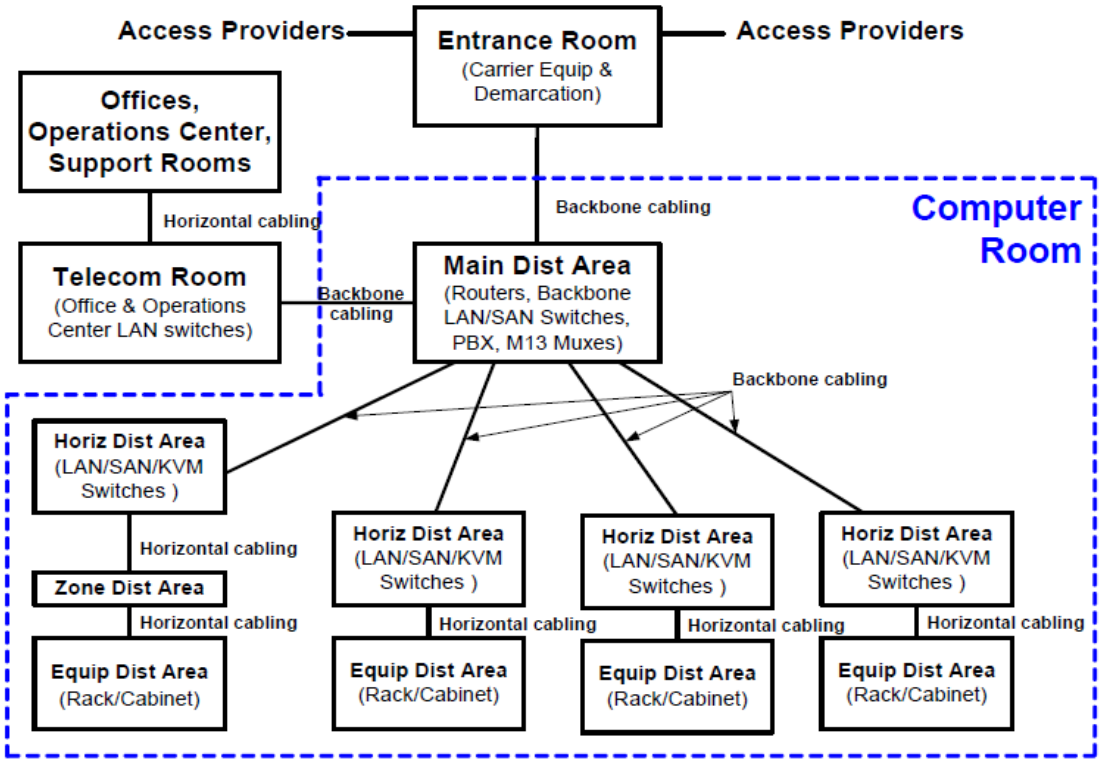


Ilustración 2.3 Ejemplo Básico de un Data Center.- Requisitos sala de computadores

Fuente: TIA-942 Cap.5

El objetivo de un Data Center es albergar los equipos y cableado, relacionados con los sistemas informáticos y sistemas de telecomunicaciones. Solo el personal autorizado tendrá acceso a esta sala, la cual debe contar con el suficiente espacio para cada equipo.

Se recomienda que la separación de cada equipo no sea mayor a la proyección del acondicionador: no más de 12 metros.

Respecto a los equipos de control eléctrico, UPS, el sistema de acondicionamiento que sobrepase los 100kVA, deberá ser situado en otra sala. La altura mínima establecida por el estándar es de 2.6 metros desde el piso hasta cualquier obstáculo ya sean tuberías aéreas, cielo falso, luminarias, cámaras. Si los bastidores o gabinetes tienen una altura de 2 metros, es recomendable que esta sala tenga 4.6 centímetros más, con respecto a los 2,6 metros.

En referencia al piso, paredes y techo, deben ser construidos y pintados con materiales de alta calidad, para minimizar la afluencia de polvo; se deberá pintar

con colores claros para mejorar la iluminación de la sala; y, los pisos deberán tener una propiedad antiestática para que no afecte desfavorablemente el funcionamiento de los equipos.

La iluminación deberá ser de 500 lux (lúmenes/m2) en el plano horizontal y de 200 lux para el plano vertical; las luminarias deberán estar situadas a 2 metros del suelo.

Para las puertas de acceso a esta sala, el estándar recomienda como mínimo 1 metro de ancho y 2,13 metros de alto; esta puerta deberá abrirse hacia el exterior. Dentro de esta sala no debe existir ningún tipo de comunicación hacia el exterior del edificio, para prevenir cualquier pérdida de información o sustracción de la misma.

El suelo de la sala debe soportar todo el peso de los equipos, por este motivo, la distribución de carga mínima debe ser de 250 lb/ft2.

Respecto a la señalización, la sala deberá contar con carteles de la salida de emergencia.

Obligatoriamente un Data Center, deberá contar con calefacción, ventilación y aire acondicionado para los equipos de soporte como el UPS, cuyo sistema de aire acondicionado entre otros, deberán trabajar y estar disponible los 365 días del año y durante las 24 horas, para asegurar una operación continua de todas las actividades del Data Center.
Los parámetros de operación en el Data Center son:

- Temperatura entre 20°C y 25°C.
- Humedad entre 40% a 55%.
- Tasa de oscilación de temperatura de 5°C por hora.

La temperatura y la humedad se deben medir cuando los equipos estén en funcionamiento. Los toma corrientes deberán tener tomas de 120V con 20A; la

separación de estos tomas será de 3.65 metros, no es adecuada la utilización de cortapicos.

En la puesta a tierra se utilizarán tiras de cobre de 8 pulgadas, soldadas como una rejilla. Los sistemas de protección contra incendios deberán cumplir con la norma NFPA-75.

Prevenir incendios, simplemente implica eliminar todas las fuentes de ignición y reducir la cantidad de materiales combustibles en la sala. En el improbable caso de que un incendio se propague desde otra área a una sala de TI, habrá que minimizar los combustibles tanto de papel como electrónicos. Se deben construir barreras corta incendios o ignifugas, ya que la mayoría de los incendios de acuerdo a estadísticas, se provocan fuera del Data Center. Para evitar inundaciones, debe existir un sistema de desagüe del mismo.

Otro aspecto importante a tomar en cuenta, es el espacio necesario para el cableado, tablero de energía, bastidores y vías para acceder a las diferentes salas.

2.4.1.4 Sistema de Cableado del Data Center

Este sistema de cableado es una infraestructura que soporta varios entornos y varios proveedores de servicios.

Cableado Horizontal:

El cableado se extiende desde la sala de equipos hasta la sala de distribución principal; reduce el costo de mantenimiento y ubicación; debe estar diseñado para futuras instalaciones de equipos. El cableado horizontal debe ser instalado en una topología de estrella; cada terminación en el área de distribución debe conectar a un equipo.

Respecto a las distancias del cableado horizontal, este no debe sobrepasar los 90 metros, independientemente del tipo de equipos o medios de comunicación y 300 metros para fibra óptica. Se muestra en la tabla 2.2.

Tabla 2.2 Tabla Longitud Máxima de los cables horizontales

Longitud	Área de Cables	Área de cables, cables conexión(UTP) y equipos
90 m	5 m	10 m
85 m	9 m	14 m
80 m	13 m	18 m
75 m	17 m	22 m
70 m	22 m	27 m

Fuente: TIA-942

Cableado Vertical o Backbone:

Este estándar recomienda y está certificado el uso de cable par trenzado categoría 6 de 100ohm, fibra óptica multimodo 50/125 y 62.5/125 fibra óptica monomodo.

Recomendaciones para el cableado:

Para la seguridad del cableado contra cualquier daño, el estándar recomienda no tener cables vistos por los usuarios o para la gente externa del Data Center, a menos que estos estén dentro de un conducto, tuberías o canaletas, que se conviertan en vías seguras para tender el cable; todos los racks, bastidores, sala de mantenimiento, cajas de empalmes deben tener candado o seguridad.

Además, se recomienda no tener el cableado cerca de los cables de alimentación; esta distancia de separación debe ser de 300 milímetros. Si dicha instalación es por tuberías metálicas, debería ser conectada a tierra. En la ilustración 2.4 se muestra el cableado horizontal y vertical.

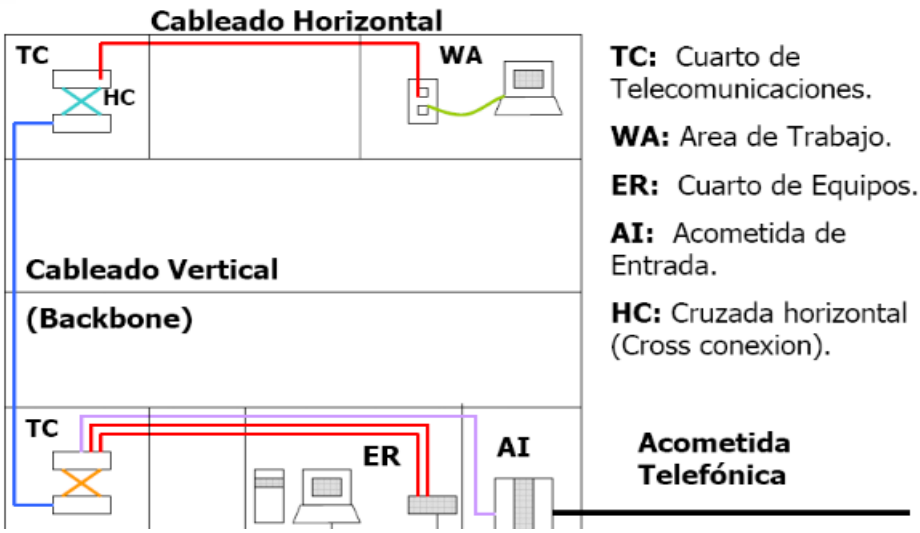


Ilustración 2.4 Tipos de Cableado

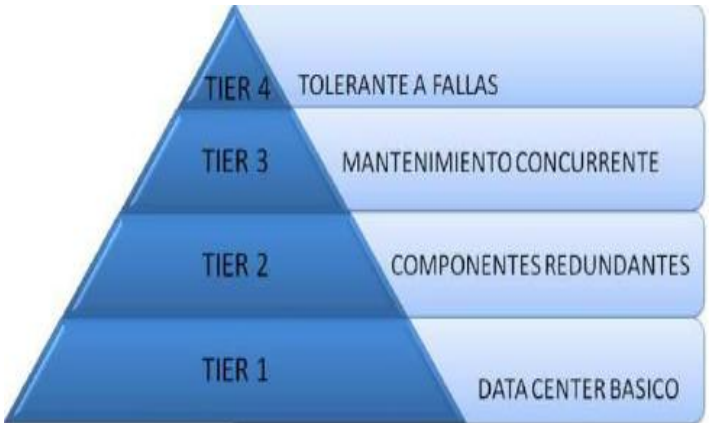
Fuente: S. Galván Cableado Estructurado

2.4.2 Uptime Institute Data Center TIER:

Uptime Institute clasificó los siguientes aspectos para un Data Center: disponibilidad, confiabilidad, costos de construcción y mantenimiento del Data Center.

En la tabla 2.3 se evidencia la funcionalidad de cada uno de los TIERs, frente a la disponibilidad ininterrumpida de servicios.

Tabla 2.3 Pirámide de Jerarquía TIER



Fuente: Artículo Técnico Cesar Erazo Cap. 2

Según la Uptime Institute, se proponen cuatro niveles para clasificar a los Data Centers de mayor fiabilidad, como se muestra en la tabla 2.4.

Tabla 2.4 Clasificación del Uptime Institute para clasificar a los Data Center

Nivel	Descripción	Disponibilidad
I	Los Data Center de nivel I corren el riesgo de disrupciones a partir de acontecimientos planificados e imprevistos. Si tienen un UPS o un generador de energía, estos son sistemas modulares únicos con muchos puntos individuales de falla. Se deberá apagar los equipos para su mantenimiento y las fallas espontáneas provocarán disrupciones en el Data Center.	99.671%
II	Los Data Center del nivel II son un poco menos propensos a las disrupciones que los Data Center del nivel I porque tienen elementos redundantes; sin embargo, tienen una trayectoria de distribución de filamento simple, lo que implica que se deberá apagar los equipos para realizar el mantenimiento en la trayectoria de energía crítica y otras piezas de la infraestructura.	99.741%
III	Se pueden realizar tareas de mantenimiento programadas sin disrupciones en los Data Centers del nivel III. Tienen la capacidad y la distribución suficientes para transportar la carga de un trayecto en forma simultánea mientras se repara el otro trayecto; sin embargo, actividades imprevistas, como errores en la operación o fallas espontáneas de elementos, causarán disrupciones.	99.982%
IV	Los Data Centers del nivel IV pueden realizar cualquier actividad programada sin disrupciones en la carga crítica y admitir al menos una de las peores fallas imprevistas sin impacto en la carga crítica. En términos eléctricos,	99.995%

	implica dos sistemas de UPS separados en los que cada sistema tenga redundancia N+1. El nivel IV exige que el hardware de todas las computadoras tenga entradas de potencia doble; sin embargo, debido a los códigos de seguridad de incendio y electricidad, habrá un tiempo de interrupción del servicio por las alarmas de incendio o personas que hagan una interrupción de energía de emergencia.	

Fuente: BICSI-002

2.4.2.1 TIER I:

Es una infraestructura básica donde no existe ningún componente redundante; existe un solo proveedor y una sola ruta de cableado. Los servicios que brinda el Data Center pueden verse interrumpidos por actividades deseadas o no deseadas; por ejemplo, corte del suministro eléctrico, tareas de mantenimiento en el Data Center. Esta infraestructura cuenta con un sistema de aire acondicionado y un sistema de distribución de energía; este, puede o no tener un UPS, generadores auxiliares, piso y cielo falso. También tiene sistema básico de puesta a tierra.

El tiempo estimado para la construcción e implementación de un Data Center Tier I es aproximadamente de tres meses. Como muestra la ilustración 2.5.

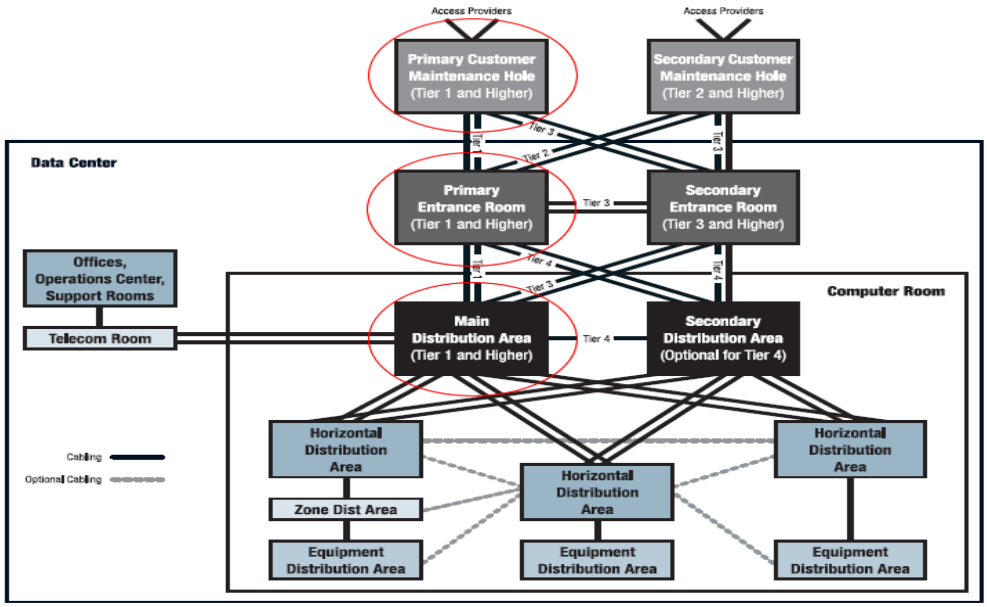


Ilustración 2.5 TIER I

Fuente: TIA-942 (TIERs)

2.4.2.2 TIER II:

Presenta una infraestructura redundante en equipos críticos de telecomunicaciones, fuentes de poder, procesadores con una sola ruta de cableado. Los servicios que brinda el Data Center pueden verse interrumpidos en menor porcentaje por actividades deseadas o no deseadas; como por ejemplo: corte del suministro eléctrico o tareas de mantenimiento en el Data Center. Esta infraestructura cuenta con UPS, generadores auxiliares, piso y cielo falso. Además cuenta con puertas de seguridad y aire acondicionado que mantienen una temperatura y humedad adecuadas. Como se muestra en la ilustración 2.6.

El tiempo estimado para la construcción e implementación de un Data Center Tier II es aproximadamente de tres a seis meses.

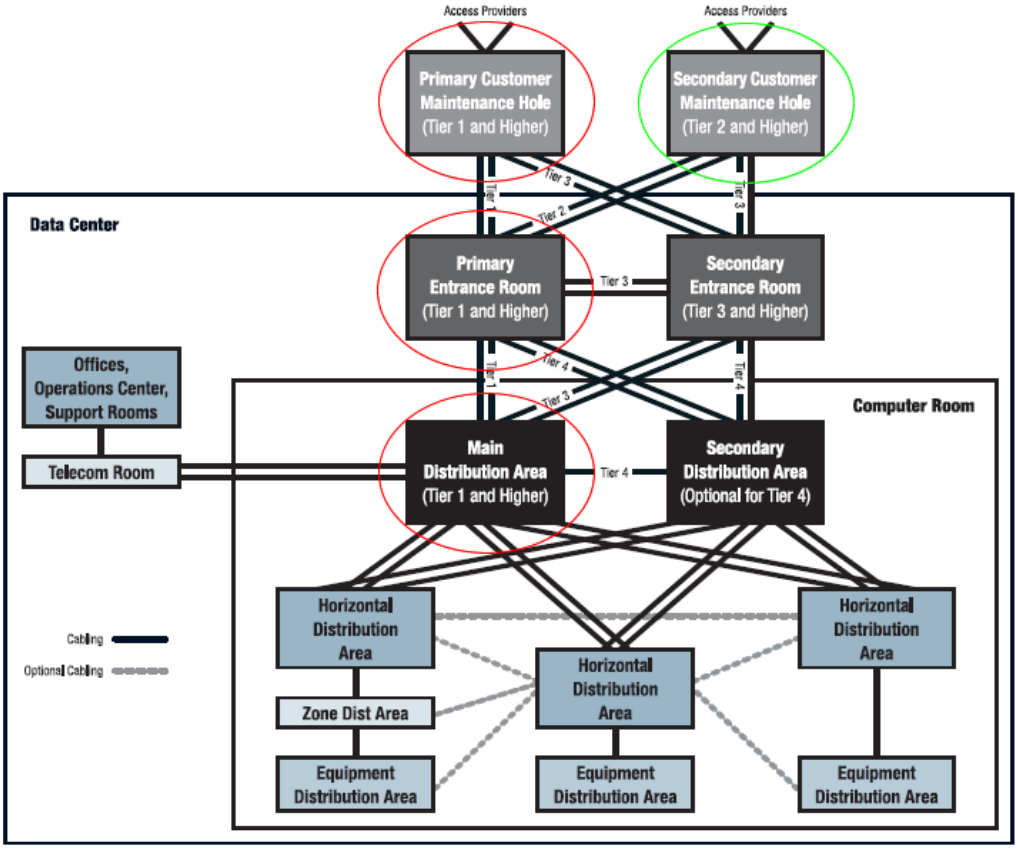


Ilustración 2.6 TIER II

Fuente: TIA-942(TIERs)

2.4.2.3 TIER III:

Presenta una infraestructura concurrente mantenible; tiene varias vías de distribución; por lo general 2 proveedores de servicios. Los servicios que brinda el

Data Center no se ven interrumpidos por mantenimiento, ya que se puede suspender una línea y dar el servicio por otra línea de distribución. Esta infraestructura cuenta con acceso controlado, sistema CCTV, múltiples unidades de aire acondicionado y detección de inundaciones. Como se muestra en la ilustración 2.7.

El tiempo estimado para la construcción e implementación de un Data Center Tier III es aproximadamente de quince a veinte meses.

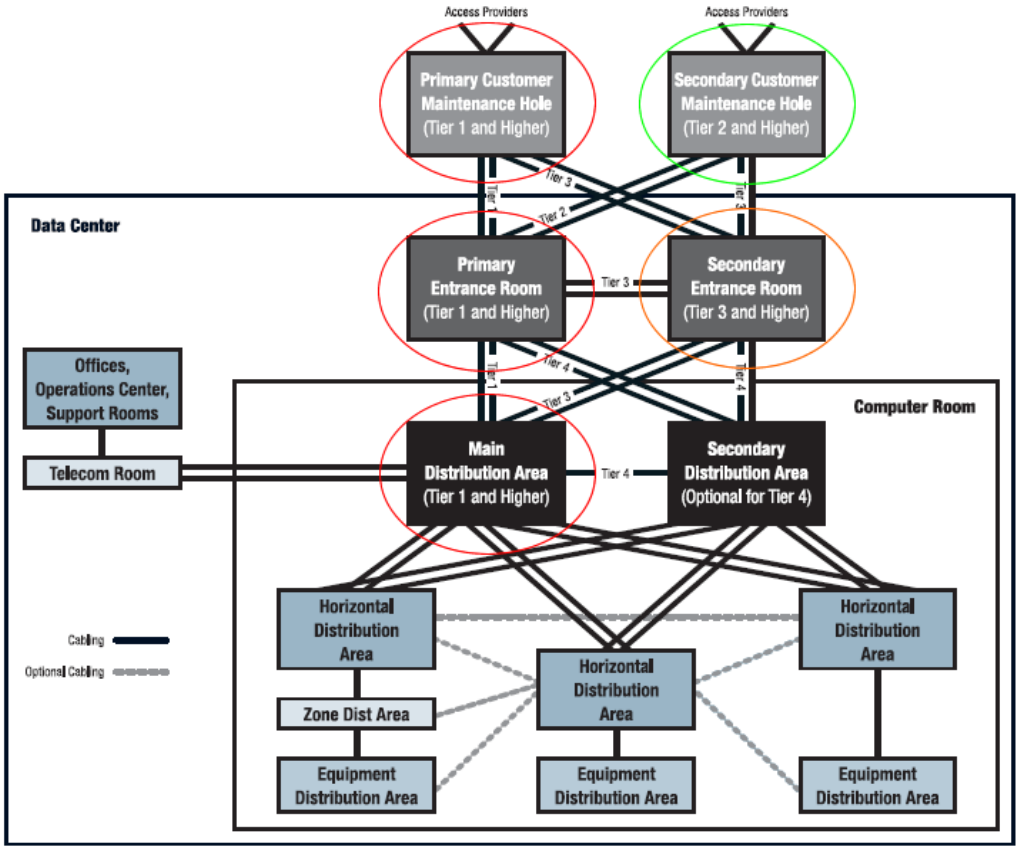


Ilustración 2.7 TIER III

Fuente: TIA-942 (TIERs)

2.4.2.4 TIER IV:

Presenta una infraestructura tolerante a fallas. Usualmente con este tipo de infraestructura cuentan las entidades financieras. Tiene componentes redundantes y varias vías de distribución. Los servicios que brinda el Data Center no se ven interrumpidos por mantenimientos, ya que se puede quitar un elemento, sin ocasionar interrupciones en los servicios del Data Center. Esta infraestructura

cuenta con protección para desastres naturales, sismos. Comprende un edificio separado (áreas aisladas) solo para el Data Center. Como se muestra en la ilustración 2.8.

El tiempo estimado para la construcción e implementación de un Data Center Tier IV es aproximadamente de quince a veinte meses.

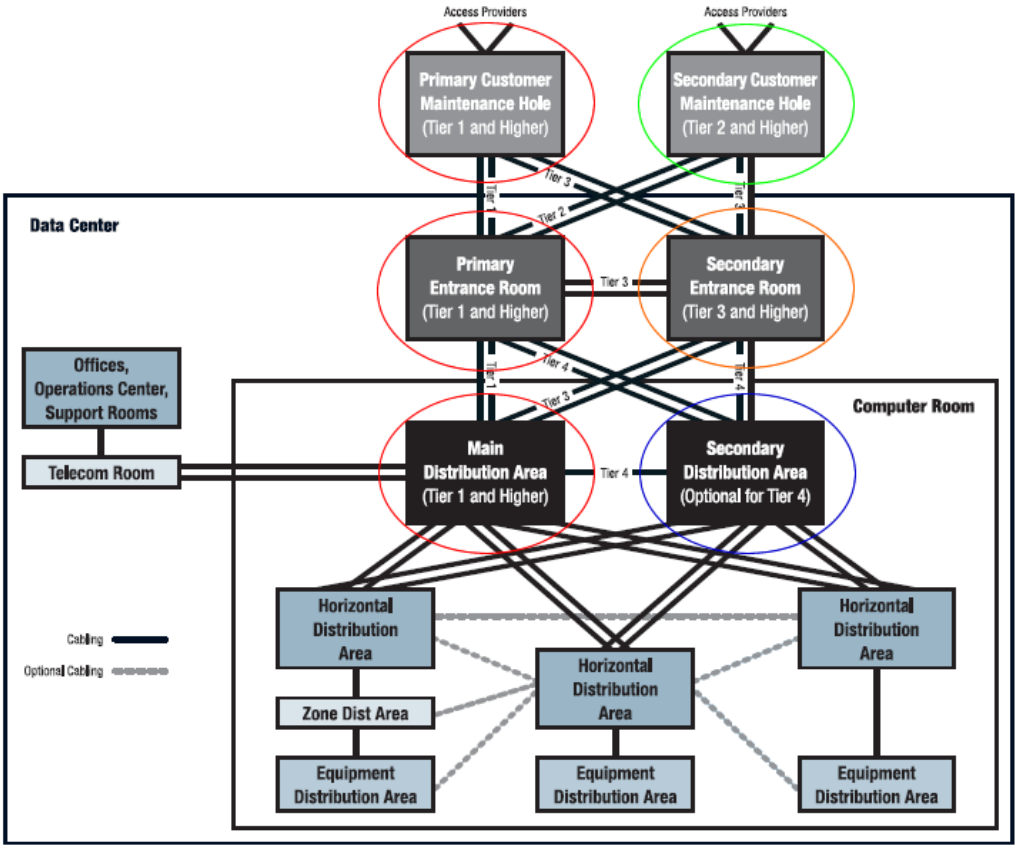


Ilustración 2.8 TIER IV

Fuente: TIA-942 (TIERs)

2.4.3 ANSI/BICSI-002-2011

Mejores Prácticas para el diseño e implementación de un Data Center

Este estándar da las mejores prácticas y métodos de implementación. Complementan otras normas y documentos que avalan a los Data Center como:

- TIA
- CENELEC
- ISO/IEC

Categoriza los criterios en dos:

Obligatorio: Estos criterios se aplican en general a la protección, el rendimiento, la administración y la compatibilidad; dándoles las especificaciones de los requisitos absolutos mínimos aceptables.

Asesoría: Estos criterios pueden ser catalogados como criterios deseables; se presentan cuando su logro mejora el rendimiento general de la infraestructura del Data Center en todas sus aplicaciones previstas.

2.4.3.1 Contenido Substancial del Estándar:

- Planificación del Espacio
- Selección del Sitio
- Arquitectura
- Estructura
- Sistemas Electrónicos
- Mecánica
- Protección contra incendios
- Seguridad
- Automatización del Edificio
- Telecomunicaciones
- Tecnologías de la Información
- Puesta en Marcha
- Mantenimiento del Data Center

2.4.3.2 Recomendaciones del Estándar:

Para un estándar de diseño se puede usar BICSI-002-2011 junto con la correspondiente norma local de la infraestructura de telecomunicaciones, los espacios y el sistema de cableado para el Data Center, como se muestra en la tabla 2.5. Las normas locales podrían ser:

- ANSI/TIA-942
- ISO/IEC 24764

Tabla 2.5 Acrónimos Espacios Data Center

Espacios del Data Center	Acrónimos
Entrada de Facilidad	EF
Área de distribución principal	MDA
Área de distribución intermedia	IDA
Área de distribución horizontal	HDA
Área de distribución zona	ZDA
Área de distribución equipos	EDA

FUENTE: BICSI-002, TIA-942

- Alimentación de los servicios Eléctricos(en la tabla 2.6 y 2.7 se muestra la fiabilidad y disponibilidad de la sistemas eléctricos)

  - **Una entrada/una vía:** Espacio dedicado, adyacente o en estrecha proximidad al espacio eléctrico de distribución principal del Data Center.

  - **Doble entrada/doble vía**: Espacios dedicados y separados el uno del otro.

  - **Una entrada/doble vía:** Espacio dedicado, equivalente a la distancia del doble de los espacios de distribución eléctrica del Data Center.

Tabla 2.6 Fiabilidad y Disponibilidad de los Sistemas Eléctricos

Clasificación	Tipo
Clase F0	Único camino para el Data Center, sin ninguno de los siguientes componentes: fuente de energía alternativa; UPS; TI adecuada conexión a tierra.
Clase F1	Data Center con único camino.
Clase F2	Data Center con único camino con componentes redundantes.
Clase F3	Data Center sustentable y operable al mismo tiempo.
Clase F4	Data Center tolerante a fallos.

FUENTE: BICSI-002

Tabla 2.7 Sistemas Eléctricos

Disponibilidad	**Explicación de las clases**	**Tácticas de las clases**
Clase F0 Objetivo Disponibilidad < 99%	Apoyar a los requisitos básicos del medio ambiente y la energía de las funciones de TI, sin equipos complementarios. La evasión del costo de capital es el principal motor. Hay un alto riesgo de caídas debido a los eventos planificados y no planificados. No hay un generador de respaldo.	**Redundancia de componentes:** 0 **Sistema de redundancia:** 0 **Control de calidad:** Estándar **Supervivencia:** 0
Clase F1 Objetivo Disponibilidad < 99%	Apoyar a los requisitos básicos del medio ambiente y la energía de las funciones de TI. Hay un alto riesgo de caídas debido a los eventos planificados; sin embargo, en las instalaciones de la clase F1, el mantenimiento se puede realizar durante las horas no regulares y el impacto del tiempo de inactividades relativamente bajo.	**Redundancia de componentes:** 0 **Sistema de redundancia:** 0 **Control de calidad:** Estándar **Supervivencia:** 0
Clase F2 Objetivo Disponibilidad < 99.9%	Proporcionar un nivel de fiabilidad superior a la definida en la clase F1para reducir el riesgo del tiempo de inactividad debido a la falta de componentes. En las instalaciones de claseF2, hay un riesgo moderado de tiempo de inactividad debido a los eventos planificados y no planificados. Las actividades de mantenimiento general, se puede realizar durante las horas programadas.	**Redundancia de componentes:** Sí para los componentes críticos **Sistema de redundancia:** 0 **Control de calidad:** Premium **Supervivencia:** Moderado

Clase F3 Objetivo Disponibilidad < 99.99%	Proveer mayor confiabilidad y facilidad de mantenimiento para reducir el riesgo de inactividad debido a los desastres naturales, desastres humanos impulsados, mantenimiento planeado, y las actividades de reparación. Para las actividades de mantenimiento y reparación general, será necesario llevarlas a cabo durante el tiempo de producción total sin posibilidad de operación.	**Redundancia de componentes:** Sí para la crítica/no crítica componentes **Redundancia del sistema:** Probable **Control de calidad:** Premium **Supervivencia:** Significativo
Clase F4 Objetivo Disponibilidad < 99.999%	Eliminar el tiempo de inactividad mediante la aplicación de las tácticas para proporcionar una operación continua, independiente de las actividades. Todos los puntos reconocibles que pueden fallar en la utilidad a los puntos de conexión a las cargas críticas son eliminados. Los sistemas son normalmente automatizados para reducir las posibilidades de error humano y cuentan con personal 24/7. Riguroso entrenamiento se proporciona al personal para atender cualquier contingencia. La compartimentación y tolerancia a fallos son los requisitos principales en una instalación de clase F4.	**Redundancia de componentes:** Sí, en críticos/no críticos componentes **Sistema de redundancia:** Si incluye redundancia de componentes **Control de calidad:** Premium **Supervivencia:** El nivel más alto

FUENTE: BICSI-002

- **Telecomunicaciones**

  - Proveedores de acceso y de planta externa:
    - Seguridad de las vías subterráneas de telecomunicaciones de entrada.
    - Rutas adyacencias con otros sistemas.
    - Instalaciones de entrada.
    - Vías subterráneas.

  - Telecomunicaciones, gabinetes informáticos y soportes
    - Gabinetes y configuraciones de rack.

- **Vías de Cableado**

    - Los caminos tendrán las dimensiones necesarias para la plena ocupación del Data Center.
    - Profundidad máxima del cableado en las vías (tabla 2.8).

Tabla 2.8 Profundidad Máxima del Cableado

Distancia entre apoyos	**Máxima altura de la pila**
0mm(0 pulgadas)	150 mm(6,0pulgadas)
100mm (4 pulgadas)	140 mm(5,5 pulgadas)
150mm (6 pulgadas)	137 m(5,4pulgadas)
250mm(10 pulgadas)	128 mm(5,0pulgadas)
500 mm(20 pulgadas)	111 mm(4,4pulgadas)
750mm (30 pulgadas)	98 mm (4 pulgadas)
1000 mm(40 pulgadas)	88 mm(3,5pulgadas)
1500 mm(60 pulgadas)	73 mm (3 pulgadas)

FUENTE: BICSI-002

a) Cableado

El cableado horizontal debe constar de uno o más de los siguientes tipos de medios y ventajas de ensamblado como se muestra en la tabla 2.9.

- Par trenzado con 4 pares de 100 ohmios Clase 6 Categoría E mínimo.
- Fibra óptica OM3, multimodo de 50/125 micras optimizada para láser, (Fibra óptica OM4, multimodo de 50/125 micras optimizada para láser: Para estas se recomienda las longitudes del cableado de fibra superior a 100m.
- Fibra óptica OS1, OS2, monomodo.
- Cable coaxial tipo 734-735 de 75 ohmios.

Tabla 2.9 Ventajas y desventajas de los ensamblajes de cableado

Característica/Beneficio	Ventaja	Desventaja
Calidad controlada de la terminaciones de fábrica	SI	
Reducir potencialmente el trabajo de instalación	SI	
Menos cables mejoran la gestión de cables	SI	
Menor dependencia en el instalador/habilidades técnicas/experiencia	SI	
Requiere un alto grado de precisión en el pedido de longitud de cable		SI
Si el ensamblado del cableado está dañado, varios cables se afectan dentro del cableado.		SI

FUENTE: BICSI-002

Cableado Backbone estará compuesto por una o más de los siguientes:

- Par trenzado Categoría 3 Clase C de 100ohm balanceado, como mínimo, (Categoría 6/Clase E o superior recomendado).
- Fibra óptica OM3, multimodo de 50/125 micras optimizada para láser, (Fibra óptica OM4, multimodo de 50/125 micras optimizada para láser.

Para estas se recomienda las longitudes del cableado de fibra superior a 100m.

- Fibra óptica OS1, OS2, monomodo.
- Cable coaxial de 75 ohmios.

Cableado centralizado de par trenzado:

- Todo el cableado centralizado de par trenzado tendrá que ser localizado en el mismo edificio y con un determinado radio de curvatura como se muestra en tabla 2.10.

Tabla 2.10 Radio de curvatura de cableado equilibrado

Cableado/ Tipos de cable	**Mínimo requerido en el interior/un radio de curvaturas en carga**	**Mínimo requerido en el interior/un radio de curvatura bajo carga**	**Recomendaciones de carga máxima de tracción bajo carga**
4-pares, de par trenzado balanceado parche /cable de equipo	Cable de diámetro interior de un tiempo	Cable de diámetro interior de un tiempo	Seguir especificaciones del fabricante
4 pares, cables de par trenzado equilibrado	Cable de diámetro interior de 4 tiempos	Cable de diámetro interior de 4 tiempos	25lb
Multipares , cables de par trenzado equilibrado	Seguir especificaciones del fabricante	Seguir especificaciones del fabricante	Seguir especificaciones del fabricante

FUENTE: BICSI-002

La norma recomienda no sobrepasar la tensión al instalar un cable como se muestra en la tabla 2.11.

Tabla 2.11 Guía de la tensión de tracción al instalar cable

Tipo de cable y detalles de instalación	Carga de tracción máxima durante la instalación	Mínimo de radios de curvatura durante la instalación	Mínimo del radio de curvatura después de la instalación
Planta interior horizontal cable con 2 y 4 fibras	220 N(50lb)	50 mm	25 mm
Planta interior cable con más de 4 fibras	Especificaciones del fabricante	20 veces del diámetro exterior del cable	10 veces del diámetro exterior del cable
Cable interior/exterior con hasta 12 fibras	300lb	20 veces del diámetro exterior del cable	10 veces del diámetro exterior del cable
Cable interior/exterior con más de 12 fibras	600lb	20 veces del diámetro exterior del cable	10 veces del diámetro exterior del cable
Cable OSP	600lb	20 veces del diámetro exterior del cable	10 veces del diámetro exterior del cable
Cable de acometida instalado por tracción	300lb	20 veces del diámetro exterior del cable	10 veces del diámetro exterior del cable
Cable de acometida enterrado, zanjas o se ha fundido en el conducto	100lb	20 veces del diámetro exterior del cable	10 veces del diámetro exterior del cable

FUENTE: BICSI-002

2.4.4 Norma ISO/IEC 24764

Tecnología de la Información – Cableado Genérico para predios de Data Center

Especifica el cableado genérico que soporta una amplia gama de servicios de comunicaciones para un Data Center. Cubre cableado, balanceado y el cableado de fibra óptica.

El cableado genérico se basa en las referencias y los requisitos de la norma ISO/ IEC 11801, donde la distancia máxima de los servicios de comunicaciones tiene que ser de 2 000m.

El objetivo de la norma es proporcionar un sistema de cableado genérico que puede soportar una amplia gama de LAN existentes y emergentes. Las aplicaciones SAN y WAN, pueden escalar y acomodar el crecimiento futuro a través del curso de vida prevista del Data Center y ser suficientemente flexible como para hacer modificaciones fáciles y eficientes.

La esperanza de vida de un sistema de cableado que cumpla los requisitos definidos, no debe exceder los 10 años.

2.4.4.1 Terminología del Estándar:

El acceso a la red del sistema de cableado se extiende desde la interfaz de red externa (ENI), donde servicios externos están conectados al Distribuidor principal (MD). La distribución principal del sistema de cableado ejecuta la Zona Distribuidor (ZD). Finalmente, la Zona de distribución del sistema de cableado se extiende desde el distribuidor de la zona (ZD) a la salida del equipo (OE), con la opción de utilizar un punto de distribución local (PLD) para mayor flexibilidad; sin embargo, La norma recomienda que cuando un PLD se utiliza, la longitud de la ZD para el PLD, debería ser al menos 15 m para reducir los efectos de pérdida y vuelta entre los conectores de la proximidad.

2.4.4.2 Diseño de la conexión de cables:

Al diseñar una infraestructura de cableado, el costo es la característica determinante del canal seleccionado; la flexibilidad y el rendimiento son considerados a continuación en la tabla 2.13:

Tabla 2.12 Diseño de Conexión de Cables fuente ISO 24764

Modelo	Costo	Flexibilidad	Rendimiento
Conector	Bajo	Bajo	Alto
Conector CP	Medio	Medio	Medio
Conector CC	Medio	Medio	Medio
Conector	Alto	Alto	Bajo

FUENTE: Norma ISO/IEC 24764

2.4.5 Norma ecuatoriana de construcción (NEC 10)

Las cargas muertas o permanentes en la estructura de la construcción, son muros, tabiques, recubrimientos sanitarios, estructuras eléctricas, equipos y maquinas.

Esta norma recomienda que para un centro de cómputo el piso debe soportar 4.8 KN/m2 (kilo newton por metro cuadrado) y para su construcción, utilizar hormigón compuesto con cemento hidráulico; materiales áridos y agua potable sin ningún tipo de contaminación.

Los tableros de energía deben proteger y administrar toda la instalación eléctrica, ya que proveen un gran nivel de seguridad y confiabilidad en la protección del personal, instalaciones y equipos electrónicos. Estos deberán ser instalados en un lugar de fácil acceso y seguridad; por una empresa calificada, la cual debe dejar su firma o nombre en el tablero, especificación del voltaje, la corriente, diagrama y el número de fases.

La altura máxima de un tablero será de dos metros desde el piso construido; además, deberá ser conectado a tierra; y, todos los cables deberán ser puestos en tuberías no metálicas.

Para prevenir cortocircuitos la norma recomienda no tener cables suelos sino aislados. Como voltaje de servicio la norma establece 12V y 24V. La calidad de energía depende mucho de la puesta a tierra y recomienda el uso de supresores transientes (picos de energía). La norma dice que la puesta a tierra debe soportar la tensión máxima para que no sea letal.

La norma ecuatoriana sigue los estándares que propone la norma TIA-942 respecto al cableado de telecomunicaciones. Ver Capitulo 2.4.1.1

Esta norma menciona que no es recomendable utilizar los pisos falsos para ventilación del Data Center, ya que se debe considerar la carga estática.

Cuando se tienen equipos sobre el piso, el cableado debajo del piso debe tener como mínimo 20mm de separación y de la losa hacia el piso falso y debe ser de 300mm.

Elementos para el sistema a puesta a tierra:

En la tabla 2.15 se muestran cada uno de los elementos y sus materiales para la construcción del sistema de puesta a tierra.

Tabla 2.13 Elementos puesta a tierra fuente NEC-10

Electrodo	Materiales	Diámetro mm	Área mm2	Espesor mm	Recubrimiento µm
Varilla	Cobre	12,7			
	Acero Inoxidable	10			
	Acero Galvanizado	16			70
	Acero recubierto cobre	14			100

Tubo	Cobre	20		2	
	Acero Inoxidable	25		2	
	Acero Galvanizado	25		2	55
Fleje	Cobre		50	2	
	Acero Inoxidable		90	3	
	Cobre Cincado		50	2	40
Cable	Cobre	1,8 cada hilo	25		
	Cobre estañado	1,8 cada hilo	25		
Placa	Cobre		20000	1,5	
	Acero Inoxidable		20000	6	

Fuente: NEC-10

2.5 Metodología COBIT (Infraestructura)

Es una metodología utilizada para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstos implican. Es manejada para planear, implementar, controlar y evaluar varios procesos realizados por una organización y directivas de auditoría casi como medidas de rendimiento y resultados, incluyendo objetivos de control.

COBIT ayuda a reducir las fallas existentes entre los objetivos que tiene un negocio versus los beneficios, riesgos, necesidades de control y aspectos técnicos propios de una entidad.

2.5.1 Recurso de TI (Infraestructura)

Se refiere a las instalaciones y la tecnología que permite el procesamiento de las aplicaciones de la organización. Se entiende por tecnología lo siguiente: redes, hardware y sistemas operativos.

2.5.2 Dominios de COBIT a utilizar:

- Planear y Organizar (PO): Provee orientación para la entrega de soluciones y servicios.

- Adquirir e Implementar (AI): Aquí se obtienen las soluciones para que luego sean convertidas en servicios.

- Entregar y dar soporte (DS): Toma las soluciones, convirtiéndolas en ideas y procesos utilizables para los usuarios finales.

- Monitorear y evaluar (ME): Para evaluar los servicios ofrecidos por terceros hacia la organización.

Como una idea muy generalizada de la importancia y la magnitud de COBIT dentro de la tecnología de la información se tendría que decir que los recursos son manejados por procesos para lograr metas con las cueles se cumpla a cabalidad con los requerimientos del negocio. Está idea básica está ilustrada en el cubo de COBIT. En la ilustración 2.9 se muestra el universo COBIT.

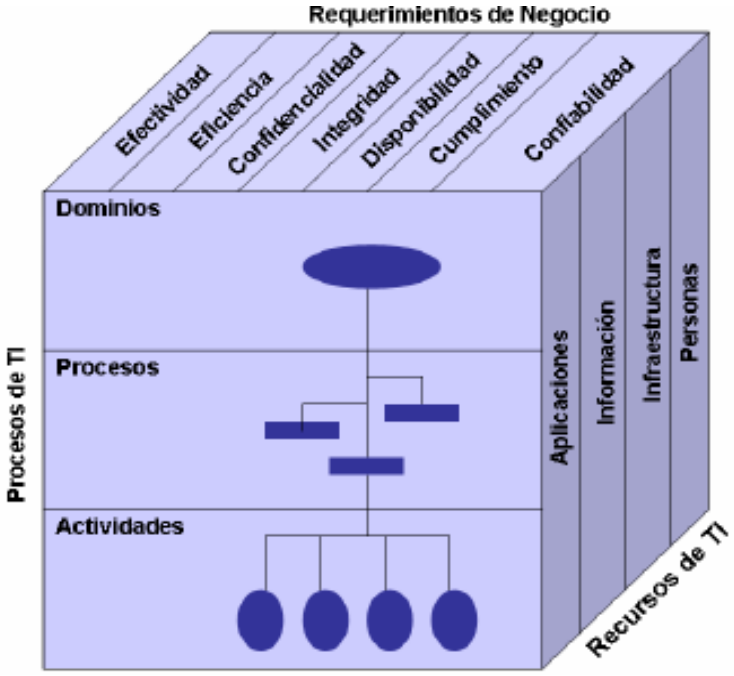


Ilustración 2.9 Cubo COBIT

FUENTE: Cobit 4.1

Para evaluar cada uno de los objetivos de control COBIT 4.1 se ofrece una valoración cuantitativa, mediante modelos de madurez. (Ver Anexo 1). Es recomendable utilizar la misma calificación para los procesos propuestos.

2.6 Medio Ambiente Data Center

Las condiciones ambientales dentro del Data Center son vitales para el buen funcionamiento y para maximizar la confiabilidad de su actividad.

Temperatura:

El excesivo calor en los equipos electrónicos reduce significativamente la vida útil de sus componentes; el excesivo frio en los equipos produce errores en su funcionamiento. La temperatura adecuada y recomendada es entre 21 y 23 grados centígrados.

La temperatura se debe medir en puntos clave del Data Center como: servidores, router´s, switch´s y bastidores (racks), esta medición se debe hacer a 5cm, al frente de los equipos donde ingresa aire frío y sale aire caliente.

Es recomendable también que no se produzcan cambios de temperatura bruscos de más de 5° centígrados y humedad de + - 10% en el transcurso de una hora.

Humedad:

Se debe tomar en cuenta que el aire caliente que recorre nuestro Data Center puede contener más humedad que el aire frio; la alta humedad produce fallos eléctricos en los equipos y con el transcurrir del tiempo, puede aparecer corrosión.

La humedad recomendada en el Data Center es de entre 45 % y 60% de humedad; se recomienda tener detectores de humedad, y evitar pisos mojados y goteras.

Para tener un buen ambiente de funcionamiento del Data Center se recomienda un sistema de calefacción, ventilación y aire acondicionado porque la mayoría de equipos extraen aire frio hacía en frente y escapa aire caliente por la parte posterior; en cuyo caso, el flujo de aire debe ser el adecuado para que no entre aire caliente a otro equipo que esté a lado o al frente de otro. El flujo de aire debe ser constante.

El mal control y despreocupación por las condiciones en el Data Center puede acortar la vida útil del equipo; el sobrecalentamiento puede provocar fallas intermitentes, y en casos extremos, que el equipo falle catastróficamente. El costo en tiempo, dinero y productividad de las empresas puede ser considerable.

2.7 Seguridad.

2.7.1 Seguridad del Data Center

Se comenzará con una clasificación de las personas autorizadas para el ingreso a un Data Center por ejemplo:

- Jefe del Área de TI.
- Encargado del mantenimiento de los servidores.
- Personal calificado del proveedor de Servicios.

2.7.1.1 Métodos del grado de Confiabilidad.

Tarjetas Magnéticas: Ofrecen una seguridad de nivel bajo; solo la persona con la tarjeta podrá entrar.

Lecturas biométricas: Ofrecen un nivel de seguridad medio, es mucho más complicado que un ladrón pueda falsificar el PIN o las huellas digitales del encargado. Este método puede guardar los datos de acceso, como la identidad de la persona y el horario de entrada. Otra posibilidad sería que permitan accesar al dispositivo por medio de la red, lo que ayudaría al Jefe de TI a tener un reporte diario de las personas que ingresan al Data Center y por cuanto tiempo lo hicieron.

Existen dos tipos de fallas en este método:

Falso rechazo: Sucede cuando no se reconoce a un usuario legítimo.

Falsa aceptación: Sucede cuando se reconoce a un usuario por otro o por aceptar a un impostor como un usuario legítimo.

Cerraduras de Teclado y de Combinación: Fácil de utilizar pero con seguridad limitada ya que toda contraseña puede a la larga adivinarse o divulgarse. Consiste en un teclado similar al de un teléfono celular y cada usuario tiene su PIN para ingresar. La seguridad puede aumentar al momento de cambiar periódicamente las combinaciones para cada usuario.

CCTV: Se utilizan cámaras de video ocultas o visibles, que son utilizadas para el monitoreo interno y revisión posterior de algún accidente. Con este método se pueden grabar distintos tipos de imágenes: fijas, giratorias o controladas de forma remota. Existe una nueva tecnología que mediante programas de Software, se observarían los cambios en el movimiento de la imagen de la pantalla.

Guardias de Seguridad: Es muy necesario en la actualidad a pesar de todos los avances tecnológicos, contar con un cuerpo de seguridad para que complemente las seguridades tecnológicas.

Sensores y Alarmas: Este método recomienda utilizar algunos tipos de sensores como son: sensores de rayos laser, de pisadas, táctiles, de vibración.

2.7.1.2 Factores de Seguridad que se debe tomar en cuenta.

- Utilizar puertas de acero macizas para que no se puedan extraer las bisagras desde el exterior.
- Utilizar los sensores empotrados en las paredes para que detecten cualquier alteración.
- La sala del Data Center no debe colindar con ninguna pared exterior.
- Evitar crear espacios donde se puedan esconder personas u objetos.

2.8 Software para la monitorización de los elementos del Data Center

Para verificar el rendimiento de los equipos presentes en el Data Center se recomienda utilizar herramientas software de monitoreo, los cuales ayudarán a determinar el uso de recursos, el estado de las aplicaciones o servicios; ver el estado actual del hardware e incluso se podrán solucionar problemas actuales.

Las ventajas de utilizar herramientas de monitoreo son:

- Realizar un inventario de hardware y software utilizado en los equipos.
- Monitorear los servicios que estén funcionando correctamente en los servidores.
- Alertar sobre problemas actuales.
- Mostrar gráficas, reportes de los servicios o del rendimiento del servidor en ese momento.

Actualmente existen en el mercado informático varias herramientas software. Para monitorear los servicios del Data Center de la ESPE, se encontró algunas muy útiles y son las siguientes:

- IPHost Network Monitor
- RedEyes
- NetCrunch
- LOGINventory
- PTRG

CAPÍTULO 3

3 EVALUACIÓN

3.1 Situación actual del Data Center de la ESPE

¿Qué es la UTIC?

La UTIC administra los recursos tecnológicos requeridos por la Institución, maneja la información y mantiene una adecuada comunicación, para lo cual ejecuta los procesos de gestión estratégica de la tecnología informática; de soporte técnico, de administración de redes y comunicaciones; de desarrollo, implantación y mantenimiento de aplicativos; y, de administración de software (sgc.espe.edu.ec).

Objetivo de la UTIC

Asegurar la disponibilidad, actualización tecnológica, innovación y operación de los recursos y servicios TIC's, para alcanzar un alto nivel de Tecnología y estándares de calidad acorde con las exigencias Institucionales (sgc.espe.edu.ec).

Misión de la UTIC

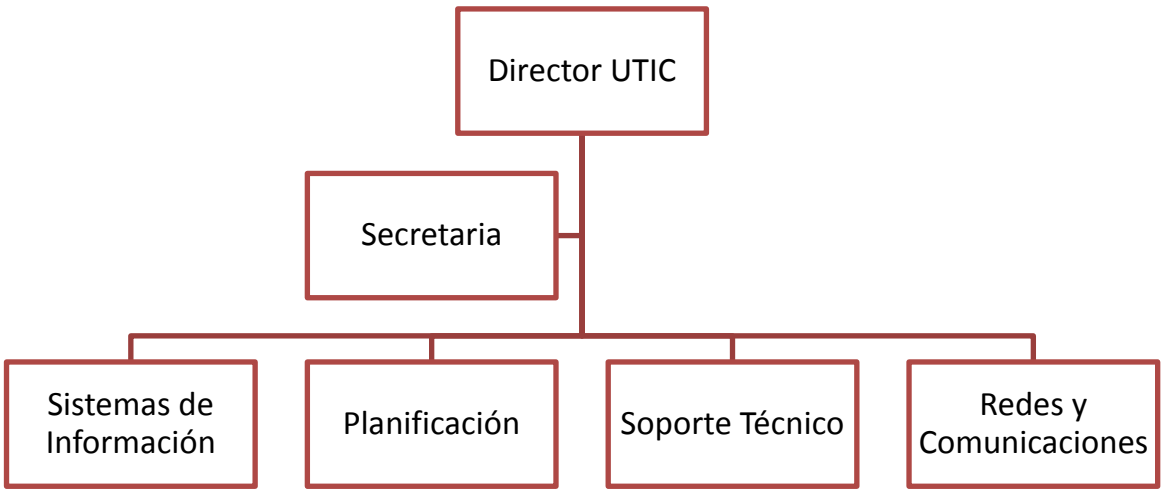
Administrar y proveer de forma eficiente y segura los recursos y servicios de TIC´s, de acuerdo a las necesidades institucionales y tendencias globales, cumpliendo normas y estándares internacionales (fuente sgc.espe.edu.ec).

Visión UTIC

Ser reconocida como una unidad Estratégica de la Institución, que contribuye al desarrollo innovación y transferencia de TIC`s, cumpliendo normas y estándares internacionales, con responsabilidad social y de medio ambiente (sgc.espe.edu.ec).

3.2 Organigrama Administrativo UTIC

El organigrama administrativo de la UTIC es el siguiente:



Fuente: Redes y Comunicaciones UTIC

3.3 Inventario de Hardware y Software del Data Center

3.3.1 Hardware

Servidores:

- **EXCHANGE ADMINISTRATIVOS:**HP PROLIANT ML 570 G4
- **ACTIVE DIRECTORY PRINCIPAL ADMINISTRATIVOS**:
- DELL POWEREDGE 2900
- **Astaro:** DELL POWEREDGE 2900
- **AD PRINCIPAL ALUMNOS:**HP PROLIANT ML 350
- **SERVIDOR NETBACKUP:**DELL POWEREDGE 1950
- **ISA SERVER:**HP PROLIANT ML 350
- **BASE DE DATOS ORACLE DEL PORTAL WEB:**HP PROLIANT ML 350
- **ESX CONSOLE:**CLON
- **Virtualizados:** HP PROLIANT 380 G5
- **Virtualizados:** HP PROLIANT 380 G5
- **Virtualizados:** HP PROLIANT 380 G5
- **BDD - ESPE Digital; Portal Luminis:** SPARC M5000 ENTERPRISE

- **ERP - ESPE Digital; Redundancia BDD - ESPE Digital:** SPARC ENTERPRISE M4000
- **SISTEMA FINANCIERO:** FUJITSU Primergi TX300 S4
- **ALMACENAMIENTO SERVIDORES PROYECTO ESPE DIGITAL UNIFICADO:** Fujitsu FiberCAT SX80
- **Autoservicios:** Prime Power 650
- **PORTAL WEB Institucional:** SUN FIRE V890
- **BDD - Sistema Académico Actual:** SUN FIRE V890
- **Educativa Principal:** DELL POWER EDGE R900
- **Educativo (Desarrollo Web):** DELL POWER EDGE R900
- **Citrix:** DELL POWER EDGE 6600
- **SMS TP:** DELL POWER EDGE 1850
- **ALMACENAMIENTO SERVIDORES PROYECTO ESPE DIGITAL UNIFICAO:** STORAGE SUN 6130
- **4 Switch de Fibra Almacenamiento:** 4Switxh Fibra SanboxQlogic
- **Luminis Test:** Sun Fire T2000
- **LIBRERÍA:** DELL POWER VAULT TL2000
- **Consola de Administración de Fujitsu:** CONSOLA ESPRIMO FUJITSU

Networking:

- **4 unidades de SwitchCore:** 2 de modelo 5500G-EI SFP; 2 de modelo 5500G-EI (24 puertos)
- **Enlace E1 CNT:** LOOP-O PDH (4 puertos)
- **Juniper:** SSG140 (10 puertos)
- **Ratio CFM-M-MUX:** sin modelo (2 puertos)
- **TIPPING POINT 200E:** 200E (2 segmentos)
- **SWITCH DE LA RED DMZ:** 3COM 5500 (24 puertos)
- **SWITCH PUBLICO:** 3COM 4500 (48 puertos)
- **CENTRAL TELEFONICA:** NBX V 5000 (2 NCP; 4 Chasis)
- **SWITCH LABORATORIOS Y ELECTRONICA:** 3COM4050 (no hay descripción de puertos)
- **SWITCH DE DISTRIBUCIÓN 1:** 3COM 4400 (48 puertos)
- **SWITCH DE DISTRIBUCIÓN 2:** 3COM 4400 (48 puertos)

- **SWITCH DE DISTRIBUCIÓN 3:** 3COM 4500 (50 puertos)
- **SWITCH DE DISTRIBUCIÓN 4:** 3COM 4500 (50 puertos)
- **SWITCH CEDIA:** CISCO CATALYST 3550 (24 puertos)
- **ROUTER INTERNET GLOBALCROSSING:** CISCO 2800 (2 ETH)
- **ROUTER WWW GLOBALCROSSING:** CISCO 1800 (4 ETH)
- **ROUTER LABORATORIOS GLOBALCROSSING:** CISCO 1800 (4 ETH)
- **ROUTER CNT RED WAN:** CISCO 1800 (4 ETH)
- **CHASIS CEDIA INTERNET 2:** CISCO 7604 (10 ETH)
- **ROUTER INTERNET 2 TELCONET:** CISCO 1800 (4 ETH)
- **ROUTER TELCONET:** CISCO 1800 (4 ETH)
- **SWITCH CATALYST:** CISCO 2960(8 puertos)
- **SWITCH VIDEO CONFERENCIA:** 5500G-EI(24 puertos)
- **TRANSCEIVER:** no existe descripción del modelo (13 puertos)
- **SWITCH CEDIA:** 5500 SI(52 puertos)

Racks:

- **MONITOREO DATA CENTER:** Swicth 3com 4500
- **Balanceador de Carga:** ROUTER CISCO 2900
- **BLUECOAT:** PACKET SHAPER 7500
- **2 Video BorderProxy:** 2Polycom VBP 5300
- **2 Switch SAN:** 2Brocade 300
- **Switch:** Fujitsu KVM S2-0801
- **Consola:** M4000 - M5000 Fujitsu Siemens
- **Portal:** HP PROLIANT ML350
- **Citrix Netscaler MPX**
- **Centralized Server:** Polycom RSS 4000
- **Plataforma para conferencias:** Polycom RMX 2000
- **Administración de aplicaciones convergentes:** Polycom CMA 4000
- **TIPPING POINT:** PowerEdge 1850
- **NETBACK UP:** PowerEdge 1950
- **Luminis:** SUNFIRE T2000
- **VMWARE esx1:** HP Proliant DL380 G5

- **VMWARE esx2:**HP Proliant DL380 G5
- **VMWARE esx3:**HP Proliant DL380 G5
- **Educativa:** Power Edge R900
- **www3:** Power Edge R900
- **Consola Fujitsu Siemens:** Fujitsu Prime Power 250; 6 Primergy RX 300 S4
- **Almacenamiento DCC:** Fujitsu Storage FibreCat SX80
- **ATS / PATH PANEL F.0. (BACK)**
- **PATCH PANEL CAT. 6 (BACK)**
- **Switch SAN Qlogic 4**
- **Switch SAN Qlogic 3**
- **Switch SAN Qlogic 2**
- **Switch SAN Qlogic 1**
- **Respaldo Cintas:** Dell Power Vault TL200
- **Storage Fujitsu Siemens:** Fiber Cat SX80
- **Storage:** StorEdge 6100
- **Servidor Financiero:** Fujitsu TX340 S4
- **Autoservicios:** Fujitsu Prime Power 650
- **Portal WEB:** SunFire 890
- **ERP:** Fujitsu Siemens Sparc Enterprise M4000
- **Servicios ESPE:** Sunfire v890
- **ESPE DIGITAL:** Fujitsu Siemens Sparc Enterprise M5000
- **Switch de Distribución 1:** Switch cisco Catalyst 6506
- **Switch de Distribución 2:** Switch cisco Catalyst 6506
- **Service Console IBM:** Storage IBM(IBM XT3512); IBM Blade Center
- **ACTIVE DIRECTORY SECUNDARIO:** Dell Power Edge 2650
- **ACTIVE DIRECTORY ALUMNOS:** HP ML 350
- **ACTIVE DIRECTORY PRINCIPAL:** DELL POWER EDGE 2900
- **ISA SERVER:** HP ML 350
- **ASTARO:** DELL POWER EDGE 2900

3.3.2 Software

Servidores:

- **EXCHANGE ADMINISTRATIVOS:** WIN 2003 Server Pack 2
- **ACTIVE DIRECTORY PRINCIPAL ADMINISTRATIVOS**: WIN 2008 Server Pack 2 32 bits
- **Astaro:** WIN 2008 Server Pack 2 32 bits
- **AD PRINCIPAL ALUMNOS:**WIN 2003 Server Pack 2
- **SERVIDOR NETBACKUP:** WIN 2003 Server Pack 2
- **ISA SERVER:** WIN 2003 Server Pack 2
- **BASE DE DATOS ORACLE DEL PORTAL WEB:**WIN 2003 Server Pack 2
- **ESX CONSOLE:** WIN 2003 Server Pack 2
- **Virtualizados:**WIN 2003 Server Pack 2
- **Virtualizados:**WIN 2003 Server Pack 2
- **Virtualizados:**WIN 2003 Server Pack 2
- **BDD - ESPE Digital; Portal Luminis:** SOLARIS 10
- **ERP - ESPE Digital; Redundancia BDD - ESPE Digital:** SOLARIS 10
- **SISTEMA FINANCIERO:** Windows Server 2003 Enterprise Edition Release 2
- **ALMACENAMIENTO SERVIDORES PROYECTO ESPE DIGITAL UNIFICAO:** no existe descripción de software
- **Autoservicios:** WIN 2003 Server Pack 2
- **PORTAL WEB Institucional:** SOLARIS 10
- **BDD - Sistema Académico Actual:** SOLARIS 10
- **Educativa Principal:** GENTOO
- **Educativo (Desarrollo Web):** RED HAT
- **Citrix:** WIN 2003 Server Pack 2
- **SMS TP:** RED HAT

3.4 Aplicaciones en red de la ESPE

a. Sistema Académico:

Se encuentra en un servidor SOLARIS 10. La versión de esta aplicación actualmente está en la versión 7.0. El Área Sistemas de Información es responsable de su funcionamiento y correcta operación.

b. Sistema Financiero OLYMPO:

Esta aplicación fue desarrollada con la herramienta de desarrollo Visual Basic, su versión 6.0; se encuentra en un servidor Windows Server 2003.
El Área Sistemas de Información es responsable de su funcionamiento y correcta operación.

c. Sistema de Recursos Humanos:

Es la aplicación que tiene menos versiones o mejor dicho actualizaciones, ya que está en la versión 1.0, fue desarrollada en PowerBuilder, se encuentra sobre un servidor Windows Server 2003.

Las Áreas Sistemas de Información y Talento Humano son responsables de su funcionamiento y correcta operación.

d. Portal WEB:

Es la aplicación que se usa como fachada virtual de la ESPE, dentro de este aplicativo se puede visualizar: Servicios Intranet, información acerca de todas las carreras que ofrece la universidad, links para acceder a la MED y noticias de la comunidad politécnica.

El Área Sistemas de Información es responsable de su funcionamiento y correcta operación. Para acotar fue desarrollado en JAVA.

e. Sistema de Educación Virtual:

Esta aplicación es de utilidad para los estudiantes de Educación a Distancia, en esta plataforma pueden interactuar con los compañeros y tutor, participar en foros, subir fotos y actualizar datos personales; subir guías y documentos; existe la posibilidad de rendir pruebas online.

Está plataforma fue desarrollada por EDUCATIVA, esta sobre un servidor SOLARIS. El Área Sistemas de Información es responsable de su funcionamiento y correcta operación.

f. Sistema ESPE MEDIC:

Aplicación desarrollada en PowerBuilder, actualmente se encuentra en la versión 7.0, está sobre un servidor SOLARIS.

El Área Sistemas de Información es responsable de su funcionamiento y correcta operación.

g. Sistema de Pedidos:

La aplicación fue desarrollada en PowerBuilder, la última actualización de su versión es la 7.0, se encuentra sobre un servidor SOLARIS.

El Área Sistemas de Información es responsable de su funcionamiento y correcta operación.

h. Sistema BANNER ESPE:

BANNER, es la aplicación que por el momento centraliza varios de los procesos que la ESPE ha virtualizado, abarca varios servicios como: matriculación, calificaciones, mail, horarios, educación a distancia, asistencias, historia académica, manuales de uso; está compuesto de varios módulos para abastecer las necesidades de cada uno de los administrativos de la ESPE.

Es lógico decir que tiene varios niveles y claves de usuario según el cargo y necesidad de las personas que lo estén utilizando.
Es una aplicación indispensable para la ESPE, como: información adicional y base de datos ORACLE. La versión de la aplicación BANNER 8.0, está sobre un servidor Windows.

Gracias a su alta prioridad de funcionamiento, UTIC es responsable de su funcionamiento y su operación 24/7.

i. Sistema Telefónico:

Tiene por sistema operativo VxWorks, posee un solo módulo y tiene que estar siempre operativo para 400 usuarios.

j. Sistema de VideoConferencia:

La Video-Conferencia tiene un software propietario de Polycom, compuesto por tres módulos con los cuales se controlan los siete terminales que ofrece este servicio.

3.5 Diseño de la red LAN del Data Center

En la ilustración 3.1 se muestra el diseño de la red dentro del Data Center ESPE.

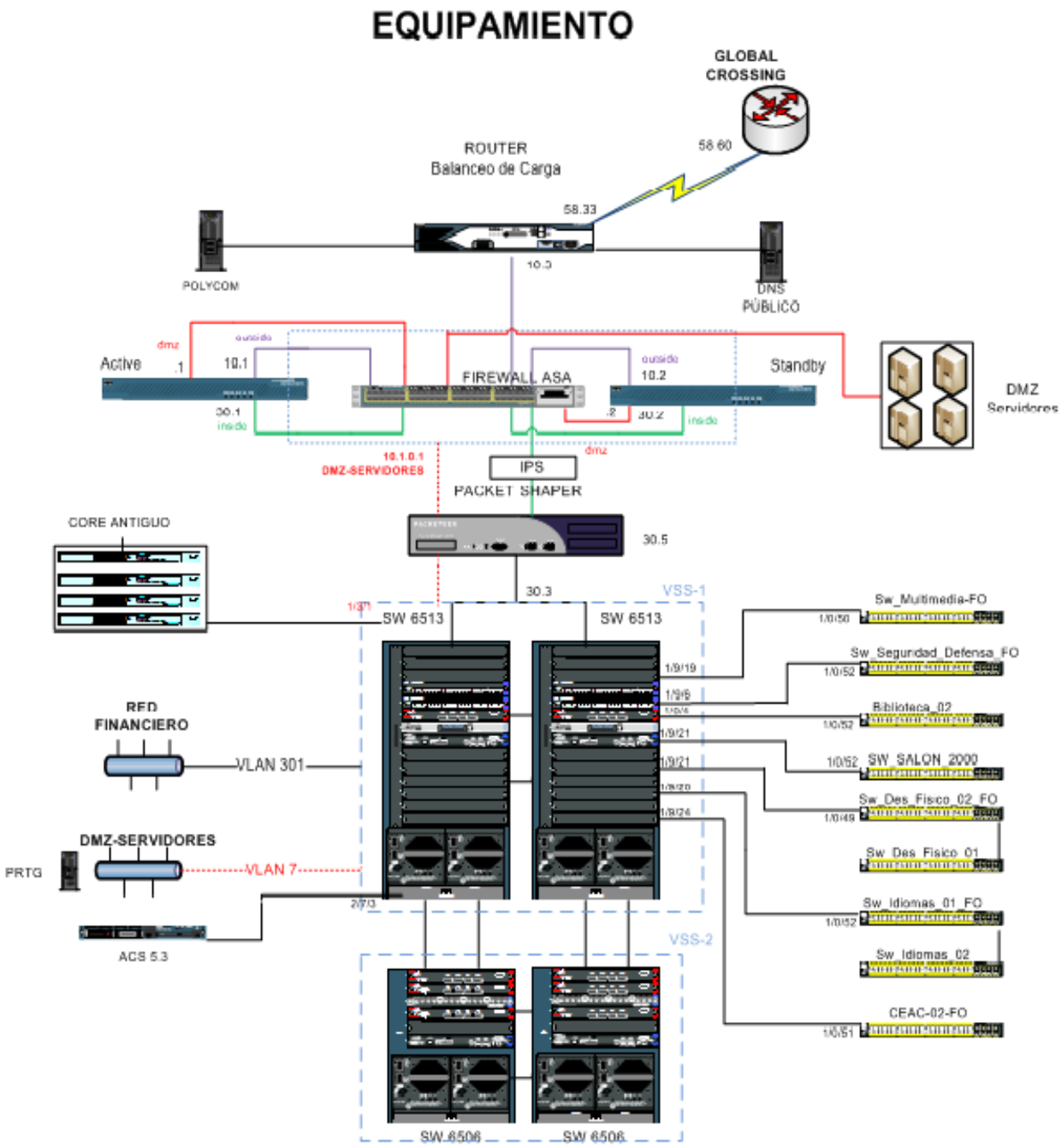


Ilustración 3.1 Diagrama Red Data Center ESPE

Fuente: Redes y Comunicaciones UTIC ESPE

3.6 Diagrama Unifilar Racks ESPE

En la ilustración 3.2 se muestra el diagrama unifilar de racks de la ESPE Sangolquí.

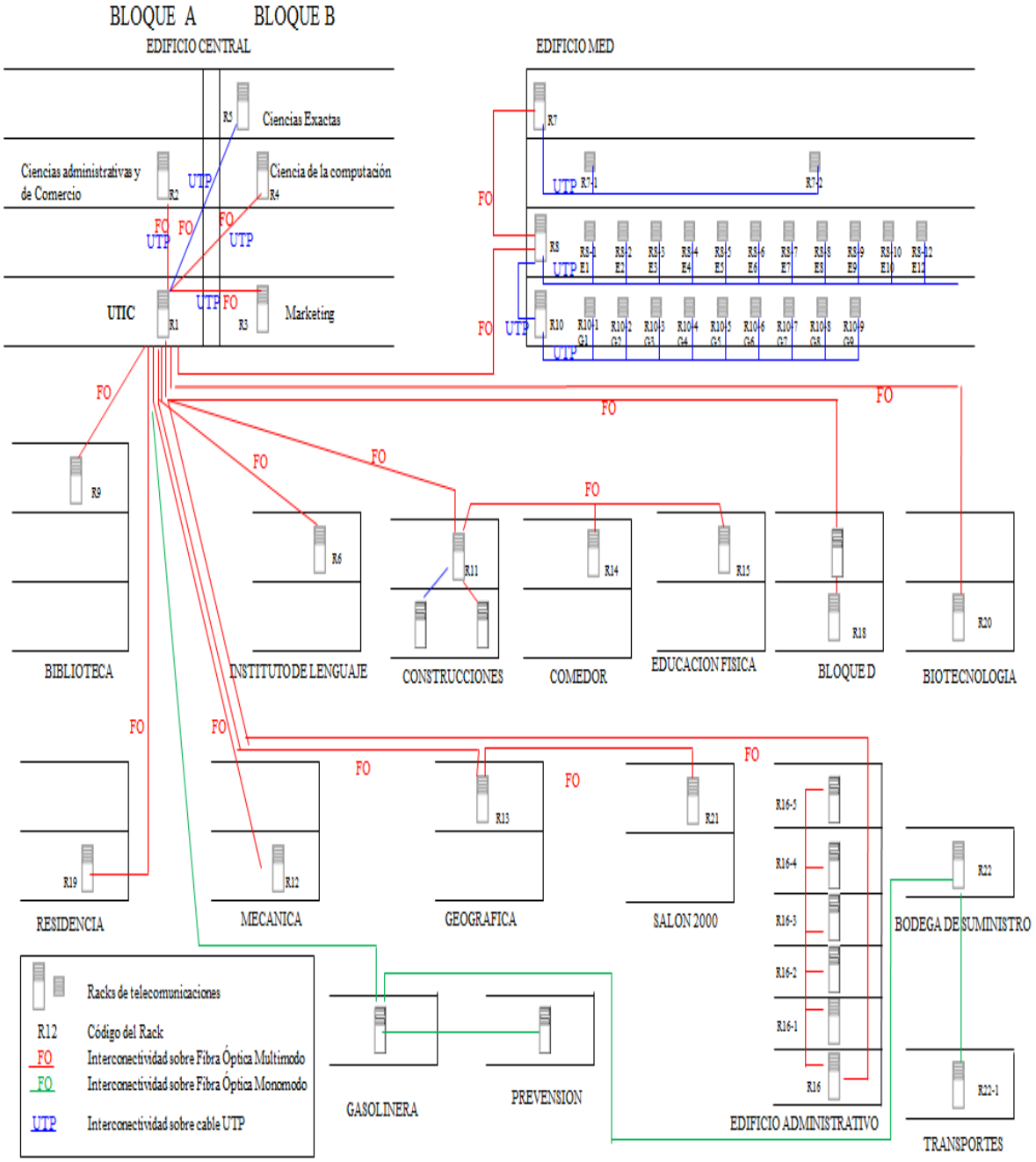


Ilustración 3.2 Diagrama Unifilar Racks ESPE

FUENTE: Redes y Comunicaciones UTIC ESPE

3.7 Gráfico de la distribución del Data Center

El diagrama de distribución interna del Data Center se muestra en la ilustración 3.3.

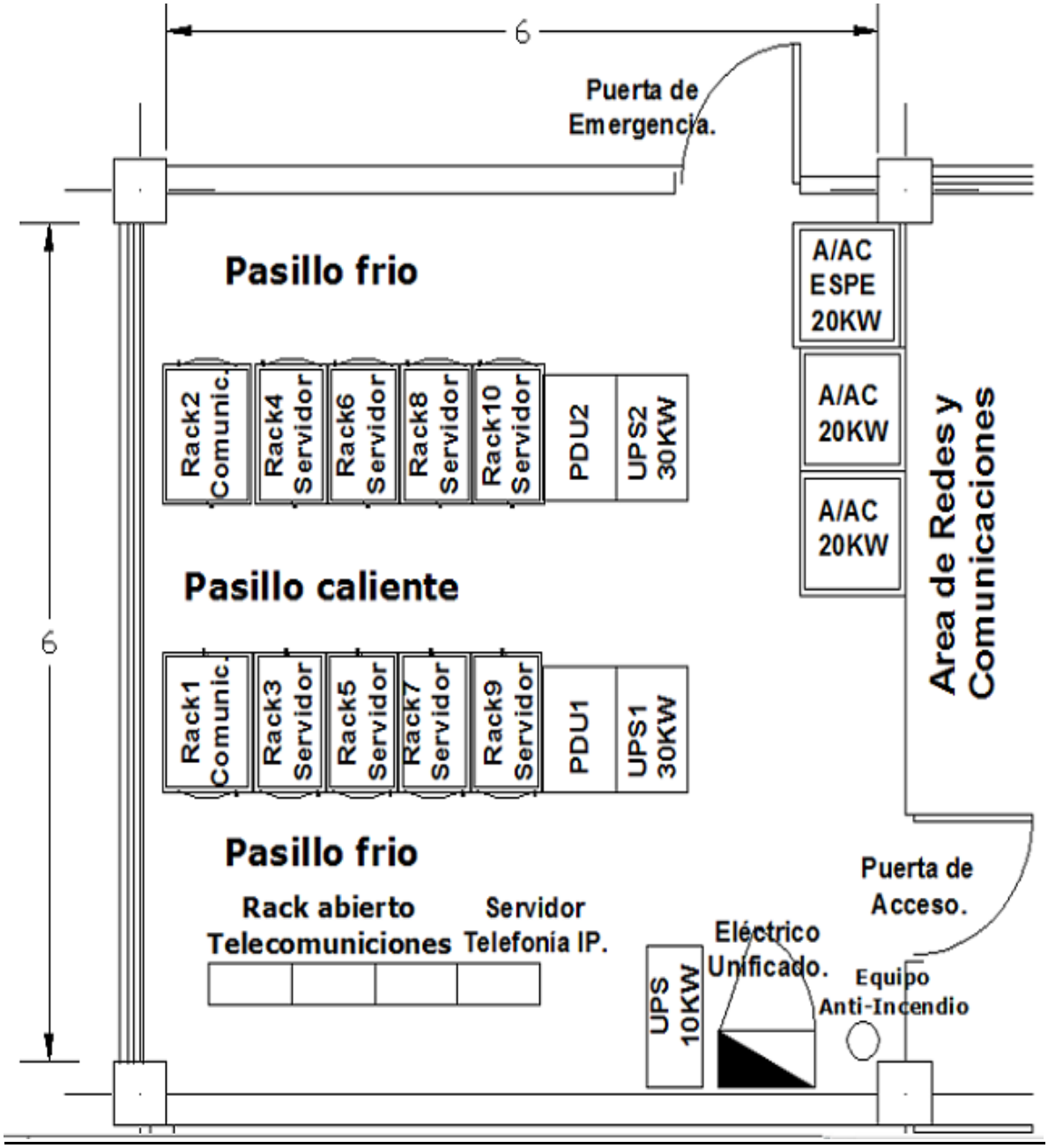


Ilustración 3.3 Distribución Interna Data Center ESPE

FUENTE: Data Center ESPE

3.8 Diagrama general de respaldo y distribución de Energía

El diagrama general de respaldo y distribución de energía para el Data Center ESPE se muestra en la ilustración 3.4.

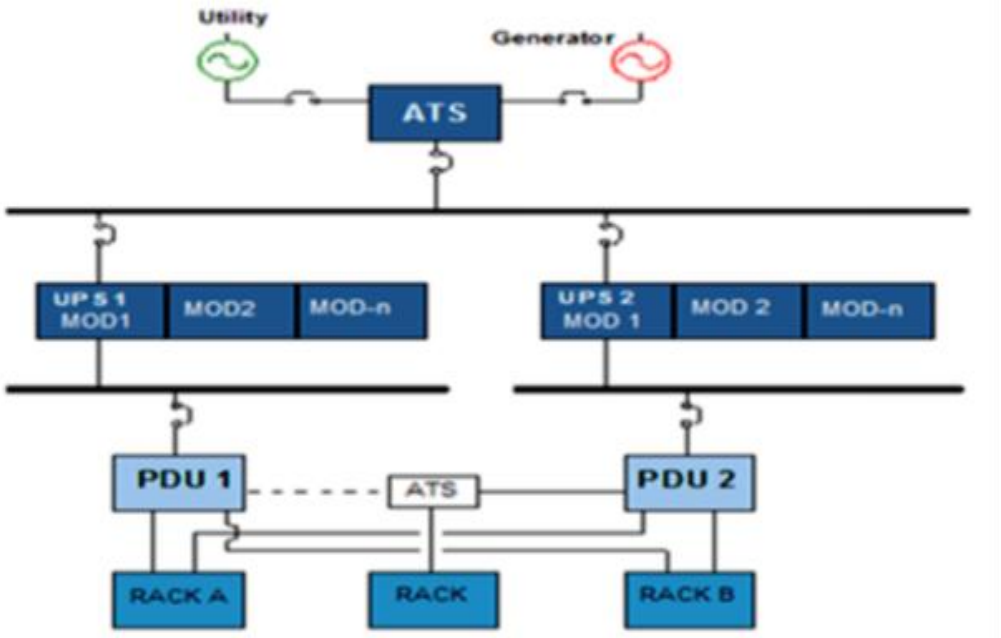


Ilustración 3.4 Respaldo y Distribución de Energía Data

Fuente: Redes y Comunicaciones UTIC ESPE

3.9 Detalle de Actividades

En la tabla 3.1 se describe las actividades a realizar dentro del Data Center.

Tabla 3.1 Detalle de Actividades dentro Data Center ESPE

Actividad	Responsables	Objetivo	Lugar	Duración	Observaciones
Revisión Acometidas	José Barba Giovanny Viteri	Revisar el número de acometidas que cuenta el tablero de distribución	Data Center ESPE	1 día	Ninguna
Revisión Tablero de Distribución	José Barba Giovanny Viteri	Verificar si el tablero es monofásico, polifásico o trifásico	Data Center ESPE	1 día	Tablero Trifásico

Verificar el funcionamiento UPS	José Barba Giovanny Viteri	Revisar todas las opciones en el panel de los UPS y verificar los valores	Data Center ESPE	1 día	2 UPS funcionales
Medir el Amperaje en el tablero de distribución	José Barba Giovanny Viteri	Utilizando la pinza amperimétrica medir en casa fase	Data Center ESPE	1 día	Ninguna
Observación iluminación	José Barba Giovanny Viteri	Utilizar el luxómetro y verificar si la iluminación es adecuada	Data Center ESPE	1 día	Ninguna
Medición puesta a tierra	José Barba Giovanny Viteri	Realizar la medición con el óhmetro	Campus ESPE	1 día	Ninguna
Verificar el funcionamientos de las cámaras IP	José Barba Giovanny Viteri	Utilizando el software preinstalado verificar el funcionamiento de las cámaras	Data Center ESPE	1 día	El monitoreo del Data Center debería ser 24/7
Verificar puertas de acceso	José Barba Giovanny Viteri	Verificar el funcionamiento del sistema biométrico	Data Center ESPE	1 hora	Cuenta con el acceso principal y salida de emergencia. No existe seguridad en la puerta de emergencia
Inspeccionar el sistema de incendios	José Barba Giovanny Viteri	Inspeccionar los detectores de humo y la locación de los mismos	Data Center ESPE	1 día	Ninguna
Verificar las señalizaciones	José Barba Giovanny Viteri	Observar la señalética en caso de emergencia	Data Center ESPE	1 día	Cuenta con 2 luces de emergencia y la señalización respectiva

Verificar los kvas del AACC	José Barba Giovanny Viteri	Utilizar el multímetro y medir los kvas del AACC	Data Center ESPE	1 día	Disponibilidad 2 AACC y 1 redundante
Medición de pisos fríos y calientes	José Barba Giovanny Viteri	Utilizar el fluxómetro y comparar las medidas con la norma TIA-942	Data Center ESPE	1 día	Ninguna
Verificación cableado estructurado	José Barba Giovanny Viteri	Observar el cableado estructurado ordenado	Data Center ESPE	1 día	Sin estándares de Cableado
Verificación de servidores	José Barba Giovanny Viteri	Utilizando herramienta software identificar cada servidor	Data Center ESPE	2 días	Ninguna
Realizar pruebas servidores	José Barba Giovanny Viteri	Utilizando varias herramientas software para realizar pruebas y presentar resultados de las mismas	Data Center ESPE	2 días	Ninguna

3.10 Análisis de las políticas y procedimientos en el Data Center de la ESPE.

COBIT en la parte de los recursos de TI, ofrece la posibilidad de evaluar la infraestructura de una organización; al estar regido por estándares y normas avaladas por el Instituto de Estándares y Tecnología (NIST), obtiene una gran credibilidad como metodología que servirá para realizar un análisis de las políticas y procedimientos del Data Center de la Escuela Politécnica del Ejército.

3.10.1 Análisis de Riesgos de la Gestión de la Infraestructura del Data Center de la ESPE

Se identifica todos los recursos hardware, software y aplicaciones que estén dentro del Data Center para tener una visión completa de toda la infraestructura con la que cuenta, identificando así, el alcance de la evaluación de riesgos.

3.10.1.1 Identificación de Recursos que deben ser protegidos

Software:

Sistema Operativo:

- Solaris SPARC 10
- Windows Server 2003 Enterprise Edition
- Red Hat Enterprise 5.0
- SW Core 3COM
- Cisco PIX
- Tipping Point
- ASTARO

Antivirus:

- Kaspersky

Base de Datos:

- SYBASE 12.5.1
- ORACLE 11.0

Aplicaciones:

- Sistema Académico
- Sistema Financiero OLYMPO
- Sistema de Recursos Humanos
- Portal WEB
- Sistema de Educación Virtual
- Sistema ESPE MEDIC
- Sistema de Pedidos
- Sistema BANNER ESPE

- Sistema Telefónico
- Sistema de VideoConferencia

Servicios:

- Red WAN (CNT)
- Internet (Global Crossing)
- FTP (ESPE)
- Correo Electrónico
- Telefonía (CNT-ESPE)
- Video Conferencia

3.10.1.2 Medio Operacional sobre Infraestructura.

Seguridad del ambiente físico.

El ingreso al Data Center es restringido solo para personal autorizado, en este caso los empleados de redes y comunicaciones y en ciertas ocasiones el director de UTIC pueden acceder libremente; tiene dos puertas de ingreso, por la principal se accede mediante tarjetas magnéticas y biométrico; la puerta secundaria es de emergencia.

Dentro del centro de datos la supervisión se realiza mediante cámaras IP complementadas por el software propietario.

Medioambiente del Data Center.

Los servidores, switch´s, racks, sistemas de aire acondicionado, UPS´s, PDU´s, ATM, iluminarias, extintores de incendio y toda clase de cables, se encuentran ubicados dentro del Data Center, el mismo que ha sido construido en la planta baja del edificio central de la ESPE. Estaría expuesto a algunas amenazas ambientales como la humedad o inundaciones.

3.10.2 Recolección de Información

La información obtenida fue posible gracias a la aplicación de técnicas previamente estudiadas y reconocidas. Se utilizaron las siguientes:

- Entrevista y encuesta (anexo 3) al Administrador de Redes y Comunicaciones.
- Revisión de Plan de Contingencia UTIC, procedimientos, inventarios de hardware y software.
- Visita y Observación al Data Center

3.10.2.1 Individualización de amenazas y vulnerabilidad.

Amenazas

Se tomaron en cuenta algunos conceptos presentes en el Plan de Contingencia de la UTIC para clasificar las amenazas y vulnerabilidad; también se pensó en otras que no han sido contempladas en dicho Plan.

- Amenazas naturales: Descritas en el Plan de Contingencia de la UTIC.
- Amenazas humanas y de origen técnico: Descritas en el Plan de Contingencia de la UTIC.
- Otras amenazas: falla ininterrumpida de energía eléctrica, falla temporal de los servidores.

Vulnerabilidad

- No existe un procedimiento para el respaldo de información, en el que se detallen los procedimientos a llevarse a cabo, en caso de que ocurra una contingencia.
- No existe un procedimiento para monitorear software malicioso sobre los servidores, aplicaciones o servicios.
- No existe la actualización del Plan de Contingencia.
- No existe un respaldo de información para la caída de servidores.

3.10.2.2 Definición del Impacto de las Amenazas

En concordancia con lo descrito en el Plan de Contingencia de la UTIC, se tomarán los mismos parámetros cuantitativos para analizar el índice de ocurrencia del impacto de las amenazas. Como se muestra en la tabla 3.2:

Tabla 3.2 Valoración Cuantitativa de las Amenazas

PROBABILIDAD		IMPACTO	
CALIFICACIÓN	NIVEL	CALIFICACIÓN	NIVEL
5	Alto	5	Terminal
3	Medio	3	Crítico
1	Bajo	1	Aceptable

Fuente: Plan de Contingencia UTIC

La ponderación para cada uno de los riesgos se describe en la tabla 3.3:

Tabla 3.3 Ponderación de los Riesgos

RIESGO	RANGO
Alto	25
Medio	9-15
Bajo	1-5

FUENTE: Plan de Contingencia UTIC

3.10.2.3 Matriz de Evaluación de Riesgos

Esta matriz contiene toda la información sobre el análisis detallado de cada uno de los recursos que se han considerado como los más vulnerables a las amenazas; también se incluye lo analizado en el Plan de contingencia de UTIC. Esta información se obtuvo a partir de la entrevista con el encargado de Red y Conectividad, y checklist, proponiendo un nivel de riesgo y recomendaciones de control. Como se muestra en la tabla 3.4.

Tabla 3.4 Matriz de Evaluación de Riesgos

Riesgo	Recurso	Amenaza	Impacto	Probabilidad	Tipo de Riesgo	Recomendación
Incendio		- Daño de los equipos del Data Center. - Falla de telefonía IP. - Pérdida permanente de información.	5	3	Medio(15)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
Erupción Volcánica		- Obstrucción de ventiladores por ceniza volcánica. - Pérdida permanente de información.	5	3	Medio(15)	Cumplir a cabalidad procedimiento de contingencia detallado en Plan de Contingencia UTIC.
Terremoto		- Destrucción irreparable de los equipos por colapso de edificio. - Destrucción del piso falso. - Falla de comunicaciones internas.	5	3	Medio(15)	Cumplir a cabalidad procedimientos de contingencia, detallado en Plan de Contingencia UTIC.
Falla del UPS		- Pérdida de respaldo energético ante los apagones. - Falla técnica de los servidores.	5	5	Alto(25)	Cumplir a cabalidad procedimiento de contingencia detallado en Plan de Contingencia UTIC.

Robo Físico de Equipos		- Pérdida permanente de información sin respaldo. - Interrupción de servicios de red y monitoreo de Data Center	3	3	Medio(9)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
Explosión		- Destrucción de equipos. - Daño infraestructural del Data Center.	5	3	Medio(15)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
Falla del aire acondicionado		- Sobrecalentamiento de los equipos del Data Center. - Pérdida de información por quema de hardware. - Posibilidad de incendios.	5	5	Alto(25)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
Ataques de virus		- Robo de información - Modificaciones de Archivos - Perdida de la estructura de la unidades del disco(formateo) - Ataques a sistemas de memoria y arranque.	3	3	Medio(9)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia. UTIC
Suspensión		- Imposibilidad de comunicación	3	3	Medio(9)	Cumplir a

Central Telefónica		interna dentro del Campus Universitario.				cabalidad procedimientos de contingencia detallado en el Plan de Contingencia UTIC.
Suspensión del Servicio de Red		- Falla de aplicativos software que se ejecutan en red. - No hay manera de monitorear los equipos del Data Center que estén en red. - No se garantiza la seguridad visual dentro del Data Center.	5	3	Medio(15)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
Daño físico o lógico de dispositivos de red		- No existe conexión con la red. - No se puede enviar paquetes por medio de la red.	3	3	Medio(9)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
Daño del cableado estructurado		- Caída de los servicios, aplicativos y telefonía IP.	3	3	Medio(9)	Cumplir a cabalidad procedimiento de contingencia detallado en el Plan de Contingencia UTIC
Daño físico de los		- Pérdida de información que no esté respaldada.	5	5	Alto(25)	Cumplir a cabalidad

componentes		- Falla de los aplicativos en red. - Suspensión de la red. - Mal uso de recursos.				procedimiento de contingencia detallado en el Plan de Contingencia UTIC.
	Sistema Académico (Aplicación en Red)	- Ingreso no autorizado al sistema con intención de revisar información privilegiada. - Cambio, eliminación, aumento de información sin autorización.	3	3	Medio(9)	Revisión periódica de los ingresos de los usuarios al aplicativo. Apelar a la responsabilidad que tiene cada uno de los usuarios al utilizar un perfil de usuario.
	Sistema Financiero OLYMPO(Aplicación en Red)	- Ingreso no autorizado al sistema con intención de revisar información privilegiada. - Cambio, eliminación, aumento de información sin autorización.	3	3	Medio(9)	Reforzar el compromiso de empresa en los empleados del Departamento de Finanzas.
	Sistema Recursos Humanos (Aplicación en Red)	- Ingreso no autorizado al sistema con intención de revisar información privilegiada. - Cambio, eliminación, aumento de información sin autorización.	3	3	Medio(9)	El informe de RRHH sobre la salida del personal de la ESPE, debe ser periódico.
	Portal Web(Aplicación	- Cambio, eliminación, aumento de información sin autorización.	3	1	Bajo(3)	Revisar diariamente la

	en Red)					información publicada en el Portal Web, ya que es la cara de presentación de la empresa.
	Sistema de Educación Virtual (Aplicación en Red)	- Ingreso no autorizado al sistema con intención de revisar información privilegiada. - Cambio, eliminación, aumento de información sin autorización.	1	3	Bajo(3)	Los profesores de cada materia deben revisar los contenidos para que ninguno de sus estudiantes sean perjudicados.
	Sistema ESPE MEDIC (Aplicación en Red)	- Ingreso no autorizado al sistema con intención de revisar información privilegiada. - Cambio, eliminación, aumento de información sin autorización.	3	3	Medio(3)	El reporte emitido por los empleados de MEDIC, debe ser revisado periódicamente preservando siempre la integridad de los datos.
	Sistema de Pedidos (Aplicación en Red)	- Cambio, eliminación, aumento de información sin autorización.	1	3	Bajo(3)	Definir la responsabilidad de cada uno de los usuarios sobre el uso de sus perfiles
	Sistema BANNER ESPE	- Ingreso no autorizado al sistema con intención de revisar información privilegiada.	3	5	Medio(15)	Revisar el ingreso al sistema Banner.

3.10.2.4 Alcance del Análisis de las Políticas y Procedimientos del Data Center

Para el análisis y evaluación de los procesos referentes a la infraestructura del Data Center, se aplicó la metodología COBIT.

Debido al reconocimiento nacional que tiene la Escuela Politécnica del Ejército, necesita ofrecer servicios de calidad a sus estudiantes; para ello, cada uno de sus departamentos debe asegurar que sean de calidad, por lo que deben estar en constante comunicación, dependiendo de la eficiencia de la red informática que ofrece el Data Center.

Aquí inicia el análisis en el cual se identificarán las debilidades y riesgos potencialmente graves, previo a dar recomendaciones sobre los actuales procedimientos y control de seguridad con el fin de mejorar la infraestructura del Data Center.

Objetivo del análisis

- Evaluar la actual gestión de la infraestructura del Data Center de la ESPE.

- Proponer recomendaciones sobre las mejoras en la gestión de la infraestructura, sí amerita.

3.10.2.5 Listado Descriptivo de los Procesos COBIT aplicables a la Gestión de Infraestructura Data Center

Después de un estudio exhaustivo de la metodología COBIT, se han seleccionado los procesos en los cuales se observó la actual situación de gestión de la infraestructura del Data Center y por supuesto los procesos aplicables a la naturaleza de la empresa y los objetivos de la empresa a alcanzar.

A continuación se presenta el listado de los objetivos de control por dominios que fueron escogidos para la ejecución del análisis, para complementar la tabla 3.5 muestra los recursos de TI afectados.

- PO4. Definir los Procesos, Organización y Relaciones de TI

- PO9. Evaluar y Administrar los Riesgos de TI

- AI3. Adquirir y Mantener la Infraestructura Tecnológica

- DS2. Administrar los servicios de Terceros

- DS4. Garantizar la continuidad del Servicio

- DS5. Garantizar la seguridad de los sistemas

- DS12. Administración del Ambiente Físico

- ME3. Garantizar el Cumplimiento con Requerimientos Externos

Tabla 3.5 Objetivos de Control y Recursos TI afectados

Dominio	Proceso	Requerimientos de Negocio							Recursos de TI			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Información	Infraestructura	Personas
Planificación y Organización	PO4. Definir los Procesos, Organización y Relaciones de TI	P	P									X
	PO9. Evaluar y Administrar los Riesgos de TI	S	S	P	P	P	S	S	X	X	X	X
Adquisición e Implementación	AI3. Adquirir y Mantener la Arquitectura Tecnológica	S	P		S	S					X	
Entrega de Servicios y Soporte	DS2. Administrar los servicios de Terceros	P	P	S	S	S	S	S	X	X	X	X
	DS4. Garantizar la continuidad del Servicio	P	S			P			X	X	X	X
	DS5. Garantizar la seguridad de los sistemas			P	P	S	S	S	X	X	X	X
	DS12. Administración del Ambiente Físico				P	P					X	
Monitorear y Evaluar	ME3. Garantizar el Cumplimiento con Requerimientos Externos						P	S	X	X	X	X

Fuente: Marco Referencial COBIT

P: Facilitador Primario

S: Facilitador Secundario

3.10.2.6 Estructura de los Dominios de Control

PO4. Definir los Procesos, Organización y Relaciones de TI

Para garantizar el soporte oportuno de todos los requerimientos como negocio y conocer que las responsabilidades de cada persona estén bien definidas para asegurar los componentes del Data Center.

Los objetivos de control a ser considerados son:

PO4.6 Establecimiento de Roles y responsabilidades
PO4.11 Segregación de Funciones

PO9. Evaluar y Administrar los Riesgos de TI

Se debe encontrar la manera de asegurar equipos y datos que en una calamidad se vuelvan críticos para el negocio; garantizando el logro de los objetivos del negocio, al procurar que todo salga bien respecto a la seguridad física y lógica del Data Center.

El objetivo de control a ser considerado es: PO9.3 Identificar eventos.

AI3. Administrar y Mantener Infraestructura Tecnológica

Para garantizar que exista un soporte tecnológico continuo en todas las aplicaciones del Data Center.

Los objetivos de control a ser considerados son:

AI3.2 Proteger y disponer del Recurso de Infraestructura.
AI3.3 Mantener la Infraestructura.

DS2. Administrar los servicios de Terceros

Para minimizar los riesgos del negocio, asociados con los proveedores de equipos y servicios para el Data Center.
El objetivo de control a ser considerado es:

DS2.3 Administrar riesgos del proveedor

DS4. Garantizar la continuidad del Servicio

Es la capacidad del Data Center para seguir brindando servicio con la ayuda de un plan de contingencias y de por medio, recuperar fallas y políticas de respaldo de información.

Los objetivos de control a ser considerados son:

DS4.3 identificar los recursos críticos de TI.
DS4.9 Almacenar respaldos fuera de las Instalaciones.

DS5. Garantizar la seguridad de los sistemas

Se debe llevar una correcta administración de seguridad, con la que se pueda proteger los equipos y datos, para minimizar el impacto de incidentes de seguridad.

El objetivo de control a ser considerado es:

DS5.9 Prevenir, detectar y corregir algún software malicioso

DS12. Administración del Ambiente Físico

Para que exista una efectiva administración del ambiente físico, es necesario reducir las interrupciones de las actividades como empresa, ocasionadas por daños al equipo.

Los objetivos de control a ser considerados son:

DS12.2 Adoptar medidas de seguridad física.
DS12.3 Prever el acceso físico.
DS12.4 Adoptar medidas protectoras en contra de factores ambientales.
DS12.5 Administrar las instalaciones físicas.

ME3. Garantizar el cumplimiento Regulatorio

Para garantizar un nivel de confianza aceptable entre la organización y los proveedores externos.

El objetivo de control a ser considerado:

ME3.3 Evaluar el cumplimiento con requerimientos externos

3.10.2.7 Herramienta para el desarrollo del análisis

Directrices de Auditoría COBIT

Estas directrices ayudarán a verificar el cumplimiento de los objetivos de control que serán previstos en base a posibles controles que deben aplicarse a cada objetivo y pruebas, para que puedan ser evaluados, como se muestra en las siguientes tablas.

3.10.2.8 Procesos en todos los Dominios

Objetivo de Control PO4.6

Tabla 3.6 PO4.6 Establecimiento de Roles y Responsabilidades

Dominio: Planeación y Organización	
PO4. Definir los Procesos, Organización y Relaciones de TI	
Para garantizar el soporte oportuno de todos los requerimientos como negocio y conocer que las responsabilidades de cada persona estén bien definidas y dar seguridad a los componentes del Data Center.	
Objetivo de Control	**Factores de Riesgo**
PO4.6Establecimiento de roles y responsabilidades: - Un encargado de Redes y Comunicaciones de la UTIC que manejen información dentro del Data Center , deberá asumir responsabilidades para mantener la seguridad física y lógica de todos los activos. - El encargo deberá reportar en un tiempo determinado al Director de la UTIC todas las incidencias de seguridad.	- El plan de contingencia no contempla procedimientos específicos para incidentes de seguridad. - No existen acciones para garantizar la seguridad de los activos, en las políticas de uso del Data Center.

Descripción de Pruebas PO4.6

Tabla 3.7 Matriz de Pruebas: Establecimiento de Roles y Responsabilidades

Dominio: Planeación y Organización		
PO4 Definir los Procesos, Organización y Relaciones de TI		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
PO4.6 Establecimiento de roles y responsabilidades: • Un jefe de Redes y Comunicaciones de la UTIC deberá asignar responsabilidades a quien maneje información dentro del Data Center para que reporte en un tiempo determinado al Director de la UTIC, todas las incidencias para mantener la seguridad física y lógica de todos los activos.	**Análisis de control:** • Dentro de las políticas de uso del Data Center existen procedimientos para un cuidado muy minucioso de la seguridad de los equipos. • Se describe dentro de este documento a un administrador que ha sido asignado para que reporte cualquier novedad al Director de la UTIC. • En el Plan de Contingencia se describen claramente las responsabilidades sobre la seguridad física y lógica de los equipos que contienen información Comprobando que: • El personal de conectividad y redes está encargado de la seguridad física y lógica del Data Center.	• Revisión del Plan de Contingencia del Data Center. • Revisión de Las Políticas de uso del Data Center. • Entrevista con un encargado de Conectividad y Redes.

Objetivo de Control PO4.11

Tabla 3.8 PO4.11 Segregación de Funciones

Dominio: Planeación y Organización	
PO4. Definir los Procesos, Organización y Relaciones de TI	
Para garantizar el soporte oportuno de todos los requerimientos como negocio y conocer que las responsabilidades de cada persona estén bien definidas para la seguridad de los componentes del Data Center.	
Objetivo de Control	**Factores de Riesgo**
PO4.11 Segregación de Funciones: • El jefe del área de Redes y Comunicaciones debe implementar una división de funciones para realizar procesos necesarios a efecto de mantener los equipos siempre operativos. • El jefe se asegurará que cada funcionario sólo realice las tareas que se asignan según su puesto que ocupa. Para el mantenimiento de la infraestructura se asignarán funciones como: • Responsabilidad Housing. • Respaldo de servicios. • Monitoreo Infraestructura Data Center	• Acceso no autorizado al Data Center y datos privados. • Confusión en las responsabilidades por parte de los encargados de realizar el mantenimiento de la infraestructura.

Descripción de Pruebas PO4.11

Tabla 3.9 Matriz de Pruebas: Segregación de Funciones

Dominio: Planeación y Organización		
PO4 Definir los Procesos, Organización y Relaciones de TI		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
PO4.11 Segregación de Funciones: • El jefe del área de Redes y Comunicaciones debe implementar una división de funciones para realizar procesos de mantenimiento con el fin de que los equipos estén siempre operativos. • Como jefe se asegurará que el personal solo realice las tareas que cada persona debe realizar, según su puesto. • Para el mantenimiento de la infraestructura se asignarán funciones como: - Responsabilidad Housing - Respaldo de Servicios - Monitoreo de la Infraestructura Data Center	**Análisis de control:** • Existe una planificación semanal que se realiza anualmente, en la cual se describen las responsabilidades de todo el personal de Redes y Comunicaciones; cada funcionario cuenta con la suficiente autoridad para realizar las tareas de mantenimiento. • Existe segregación de funciones en el mantenimiento de la Infraestructura del Data Center. • Comprobar que el personal de Redes y Comunicaciones tenga claramente delimitadas sus responsabilidades y autoridad, frente al mantenimiento del Data Center operativo 24/7.	• Revisión del documento Formatos para Gestión DC 03-04-2012 • Entrevista con un encargado de Conectividad y Redes.

Objetivo de Control PO9.3

Tabla 1.10 PO9.3 Identificación de Eventos

Dominio: Planeación y Organización	
PO9. Evaluar y Administrar los Riesgos de TI	
Se debe encontrar la manera de asegurar equipos y datos que en una calamidad se vuelvan críticos para el negocio, garantizando los objetivos del negocio, al procurar que nada salga mal en respecto a la seguridad física y lógica del Data Center.	
Objetivo de Control	**Factores de Riesgo**
PO9.3Identificación de Eventos: • La estimación de riesgos debe enfocarse en encontrar los elementos primordiales que en el momento de una falla, se conviertan en un riesgo para la organización. • Estos elementos dentro del Data Center serían activos tangibles e intangibles y su valor. • La identificación de los riesgos debe tener una calificación cuantitativa que se logra mediante reuniones entre todas las áreas de trabajo de la UTIC; planeaciones estratégicas y análisis anteriores. • El análisis de riesgos deberá considerar la tecnología, riesgos del personal, aspectos legales, estándares y negocio.	• Los riesgos no identificados no podrán constar en el Plan de Contingencia, lo que puede tener una repercusión económica negativa. • Identificar los riesgos de la seguridad de la información ante un ataque malicioso, mermará el impacto de un ataque de seguridad.

Descripción de Pruebas PO9.3

Tabla 3.11 Matriz de Pruebas: Identificación de Eventos

Dominio Planeación y Organización		
PO9. Evaluar y Administrar los Riesgos de TI		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
PO9.3 Identificación de Eventos • La estimación de riesgos se debe enfocar en encontrar los elementos primordiales que en el momento de una falla se conviertan en un riesgo para la organización. • Estos elementos dentro del Data Center serían activos tangibles e intangibles y su valor. • La identificación de los riesgos debe tener una calificación cuantitativa que se logra mediante reuniones entre todas las áreas de trabajo de la UTIC; planeaciones estratégicas y análisis anteriores. • El análisis de riesgos deberá considerar la tecnología, riesgos del personal, aspectos legales, estándares y negocio.	**Análisis de control** • El objetivo de proteger los activos del Data Center es evidente en el proceso de identificación de riesgos. • Se incluyen responsabilidades, inventario de activos, descripción de riesgos y una calificación cuantitativa de los mismos según su impacto. Comprobando que: • UTIC como departamento comprende que los riesgos y amenazas son un factor primordial al considerar los objetivos de negocio. • El personal de Redes y Comunicaciones comprende que la monitorización permanente de estos riesgos irá reduciendo progresivamente el impacto de los mismos.	• Revisión Plan de Contingencia • Entrevista con un encargado de Conectividad y Redes.

Objetivo de Control AI3.2

Tabla 3.12 AI3.2 Protección y Disponibilidad del Recurso de Infraestructura

Dominio: Adquirir e Implementar	
AI3. Administrar y Mantener la Infraestructura Tecnológica	
Para garantizar que exista un soporte tecnológico continuo para todas las aplicaciones que tiene el Data Center	
Objetivo de Control	**Factores de Riesgo**
AI3.2 Protección y Disponibilidad del Recurso de Infraestructura El personal de Redes y Comunicaciones de UTIC ESPE deberán programar un mantenimiento periódico del hardware para evitar el impacto de las fallas.	• Pérdida total o permanente de la información guardada en los servidores. • Daño total o permanente de los equipos que puede repercutir económicamente. • Insatisfacción en los usuarios por fallas en la conexión de la red e internet.

Descripción de Pruebas AI3.2

Tabla 3.13 Matriz de Pruebas: Protección y Disponibilidad del Recurso de Infraestructura

Dominio Adquirir e Implementar		
AI3. Administrar y Mantener Infraestructura Tecnológica		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
AI3.2 Protección y Disponibilidad del Recurso de Infraestructura El personal de Redes y Comunicaciones de UTIC ESPE deberán programar un mantenimiento periódico del hardware para evitar el impacto de las fallas.	**Análisis de control** • Existen procedimientos para el mantenimiento preventivo de hardware con el cual se logrará reducir el impacto de las fallas; y, la satisfacción de los usuarios finales. • Se debe garantizar la disponibilidad del Data Center 24/7. • Se debe tomar en cuenta también lo que sugiere el proveedor de los equipos en relación a su mantenimiento Comprobando que: • El monitoreo o mantenimiento programado se realice cuando la carga de trabajo a los equipos no se encuentre en los periodos pico. • Se garantice la disponibilidad de todos lo servicios y aplicaciones en Red 24/7.	• Revisión del documento Formatos para Gestión DC 03-04-2012 • Entrevista con un encargado de Conectividad y Redes.

Objetivo de Control AI3.3

Tabla 3.14 AI3.3 Mantenimiento de la Infraestructura

Dominio: Adquirir e Implementar	
AI3. Administrar y Mantener Infraestructura Tecnológica	
Para garantizar que exista un soporte tecnológico continuo para todas las aplicaciones que existen en el Data Center	
Objetivo de Control	**Factores de Riesgo**
AI3.3 Mantenimiento de la Infraestructura • El personal de Redes y Comunicaciones UTIC ESPE deberá programar un mantenimiento correctivo de la infraestructura. • Se debe utilizar un plan de mantenimiento con el cual se llevará permanentemente un control de todos lo cambios y actualizaciones realizadas.	• Pérdida total o permanente de la información guardada en los servidores. • Daño total o permanente de los equipos que puede repercutir económicamente de manera negativa. • Insatisfacción en los usuarios por fallas en la conexión de la red e internet.

Descripción de Pruebas AI3.3

Tabla 3.15 Matriz de Pruebas: Mantenimiento de la Infraestructura

Dominio Adquirir e Implementar		
AI3. Administrar y Mantener Infraestructura Tecnológica		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
AI3.3 Mantenimiento de la Infraestructura • El personal de Redes y Comunicaciones UTIC ESPE deberá programar un mantenimiento correctivo de la infraestructura. • Se debe utilizar un Plan de mantenimiento con el que se llevará permanentemente un control de todos los cambios y actualizaciones realizadas.	**Análisis de control** • La programación de los procedimientos que garanticen un mantenimiento preventivo debe constar dentro de un plan de mantenimiento. • La ejecución de un Plan de mantenimiento facilitará el control de las actividades realizadas dentro del Data Center. Comprobando que: • El plan para el mantenimiento correctivo se lo realice con la convicción de que no se debe interrumpir el trabajo del Data Center ni sus operaciones 24/7	• Revisión del documento Formatos para Gestión DC 03-04-2012 • Entrevista con un encargado de Conectividad y Redes. • Revisión de contratos para la realización de mantenimiento • Aplicación de checklist

Objetivo de Control DS2.3

Tabla 3.16 DS2.3 Administración de Riesgos del Proveedor

Dominio: Entrega de Servicios y Soporte	
DS2. Administrar los servicios de Terceros	
Para minimizar los riesgos del negocio asociados con los proveedores de equipos y servicios para el Data Center.	
Objetivo de Control	**Factores de Riesgo**
DS2.3 Administración de Riesgos del Proveedor • Las relaciones con los proveedores de servicios y de equipos deben procurar tener la mayor seguridad y confidencialidad, para llegar a acuerdos de tal manera que tanto los proveedores cuanto la ESPE, sigan los estándares de negocios de equipamiento. • De cada una de las partes se desglosan algunas obligaciones legales que se deben cumplir por medio de los contratos.	• Revisión inadecuada de la información proporcionada por los proveedores. • No cumplimiento de las responsabilidades legales por parte de terceros.

Descripción de Pruebas DS2.3

Tabla 3.17 Matriz de Pruebas: Administración de Riesgos del Proveedor

Dominio: Entrega de Servicios y Soporte		
DS2. Administrar los servicios de Terceros		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
DS2.3 Administración de Riesgos del Proveedor • Las relaciones con los proveedores de servicios y de equipos deben procurar tener la mayor seguridad y confidencialidad, con lo que luego se debe llegar acuerdos para que tanto los proveedores como la ESPE, sigan los estándares de negocios, de equipamiento. • De cada una de las partes se desglosan algunas obligaciones legales que se debe cumplir por medio de los contratos.	**Análisis de control** Los contratos con terceros o proveedores por lo menos deben incluir: 1.- Acuerdos de seguridad. 2.- Acuerdos de confidencialidad. **Comprobando que:** Dentro de estos acuerdos de seguridad se detalle los proveedores o terceros que están autorizados para ingresar al Data Center a realizar algún arreglo o mantenimiento.	Entrevista con un encargado de Conectividad y Redes.

Objetivo de Control DS4.3

Tabla 3.18 DS4.3 Recursos Críticos de TI

Dominio: Entrega de Servicios y Soporte	
DS4. Garantizar la continuidad del Servicio	
Es la capacidad del Data Center para seguir brindando servicio con la ayuda de un plan de contingencias para recuperación de fallas y políticas de respaldo de información.	
Objetivo de Control	**Factores de Riesgo**
DS4.3 Recursos Críticos de TI • Deberá constar en el Plan de Contingencia del Data Center, todos los recursos que serán vulnerables ante una catástrofe. • Así se identificarán equipos, aplicaciones, personal responsable, proveedores, manuales de encendido y apagado de servicios. • Cada uno de esos recursos críticos deben ser documentados.	• Pérdida total o parcial de la información. • No existe tiempo de recuperación. • Falta de aseguramiento de servicios o aplicaciones.

Descripción de Pruebas DS4.3

Tabla 3.19 Matriz de Pruebas: Recursos Críticos de TI

Dominio: Entrega de Servicios y Soporte		
DS4. Garantizar la continuidad del Servicio		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
DS4.3 Recursos Críticos de TI • Todos los recursos que sean vulnerables ante una catástrofe, deberán constar en el Plan de Contingencia del Data Center. • Así se identificarán equipos, aplicaciones, personal responsable, proveedores, manuales de encendido y apagado de servicios. • Cada uno de esos recursos críticos deben ser documentados.	**Análisis de control:** • Priorizar la lista de hardware desde el más vulnerable al menos vulnerable, en caso de una catástrofe. • Tomar en cuenta todos los equipos que puedan ser un peligro para la continuidad de los servicios. Comprobando que: • El Director de la UTIC debe revisar y aprobar el Plan de Contingencia del Data Center, asegurándose de consten todos los recursos críticos que podrían influir negativamente en la continuidad de los servicios.	Revisión del Plan de Contingencia del Data Center

Objetivo de Control DS4.9

Tabla 3.20 DS4.9 Almacenamiento de respaldos fuera de las Instalaciones

<table>
<tr><th colspan="2">Dominio: Entrega de Servicios y Soporte</th></tr>
<tr><td colspan="2">DS4. Garantizar la continuidad del Servicio</td></tr>
<tr><td colspan="2">Es la capacidad del Data Center para seguir brindando servicio con la ayuda de un plan de contingencias para recuperación de fallas y políticas de respaldo de información.</td></tr>
<tr><th>Objetivo de Control</th><th>Factores de Riesgo</th></tr>
<tr><td>DS4.9 Almacenamiento de respaldos fuera de las Instalaciones

Para la continuidad de servicios y aplicaciones el Departamento de Redes y Comunicaciones debe establecer procesos alternativos como el respaldo de información para tener la capacidad de restaurar completamente los servicios o aplicaciones en caso de un desastre o alguna contingencia.</td><td>• Pérdida total o parcial de la información y de respaldo de los servicios o aplicaciones.

• Interrupción crítica de servicios o aplicaciones.

• Falta de etiquetas en la información que se está respaldando.</td></tr>
</table>

Descripción de Pruebas DS4.9

Tabla 3.21 Matriz de Pruebas: Almacenamiento de respaldos fuera de las Instalaciones

Dominio: Entrega de Servicios y Soporte		
DS4. Garantizar la continuidad del Servicio		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
DS4.9 Almacenamiento de respaldos fuera de las Instalaciones • Para la continuidad de servicios y aplicaciones, el Departamento de Redes y Comunicaciones debe establecer procesos alternativos como el respaldo de información para tener la capacidad de restaurar completamente los servicios o aplicaciones, en caso de un desastre o alguna contingencia.	**Análisis de control:** • La información académica de alumnos, docentes, administrativos. • Los contratos de servicios con sus respectivos proveedores. • Imágenes de los servicios, redundancias y manuales de operación. Comprobando que: • Exista la cantidad necesaria de respaldos para sobrellevar un gran desastre.	Revisión de la Políticas de Respaldo de Información UTIC ESPE.

Objetivo de Control DS5.9

Tabla 3.22 DS5.9 Prevención, Detección y Corrección Software Malicioso

<table>
<tr><th colspan="2">Dominio: Entrega de Servicios y Soporte</th></tr>
<tr><td colspan="2">DS5. Garantizar la seguridad de los sistemas</td></tr>
<tr><td colspan="2">Se debe llevar una correcta administración de seguridad, con la que se pueda proteger los equipos y datos para minimizar el impacto de incidentes de seguridad.</td></tr>
<tr><th>Objetivo de Control</th><th>Factores de Riesgo</th></tr>
<tr><td>DS5.9 Prevención, Detección y Corrección de Software Malicioso

El área de Redes y Comunicaciones debe establecer medidas preventivas, detectivas y correctivas para proteger los datos críticos del Data Center y los equipos contra malware.</td><td>• Ataque de virus, gusanos, spyware, correo basura.

• Pérdida total o parcial de información.

• Colapso en el funcionamiento de servicios y aplicaciones.</td></tr>
</table>

Descripción de Pruebas DS5.9

Tabla 3.23 Matriz de Pruebas: Prevención, Detección y Corrección Software Malicioso

Dominio: Entrega de Servicios y Soporte		
DS5. Garantizar la seguridad de los sistemas		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
DS5.9 Prevención, Detección y Corrección de Software Malicioso El área de Redes y Comunicaciones debe establecer medidas preventivas, detectivas y correctivas para proteger los datos críticos del Data Center y los equipos contra malware.	**Análisis de control:** • El personal de Redes y Comunicaciones debe entrenarse en la manera de proteger los equipos y datos contra virus existentes y nuevas definiciones. • Las medidas preventivas, detectivas y correctivas deben ser conocidas por todo el personal para una continua protección. Comprobando que: • Debe realizarse una revisión periódica de los equipos que sean susceptibles a intrusos o virus malintencionados. • Deben existir políticas sobre el uso de los antivirus.	Aplicación de Checklist

Objetivo de Control DS12.2

Tabla 3.24 DS12.2 Medidas de Seguridad Física

Dominio: Entrega de Servicios y Soporte	
DS12. Administración del Ambiente Físico	
Para que exista una efectiva administración del ambiente físico, se deben reducir las interrupciones de actividades ocasionadas por daños al equipo.	
Objetivo de Control	**Factores de Riesgo**
DS12.2 Medidas de Seguridad Física • Se deben definir medidas de seguridad física para la instalación donde se encuentran los equipos y datos críticos del Data Center. • Se debe tomar en cuenta que la seguridad debe estar orientada no solo al lugar donde se encuentra el hardware sino también el cableado, utilizado para conectar los elementos requeridos para la operación de todos los sistemas dentro de la UTIC. • Se deben proteger todos los equipos y datos críticos de robo o pérdida.	• Daño malintencionada de hardware. • Pérdida, robo de equipos o datos críticos necesarios para la continuidad de servicios.

Descripción de Pruebas DS12.2

Tabla 3.25 Matriz de Pruebas: Medidas de Seguridad Física

Dominio: Entrega de Servicios y Soporte		
DS12. Administración del Ambiente Físico		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
DS12.2 Medidas de Seguridad Física • Se deben definir medidas de seguridad física para la instalación donde se encuentran los equipos y datos críticos del Data Center. • Hay que tener en cuenta que la seguridad debe estar orientada no solo al lugar donde se encuentra el hardware sino también al cableado, utilizado para conectar los elementos requeridos en la operación de todos los sistemas dentro de la UTIC. • Se debe proteger todos los equipos y datos críticos de robo o pérdida.	**Análisis de control:** • La ubicación del Data Center no debe ser obvia para los visitantes. • Para el ingreso al Data Center se necesita autorización del Director de la UTIC o del personal de Redes y Comunicaciones. • Ingreso biométrico o tarjetas magnéticas para poder ver el interior del Data Center. • Las medidas de control deben existir al momento de sacar un equipo del Data Center cualquiera que sea la intención. • Los visitantes al Data Center	• Revisión Plan de Contingencia de la UTIC. • Observación al área de Redes y Comunicaciones UTIC. • Entrevista con un encargado de Redes y Comunicaciones. • Aplicación checklist.

	deben registrar su nombre; es obligación de un responsable de seguridad, revisar los registros como un procedimiento de seguridad. • Deben existir procedimientos a realizar el momento que se active la alarma de seguridad. • El personal de Redes y Comunicaciones UTIC ESPE monitoreará el cableado estructurado del Data Center. Comprobando que: • Los servidores, racks, aire acondicionado, cableado estructurado, cámaras ip, tableros de distribución, UPS, PDU y sistemas contra incendio estén protegidos físicamente contra un posible acceso no autorizado. • Existan procedimientos para el acceso al Data Center en caso de un visitante autorizado.	

Objetivo de Control DS12.3

Tabla 3.26 DS12.3 Acceso Físico

Dominio: Entrega de Servicios y Soporte	
DS12. Administración del Ambiente Físico	
Para que exista una efectiva administración del ambiente físico y reducir las interrupciones de las actividades como empresa, ocasionadas por daños al equipo.	
Objetivo de Control	**Factores de riesgo**
DS12.3 Acceso físico El acceso a los equipos para monitorearlos o alguna visita técnica o académica, debe justificada, autorizada y debe registrarse en las bitácoras de visita para evitar conflictos de seguridad.	• Daño malintencionada de hardware. • Pérdida, robo de equipos o datos críticos necesarios para la continuidad de servicios.

Descripción de Pruebas DS12.3

Tabla 3.27 Matriz de Pruebas: Acceso físico

Dominio: Entrega de Servicios y Soporte		
DS12. Administración del Ambiente Físico		
Objetivo de Control	**Revisión**	**Descripción de pruebas**
DS12.3 Acceso Físico El acceso a los equipos para monitorearlos, alguna visita técnica o académica deben ser justificadas y autorizadas; deben registrarse en las bitácoras de visita para evitar conflictos de seguridad.	**Análisis de control:** • Existen procedimientos de seguridad bien definidos para el ingreso de visitantes y personal al Data Center. Comprobando que: • Existan plantillas para ingresar resultados del monitoreo del Data Center. • Documentos de responsabilidades en los que se detalle lo que el personal tiene que realizar, para garantizar un servicio continuo del Data Center.	• Formatos para Gestión DC 03-04-2012. • Entrevista con un encargado de Redes y Comunicaciones. • Aplicación de Checklist.

Objetivo de Control DS12.4

Tabla 3.28 DS12.4 Protección contra factores ambientales

Dominio: Entrega de Servicios y Soporte	
DS12. Administración del Ambiente Físico	
Para que exista una efectiva administración del ambiente físico, reduce las interrupciones de las actividades como empresa ocasionadas por daños al equipo.	
Objetivo de Control	**Factores de Riesgo**
DS12.4 Protección contra factores ambientales • El personal de Redes y Comunicaciones deberá asegurar que los equipos siempre estén en funcionamiento, lo que quiere decir que los mismos deben estar protegidos contra los factores ambientales. • Deben instalarse dispositivos especializados como sensores dentro del Data Center para una correcta protección.	Daño de hardware y cableado dentro del Data Center.

Descripción de Pruebas DS12.4

Tabla 3.29 Matriz de Pruebas: Protección contra factores ambientales

Dominio: Entrega de Servicios y Soporte		
DS12. Administración del ambiente físico		
Objetivo de control	**Revisión**	**Descripción de Pruebas**
DS12.4 Protección contra factores ambientales El acceso a los equipos para monitorearlos o alguna visita técnica o académica debe ser justificada, y autorizada; debe registrarse en las bitácoras de visita para evitar conflictos de seguridad.	**Análisis de control:** • Los procedimientos contra incendios, demasiada humedad, inundaciones, problemas eléctricos y mal funcionamiento de alarmas, para ofrecer un buen nivel de confiabilidad frente a una catástrofe. • Cuando se realiza un mantenimiento también se comprueba la respuesta de los sensores. Comprobando que: El equipo de monitoreo dentro del Data Center recibe mantenimiento periódicamente.	• Entrevista con un encargado de Redes y Comunicaciones. • Observación dentro del Data Center. • Revisión Plan de Contingencia del Data Center.

Objetivo de Control DS12.5

Tabla 3.30 DS12.5 Administración de instalaciones físicas

Dominio: Entrega de servicios y soporte	
DS12. Administración del ambiente físico	
Para que exista una efectiva administración del ambiente físico y se reduzcan las interrupciones de las actividades como empresa ocasionadas por daños al equipo.	
Objetivo de control	**Factores de riesgo**
DS12.5 Administración de Instalaciones físicas Para una correcta administración se debe garantizar un suministro de energía ininterrumpido, con el fin de controlar los servicios, aplicaciones y las comunicaciones, durante un tiempo prudente.	• Falla de suministro eléctrico. • Interrupción de servicios y aplicaciones. • Pérdida o daño de información.

Descripción de Pruebas DS12.5

Tabla 3.31 Matriz de Pruebas: Administración de instalaciones físicas

Dominio: Entrega de servicios y soporte		
DS12. Administración del ambiente físico		
Objetivo de Control	**Revisión**	**Descripción de Pruebas**
DS12.5 Administración de Instalaciones físicas Para una correcta administración se debe garantizar un suministro de energía ininterrumpido, con el fin de controlar los servicios, aplicaciones y comunicaciones durante un tiempo prudente.	**Análisis de control:** • Existan elementos que garanticen el suministro ininterrumpido de energía (UPS). Comprobando que: • Controlar el correcto funcionamiento de los UPS según las sugerencias y recomendaciones operacionales del proveedor para asegurar el flujo eléctrico.	• Entrevista con un encargado de Redes y Comunicaciones. • Observación dentro del Data Center.

Objetivo de Control ME3.4

Tabla 3.32 ME3.4 Aseguramiento positivo del cumplimiento

Dominio: Monitorear y Evaluar	
ME3. Garantizar el Cumplimiento con requerimientos externos	
Para garantizar un nivel de confianza aceptable entre la organización y los proveedores externos.	
Objetivo de control	**Factores de riesgo**
ME3.4 Aseguramiento positivo del cumplimiento Debe asegurarse que en la organización exista garantía de cumplimiento de los requerimientos legales para que no haya ninguna brecha en los contratos con lo proveedores.	Las compañías proveedoras de servicios no cumplan con los contratos estipulados.

Descripción de Pruebas ME3.4

Tabla 3.33 Matriz de Pruebas: Aseguramiento del cumplimiento

Dominio: Monitorear y evaluar		
ME3. Garantizar el cumplimiento con requerimientos externos		
Objetivo de control	**Revisión**	**Descripción de pruebas**
ME3.4 Aseguramiento Positivo del cumplimiento Debe asegurarse que en la organización exista garantía de cumplimiento de los requerimientos legales para que no exista ninguna brecha en los contratos con los proveedores.	**Análisis de control:** • Se aplica una revisión o acreditación antes de utilizar a los proveedores de servicios. • Evalué el desempeño de cada uno de los proveedores de servicios Comprobando que: • La revisión o acreditación de los proveedores de servicios. • Evaluación de los proveedores en busca de un mejor desempeño dentro del Data Center.	Entrevista con un encargado de Redes y Comunicaciones.

3.10.2.9 Resultado del Análisis

Resultado del Análisis objetivo de control PO4.6

Tabla 3.34 Resultado Análisis: Establecimiento de roles y responsabilidades

Dominio: Planeación y organización				
PO4. Definir los procesos, organización y relaciones de TI				
PO4.6 Establecimiento de roles y responsabilidades				
Revisión	**Descripción de pruebas**	**Análisis definido**	**Documentos de respaldo**	**Recomendación**
• Dentro de las políticas de uso del Data Center existen procedimientos para un cuidado muy minucioso de la seguridad de los equipos. • Se describe dentro de este documento a un administrador que ha sido asignado para que reporte cualquier novedad al Director de la UTIC. • En el Plan de Contingencia se describen claramente las responsabilidades sobre la seguridad física y lógica de los equipos que contienen información. Comprobando que: • El personal de conectividad y redes está encargado de la seguridad física y lógica.	• Revisión del Plan de Contingencia del Data Center. • Revisión de Las Políticas de uso del Data Center. • Entrevista con un encargado de Conectividad y Redes. • Revisión del documento Formatos para Gestión DC 03-04-2012.		• Plan de Contingencia UTIC. • Políticas Data Center 04-05-2012. • Responsabilidad DC(A) ANX1.	

Resultado del Análisis objetivo de control PO4.11

Tabla 3.35 Resultado Análisis: Segregación de funciones

Dominio: Planeación y Organización				
PO4. Definir los procesos, organización y relaciones de TI				
PO4.11 Segregación de funciones				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Existe una planificación semanal que se realiza anualmente en la cual se describen las responsabilidades de todo el personal de Redes y Comunicaciones; cada uno de ellos cuenta con la suficiente autoridad para realizar las funciones de mantenimiento. • Existe segregación de funciones en el mantenimiento de la infraestructura del Data Center. Comprobando que: • El personal de Redes y Comunicaciones tiene delimitadas claramente sus responsabilidades y autoridad frente al mantenimiento de un Data Center operativo 24/7.	• Revisión del documento Formato para Gestión DC 03-04-2012 • Entrevista con un encargado de Conectividad y Redes.	Administrado y medible	• Responsabilidad DC(A) ANX1 • Responsabilidad DC ANX1(B) • Monitoreo de fin de Semana ANX2.	

Resultado del Análisis objetivo de control PO9.3

Tabla 3.36 Resultado Análisis: Identificación de eventos

Dominio: Planeación y organización				
PO9. Evaluar y administrar los riesgos de TI				
PO9.3 Identificación de Eventos				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• El objetivo de proteger los activos del Data Center se ve evidenciado en el proceso identificación de riesgos. • Se incluyen responsabilidades, inventario de activos, descripción de riesgos y una calificación cuantitativa de los riesgos según su impacto. Comprobando que: • UTIC como departamento comprende que los riesgos y amenazas son un factor primordial al considerar los objetivos de negocio. • El personal de Redes y Comunicaciones comprende que la monitorización permanente de estos riesgos irá reduciendo progresivamente el impacto de los mismos.	• Revisión Plan de Contingencia. • Entrevista con un encargado de Conectividad y Redes.	Definido	Plan Contingencia UTIC	

Resultado del Análisis objetivo de control AI3.2

Tabla 3.37 Resultado Análisis: Protección y disponibilidad del recurso de infraestructura

Dominio: Adquirir e implementar				
AI3. Administrar y mantener infraestructura tecnológica				
AI3.2 Protección y disponibilidad del recurso de infraestructura				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Existen procedimientos para el mantenimiento preventivo de hardware con el cual se logrará reducir el impacto de las fallas e insatisfacción de los usuarios finales. • Se debe garantizar la disponibilidad del Data Center 24/7. • También se debe tomar en cuenta lo que sugiere el proveedor de los equipos, en relación a su mantenimiento. Comprobando que: • El monitoreo o mantenimiento programado se lo realice cuando la carga de trabajo a los equipos no se encuentre en los periodos pico. • Se garantice la disponibilidad de todos lo servicios y aplicaciones en red 24/7.	• Revisión del documento Formatos para Gestión DC 03-04-2012. • Entrevista con un encargado de Conectividad y Redes.	Optimizado	• Monitoreo Fin Semana ANX2. • Registo monitoreo ANX3 (Ver anexo 2). • Ingreso DC ANX4 (Ver anexo 2).	

Resultado del Análisis objetivo de control AI3.3

Tabla 3.38 Resultado Análisis: Mantenimiento de la infraestructura

Dominio: Adquirir e implementar				
AI3. Administrar y mantener infraestructura tecnológica				
AI3.3 Mantenimiento de la Infraestructura				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• La programación de los procedimientos que garantice un mantenimiento preventivo, debe constar dentro de un Plan de mantenimiento. • La utilización de un Plan de mantenimiento facilitará el control de las actividades realizadas dentro del Data Center Comprobando que: • El Plan para el mantenimiento correctivo se realice con la convicción de no interrumpir el trabajo del Data Center y sus operaciones 24/7.	• Revisión del documento Formatos para Gestión DC 03-04-2012. • Entrevista con un encargado de Conectividad y Redes. • Revisión de contratos para la realización de mantenimiento. • Aplicación de checklist.	• Administrado y medible	• Registro monitoreo ANX3 (Ver anexo 2). • Memo al Gerente Administrativo y Financiero. • Comprobante de Servicio Técnico. (Ver anexo 3).	

Resultado del Análisis objetivo de control DS2.3

Tabla 3.39 Resultado análisis: Administración de riesgos del proveedor

Dominio: Entrega de servicios y soporte				
DS2. Administrar los servicios de terceros				
DS2.3 Administración de Riesgos del Proveedor				
Revisión	**Descripción de Pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Los contratos con los terceros o proveedores, por lo menos deben incluir: 1.- Acuerdos de seguridad. 2.- Acuerdos de confidencialidad. Comprobando que: • Dentro de estos acuerdos de seguridad se detallen los proveedores o terceros que están autorizados a ingresar al Data Center para realizar algún arreglo o mantenimiento.	Entrevista con un encargado de Conectividad y Redes.	Administrado y medible.	Contratos con terceros.	

Resultado del Análisis objetivo de control DS4.3

Tabla 3.40 Resultado Análisis: Recursos Críticos de TI

Dominio: Entrega de servicios y soporte				
DS4. Garantizar la continuidad del servicio				
DS4.3 Recursos críticos de TI				
Revisión	**Descripción de Pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Priorizar la lista de hardware del más vulnerable al menos vulnerable, en caso de una catástrofe. • Tomar en cuenta todos los equipos que puedan ser un peligro para la continuidad de los servicios. Comprobando que: • El Director de la UTIC debe revisar y aprobar el Plan de Contingencia del Data Center, asegurándose de que consten todos los recursos críticos que podrían influir en la continuidad de los servicios.	• Revisión del Plan de Contingencia del Data Center. • Revisión de descripción de equipamiento Data Center.	• Definido.	• Plan de Contingencia UTIC. • Descripción de equipamiento del Data Center.	

Resultado del Análisis objetivo de control DS4.9

Tabla 3.41 Resultado Análisis: Almacenamientos de respaldos fuera de las instalaciones

Dominio: Entrega de servicios y soporte				
DS4. Garantizar la continuidad del servicio				
DS4.9 Almacenamiento de respaldos fuera de las Instalaciones				
Revisión	**Descripción de Pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• La información académica de alumnos, docentes, administrativos. • Los contratos de servicios con sus respectivos proveedores. • Imágenes de los servicios, redundancias, manuales de operación. Comprobando que: • Exista la cantidad necesaria de respaldos para sobrellevar un gran desastre.	Revisión de la políticas de respaldo de información UTIC ESPE.	Administrado y medible.	GT1-Politicas respaldo información.	

Resultado del Análisis objetivo de control DS5.9

Tabla 3.42 Resultado Análisis: Prevención, detección y corrección de Software malicioso

Dominio: Entrega de Servicios y Soporte				
DS5. Garantizar la seguridad de los sistemas				
DS5.9 Prevención, detección y corrección de Software malicioso				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• El personal de Redes y Comunicaciones debe entrenarse en la manera de proteger los equipos y datos contra virus existentes y nuevas definiciones. • Las medidas preventivas, detectivas y correctivas deben ser conocidas por todo el personal para una continua protección. Comprobando que: • Debe realizarse una revisión periódica de los equipos que sean susceptibles a intrusos o virus malintencionados. • Deben existir políticas sobre el uso de los antivirus.	Aplicación de checklist.	Definido.	• Políticas de seguridad del Data Center. • (Ver anexo 3)	

Resultado del Análisis objetivo de control DS12.2

Tabla 3.43 Resultado Análisis: Medidas de seguridad física

Dominio: Entrega de servicios y soporte				
DS12. Administración del ambiente físico				
DS12.2 Medidas de seguridad física				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• La ubicación del Data Center no debe ser obvia para los visitantes. • Para el ingreso al Data Center se necesita autorización del Director de la UTIC o del personal de Redes y Comunicaciones. • Ingreso biométrico o tarjetas magnéticas para ingresar al Data Center. • Las medidas de control deben existir al momento de sacar un equipo del Data Center, cualquiera que sea la intención con la que se saca el equipo. • Los visitantes al Data Center se deben registrar y es obligación	• Revisión Plan de Contingencia de la UTIC. • Observación al área de Redes y Comunicaciones UTIC. • Entrevista con un encargado de Redes y Comunicaciones. • Aplicación de Checklist.	Optimizado.	• Plan de contingencia UTIC (Ver anexo 3)	

de un responsable de seguridad revisar los registros como un procedimiento de seguridad. • Deben existir procedimientos a realizar el momento que se active la alarma de seguridad. • El personal de Redes y Comunicaciones UTIC ESPE monitoreará el cableado estructurado del Data Center. Comprobando que: • Los servidores, racks, aire acondicionado, cableado estructurado, cámaras ip, tableros de distribución, UPS, PDU y sistemas contra incendio, estén protegidos físicamente contra un posible acceso no autorizado. • Existan procedimientos para el acceso al Data Center en caso de un visitante autorizado.				

Resultado del Análisis objetivo de control DS12.3

Tabla 3.44 Resultado Análisis: Acceso físico

Dominio: Entrega de servicios y soporte				
DS12. Administración del ambiente físico				
DS12.3 Acceso físico				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Existen procedimientos de seguridad bien definidos para el ingreso de visitantes y personal al Data Center. Comprobando que: • Existan plantillas para ingresar resultados del monitoreo del Data Center • Documento o documentos de responsabilidades en el que se detalle lo que el personal tiene que realizar para garantizar un servicio continuo del Data Center.	• Formatos para Gestión DC 03-04-2012. • Entrevista con un encargado de Redes y Comunicaciones. • Aplicación de Ckecklist.	Optimizado	• Formatos para Gestion DC 03-04-2012. • Bitácoras de Visitas. (Ver anexo 3).	

Resultado del Análisis objetivo de control DS12.4

Tabla 3.45 Resultado Análisis: Protección contra factores ambientales

Dominio: Entrega de servicios y soporte				
DS12. Administración del ambiente físico				
DS12.4Protección contra factores ambientales				
Revisión	**Descripción de Pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Los procedimientos contra incendios, demasiada humedad, inundaciones, la madre naturaleza y problemas eléctricos, así como sus alarmas, ofrezcan un gran nivel de confiabilidad frente a una catástrofe. • Cuando se realiza un mantenimiento también se comprueba la respuesta de los sensores. Comprobando que: • El equipo de monitoreo dentro del Data Center tiene mantenimiento periódico.	• Entrevista con un encargado de Redes y Comunicaciones.. • Observación dentro del Data Center • Revisión Plan de Contingencia del Data Center	Optimizado.	Plan de Contingencia UTIC.	

Resultado del Análisis objetivo de control DS12.5

Tabla 3.46 Resultado Análisis: Administración de instalaciones físicas

Dominio: Entrega de servicios y soporte				
DS12. Administración del ambiente físico				
DS12.5 Administración de instalaciones físicas				
Revisión	**Descripción de pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Existan elementos que garanticen el suministro ininterrumpido de energía (UPS). Comprobando que: • Controlar el correcto funcionamiento de los UPS según las sugerencias y recomendaciones operacionales del proveedor para asegurar el flujo eléctrico.	• Entrevista con un encargado de Redes y Comunicaciones. • Observación dentro del Data Center.	Definido.	Políticas Data Center 04-05-2012.	

Resultado del Análisis objetivo de control ME3.4

Tabla 3.47 Resultado Análisis: Aseguramiento positivo del cumplimiento

Dominio: Monitorear y Evaluar				
ME3. Garantizar el Cumplimiento con requerimientos externos				
ME3.4 Aseguramiento positivo del cumplimiento				
Revisión	**Descripción de Pruebas**	**Análisis**	**Documentos de respaldo**	**Recomendación**
• Se realiza una revisión o acreditación antes de utilizar a los proveedores de servicios. • Evaluar el desempeño de cada uno de los proveedores de servicios Comprobando que: • La revisión o acreditación de los proveedores de servicios. • Evaluación de los proveedores en busca de un mejor desempeño dentro del Data Center.	Entrevista con un encargado de Redes y Comunicaciones.	Definido	Contratos con terceros.	

3.10.2.10 Análisis de los resultados

PO4.6 Establecimiento de roles y responsabilidades

En la UTIC reposan documentos en los cuales existe una descripción de todo el personal que labora en esta unidad; también existen manuales para apagado y levantamiento de servicios, garantizando de esta manera que cualquier empleado de Redes y Comunicaciones pueda realizar esas actividades.

En el documento de responsabilidades de Housing, está definida la responsabilidad de cada área de la UTIC, frente a la continuidad de servicios.

PO4.11 Segregación de funciones

Actualmente, se dispone de tres documentos en los cuales se detallan las responsabilidades del personal.

En el primer documento habla de las responsabilidades frente al Housing.

El segundo documento corresponde a las responsabilidades para el respaldo de servicios; también comprende a los profesionales responsables de administrar el servidor, de respaldos automáticos a cintas.

El tercer documento detalla las responsabilidades anuales para la atención del Data Center.

PO9.3 Identificación de eventos

El Plan de Contingencia UTIC contiene todos los activos codificados a proteger del Data Center; detalla los servicios aplicativos y hardware.
Se han definido los riesgos con los cuales se podrían ver afectados el Data Center así como el impacto de los mismos sobre los activos que están analizados de forma cuantitativa. También se ha detallado la mejor manera de ofrecer una continuidad de los servicios en caso de que se dé una catástrofe.

AI3.2 Protección y disponibilidad del recurso de infraestructura y mantenimiento de la infraestructura

El personal se guía mediante el documento de Monitoreo Fin Semana ANX2, útil para realizar un monitoreo semanal de los equipos dentro del Data Center, por lo que se puede observar en el mismo documento, el mantenimiento de los equipos que se realiza cada seis meses. El monitoreo y mantenimiento se realiza los fines de semana cuando el tráfico de los servidores es menor.

Se constata la existencia de un memorándum dirigido al Gerente Administrativo y Financiero para informarle acerca del mantenimiento de la infraestructura; también existen comprobantes del Servicio Técnico.

DS2.3 Administración de riesgos del proveedor

En relación a los contratos con proveedores o terceros se obtuvo la siguiente información:

- Los contratos se realizan por medio del método de la subasta inversa; esto quiere decir que se califica solamente el precio que ofrecen los participantes.
- Existe una evaluación de servicios, porque si se endurecen las políticas internas de servicios, se buscarán mejores proveedores.
- Los contratos se realizan solamente para un año como estipula la ley.

DS4.3 Recursos Críticos de TI

En el Plan de Contingencia se ha valorizado todo el equipo que es susceptible de riesgos o amenazas; además existe un documento de Distribución del Equipamiento, en el que se detallan todos los equipos y su distribución dentro del Data Center.

DS4.9 Almacenamiento de respaldos fuera de las Instalaciones

En el documento de Políticas de Respaldo de información se detalla el lugar donde se llevarán los respaldos, la persona que está encargada de llevar los respaldos y por último en el documento “Responsabilidad de Respaldo de Servicios” se menciona los responsables de realizar los respaldos y administrar las cintas.

DS5.9 Prevención, detección y corrección de Software malicioso

Se tiene un control muy detallado de Firewall, el mismo que es monitoreado mediante software.

La actualización de los antivirus es diaria y se escanea frecuentemente los servidores con los antivirus. La responsabilidad de mantener los servidores sin virus no es solamente del Área de Redes y Comunicaciones sino también del Área de Sistemas de Información.

DS12.2 Medidas de seguridad física y DS12.3 Acceso Físico

El ingreso al Data Center está muy bien monitoreado, no es posible entrar al mismo sin previa autorización o con la compañía del personal de Redes y Comunicaciones; existen bitácoras de visitas técnicas o académicas.

Es imposible que personal civil sepa de la ubicación exacta del Data Center, lo cual garantiza su seguridad ante posibles robos.

El lector biométrico y las tarjetas magnéticas ofrecen un plus en la seguridad, ya que registra las entradas y salidas de los empleados de Redes y Comunicaciones.

En conclusión, todas las entradas son monitoreadas ya sea para visitas, mantenimiento o monitoreo.

DS12.4 Protección contra factores ambientales

Dentro del Plan de Contingencia están muy diferenciados cada uno de las riesgos naturales que pueden afectar la continuidad de los servicios del Data Center; además se pudo confirmar que existen sensores para la prevención de humedad, que al no ser supervisado se podría ver afectado el cableado estructurado.

DS12.5 Administración de instalaciones físicas

Para garantizar el suministro ininterrumpido de energía eléctrica, existen dos UPS que permiten la continuidad de los servicios por un tiempo determinado, según la carga que en ese momento dispongan.

ME3.3 Evaluación del Cumplimiento con requerimientos externos

Se realiza una evaluación del cumplimiento de los contratos con terceros, al terminar el año de contrato; si la empresa proveedora no puede cumplir con los requerimientos internos, se busca otro proveedor de servicios que pueda hacerlo.

3.11 Proceso de evaluación técnica del Data Center

A continuación se describen los valores obtenidos de cada uno de los sistemas que forman parte del funcionamiento del Data Center, para su correspondiente análisis en el informe técnico, basado en las normas internacionales.

3.11.1 Sistema Eléctrico

Acometidas:

Es una fracción de la instalación eléctrica que se construye desde el transformador del poste de energía eléctrica, hasta las conexiones o instalaciones del usuario.

Existen tres tipos de acometidas: monofásica, bifásica y trifásica.

Monofásica:

El cable conductor es de tres hilos (una fase o activo, un neutro y tierra), normalmente este tipo de acometida es utilizada en las instalaciones de viviendas.

Bifásica:

El cable conductor es de cuatro hilos dos fases o activo, un neutro y tierra)

Trifásica:

El cable conductor consta de cinco hilos (tres fases o activo, un neutro y tierra); normalmente este tipo de acometida es utilizada en las instalaciones de edificios.

Dentro del Data Center de la ESPE se constató que tienen siete acometidas trifásicas las cuales constan de cinco hilos o cables (tres fases o activos, un neutro y tierra); estas desembocan en un tablero de distribución de energía como se muestra en la ilustración 3.5.

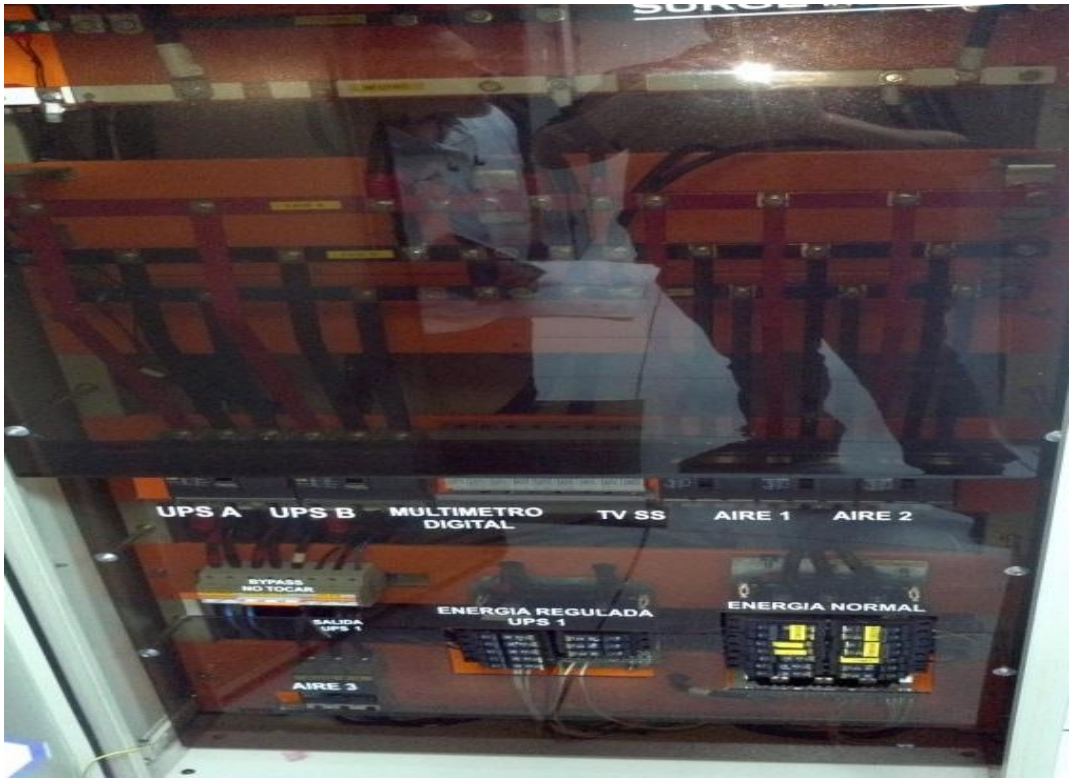


Ilustración 3.5 Tablero de Distribución Data Center ESPE

FUENTE: Data Center ESPE

Tablero de distribución:

Este es uno de los componentes principales en una instalación eléctrica; en él se protege todos los circuitos eléctricos; estos cuentan con breakers, elementos de medición y conexiones, tal como se indica en la ilustración 3.6.

Los tableros de distribución deben estar ubicados en lugares y en atención a las siguientes condiciones:

- Los espacios asignados deben ser dedicados exclusivamente para los tableros.

- No deben existir tuberías, ductos o equipos ajenos a la instalación eléctrica, excepto los rociadores contra incendio y los equipos de control que deben estar adyacentes.

- El espacio de acceso y de trabajo deben permitir el funcionamiento y el mantenimiento fácil y seguro.

- Para instalaciones en exteriores deben utilizarse encerramientos adecuados para protección contra contacto accidental, manejo de personal no autorizado, tráfico y operación de vehículos; grúas y contra fugas de líquidos y vapores.

Ilustración 3.6 Tablero de Distribución

FUENTE: Data Center ESPE

Medición del voltaje en el tablero de distribución

En la tabla 3.48 y la ilustración 3.7 se indica las medidas del voltaje del tablero de distribución.

Tabla 3.48 Voltajes del tablero de distribución Data Center ESPE

Fase	Medido	Multímetro Digital
1	204,9 V	205,3 V
2	208,3 V	208,9 V
3	209,1 V	209,6 V

Ilustración 3.7 Voltajes del Tablero de Distribución amperímetro digital

FUENTE: Data Center ESPE

Medición del amperaje en cada fase (tal como se indica en la tabla 3.49**):**

Tabla 3.49 Medición de Amperios en cada fase (3fases)

Fase	Pinza Amperimétrica
1	126 A
2	137,6 A
3	128 A

Cabe recalcar que el tablero de distribución cuenta con un TVSS; es un supresor de picos, dispositivo protector contra sobretensiones (elevaciones de voltaje), tal como se muestra en la ilustración 3.8.

Ilustración 3.8 TVSS supresor de Picos del Data Center ESPE

FUENTE: Data Center ESPE

Gráfico de Acometidas dentro y fuera del Data Center

Las acometidas desde los generadores hasta el Data Center se indican en la ilustración 3.9.

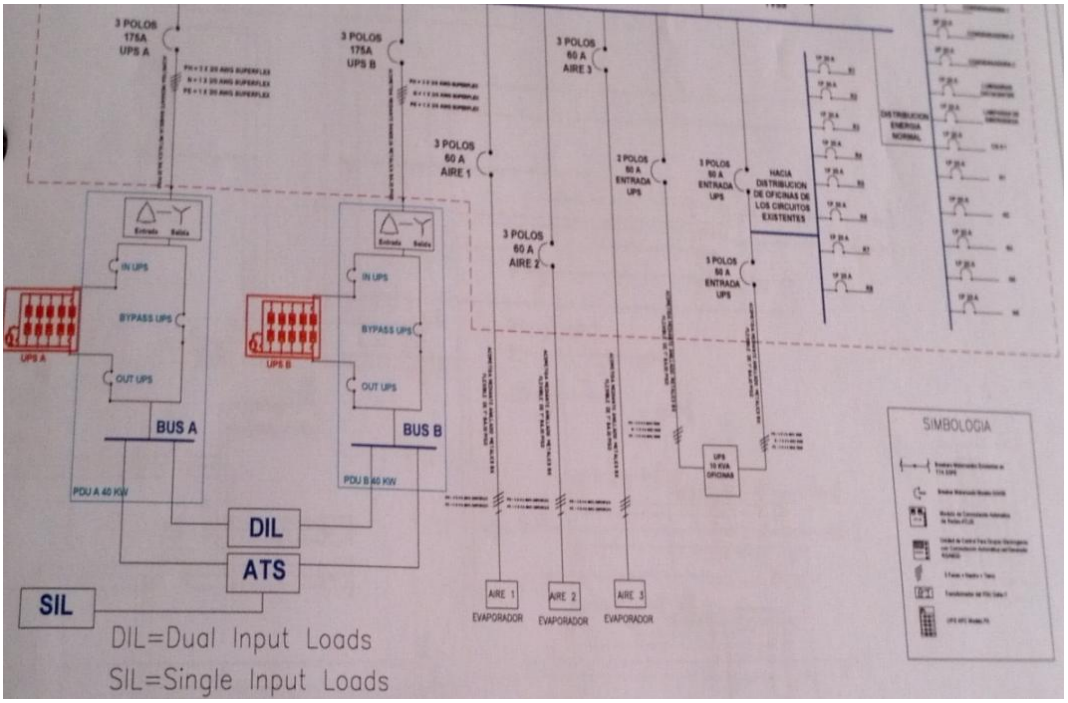


Ilustración 3.9 Gráfico de acometidas desde los generadores hasta el Data Center ESPE

Fuente: Memoria técnica Data Center ESPE

UPS

Es el sistema de alimentación ininterrumpida; cuenta con baterías internas que almacenan energía. Este dispositivo proporciona energía en caso de emergencia y cuando el generador eléctrico del Data Center de la ESPE falle o no haya energía eléctrica por parte de la Empresa Eléctrica de Quito.

Configuraciones y monitoreo de los UPS´s con los que cuenta el Data Center de la ESPE:

Este Data Center cuenta con dos UPS APC modelo SY30K40F con redundancia N+1; estos UPS cuentan con la tecnología SAI (ilustración 3.10).

Ilustración 3.10 UPS Data Center ESPE

FUENTE: Data Center ESPE

A continuación se observan las configuraciones y mediciones de uno de ellos. El monitoreo de estos se realiza con el programa en red InfraStruXure Central. Tal como se indica en la ilustración 3.11.

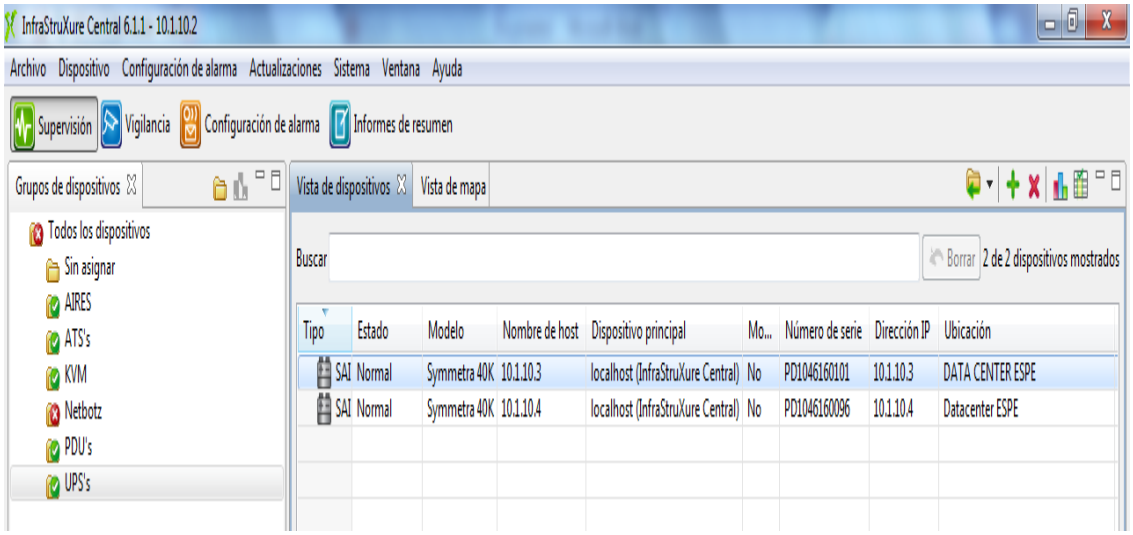


Ilustración 3.11 Monitoreo UPS Software InfraStruXureCentrel

FUENTE: Redes y Comunicaciones UTIC

En la ilustración 3.12 están descritos los eventos, acontecimientos o errores:

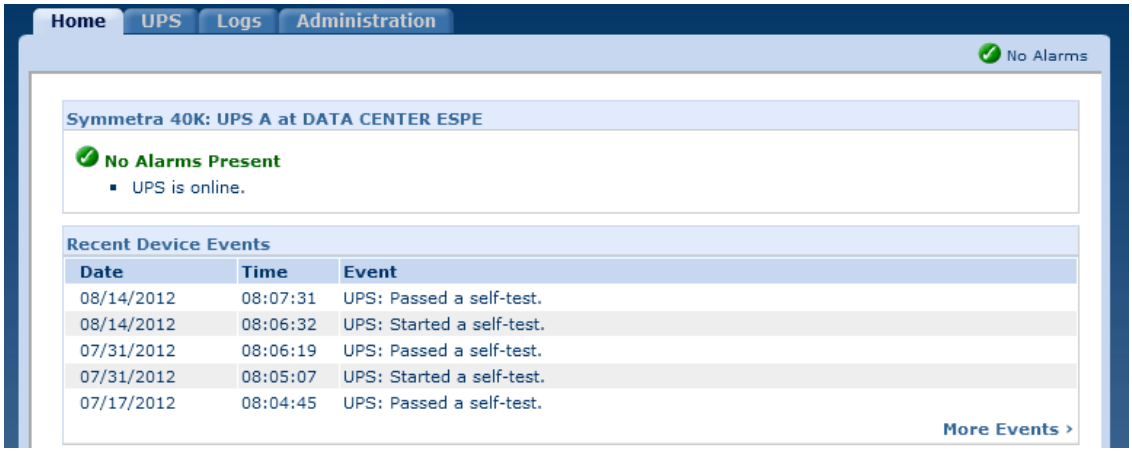


Ilustración 3.12 Monitoreo de Eventos o Errores del UPS A

FUENTE: Redes y Comunicaciones UTIC

En las ilustraciones 3.13, 3.14 y 3.15 se evidencia el nivel de carga en watts del UPS, el estado de la batería, los voltajes de entrada y de salida en cada una de las fases y el tiempo que soportaría o abarcaría a los equipos, en caso de interrupción de energía, en este caso 20 minutos.

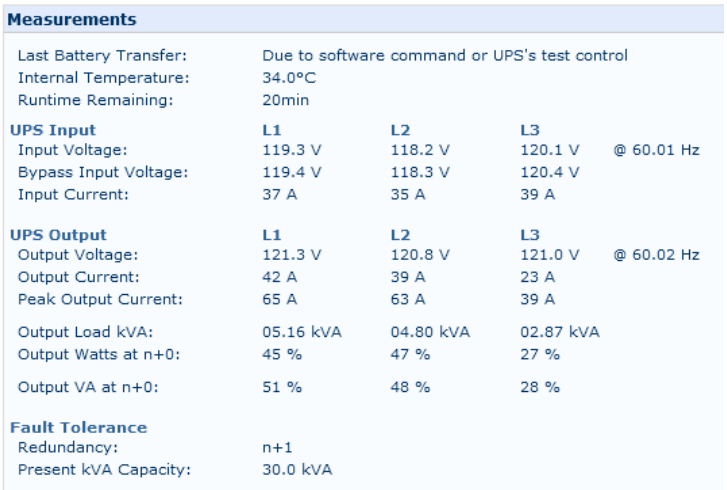


Ilustración 3.13 Monitoreo de mediciones UPS, Data Center ESPE

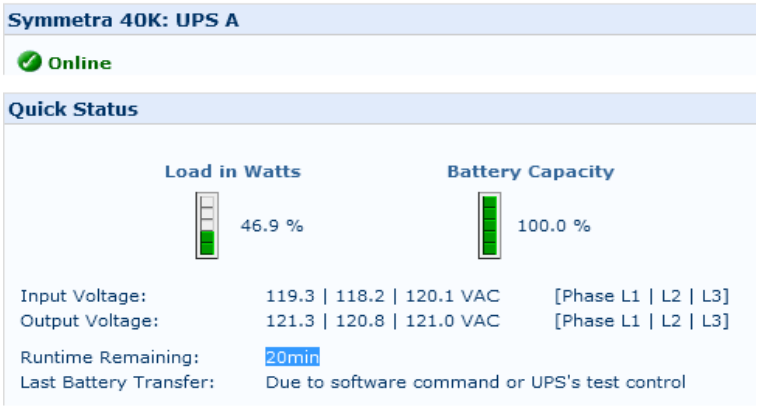


Ilustración 3.14 Monitoreo carga Data Center ESPE

Ilustración 3.15 Monitoreo Status de Módulos de Poder

FUENTE: Redes y Comunicaciones UTIC

ATS:

Este dispositivo es un interruptor que reconecta la fuente de energía principal, este caso es el Data Center de la ESPE, con las acometidas a una fuente de reserva o backup, igualmente en este caso, a los UPS.

Un interruptor de transferencia automática o ATS por lo general se encuentra instalado en un generador de reserva, de manera que el generador pueda proporcionar energía eléctrica temporal si falla la fuente de energía principal.
El Data Center de la ESPE cuenta con seis ATS marca APC, que permiten redundancia en equipos de fuente simple. Como se indica en la ilustración 3.16.

Ilustración 3.16 ATS Data Center ESPE

FUENTE: Data Center ESPE

Además, la ESPE tiene un generador eléctrico de emergencia marca CUMMINS modelo c110 de 140 KVA, exclusivamente para el Data Center.

Monitoreo del ATS:

En las ilustraciones 3.17 y 3.18 presentan como está configurado el ATS monitoreado, desde el software propietario de APC. Se describe la ip, los UPS que controla, su tiempo de actividad; además se lo puede configurar desde el software.

Ilustración 3.17 Monitoreo ATS

FUENTE: Redes y Comunicaciones UTIC

Ilustración 3.18 Configuración ATS desde software propietario

FUENTE: Redes y Comunicaciones UTIC

PDU:

Es la unidad de distribución de energía; este dispositivo está equipado con múltiples salidas, diseñadas para distribuir la energía eléctrica.

El Data Center de la ESPE dispone de dos PDU marca APC, modelo PD40F6FK1-M, 22 PDU's verticales para rack, marca APC, modelo AP7530 y 10 PDU's, marca APC, modelo AP7541. Como se muestra en la ilustración 3.19.

Ilustración 3.19 PDU modelo PD40F6FK1-M

FUENTE: Data Center ESPE

3.11.2 Sistema de Iluminación

La iluminación es importante dentro del Data Center, ya sea para hacer trabajos dentro de él, en caso de vigilancia con las cámaras IP o CCTV y para detectar algún daño físico dentro de los equipos.

Dentro del Data Center de la ESPE se pudo constatar que cuentan con diez luminarias fluorescentes tipo T8 marca Narva, con difusor parabólico de 60x60cm, 3x17watts y sus medidas de lúmenes en la tabla 3.50.

Tabla 3.50 Valores medidos dentro del Data Center de la ESPE

Medidas de la distancia y nivel de iluminación
2,55 metros sobre piso falso
1000 lux

Con el luxómetro se comprobó que las luminarias garantizan y cumplen con los estándares de funcionamiento de la norma TIA-942 y BICSI 002, ya que deben ser mayores de 500 lux. En la ilustración 3.20 se indica las luminarias utilizadas por el Data Center ESPE.

Ilustración 3.20 Gráfico de las luminarias del Data Center

3.11.3 Sistema de conexión a tierra

Es un sistema de protección al usuario de los aparatos conectados a la red eléctrica. Consiste en una pieza metálica (electrodo) enterrada en suelo con poca resistencia y conectada a una malla.

En el caso de la ESPE, tiene un sistema de puesta a tierra en el patio exterior, como se muestra en las ilustraciones 3.21 y 3.22. Está constituido por seis varillas de cobre de 5/8” x 1,8 metros de diámetro con cable 2/0awg y zanjas de 30x50cm por donde pasa el cable.

Ilustración 3.21 Mallas para conexión a tierra
FUENTE: Memoria Técnica Data Center ESPE

Ilustración 3.22 Conexión a Tierra
FUENTE: Memoria Técnica Data Center ESPE

Todo el sistema eléctrico está conectado al sistema de puesta a tierra dentro del Data Center y bajo el piso falso, como se muestra en la ilustración 3.23, cumpliendo con el estándar NFPA-75.

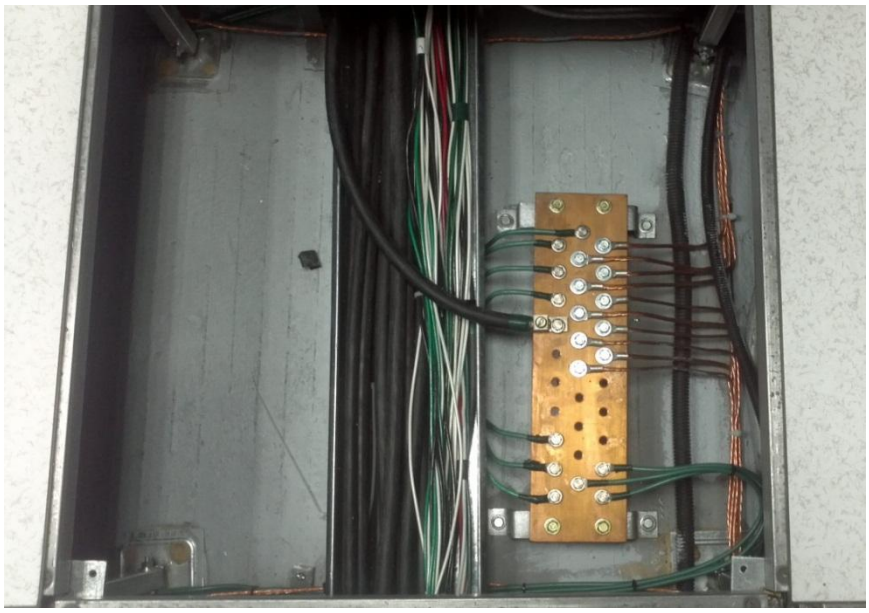


Ilustración 3.23 Conexión de puesta a tierra bajo piso falso

FUENTE: Data Center ESPE

3.11.4 Sistema de control de seguridad

El monitoreo que se realiza dentro del Data Center, se realiza por medio de cámaras IP; se dispone de tres cámaras en cada uno de los pasillos y la entrada principal. El monitoreo se realiza por medio de un computador y la dirección IP como se observa en la ilustración 3.24.

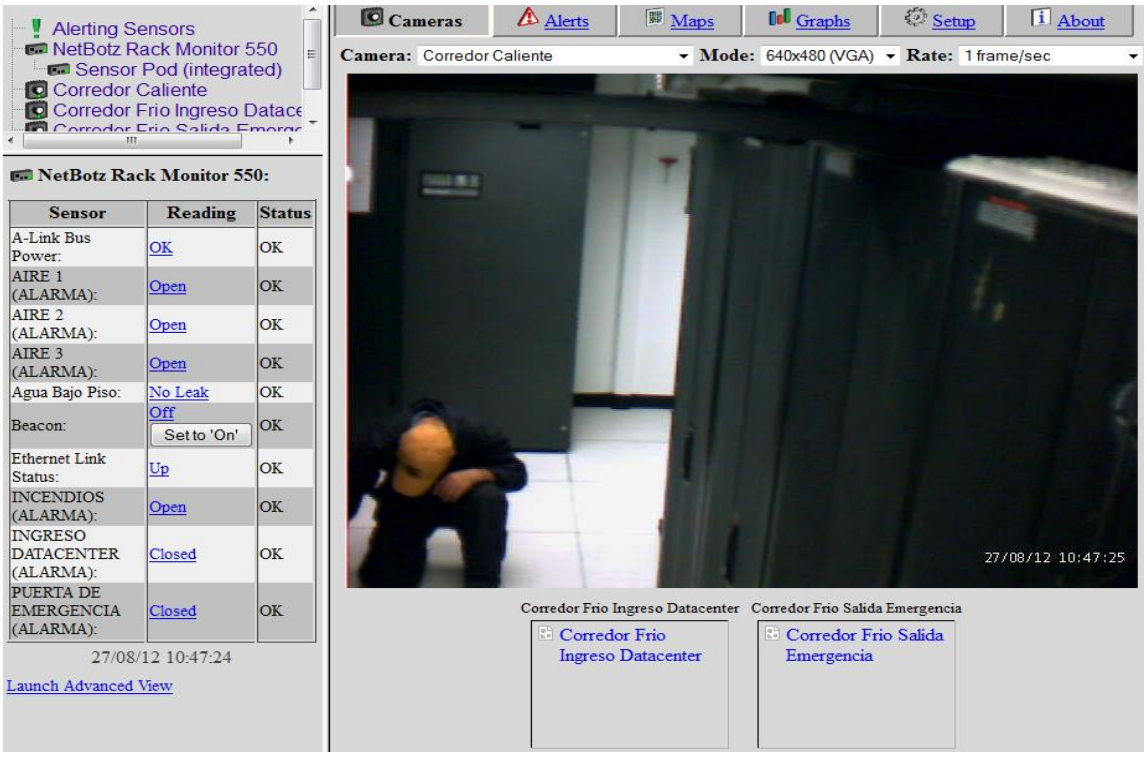


Ilustración 3.24 Monitoreo Cámaras IP

FUENTE: Redes y Comunicaciones UTIC

3.4.5. Accesos:

Para el acceso al Data Center de la ESPE se cuenta con dos puertas de acero; una para la entrada principal con blindaje y la otra puerta de salida de emergencia, cuando se suscite algún inconveniente.

Medidas de las puertas: En la tabla 3.51 los valores medidos de las puertas con los que cuenta el Data Center ESPE

Tabla 3.51 Medida de puertas del Data Center de la ESPE

Puerta	Largo	Ancho
Principal	2,20 m	1,01 m
Emergencia	2,20 m	0,93 m

El Data Center de la ESPE cuenta con dos puertas de acero, provistas de una película de pintura anti-inflamable.

Además posee un lector biométrico marca Bioscrypt para el acceso solo a personal autorizado con tarjetas magnéticas.

Cuenta con una aplicación remota que permite monitorear por unos sensores que lapso de tiempo, incluyendo la hora en que se abrió la puerta principal como se indica en la ilustración 3.25.

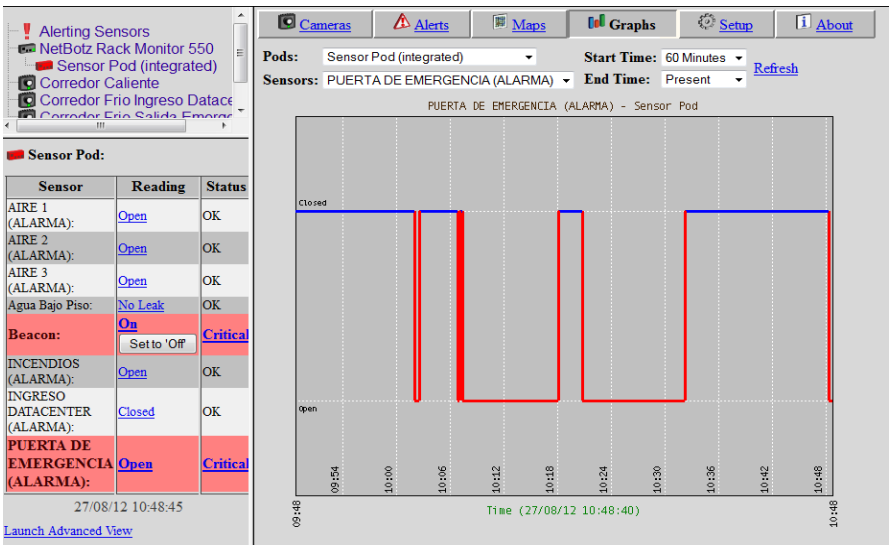


Ilustración 3.25 Monitoreo puertas de acceso

FUENTE: Redes y Comunicaciones UTIC

3.11.5 Sistema contra incendios

El Data Center posee un sistema de detección y extinción de incendios, el cual cuenta con: cinco sensores de humo ubicados estratégicamente dentro del Data Center; un sistema FM200 que descarga un gas no liquido; una alarma de incendios; y, cuatro luces de emergencia como se muestra en la ilustración 3.26.

Ilustración 3.26 Sistema Contraincendios

FUENTE: Data Center ESPE

Cabe recalcar que el Data Center ha sido construido con materiales no inflamables, según está descrito en las normas internas.

3.11.6 Señalética

El Data Center cuenta con dos letreros de salida en caso de emergencia; estos letreros tienen una batería en caso que se suspenda el suministro de energía eléctrica; de igual manera, cada uno de los equipos electrónicos está correctamente etiquetado con su nombre como se indica en la ilustración 3.27.

Para su funcionamiento estos productos se componen de aluminatos o acumuladores de luz que se componen de cristales en forma de polvo, incrustados en materiales altamente transparentes; son muy inofensivos y nada tóxicos.

Ilustración 3.27 Salidas de emergencia

FUENTE: Salidas de emergencia

3.11.7 Sistema de Aire acondicionado

El Data Center cuenta con tres sistemas de aire acondicionado: dos están en funcionamiento continuo (Marca STULZ modelo ASD211G, como se indica en la ilustración 3.29) y uno como reserva redundante. Para ofrecer refrigeración eficiente se debe eliminar el aire de bypass. Se utiliza los entornos con piso elevado (indicados en la ilustración 3.28) como lo tiene el Data Center de la ESPE, lo que proporciona mayores ahorros de energía.

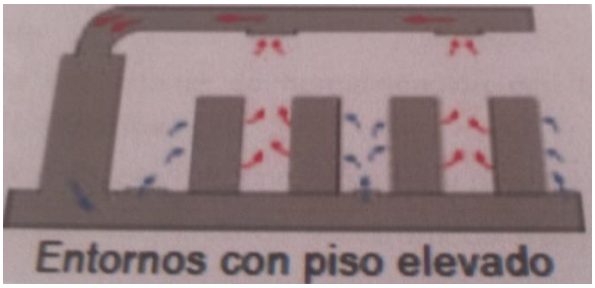


Ilustración 3.28 Entorno con piso elevado Data Center
FUENTE: Memoria técnica Data Center

Características de STULZ:

- Ofrecen la mayor capacidad de refrigeración utilizando la menor superficie (1m cuadrado).
- Reduce el nivel sonoro a 5dB.
- Condensación por aire, por agua glicolada o agua fría.
- Mantenimiento sencillo a través de un panel frontal.

Ilustración 3.29 Aire acondicionado Data Center ESPE
FUENTE: Data Center ESPE

Mediciones de temperatura y humedad

En la tabla 3.52 se muestran los valores obtenidos de la mediciones de temperatura y humedad.

Tabla 3.52 Mediciones temperatura y humedad del ambiente dentro del Data Center de la ESPE

A/C del Data Center de la ESPE	Temperatura	Humedad
Medición	23,2 C°	35,60%
Oscilación	5 C° por hora	

En la ilustración 5.30 se muestra el monitoreo por software del aire acondicionado.

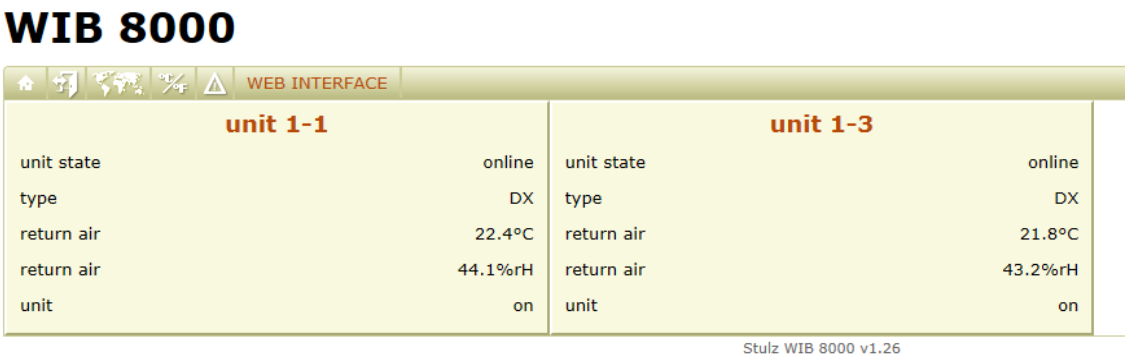


Ilustración 3.30 Monitoreo con Software con WIB 800

FUENTE: Redes y Comunicaciones UTIC

3.11.8 Piso falso

Como dato importante, el Data Center de la ESPE cuenta con 36 metros cuadrados de construcción, en el primer piso del Edificio Central.

La distancia de la loza con respecto al piso falso es de 30cm, para que por allí pase el cableado horizontal y no existan filtraciones de agua como se muestra en las ilustraciones 3.31 y 3.32.

Ilustración 3.31 Conexión Cableado Estructurado bajo piso falso

FUENTE: Data Center ESPE

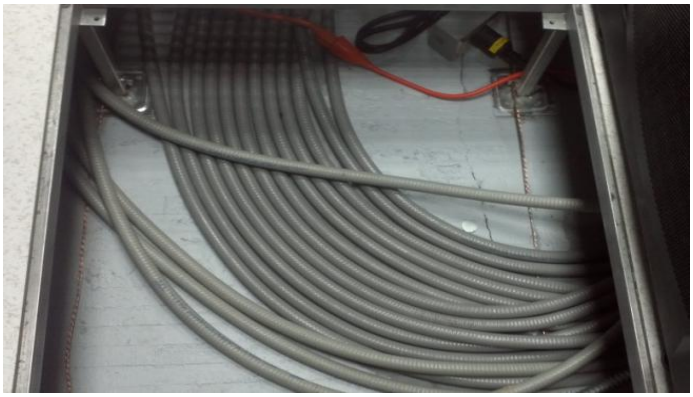


Ilustración 3.32 Cableado estructurado bajo Piso Falso Data Center

FUENTE: Data Center ESPE

El piso falso está constituido por baldosas independientes y removibles en metal como se indica en la ilustración 3.33; de dimensiones variables y recubiertas de un revestimiento plástico. Las baldosas reposan sobre soportes de altura de 30cm. El piso falso soporta más de 250 lb/ft (cuadrado).

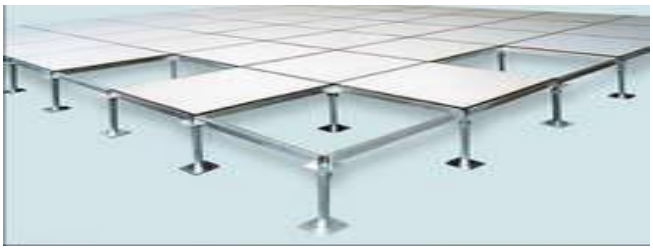


Ilustración 3.33 Piso Falso Marca ASM y paneles FS100

FUENTE: ENERBOZ

3.11.9 Red Interna

Como se puede observar en el siguiente gráfico se muestran todas las conexiones de fibra óptica y su distribución dentro del Data Center; como complemento se analizan las características del switchcore que está siendo utilizado como backbone.

A continuación la tabla 3.53 con las características del switch Cisco 6500:

Tabla 3.53 Características Switch Core Data Center ESPE

Característica	**Cisco Catalyst 6500 Series**
Configuraciones de Chasis	• 9-slot
Ancho de banda del Backplane	• 256-Gbps switch fabric
Tres niveles de rendimiento y de renvío	• Catalyst 6500 Supervisor Engine 2 MSFC2: hasta 210 Mpps
Sistema Operativo	• Cisco Catalyst OS
Supervisión de Motores Redundantes	Sí, con reconexión dinámica
Componentes redundantes	• Fuentes de alimentación (1 +1) • Conectar tela (1 +1) • Reloj reemplazable • Bandeja de ventilador reemplazable
De alta disponibilidad	• Load Balancing Protocolo de puerta de enlace • Hot Standby Router Protocol (HSRP) • multimódulo tecnología EtherChannel • Rapid Spanning Tree Protocol (RSTP) • Multiple Spanning Tree Protocol (MSTP)
Módulos de servicios avanzados	• Servicios de Contenido de puerta de enlace • CSM • Módulo Corta Fuegos • IDS módulo • Seguridad IP (IPSec) VPN módulo • Red módulo de análisis

	• Dispositivo de almacenamiento persistente • Módulo SSL • LAN inalámbrica módulo de servicios

FUENTE: Cisco Catalyst 6500 y 6500-E Series Data Sheet

Un escenario propuesto para la implementación se indica en la ilustración 3.34.

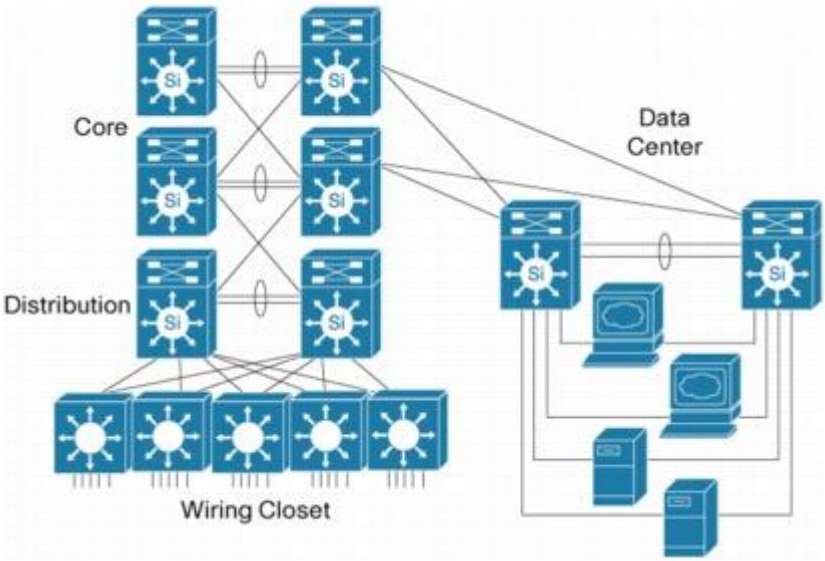


Ilustración 3.34 Situación de implementación de redes dentro de un campus

FUENTE: Cisco Catalyst 6500 y 6500-E Series Data Sheet

Las características de este modelo son:

- Módulos autosending de 10/100Mbps y 10/100/1000Mbps que proporcionan alimentación en línea para el armario del cableado.
- Robustas características de alta disponibilidad, seguridad y capacidad de administración.
- Software de clase mundial de redes.
- Interfaz de red con módulos de hasta 10 gigabit.
- Gestión de red de distribución y núcleo.

El cableado de fibra óptica del Data Center de la ESPE está distribuido de tal forma que se asemeja a la implementación propuesta en el DataSheet de Cisco Catalyst, manteniéndolo con las características mencionadas anteriormente. El gráfico de red se indica en la ilustración 3.35.

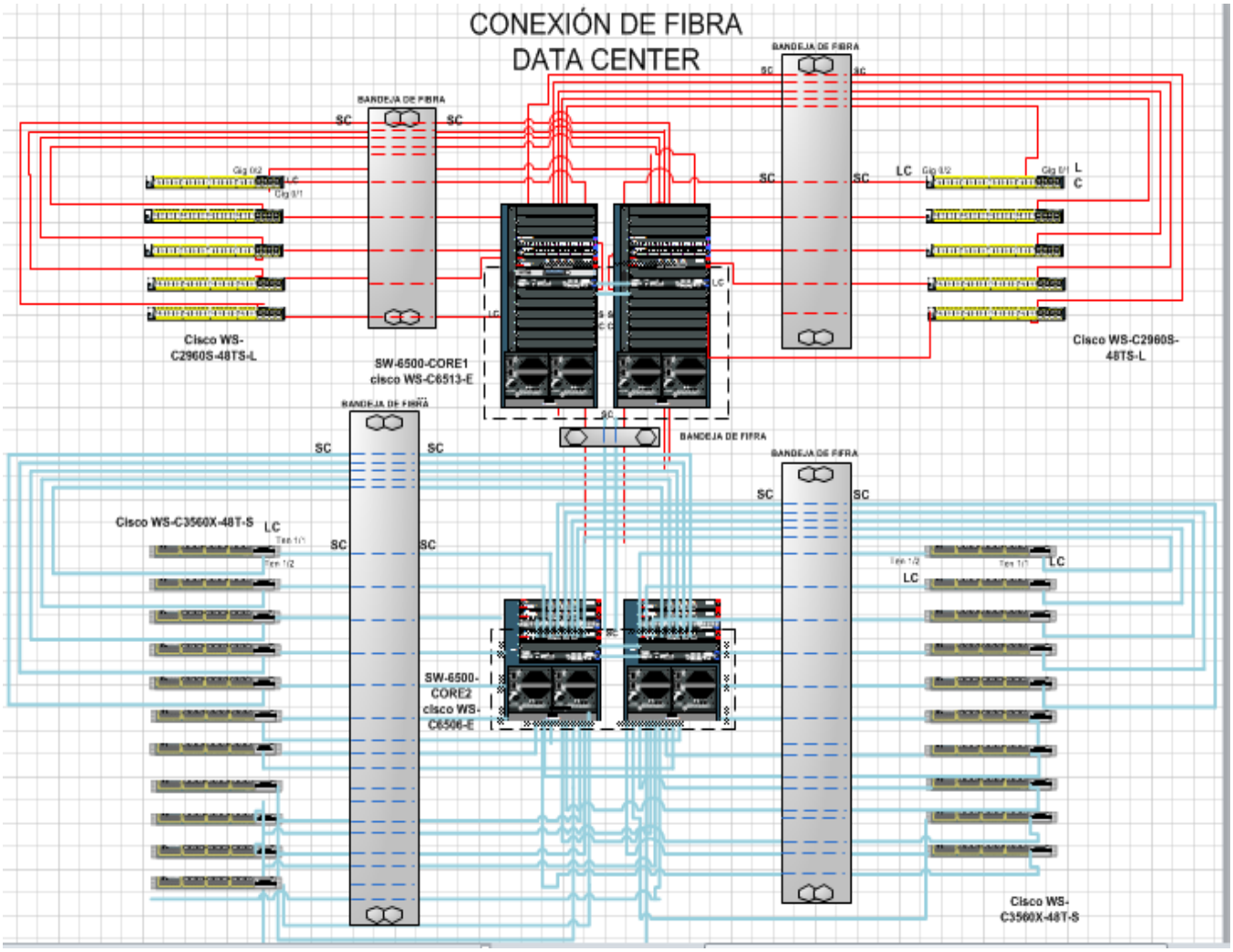


Ilustración 3.35 Conexión de fibra óptica dentro del Data

FUENTE: Redes y Comunicaciones UTIC

De acuerdo con el cumplimiento de la norma ecuatoriana NEC-10:

- Se verificó que el Data Center tiene sus cables de energía dentro de tuberías no metálicas.
- No se observó cables sueltos, lo cual previene cortocircuitos.
- Se comprobó que tiene 30 cm de separación de la loza hacia el piso falso.

Cumpliendo con las normas BICSI 002 y ISO-IEC 24764 para cableado dentro del Data Center se estima lo siguiente:

- Mínimo canal de cobre Categoría 6 A.
- Utilizar fibra óptica de calidad láser optimizada OF300 (OM3), con lector LC y conector MPO de dos fibras.
- La red debe tener realizado un trunking.
- Soportar 10 GBASE-T.
- El cableado de 10 GBASE-T no debe sobrepasar la longitud de 15m.

3.11.10 Valoración del Data Center según Uptime Institute Data Center TIER

El Data Center ESPE tiene características tanto de TIER I cuanto de TIER II. Se nombran a continuación:

- TIER I:
    - Una vía de distribución no redundante (un solo generador un solo tanque de combustible).
    - Un solo proveedor, una sola ruta de cableado y no cuenta con redundancia en equipos críticos.
    - PDU y paneles de distribución.
    - El generador debe tener una capacidad apropiada para soportar los UPS.
    - Monitoreo por cámaras IP, CCTV opcional.

- TIER II:
    - Protección mínima a eventos críticos.
    - Puertas de Seguridad.
    - UPS redundante (N+1).
    - Aire Acondicionado Redundante.
    - Sistema de detección de fugas de agua (Sensores).

3.11.11 Software propuesto para la optimización del monitoreo de los elementos del Data Center

IPHost Network Monitor: Monitor de Redes de Servidores IP

Ofrece una interfaz muy amigable con el usuario; detecta automáticamente las redes dentro de un rango de IPs como se indica en la ilustración 3.36. Cuando se ha encontrado la IP de un servidor, se puede realizar el monitoreo del mismo, con todos los sensores que ofrece el programa.

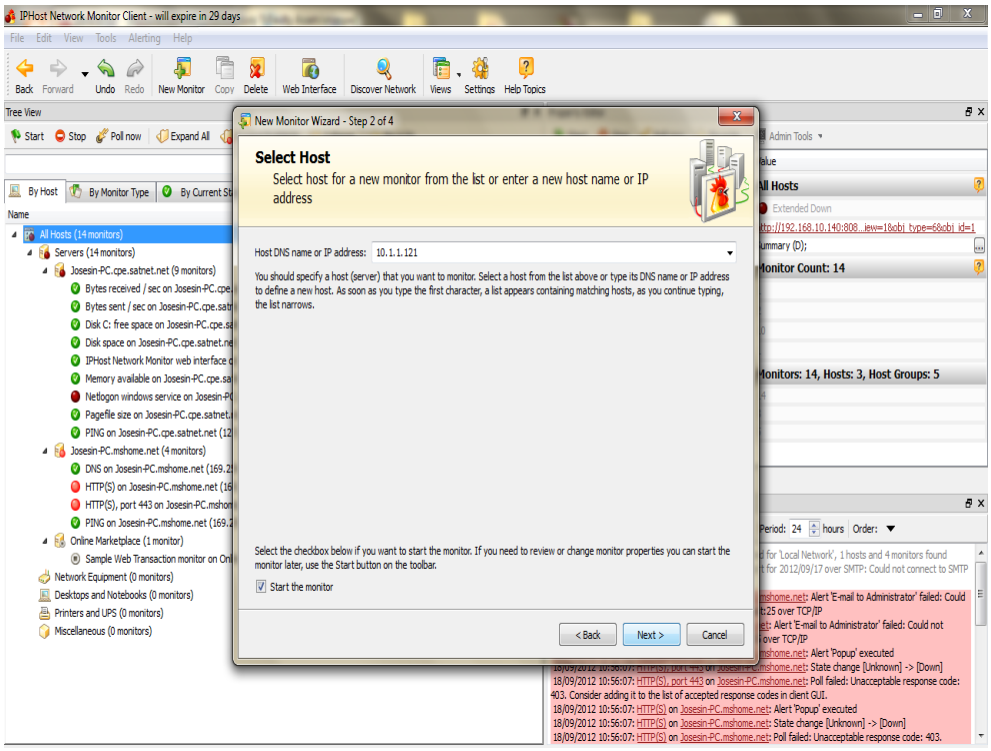


Ilustración 3.36 Selección de Host a ser monitoreado

En la ilustración 3.37 es posible evidenciar cuántos host están conectados a la red en ese momento y cuántos de ellos están disponibles; también diferencia los que son servidores de los terminales normales. En la parte derecha se puede observar un reporte en el que se resumen: los host que han respondido a los sensores del programa y el rendimiento de los sensores.

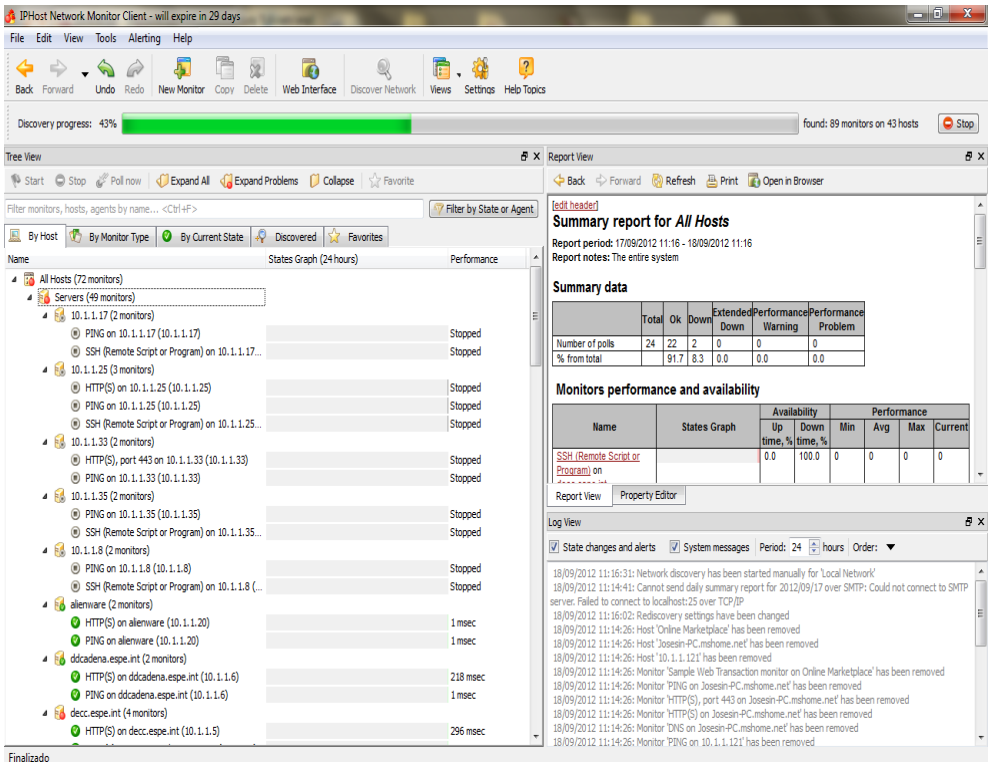


Ilustración 3.37 Host Monitorizados y Reporte de los mismos

Los reportes también pueden ser observados en la interfaz web. Tienen la posibilidad de enviar los resultados al mail del administrador o imprimirlos para su respectivo análisis. En la parte izquierda hay un árbol de navegación y reportes por host, como se muestra en la ilustración 3.38.

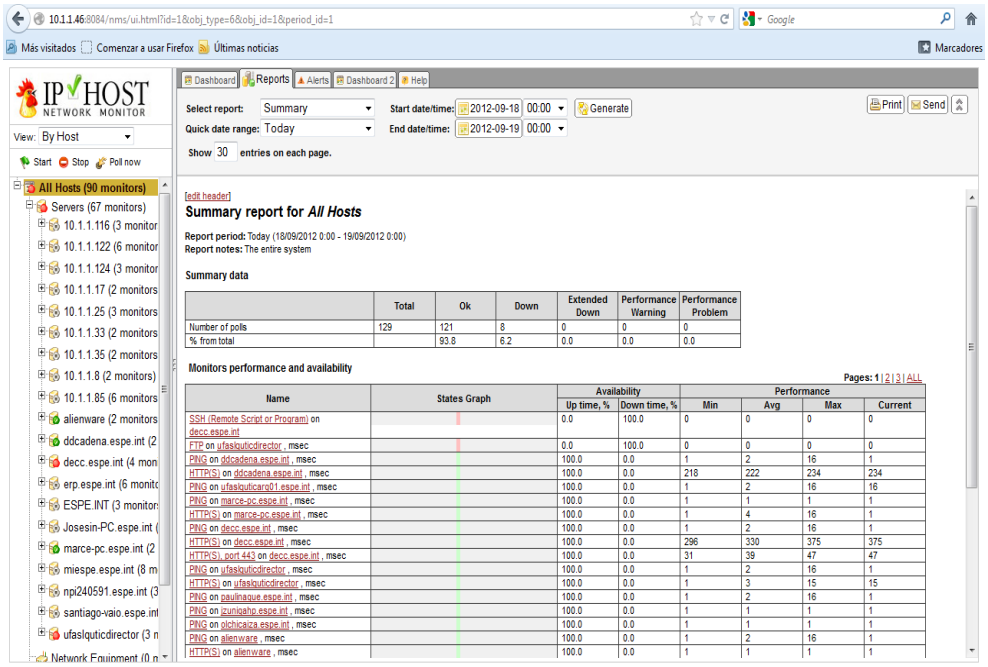


Ilustración 3.38 Interfaz Web Reportes IP Host Monitor

Como se mencionó en las características que la aplicación, existe la posibilidad de observar los resultados de los sensores sobre los host en forma de gráficos en un intervalo de tiempo.

A continuación en las ilustraciones 3.39 y 3.40 se muestran resultados gráficos de dos sensores:

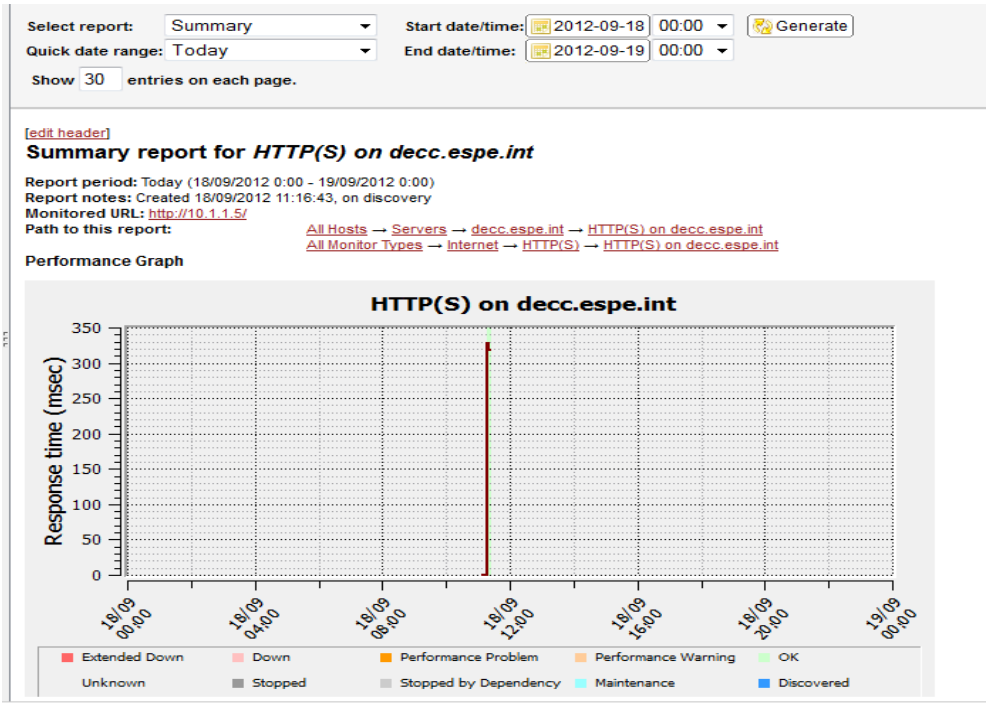


Ilustración 3.39 Gráfico Sensor HTTP

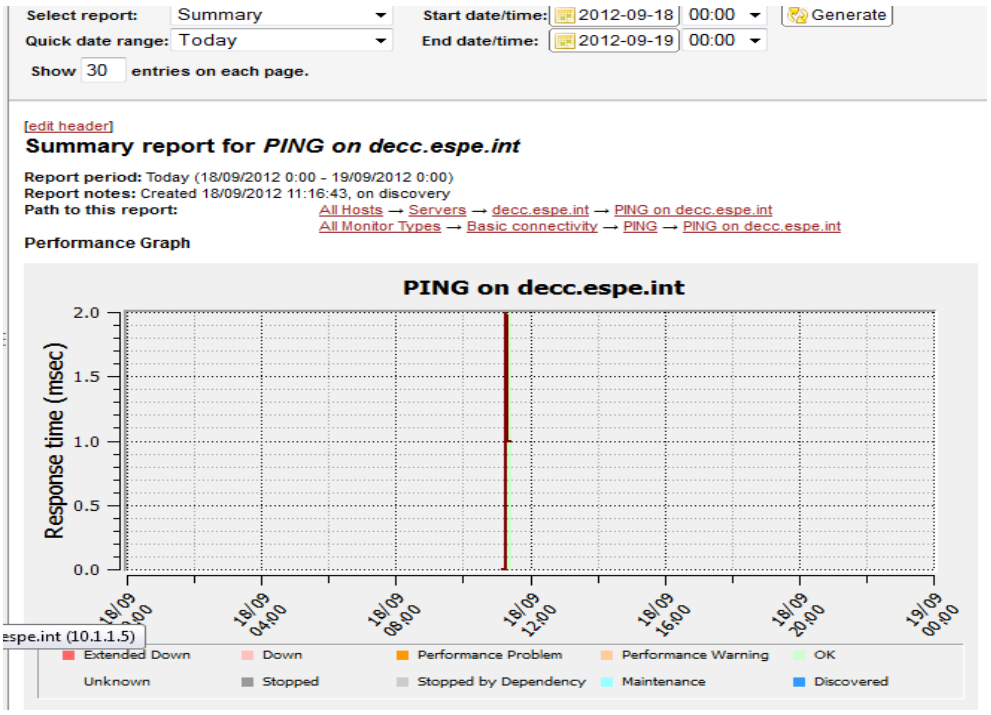


Ilustración 3.40 Gráfico Sensor PING

Cada sensor tiene sus tablas de rendimiento que se muestran en la ilustración 3.41.

Performance and Availability Summary (with Trend Data)

Name	States Graph	Availability		Performance, msec			
		Up time, %	Down time, %	Min	Avg	Max	Current
Base period		100.0	0.0	31	36	47	32
Previous period		0.0	0.0	0	0	0	
Change		100.0	0.0	31	36	47	

States Log

State	From	To
Unknown	17/09/2012 11:30:00	18/09/2012 11:16:44
Ok	18/09/2012 11:16:44	18/09/2012 11:29:03

States Summary

State	Time	
	Hours	%
Extended Down	0.0	0.0
Down	0.0	0.0
Performance Problem	0.0	0.0
Performance Warning	0.0	0.0
Ok	0.2	100.0

Ilustración 3.41 Tabla de rendimiento por sensor

Las alarmas ayudarán a tener una visión de lo que no está funcionando correctamente dentro de la red como se muestra en la ilustración 3.42; esto permitirá buscar una solución en el menor tiempo posible.

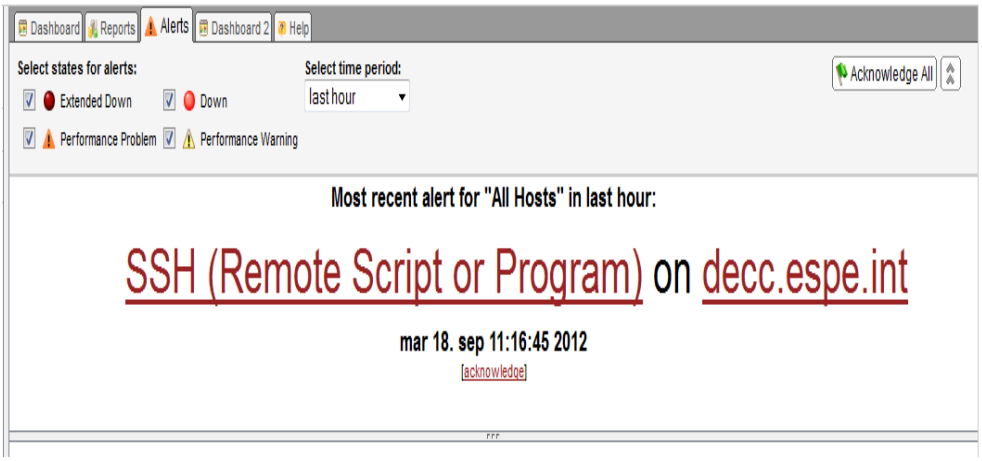


Ilustración 3.42 Alerta SSH

En la ilustración 3.43 se muestran las propiedades del sensor HTTP(S) aplicado a decc.espe.int por el puerto 443; también se pueden visualizar las siguientes características:

- IPs

- Método de Request

- Propiedades del Servidor Proxy

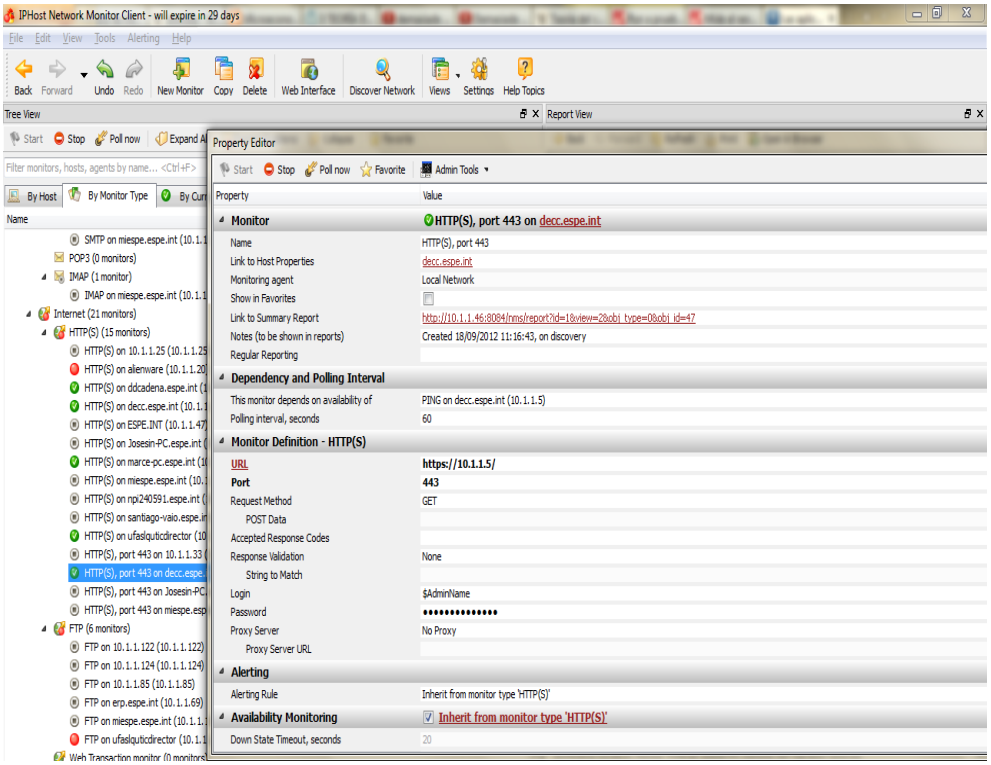


Ilustración 3.43 Propiedades del Sensor HTTP(S)

Red Eyes: Herramienta de verificación y monitoreo de host remoto

Con una interfaz sencilla para su uso, Red Eyes ofrece la capacidad de construir un rango de IPs para realizar un Ping y ver cuántos de los equipos responden en la red. Se monitoreó el rango de direcciones IPs 10.1.1.1-124, como se indica en la ilustración 3.44.

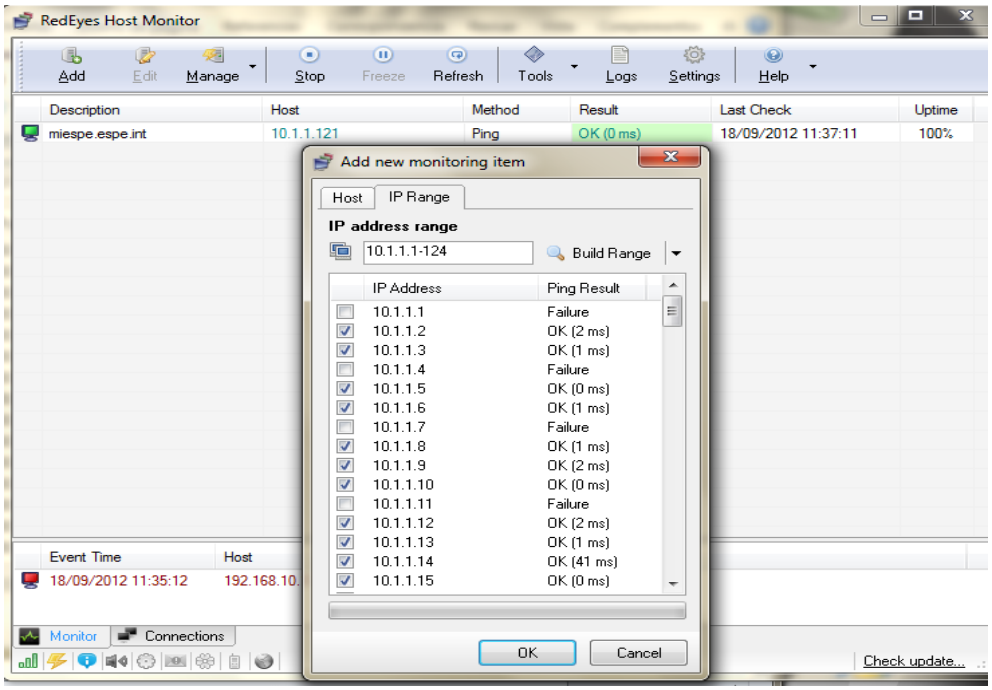


Ilustración 3.44 Monitoreo de un Rango de Direcciones IP ESPE

El programa identifica mediante el sensor Ping, el nombre de cada uno de los terminales con su respectiva IP; en algunos casos, determina el DNS de la IP, como se indica en la ilustración 3.45.

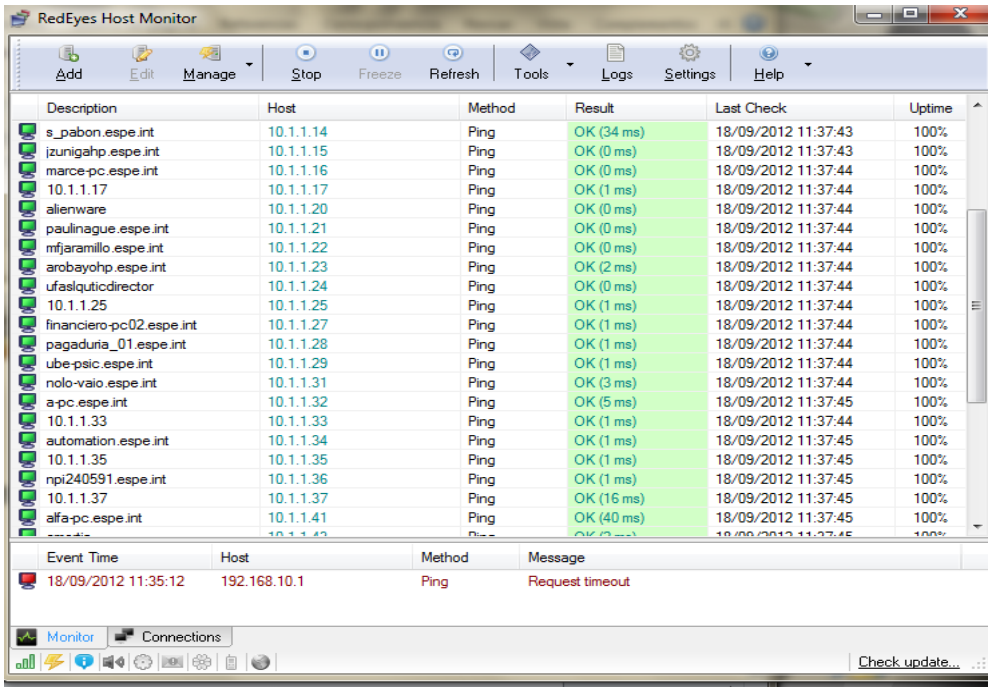


Ilustración 3.45 Identificación de DNS de cada IP

Mediante un algoritmo interno el programa identifica los puertos que están siendo utilizados por cada IP, lo cual ayuda a que los datos de los puertos sean muy fidedignos. En la ilustración 3.46, se identifican los puertos de miespe.espe.int.

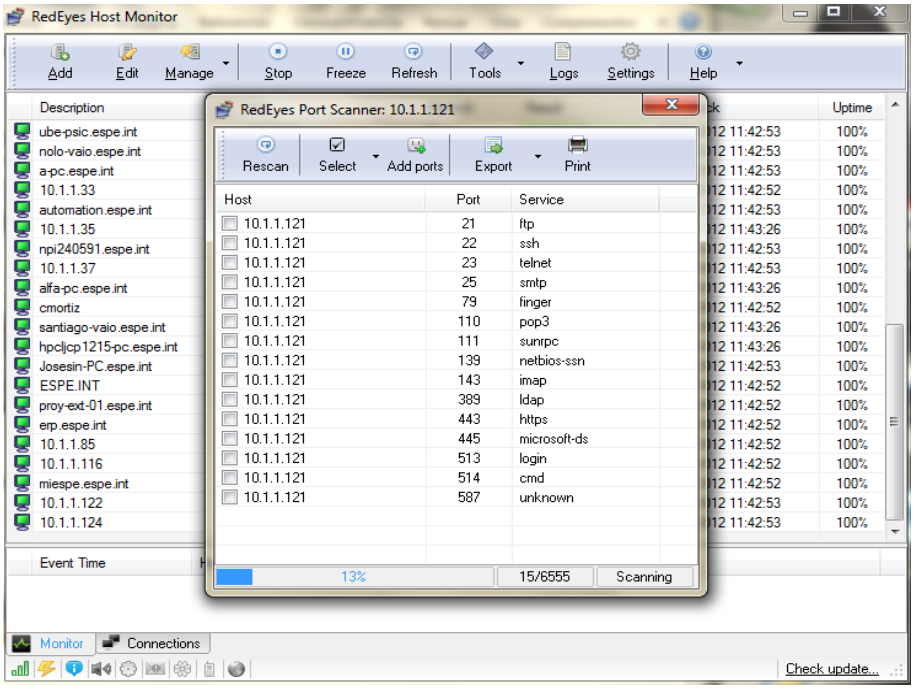


Ilustración 3.46 Identificación de Puertos por IP

La ruta que sigue la traza hasta llegar a la dirección miespe.espe.int, es otra funcionalidad del programa que describe la llegada hasta con un máximo de saltos y el tiempo, como se indica en la ilustración 3.47.

Ilustración 3.47 Seguimiento de la Traza hasta una dirección IP

Por último, existe la funcionalidad de conexión a cualquier dirección IP, ya que el programa puede utilizar un servidor FTP para realizar dicha conexión.

En la ilustración 3.48 se muestra la conexión a miespe.espe.int que tiene la dirección IP: 10.1.1.121.

Ilustración 3.48 Conexión por servidor FTP

NetCrunch: Monitorización de Red

Como se mencionó anteriormente es un software de monitoreo de red; la utilización de este programa es fácil por su amigable interfaz. Como primer paso, NetCrunch realizará un atlas de la red por medio de las IP´s de cada nodo; tiene la capacidad de formar un diagrama con equipos terminales de toda la red, esto se indica en la ilustración 3.49.

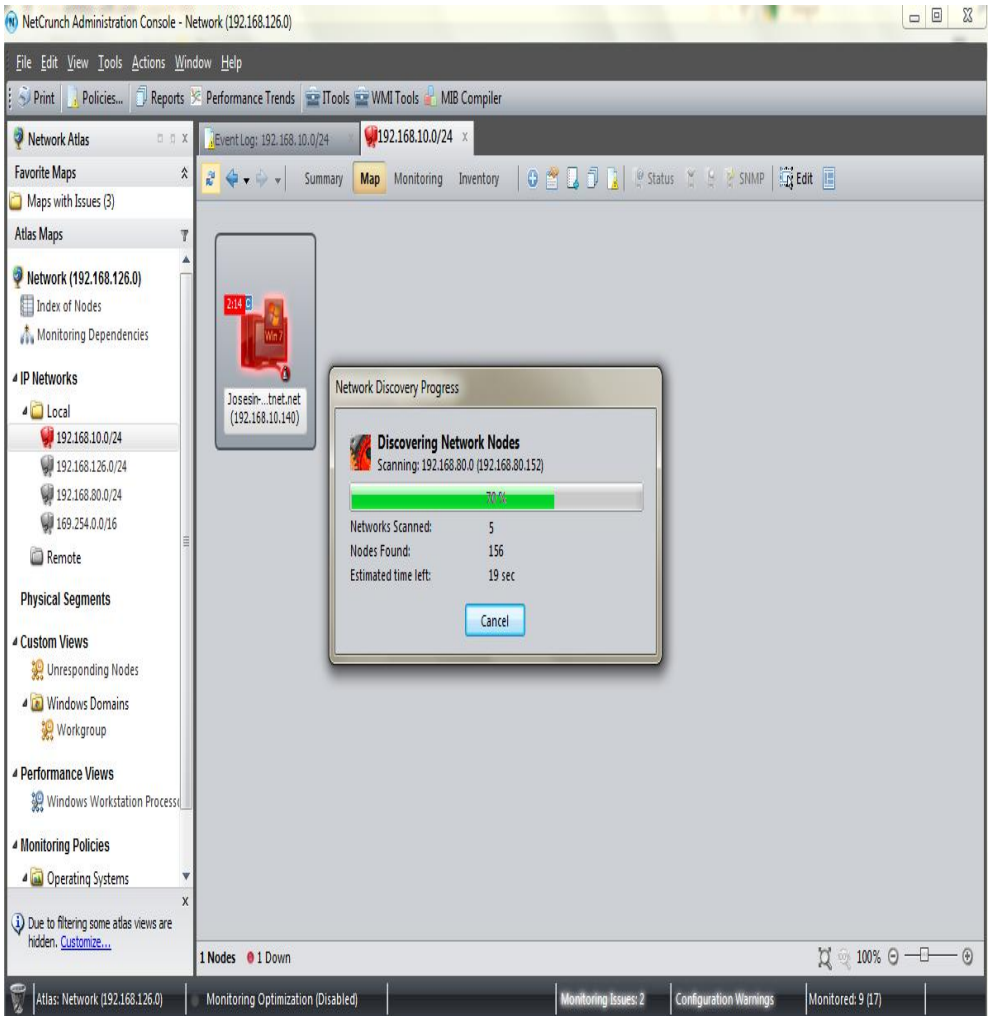


Ilustración 3.49 Descubrimiento automático de los Nodos de la Red

Una vez que ya descubrió cada nodo de la Red, crea un atlas. Para que el atlas sea concluido hay que realizar algunos pasos secuenciales que se describirán a continuación:

Lo primero es escoger si se desea distinguir todos los nodos en nuestro atlas de red, como por ejemplo: servidores, estaciones de trabajo y servicios de red. En la ilustración 3.50 se muestra el atlas que realiza el programa.

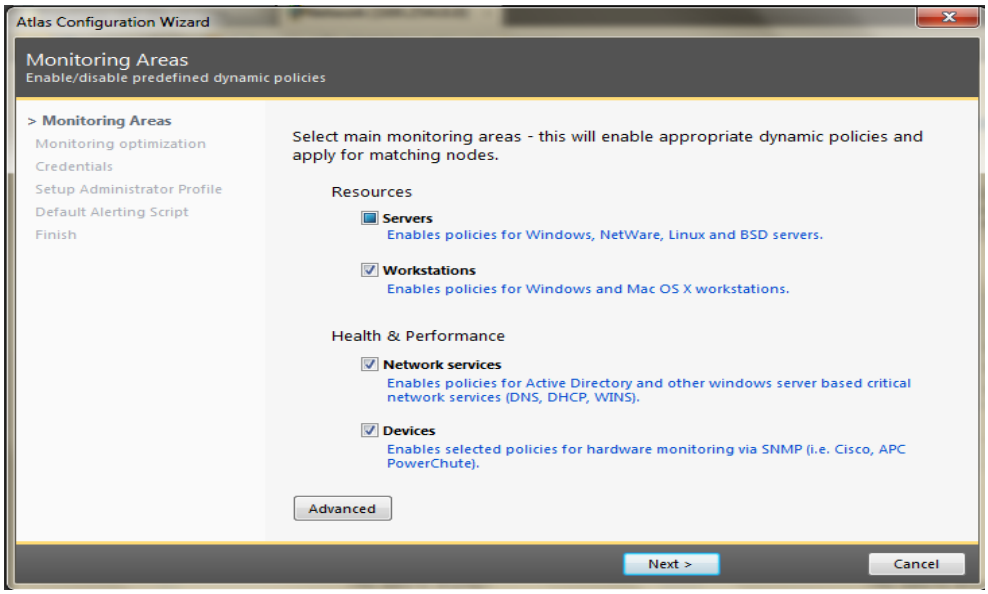


Ilustración 3.50 Selección de Nodos a graficarlos en el Atlas de Red

La siguiente opción es escoger un monitoreo extensivo de los nodos para que ningún dispositivo se quede sin ser monitoreado, como se muestra en la ilustración 3.51.

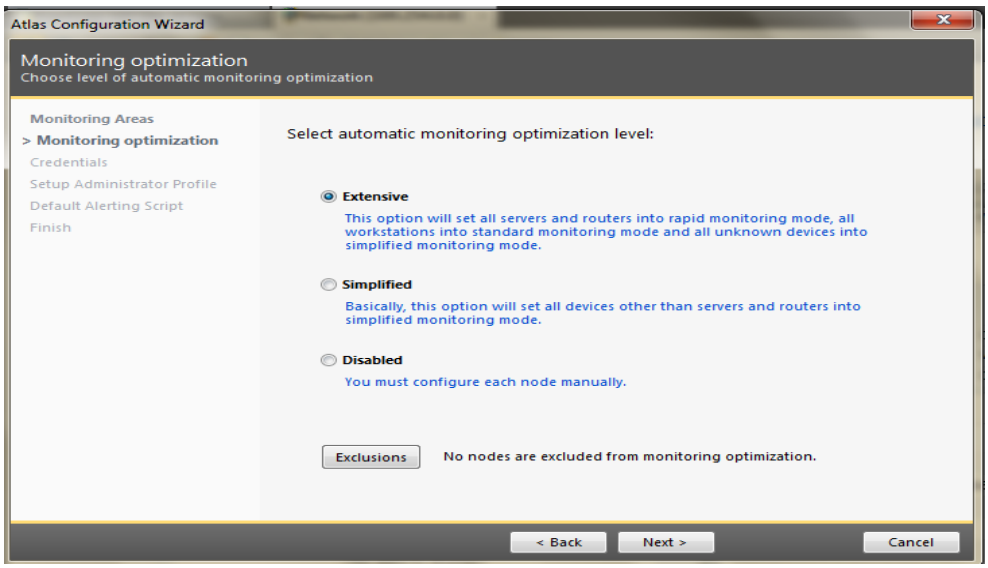


Ilustración 3.51 Selección Monitoreo Extensivo

El resultado de la creación del atlas de red, será un gráfico con equipos terminales en los que se describe: el sistema operativo de cada terminal, la dirección IP y el DNS.

Como resultado se tiene un mapa de la red. Para este caso la red monitoreada es la 10.1.0.0/23. Como se indica en la ilustración 3.52.

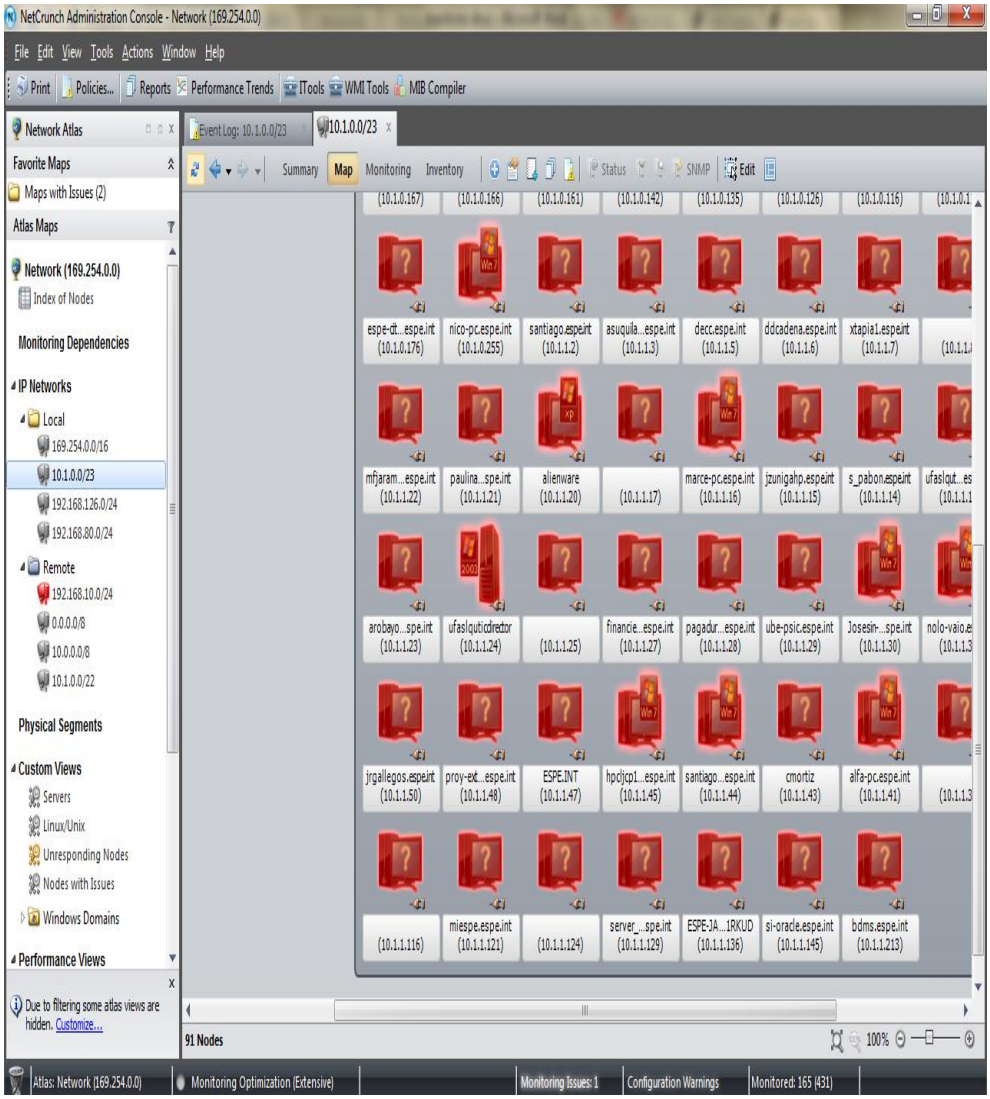


Ilustración 3.52 Atlas de la Red 10.1.0.0/23

La ilustración 3.53 es muy interesante ya que muestra cada uno de los servidores que se identificaron dentro de la red, con sus respectivas conexiones, sistemas operativos y direcciones IP.

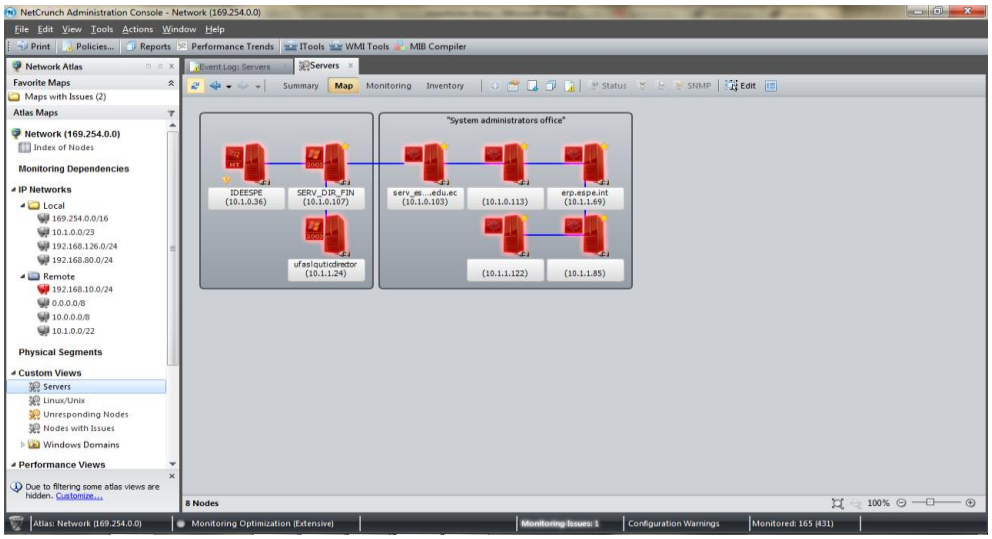


Ilustración 3.53 Servidores Identificados en la Red

Cada servidor tiene sus propias funcionalidades. Por esta ocasión se va a monitorear el serv_espe_s.espe.edu.ec.

Lo que primero salta a la vista en la ilustración 3.54 es un resumen de todos lo componentes de ese servidor.

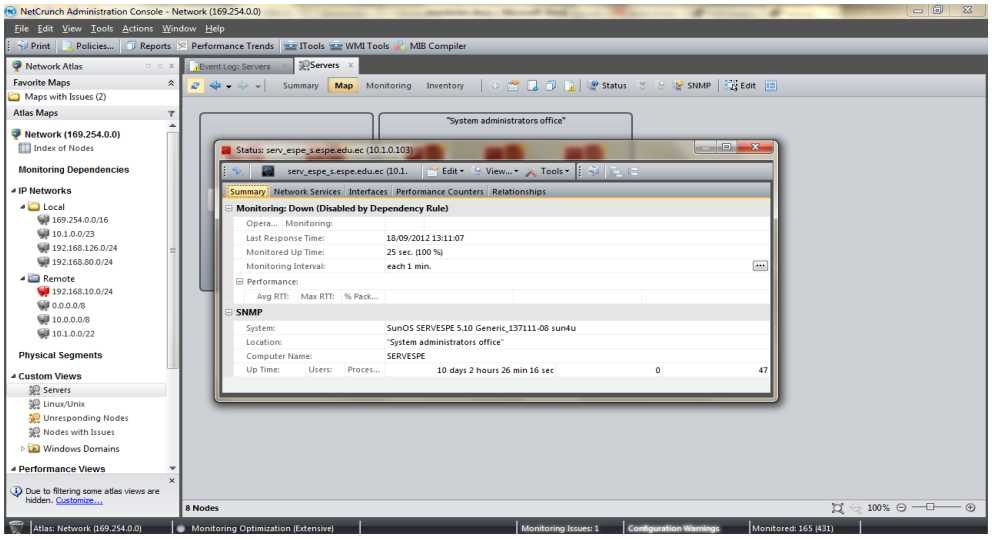


Ilustración 3.54 Resumen de componentes del Servidor

En la segunda pestaña se mostrarán los servicios que proporciona dicho servidor por la red. En este caso se encuentran inactivos, esto sucede debido a la protección que tienen los servidores de la ESPE ante atacantes externos. Es digno de relevar la manera de proteger todos los activos de la organización ya sean equipos, datos críticos, otros. Como se muestra en la ilustración 3.55.

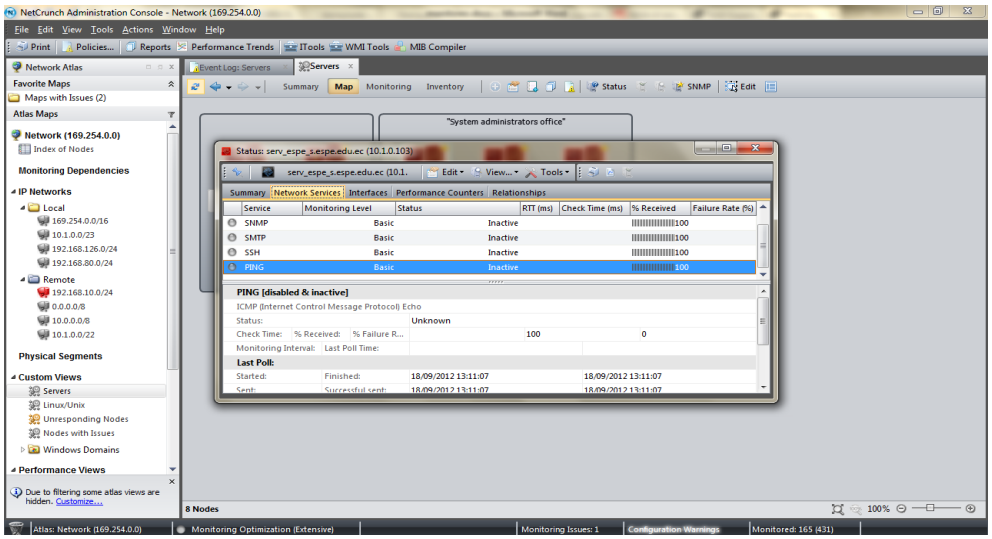


Ilustración 3.55 Servicios en Red del Servidor

Existen funcionalidades extras del software. En la siguiente pestaña se muestran las interfaces del servidor. Esto se indica en la ilustración 3.56.

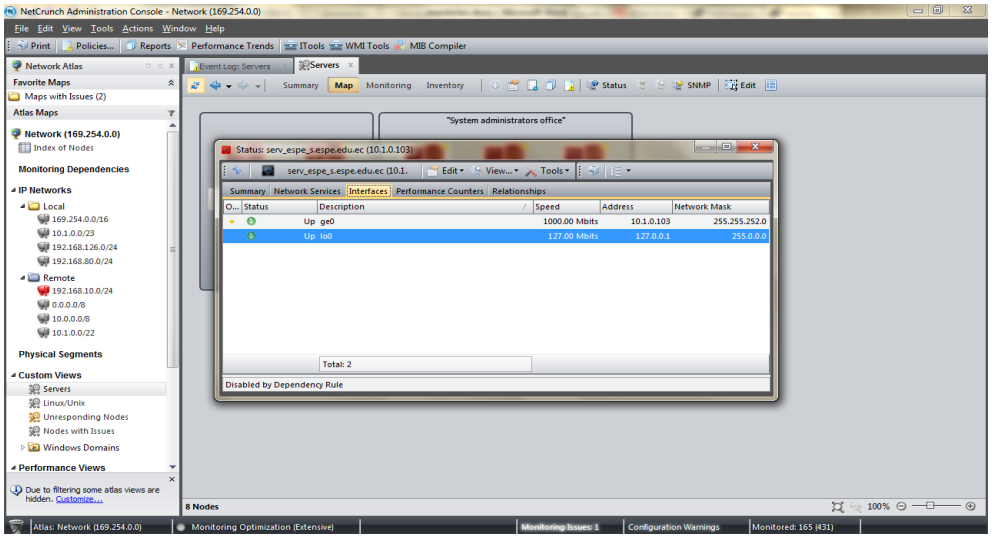


Ilustración 3.56 Interfaces descritas del Servidor

El programa realiza varios gráficos de la red con sus respectivos nodos. La ilustración 3.57 es una de las más completas ya que muestra toda la red monitorizada; además de sus nodos y su respectiva conexión.

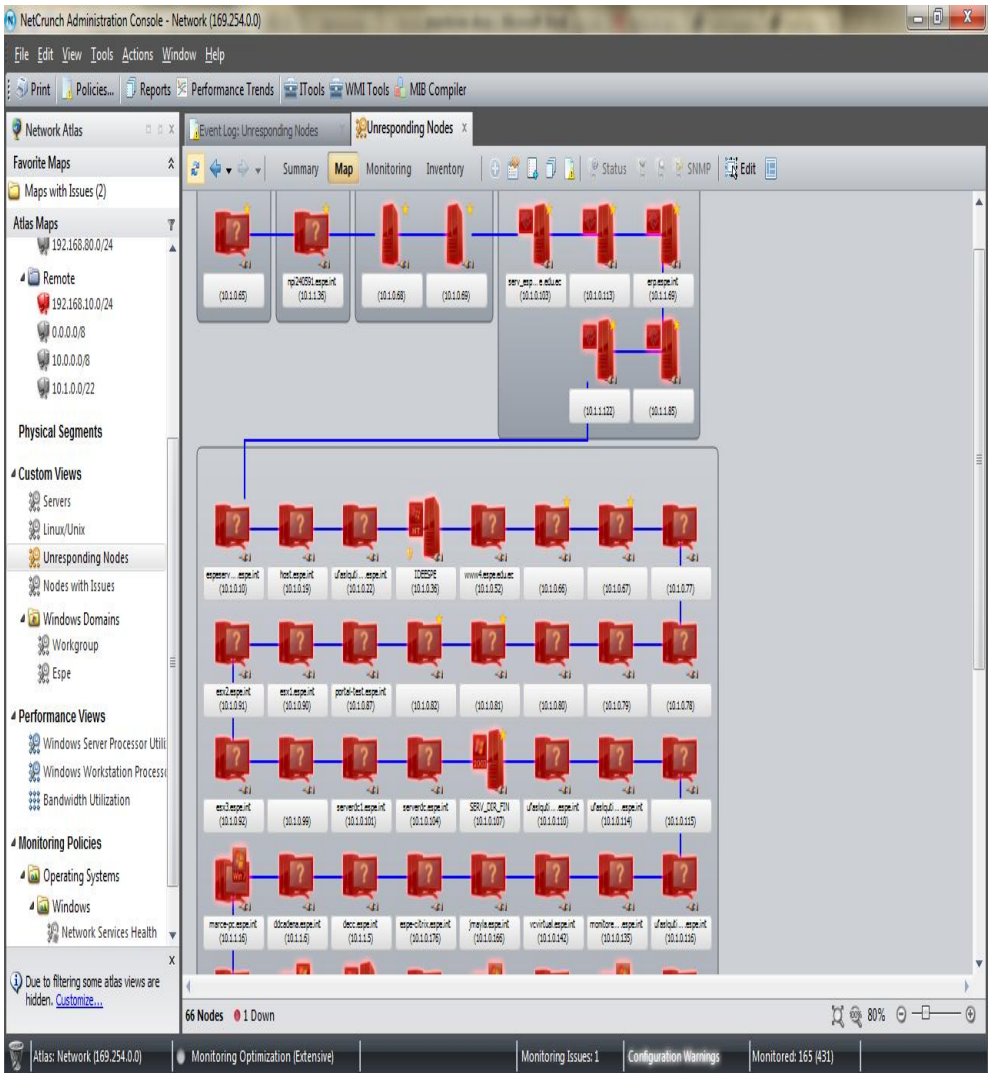


Ilustración 3.57 Red completa con nodos y conexiones.

En cuestión de gráficos comparativos el aplicativo ofrece tres clases: PING, 2 gráficos de conexión. Estos se pueden realizar de cualquier nodo independiente, si son servidores o terminales.

- En la ilustración 3.58 se muestra el gráfico de PING.

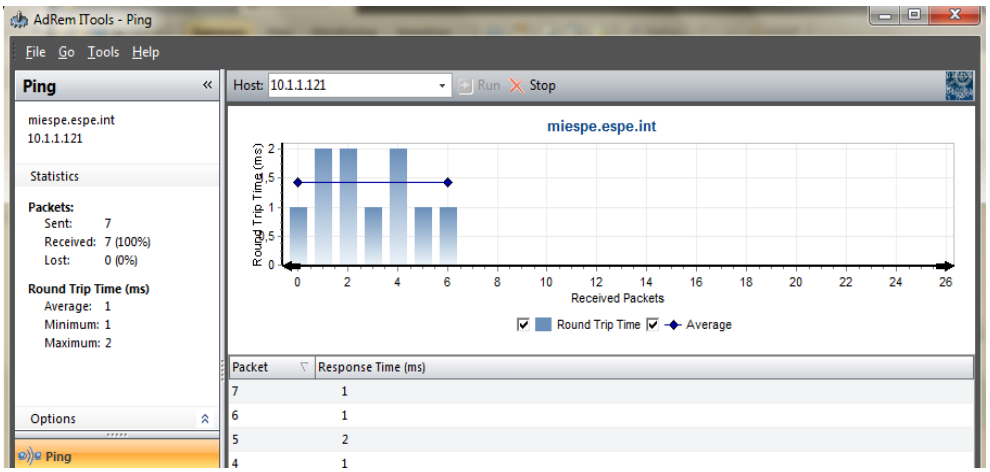


Ilustración 3.58 Gráfico de la Respuesta PING en tiempo.

- En la ilustración 3.59 se muestra el gráfico de conexión y en la ilustración 3.60 la confiabilidad de la conexión.

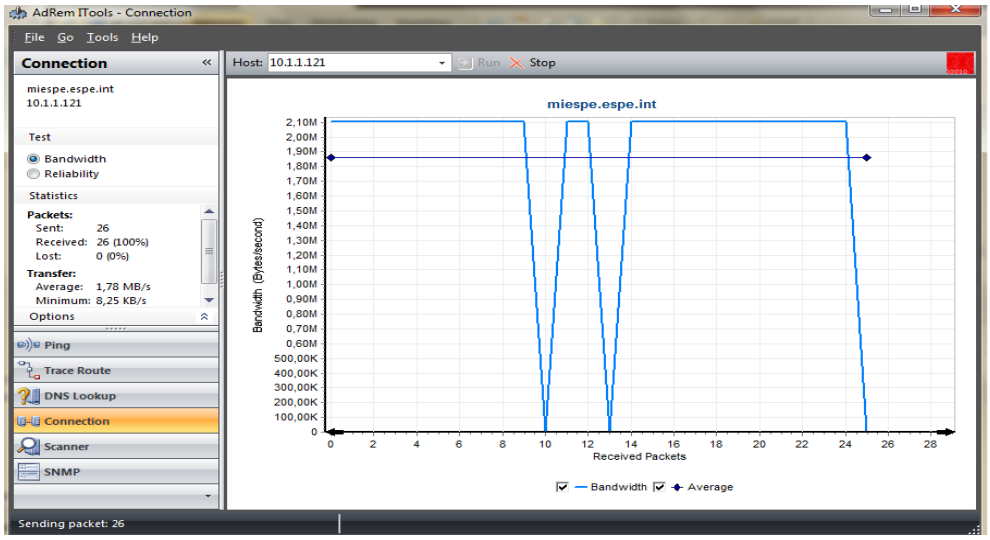


Ilustración 3.59 Gráfico Paquetes recibidos vs Bandwidth(bytes/segundo)

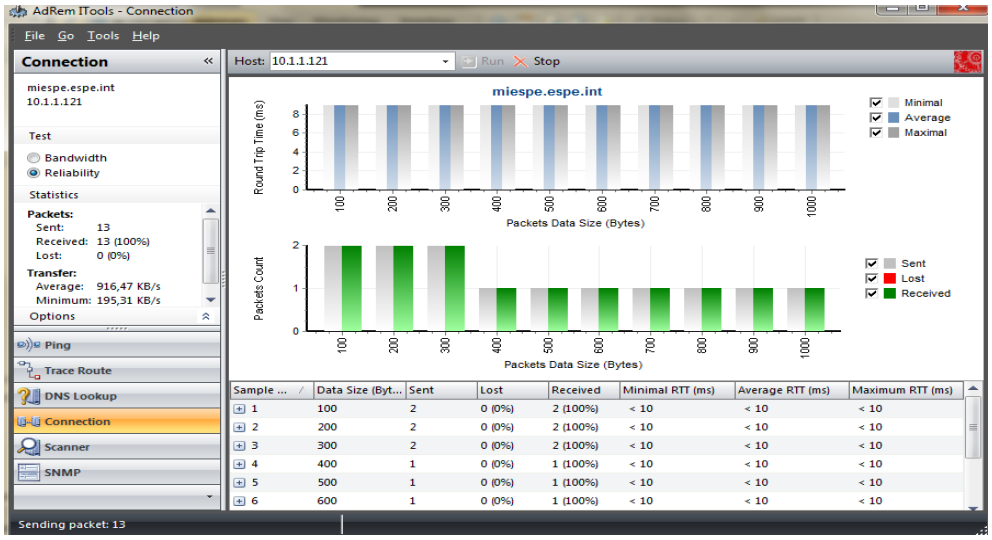


Ilustración 3.60 Gráfico confiabilidad de la conexión

Tiene la funcionalidad de escanear un servidor o un terminal mediante la IP; claro está, que si el terminal está protegido con contraseña en el programa NetCrunch, se pedirá contraseña y clave, para poder acceder a la información general de ese

terminal como: SO, utilización de la memoria, procesos, servicios y hardware. Como se muestra en la ilustración 3.61.

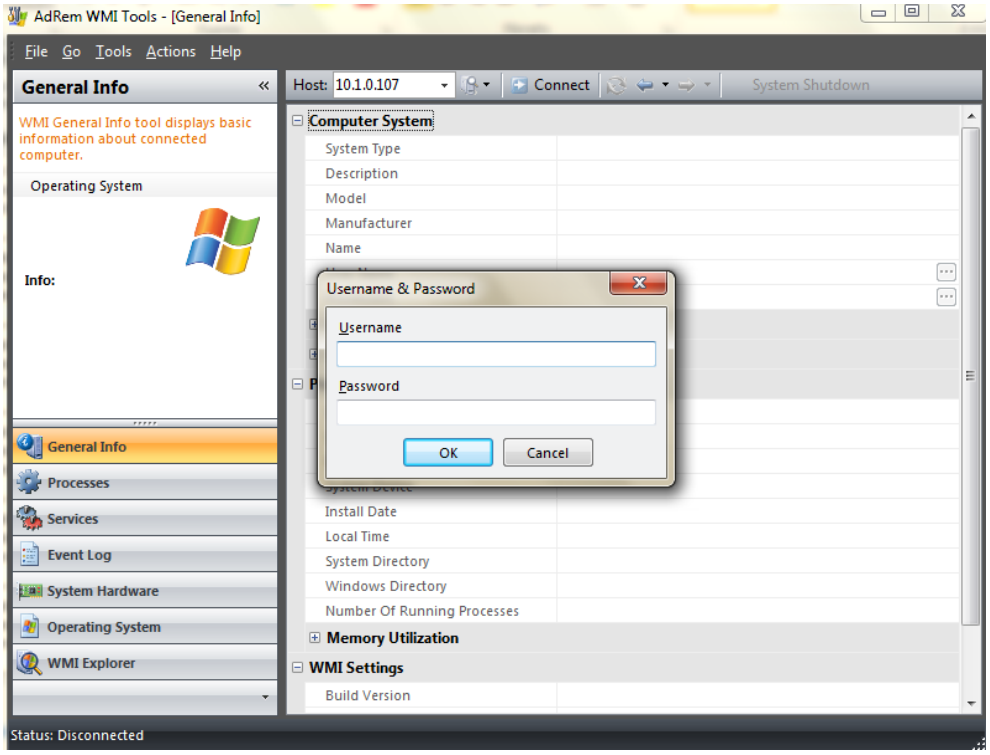


Ilustración 3.61 Información General de un Terminal

LOGINventory: Inventario Detallado del Hardware y Software en Red.

Se realizará un inventario de hardware y software automático; solo con escanear la red, el programa saca un inventario de todos los equipos conectados a esa red.

En este caso se realizó el escaneo de un punto de red que facilitó en Redes y Comunicaciones UTIC ESPE. Los resultados obtenidos no fueron del todo fidedignos debido a la extensa protección ante atacantes externos que tienen los equipos dentro del Data Center. Esto se indica en la ilustración 3.62.

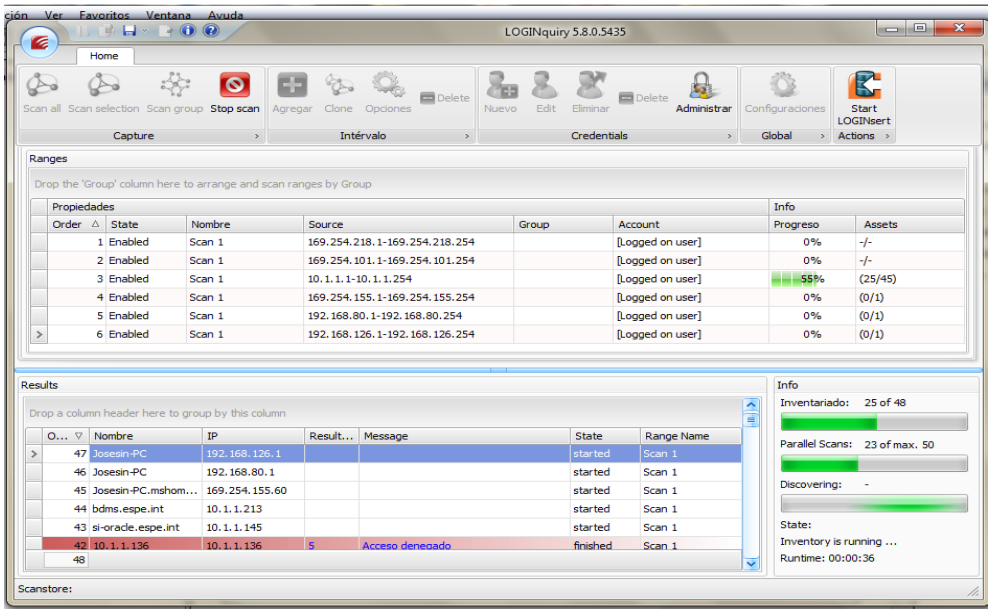


Ilustración 3.62 Escaneo Automático de Hardware y Software

Luego del escaneo automático, se presentan los resultados de forma jerárquica y se muestran en forma de árbol en la parte izquierda de la pantalla.

En el caso práctico que se realizó, se nota que han respondido cuatro terminales y de cada uno de ellos, se tendrá una lista de hardware y software, como se muestra en la ilustración 3.63.

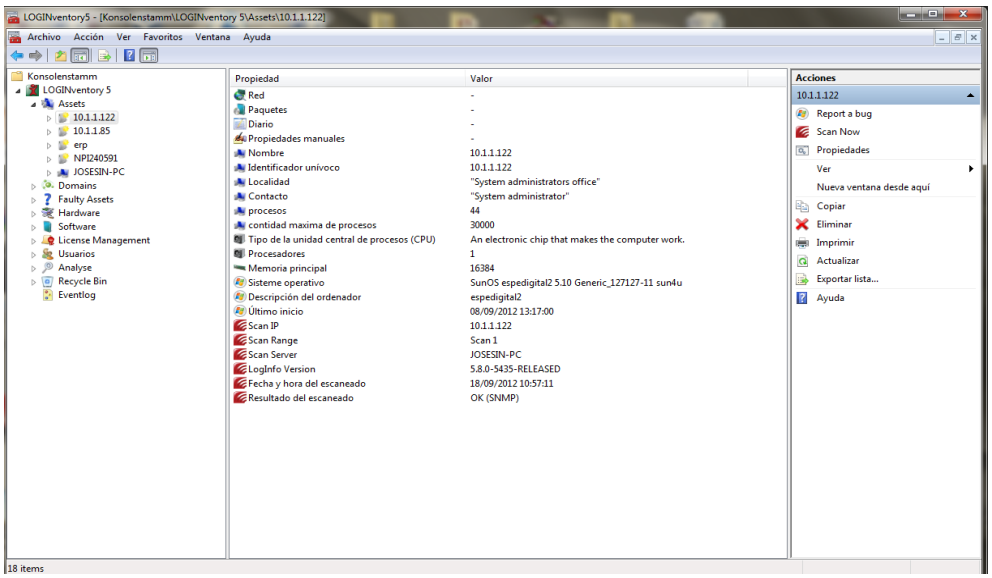


Ilustración 3.63 Resultados del Escaneo hardware y software

Los servidores o terminales que no han respondido o no se haya podido acceder a ellos, solo reconocerán el nombre del equipo y la dirección IP. Así lo muestra la ilustración 3.64.

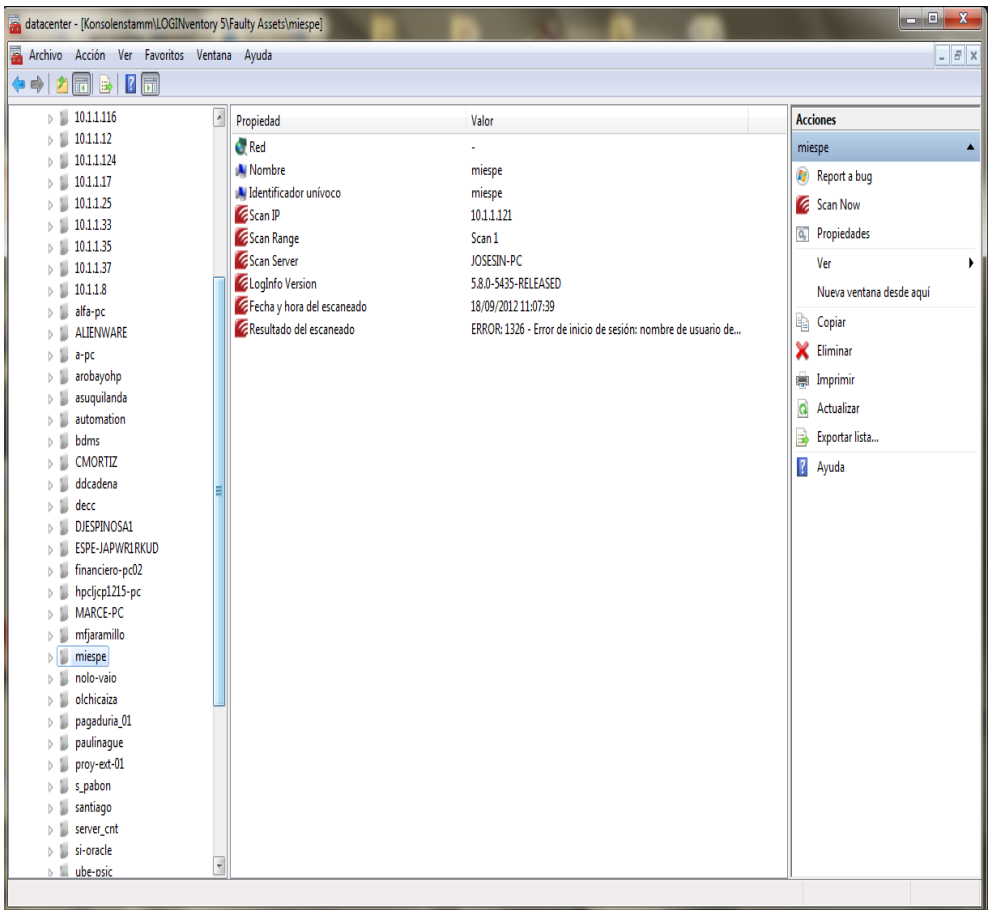


Ilustración 3.64 Error en escaneo de Terminal en Red

JMETER: Software para prueba de carga

Se realizó una prueba de carga HTTP para diez usuarios a la página www.espe.edu.ec, esto significa ir contra el sitio web; es un software portable por lo que no es necesario que esté instalado en algún terminal.

Lo primero a realizar es crear usuarios virtuales para cargar el sitio web. Los usuarios en el programa están como hilos, por lo que se añade un grupo de hilos, como se indica en la ilustración 3.65.

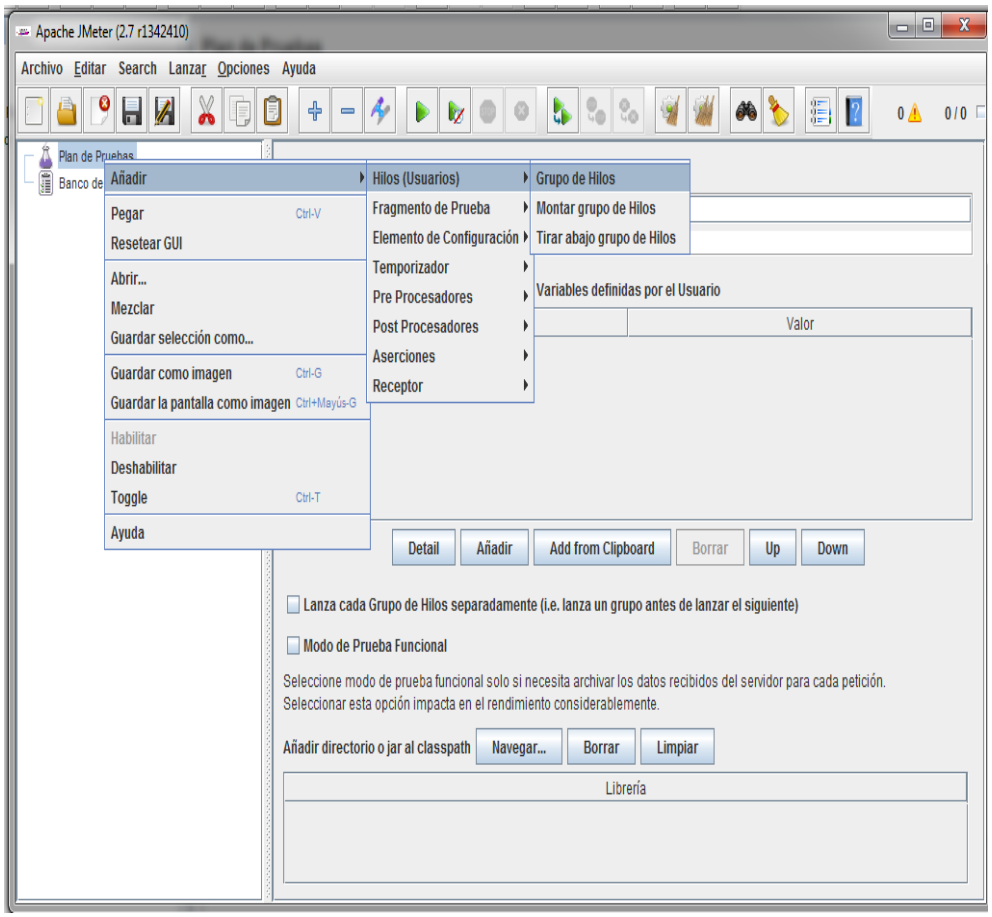


Ilustración 3.65 Forma de añadir hilos (usuarios) en JMeter

Una vez añadidos los usuarios o hilos, se añadirá un tiempo en segundos de subida, como se indica en la ilustración 3.66.

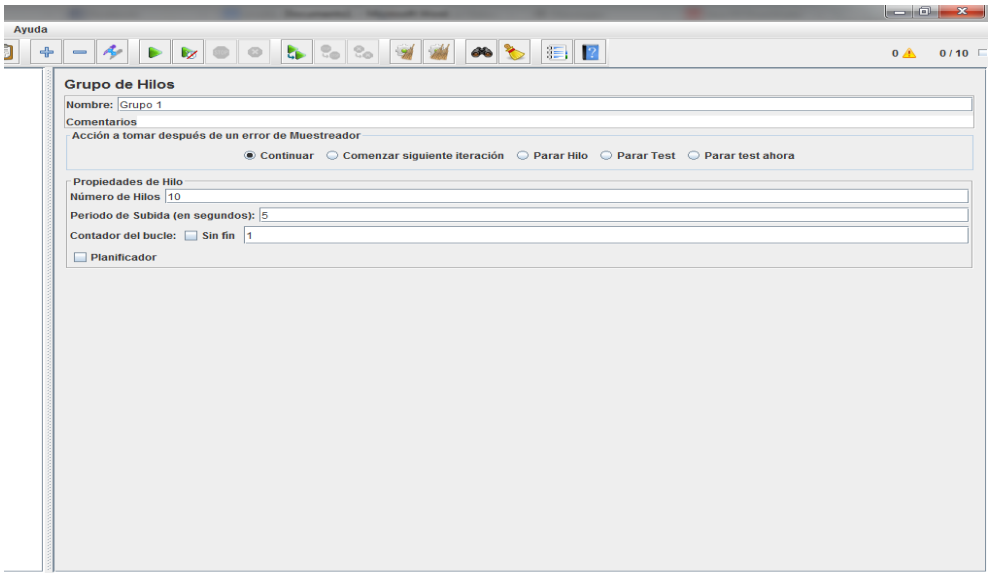


Ilustración 3.66 Configuración de un Grupo de Hilos (Usuarios)

La petición HTTP se realiza dentro del grupo de hilos (usuarios), para lo cual se tendrá que especificar la IP; el método que se va obtener en este caso es un GET; esto se indica en la ilustración 3.67 para configurar un monitor avanzado.

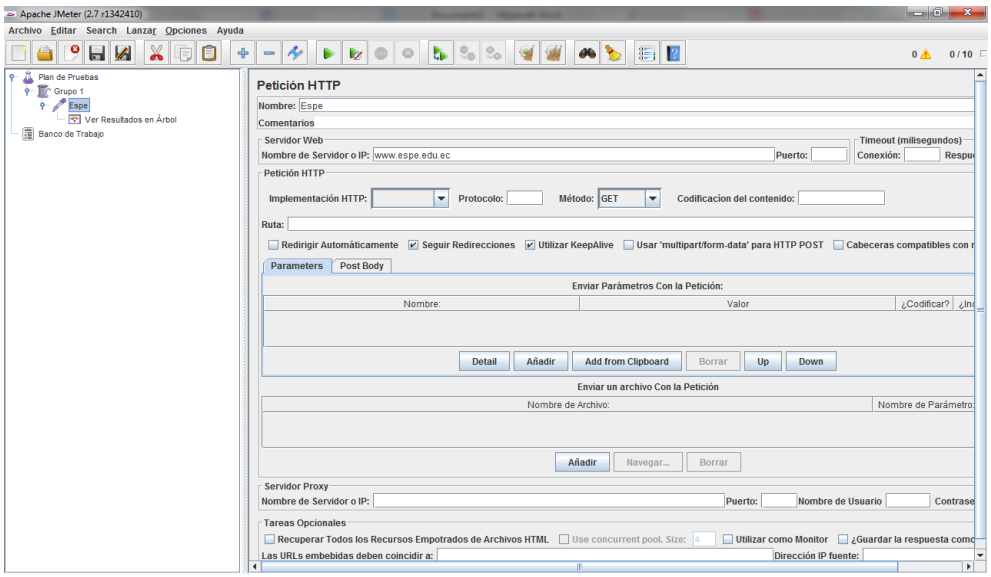


Ilustración 3.67 Petición HTTP JMeter

Terminada la configuración, se necesita un visualizador o listener de resultados; en este caso se los visualizará en forma de árbol. Como se muestra en la ilustración 3.68.

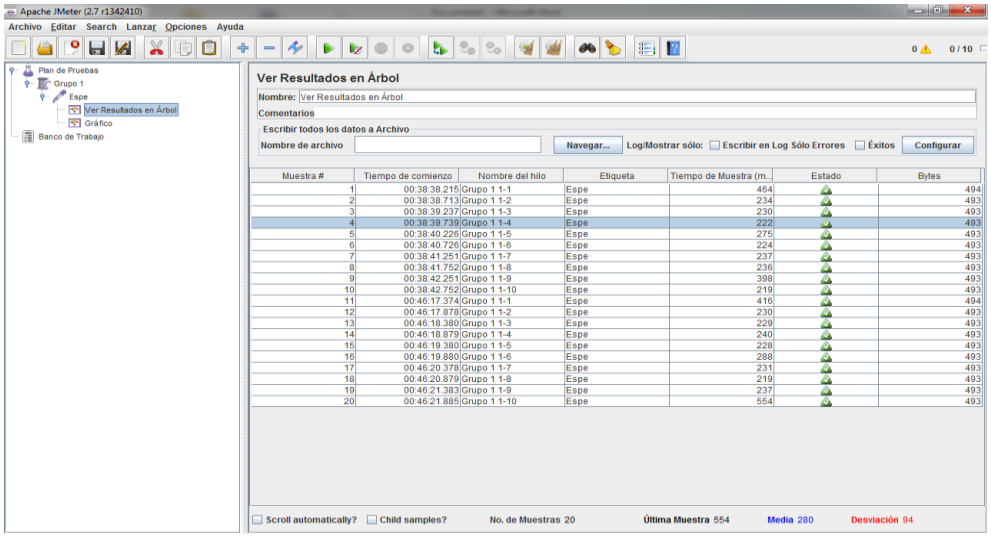


Ilustración 3.68 Resultados Petición HTTP JMeter

3.11.12 PTRG: Software utilizado por el Área de Redes y Comunicaciones para monitoreo del Data Center de la ESPE

El área de Redes y Comunicaciones UTIC ESPE permitió la observación del monitoreo de su red; ellos utilizan el software PTRG. Para acceder a la interfaz web de la aplicación, se deben autenticar como se muestra en la ilustración 3.69.

Ilustración 3.69 Autenticación Acceso a PTRG NETWORK MONITOR
FUENTE: Redes y Comunicaciones UTIC ESPE

Los servicios monitoreados en el momento de la observación fueron los siguientes:

Servicios de Sistemas de Información: Como se puede observar en la ilustración 3.70, se listan los servidores y las bases de datos:

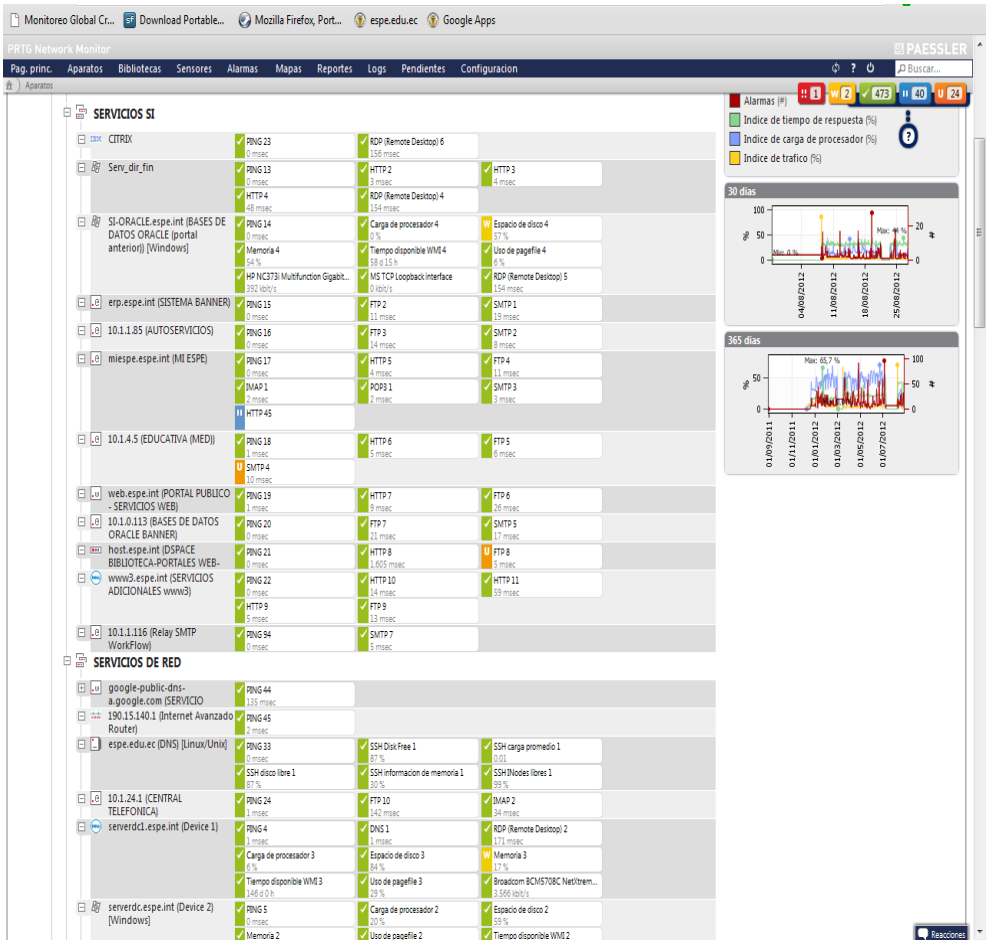


Ilustración 3.70 Monitoreo Servicios de Sistemas de Información

FUENTE: Redes y Comunicaciones UTIC ESPE

- Se observa el monitoreo de los servicios de red, en la ilustración 3.71 constan: router, switch, central telefónica y servidores de servicios.

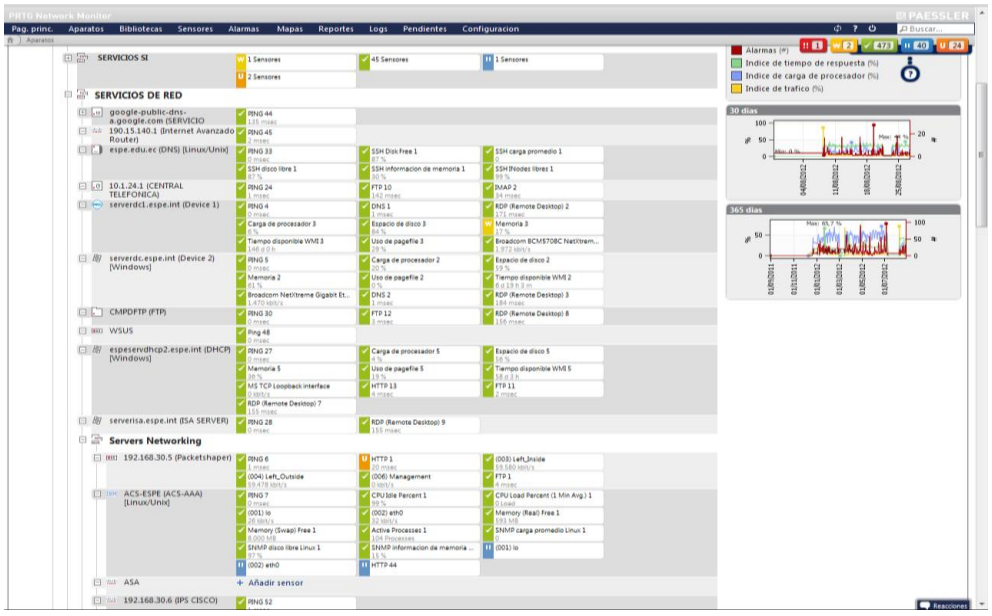


Ilustración 3.71 Monitoreo de Servicios en Red

FUENTE: Redes y Comunicaciones UTIC ESPE

Cada uno de los switch dentro del Data Center están monitoreados y muy bien reconocidos con su respectivo nombre, y lugar al que dan servicio, como se indica en la ilustración 3.72.

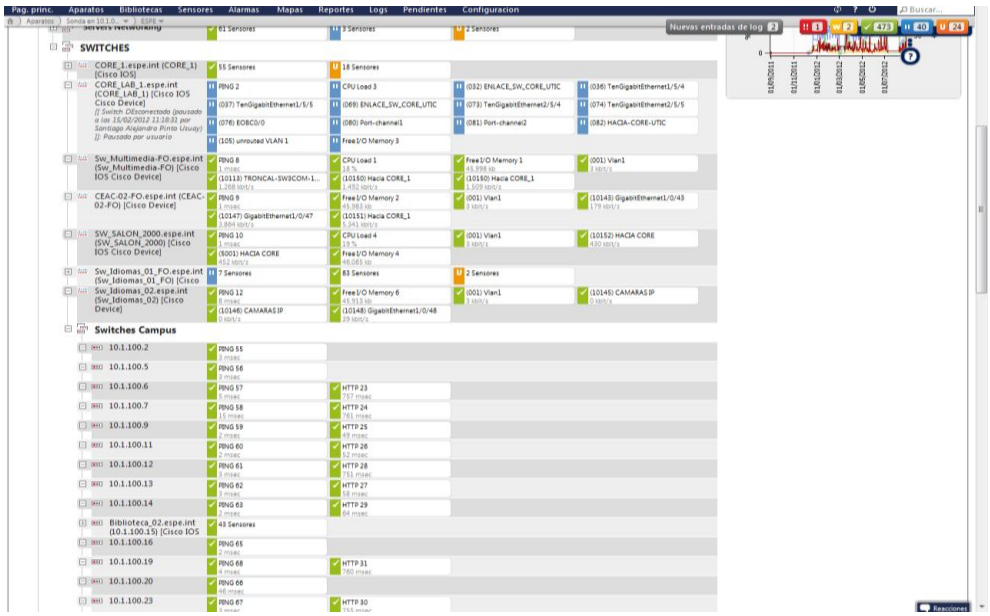


Ilustración 3.72 Captura: Monitoreo Switch´s dentro de Data Center

FUENTE: Redes y Comunicaciones UTIC ESPE

En la ilustración 3.73 se observa un ejemplo de parámetros configurados a un servidor de Dominio de la ESPE. En la parte derecha se ve los gráficos del monitoreo con sus respectivas variaciones y alertas y en un tiempo determinado.

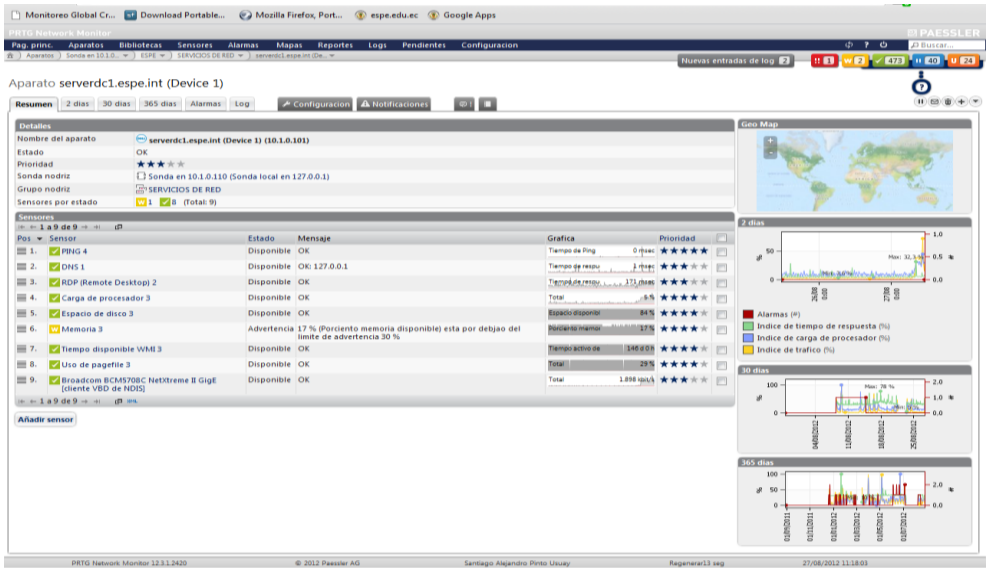


Ilustración 3.73 Parámetros configurados a servidor de Dominio ESPE

FUENTE: Redes y Comunicaciones UTIC ESPE

3.11.13 Software para ayudar al medio ambiente

a) Eficiencia Eléctrica Data Center (Ver Anexo 5)

Esta aplicación permite calcular la eficacia del uso de energía, eficiencia de la infraestructura y asignación de energía eléctrica del Data Center de la ESPE.

Se muestra una proyección anual de costo de la energía necesaria para establecer un presupuesto anual que garantice el servicio del Data Center 24/7.

b) Asignación de Costos para el Carbono y Energía (Ver Anexo 5)

Este aplicativo contiene valores mucho más desglosados sobre:

- Costo de energía por UPS.
- Toneladas de CO2 del Data Center y por UPS.
- Gráficas de la asignación de energía por servidor
- Estimación de la asignación de energía, emisiones CO2 a 15 años en el futuro.

c) Calculadora de Carbón del Data Center (Ver Anexo 5)

Esta aplicación permitirá establecer dos escenarios que podrían ser mediciones del Data Center en dos años consecutivos, para que el programa pueda compararlos, luego pueda arrojar resultados sobre el impacto ambiental del Data Center y proveer una estimación a 15 años.

Este programa tecnológico puede ser de ayuda al momento de adquirirlo para el Data Center de la ESPE, por la siguiente razón: se podría comparar una tecnología “verde” con el equipamiento actual, verificando así cuál de ellas brinda más beneficios para la empresa y el medio ambiente.

3.12 Entregables, análisis y evaluación del Data Center

En esta sección se toman en cuenta dos entregables:

- Manual de Procedimientos para llevar a cabo el análisis y evaluación del Data Center ESPE.
- Informe Técnico de Mediciones con el respectivo análisis, basado en los estándares y normas.

3.12.1 Manual de Procedimientos para realizar el análisis y evaluación de la Infraestructura del Data Center ESPE. Ver anexo 6

3.12.2 Informe Técnico de análisis de la Infraestructura del Data Center

El objetivo del presente documento es informar acerca del análisis de los equipos dentro del Data Center; para ello, se ha procedido a realizar visitas de campo y se ha revisado el estado actual del Data Center.

Desarrollo:

A continuación el análisis de los valores detallados en cada uno de los sistemas analizados.

a) Sistema eléctrico

Acometidas: Consta de siete acometidas trifásicas, integradas por cinco hilos o cables (tres fases o activos, tierra y un neutro); estos desembocan en un tablero de distribución de energía.

b) Tablero de Distribución

Medición de voltaje:

Tabla 3.54 Mediciones de Voltaje Tablero de Distribución

Fase	Medido con pinza amperimétrica	Multímetro Digital	Porcentaje de Error entre fase y fase ±5%	Cumplimiento del Data Center ESPE
1	204,9 V	205,3 V	Entre fase 1-2 error de 1,63 %	Sí cumple con el requerimiento de un circuito trifásico balanceado, demostrado por un mínimo porcentaje error, entre las tensiones de cada fase.
2	208,3 V	208,9 V	Entre fase 2-3 error de 2,01 %	
3	209,1 V	209,6 V	Entre fase 3-1 error de 0,39 %	

Medición del amperaje:

Tabla 3.55 Medición de amperaje en el Tablero de Distribución

Fase	Pinza Amperimétrica	Porcentaje de Error entre fase y fase ±5%	Cumplimiento del Data Center ESPE	Propuesta de Optimización
1	126 A	Entre fase 1-2 error de 8,42%	No cumple, porque la corriente de la fase 2 está sobrecargada	Balancear las cargas; es decir, distribuir los equipos de forma equitativa entre las tres fases para que la fase 2 no esté sobrecargada,
2	137,6 A	Entre fase 2-3 error de 6,97%	No cumple, porque la corriente de la fase 2 está sobrecargada	

				según el consumo de energía de cada equipo dentro del Data Center ESPE.
3	128 A	Entre fase 1-3 error de 1,58%	Sí cumple	

TVSS: En cumplimiento de las normas TIA-942 y BICSI-002, el Data Center ESPE tiene instalado un TVSS para proteger las instalaciones eléctricas internas de elevaciones de voltaje.

UPS

- **Voltaje de entrada**

Tabla 3.56 Voltaje Entrada UPS A

Medición Remota de UPS Data Center	**Fase L1**	**Fase L2**	**Fase L3**	**Porcentaje de Error entre fase y fase ±5%**			**Cumplimiento del Data Center ESPE**
				Fase 1-2	**Fase 2-3**	**Fase 3-1**	
Voltaje de Entrada	119.3 V	118.2 V	120.1 V	0,92%	1,60%	0,67%	Sí cumple
Corriente de Entrada	37 A	35 A	39 A	5,4%	10,26%	5,1%	Sí cumple

- **Voltaje de salida**

Tabla 3.57 Voltaje de Salida UPS A

Medición remota de UPS Data Center	**Fase L1**	**Fase L2**	**Fase L3**	**Porcentaje de error entre fase y fase ±5%**			**Cumplimiento del Data Center ESPE**
				Fase 1-2	**Fase 2-3**	**Fase 3-1**	
Voltaje de	121.3 V	120.8 V	121 V	0,41%	0,17%	0,24%	Sí cumple

Salida							
Corriente de Salida	42 A	39 A	23 A	Hasta 65 A	Hasta 63 A	Hasta 39 A	Sí cumple

- **Estado de los módulos de potencia**

Tabla 3.58 Módulos de Potencia UPS

	Valores Obtenidos en la medición	**Porcentaje de Carga del UPS**	**Porcentaje máximo de carga para un óptimo funcionamiento**	**Recomendación del Fabricante, hasta 75 % de la capacidad de carga máxima**
Capacidad Actual KVA	30 KVA	46,9% de los 30 KVA	100 % de los 30 KVA	Sí cumple el Data Center ESPE
Capacidad Máxima	40 KVA	35,18 % de los 40 KVA	Hasta 75 % de los 40 KVA	Sí cumple el Data Center ESPE
Tolerancia Fallos	Redundancia n+1			

Los UPS´s del Data Center de la ESPE están configurados, de tal manera que la capacidad de carga conectada no sobrepasa los 30 KVA, que es el 75% de la carga máxima de los mismos (40 KVA). El fabricante recomienda el 75% para obtener el mayor porcentaje de eficiencia de los UPS APC, que es el 92,6%.

- **Tiempo de ejecución restante:** 20 minutos.
- **Temperatura Interna:** 34 °C; la base está dada por el fabricante entre 0° y 40° en ambiente operativo, por lo que sí cumple con las recomendaciones propuestas.

ATS: El Data Center ESPE cumple con las normas TIA-942 y BICSI-002 al tener instalados 6 ATS, que proporcionan alimentación redundante a los equipos. Si falla un suministro primario el dispositivo da paso automáticamente al suministro de la fuente alternativa.

Sistema de iluminación:

Medición de Lux

Tabla 3.59 Lux Data Center

Mediciones dentro del Data Center ESPE	Parámetros descritos por las normas TIA-942/BICSI 002	Cumplimiento del Data Center ESPE
Las luminarias están a 2,55 metros del piso falso.	Las luminarias deben estar situadas por lo menos a 1 metro del piso falso.	Sí cumple
El nivel de iluminación de las luminarias es de 1000 lux.	Las luminarias deben tener un nivel de iluminación mínimo de 500 lux.	Sí cumple

Puesta a Tierra: Constituido por seis varillas de cobre de 5/8" x 1,8 metros de diámetro con cable 2/0awg y zanjas de 30x50cm, por donde pasa el cable.

Tabla 3.60 Medida ohmios Tierra

Mediciones de la resistencia	Valores medidos	Parámetros descritos en la norma Tia-942	Cumplimiento del Data Center ESPE
Resistencia 1	2,2 ohmios	Menor a 5 ohmios	Sí cumple
Resistencia 2	1,8 ohmios		
Resistencia 3	1,4 ohmios		
Promedio método de la pendiente	2,1 ohmios		

Con respecto a la resistencia de la malla de puesta a tierra, en el patio posterior al Data Center de la ESPE, cumple con la norma TIA-942, donde el valor de la resistencia en ohmios debe ser menor a 5 ohmios.

Sistema de control de seguridad:

- **Cámaras:** El Data Center de la ESPE dispone de 3 cámaras IP, situadas en áreas específicas para el monitoreo; la norma TIA-942 solo recomienda pero

no es obligatorio contar con este sistema de monitoreo dentro y fuera del Data Center, en el nivel de TIER I y TIER II.

- **Sensores:** El Data Center de la ESPE cuenta con sensores bajo el piso falso, colocados a la altura de la loza para prevenir inundaciones y localizar fugas de agua; la norma TIA-942 solo recomienda pero no es obligatorio contar con este sistema de sensores dentro y fuera del Data Center, en el nivel de TIER I y TIER II.

- **Acceso Físico:** El Data Center de la ESPE tiene dos puertas de acero para la entrada y salida con sensores de apertura; estas cuentan con una pintura anti inflamable y bisagras para abrir hacia afuera. Estos requerimientos van de la mano con el cumplimiento de la norma TIA-942 y el Data Center de la ESPE.

Tabla 3.61 Medidas Puertas Data Center

Puerta Data Center ESPE	Largo	Ancho	Parámetros descritos en las norma TIA-942 y BICIS-002	Cumplimiento del Data Center ESPE	Propuesta de Optimización
Principal	2,20 m	1,01 m	Para la puerta principal: 2,13 m. de largo y 1 m. de ancho-	Sí cumple-	
Emergencia	2,20 m	0,93 m	Para la puerta de emergencia: 2,13 m. de largo y 1 m. de ancho	No cumple con el valor mínimo de ancho 0,93 m < 1m.	Remplazar por otra puerta que tenga 1m de ancho como mínimo, para facilitar el ingreso y salida de equipos y personal

Sistema Contra Incendios: El Data Center de la ESPE cuenta con cinco sensores de humo, ubicados estratégicamente dentro del mismo; un sistema FM200 que descarga un gas no liquido; una alarma de incendios; y, cuatro luces de emergencia. Este sistema cumple con las normas TIA-942 y BICSI002, ya que estas recomiendan tener un sistema de prevención y extinción de incendios, en todos los niveles de TIER.

Señalética: Las normas TIA-942 y BICSI-002 recomiendan el uso de un set de señalética. El Data Center de la ESPE tiene dos letreros de salida en caso de emergencia, los cuales disponen de una batería interna cuando el suministro de energía eléctrica se pierda.

Sistema de Aire Acondicionado: Cuenta con tres sistemas de aire acondicionado: dos están en funcionamiento continuo (Marca STULZ modelo ASD211G) y uno, como reserva redundante.

- **Mediciones de temperatura y humedad**

Tabla 3.62 Medidas Aire Acondicionado Data Center

Aire Acondicionado	Mediciones dentro del Data Center ESPE	Parámetros descritos en las norma TIA-942 y BICSI-002	Cumplimiento del Data Center ESPE	Propuesta de Optimización
Temperatura	23,2 C°	La temperatura promedio del ambiente debe estar entre 20-25 C°	Sí cumple	
Humedad	35,60%	La temperatura promedio del ambiente debe estar entre 40% - 50%	No cumple	Cambiar los valores de humedad entre 40% y 50% en el panel de configuración del equipo; también se puede realizar este proceso vía remota, porque el porcentaje actual

				de humedad puede provocar cortocircuito de los componentes internos de los equipos.
Oscilación de temperatura	5 C°	No mayor a 5 C°, para evitar condensación de equipos.	Sí cumple	

Piso Falso: El Data Center de la ESPE cumple con 30cm. de espacio que debe existir entre la loza y el piso falso. Se recomienda la aplicación de las normas TIA-942/BICSI 002, para que por ahí pase el cableado horizontal y no existan filtraciones de agua.

CAPÍTULO 4

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones:

- La segregación de las funciones del personal de la UTIC, permite mantener y monitorear frecuentemente el Data Center.

- En el Plan de Contingencia UTIC se evidencia la identificación de los recursos críticos que hay que proteger, el análisis de los riesgos, la evaluación y tratamiento de los riesgos, monitoreo, el plan de pruebas y la capacitación al personal así como las soluciones al experimentar una catástrofe.

- Los respaldos de información son etiquetados y almacenados dentro de un lugar seguro. Están detallados en el documento de "Políticas de Respaldo de Información", para su eventual uso en caso de una contingencia.

- Se Identificaron los recursos que deben ser protegidos en el Data Center de la ESPE: antivirus; recursos hardware y software; base de datos; aplicaciones y servicios.

- La información obtenida fue posible gracias a la aplicación de técnicas previamente estudiadas como: entrevista y encuesta al Administrador de Redes y Comunicaciones; revisión de Plan de Contingencia UTIC, procedimientos, inventarios de hardware y software; visita y observación al Data Center.

- Los valores que arroja la evaluación de los sistemas: iluminación, extinguidores de incendios, red (cableado), piso falso, aire acondicionado, conexión a tierra, control de seguridad así como la señalética, cumplen con parámetros mínimos establecidos en las normas y estándares: TIA 942, BICSI 002, NEC-10, ISO 24764.

- Los investigadores realizaron en detalle, las siguientes actividades dentro Data Center ESPE, como: revisión de: acometidas y del tablero de distribución; medir el amperaje en el tablero de distribución y temperatura de los de pisos fríos y calientes, puesta a tierra; observación de la iluminación; verificar el funcionamiento de: UPS, de las cámaras IP, puertas de acceso, sistema de incendios, las señalizaciones, los kvas del A/C y cableado estructurado de servidores.

- Actualmente existen en el mercado informático varias herramientas software, para monitorear los servicios del Data Center de la ESPE, como: IPHost Network Monitor, RedEyes, NetCrunch, LOGINventory y PTRG.

- El Data Center ha sido construido en la planta baja del edificio central de la ESPE, donde estaría expuesto a amenazas ambientales como la humedad o inundaciones.

- Con el manual de procedimientos se puede realizar paso a paso el análisis y evaluación para verificar los parámetros mínimos de funcionamiento del Data Center ESPE basado en las normas y estándares nacionales e internacionales de calidad.

4.2 Recomendaciones:

- Utilizar las herramientas que ofrece la metodología COBIT como matriz de riesgos y objetivos de control para realizar un análisis de la gestión actual del Data Center ESPE.

- Ubicar al Data Center entre la planta alta y baja para evitar el peso del Data Center e inundaciones.

- Etiquetar y ordenar el cableado estructurado, para evitar la confusión al detectar y reparar una falla.

- Realizar un muestreo de las grabaciones de las cámaras IP.

- Reinstalar las puertas de ingreso o emergencia del Data Center; estas no deben tener salida al exterior del edificio.

- Verificar por lo menos una vez al mes, el correcto funcionamiento de la palancas manuales, detectores de humo y fecha de caducidad del Sistema contra incendios.

- Checar el filtro, los refrigerantes y el voltaje de entrada del Sistema de aire acondicionado.

- Aplicar el Manual de Procedimientos de Evaluación y Análisis de la infraestructura del Data Center propuesto, para verificar el cumplimiento de los requisitos mínimos estipulados en las normas y estándares internacionales.

4.3 Referencias Bibliográficas

- Surge Ingeniería *Memoria Técnica Remodelación Data Center ESPE*

4.4 Referencias Electrónicas

- AdRemNetCrunch: http://www.adremsoft.com/netcrunch/doc/NC6_Users_Guide.pdf (20/09/2012).
- Apache Software Foundation: http://jmeter.apache.org/ (20/09/2012).
- APC *Herramientas TradeOff:* http://www.apc.com/prod_docs/results.cfm?DocType=Trade-Off%20Tool&ISOCountryCode=ec (01/09/2012).
- **CALLEJAS** Gutierrez, Ismael Fernando: Tableros de distribuciones eléctricos http://tablerosdedistribucinelectricos.blogspot.com/ (10/08/2012).
- Cableado Estructurado: http://www.slideshare.net/sgalsan/cableado-estructurado-1946267 (10/02/2012).
- Chris Diminico *Telecommunications Infrastructure Standard for Data Centers:*

http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf (10/02/2012).

- Data Center Desing and Implementation Best Practices: http://www.bicsi.com.au/Joomla/Downloads/BICSI2011/Day_2/Data_Centre_Standard_Siemon.pdf (20/07/2012).
- Data Centres TrueNet: http://www.adckrone.com/eu/es/webcontent/support/PDFs/enterprise/103297ES.PDF (11/08/2012).
- DC Consultores *Normas, estándares y auditoria en Datacenter*: http://www.isertec.com/userfiles/isertec.com/i_admin/file/datacenter_summit/_pres_pdf/009%20-%200415%20p.m.%20Octavio%20Delgado%20-%20Necesidad_de_aplicar_normas_estandares_y_auditoria_en_un_Data%20Center.pdf (10/08/2012).
- Erazo, César *Modulo de Cableado Estructurado:* http://es.scribd.com/doc/66862948/Articulo-Tecnico-Cesar-Erazo (10/02/2012).
- Ip Host Network Monitor: http://www.iphostmonitor.com/features.html (22/09/2012).
- IT Governance Institute, Cobit 4.1: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf (07/09/2012).
- IBM *Directrices generales para centros de datos:* http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=/p7ebe/p7ebegeneralguidelines.htm (10/02/2012).
- Jonathan Jew, J&M Consultants: http://www.cablinginstall.com/articles/print/volume-18/issue-5/features/what-will-be-in-the.html (23/09/2012).
- Monge Torres, José Miguel *Estándares sobre Diseño y Funcionamiento de Data Center:* http://www.grupoelectrotecnica.com/pdf/estandaresdatacenter.pdf (11/08/2012).
- Neil Rasmussen *Implementación de centros de datos con alta eficiencia energética*: http://www.itnews.ec/documentos/Informe114.pdf (11/08/2012).

- Norma NEC-10 *Norma Ecuatoriana de la Construcción:* http://www.cicp-ec.com/index.php?option=com_content&view=article&id=131&Itemid=39 (25/01/2012).
- Norma TIA-942 *Telecommunications Infrastructure Standard for Data Centers:* http://informatica.iessanclemente.net/manuais/images/9/9f/Tia942.pdf (23/01/2012).
- Paessler: http://www.paessler.com/common/files/pdf/productflyer_prtg_en.pdf (19/09/2012).
- RedEyes Software: http://res-software.com/online-help/ (23/09/2012).
- Schmidt's LOGIN GmbH: http://www.loginter.net/files/loginventory5-flyer.pdf (20/09/2012).
- Secure Bytes: http://www.secure-bytes.com/DatasheetSA.pdf (23/09/2012).

4.5 Glosario de términos y abreviaturas

4.5.1 Términos:

Administración: es el método para el etiquetado, identificación, documentación y el uso necesario para poner en práctica los cambios en la infraestructura de las telecomunicaciones.

Backbone: es una instalación entre cualquiera de los siguientes espacios: sala de telecomunicaciones, terminales, salas de equipos y áreas de distribución.

Blindaje: es un elemento del cable que sirve de protector a las interferencias electromagnéticas.

Cable: conjunto de uno o más conductores aislados pueden ser de cobre o fibra óptica.

Canal: es la vía de transmisión de un extremo a otro entre dos puntos o dos terminales.

Conducto: es una canaleta donde se pasa el cableado.

Enlace: es la unión permanente de partes metálicas para formar una trayectoria eléctricamente conductora para asegurar la continuidad eléctrica y la capacidad para conducir con seguridad cualquier corriente.

Fibra óptica: es un filamento fabricado de materiales dieléctricos que guía la luz.

Gabinete: es un contenedor que puede incluir dispositivos de conexión, terminaciones de cables, aparatos electrónicos y equipo informático.

Identificador: es un elemento de información que vincula a un elemento específico de las telecomunicaciones con su correspondiente registro.

Inalámbrico: son señales que viajan a través del espacio, para transmitir información sin tener cable, el medio de transmisión es el aire.

Interconexión: es el cruce entre usuarios y servicios.

Link: es una vía de transmisión entre dos puntos, sin incluir los equipos terminales, área de trabajo y cables de equipo.

Medios de comunicación: alambre, cable o conductores utilizados para las telecomunicaciones.

Patchcord: Es un cordón de conexión que facilita la administración del sistema de cableado.

Piso de acceso o piso falso: es un sistema formado por paneles de piso totalmente desmontables e intercambiables que se apoyan sobre pedestales ajustables, para permitir el acceso a la zona inferior.

Proveedor de acceso: es el operador que brinda servicios de telecomunicaciones tanto de internet como de acceso celular.

Sala de computadores: es un espacio cuya función principal es dar cabida a los equipos de procesamiento.

Sala de telecomunicaciones: es un espacio cerrado para la utilización de equipos y las conexiones del backbone.

Suministro ininterrumpido de energía: es un repositorio entre el suministro de energía (fuente de alimentación) y una carga de energía; esta debe ser precisa y continua para que no hayan daños en el equipo electrónico.

Telecomunicaciones: es toda transmisión, emisión y recepción de signos, señales, escritos, imágenes y sonidos; es decir, información de cualquier naturaleza por cable, radio u óptico.

Tierra: es una conexión conductora, ya sea intencional o accidental, entre un circuito eléctrico (Por ejemplo, telecomunicaciones) o equipo y la tierra o algún cuerpo conductor que sirva de tierra.

Topología: es la disposición física y lógica de un sistema de comunicaciones.

4.5.2 Abreviaturas:

AI3: Adquirir e implementar, proceso de COBIT 4.1: Adquirir y mantener infraestructura tecnológica. (pág. 66)

AS/NZS: Standars Australia, es una organización independiente, sin fines de lucro, reconocida por el Gobierno australiano como el cuerpo de normas gubernamentales. (pág. 13)

ATM: Modo de Transferencia Asíncrona o Asynchronous Transfer Mode. (pág. 94)

BICSI-002: Norma para el diseño de un Data Center y la Implementación de las mejores prácticas. (pág. 13)

C°: Unidad de temperatura grados Celsius. (pág. 176)

CCTV: Circuito cerrado de televisión. (pág. 19)

CENELEC: Comité Europeo de Normalización Electrotécnica. (pág. 42)

COBIT 4.1: Metodología que contiene los objetivos de control para tecnologías de información. (pág. 15)

Disrupción: Alterar, interrumpir, romper el equilibrio de las funciones de un sistema. (pág. 37)

DS12: Entregar y dar soporte, proceso de COBIT 4.1: Administración del ambiente físico. (pág. 67)

DS2: Entregar y dar soporte, proceso de COBIT 4.1: Administrar los servicios de terceros. (pág. 66)

DS4: Entregar y dar soporte, proceso de COBIT 4.1: Garantizar la continuidad del servicio. (pág. 67)

DS5: Entregar y dar soporte, proceso de COBIT 4.1: Garantizar la seguridad de los sistemas. (pág. 67)

EDA: Área de distribución de equipos para diseñar un Data Center. (pág. 31)

HDA: Área de distribución horizontal para diseñar un Data Center. (pág. 31)

IEC: Comisión Electrotécnica Internacional. (pág. 13)

ISO: Organización Internacional para la Estandarización. (pág. 13)

Log: Es un término anglosajón, equivalente a la palabra bitácora en español. (pág. 18)

MDA: Área principal de distribución para diseñar un Data Center. (pág. 31)

ME3: Monitorear y evaluar, proceso de COBIT 4.1: Garantizar el cumplimiento con requisitos externos. (pág. 68)

NFPA-75: Norma para la protección de equipos electrónicos. (pág. 13)

OLTS: Equipo de prueba de pérdida óptica (Optical Loss Test Set). (pág. 52)

PO4: Planear y organizar, proceso de COBIT 4.1 que define los procesos, organización y relaciones TI. (pág. 65)

PO9: Planear y organizar, proceso de COBIT 4.1: Evaluar y administrar los riesgos de TI. (pág. 66)

SW: Software. (pág. 92)

TI: Tecnologías de la información; agrupan los elementos y las técnicas usadas en el tratamiento y la transmisión de la información. (pág. 15)

TIA-942: Norma para las telecomunicaciones y la infraestructura del Data Center; fue creada por la Asociación de la Industria de las Telecomunicaciones. (pág. 13)

UPS: Dispositivo de alimentación eléctrica ininterrumpida. (pág. 13)

ZDA: Área de la zona de distribución para diseñar un Data Center. (pág. 31)