



**Universidad Tecnológica
del Centro de Veracruz.**

**Programa educativo: Ingeniería en Tecnologías de la
Información.**

**Reporte para obtener título de Ingeniero en Tecnologías de la
Información.**

Proyecto de estadía realizado en Palladium Hotel Group.

**Nombre del proyecto: Auditoria interna para la reestructuración
lógica de las redes en Grand Palladium Hotel Group.**

Presenta: Rodríguez Hernández Linda Rosario.



**Universidad Tecnológica
del Centro de Veracruz**

**Programa educativo: Ingeniería en Tecnologías de la
Información.**

Asesor Industrial: Ing. Oscar B. Bonilla Ramírez.

Asesor Académico: I.S.C. Merced Sosa Luna

Presenta: Rodríguez Hernández Linda Rosario.

Índice

| | |
|---|----|
| Resumen..... | 3 |
| Introducción..... | 4 |
| Antecedentes..... | 5 |
| Descripción de la problemática..... | 6 |
| Justificación..... | 7 |
| Objetivo general..... | 7 |
| Objetivos específicos..... | 7 |
| Alcance..... | 7 |
| Metodología..... | 8 |
| Diseño de estrategias..... | 13 |
| Investigación de normas aplicables a la auditoria..... | 13 |
| Diagramas..... | 15 |
| | 18 |
| Procedimiento..... | 19 |
| Evaluación de la estructura del departamento y redes..... | 19 |
| Conclusiones..... | 21 |
| Propuesta de solución..... | 22 |
| Referencias..... | 24 |
| Apéndices o Anexos..... | 25 |

Resumen.

Las Tecnologías de la Información (TI) o también denominadas como nuevas tecnologías es la aplicación de ordenadores y equipos de telecomunicación para almacenar, transmitir y manipular datos utilizados en diferentes entornos, desde sectores como la educación hasta área de hotelería; la finalidad de las TI es mejorar la calidad de vida de las personas dentro de un entorno. Debido a la importancia que tienen las TI en el funcionamiento de una organización, existe la auditoría informática. El término de auditoría se ha empleado con frecuencia de forma incorrecta, porque ha sido tomado como sinónimo de detección de errores y fallas. El concepto de auditoría es mucho más que eso, pues tiene como fin evaluar y mejorar la eficacia y eficiencia de una organización, al examinar su gestión.

La auditoría informática es un proceso evolutivo que mediante técnicas y procedimientos aplicados en una organización por personal independiente a la operación de la misma, evalúa la función de tecnología de información y su aportación al cumplimiento de los objetivos institucionales; emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de apoyo al cumplimiento de dichos objetivos.

Introducción.

El siguiente documento contiene información y propuestas para el análisis y mejora del departamento de sistemas en Grand Palladium Hotel Group enfocado a la red, todo esto mediante la aplicación de una auditoría lógica interna, es decir, mediante la identificación física de algunos de los dispositivos encargados de administrar el acceso a internet ofreciendo un diagnóstico o proponiendo algunas normas como la TIA/EIA606 con los puntos más importantes y accesibles favoreciendo la mejora continua y progresiva, formando así una propuesta de solución eficaz.

La estructura del documento está conformada por puntos como antecedentes donde incluye información sobre el giro de la empresa, en el punto de la metodología se muestra a CRMR y los puntos que se abarcaron durante el desarrollo e investigación para la realización de la auditoría, en diseño de estrategias se incluyen aquellos puntos importantes que favorecieron al análisis e investigación, en procedimiento incluye los cuestionarios y todas aquellas evaluaciones que se realizaron para llegar a las conclusiones, evaluación de resultados, conclusiones incluye resultados finales y todos aquellos procesos que deberían ser tomados en cuenta para la mejora de algunos procesos.

Antecedentes.

Palladium Hotel Group.

Con sede en Ibiza, en las Islas Baleares, España, PALLADIUM HOTEL GROUP es una corporación multinacional que surge hace más de cuarenta años, con la finalidad de promover la isla en España y en el Continente. Con el tiempo se ha consolidado como una de las empresas españolas con mayor proyección mundial.

Palladium Hotel Group, es una reconocida empresa que se ha preocupado por realizar una segmentación de sus hoteles y el lanzamiento de nuevas marcas para cada uno de ellos, siguiendo una verdadera política de expansión y cumpliendo con precisos estándares de calidad.

En la actualidad, el grupo cuenta con establecimientos en diferentes lugares del mundo, tales como: Ibiza, Mallorca, Menorca, Barcelona, Madrid, Valencia, Oviedo, Fuerteventura, Tenerife, Córdoba y Sevilla en España, Sicilia en Italia, Riviera Maya y Riviera Nayarit en México, Punta Cana y Playa Bávaro en Santo Domingo, Jamaica y Brasil.

Descripción de la problemática.

Palladium Hotel Group maneja diferente información con sus clientes y trabajadores, información que incluye desde registro de habitaciones, reservaciones y/o pagos, esta información es manejada por distintos programas con acceso a internet es por ello que la conexión debe ser eficiente y constante permitiendo que los clientes puedan disfrutar de conexión y los empleados puedan trabajar sin problema alguno. Cabe mencionar que para los clientes no existe ningún tipo de restricción en cuanto el uso de internet, el registro es mediante la página de internet proporcionando el número de habitación y correo electrónico, en cuanto a los trabajadores el acceso a internet es mediante la red, es decir, que todo aquel que quiera tener acceso a internet deberá proporcionar su equipo a sistemas para ingresarlo al dominio y proporcionarle una dirección ip para que pueda navegar y realizar configuraciones que le permitan tener o no acceso completo. Sistemas es el departamento encargado de proporcionar soluciones a los empleados; cualquier problema que incluya desde el uso de internet hasta el uso de programas que llevan en sus computadoras, debido a la demanda de equipos y programas, sistemas sabe que la seguridad de la información es una parte importante del servicio, junto con esto la administración de la direcciones para evitar redundancia y desconfianza entre equipos es por ello que se realiza una auditoria interna.

Justificación.

La administración de los equipos forma parte esencial de la seguridad en cualquier empresa, ya que facilita diferentes aspectos no solo la seguridad, la administración facilita el control, manejo, se adapta a las necesidades particulares de cada organización.

Se decide aplicar una auditoria interna ya que es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización, entre esas operaciones incluye estructura, identificación de equipos, aplicación de vlans.

Objetivo general.

Identificar y proporcionar un diagnóstico de la estructura de redes de Grand Palladium Hotel Group mediante la aplicación de una auditoria lógica interna que facilite la ubicación de las direcciones ip, control de puertos, switchs y servidores que administran las redes.

Objetivos específicos.

- Recopilar la información actual de la estructura de redes del hotel.
- Investigar las normas aplicables a la estructuración de redes.
- Integrarse al proceso de identificación física para facilitar la búsqueda de puntos débiles.

Alcance.

Se tiene como alcance crear un documento que cuente con una propuesta de identificación del cable estructurado de Grand Palladium Hotel Group esto con el fin de ayudar a facilitar la identificación, facilitar solución de errores dentro de la comunicación.

Metodología.

CRMR son las siglas de “Computer resource management review”, su traducción más adecuada es “Evaluación de la gestión de recursos informáticos”. En cualquier caso, esta terminología quiere destacar la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio del management.

Una revisión de esta naturaleza no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones más rápidas a problemas concretos y notorios.

Supuestos de aplicación.

En función de la definición dada, la metodología abreviada CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.

Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor informático encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión.

Áreas de aplicación.

Las áreas en que el método CRMR puede ser aplicado se corresponden con las sujetas a las condiciones de aplicación señaladas en punto anterior:

- Gestión de Datos
- Control de Operaciones
- Control y utilización de recursos materiales y humanos
- Interfaces y relaciones con usuarios
- Planificación
- Organización y administración

Ciertamente, el CRMR no es adecuado para evaluar la procedencia de adquisición de nuevos equipos (Capacity Planning) o para revisar muy a fondo los caminos críticos o las holguras de un Proyecto complejo.

Objetivos

CRMR tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un Centro de Proceso de Datos. Las Recomendaciones que se emitan como resultado de la aplicación del CRMR, tendrán como finalidad algunas de las que se relacionan:

- Identificar y fijar responsabilidades
- Mejorar la flexibilidad de realización de actividades.
- Aumentar la productividad
- Disminuir costes
- Mejorar los métodos y procedimientos de Dirección.

Alcance

- Se fijarán los límites que abarcará el CRMR, antes de comenzar el trabajo.
- Se establecen tres clases:
- 1. Reducido. El resultado consiste en señalar las áreas de actuación con potencialidad inmediata de obtención de beneficios.
- 2. Medio. En este caso, el CRMR ya establece conclusiones y Recomendaciones, tal y como se hace en la auditoría informática ordinaria.

- 3. Amplio. El CRMR incluye Planes de Acción, aportando técnicas de implementación de las Recomendaciones, a la par que desarrolla las conclusiones.

Se desarrollaron las actividades correspondientes con base al siguiente cronograma:

| | | | 2016 | | | | | | | | | | | | | | | | | |
|--|---------------------------|--------------------|-------|---|---|---|---------|---|---|---|-------|---|---|---|-------|---|---|---|--|--|
| | | | Enero | | | | Febrero | | | | Marzo | | | | Abril | | | | | |
| Actividad | Entregables | Tiempo de entrega. | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | | |
| División y solicitud de la información de las redes | Esquema del área y redes. | Tiempo real | ■ | ■ | | | | | | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Definición de objetivo general, específicos y alcance. | Documento | Tiempo real | | ■ | ■ | | | | | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Investigación y diseño de instrumentos para la auditoría | Cuestionarios | Tiempo real | | | | ■ | ■ | | | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Investigación y verificación de las normas | Documento | Tiempo real | | | | ■ | ■ | | | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Observación y análisis de las redes | | Tiempo real | | | | ■ | ■ | ■ | ■ | ■ | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Reestructuración lógica de las redes | Esquema | Tiempo real | | | | | | ■ | ■ | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Evaluación de la estructura de redes | Documento | Tiempo real | | | | | | | ■ | ■ | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Creación de informe por prueba | Documento | Tiempo real | | | | | ■ | ■ | ■ | ■ | ■ | ■ | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Corrección de los resultados, observaciones y recomendaciones. | | Tiempo real | | | | | | | | | | | ■ | ■ | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Elaboración del informe final. | Documento | Tiempo real | | | | | | | | | | | | | | | ■ | | | |

| | | | | | | | | | | | | | | | | | | | | |
|--------------------------|-----------|--------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Elaboración de la tesina | Documento | Tiempo real | | | | | | | | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |
| Cierre de estadia. | Documento | Tiempo real | | | | | | | | | | | | | | | | | | |
| | | Tiempo prog. | | | | | | | | | | | | | | | | | | |

Tabla 1. Cronograma de actividades.

Diseño de estrategias.

Investigación de normas aplicables a la auditoría.

Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña ya la información que rinde como resultado de este trabajo.

Las normas de auditoría se clasifican en:

- a. Normas personales.
- b. Normas de ejecución del trabajo.
- c. Normas de información.

Normas personales

Son cualidades que el auditor debe tener para ejercer sin dolo una auditoría, basados en un sus conocimientos profesionales así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.

Normas de ejecución del trabajo

Son la planificación de los métodos y procedimientos, tanto como papeles de trabajo a aplicar dentro de la auditoría.

Normas de información

Son el resultado que el auditor debe entregar a los interesados para que se den cuenta de su trabajo, también es conocido como informe o dictamen.

Normas de ejecución del trabajo.

ISO 27001.

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento;

ISO 27004. Creada para complementar la ISO 27001, nos enseña cómo debemos medir dichos controles, su objetivo consiste en hacerlos medibles. El uso de esta normativa constituye una medición de la seguridad de la información. El sistema de gestión de la seguridad de la información nos ayudará evaluar y a identificar aquellos procesos o normas ineficaces en nuestro sistema de la seguridad de la información, así como los controles y prioridades de las acciones asociadas. Esta normativa aconseja sobre las siguientes actividades.

- Medida de desarrollo
- Aplicación y operación de un programa de seguridad de la información en relación a la medición.
- Recogida y análisis de datos
- Elaboración de los resultados de la medición
- Comunicar los resultados de la medición desarrollados para las partes interesadas.
- Utilizar los resultados de medición a la hora de tomar las decisiones relacionadas con el SGSI
- Utilizar los resultados de medición para mejorar el SGSI (alcance, políticas, controles, procesos, objetivos y procedimientos)
- Facilitar la mejora continua de la seguridad de la información Para finalizar hay que indicar que con dicha normativa nunca se podrá garantizar la seguridad total.

Diagramas.

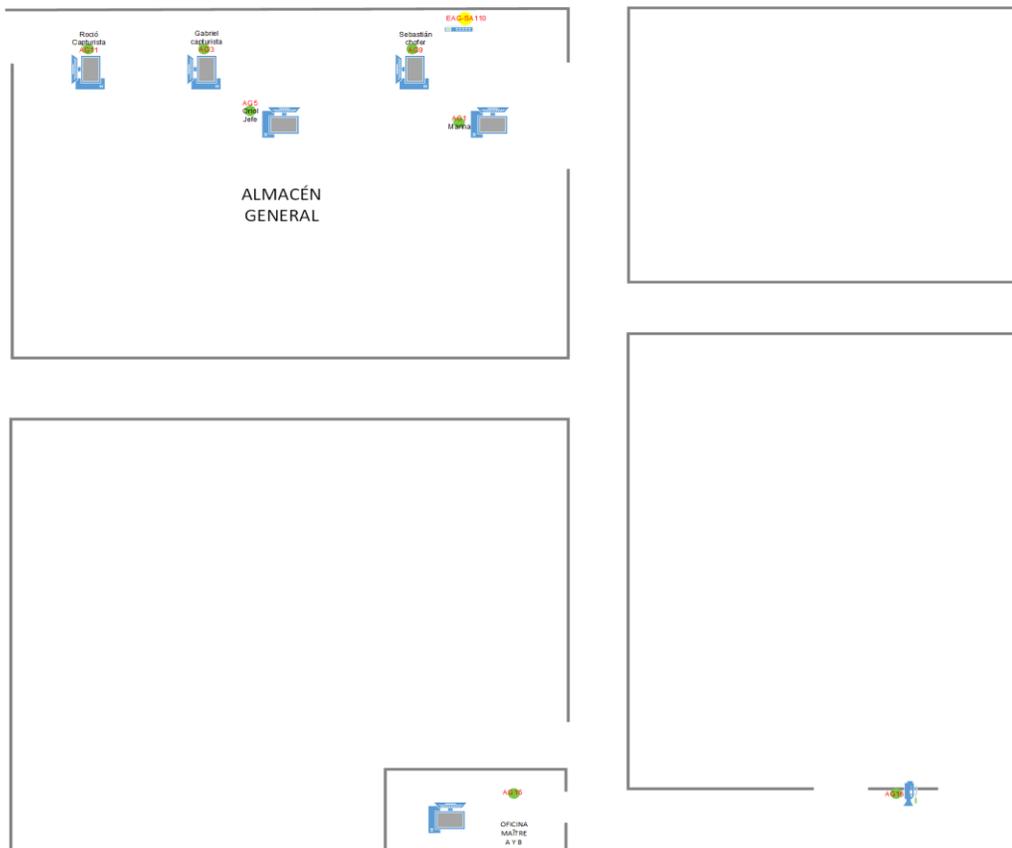
Departamentos RRHH imagen 1, bodas imagen 3, almacén de mantenimiento imagen 2.

Composición de algunos de los departamentos y nos permiten ver de manera gráfica la distribución de las máquinas.

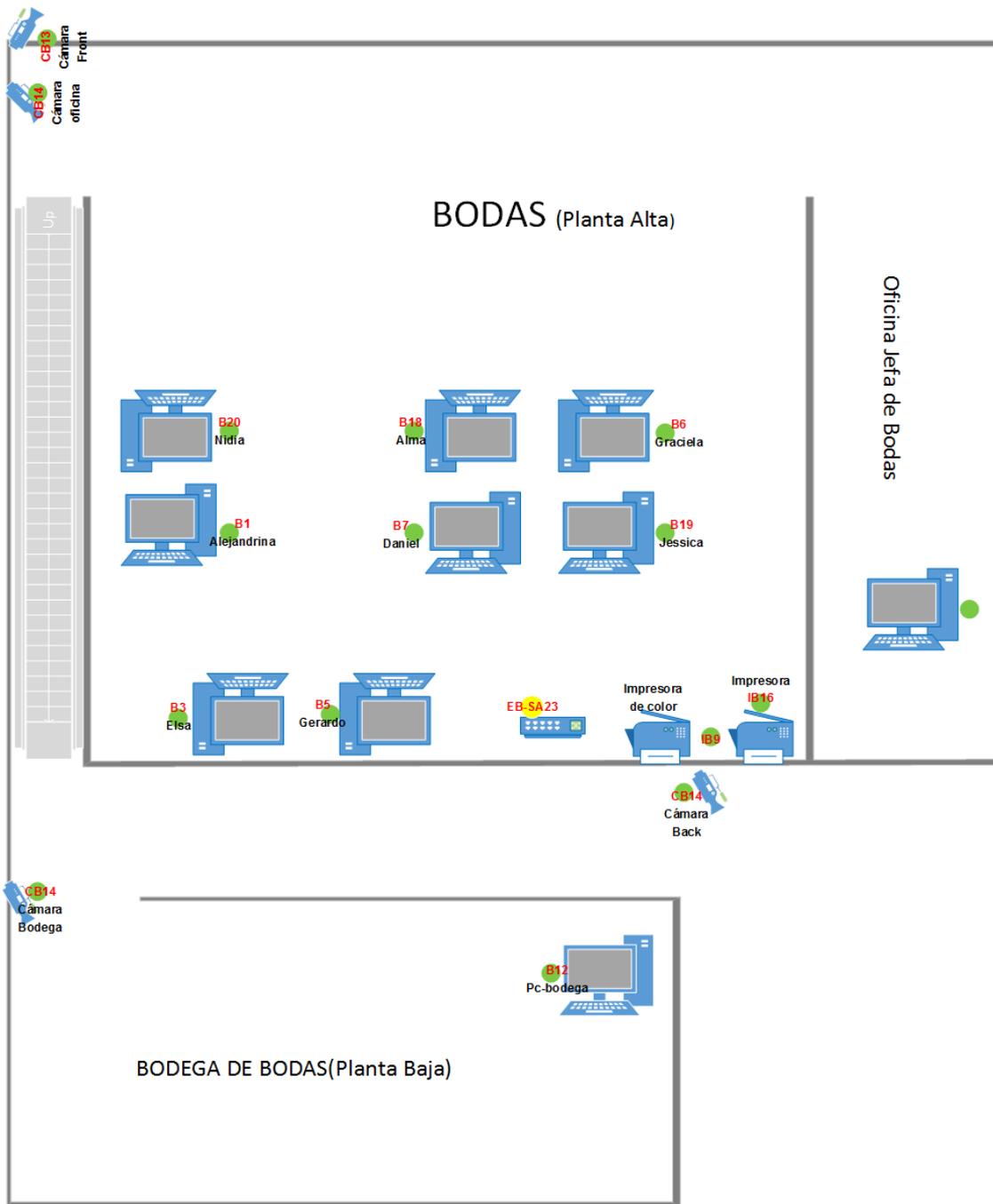
En la imagen número 4 nos muestra la nueva estructura que se desea implementar con los vlans y la identificación de puertos y patch panel.



1 Diagrama del departamento de RRHH



2 Almacén general.



3 *Departamento de bodas*

Procedimiento.

Dentro de este apartado se decide realizar un cuestionario básico adquiriendo así toda la información necesaria para realizar las conclusiones y resultados para el diagnóstico y propuesta de mejora. También se agrega evidencia del registro que se realizó durante la estadía, de los dispositivos, departamentos y vlans, esta evidencia se encuentra en el apartado de anexos con el título de ilustración, abarcando el número desde la 8 a la 11; el proceso de etiquetado se hizo mediante el uso de una impresora de etiquetas marca Brother modelo p-touch que facilitaba la creación de etiquetas y garantizando mayor duración de éstas.

Evaluación de la estructura del departamento y redes.

El siguiente cuestionario fue aplicado al asistente de sistemas, quien es el encargado del etiquetado e identificación de equipos.

1. El lugar donde se ubica el departamento de sistemas, ¿está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?
2. ¿El centro de servidores da hacia el exterior?
3. ¿El material con que está construido el departamento de sistemas es confiable?
4. ¿Dentro del centro de servidores existen materiales que puedan ser inflamables o causar algún daño a los equipos?
5. ¿Existe lugar suficiente para los equipos?
6. ¿Aparte del departamento de sistemas se cuenta con algún lugar para almacenar otros equipos de cómputo, muebles, suministros, etc.?
7. ¿Es adecuada la iluminación del departamento de sistemas?
8. ¿La temperatura a la que trabajan los equipos es la adecuada de acuerdo a las normas bajo las cuales se rige?
9. ¿La ubicación de los aires acondicionado es adecuada?
10. ¿Existe algún otro medio de ventilación aparte del aire acondicionado?
11. ¿El aire acondicionado emite algún tipo de ruido?
12. ¿La tierra física cumple con los requisitos establecidos en las normas bajo las cuales se rige?

13. ¿El cableado se encuentra correctamente instalado?
14. ¿Los contactos de los equipos de cómputo están debidamente identificadas?
15. ¿Los equipos cuentan con un regulador?
16. ¿Se verifica la regulación de las cargas máximas y mínimas?
17. ¿Se tiene switch de apagado en caso de emergencia en algún lugar visible?
18. ¿Los cables están dentro de paneles y canales eléctricos?
19. ¿Los interruptores de energía están debidamente protegidos y sin obstáculos para alcanzarlos?
20. ¿Se cuenta con alarma contra incendios?
21. ¿Dónde se encuentran ubicadas?
22. ¿Se cuenta con extintores?
23. ¿Dónde se encuentran ubicadas?
24. ¿Cuentan con manuales para cada programa que se maneja?
25. ¿El personal sabe del contenido de estos manuales?
26. ¿Qué tipo de mantenimiento realizan?
 - a. Preventivo b. Correctivo
27. ¿Qué materiales utilizan para realizar el mantenimiento de cables?
28. ¿Tienen un lugar específico para guardar el material de mantenimiento de cables?
29. ¿Los usuarios tienen la suficiente confianza como para presentar su queja cuando fallan los equipos?
30. ¿Con que tipo de topología de red cuenta?
31. ¿Qué compañía tiene usted contratada de internet?

Conclusiones.

Con la creación del cuestionario se llegó a la conclusión de que existe el peligro en cuanto a robo pues algunas veces la oficina ubicada en la zona de Colonial solía no estar cerrada y gente externa podía entrar fácilmente, ninguno de los cuartos de servidores se encontraba con contacto al exterior, el material era de buena calidad, uno de los centros de servidores se encontraba con cables, teclados, impresoras inservibles por falta de espacio, la iluminación era adecuada, cada cuarto de servidores era monitoreado para checar la temperatura de estos, no existían otros medios de ventilación únicamente aire acondicionado, el cableado se encuentra mal instalado, no tiene orden y no está etiquetado, tal y como se muestra en las imágenes que se anexan, la mayoría de los equipos se encuentra con regulador de corriente pero no se realizan chequeos de cargas mínimas o máximas, los switch de apagado y encendido se encuentran etiquetados y separados por secciones, el mantenimiento que se realiza es de tipo correctivo, se cuenta con topología de red de tipo estrella, existen manuales para el uso de todos los programas donde explican de que tratan y algunos pasos o recomendaciones de cómo utilizarlos.

Propuesta de solución.

Cualquiera de las normas nombradas a continuación podrían ser utilizadas para realizar el etiquetado de cableado estructurado, pero más adelante se hace la recomendación de cuál sería más aplicable; TIA/EIA606, UNE-EN 50174-1:2011 o ISO/IEC 14763-1:1999, estos estándares están enfocados al etiquetado de cables estructurados facilitando y agilizando los movimientos, adiciones o cambios, cuyo único objetivo es seguir los lineamientos de administración y, consecuentemente, de identificación de un sistema de cableado estructurado.

Se utiliza la metodología CRMR sus siglas en español quieren decir “Evaluación de la Gestión de Recursos Informáticos” en clase media ya que esta nos permite establecer conclusiones y recomendaciones.

Se propone el etiquetado de cableado estructurado basado en la norma TIA/EIA606-A para facilitar la ubicación de conexiones de los cables facilitando futuras migraciones, detección de errores e identificación de departamentos. Se selecciona esta norma ya que fijan reglas precisas para ser cumplidas por el instalador permitiendo así tener un control adecuado evitando que las etiquetas tengan nomenclatura diferente haciéndolas imprecisas y difíciles de ubicar.

En el caso de Palladium Hotel Group la clase corresponde al número 3, ya que está enfocada en sistemas que están diferentes edificios, existiendo por tanto varios cuartos de telecomunicaciones.

Ejemplo de etiquetado:

E1-1C-B15: Edificio1, primera planta, rack C, panel de parcheo B, toma 15.

Los elementos deben de ser etiquetados, tanto en los cuartos de telecomunicaciones como en las áreas de trabajo.

La fiabilidad de una instalación de cableado estructurado depende de una administración eficaz y que ningún sistema de cableado puede ser administrado correctamente sin un etiquetado lógico y claro.

En cuanto al etiquetado de equipos como lo son laptops y computadoras de escritorio, se tenía preestablecida una nomenclatura, esto dificultó la posibilidad de cambiar pues dentro de documentos ya se tenía registrado y un 90% de los equipos se encontraban etiquetados, la nomenclatura era la siguiente:

Dispositivos de escritorio:

Tercer número perteneciente al IP-000-último número de la IP-PC

030-000-130-PC

Dispositivos portátiles:

Tercer número perteneciente al IP-001-último número de la IP-PO

030-000-131-PO

Referencias.

(Dpto. Electrónica IEFPS Tartanga Erandio Bizkaia, 2014)

(BSIGroup, s.f.)

(Quirós, 2010)

Apéndices o Anexos.

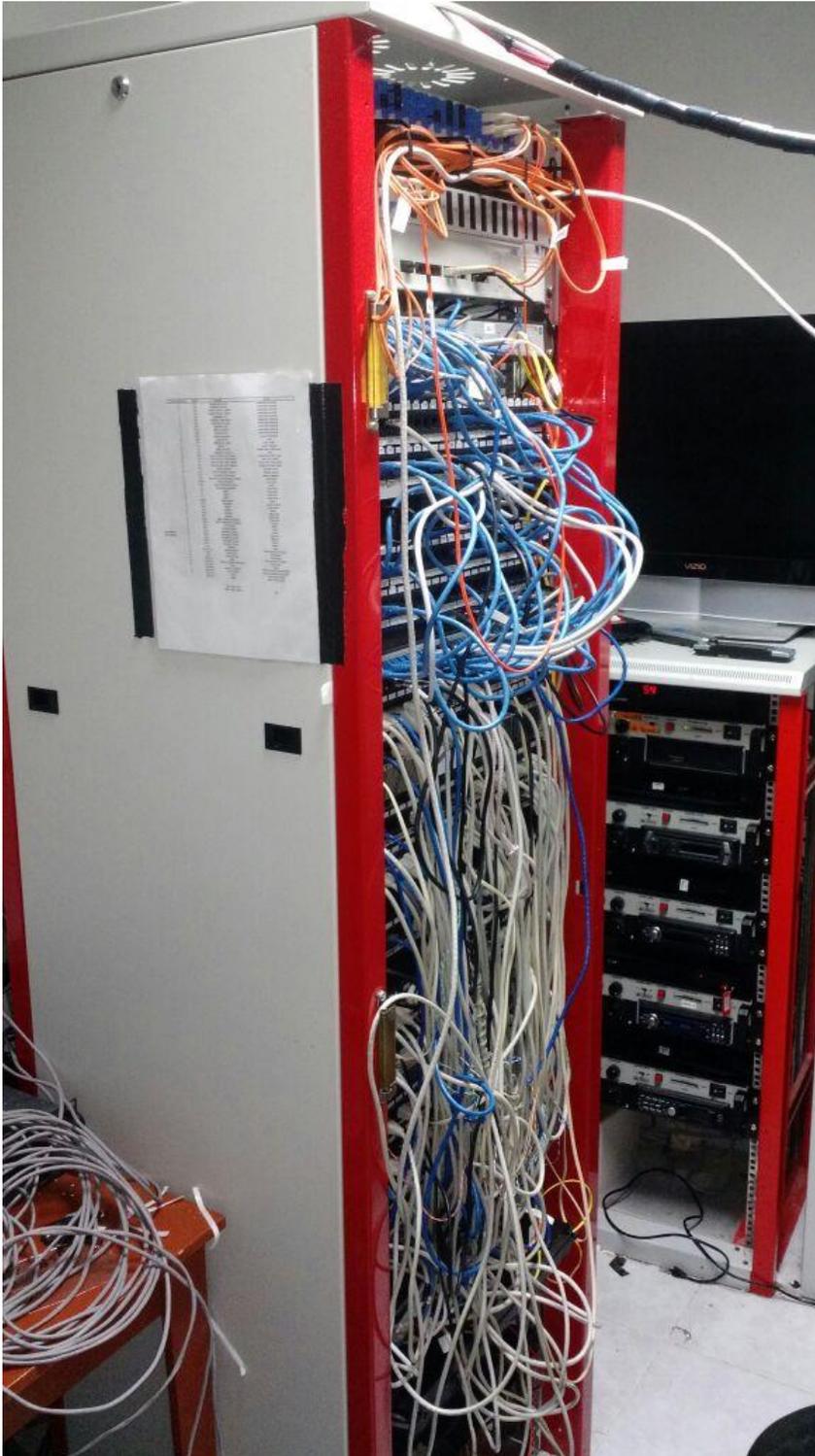


Ilustración 5 Switch que controla la fase 2 y proporciona conexión entre edificio 1 y 2.

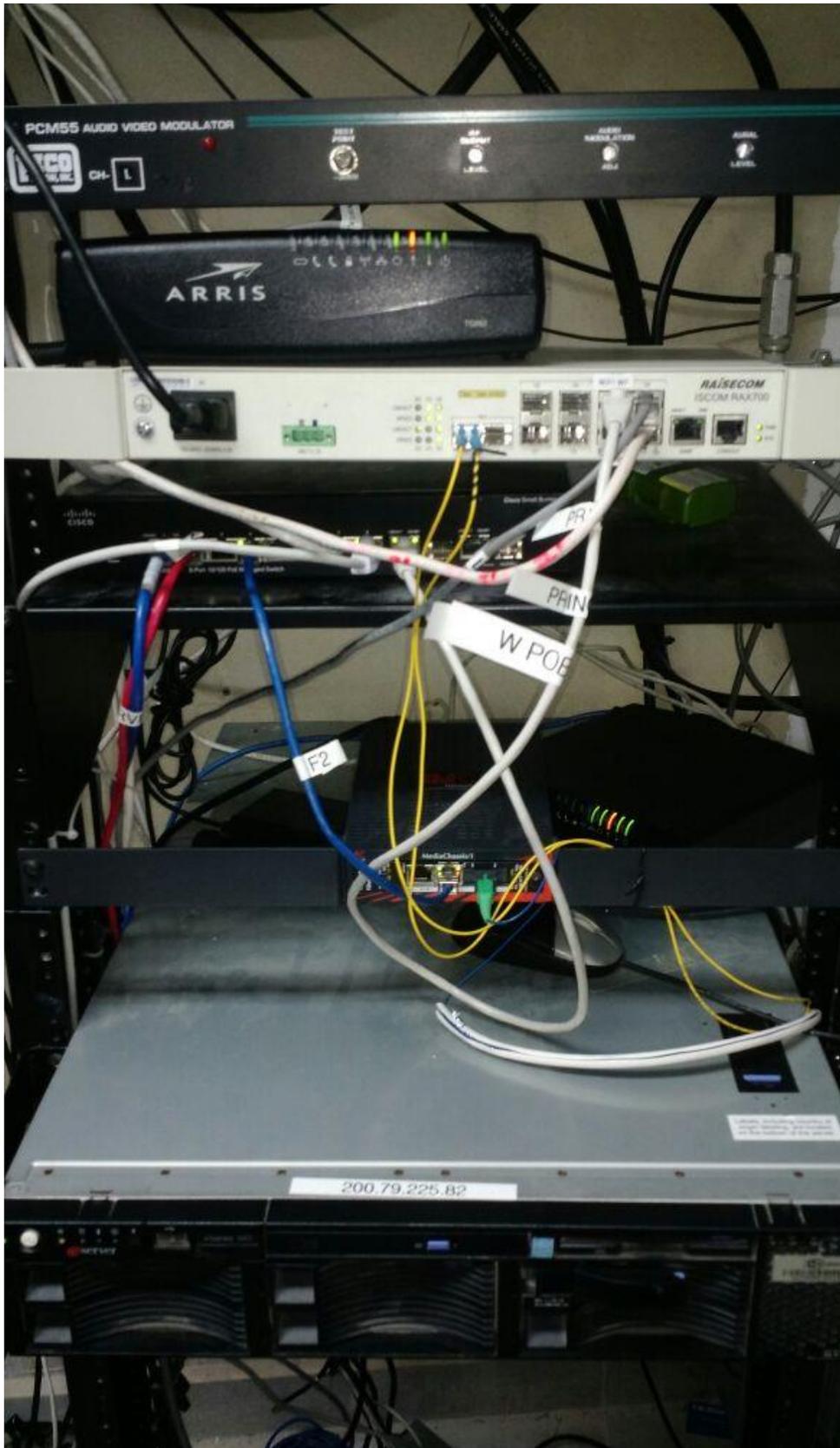
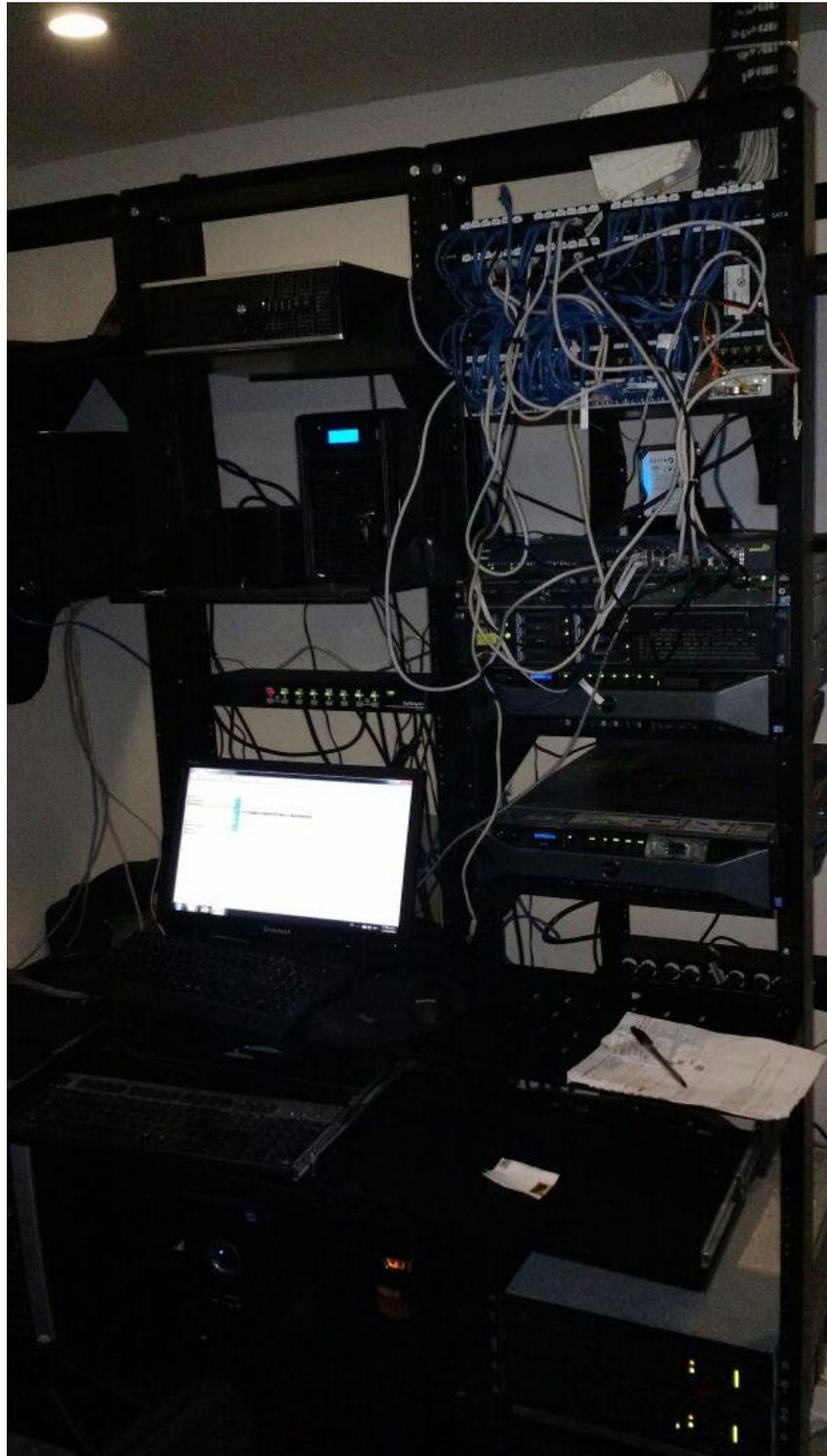


Ilustración 6 Switch 3com que controla departamento de bodas.

Ilustración 7 Cuarto de servidores, controla los programas principales y el servicio de red.



| | VLAN | | | | | | | | | | | DESCRIPCIÓN | DESCRIPCIÓN | | | | | | |
|----|------|----|----|----|------|------|------|------|------|------|------|-------------|-------------|------|------|-----------------------|----------------|-------------------|--------------|
| | 1 | 20 | 30 | 50 | 1000 | 1030 | 1031 | 1096 | 1114 | 1200 | 1720 | | 1721 | 1800 | 2500 | ID | NOMBRE | VLAN | U = UNTAGGED |
| 1 | U | | | | | | | | | | | | | | | | | | |
| 2 | T | T | T | T | | | | | T | U | T | T | | | 1 | Default VLAN | 1,5,20,25,26 | 2,11-21,27 | |
| 3 | | | | | | | | | | U | T | T | | | 20 | WINET PREMIUM-GESTION | 23 | 2,30,31,34,37 | |
| 4 | | | | | | | | | | | | | | | 30 | WINET PFG WIFI | | 2,3,20,21,33,37 | |
| 5 | U | | | | | | | | | | | | | | 30 | WINET ROYAL | | 2,20,21,33,37 | |
| 6 | | | | | | | | | | | | | | | 1000 | Administrativa | | 20,24 | |
| 7 | | | | | | | | | | T | | | | | 1090 | FASE I | | 2,20,32 | |
| 8 | | | | | | | | | U | U | T | | | | 1031 | FASE II | | 2,20,32 | |
| 9 | | | | | | | | | U | | | | | | 1096 | KMC | 17-19 | 20,24 | |
| 10 | | | | | | | | | | | U | | | | 1114 | Mangadora | 9,11-16,38 | 2,20,24 | |
| 11 | | | | | | | | | U | | | | | | 1100 | Gestion Switch | 2-5,8,11,33,37 | 2,20,24 | |
| 12 | | | | | | | | | U | | | | | | 1720 | WPHG | 10 | 2-5,8,10,11,24,27 | |
| 13 | | | | | | | | | U | | | | | | 1721 | PTC-URCOISA | 4 | 2-3,10,31,37 | |
| 14 | | | | | | | | | U | | | | | | 1800 | SSID_oficio_01 | 6,7 | 8,20,32 | |
| 15 | | | | | | | | | U | | | | | | 2500 | DATOS BLOQUE K | | 8,20 | |
| 16 | | | | | | | | | U | | | | | | | | | | |
| 17 | | | | | | | | | U | | | | | | | | | | |
| 18 | | | | | | | | | | | | | | | | | | | |
| 19 | | | | | | | | | | | | | | | | | | | |
| 20 | U | T | T | T | T | T | T | T | T | T | T | T | T | | | | | | |
| 21 | T | | | | | | | | | | | | | | | | | | |
| 22 | T | T | T | T | | | | | | U | | | | | | | | | |
| 23 | | U | T | T | | | | | | | U | T | T | | | | | | |
| 24 | | | | | | | | | T | T | T | T | | | | | | | |
| 25 | U | | | | | | | | | | | | | | | | | | |
| 26 | U | | | | | | | | | | | | | | | | | | |
| 27 | T | T | T | T | | | | | | | | | | | | | | | |
| 28 | T | T | T | T | | | | | U | | U | T | T | | | | | | |

Ilustración 8 Documentación de la dirección 10.30.200.11

| | VLAN | | | | | | | | | | | DESCRIPCIÓN | DESCRIPCIÓN | | | | | | |
|----|------|----|----|----|------|------|------|------|------|------|------|-------------|-------------|----|--------|------|--------------|------------|--|
| | 1 | 20 | 30 | 50 | 1000 | 1030 | 1031 | 1114 | 1120 | 1200 | 1720 | | 1721 | ID | NOMBRE | VLAN | U = UNTAGGED | T = TAGGED | |
| 1 | U | | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | U | | | | | | | | |
| 3 | T | T | T | T | | | | | | | U | T | T | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | |
| 5 | U | | | | | | | | | | | | | | | | | | |
| 6 | U | | | | | | | | | | | | | | | | | | |
| 7 | U | | | | | | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | | | | | | | |
| 11 | U | | | | | | | | | | | | | | | | | | |
| 12 | | | | | | | | | | | | | | | | | | | |
| 13 | U | | | | | | | | | | | | | | | | | | |
| 14 | U | | | | | | | | | | | | | | | | | | |
| 15 | U | | | | | | | | | | | | | | | | | | |
| 16 | T | | | | | | | | | | | | | | | | | | |
| 17 | U | T | T | T | T | T | T | | | | | | | | | | | | |
| 18 | U | | | | | | | | | | | | | | | | | | |
| 19 | U | | | | | | | | | | | | | | | | | | |
| 20 | | U | | | | | | | | | | | | | | | | | |
| 21 | U | | | | | | | | | | | | | | | | | | |
| 22 | T | | | | | | | | | | | | | | | | | | |
| 23 | U | | | | | | | | | | | | | | | | | | |
| 24 | U | | | | | | | | | | | | | | | | | | |
| 25 | U | | | | | | | | | | | | | | | | | | |
| 26 | U | | | | | | | | | | | | | | | | | | |
| 27 | U | | | | | | | | | | | | | | | | | | |
| 28 | U | T | T | T | | | | | T | T | T | T | T | | | | | | |

Ilustración 9 Documentación de la dirección 10.30.200.12

