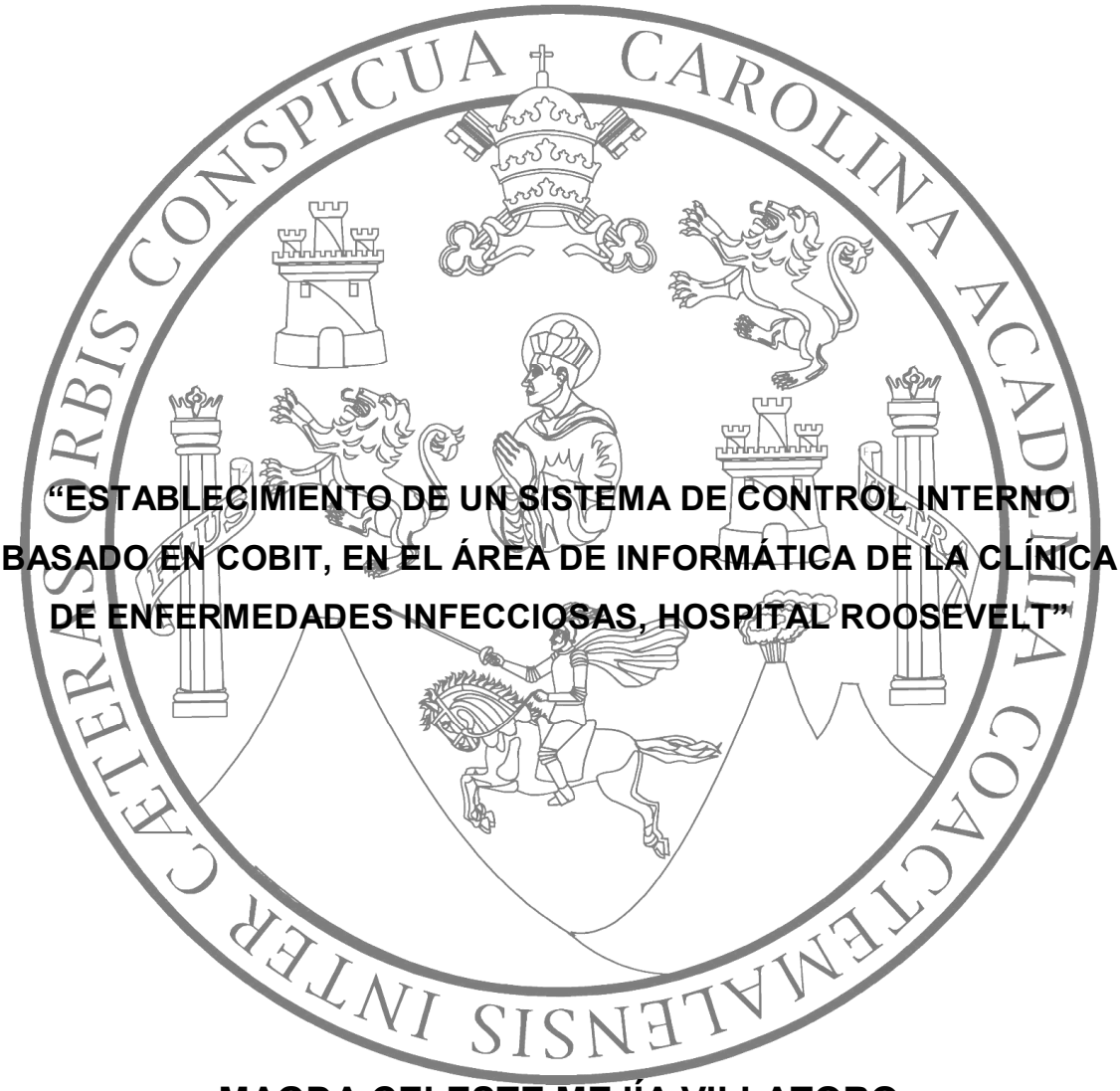
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONÓMICAS



"ESTABLECIMIENTO DE UN SISTEMA DE CONTROL INTERNO BASADO EN COBIT, EN EL ÁREA DE INFORMÁTICA DE LA CLÍNICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT"

MAGDA CELESTE MEJÍA VILLATORO
CONTADORA PÚBLICA Y AUDITORA

GUATEMALA, FEBRERO DE 2011

MIEMBROS DE LA JUNTA DIRECTIVA DE LA

FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. José Rolando Secaida Morales
Secretario	Lic. Carlos Roberto Cabrera Morales
Vocal Primero	Lic. Albaro Joel Girón Barahona
Vocal Segundo	Lic. Mario Leonel Perdomo Salguero
Vocal Tercero	Lic. Juan Antonio Gómez Monterroso
Vocal Cuarto	P.C. Edgar Arnoldo Quiché Chiyal
Vocal Quinto	P.C. José Antonio Vielman

EXONERADA DE EXÁMENES DE ÁREAS PRÁCTICAS BÁSICAS

De conformidad con los requisitos establecidos en el capítulo III, articulo 15 y 16 del Reglamento para la Evaluación Final de Exámenes de Áreas Prácticas Básicas y Examen Privado de Tesis y al inciso del punto 6.3, del Acta 26-2009 de la sesión celebrada por Junta Directiva el 24 de Noviembre de 2009.

PROFESIONALES QUE REALIZARON EL EXAMEN PRIVADO DE TESIS

PRESIDENTE	Lic. Jorge Luis Monzón Rodríguez
SECRETARIO	Lic. Jorge Luis Reyna Pineda
VOCAL	Lic. Felipe Hernández Sincal

Lic. MSc. Albaro Joel Girón Barahona
CONTADOR PÚBLICO Y AUDITOR
Colegiado No. 1047
MASTER EN CONSULTORÍA TRIBUTARIA

Guatemala,
22 de julio de 2010

Licenciado
José Rolando Secaida Morales
Decano de la Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Su Despacho

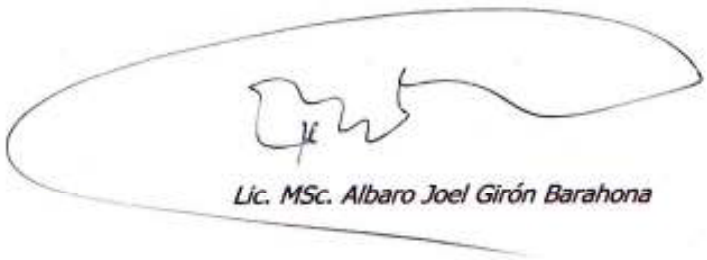
Respetable Señor Decano:

De conformidad con la designación para asesorar a MAGDA CELESTE MEJÍA VILLATORO, en su trabajo de tesis denominado "ESTABLECIMIENTO DE UN SISTEMA DE CONTROL INTERNO BASADO EN COBIT, EN EL ÁREA DE INFORMÁTICA DE LA CLÍNICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT", me permito informarle que, de acuerdo con la revisión efectuada, el trabajo indicado llena los requisitos que el reglamento establece.

El trabajo referido constituye un valioso aporte para los profesionales de las ciencias económicas y personas interesadas en COBIT. Además, en vista de la trascendencia del tema para los Contadores Públicos de nuestro país, la investigación realizada reviste particular relevancia. En tal virtud, en opinión del suscrito, el trabajo presenta una investigación cuya actualidad y calidad, reúne los requisitos académicos necesarios que el caso amerita.

Con base en lo anteriormente expuesto, recomiendo que el trabajo realizado sea aprobado para su presentación por MAGDA CELESTE MEJÍA VILLATORO, en el Examen Privado de Tesis, previo a conferírsele el título de Contadora Pública y Auditora en el grado de Licenciada.

Atentamente,



Lic. MSc. Albaro Joel Girón Barahona

11 calle B 32-74 zona 7, Col. Centroamérica
Telefax: 24397194
Correo Electrónico: *ajgb2007@hotmail.com* ***y*** *albarogiron@yahoo.com*

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE
CIENCIAS ECONOMICAS
Edificio "S-8"
Ciudad Universitaria, Zona 12
Guatemala, Centroamérica

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA, ONCE DE ENERO DE DOS MIL ONCE.

Con base en el Punto QUINTO, inciso 5.3, subinciso 5.3.1 del Acta 21-2010 de la sesión celebrada por la Junta Directiva de la Facultad el 26 de noviembre de 2010, se conoció el Acta AUDITORIA 205-2010 de aprobación del Examen Privado de Tesis, de fecha 2 de noviembre de 2010 y el trabajo de Tesis denominado: "ESTABLECIMIENTO DE UN SISTEMA DE CONTROL INTERNO BASADO EN COBIT, EN EL ÁREA DE INFORMÁTICA DE LA CLINICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT", que para su graduación profesional presentó la estudiante **MAGDA CELESTE MEJÍA VILLATORO**, autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

FACULTAD DE CIENCIAS ECONOMICAS
EL SECRETARIO
Guatemala, C. A.

LIC. JOSE ROLANDO SECAIDA MORALES
DECANO

FACULTAD DE CIENCIAS ECONOMICAS
EL DECANO
GUATEMALA, C. A.

Smp.

Ingrid

ACTO QUE DEDICO

A DIOS	TODO LO QUE HAGÁIS, HACEDLO DE CORAZÓN, COMO PARA EL SEÑOR Y NO PARA LOS HOMBRES **Colosenses 3:23**
A MIS PADRES	CARLOS MEJÍA LEMUS MAGDA VILLATORO DE MEJÍA **Gracias**
A MIS HIJOS	MAGDA PATRICIA DIANA CAROLINA ROLANDO ALEJANDRO **Que este triunfo sea un ejemplo para ellos**
A MIS HERMANOS	CARLOS RODOLFO SERGIO RAUL MARIO ROBERTO MARCO ANTONIO **Gracias**
A MIS SOBRINOS	CARLOS ROBERTO MARÍA JHANNINE **SANTIAGO MARTÍN Muy especialmente!** RICARDO ANTONIO DIEGO FELIPE JOSE ADOLFO RODRIGO ALBERTO MARÍA ALEJANDRA **Por el amor que siempre me han brindado**
A MIS CUÑADAS	HILDA LETICIA LESLY ROSANA
A MI ASESOR DE TESIS	**LICENCIADO ALBARO JOEL GIRÓN BARAHONA** Gracias por todos los conocimientos trasmitidos, por su sincera amistad y comprensión.
AL SEÑOR DECANO DE LA FACULTAD DE CIENCIAS ECONÓMICAS	**LICENCIADO JOSÉ ROLANDO SECAIDA MORALES** Por su contribución académica en mi recorrido por esta casa de estudios.
A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA	

ÍNDICE

CAPÍTULO III

COBIT (Objetivos de control para la información y la tecnología relacionada)

CAPÍTULO IV
ESTABLECIMIENTO DE UN SISTEMA DE CONTROL INTERNO BASADO EN COBIT, EN EL ÁREA DE INFORMÁTICA DE LA CLÍNICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT
(CASO PRÁCTICO)

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

INDICE DE FLUJOGRAMAS

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nuevas tecnologías. Por lo tanto, la administración de la Clínica de Enfermedades Infecciosas, Hospital Roosevelt tomó esto en cuenta y decidió tener un entendimiento básico de los riesgos y limitantes del empleo de la tecnología de información para proporcionar una dirección efectiva y controles adecuados.

Es por eso que se realizó un estudio del establecimiento de controles en el área de Informática basada en COBIT 4.1 (OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y LA TECNOLOGÍA RELACIONADA); que ayudará a salvar las brechas existentes entre riesgos de la organización, necesidades de control y aspectos técnicos. Proporcionará "prácticas sanas" por medio de un marco referencial de dominios y procesos, presenta actividades en una estructura manejable y lógicas. Las prácticas sanas de COBIT representan el consenso de los expertos (ayudarán a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo que serán juzgados si las cosas salen mal).

Las organizaciones deben cumplir con requerimientos de calidad y de seguridad, tanto para su información, como para sus activos. La administración de la Clínica de Enfermedades Infecciosas deberá obtener un balance adecuado en el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la administración deberá establecer un sistema adecuado de control interno en el área de informática.

Metodología

La investigación se realizó en base al método científico deductivo, por medio de varias etapas que consistieron en la elaboración de un plan de trabajo, cronograma de actividades, consultas de fuentes secundarias y documentos relacionados con el tema

general, visita de reconocimiento a la Clínica de Enfermedades Infecciosas, Hospital Roosevelt, entrevistas, cuestionarios al personal administrativo y operativo de la entidad, para obtener de ellos, información importante, así como el estudio de toda la documentación relacionada con TI perteneciente a la institución, respecto a la situación actual de la clínica.

El análisis estadístico efectuado sobre los datos e información recolectada permitió determinar necesidades y grado de convencimiento tanto de autoridades de la clínica como de las personas que laboran en la misma sobre establecimiento de controles en el área de informática.

Como resultado de la investigación se presentan cuatro capítulos, en los que se desarrollan aspectos generales de la entidad, análisis de qué es control interno, aspectos del Marco COBIT 4.1 y un diagnóstico de madurez de la entidad en el que se encuentran, nivel general en los cuatro Dominios de 2, donde los procedimientos de control todavía se dan en forma intuitiva y no definida. Es importante señalar que algunos términos utilizados en este trabajo son complejos por lo que es recomendable utilizar el glosario de términos **(Anexo 1).**

El primer capítulo, se refiere a los antecedentes y características de la Institución así como qué tipo de actividades realiza el personal que labora en la misma, fondos con los que cuenta, Organización, Misión, Visión, ilustra sus operaciones más importantes en relación al tratamiento y diagnóstico de enfermedades que atienden en la entidad: SIDA, MALARIA, TUBERCULOSIS y otras.

El segundo capítulo, se orienta a un análisis de control interno desde el año 1949, hasta la evolución que dio paso al Informe COSO (por las siglas en inglés del comité que patrocinó los estudios que lo produjeron) en 2002, se analiza COSO II ERM así como COBIT, (focalizado en controles en materia de tecnología).

El tercer capítulo, presenta un análisis más concreto sobre COBIT; comienza estudio, evolución de COBIT 3ª Edición a COBIT 4.1, qué representan los dominios, los 34

procesos, objetivos de control detallados, aspectos generales del Informe COBIT, institución que realiza investigaciones sobre el mismo (ISACA), sin ánimo de lucro, y descripción del proyecto.

El cuarto capítulo, presenta el diagnóstico del nivel de madurez en el área de control de la organización, primera prueba de controles y análisis basado en los cuatro dominios COBIT.

Finalmente se presentan conclusiones, recomendaciones, resultado del análisis así como anexos: Glosario de términos, Manual de Seguridad Informática, Manual de Elección de proveedores. Todo con el propósito de contribuir al mejoramiento de la seguridad informática, cuya aplicación sea de beneficio y utilidad para la Administración de la Clínica de Enfermedades Infecciosas, Hospital Roosevelt, en la actualidad y en el futuro, pero sobre todo en beneficio de los pacientes.

CAPÍTULO I

CLÍNICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT

1.1 Antecedentes

La Clínica de Enfermedades Infecciosas del Hospital Roosevelt es la División de Seguimiento por Consulta Externa de la Unidad de Enfermedades Infecciosas del Departamento de Medicina Interna del Hospital Roosevelt de la ciudad de Guatemala. Nació en los años 70 como una necesidad para brindar seguimiento a los pacientes del Departamento de Traumatología y Ortopedia con problemas infecciosos tales como: osteomielitis aguda y crónica y artritis séptica. Funcionó de esta manera hasta finales de la década de los 80, ofreció consulta una vez por semana. En agosto de 1989 sin una sede fija inicia el diagnóstico y seguimiento de personas infectadas con el virus de inmunodeficiencia humana que se empezaban a detectar esporádicamente en los servicios de encamamiento general del Departamento de Medicina. Actualmente su misión es prestar la atención integral debida a las personas que sospechan que tienen o que viven con el virus de la inmunodeficiencia humana y a los que padecen del síndrome de inmunodeficiencia adquirida, de forma oportuna y científica cuenta para ello con el personal capacitado y especializado, para mejorar la salud de las mismas, brinda una mayor esperanza de vida y optimizar los recursos disponibles para mejorar la calidad de atención. Realizar las gestiones necesarias para la adquisición de donantes de medicamentos para los pacientes que viven con el VIH y/o que padecen de SIDA. Así como gestionar el lugar y la construcción de la nueva clínica de SIDA que dará albergue a XX pacientes. Desarrollar un sistema de registro de datos que identifique adecuadamente el comportamiento de los casos y de respuesta a las necesidades de información sobre el avance de la epidemia que ofrezca la oportunidad de identificar adecuadamente formas de prevención y que conduzca a una administración de la clínica de forma moderna y ágil . Además de la infección por VIH, la clínica atiende personas con infecciones crónicas serias que requieren manejo más

especializado, tales como: osteomielitis agudas y crónicas, artritis sépticas, hepatitis virales agudas y crónicas, micosis sistémicas fuera del contexto de la Infección VIH, Infecciones de Transmisión sexual y Tuberculosis complicadas. En el año 2002 se ha iniciado el seguimiento y tratamiento de la Enfermedad de Chagas en un Proyecto conjunto con la Facultad de Ciencias Químicas y Farmacia de la Universidad de San Carlos de Guatemala y el Programa de Vectores del Ministerio de Salud Pública y Asistencia Social. El apoyo de la Oficina Sanitaria Panamericana con proyectos que han fortalecido el diagnóstico microbiológico de las principales infecciones oportunistas que afectan a las personas que viven con VIH, ha contribuido con los esfuerzos locales tanto de la Unidad de Enfermedades Infecciosas del Departamento de Medicina, como de la Sección de Microbiología del Departamento de Laboratorios Clínicos, a mejorar el pronóstico de las personas afectadas por infecciones serias provocadas por Criptococcus neoformans, Histoplasma capasulatum, Coccidiodes immitis y Micobacterium tuberculosis, y proveer a médicos, químicos biólogos, patólogos clínicos y farmacéuticos, en formación a desarrollar experiencia clínica en el diagnóstico, tratamiento y seguimiento de estos enfermos.

La demanda de atención ha tenido un crecimiento tan grande, que ya para el año 2004, y como beneficiarios del Fondo Mundial de Lucha contra el SIDA, la Malaria y la Tuberculosis Guatemala como país por medio de un tipo de organización bastante innovador dentro de la salud en el país, ha permitido estar en la misma mesa de negociaciones, tanto a quienes ejecutan las acciones como a la representación del Despacho del Ministro de Salud Pública, como a los directores de los Programas Nacionales de ITS-VIH-SIDA, al de Tuberculosis y al de Vectores, al lograr hasta ahora el país, ser uno de los países más exitosos en la implementación de la propuesta de SIDA, la cual inició en 2008, su cuarto año de trabajo.

Esta entidad Privada tiene como requisito la conformación de un ente nacional representativo y participativo denominado Mecanismo Coordinador de País, el cual en Guatemala ha sido muy activo y dentro del cual la clínica ha participado de manera muy activa desde el momento de preparación y sometimiento de las propuestas de país no sólo para SIDA, sino también para Malaria y Tuberculosis. Este mecanismo de

país, escogió a una institución administrativa denominada en la terminología del Fondo Mundial (también conocido como Fondo global) a un receptor principal, que ejerce las funciones administrativo-financiero y logísticas para la implementación de la propuesta en las llamadas Unidades Ejecutoras, como el caso de la Clínica. El receptor principal de país es la Fundación Visión Mundial Guatemala y la contraparte del Hospital como sub-receptor es el Patronato de Asistencia Social del Hospital Roosevelt, con el aval de las direcciones del Hospital y de los Departamentos involucrados. Dado el nivel de especialización que se ha generado en la Clínica, ahora es centro de enseñanza para personal de salud que brindará atención en otras áreas del país como en Centroamérica. Se participa en múltiples actividades de formación de personal de salud, tanto a nivel del Hospital como de otras instituciones, a través de pláticas, cursos o bien con el desarrollo de trabajos de tesis de graduación, que aportan datos que de otra manera no podrían realizarse, incluyendo los proyectos más recientes de: Evaluación de pruebas rápidas para el desarrollo del algoritmo nacional de diagnóstico con la Universidad del Valle y CDC con el Programa Nacional de SIDA y la Prevalencia de Enfermedad de Chagas en pacientes con Infección VIH. Se han desarrollado múltiples investigaciones durante este período que han sido presentadas en Congresos internacionales como: Congreso Panamericano de Infectología, ICAAC (Interscienses Congreso on Antimicrobial Agents and Chemotherapy) de Estados Unidos, Internacional AIDS Society (IAS) y el Congreso de la ISID (Internacional Society of Infectious Diseases), así como Congresos local y regionales como el CONCASIDA (Congreso Centroamericano y del Caribe de SIDA).

El Proyecto de Prevención de la Transmisión vertical del VIH con patrocinio de UNICEF y APRESAL (Unión Europea), permitió ofrecer el tamizaje voluntario gratuito y confidencial a las mujeres que llegan a la Consulta Prenatal del Hospital Roosevelt y la Maternidad Periférica de la zona 19 en sus inicios en el año 2002-2003. Este Programa ha funcionado ininterrumpidamente desde agosto del 2002 en la Consulta Prenatal de Hospital Roosevelt, extendiéndose a otros 9 Hospitales Departamentales desde el segundo semestre del año 2005, ofrece de manera voluntaria y gratuita el tamizaje de

VIH, Hepatitis B y Sífilis a todas las mujeres que llegan a la Consulta prenatal de los centros incluidos.

- **Docencia**

El Diplomado en Atención Integral para la descentralización del manejo y tratamiento del VIH/SIDA, ha sido hasta diciembre 2007, una iniciativa de la Clínica de Enfermedades Infecciosas-Hospital Roosevelt, Clínica Familiar Luis Ángel García y la Fundación Preventiva del SIDA Fernando Iturbide, quienes ante la magnitud de la epidemia y las necesidades de recurso humano capacitado para enfrentar la epidemia, desarrolló en el período 2004 al 2007, cuatro diplomados de Atención Integral para diversas ramas de las Ciencias de la Salud y para la atención médica del VIH en el país. Por la necesidad de implementar cursos dirigidos a un mayor de número de profesionales, cada entidad ha sido dejada en libertad de organizar Diplomados de Atención Integral para llegar a un número mayor de profesionales, desde los centros de referencia del país, con la finalidad de fortalecer las necesidades de descentralización de la Atención, tan urgentemente necesaria en el país. Las metas de capacitación del Diplomado incluyen una serie de acciones en materia de información, educación y comunicación al personal de salud con el objetivo de diseminar el concepto de la Atención Integral del VIH-SIDA desde el punto de vista médico y coordinando con otras profesiones de las ciencias de la salud, con el fin de brindar una mejor calidad de vida y sobrevida, a las personas viviendo con el VIH-SIDA, con énfasis en el manejo adecuado del diagnóstico de la infección VIH, diagnóstico y manejo de infecciones oportunistas, así como el manejo correcto de la terapia antiretroviral. Es importante propiciar en un futuro próximo en el país, el desarrollo de esta nueva especialidad médica y de las ciencias de la salud, que está naciendo desde las especialidades de medicina interna y enfermedades infecciosas, la Medicina del VIH (HIV Medicine en inglés), la cual está en proceso de conformarse en países como Estados Unidos y Europa Occidental.

1.2 Valores éticos morales de la Clínica de Enfermedades Infecciosas, Hospital Roosevelt

- **Visión**

Contar con un ambiente específico, adecuado, moderno y con el personal especializado, capacitado y necesario para prestar atención integral con calidad, oportunidad y confiabilidad a pacientes que viven con virus de la inmunodeficiencia humana adquirida, brindar de forma personalizada las indicaciones necesarias para aceptar su enfermedad, proporcionar de forma científica y protocolizada los medicamentos necesarios para mejorar su estado de salud.

- **Misión**

Realiza gestiones necesarias para la adquisición de donantes de medicamentos para los pacientes que viven con el VIH y/o que padecen de SIDA. Desarrolla un sistema de registro de datos que identifique adecuadamente el comportamiento de los casos y de respuesta a las necesidades de información sobre el avance de la epidemia que brinde la oportunidad de identificar de forma adecuada formas de prevención.

Es importante mencionar que los valores éticos morales con que se conducen las personas que laboran en la Clínica en relación a la atención de los pacientes por enumerar algunos se encuentran los siguientes: autenticidad, compromiso, confidencialidad, cooperación, dedicación, discreción, empatía, equilibrio, respeto, responsabilidad, sensibilidad, sinceridad, solidaridad, unidad autoestima.

1.3 Servicios que presta la Clínica

1. Consejería y Tamizaje Voluntario para VIH.

2. Diagnóstico de la Infección VIH.

3. Seguimiento de la Infección VIH de manera ambulatoria.

4. Diagnóstico y Tratamiento de Infecciones oportunistas tanto ambulatorio como hospitalario.

5. Diagnóstico, seguimiento y tratamiento de la Infección VIH en el embarazo.

6. Manejo de muestras de laboratorio de rutina, cargas virales y CD4.

7. Diagnóstico y tratamiento de las Hepatitis virales agudas y crónicas.

8. Diagnóstico y tratamiento de Infecciones de Transmisión sexual.

9. Diagnóstico y seguimiento de pacientes con Enfermedad de Chagas.

10. Diagnóstico y seguimiento de Infecciones Osteo-articulares.

11. Diagnóstico y seguimiento de otras Infecciones Crónicas.

12. Servicio de Atención Psicológica (Pediátrico y de Adultos).

13. Servicio de Atención Oftalmología (Departamento de Oftalmología).

14. Seguimiento de los casos hospitalarios.

15. Visitas Domiciliarias (En coordinación con entidades de auto-apoyo).

16. Manejo de Farmacia de Proyecto MSF (Incluye Atención Farmacéutica).

17. Manejo de Farmacia de ARV: Con Programa Nacional de SIDA y el Programa de Prevención de la Transmisión Vertical del VIH, Sífilis y Hepatitis B.

18. Apoyo a Proyectos de otras instituciones como lo fue con MSF Francia Suiza o España, en pacientes que requieren hospitalización.

19. Apoyo a Clínicas Departamentales como Coatepeque, Puerto Barrios y otras que lo requieren para manejo de muestras de laboratorio y pacientes que requieren hospitalización.

20. Apoyo a Proyectos Regionales en Centroamérica para períodos de observación de Personal Médico y Paramédico.

21. Participación en los Programas de Postgrado de los diferentes departamentos Clínicos del Hospital.

22. Programa de Manejo de Accidentes Laborales en Coordinación con el Comité de Control de Infecciones Nosocomiales del Hospital.

23. Participación en el desarrollo de Protocolos Nacionales de atención a personas viviendo con VIH-SIDA.

24. Coordinación con Organizaciones no gubernamentales y de personas viviendo con VIH para el manejo de la Infección.

25. Apoyo a entidades de cuidados paliativos: Hospicio San José y Hogar Marco Antonio.

26. Confirmación de diagnóstico y seguimiento de donadores de sangre del Hospital que presentan pruebas de tamizaje positivas, tales como sífilis, hepatitis virales, enfermedad de Chagas y VIH.

27. Consultas y orientaciones de Enfermera graduada a PVVS y otras situaciones de urgencia, cuando el personal médico no está disponible: violaciones, consultas de

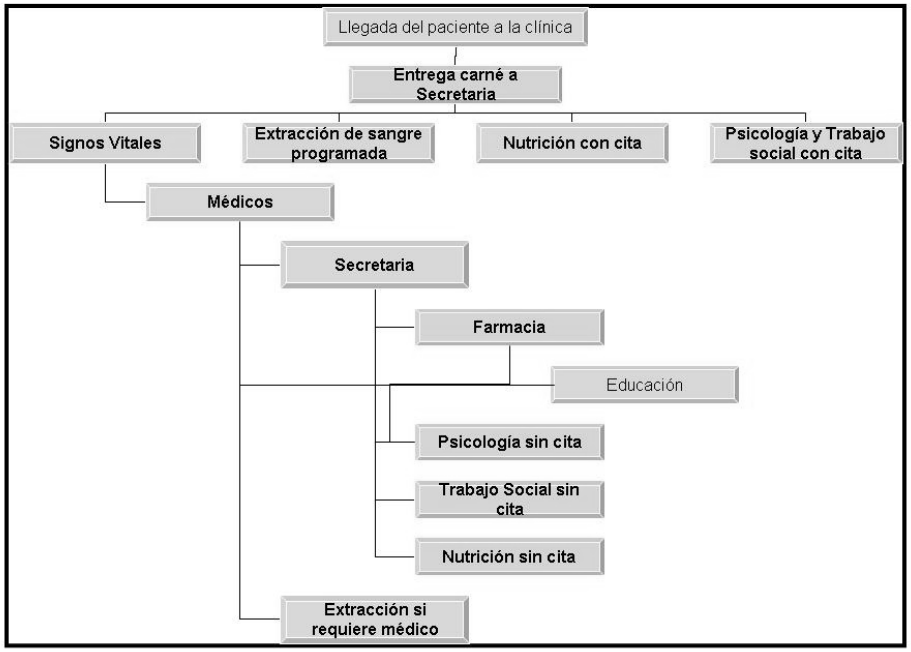
familiares, entrega de resultados y orientación de lugares de apoyo psicosocial a PVVS, etc.

28. Brindar docencia tanto dentro como fuera de la institución tanto en el área médica como de enfermería, según demanda de la actividad y disponibilidad de tiempo del personal de la clínica.

29. Desarrollo de la guía de tratamiento de Infecciones Oportunistas más comunes en la institución.

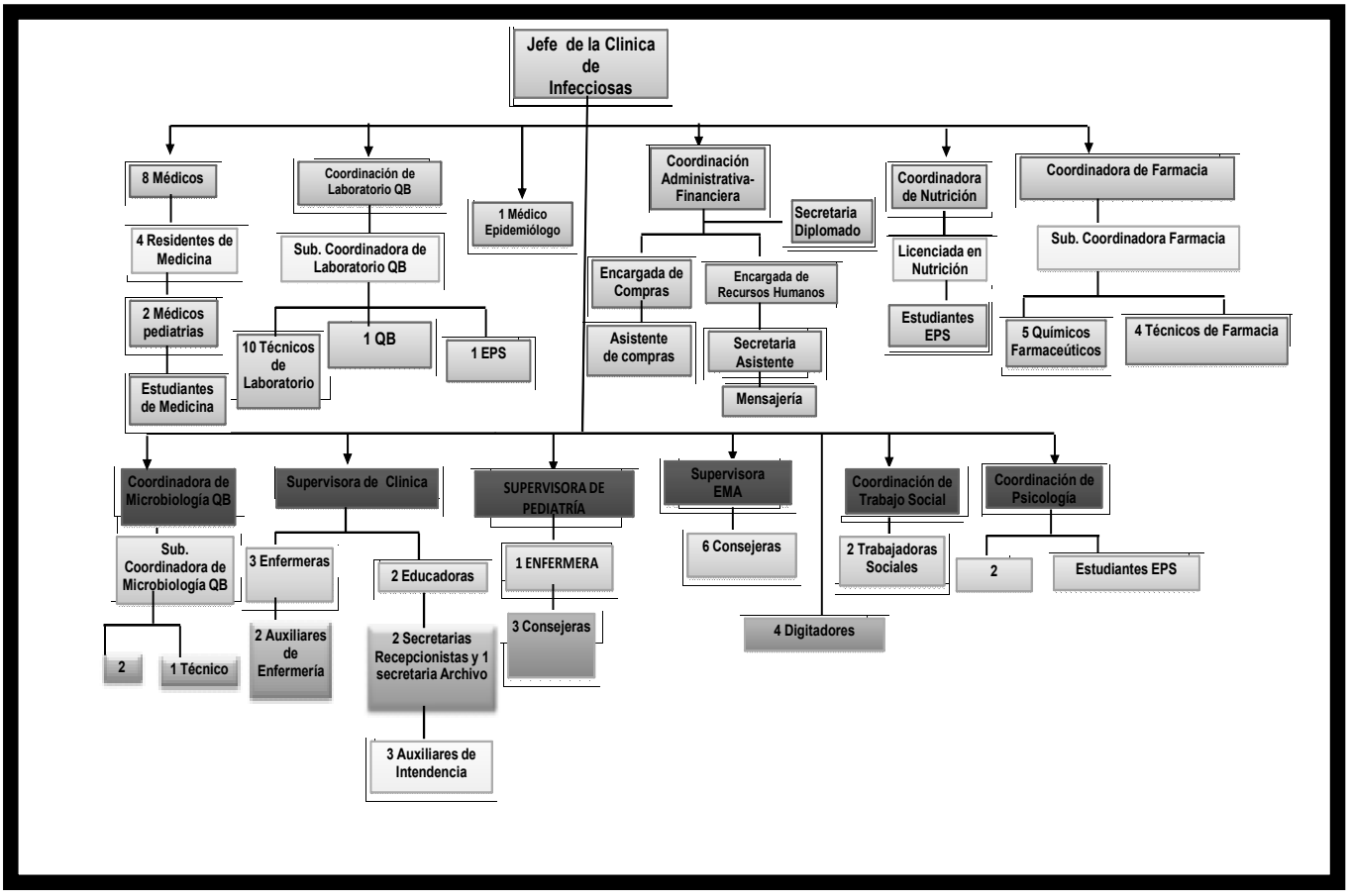
30. Participación en las labores de Vigilancia Epidemiológica del Ministerio de Salud Pública y Asistencia Social a través del reporte de casos.

Gráfica 1
Operatoria de la Clínica de Enfermedades Infecciosas, Hospital Roosevelt
Febrero 2010



Fuente: Clínica de Enfermedades Infecciosas, Hospital Roosevelt

Gráfica 2
Organigrama de la Clínica de Enfermedades Infecciosas, Hospital Roosevelt
Febrero 2010



Fuente: Elaboración propia, Clínica de Enfermedades Infecciosas, Hospital Roosevelt

1.4 Asignaciones del personal

- **Atribuciones del Jefe de la Clínica**

Coordinación y Dirección de las actividades de Atención Integral del VIH, tamizaje y prevención primaria y secundaria en la Clínica de Enfermedades Infecciosas del Hospital Roosevelt. Además realiza actividades administrativas entre las que se pueden citar revisar y aprobar solicitudes de desembolsos ante Visión Mundial, revisión y aprobación de informes mensuales de las distintas áreas de atención de la

clínica, representar al Hospital ante las instancias gubernamentales y de entidades internacionales que apoyan la propuesta. Realiza una actividad docente
Como coordinar la realización de cursos de capacitación a nivel interno en la Clínica de Enfermedades Infecciosas.

- **Atribuciones de los Médicos de la Clínica:** Médicos Internistas, Residentes del Postgrado de Enfermedades Infecciosas.

Brindar atención directa a pacientes en Consulta Externa de la Clínica de Enfermedades Infecciosas, de acuerdo a lineamientos acordados por el equipo y en concordancia con los Protocolos Nacionales vigentes. De acuerdo a su rol se encargan del seguimiento y supervisión de la atención de los pacientes de la Clínica en el área de encamamiento del Hospital: Funciones de Jefe de Servicio asignado por la Jefatura de la Clínica de Enfermedades Infecciosas a la Medicina C2.

- ✓ **Médico Pediatra**

Se da seguimiento a paciente con las siguientes patologías:

- VIH positivos y expuestos
- Infecciones por TORCH
- Sífilis
- Hepatitis B y C
- Tuberculosis
- Otros

- ✓ **Médico Encargado de Tuberculosis**

Evaluación médica de pacientes en la Consulta Externa de la Clínica de Enfermedades Infecciosas que incluye Enfermedad de Chagas, Hepatitis B y C, y Enfermedades de Transmisión Sexual, Osteomelitis, Tuberculosis.

- ✓ **Atribuciones del Médico Epidemiólogo**

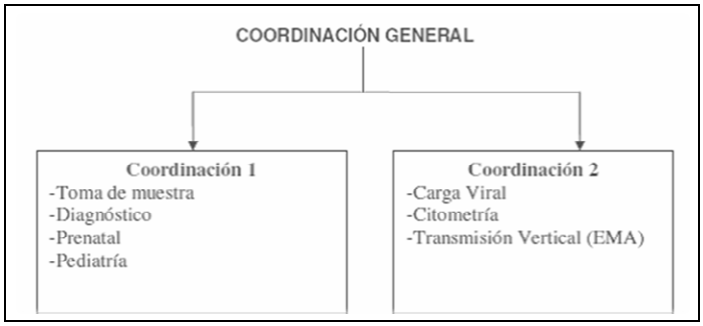
- Recolección de datos de los registros de clínica de transmisión vertical y su digitación en el programa EXCEL
- Recolección de datos de los registros de clínica de transmisión 8 y su digitación en el programa EXCEL
- Limpieza de datos de las bases de la clínica de transmisión vertical y 8.
- Análisis de datos y presentación de informes mensual.
- Apoyo en la base de datos de registro de procedimientos de laboratorio.
- Apoyo en la recolección de datos y elaboración de informes mensuales para el Programa de Visión Mundial.
- Elaboración de base de datos para el registro de los pacientes hospitalizados, así como sus salidas y posibles informes mensuales.

- **Enfermería**

Colabora con el control de signos vitales del área de enfermería (auxiliar de enfermería. Atiende al paciente con prontitud y esmero.

- **Atribuciones del Área de Laboratorio**

Gráfica 3
Organización del Área de Laboratorio
Febrero 2010



Fuente: Clínica de Enfermedades Infecciosas, Hospital Roosevelt

Comienza en el área de toma de muestras. Encargada de la recepción de muestras como heces, orina, esputos y otras. Contará con un técnico de laboratorio profesional de Química Biológica para garantizar su buen funcionamiento. Además contará con la ayuda de la estudiante de la Carrera de Química Biológica (EPS) cuando sea asignada la rotación o cuando se necesite. Los días en que el número de pacientes programados para extracción de muestras sea alta para la capacidad del personal del área, todo el personal técnico asignado a otras áreas de laboratorio tendrá que colaborar para garantizar que todas las extracciones se realicen de manera adecuada y en tiempo para no tener atrasos en la entrega de las muestras a las distintas áreas.

- **Atribuciones de la Unidad de Nutrición**

Atención nutricional a pacientes adultos y mujeres embarazadas ambulatorios de la Clínica de Enfermedades Infecciosas hospitalizados, de consulta externa, manejo de todos los programas nutricionales. Manejo de los programas de ayuda alimentaria. Asistencia y capacitaciones dirigidas al personal de la Clínica.

- **Atribuciones del Área de Psicología**

Está diseñado para el profesional de la salud mental que trabaje con personas de diversas orientaciones sexuales y que viven con la infección del VIH/SIDA, que asisten a la clínica.

- **Atribuciones del Área de Trabajo Social**

Se encargan de estudios socio-económicos a pacientes que asisten a consulta externa de la Clínica de Enfermedades Infecciosas para registro y archivo, dan seguimiento de casos de adultos, pacientes hospitalizados adultos, como pacientes del materno infantil. Coordinan con Trabajo Social del Hospital Roosevelt para exonerar a

pacientes de pago de exámenes de Rayos X, apoyo económico, traslado a hogares. Localizan vía telefónica, a pacientes que no asisten a su cita ni a recoger sus medicamentos. Localización de pacientes de casos diversos, solicitados por las diferentes áreas de la Clínica. Referencias intra hospitalarias a Hogares e instituciones afines al programa, tales como: Hogar Marco Antonio, Hogar San Vicente, Gente Positiva, Fundación Sobrevivientes y otros.

- **Área de Farmacia**

Está formado por:

- ✓ 7 Químicos Farmacéuticos
- ✓ 1 Asistente de Farmacia
- ✓ 3 Técnicos en Farmacia
- ✓ 1 digitador

Las áreas cubiertas por el equipo son:

- ✓ Servicios de Pediatría, Maternidad y sus Emergencias
- ✓ Servicios de Medicina Interna, Cirugías, Emergencia, observación e intensivo
- ✓ Consulta externa de adultos de la clínica de enfermedades infecciosas.

Para el buen funcionamiento de la farmacia se encuentra divida en dos coordinaciones las cuales su rotación es cada 6 meses, siendo éstas:

- ✓ Coordinación de Pediatría y Maternidad
- ✓ Coordinación de Adultos

En resumen esta unidad vela por la buena administración de todos los medicamentos pediátricos y de adultos, suministrados por los donantes de los proyectos Visión Mundial, PNS, y UNICEF.

- **Atribuciones de Educadoras Comunitarias**

Atender al paciente con prontitud y esmero, dar orientación, educación a los pacientes que asisten a la clínica. Desarrolla un programa educativo, dirigido a los pacientes que asisten a la consulta, antes de que pasen con el médico.

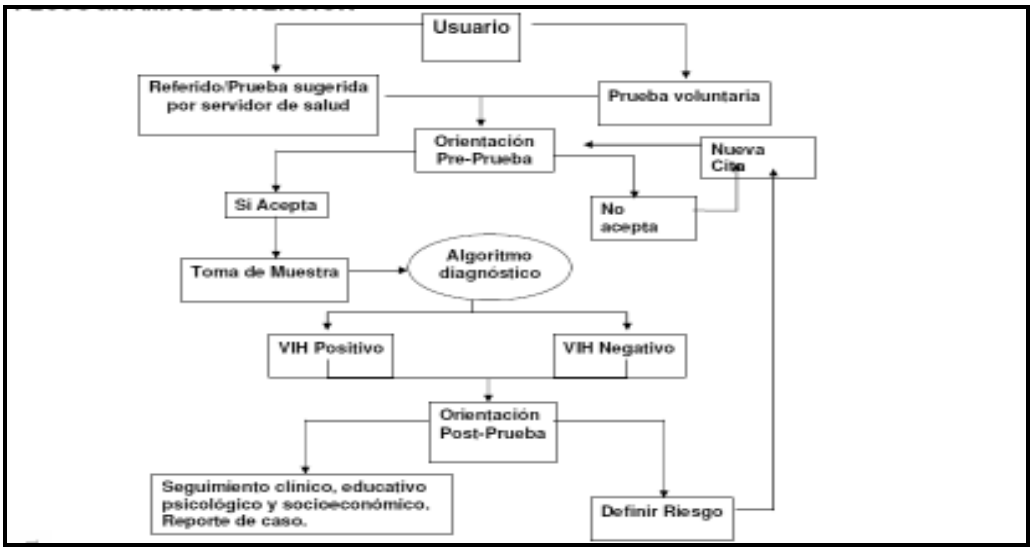
- **Atribuciones del Área de Recepción**

Prepara la papelería del archivo a pacientes en consulta, maneja la nómina de citas de todas las dependencias de la clínica, se asegura que no sobrepasen el mínimo aceptado total para atención general para no sobrecargar determinadas fechas. Llevará el control de personas esperadas para cada día podrá crear una impresión de todas las personas que asistieron a la clínica el mismo día disgregadas por área.

- **Administración de Clínica de Infecciosas**

Se encuentra bajo la dirección del Jefe de la Clínica de Enfermedades Infecciosas, cuidan de los recursos financieros como son la rentabilidad y la liquidez. Elaboran los presupuestos financieros, tomando en cuenta el techo autorizado en el Plan de Evaluación Acompañamiento y Monitoreo Gerencial de Visión Mundial y otras fuentes cuando le sea requerido. Se encuentra constituido por una Administradora, Secretaria Administrativa, Encargada de Compras, Asistente de Compras, Encargada de Recursos Humanos.

Flujograma 1
Procesos de atención al paciente
Febrero 2010



Fuente: Clínica de Enfermedades Infecciosas, Hospital Roosevelt

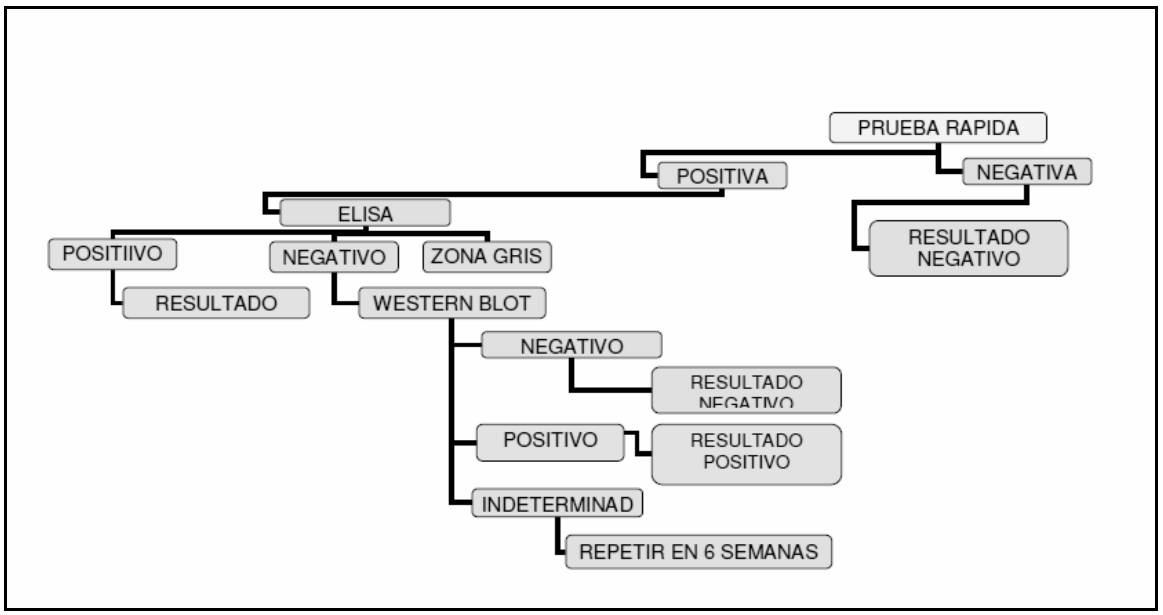
1.5 Esquema de diagnóstico, seguimiento de pacientes adultos y niños

La epidemia de VIH inicio en Guatemala en el año 1984, cuando los primeros casos fueron diagnosticados en los Hospitales Roosevelt y General San Juan de Dios. En esos años la respuesta a la misma fue eminentemente política, sin brindar apoyo a las personas que padecían el Síndrome de Inmunodeficiencia Humana. La atención médica dio sus inicios en el país en el año 1988 en el Hospital General San Juan de Dios y en el Hospital Roosevelt en mayo de 1989. Desde esos años en que las tareas estaban centradas en la medicina paliativa y cuando el hacer pruebas para el diagnóstico era muy complicado, pues los tiempos de espera para un ELISA eran de 5 a 7 días, ya que los reactivos eran escasos y se cuidaban en forma estrecha, y un Western Blot tenía que ser enviado a Costa Rica o Estados Unidos, con espera de 6 a 8 semanas, el diagnóstico de la enfermedad era eminentemente clínico. Así como el diagnóstico de las enfermedades oportunistas era complejo y en muchas situaciones tardío. La mortalidad de pacientes que llegaban a los hospitales era mayor del 75%. La sobrevida de las personas en la primera mitad de los años 90 era 4.2 a 5.4 meses luego del diagnóstico de SIDA.

El progreso logrado en estos primeros 20 años de Atención Integral del VIH SIDA en el Hospital Roosevelt, ha sido dramático, transformándose en este tiempo en la Clínica más grande del país que brinda múltiples servicios y sirve de centro de capacitación a personas del nivel departamental y centroamericano en las diversas disciplinas de las ciencias de la salud, e inclusive en el área administrativa de centros de atención del nivel departamental. Se incluyen flujogramas de atención de las personas que acuden a la clínica, así como algoritmos de manejo de antirretrovirales y diagnóstico de la infección VIH, los cuales se basan en los protocolos de país vigentes para la Atención de Personas que viven con VIH en Guatemala, según protocolos nacionales de los años 2002, 2005-2006 y el más reciente revisado de agosto del 2007, pendiente de publicación. Se han incluido los criterios para diagnóstico y seguimiento de pacientes con problemas de Hepatitis B y C y Sífilis, basados en publicaciones internacionales y

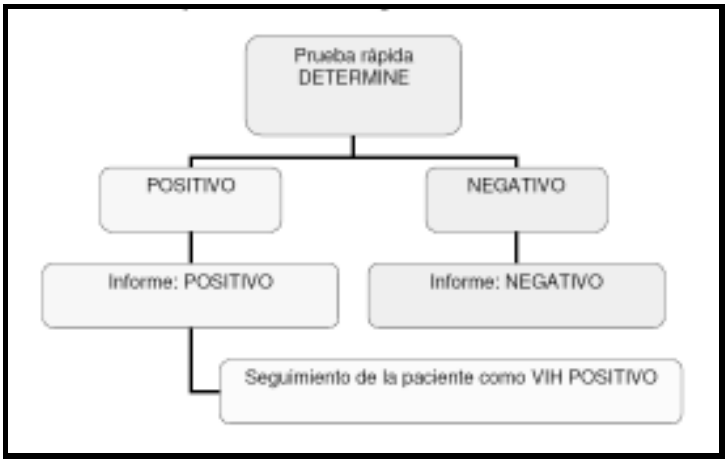
el de Enfermedad de Chagas basado en protocolo de manejo nacional del Programa Nacional de Vectores del Ministerio de Salud Pública. A continuación Algoritmos de Diagnósticos, flujogramas de seguimiento la clínica.

Gráfica 4
Algoritmo para Diagnóstico de VIH, Consulta Externa
Febrero 2010



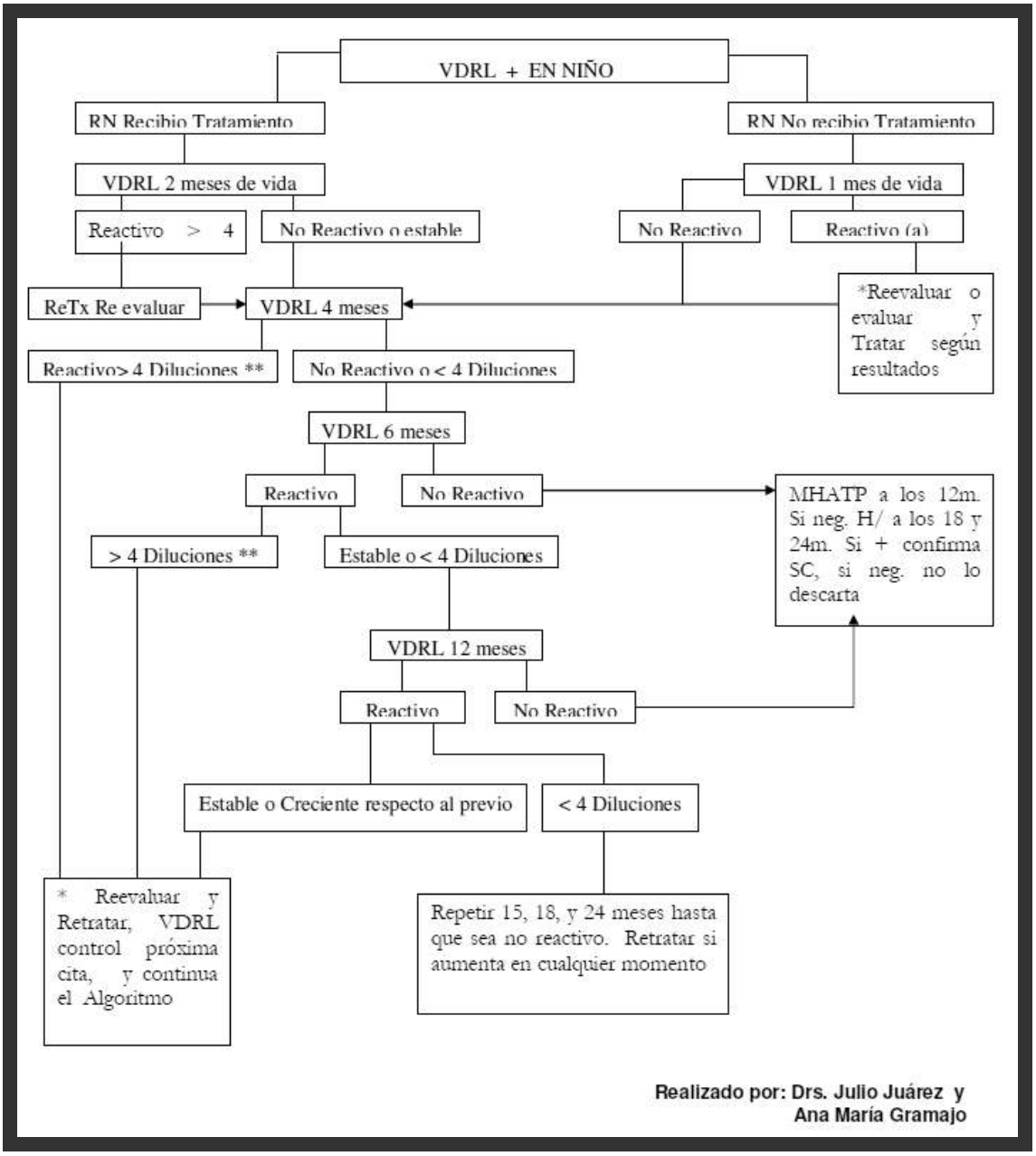
Fuente: Clínica de Enfermedades Infecciosas, Hospital Roosevelt

Gráfica 5
Tamizaje de VIH en la Emergencia de la Maternidad
Febrero 2010



Fuente: Clínica de Enfermedades Infecciosas, Hospital Roosevelt

Gráfica 6
Algoritmo para seguimiento del Recien Nacido
Febrero 2010



Fuente: Clínica de Enfermedades Infecciosas, Hospital Roosevelt

VDRL Es una prueba de detección para sífilis. Este examen mide sustancias, llamadas anticuerpos, que se pueden producir en repuesta al *Treponema pallidum*, la bacteria que causa la sífilis. **infecciones oportunistas que a menudo se relacionan con la de VIH**

1.6 Manual de Normas y Procedimientos Administrativos y Financieros para las Unidades Ejecutoras (Sub-receptores) del proyecto

El presupuesto aprobado para la Unidad Ejecutora (Clínica de Enfermedades Infecciosas, Hospital Roosevelt); se encuentra en el acuerdo suscrito con el Receptor Principal (Visión Mundial) y contiene la programación de gastos de la Unidad Ejecutora para el logro de los objetivos, indicadores y metas del proyecto.

- La Unidad Ejecutora deberá respetar el presupuesto aprobado por objetivo, categoría de gasto y año de ejecución. Cualquier modificación deberá solicitarse por escrito al Receptor Principal donde se justifique la modificación. La aprobación del Receptor Principal deberá estar por escrito.

- Mensualmente se deberá comparar los gastos reales contra los presupuestados y explicar cualquier variación significativa (superior o inferior al 10%).

- Se podrá reprogramar cualquier saldo no ejecutado el cual deberá contemplarse en el Flujo de Efectivo proyectado para el siguiente mes.

❖ Tabla de categorías, cuentas y subcuentas de gasto de Ambientes TI. (CLÍNICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT)

Para mejor comprensión de cómo se presupuestan los gastos para el área de tecnología a continuación se muestra la tabla de cuentas y subcuentas, con sus respectivos códigos.

Es importante resaltar que todas las transacciones de compra deben ser conducidas de manera libre y competitiva y que cumplan con los principios de comercio, la legislación nacional, la normativa del Fondo Mundial y del Receptor Principal, en materia de adquisiciones de bienes y contrataciones de servicios.

Tabla 1
Clasificaciones de Cuentas, área de Tecnología- Proyecto Fondo Mundial VIH/SIDA: Manual de Normas y Procedimientos Administrativos y Financieros para las Unidades Ejecutoras del Proyecto
Febrero 2010

CÓDIGOS			DESCRIPCIÓN
CATEGORÍA	CUENTA	SUBCUENTA	
02	**000**	**000000**	**INFRAESTRUCTURA Y EQUIPOS GASTOS MAYORES US$1000.00**
02	811	811000	**INFRAESTRUCTURA Y EQUIPOS MAYORES**
02	811	811002	Equipo de Computación e Informática
02	811	811003	Mobiliario y Equipo
02	811	811004	Software y Licencias de Computación
02	812	812000	**INFRAESTRUCTURA Y EQUIPOS MENORES GASTOS MENORES S$1000.00**
02	812	812001	Equipo de Computación
02	812	812002	Mobiliario y Equipo
02	812	812003	Software y Licencias de Computación
03	**000**	**000000**	**CAPACITACIÓN**
03	802	802000	**CAPACITACIONES Y TALLERES**
03	802	802001	Becas
03	802	802002	Cursos, Seminarios, Talleres
03	802	802003	Honorarios por Consultorías
08	840	840000	**GASTOS ADMINISTRATIVOS DE LOCAL**
08	840	840004	Reparaciones y mantenimiento de Local

Fuente: Elaboración propia, Clínica de Enfermedades Infecciosas, Hospital Roosevelt

Dentro de las políticas más importantes resalta que en la adquisición de bienes y servicios que requiera la Unidad Ejecutora, se deberán obtener las mejores condiciones que combinen en el caso de **bienes**: calidad, precios técnicamente habilitados más bajos, plazos de entrega, formas de pago y garantías de mantenimiento y repuestos y en el caso de **servicios**: prestar los servicios en los tiempos acordados, con el personal clave y realizar las capacitaciones (cuando aplique).

- **Registro de proveedores**

La Unidad Ejecutora podrá formar su propia lista de proveedores conforme a sus necesidades, utilizando como criterio primordial que todos los proveedores deben estar:

- ✓ Legalmente establecidos (como mínimo un año de formación de la empresa) e
- ✓ Inscritos en el Registro Tributario de la Superintendencia de Administración Tributaria (SAT)

- **Procedimientos para la adquisición de bienes y contratación de servicios**

Para realizar estas adquisiciones dependerá del monto de la compra, de acuerdo con la siguiente escala, en donde se indica también el responsable de realizar el proceso de adquisición de bienes y servicios.

Cuadro 1
Proceso de adquisición de bienes y servicios: : Manual de Normas y Procedimientos Administrativos y Financieros para las Unidades Ejecutoras del Proyecto.
Febrero 2010

PROCESO NO.	RANGOS	TIPO DE PROCESO NO. DE COTIZACIONES MÍNIMAS REQUERIDAS	RESPONSABLE
1	De Q 0.01 a Q 200.00	Compra Caja Chica (1)	Unidad Ejecutora
2	De Q 200.01 a Q 2,000.00	Solicitudes de Cotización (2 a 3)	Unidad Ejecutora
3	De Q2,000.01 a Q 10,000.00	Solicitudes de Cotización (Mínimo de 3)	Unidad Ejecutora
4	De Q10,000.01 a Q 100,000.00	Solicitudes de Cotización I (Mínimo de 3)	Unidad Ejecutora
5	De Q100,000.01 a Q 800,000.00	Solicitudes de Cotización II (Mínimo de 3)	Receptor Principal
6	De Q800,000.01 a Q 1,200,000.00	Licitación Pública Nacional (abierta)	Receptor Principal
7	De Q 1,200,000.01	Licitación Pública Internacional (abierta)	Receptor Principal

Fuente: Elaboración propia, Clínica de Enfermedades Infecciosas, Hospital Roosevelt

CAPÍTULO II

CONTROL INTERNO

2.1 Antecedentes

Desde la primera definición de control interno establecida por el Instituto Americano de Contadores Públicos Certificados-AICPA en 1949 y las modificaciones incluidas en SAS N. 55 en 1978, este concepto no sufrió cambios importantes hasta 1992, cuando la Comisión Nacional sobre Información Financiera Fraudulenta en los Estados Unidos, conocida como la *"Comisión Treadway",* establecida en 1985 como uno de los múltiples actos legislativos y acciones que se derivaron de las investigaciones sobre el caso *Watergate*, emite el documento denominado "Marco Integrado del Control Interno"(*Framework Internal Control Integrated)*, el cual desarrolla con mayor amplitud el enfoque moderno del control interno en el documento conocido como el Informe COSO *(Committee of Sponsoring Organizations of the Treadway Commission).* En el ámbito público, después de haber sido materia de discusión el tema del control interno en sucesivos congresos internacionales, en 1971 se define el concepto de control interno. Ello ocurre en el Seminario Internacional de Auditoría Gubernamental realizado en Austria en 1971, bajo el patrocinio de la Organización de Naciones Unidas y la Organización Internacional de las Entidades Fiscalizadoras Superiores (*INTOSAI*), definiendo el control interno de la siguiente manera: “Es el plan de organización y el conjunto de medidas y métodos coordinados, adoptados dentro de una entidad pública para salvaguardar sus recursos, verificar la exactitud y el grado de confiabilidad de sus datos contables, promover la eficiencia en las operaciones y estimular la observación de la política."(1:2-5)

El interés por este tema respondía a dos hechos importantes: en primer lugar, a partir de la década de los 70' el sector público había crecido de manera significativa en los países en desarrollo, tanto en magnitud como en volumen de operaciones, y, en segundo lugar, las entidades públicas eran muy reacias a efectuar cambios para

disponer de una administración moderna y eficaz, a pesar que se encontraban en un escenario distinto.

Con ocasión del XII Congreso Mundial de Entidades Fiscalizadoras Superiores realizado en Washington, en 1992, se aprueban las directrices del control interno que fueron elaboradas por la Comisión de Normas de Control Interno integrada por diversas Instituciones Superiores de Auditoría-ISA's. Estas directrices fueron instituidas, con el propósito de fortalecer la gestión financiera en el sector público, mediante la implementación de controles internos efectivos. En su contenido se define con claridad los objetivos del control interno en el ámbito público, así como las responsabilidades de cada entidad en la creación, mantenimiento y actualización de su estructura de control interno.

INTOSAI, establece que la estructura de control interno es el conjunto de planes, métodos, procedimientos y otras medidas, incluye la actitud de la dirección que dispone una institución para ofrecer una garantía razonable de que han sido cumplidos los siguientes objetivos: a) preservar las operaciones metódicas, económicas, eficientes y eficaces y los productos y servicios de calidad, acorde con la misión que la institución debe cumplir; b) preservar los recursos frente a cualquier pérdida por despilfarro, abuso, mala gestión, errores, fraude e irregularidades; c) respetar las leyes, reglamentos y directivas de la dirección; y, d) elaborar y mantener datos financieros y de gestión fiables y presentarlos correctamente en informes oportunos. Además la Ley *Sarbanes-Oxley*, conocida y emitida en el año 2002 también como *SarOx o SOA* (por sus siglas en inglés Sarbanes Oxley Act), es la ley que regula las funciones financieras contables y de auditoría y penaliza en una forma severa, el crimen corporativo y de cuello blanco. Debido a los múltiples fraudes, la corrupción administrativa, los conflictos de interés, la negligencia y la mala práctica de algunos profesionales y ejecutivos que aunque conocen los códigos de ética, sucumbieron ante el atractivo de ganar dinero fácil por medio de empresas y corporaciones engañando a socios, empleados y grupos de interés, entre ellos sus clientes y proveedores.

Desde hace algunas décadas la gerencia moderna ha creado nuevas formas para mejorar los controles en las empresas del sector privado. Ello es importante tener en cuenta, por cuanto el control interno tiene una vinculación directa con el curso que debe mantener la empresa hacia el logro de sus objetivos y metas. El control interno no puede existir si previamente no existen objetivos, metas e indicadores de rendimiento. Si no se conocen los resultados que deben lograrse, es imposible definir las medidas necesarias para alcanzarlos y evaluar su grado de cumplimiento en forma periódica.

2.2 Definición de control interno

"El control interno es el proceso diseñado y efectuado por los encargados del gobierno corporativo, la administración y otro personal para proporcionar seguridad razonable sobre el logro de los objetivos de la entidad respecto de la confiabilidad de la información financiera, efectividad y eficiencia de las operaciones y cumplimiento de las leyes y reglamentaciones aplicables. El control interno se diseña e implementa para atender a riesgos de negocio identificados que amenazan el logro de cualquiera de estos objetivos" (3-269)

2.3 Concepto de control interno

Con base al trabajo realizado por la investigadora, se conceptualiza como control interno: el conjunto de normas, procedimientos y recursos adoptados para efectuar, supervisar y revisar en forma adecuada y conveniente las operaciones y la administración de una empresa.

2.4 Integración de conceptos COSO, COCO, COBIT

El informe COSO por las siglas en inglés del comité que patrocinó los estudios que lo produjeron; (*Committe of sponsoring organizations of the Treadway Commission Internal Control Integrated Framewok* 1992), el canadiense COCO *(Canadian Institute of Certified Accountants*. *Control Concepts 1992*). COBIT (focalizado en controles en materia de tecnología de la información, cuyo nombre es la sigla en inglés de la

expresión “Objetivos de control para la información y tecnologías relacionadas). COCO y COBIT citan expresamente su compatibilidad con COSO, modelo que se tomará como principal referencia para el desarrollo de este apartado.

COSO define al control interno como un proceso, efectuado por el directorio, la gerencia y el resto del personal, diseñado para proveer una seguridad razonable respecto al logro de los objetivos de las organizaciones, a los que, en forma artificial, subdivide en las siguientes tres categorías:

- Objetivos relacionados con la efectividad y eficiencia de las operaciones.
- Objetivos vinculados con la confiabilidad de la información contable para publicar.
- Objetivos relativos a con el cumplimiento con leyes y otras regulaciones aplicables a la entidad.

Al mencionar en primer lugar a los objetivos relacionados con eficacia y eficiencia, resalta implícitamente que, además de fortalecer la credibilidad de su información contable y asegurar que cumple cabalmente las leyes y reglas a que esté sujeta y evitar daños a su reputación u otras consecuencias negativas, el control interno puede ayudar a una entidad a conseguir sus metas de desempeño y rentabilidad y a evitar el desperdicio de recursos.

2.5 Marco Integrado de Control COSO

“El control interno según COSO consta de cinco componentes interrelacionados que se derivan de la forma cómo la administración maneja el negocio, y están integrados a los procesos administrativos. Los componentes son:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión y seguimiento del sistema de control.

El control interno, no consiste en un proceso secuencial, en donde algunos de los componentes afectan sólo al siguiente, sino en un proceso multidireccional repetitivo y permanente, en el cual más de un componente influye en los otros. Los cinco componentes forman un sistema integrado que reacciona dinámicamente a las condiciones cambiantes." (1:4-5)

- **Efectividad**

Los sistemas de control interno de entidades diferentes operan con diferentes niveles de efectividad. En forma similar, un sistema en particular puede operar en forma diferente en tiempos diferentes. Cuando un sistema de control interno alcanza una calidad razonable, puede ser efectivo.

El control interno puede ser juzgado efectivo, si el Consejo de Administración y la Gerencia tienen una razonable seguridad de que:

- Se conoce el grado en que los objetivos y metas de las operaciones de las entidades están siendo alcanzados.
- Los informes financieros están siendo preparados con información confiable.
- Se están observando las leyes y los reglamentos aplicables.

Dado que el control interno es un proceso, su efectividad es un estado o condición del mismo en un punto en el tiempo. Determinar si un sistema de control interno en particular es "efectivo": es un juicio subjetivo resultante de una evaluación de si los cinco componentes mencionados están presentes y funcionando con efectividad. Su funcionamiento efectivo da la seguridad razonable, en cuanto al logro de los objetivos de uno o más de los logros citados. De esta manera, estos componentes constituyen también criterios para un control interno efectivo. A pesar de que los cinco criterios deben ser adecuados, esto no significa que cada componente deba funcionar idénticamente o al mismo nivel, en entidades diferentes. Puede haber algunos ajustes entre ellos dado que los controles pueden obedecer a una variedad de propósitos,

aquellos incorporados a un componente en que previenen un riesgo en particular, sin embargo en combinación con otros pueden lograr un efecto de conjunto satisfactorio.

- **Ambiente de control**

El estudio de COSO establece a este componente como el primero de los cinco y se refiere al establecimiento de un entorno que estimule e influencie las actividades del personal con respecto al control de sus actividades. Es en esencia el principal elemento sobre el que se sustentan o actúan los otros cuatro componentes e indispensables, a su vez, para la realización de los propios:

- **Integridad y valores éticos**

Tiene como propósito establecer pronunciamientos relativos a los valores éticos y de conducta que se espera de todos los miembros de la organización durante el desempeño de sus actividades, ya que la efectividad del control interno depende de la integridad y valores de la gente que lo diseña y lo establece.

Es importante tener en cuenta la forma en que son comunicados y fortalecidos estos valores éticos y de conducta. La participación de la alta administración es clave en este asunto, ya que su presencia dominante fija el tono necesario a través de su empleo, la gente imita a sus líderes. Debe tenerse cuidado con aquellos factores que pueden inducir a conductas adversas a los valores éticos como pueden ser: controles débiles, debilidad de la función de auditoría; inexistencia o inadecuadas sanciones para quienes actúan inapropiadamente.

- **Competencia del personal**

Se refiere a los conocimientos y habilidades que debe poseer el personal para cumplir adecuadamente con sus tareas.

- **Consejo de Administración y/o Comité de Auditoría**

Debido a que estos órganos fijan los criterios que perfilan el ambiente de control, es determinante que sus miembros cuenten con la experiencia, dedicación e

involucramiento necesario para tomar las acciones adecuadas e interactúen con los auditores internos y externos.

- **Filosofía administrativa y estilo de operación**

Los actores más relevantes son las actitudes mostradas hacia la información financiera, el procesamiento de la información y principios y criterios contables, entre otros. Otros elementos que influyen en el ambiente de control se refieren a aspectos relacionados con: estructura organizativa, delegación de autoridad y responsabilidad y políticas de recursos humanos. El ambiente de control tiene gran influencia en la forma como se desarrollan las operaciones, se establecen los objetivos y se estiman los riesgos. Tiene que ver igualmente en el comportamiento de los sistemas de información y con la supervisión en general. A su vez es influenciado por la historia de la entidad y su nivel de cultura administrativa.

- **Evaluación de riesgos**

El segundo componente del control, involucra la identificación y análisis de riesgos relevantes para el logro de los objetivos y la base para determinar la forma en que tales riesgos deben ser manejados. Asimismo se refiere a los mecanismos necesarios para identificar y manejar riesgos específicos asociados con los cambios, tanto los que influyen en el entorno de la organización como en el interior de la misma. Para lo anterior, es indispensable primeramente el establecimiento de objetivos tanto a nivel global de la organización como al de las actividades relevantes, obteniendo con ello una base sobre la cual sean identificados y analizados los factores de riesgos que amenazan su oportuno cumplimiento. La evaluación, o mejor dicho la autoevaluación de riesgo debe ser una responsabilidad ineludible para todos los niveles que están involucrados en el logro de objetivos.

- **Objetivos**

Para todos es clara la importancia que tiene este aspecto en cualquier organización, ya que representa la orientación básica de todos los recursos y esfuerzos, proporciona una base sólida para un control interno efectivo. La fijación de objetivos es el camino

adecuado para identificar factores críticos de éxito, particularmente a nivel de actividad relevante. Una vez que tales factores han sido identificados, la gerencia tiene la responsabilidad de establecer criterios para medirlos y prevenir su posible ocurrencia a través de mecanismos de control e información, a fin de estar enfocando permanentemente tales factores críticos de éxito.

"El estudio de COSO propone una categorización que pretende unificar los puntos de vista al respecto, tales categorías son las siguientes:

- **Objetivos de operación.** Son aquellos relacionados con la efectividad y eficiencia de las operaciones de la Organización.
- **Objetivos de información financiera.** Se refiere a la obtención de información financiera contable.
- **Objetivos de cumplimiento.** Están dirigidos a la adherencia a leyes y reglamentos federales o estatales. Así como también a las políticas emitidas por la gerencia. En ocasiones la distinción entre estos tipos de objetivos es demasiado sutil, debido a que unos se traslapan o apoyan a otros. El logro de los objetivos antes mencionados está sujeto a los siguientes eventos:
    - Controles internos efectivos proporcionan una garantía razonable de que los objetivos de información financiera y de cumplimiento serán logrados, debido a que están dentro del alcance de la gerencia.
    - En relación con los objetivos de operación, la situación difiere debido a que existen eventos fuera del control de la empresa. Sin embargo, el propósito de los controles en esta categoría está dirigido a evaluar la consistencia e interrelación entre los objetivos y metas en los distintos niveles, la identificación de factores críticos de éxito y la manera en que se reporta el avance de los resultados y se implementen las acciones indispensables para corregir desviaciones. Todos los organismos enfrentan riesgos y éstos deben ser evaluados." (1:19-20)

- **Riesgos**

El proceso mediante el cual se identifica, analiza y se manejan los riegos forma parte de un sistema de control efectivo. Para ello la organización debe establecer un proceso suficientemente amplio que tome en cuenta sus interacciones más importantes entre todas las áreas y de éstas con el exterior. Desde luego los riegos a nivel global incluye no sólo factores externos sino también internos, interrupción de un sistema de procesamiento de información; calidad del personal; capacidad o cambios en relación con las responsabilidades de la gerencia.

Los riesgos a nivel de actividad también deben ser identificados, ayudando con ellos a administrar los riesgos en las áreas o funciones más importantes. Desde luego las causas del riesgo en este nivel permanecen a un rango amplio que va desde lo obvio hasta lo complejo y con distintos grados de significación.

El análisis de riesgos y su proceso, sin importar la metodología en particular, debe incluir entre otros aspectos los siguientes:

- Estimación del significado del riesgo y sus efectos.
- Evaluación de la probabilidad de ocurrencia.

Consideraciones de cómo debe manejarse el riesgo, evaluación de acciones que deben tomarse.

- **Manejo de cambios**

Este elemento resulta de vital importancia debido a que está enfocado a la identificación de los cambios que pueden influir en la efectividad de los controles internos. Tales cambios son importantes, ya que los controles diseñados bajo ciertas condiciones pueden no funcionar en forma apropiada. De lo anterior se deriva la necesidad de contar con un proceso que identifique las condiciones que pueden tener un efecto desfavorable sobre los controles internos y la seguridad razonable de que los objetivos sean logrados.

El manejo de cambios debe estar ligado con el proceso de análisis de riesgos comentado anteriormente y debe ser capaz de proporcionar información para identificar y responder a las condiciones cambiantes. La responsabilidad primaria sobre los riesgos, su análisis y manejo es de la gerencia, mientras que a la auditoría interna le corresponde apoyar el cumplimiento de tal responsabilidad. Existen factores que requieren de atenderse con oportunidad ya que representan sistemas relacionados con el manejo de cambios como son: nuevo personal, sistemas de información nuevos o modificados; crecimiento rápido; nueva tecnología, reorganizaciones corporativas, cambios como son: Los mecanismos contenidos en este proceso deben tener un marcado sentido de anticipación que permita planear e implantar las acciones necesarias. Tales mecanismos deben responder a un criterio de costo beneficio.

- **Actividades de Control**

"Las actividades de control son aquellas que realiza la gerencia y demás personal de la organización para cumplir diariamente con actividades asignadas. Estas actividades están relacionadas con las políticas, sistemas y procedimientos principalmente. Ejemplo de estas actividades son aprobación, autorización, verificación, conciliación, inspección, revisión de indicadores de rendimiento. También la salvaguarda de los recursos, la segregación de funciones, la supervisión y la capacitación adecuada. Las actividades de control tienen distintas características. Pueden ser manuales o computarizadas, gerenciales u operacionales, general o específicas, preventivas o detectivas. Sin embargo, lo trascendente es que sin importar su categoría o tipo, todas ellas estén apuntando hacia los riesgos reales o potenciales en beneficio de la organización, su misión y objetivos, así como a la protección de los recursos.

Las actividades de control son importantes no sólo porque en sí mismas implican la forma correcta de hacer las cosas, sino debido a que son el medio idóneo de asegurar en mayor grado el logro de los objetivos y estos sí que tiene mayor relevancia que hacer las cosas de forma correcta.

- **Control en los sistemas de información.** Los sistemas están diseñados en toda la empresa y todos ellos atienden a uno o más objetivos de control. De manera más amplia se considera que existen controles generales y controles de aplicación sobre los sistemas de información.

- **Controles generales.** Tienen como propósito asegurar una operación y continuidad adecuada e incluyen el control sobre el centro de procesamiento de datos y su seguridad física, contratación y mantenimiento del hardware y software, así como la operación propiamente dicha. También lo relacionado con las funciones de desarrollo y mantenimiento de sistemas, soporte técnico, administración de base de datos y otros.

- **Controles de aplicación.** Están dirigidos hacia el "interior" de cada sistema y funcionan para lograr el procesamiento, integridad y confiabilidad de la información, mediante la autorización y validación correspondiente. Desde luego estos controles incluyen las aplicaciones destinadas a interrelacionarse con otros sistemas de los que reciben o entregan información". (1:72-75)

Los sistemas de información versus tecnología son y serán sin duda un medio para incrementar la productividad y competitividad. Ciertos hallazgos sugieren que la integración de la estrategia, la estructura organizacional y la tecnología de la información es un concepto clave para lo que queda de este siglo y el inicio del próximo. Es conveniente considerar en esta parte las tecnologías que evolucionan a los sistemas de información y que también, en su momento, será necesario diseñar controles por medio de ellas. Tal es el caso de la Ingeniería de Software Asistida por Ordenador (*CASE*), el procesamiento de imágenes y el intercambio electrónico de datos, de la estrategia, la estructura. Conviene aclarar, al igual que en los demás componentes, que las actividades de control, sus objetivos y su estructura deben responder a las necesidades específicas de cada organización.

- **Información**

Es obvio que para poder controlar una empresa y tomar decisiones correctas respecto a la obtención, uso y aplicación de los recursos, es necesario disponer de información adecuada y oportuna ciertamente los estados financieros constituyen una parte importante de esa información. Su contribución es incuestionable. Sin embargo, como primera reflexión sería que la información contable tiene fronteras. Ni se puede usar para todo, ni se puede esperar todo de ella. Esto puede parecer evidente, pero hay quienes piensan que la información de los estados financieros pudiera ser suficiente para tomar decisiones acerca de una empresa. Con frecuencia se pretende evaluar la situación actual y predecir la situación futura sólo con base en la información contable. Este enfoque simplista, por su parcialidad, sólo puede conducir a juicios equivocados. Para todos los efectos, es preciso estar conscientes que la contabilidad dice en parte lo que ocurrió pero no lo que va a suceder en el futuro. Por otro lado, en ocasiones la información no financiera constituye la base para la toma de ciertas decisiones, pero igualmente resulta insuficiente para la adecuada conducción de una empresa.

- **Información y Comunicación**

Consecuentemente la información pertinente debe ser identificada, capturada, procesada y comunicada al personal en forma y dentro del tiempo indicado, de forma tal que le permita cumplir con sus responsabilidades. Los sistemas producen reportes conteniendo información operacional, financiera y de cumplimiento que hace posible conducir y controlar la organización.

Todo el personal debe recibir un claro mensaje de la alta gerencia de sus responsabilidades sobre el control así como la forma en que las actividades individuales se relacionan con el trabajo de otros. Asimismo, debe contarse con medios para comunicar información relevante hacia los mandos superiores, así como a entidades externas. A continuación se comenta brevemente los elementos que integran este componente:

- **Información**

Está fuera de discusión la importancia de este elemento durante el desarrollo de las actividades, La información tanto generada internamente como aquella que se refiere a eventos acontecidos en el exterior, es también parte esencial de la toma de decisiones así como del seguimiento de las operaciones. La información cumple distintos propósitos a diferentes niveles.

- **Sistemas integrados a la estructura**

No hay duda que los sistemas están integrados o entrelazados con las operaciones. Sin embargo se observa una tendencia a que éstos deben apoyar de manera contundente la implantación de estrategias. Los sistemas de información, como un elemento de control, ligados a los procesos de planeación estratégica son un factor clave de éxito en muchas organizaciones.

- **Sistemas integrados a las operaciones**

En este sentido es evidente cómo los sistemas son medios efectivos para la realización de las actividades de la empresa. Desde luego el grado de complejidad varía según el caso, y se observa que cada día están mis integrados con las estructuras o sistemas de organización.

- **La calidad de la información**

Esto es tan trascendente que constituye un activo, un medio y hasta una ventaja competitiva en todas las organizaciones importantes, ya que está asociada a la capacidad gerencial de las empresas. La información, para actuar como un medio efectivo de control, requiere de las siguientes características: relevancia del contenido, oportunidad, actualización, exactitud y accesibilidad, principalmente. En lo anterior se invierte una cantidad importante de recursos. En la medida que los sistemas de información apoyan las operaciones, en esa misma medida se convierten en un mecanismo de control útil.

- **Comunicación**

Al respecto también es claro que deben existir adecuados canales para que el personal conozca sus responsabilidades sobre el control de sus actividades. Estos canales deben comunicar los aspectos relevantes del sistema de información indispensable para los gerentes, así como los hechos críticos para el personal encargado de realizar las operaciones críticas. También los canales de comunicación entre la Gerencia y el Consejo de Administración o los Comités es de vital importancia. En relación con los canales de comunicación con el exterior, éstos son el medio a través del cual se obtiene o proporciona información relativa clientes, proveedores, contratistas, entre otros. Así mismo son necesarios para proporcionar información a las entidades reguladoras sobre las operaciones de la empresa e inclusive sobre el funcionamiento de su sistema de control.

- **Supervisión y seguimiento del sistema de control**

En general los sistemas de control están diseñados para operar en determinadas circunstancias. Claro está que para ello se tomaron en consideración los riesgos y las limitaciones inherentes al control; sin embargo, las condiciones evolucionan debido tanto a factores externos como internos colocando con ello que los controles pierdan su eficiencia. Como resultado de todo ello, la gerencia debe llevar a cabo la revisión y evaluación sistemática de los componentes y elementos que forman parte de los sistemas. Lo anterior no significa que tengan que revisarse todos los componentes y elementos, como tampoco que deba hacerse al mismo tiempo. Ello dependerá de las condiciones específicas de cada organización, de los distintos niveles de riesgos existentes y del grado de efectividad mostrado por los distintos componentes y elementos de control. La evaluación debe conducir a la identificación de los controles débiles, insuficientes o necesarios, para promover con el apoyo decidido de la gerencia, su reforzamiento e implantación. Esta evaluación puede llevarse a cabo de tres formas: durante la realización de las actividades de supervisión diaria en distintos niveles de organización; de manera independiente por personal que no es responsable

directo de la ejecución de las actividades, incluidas las de control, mediante la combinación de las dos formas anteriores.

- **Actividades de supervisión**

Como ya se comentó, la realización de las actividades diarias permite observar si efectivamente los objetivos de control se están cumpliendo y si los riesgos se están considerando adecuadamente. Los niveles de supervisión y gerencia juegan un papel importante al respecto, ya que ellos son quienes deben concluir si el sistema de control es efectivo o ha dejado de serlo tomando las acciones de corrección o mejoramiento que el caso exige. Sobre estas actividades se presentan a continuación algunos ejemplos:

- La tendencia de la efectividad del sistema de control obtenida en el día con día, verificaciones de registros contra la existencia física de los recursos.
- Análisis de los informes de auditoría, contaduría, reporte de deficiencias, auto diagnóstico y otros.
- Comparación de información generada internamente con otra preparada por entidades externas.
- Juntas de trabajo y de evaluación en las que se traten asuntos relacionados con problemas de operación asociados con la efectividad de los controles.
- Detección de fraudes u otros actos indebidos perpetrados por el personal o por terceros.
- Obtención de reportes con bajo nivel de oportunidad y confiabilidad.

- **Evaluaciones independientes**

Este tipo de actividades también proporciona información valiosa sobre la efectividad de los sistemas de control. Desde luego las ventajas de este enfoque es que tales evaluaciones tienen un carácter independiente, que se traduce en objetividad y que están dirigidas respectivamente a la efectividad de los controles por adición a la evaluación de la efectividad de los procedimientos de supervisión y seguimiento del

sistema de control. Los objetivos, enfoque y frecuencia de las evaluaciones de control varían en cada organización dependiendo de las circunstancias específicas. La otra posibilidad para evaluación de los sistemas de control, es la combinación de las actividades de supervisión y las evaluaciones independientes, buscando con ello maximizar las ventajas de ambas alternativas y minimizar sus debilidades. La supervisión y seguimiento de los sistemas de control mediante las evaluaciones correspondientes, pueden ser ejecutadas por el personal encargado de sus propios controles, por los auditores internos durante la realización de sus actividades regulares, por auditores independientes, y finalmente por especialistas de otros campos.

La metodología de evaluación varía en un rango amplio que va desde cuestionarios y entrevistas hasta técnicas cuantitativas y otras más sofisticadas. Sin embargo, lo verdaderamente importante es la capacidad para entender las distintas actividades, componentes y elementos que integran un sistema de control, ya que de ello depende la calidad y profundidad de las evaluaciones. También es importante documentar las evaluaciones a un nivel adecuado, con el fin de lograr mayor utilidad de ellas.

El cuadro volumen del informe contiene material que puede ser útil al llevar a cabo una evaluación de un sistema de control interno.

- **Reporte de deficiencias**

El proceso de comunicar las debilidades y oportunidades de mejoramiento de los sistemas de control, debe estar dirigido hacia quienes son los propietarios y responsables de operarlos, con el fin de que implementen las acciones necesarias. Dependiendo de la importancia de las debilidades identificadas, la magnitud del riesgo existente y la probabilidad de ocurrencia, se determinará el nivel gerencial al cual deban comunicarse las deficiencias.

- **Participantes y sus responsabilidades**

“Todo el personal tiene alguna responsabilidad sobre el control. La gerencia es la responsable del sistema de control y debe asumir su propiedad. Los ejecutivos

financieros tienen un papel importante en la forma en que la gerencia ejercita el control, no obstante que todo el personal es responsable de controlar sus propias áreas. De igual manera, el auditor interno contribuye a la marcha efectiva del sistema de control, sin tener responsabilidad directa sobre su establecimiento y mantenimiento. En ambos casos aportan información útil acerca del nivel de calidad del sistema de control y cómo mejorarlo. El Consejo de Administración y el Consejo de Auditoría vigilan y dan atención al sistema de control interno. Otras partes externas, como son los auditores independientes y distintas autoridades, contribuyen al logro de los objetivos de la organización y proporcionan información útil para el control interno. Ellos no son responsables de su efectividad, ni forman parte de él, sin embargo aportan elementos para su mejoramiento.

Internamente las responsabilidades sobre el control corresponden conforme a lo siguiente:

- **Consejo de Administración:** Establece no sólo la misión y los objetivos de la organización, sino también las expectativas relativas a la integridad y los valores éticos.
- **Gerencia:** Debe asegurar que existe un ambiente propicio para el control.
- **Ejecutivos financieros:** Entre otras cosas, apoyan la prevención y detección de reportes financieros fraudulentos.
- **Comité de Auditoría:** Es el órgano que no sólo tiene la facultad de cuestionar a la gerencia en relación con el cumplimiento de sus responsabilidades, sino también asegurar que se tomen las medidas correctivas necesarias.
- **Comité de Finanzas:** Contribuye cumpliendo con la responsabilidad de evaluar la consistencia de los presupuestos con los planes operativos.
- **Auditoría Interna:** A través del examen de la efectividad y adecuación del sistema de control interno y mediante recomendaciones relativas a su mejoramiento.
- **Área Jurídica:** Llevando a cabo la revisión de controles y otros instrumentos legales, con el fin de salvaguardar los bienes de la Empresa.

- **Personal de la Organización:** Mediante la ejecución de las actividades que tiene cotidianamente asignadas y tomando las acciones necesarias para su control. También siendo responsable de comunicar cualquier problema que se presente en las operaciones, incumplimiento de normas o posibles faltas al código de conducta y otras violaciones.

En forma extrema la participación de las entidades externas consiste en lo siguiente:

Auditores Independientes: Proporcionan al Consejo de Administración y a la Gerencia un punto de vista objetivo e independiente, que contribuye al cumplimiento del logro de los objetivos de los reportes financieros, entre otros.

Autoridades (ejecutivas/legislativas): Participan mediante el establecimiento de requerimientos de control interno, así como en el examen directo de las operaciones de la organización, haciendo recomendaciones que lo fortalezcan." (1:122-128)

2.6 Origen ERM COSO II

"El COSO ERM, es una ampliación de la primera versión basada en el riesgo que se originó por al aumento de preocupación por la administración de riesgos, *The Committee of Sponsoring Organisations of the Treadway Commission* determinó la necesidad de la existencia de un marco reconocido de administración integral de riesgos. En septiembre de 2004, se publica el informe denominado *Enterprise Risk Management – Integrated Framework*, el cual incluye el marco global para la administración integral de riesgos. *Enterprise Risk Management - Integrated Framework* incluye el control interno, por lo que en ningún caso reemplaza a *Internal Control - Integrated Framework.*

ERM comenzó en las empresas de servicios financieros, seguros, servicios públicos, petróleo, gas, e industrias manufactureras químicas, ya que en estas industrias los riesgos están bien documentados y medidos; comúnmente se utilizan sofisticados

modelos estadísticos; existe entendimiento y supervisión sobre la sensibilidad del mercado y riesgos.

- **Conceptos clave sobre ERM**

- Valor
- Incertidumbre
- Riesgo

- **Premisas fundamentales**

Las premisas con las que cuenta el COSO ERM son:

- **Valor**

La premisa principal de la administración corporativa de riesgos es que cada entidad, con o sin fines de lucro, existe para "crear valor a sus grupos de interés". No obstante, todas las organizaciones encaran incertidumbre, el desafío para la administración es determinar cuánta incertidumbre está preparada para aceptar en la búsqueda de aumentar el valor de los grupos de interés.

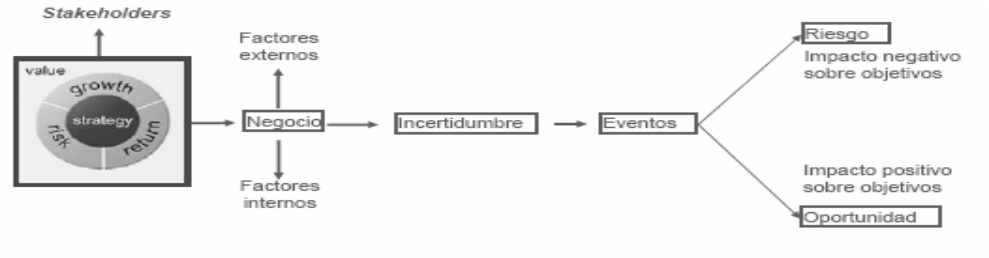
- **Incertidumbre**

La incertidumbre proviene tanto del entorno como de las decisiones dentro de la organización (fuentes internas y externas) y ésta se puede presentar como riesgo y oportunidad, con el potencial de destruir o generar valor.

- **Riesgo**

La administración de riesgos corporativos permite a la administración (*skateholder*) manejar esa incertidumbre, su riesgo y oportunidad asociado y, por lo tanto, incrementar la capacidad de la organización para construir valor. Representado en forma gráfica se apreciaría de la siguiente forma:

Figura 1
Administración de riesgo



Fuente: www.coso.org

- **Importancia de COSO ERM**

Es importante porque proporciona un marco integral del control interno y herramientas de evaluación para sistemas de control. Además proporciona una terminología utilizada comúnmente y principios usados como guía para desarrollar una arquitectura efectiva para la administración de riesgos y proporciona una visión integral del sistema de control institucional.

- **Beneficios de ERM**

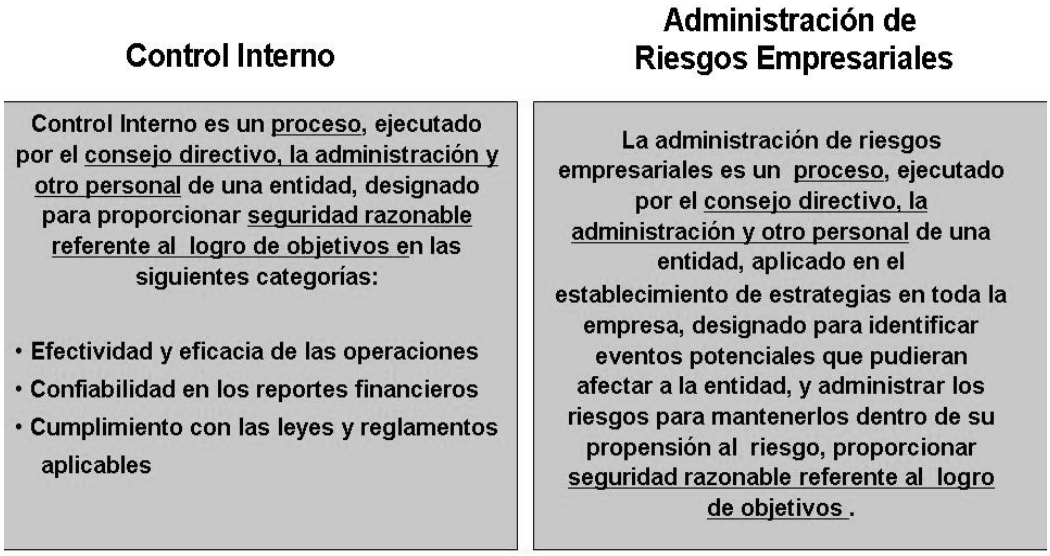
Los beneficios que proporciona el nuevo modelo de COSO son los siguientes:

- Alinear el apetito al riesgo con la estrategia.
- Relacionar crecimiento, riesgo y retorno.
- Mejorar las decisiones de respuesta al riesgo.
- Reducir sorpresas y pérdidas operacionales.
- Identificar y gestionar la diversidad de riesgos por compañía y grupo agregado.
- Aprovechar las oportunidades.
- Mejorar la asignación de capital." (12:1-20)

- **Diferencias entre el Informe COSO I y COSO ERM II**

El siguiente cuadro muestra las diferencias más importantes entre el control interno y la administración de riesgos empresariales, que es lo esencial en el modelo COSO ERM. (12: 1-5)

Figura 2
Comparaciones entre Informe COSO I y COSO ERM II



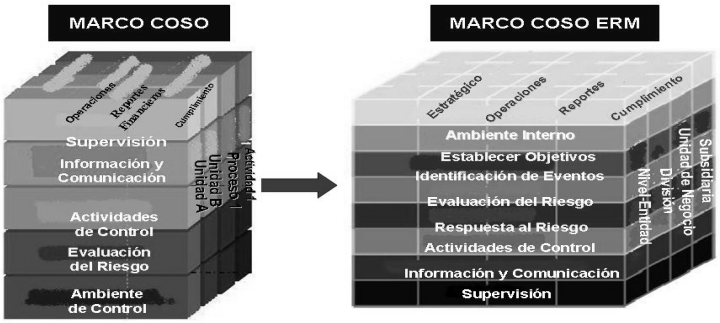
Fuente: www.coso.org

Se debe tomar en cuenta que el COSO ERM es diferente a:

- Una herramienta para la toma de decisiones.
- Una técnica de clasificación para dar seguimiento a controles internos.
- El único seguro al respecto.
- El trabajo de unos cuantos.

La forma gráfica y en que mejor se aprecia el cambio o evolución de COSO a COSO ERM es el siguiente:

Figura 3
Evolución Marco COSO I a COSO ERM II



Fuente: www.coso.org

- **Ambiente interno**

El ambiente interno tiene como función principal lo siguiente:

- Fundamento para todos los demás componentes de ERM
- Influye en estrategia y objetivos.
- Influye en diseño de actividades de control, sistemas de información y comunicación y supervisión de actividades.
- Incluye valores éticos, competencia del personal, estilo de operación, asignación de autoridad y responsabilidad y estructura organizacional. La Dirección se reconoce responsable de los riesgos y de ella emana la filosofía y estilo gerencial e integra y promueve el ERM.
- Evidencia de la cultura organizacional
    - ✓ Acuerdos con sus empleados
    - ✓ Trato a clientes y a otros externos
    - ✓ La incidencia de violaciones a leyes y reglamentos
    - ✓ El tono desde lo alto
    - ✓ Prudencia financiera

- ✓ La calidad de los productos y servicios ofrecidos
- ✓ Sus respuestas a las crisis
- ✓ Su imagen pública

Las culturas organizacionales cambian en el transcurso del tiempo:

- Jóvenes con entusiasmo vs compañías más maduras.
- Conforme maduran las empresas, sus estructuras de control interno deben madurar también
- Las empresas con dificultades financieras, a menudo minimizan costos en formas tales que reducen los controles internos

➢ **Establecimiento de objetivos**

Para mejor comprensión en lo que se refiere al establecimiento de objetivos se puede observar el siguiente cuadro:

Cuadro 2
Establecimiento de objetivos

Objetivos Estratégicos	Objetivos Relacionados	Objetivos Seleccionados	Propensión al Riesgo	Tolerancia al Riesgo
•Metas estratégicas •Misión/Visión •Elección de estrategia	•Operación •Información •Cumplimiento •Salvaguarda	•Alineación y apoyo •Decisiones de la Admón.	•Crecimiento, riesgo y entorno •Asig. Recursos •Gente, procesos e Infraestructura	•Variaciones aceptables •Métrica de Medición de Objetivos.

Fuente: www.coso.org

Para el establecimiento de objetivos debe de tenerse presente lo siguiente:

- o Deben existir objetivos antes de que la administración pueda identificar eventos que potencialmente afecten su logro.
- o Alinear misión/visión con objetivos

- Tipos: Estratégicos: relacionados con metas de alto nivel
- Reportes: confiabilidad en los mecanismos de reportes
- Cumplimiento: con leyes y reglamentos aplicables

Aquellos involucrados en el pensamiento estratégico deberían tener esta información:

- ✓ Tendencias económicas generales y en la industria específica
- ✓ Desarrollo de nuevos productos y procesos
- ✓ Tendencias tecnológicas
- ✓ Desarrollos en habilidades clave
- ✓ Marcos competitivos de desempeño
- ✓ Planes y metas estratégicas internas
- ✓ Resultados históricos de desempeño
- ✓ Oportunidades para incrementar el potencial de productos o mercados
- ✓ Disponibilidad de recursos
- ✓ Asuntos regulatorios
- ✓ Asuntos ambientales
- ✓ Efectos en empleados

- **Identificación de eventos**

Para poder identificar los eventos de las diferentes clases debe de observarse:

Cuadro 3
Identificación de eventos

Eventos	Factores Influy. Estrat. y Objs.	Metodología y técnicas	Eventos Inter-dependientes	Categorías de Eventos	Riegos y Oportunidades
•Incidental •Impacto positivo y/o negativo	•Internos •Externos	•Durante •Periódico •Pasado y Futuro	•Eventos precursores (reacciones en cadena) •Interrelacionados	•Grupos de riesgo por proceso y/o función	•Imp. Neg: Riesgo •Imp. Pos: Oport. •Disminución del riesgo

Fuente: www.coso.org

- **Evaluación de riesgos**

"Riesgo es la posibilidad de ocurrencia de un evento que pudiera afectar adversamente el logro de objetivos. Para poder controlar los riesgos e identificar cada uno de los eventos propensos a convertirse en riesgos debe de tomarse en cuenta lo siguiente:" (12: 45-46)

Cuadro 4

Evaluación de riesgos

Riesgo Inherente y Residual	Probabilidad e Impacto	Metodologías y Técnicas	Correlación
•Accs. Admvas. Previas •Accs. Admvas. Post. •Esperadas e Inesperadas	•Esperadas •Horizonte de tiempo •Métrica de medición •Datos observables	•Cualitativas •Cuantitativas	•Secuencia de eventos •Categorías •Escenarios

Fuente: www.coso.org

"Existen ciertas condiciones que pueden crear un riesgo adicional, entre las cuales tenemos:

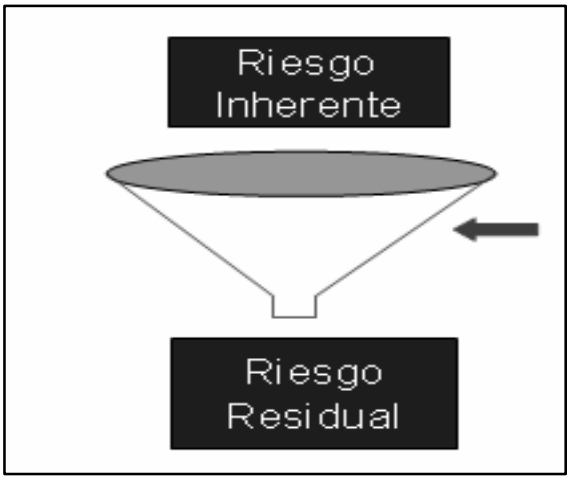
- Diseño u operación inadecuada del control interno
- Metas y planeación fuera de la realidad

- Actividades no autorizadas
- Entendimiento insuficiente de nuevas inversiones, productos, iniciativas y actividades de negocio similares
- Acciones correctivas pobremente planeadas o implementadas. Considerar los riesgos a largo plazo.

➢ **Riesgo inherente**: riesgo para la entidad en ausencia de cualquier acción realizada por la administración para alterar la probabilidad o el impacto.

➢ **Riesgo residual**: riesgo remanente después de la acción realizada por la administración para alterar su probabilidad o impacto.

Figura 4
Respuesta al riesgo: Control Interno



Fuente: www.coso.org

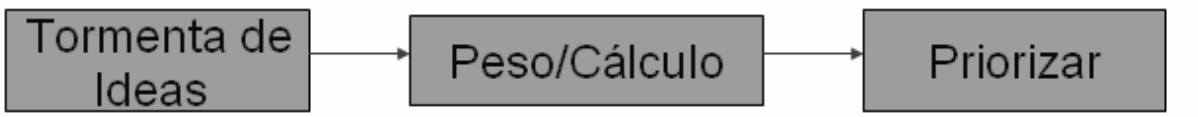
La forma en que debe de buscarse la solución adecuada al riesgo según ERM es la siguiente:

- Tormenta de ideas sobre riesgos y oportunidades.
- Identificar de raiz las causas y las correlaciones.

- La mejor forma es tener sesiones de facilitación
- Calcular el impacto del riesgo usando la misma medida de los objetivos
- Calcular los escenarios mínimo, máximo y probable
- Preparar un programa de riesgo
- Priorizar riesgos y oportunidades basados en su valor ponderado
- Identificar los riesgos clave que requieren atención estratégica

Los ocho puntos anteriores se resumen a:

Figura 5
Solución al riesgo: Control Interno



Fuente: www.coso.org

- **Respuesta al riesgo**

Existen Cuatro formas de respuesta al riego, las cuales son:

- Evasión
- Compartir
- Reducción
- Aceptación" (12: 47-73)

La respuesta al riesgo puede resumirse a:

Cuadro 5
Respuesta al riesgo

Identificación de Respuestas	Evaluación Posibles Respuestas	Elección de Respuesta	Visión Integral
•Evadir •Compartir •Reducir •rAceptar	•Impacto •Probabilidad •Costo Vs. Beneficio •Respuestas Innovativas	•Toma de decisiones	•Nivel entidad •Nivel Unidad de negocio •Base Inherente y residual

Fuente: www.coso.org

- **Actividades de control**

"Las actividades de control también incluyen sistemas, procesos, iniciativas, técnicas, programas, proyectos y otras formas de lograr los objetivos. Los controles internos que son efectivos bajo un conjunto de circunstancias, pueden no ser efectivos cuando cambian las condiciones." (12:79)

Cuadro 6
Actividades de control

Integradas a las Respuestas	Tipos de Control	Controles Generales	Controles de Aplicación	Específicos
•Implícitas en los procesos del negocio	•Políticas •Procedimientos •Preventivos •Detectivos •Manuales •Automatizados	•Admon. TI •Infraestructura TI •Admon. Seguridad •Desarrollo y Mantenimiento de software	•Integridad •Exactitud •Autorización •Validación	•Estrategias y objetivos específicos •Ambiente Operacional •Complejidad de la entidad

Fuente: www.coso.org

- **Información y Comunicación**

"La información puede obtenerse de diferentes fuentes y la comunicación generarse por varias vías, entre las cuales están:

- De fuentes internas y externas
- Identifica, captura, analiza y comunica a quienes lo necesitan
- Forma y tiempo.

- Útil para llevar a cabo responsabilidades
- Fluye hacia abajo, hacia arriba y a lo largo de la organización
- Intercambio con partes externas: clientes, proveedores, legisladores, accionistas
- Útil para identificar, evaluar y responder a riesgos, mover la entidad y lograr los objetivos.
- Información relevante. (12: 85)

➢ Supervisión

"La supervisión es verificar que los componentes están presentes y funcionando, y su calidad en el curso del tiempo, las cuales pueden ser de dos tipos, evaluaciones sobre la marcha o independientes.

La supervisión se realiza con la finalidad de reportar las deficiencias a quienes pueden tomar la acción apropiada.

La deficiencia se puede percibir, sea potencial o real. También la oportunidad para fortalecer el proceso, para aumentar la probabilidad del logro de objetivos." (12:103)

Cuadro 7
Seguimiento y Evaluación

Durante las Operaciones	Evaluaciones Independientes	Reporte Deficiencias
•Tiempo real •Implícito •Operaciones día a día	•Alcance •Frecuencia •Autoevaluación (facilitación Auditores Internos) •Ampliamente documentada	•Durante las Operaciones •Entidades externas •Protocolos •Canales alternos

Fuente: www.coso.org

2.7 Metodología y técnicas del control interno en TI

La Primera tarea consiste en estudiar modelos internacionales tales como COSO, COCO, SAC, etc., como referencia para implantación de modelos de control en sistemas complejos y altamente automatizados, que evidencia que el Modelo COBIT diseñado para el buen gobierno de las Tecnologías de Información era el adecuado. Es necesario ahondar sobre el Modelo COBIT por cuanto constituye un modelo de control interno dirigido a las necesidades de control de las tecnologías de información, es una herramienta innovadora que ayuda tanto a los directivos a comprender y administrar los riesgos asociados con estas tecnologías así como a los auditores a evaluar acertadamente el cumplimiento de estas políticas en aras de obtener informaciones con la calidad y seguridad que la alta dirección necesita para emitir criterios que faciliten el cumplimiento de los 210 objetivos de control detallados agrupados en 4 Dominios.

2.8 COBIT, historia y evolución

"La orientación de los negocios es el gran tema que abarca COBIT. Fue diseñado no sólo para ser implementado por los usuarios, sino que también y aún más importante, para los dueños de los negocios. Incluye todo el refuerzo de los procesos de las entidades, por lo que tiene total responsabilidad de todos los aspectos del proceso del negocio. En particular incluye todos los controles adecuados. En la primera edición del marco COBIT se define, el uso de estándares internacionales, las pautas y la investigación en las mejores prácticas condujeron al desarrollo de los objetivos del control. Las pautas de la intervención fueron desarrolladas después para determinar si estos objetivos del control están puestos en ejecución apropiadamente.

La investigación para las primeras y segundas ediciones incluyó la colección y el análisis de fuentes internacionales identificadas y fue realizada por los equipos en Europa (Universidad Libre de Amsterdam), los E.E.U.U. (Universidad Politécnica de California) y Australia (Universidad de Nuevo Gales del Sur). Cargaron a los investigadores con la compilación, la

revisión, el gravamen y la incorporación apropiada de los estándares técnicos internacionales, códigos de la conducta, estándares de calidad, estándares profesionales en la revisión, y las prácticas y los requisitos de la industria, como se relacionan con el marco y con los objetivos del control individual. Después de la colección y del análisis, desafiaron a los investigadores a examinar cada dominio, a procesar y profundizar y a sugerir los nuevos o modificados objetivos del control aplicables a ese detalle del proceso. La consolidación de los resultados fue realizada por el comité de dirección de COBIT.

El proyecto de la edición de COBIT 3ro consistió en desarrollar de las pautas de la gerencia y el poner al día la edición de COBIT 2do basado en nuevas y revisadas referencias internacionales.

Además, el marco de COBIT fue revisado y realzado para apoyar, el aumento de control de la gerencia, introduce gerencia de funcionamiento y la desarrolla más lejos a gobierno. Proveer a la gerencia un uso del marco, así que de él puede determinar y hacer las opciones para la puesta en práctica y las mejoras del control sobre su información y tecnología relacionada, así como funcionamiento de la medida, las pautas de la gerencia incluyen modelos de madurez, factores críticos del éxito, los indicadores dominantes de la meta y los indicadores dominantes del funcionamiento relacionados con los objetivos del control.

Las pautas de la gerencia fueron desarrolladas, se utilizó un panel mundial de 40 expertos de la academia; gobierno corporativo en TI para el aseguramiento, del control y de la seguridad. Estos expertos participaron en un taller residencial dirigido por los facilitadores profesionales que utilizaron las pautas del desarrollo definidas por el Comité de Dirección de COBIT. El taller fue apoyado fuertemente por el grupo de *PricewaterhouseCoopers* de *Gartner*, que no sólo proporcionaron la dirección del pensamiento pero también envió varias de sus expertos en control, de gerencia de funcionamiento y de seguridad de la información. Los resultados del taller eran modelos de la madurez del bosquejo, factores críticos del éxito, indicadores dominantes de la meta e indicadores dominantes del funcionamiento para cada uno de los objetivos de alto nivel del control de COBIT. La garantía de calidad de los objetivos iniciales fue conducida por el Comité de Dirección de COBIT y los resultados fueron fijados para la exposición en la

página web de ISACA. El documento de las pautas de la gerencia ofreció un nuevo sistema gerencia-orientado de herramientas, mientras que proveía de la integración y de la consistencia al marco COBIT.

La actualización a los objetivos del control en la edición de COBIT 3ro, basada en nuevas y revisadas referencias internacionales, fue conducida por los miembros de los capítulos de ISACA, bajo la dirección de los miembros del Comité de Dirección de COBIT. La intención no era realizar un análisis global de todo el material o de una reconstrucción de los objetivos del control, sino proporcionar un proceso incremental de la actualización. Los resultados del desarrollo de las pautas de la gerencia entonces fueron utilizados para revisar el marco de COBIT, especialmente las consideraciones, las metas y las declaraciones del activador de los objetivos de alto nivel del control. La edición de COBIT 3ro fue publicada en julio de 2000. Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) son un juego de las mejores prácticas (el marco) para la información (TI) la dirección creada por la Revisión de cuentas de Sistemas de Información y la Asociación de Control (ISACA), y el Instituto de Gobernación TI (ITGI) en 1992.

"COBIT 4.0 ayudaba a llevar las directrices de Gobierno TI a más ejecutivos de negocio y de TI ", según Frank Yam, vicepresidente de Information Systems Audit and Control Association (ISACA).

La primera edición fue publicada en 1996; la segunda en 1998; la tercera en 2000 (la edición en línea se hizo disponible en 2003); la cuarta edición en diciembre de 2005. Esto recientemente ha sido bien recibido debido a acontecimientos externos, sobre todo el escándalo Enron y el paso subsecuente de la puesta en vigencia de la ley *Sarbanes-Oxley.*

COBIT 4.0 es la primera actualización del contenido de COBIT ya que COBIT la 3a Edición fue liberado en 2000. La última edición fue emitida en 2007, y se denomina COBIT 4.1." (2: 187)

- **COBIT y OTRAS NORMAS**

COBIT e ISO/IEC 17799:2005

“Las dos normas internacionales usadas al comienzo son COBIT E ISO/IEC 17799:2005. COBIT (Objetivos de Control para la Información y la Tecnología relacionada) fue liberado y usado principalmente por la comunidad TI. En 1998, las directrices de dirección fueron añadidas, y COBIT se hizo el marco internacionalmente aceptado para la gobernación TI y el control. ISO/IEC 17799:2005 (el Código de práctica para la Seguridad de Información de la Dirección) es también un estándar internacional y es lo mejor para poner en práctica la dirección de seguridad. Las dos normas no compiten la una con la otra y en realidad se complementan. COBIT típicamente cubre una más amplia área mientras ISO/IEC 17799 profundamente es enfocado (concentrado) en el área de seguridad.

Abajo se describe la interrelación de las dos normas así como ISO/IEC 17799 puede ser integrado con COBIT.

Figura 6
Mapa de correlación entre COBIT y Norma ISO

COBIT DOMINIO	1	2	3	4	5	6	7	8	9	10	11	12	13
El plan y Organiza	-	+	-	-	+	+	+	+	-	-	0	.	.
Adquiera y el Instrumento	+	0	0	-	0	+	.	.	.	.	.	.	.
Entregue y el Apoyo	-	+	0	+	+	.	+	0	0	0	+	0	0
El monitor y Evalúa	-	0	-	0	.	.	.	.	.	.	.	.	.

Fuente: Organización Internacional para la Estandarización

(+) El marcar bueno (más de dos ISO/IEC 17799:2005 los objetivos fueron trazados un mapa de a un proceso de COBIT)

(0) En parte el marcar (un dos ISO/IEC 17799:2005 objetivos fue trazado un mapa de a un proceso de COBIT)

(-) No o el marcar menor (ningún ISO/IEC 17799:2005 el objetivo fue trazado un mapa de a un proceso de COBIT)

(.) No existe

Actualmente COBIT se relaciona con la norma ISO 27001. La norma "ISO/IEC 27001:2005- *Information Technology Security techniques*", es la evolución certificable del código de buenas prácticas ISO 17799. Avala la adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un Sistema de Gestión de Seguridad Informática, siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones." (17: 1-17)

- **COBIT y *Sarbanes Oxley***

"Requieren las empresas públicas que son sujetos a EE UU *Sarbanes Oxley* el Acto de 2002 para adoptar los marcos de control siguientes: el Comité para Patrocinar las Organizaciones de la Comisión de *Treadway* (COSO) el Control Interno integró el Marco y los Objetivos de Control del Instituto de Gobernación TI para la Información y la Tecnología Relacionada (COBIT). Al escoger cuál de los marcos de control para poner en práctica podrían cumplir con *Sarbanes-Oxley*, las Seguridades estadounidenses y la Comisión de cambio sugieren que las empresas sigan el marco COSO. COSO se integró, el Marco declara que el control interno es un proceso - establecido por la Junta Directiva de una entidad, la dirección, y otro personal - diseñado para proporcionar el aseguramiento razonable en cuanto al logro de objetivos indicados. COBIT se acerca al control de TI por mirar la información - no la información solamente (justo) financiera - que es necesario para apoyar exigencias de negocio y los recursos asociados TI y procesos. COSO objetivos de control enfocan la eficacia, la eficiencia de operaciones, el reportaje confiable financiero, y el cumplimiento con leyes y regulaciones. COBIT es ampliado para cubrir la calidad y exigencias de seguridad en siete categorías de traslape, que incluyen la eficacia, la eficiencia, la confidencialidad, la integridad, la disponibilidad, el cumplimiento, y la fiabilidad de información.

Estas categorías forman la fundación para los objetivos de control de COBIT. Los dos marcos también tienen el público diferente. COSO es útil para la dirección en general, mientras COBIT es útil para la dirección, usuarios, e interventores. COBIT expresamente es enfocado (concentrado) en mandos de TI. A causa de estas

diferencias, interventores no deberían esperar una relación de uno a uno entre los cinco componentes de control de COSO y los cuatro dominios COBIT objetivos.

El marco de trabajo COBIT provee una herramienta que facilita la delegación de responsabilidades, la cual empieza con una premisa pragmática. Para proveer información la organización necesita cumplir con sus objetivos. Los recursos TI necesitan ser manejados por un conjunto de procesos agrupados. Continúa con un conjunto de 34 niveles de control y objetivos, uno para cada proceso TI, agrupado en 4 dominios:

- ✓ **Planeamiento y Organización**
- ✓ **Adquisición e Implementación**
- ✓ **Entrega y Soporte**
- ✓ **Monitoreo y Evaluación**

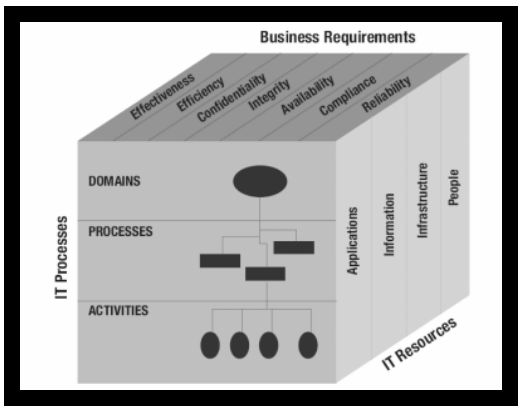
Estas estructuras cubren todos los aspectos de la información y la tecnología. Al acceder a estos 34 niveles de control, con las políticas de la organización; los dueños del proceso del negocio pueden adecuar los controles de los sistemas provistos por el ambiente TI. A esto se le suma que los 34 niveles tienen una guía de auditoría, para que la información pueda ser auditada y revisada contra los objetivos recomendados por COBIT para proveer a la Dirección de la empresa una fuente fiel de los informes de cada proceso.

2.9 Etapas en que se divide el establecimiento de controles

Los procesos TI definidos en los 4 dominios: COBIT es una herramienta que permite a los directores comunicarse y hacer de puente entre los controles de requerimiento, partes técnicas y riesgos de negocios. El desarrollo de COBIT está determinado en 5 pasos. A continuación se muestra el Cubo COBIT, que provee una visión tridimensional del control interno en TI." (4:25). Como puede observarse este consta de dominios, que se dividen en procesos y éstos a su vez en actividades, los criterios de

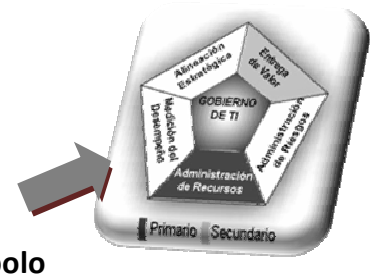
la información deben ser calidad, confianza y seguridad, aplicado a los siguientes recursos: personas, aplicaciones, información e infraestructura.

Figura 7
Cubo COBIT y Áreas de Enfoque de Gobierno de TI



FUENTE: www.isaca.org

Símbolo



	Metas	Métricas	Practicas	Modelos de Madurez
Alineamiento Estratégico	P	P		
Entrega de Valor		P	S	P
Gestión de Riesgos		S	P	S
Gestión de Recursos		S	P	P
Medición del Desempeño	P	P		S

P = Facilitador Primario S = Facilitador Secundario

FUENTE: www.isaca.org

Esta equivalencia se basa en marco de trabajo original COSO, así como COSO ERM.

- ✓ **Factor primario P= grado al cual el objetivo de control definido impacta directamente**
- ✓ **Factor Secundario S = grado al el objetivo satisface únicamente en forma indirecta**
- ✓ **Blanco podría aplicarse, sin embargo los requerimientos son satisfechos más apropiadamente por otro criterio.**

CAPÍTULO III

COBIT (Objetivos de control para la información y la tecnología relacionada)

3.1 Evolución de COBIT 3ª Edición a COBIT 4.1

"Los cambios principales al marco de trabajo de COBIT como resultado de la actualización a COBIT 4.0 son los siguientes:

- El dominio **M** se ha convertido ahora a ME, y significa **Monitorear y Evaluar.**

- **M3 Y M4** eran procesos de auditoría y no procesos de TI. Fueron eliminados debido a que están cubiertos de forma adecuada por un número de estándares de auditoría de TI. Aunque se han proporcionado referencias dentro del marco de trabajo actualizado para enfatizar la necesidad que tiene la gerencia de usar funciones de aseguramiento.

- **ME3** es el proceso relacionado con la supervisión regulatoria, el cual está cubierto en **PO8** previamente.

- **ME4** cubre el proceso de supervisión del gobierno sobre TI, conserva el propósito de COBIT de fungir como un marco de trabajo de gobierno de TI. Al posicionar ese proceso al final de la cadena, se subraya el apoyo que cada proceso previo brinda a la última meta de implementar un gobierno efectivo de TI en la empresa.

- Con la eliminación de **PO8** y la necesidad de mantener la numeración **PO9** Evaluar riesgos y **PO10** Administrar proyectos de modo consistente con la 3era. Edición de COBIT, **PO8** ahora se convierte en Administrar la calidad, que antes era el proceso **PO11.** El dominio **PO** ahora tiene **10** procesos en lugar de **11.**

- El dominio **AI** requirió dos cambios: la adición de un proceso de procuración y la necesidad de incluir en AI5 los aspectos de administración de versiones. El último cambio sugirió que éste debería ser el último proceso de dominio y por lo tanto se convirtió en AI7. El vacío que se creó en AI5 se usó para añadir el nuevo proceso de procuración. El dominio AI tiene siete procesos en lugar de seis.

❖ **Objetivos de Control Detallados**

Como se puede observar en la descripción anterior a nivel del marco de trabajo y en el trabajo para aclarar y enfocar el contenido de los objetivos de control, la actualización del marco de trabajo COBIT ha cambiado significativamente los objetivos de control dentro de éste. Estos componentes se han reducido de **215 a 210,** porque todos los materiales genéricos ahora sólo se conservan al nivel de marco de trabajo y no se repiten en cada proceso. Así mismo, todas las referencias a controles aplicativos se movieron al marco de trabajo y los objetivos específicos de control se agregaron en nuevas declaraciones. Para apoyar la actividad de transición en relación con los objetivos de control, los siguientes dos juegos de tablas muestran las referencias cruzadas entre los nuevos y viejos objetivos de control.

❖ **Directrices Gerenciales**

Las entradas y salidas se han añadido para ilustrar lo que los procesos necesitan de otros y lo que típicamente generan. También se proporcionan actividades y responsabilidades asociadas. Las entradas y las metas de las actividades reemplazan a los factores críticos de éxito de COBIT 3ª Edición. Las métricas ahora se basan en una cascada consistente de metas de negocio, de TI, de proceso y de actividades. El juego de métricas de COBIT 3ª Edición también se revisó y mejoró para hacerlo más representativo y medible." (4:179)

3.2 Aspectos Generales del Informe COBIT

"COBIT se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes y se adapta a principios de gobierno generalmente aceptados. Está posicionado a un nivel alto, impulsado por los requerimientos del negocio, cubre el rango completo de actividades de TI, y se concentra en lo que se debe lograr en lugar de cómo lograr un gobierno, administración y control efectivos. Por lo tanto funciona como un integrador de prácticas de gobierno TI y es de interés para la dirección ejecutiva; para la gerencia de la organización, para la gerencia y gobierno de TI; para los profesionales de aseguramiento y seguridad; así como para los profesionales de auditoría y control TI. Está diseñado para ser complementario y para ser usado junto con estándares y mejores prácticas.

Para lograr la alineación de las mejores prácticas con los requerimientos de la entidad, se recomienda que COBIT se utilice al más alto nivel, brinda así un marco de control general basado en un modelo de procesos TI que debe ser aplicable en general a toda la empresa. Las prácticas y los estándares específicos que cubren áreas discretas, se pueden equiparar con el marco de trabajo de COBIT, brindando así una jerarquía de materiales guía.

- **COBIT resulta de interés a distintos usuarios**

- ✓ **Dirección ejecutiva** Para obtener valor de las inversiones y para balancear las inversiones en riesgo y control de en un ambiente TI con frecuencia impredecible.

- ✓ **Gerencia del negocio** Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros.

- ✓ **Gerencia de TI** Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada.

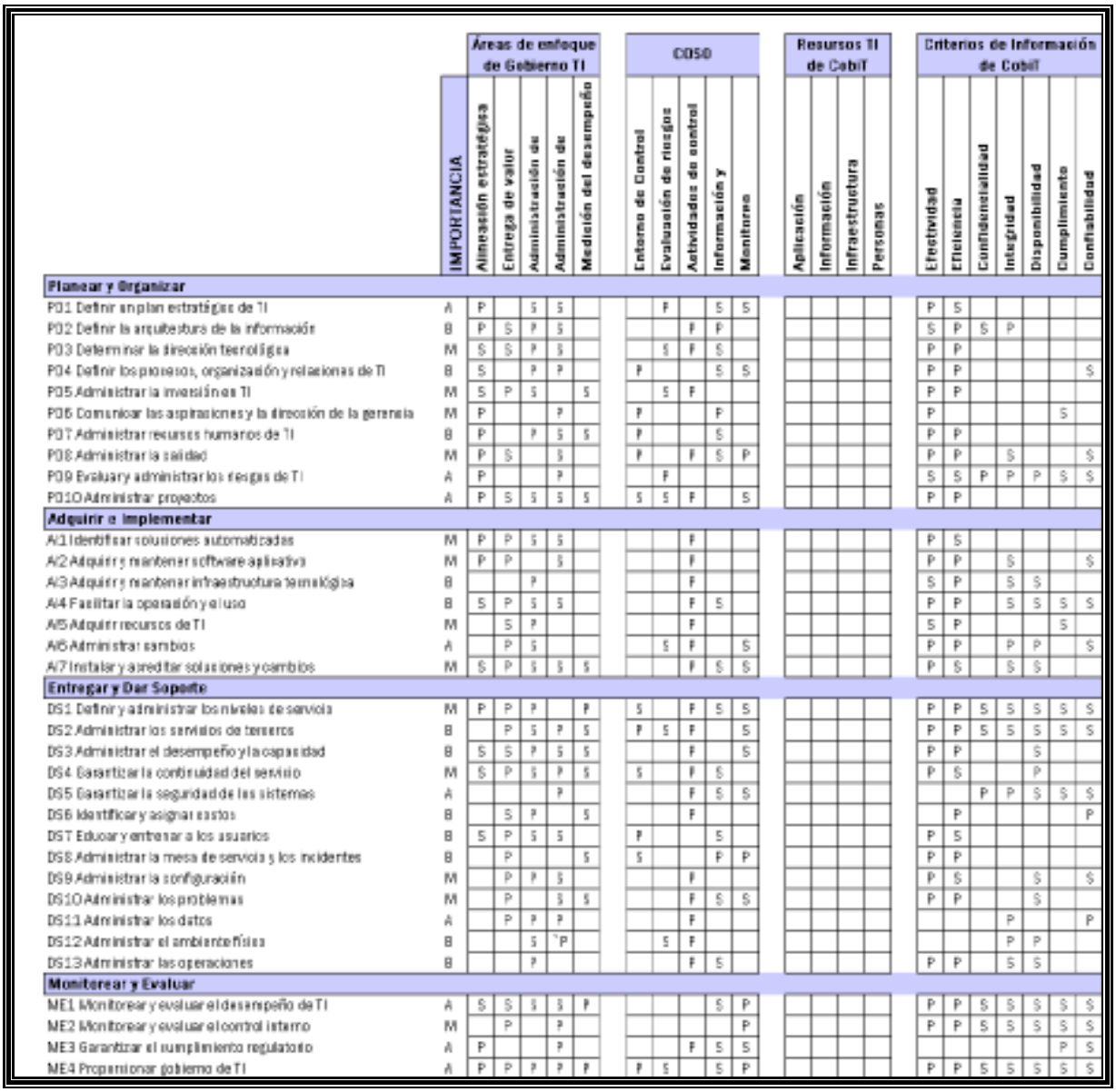
- ✓ **Auditores** Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos.

COBIT ha sido desarrollado y es mantenido por un instituto de investigación (ISACA) sin ánimo de lucro, toma la experiencia de los miembros de sus asociaciones afiliadas, de los expertos de la industria, y de los profesionales de control y seguridad. Su contenido se basa en una investigación continua sobre las mejores prácticas de TI y se le da un mantenimiento continuo, proporciona así un recurso objetivo y práctico para todo tipo de usuario.

COBIT está orientado a los objetivos y al alcance del gobierno de TI, asegura que su marco de control sea integral, que esté alineado con los principios de Gobierno Corporativo y, por lo tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva, para los auditores y reguladores. Es importante señalar que los objetivos de control detallados de COBIT, se relacionan con las cinco áreas de enfoque del gobierno de TI y con las actividades de control de COSO. Al finalizar un establecimiento de controles debe existir equivalencias entre los procesos de TI y las áreas focales del gobierno de TI, COSO, los recursos TI de COBIT y los criterios de información de COBIT, que se muestran en la siguiente matriz.” (4: 25,173).

Durante el proceso de investigación se concluye y debe de resaltarse que para el desarrollo de COBIT, se basó en COSO, pero adaptándolo a los ambientes de tecnología, como también es importante reconocer que cada versión viene mejorada en base a las aportaciones de especialistas en el área de control interno y ambientes TI. COBIT puede parecer largo pero al implementarlo tanto la administración como el auditor reconocen que es una lista bastante completa de objetivos mínimos que deben de cumplirse dentro de los ambientes TI.

Tabla 2
Matriz de Equivalencias



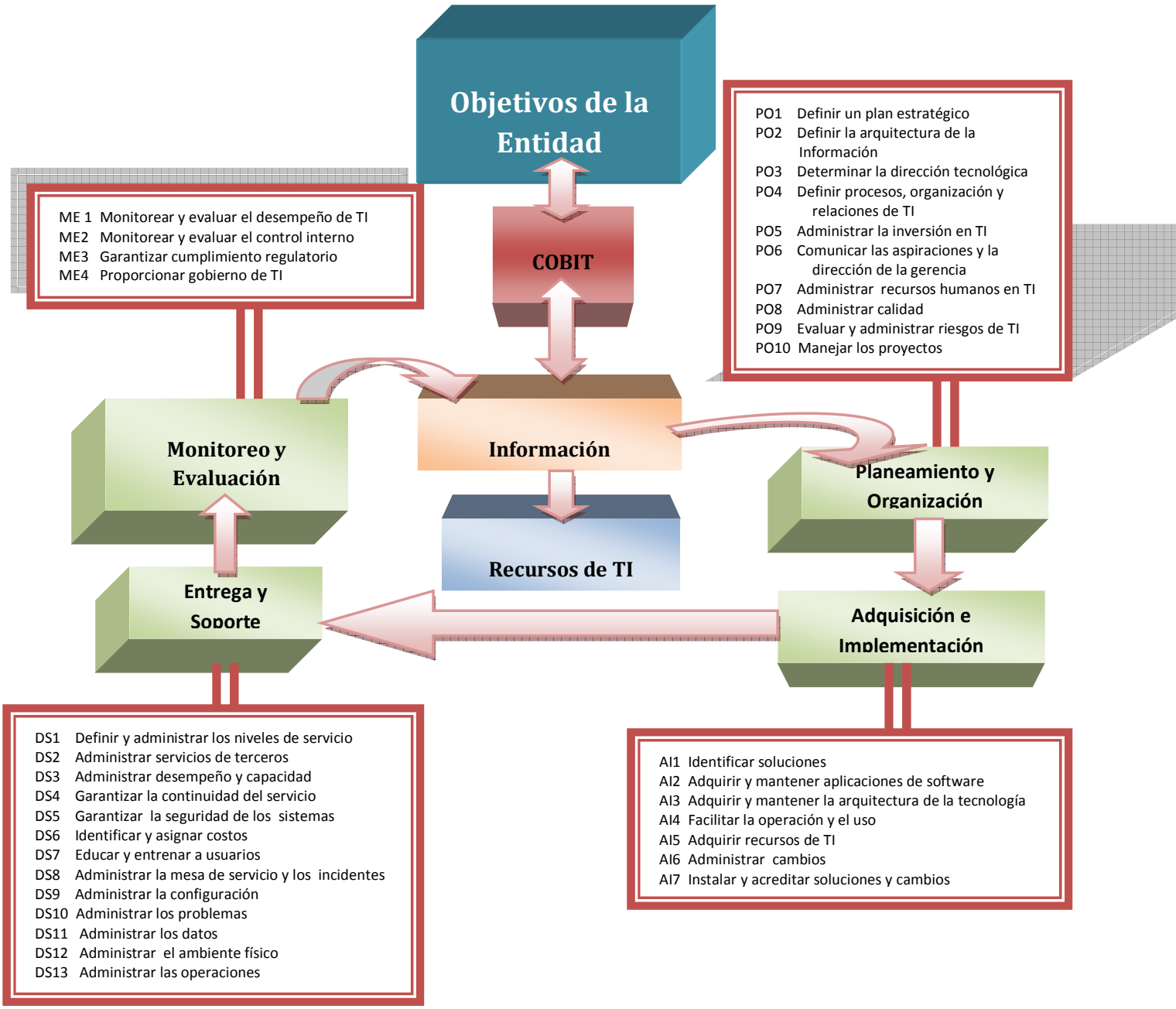
		Áreas de enfoque de Gobierno TI					COSO					Recursos TI de CobiT				Criterios de Información de CobiT						
	IMPORTANCIA	Alineación estratégica	Entrega de valor	Administración de	Administración de	Medición del desempeño	Entorno de Control	Evaluación de riesgos	Actividades de control	Información y	Monitoreo	Aplicación	Información	Infraestructura	Personas	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar																						
PO1 Definir un plan estratégico de TI	A	P		S	S			P		S	S					P	S					
PO2 Definir la arquitectura de la información	B	P	S	P	S				P	P						S	P	S	P			
PO3 Determinar la dirección tecnológica	M	S	S	P	S			S	P	S						P	P					
PO4 Definir los procesos, organización y relaciones de TI	B	S		P	P		P			S	S					P	P					S
PO5 Administrar la inversión en TI	M	S	P	S		S		S	P							P	P					
PO6 Comunicar las aspiraciones y la dirección de la gerencia	M	P			P		P			P						P					S	
PO7 Administrar recursos humanos de TI	B	P		P	S	S	P			S						P	P					
PO8 Administrar la calidad	M	P	S		S		P		P	S	P					P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	A	P			P			P								S	S	P	P	P	S	S
PO10 Administrar proyectos	A	P	S	S	S	S	S	S	P		S					P	P					
Adquirir e Implementar																						
AI1 Identificar soluciones automatizadas	M	P	P	S	S				P							P	S					
AI2 Adquirir y mantener software aplicativo	M	P	P		S				P							P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	B			P					P							S	P		S	S		
AI4 Facilitar la operación y el uso	B	S	P	S	S				P	S						P	P		S	S	S	S
AI5 Adquirir recursos de TI	M		S	P					P							S	P				S	
AI6 Administrar cambios	A		P	S				S	P		S					P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S					P	S		S	S		
Entregar y Dar Soporte																						
DS1 Definir y administrar los niveles de servicio	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	B		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	B	S	S	P	S	S			P		S					P	P			S		
DS4 Garantizar la continuidad del servicio	M	S	P	S	P	S	S		P	S						P	S			P		
DS5 Garantizar la seguridad de los sistemas	A				P				P	S	S							P	P	S	S	S
DS6 Identificar y asignar costos	B		S	P		S			P								P					P
DS7 Educar y entrenar a los usuarios	B	S	P	S	S		P			S						P	S					
DS8 Administrar la mesa de servicio y los incidentes	B		P			S	S			P	P					P	P					
DS9 Administrar la configuración	M		P	P	S				P							P	S			S		S
DS10 Administrar los problemas	M		P		S	S			P	S	S					P	P			S		
DS11 Administrar los datos	A		P	P	P				P										P			P
DS12 Administrar el ambiente físico	B			S	P			S	P										P	P		
DS13 Administrar las operaciones	B			P					P	S						P	P		S	S		
Monitorear y Evaluar																						
ME1 Monitorear y evaluar el desempeño de TI	A	S	S	S	S	P				S	P					P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	M		P		P						P					P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio	A	P			P				P	S	S										P	S
ME4 Proporcionar gobierno de TI	A	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

Esta equivalencia se basa en marco de trabajo original COSO, así como COSO ERM. Fuente: www.isaca.org

- ✓ **Factor primario P= grado al cual el objetivo de control definido impacta directamente**
- ✓ **Factor Secundario S = grado al el objetivo satisface únicamente en forma indirecta**
- ✓ **Blanco podría aplicarse, sin embargo los requerimientos son satisfechos más apropiadamente por otro criterio.**

3.3 MARCO DE TRABAJO COMPLETO DE COBIT

Gráfica 7
Elementos del marco de trabajo y su relación



Fuente: Elaboración propia con base en COBIT 4.1

PO = Planeación y Organización

DS= Entrega y Soporte

AI= Adquisición e Implementación

ME= Monitoreo y Evaluación

3.3.1 PLANEAR Y ORGANIZAR (PO)

"Este dominio cubre las estrategias y las tácticas, tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos de la entidad. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

- **Preguntas**
  - ✓ ¿Están alineadas las estrategias y de la organización?
  - ✓ ¿Está alcanzando un uso óptimo de sus recursos?
  - ✓ ¿Entienden todas las personas dentro de la organización los objetivos de TI?
  - ✓ ¿Es apropiada la calidad de los sistemas de TI para las necesidades de la entidad?

Para sacar una puntuación de confianza de cada control de alto nivel se utilizará una media entre los subprocesos y para el nivel de madurez de todo el dominio se sacará una media de medias de todos los procesos. Así se realizará en cada dominio. **PLANEACIÓN Y ORGANIZACIÓN posee 10 procesos de control de alto nivel y 74 objetivos de control detallados.**" (4:12)

Tabla 3
Dominio Planeación y Organización
Febrero 2010

Dominio	PROCESO	7 Criterios de Información en la Identidad								Recursos de TI			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Planeación y Organización													
PO1	Definir un Plan Estratégico de TI	P	S							✓	✓	✓	✓
PO2	Definir la Arquitectura de Información	S	p	S	P					✓	✓		
PO3	Determinar la dirección tecnológica	P	P							✓		✓	
PO4	Definir los procesos, organización y relaciones de TI	P	P										✓
PO5	Administrar la Inversión en TI	P	P					S		✓		✓	✓
PO6	Comunicar las aspiraciones y la dirección de la gerencia	P					S				✓		✓
PO7	Administrar Recursos Humanos de TI	P	P										✓
PO8	Administrar la calidad	P	P		S			S		✓	✓	✓	
PO9	Evaluar y administrar los riesgos de TI	S	S	P	P	P	S	S		✓	✓	✓	✓
PO10	Administrar proyectos	P	P							✓		✓	✓

Fuente: Elaboración propia con base en COBIT 4.1

Cuadro 8
Calificación de madurez por proceso dentro del dominio Planeación y Organización: toma en cuenta objetivos de control detallado por proceso
Febrero 2010

	No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
PO1 Definir un Plan estratégico de TI						
PO2 Definir la Arquitectura de la Información						
PO3 Determinar la Dirección Tecnológica						
PO4 Definir los procesos, Organización y Relaciones de TI						
PO5 Administrar la inversión en TI						
PO6 Comunicar las aspiraciones y la Dirección de la Gerencia						
PO7 Administrar Recursos Humanos de TI						
PO8 Administrar la calidad						
PO9 Evaluar y administrar los riesgos de TI						
PO10 Administrar proyectos						

Fuente: Elaboración propia con base en COBIT 4.1

3.3.2 ADQUIRIR E IMPLEMENTAR (AI)

"Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos de la entidad. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos de la organización.

- **Preguntas**
  - ✓ ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades de la organización?
  - ✓ ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
  - ✓ ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
  - ✓ ¿Los cambios no afectarán a las operaciones actuales de la entidad?

ADQUISICIÓN E IMPLEMENTACIÓN posee 7 procesos de control de alto nivel y 40 objetivos de control detallados." (4:13)

Dominio	Tabla 4 Dominio Adquisición e Implementación Febrero 2010	7 Criterios de Información en la Identidad								Recursos de TI			
	PROCESO	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Adquisición e Implementación													
AI1	Identificar Soluciones automatizadas	P	S							✓		✓	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S			S		✓			
AI3	Adquirir y Mantener Arquitectura de TI	S	P		S	S						✓	
AI4	Facilitar la operación y el uso	P	P		S	S	S	S		✓		✓	✓
AI5	Adquirir recursos de TI	S	P			S				✓	✓	✓	✓
AI6	Administrar Cambios	P	P		P	P		S		✓	✓	✓	✓
AI7	Instalar y acreditar soluciones y cambios	P	S		S	S				✓	✓	✓	✓

Fuente: Elaboración propia con base en COBIT 4.1

Cuadro 9
Calificación de madurez por proceso dentro del dominio Adquisición e Implementación: toma en cuenta objetivos de control detallado por proceso
Febrero 2010

	No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
AI1 Identificar soluciones automatizadas						
AI2 Adquirir y mantener software aplicativo						
AI3 Adquirir y mantener infraestructura tecnológica						
AI4 Facilitar la operación y el uso						
AI5 Adquirir recursos de TI						
AI6 Administrar cambios						
AI7 Instalar y acreditar soluciones y cambios						

Fuente: Elaboración propia con base en COBIT 4.1

3.3.3 ENTREGAR Y DAR SOPORTE (DS)

"Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

❖ **Preguntas**

- ✓ ¿Se están entregando los servicios TI de acuerdo con las prioridades de la organización?
- ✓ ¿Están optimizados los costos de TI?
- ✓ ¿Está capacitado el personal para utilizar los sistemas de TI de manera productiva y segura?
- ✓ ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

ENTREGAR Y DAR SOPORTE posee 13 procesos de control de alto nivel y 71 objetivos de control detallados." (4:13)

	Tabla 5 **Dominio Entregar y dar Soporte** **Febrero 2010**	**7 Criterios de Información en la Identidad**								**Recursos de TI**			
Dominio	**PROCESO**	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Servicios y Soporte													
DS1	Definir niveles de servicio	P	P	S	S	S	S	S		✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S		✓	✓	✓	✓
DS3	Administrar Desempeño y Capacidad	P	P			S				✓		✓	
DS4	Asegurar Servicio Continuo	P	S			P				✓	✓	✓	✓
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S		✓	✓	✓	✓
DS6	Identificar y Asignar Costos		P					P		✓	✓	✓	✓
DS7	Capacitar Usuarios	P	S										✓
DS8	Administrar la mesa de servicio y los incidentes	P	P							✓			✓
DS9	Administrar la Configuración	P	S			S		S		✓	✓	✓	
DS10	Administrar Problemas e Incidentes	P	P			S				✓	✓	✓	✓
DS11	Administrar Datos				P			P			✓		
DS12	Administrar Instalaciones				P	P						✓	
DS13	Administrar Operaciones	P	P		S	S				✓	✓	✓	✓

Fuente: Elaboración propia con base en COBIT 4.1

Cuadro 10
Calificación de madurez por proceso dentro del Dominio Entregar y dar Soporte: toma en cuenta objetivos de control detallado por proceso
Febrero 2010

	No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
DS1 Definir y administrar los niveles de servicio						
DS2 Administrar los servicios de terceros Proveedores						
DS3 Administrar el desempeño y la capacidad						
DS4 Garantizar la continuidad del servicio						
DS5 Garantizar la seguridad de los sistemas						
DS6 Identificar y asignar costos						
DS7 Educar y entrenar a los usuarios						
DS8 Administrar la mesa de servicio y los incidentes						
DS9 Administrar la configuración						
DS10 Administrar los problemas						
DS11 Administrar los datos						
DS12 Administrar el ambiente físico						
DS13 Administrar las operaciones						

Fuente: Elaboración propia

3.3.4 MONITOREAR Y EVALUAR (ME)

"Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

- **Preguntas**
  - ✓ ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
  - ✓ ¿La Jefatura de la Clínica garantiza que los controles internos son efectivos y eficientes?

- ✓ ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?

- ✓ ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

MONITOREAR Y EVALUAR posee 4 procesos de control de alto nivel y 25 objetivos de control detallados." (4:13)

	Tabla 6 Dominio Monitorear y Evaluar Febrero 2010	7 Criterios de Información en la Identidad								Recursos de TI			
Dominio	**PROCESO**	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Monitoreo													
ME1	Monitorear y evaluar el desempeño de TI	P	P	S	S	S	S	S		✓	✓	✓	✓
ME2	Monitorear y evaluar el control interno	P	P	S	S	S	S	S		✓	✓	✓	✓
ME3	Garantizar el cumplimiento regulatorio						P	S		✓	✓	✓	✓
ME4	Proporcionar gobierno de TI	P	P	S	S	S	S	S		✓	✓	✓	✓

Fuente: Elaboración propia con base en COBIT 4.1

Cuadro 11
Calificación de madurez por proceso dentro del dominio Monitorear y Evaluar: toma en cuenta objetivos de control detallado por proceso
Febrero 2010

	No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
ME1 Monitorear y Evaluar el Desempeño de TI						
ME2 Monitorear y Evaluar el Control Interno						
ME3 Garantizar el Cumplimiento Regulatorio						
ME4 Proporcionar Gobierno de TI						

Fuente: Elaboración propia con base en COBIT 4.1

3.4 Los 34 procesos TI

"COBIT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación.

- **Los procesos requieren controles**

Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Los objetivos de control de TI, proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Ellos:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

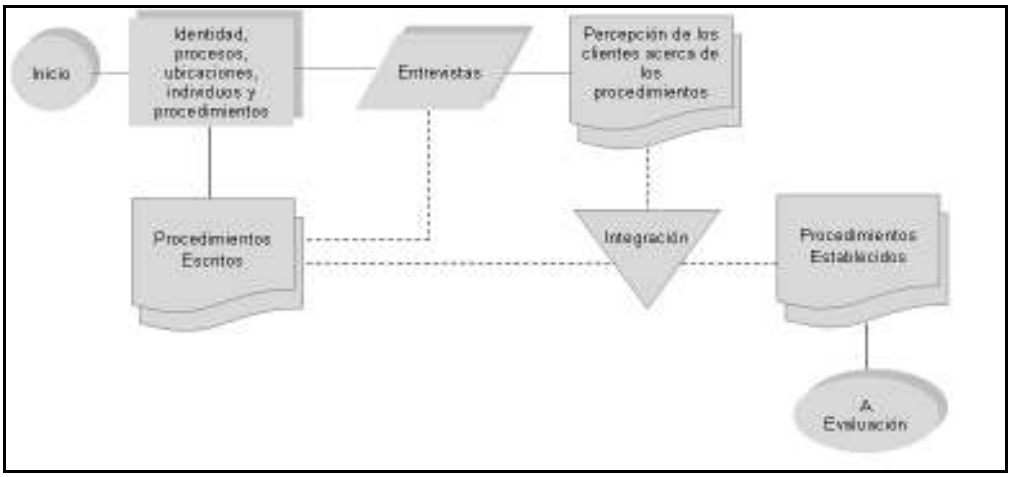
La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:

- Seleccionando aquellos aplicables
- Decidir aquellos que deben implementarse
- Elegir como implementarlos (frecuencia, extensión, automatización, etc.)
- Aceptar el riesgo de no implementar aquellos que podrían aplicar." (4:13)

3.5 Guías de gestión

Al realizar tanto una auditoría informática como un establecimiento de controles internos basados en COBIT 4.1, se aplicarán técnicas y procedimientos de auditoría.

Flujograma 2
PRIMER PASO
IDENTIFICACIÓN/DOCUMENTACIÓN



FUENTE: www.isaca.org

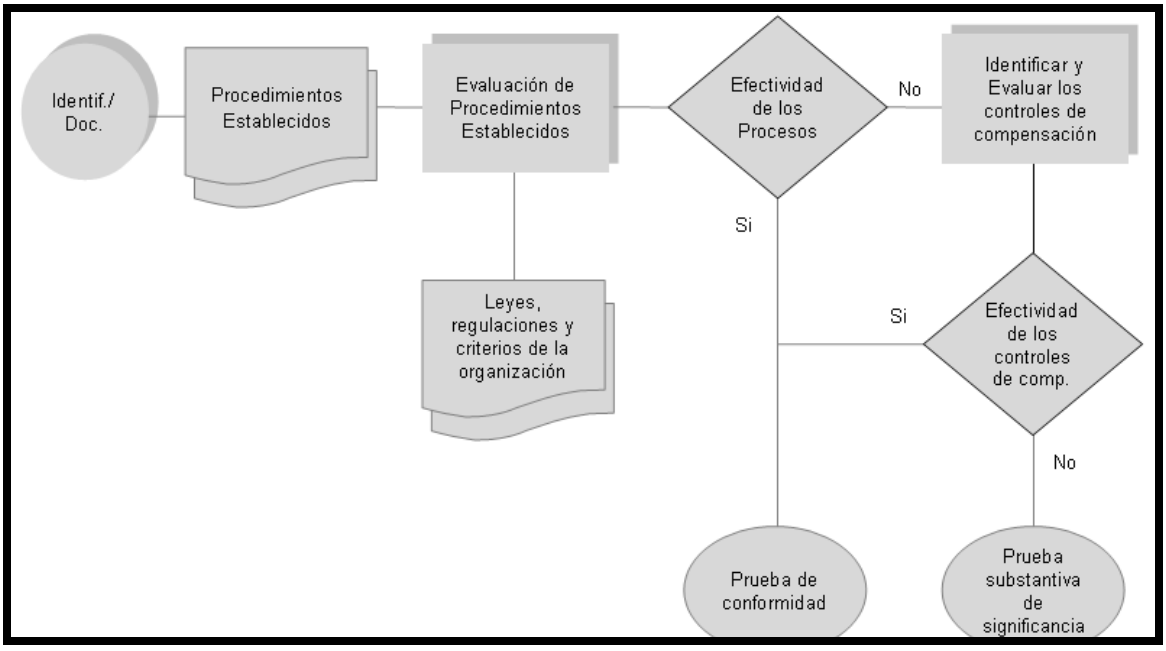
- Conocimiento de la identidad, ubicarla por medio de la técnica administrativa de **BENCHMARKING:** Situar a la organización, comparación con otras iguales del sector.
- Resultados deseados de este paso: El auditor debería identificar, documentar y verificar:

- ¿Quiénes desarrolla las tareas relacionada con TI?
- ¿Dónde se desarrolla la tarea?
- ¿Cuándo se ejecuta la tarea?
- ¿Cuáles son los inputs requeridos?
- ¿Cuáles son los resultados esperados?
- ¿Cuáles son los procedimientos establecidos para desarrollar la tarea?

Flujograma 3

PASO 2

EVALUACIÓN



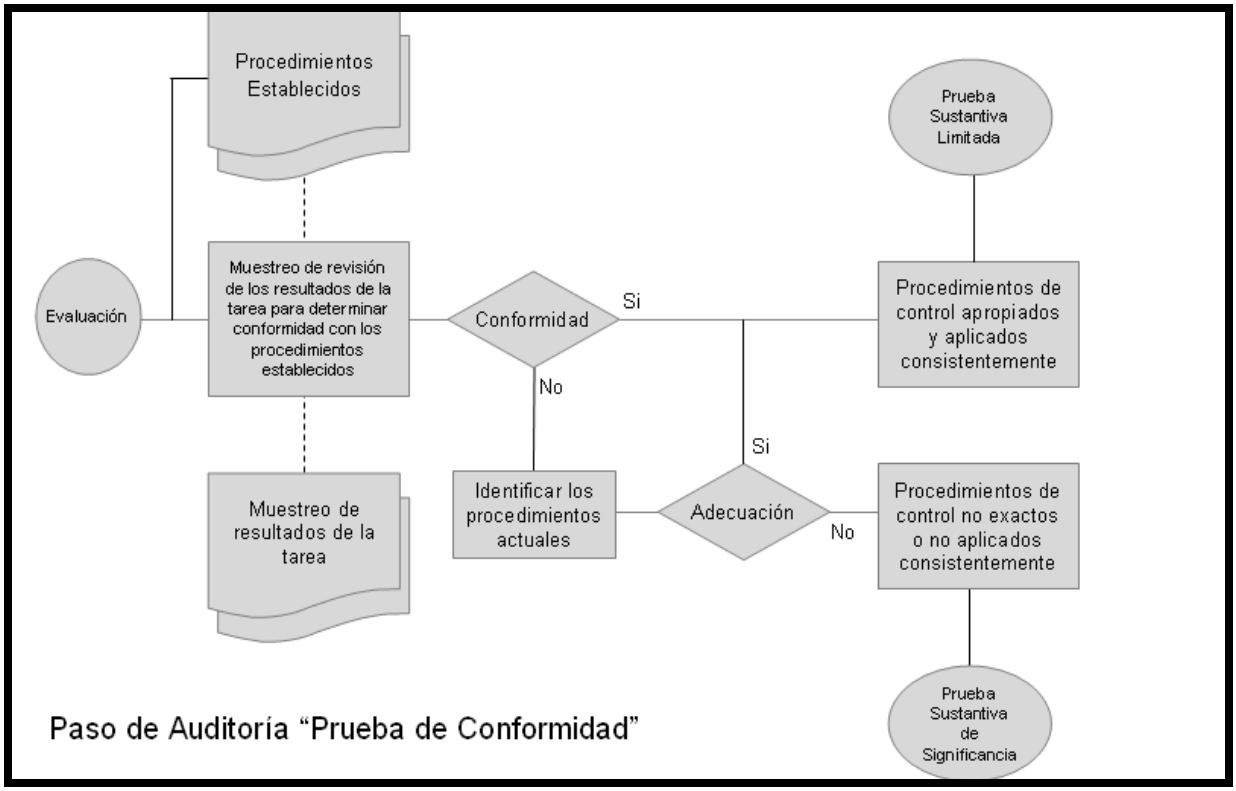
FUENTE: www.isaca.org

- El objetivo de este paso es evaluar los procedimientos establecidos y determinar si los mismos proveen una estructura de control efectivo. Los procedimientos deberían ser evaluados de acuerdo a criterios, prácticas estándares del sector al que la organización pertenece. Una estructura de control efectiva posee un costo adecuado y garantiza de forma razonable que la tarea se ejecuta de acuerdo a los objetivos de control. Resultados deseados de este paso:

- Evaluación de las leyes, regulaciones y criterios de la organización para su aplicabilidad en los procesos.
- Evaluación de los procedimientos establecidos para determinar si poseen un costo adecuado y proveen una garantía razonable de que la tarea es ejecutada y se logran los objetivos de control.
- Evaluar controles de compensación, usados para reforzar procedimientos débiles.

- Concluir si los procedimientos establecidos y los controles de compensación proveen una estructura de control efectiva.
- Identificar si es necesaria una prueba de conformidad.

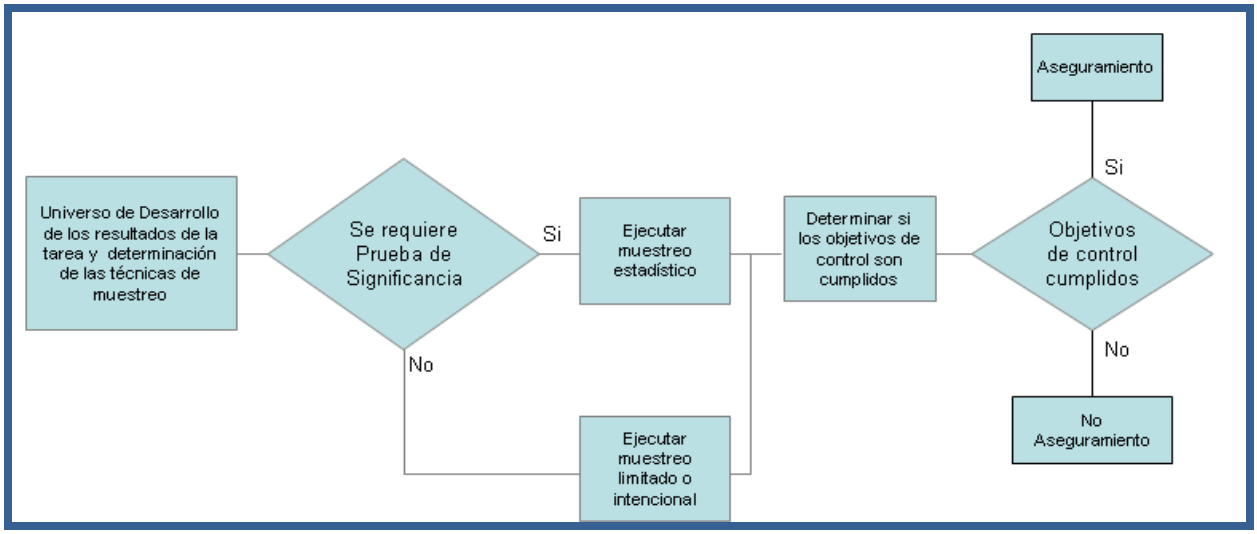
Flujograma 4
PASO 3
PRUEBA DE CONFORMIDAD



FUENTE: www.isaca.org

El objetivo de este paso es analizar la adherencia de la organización a los controles prescritos. Los procedimientos actuales y los controles de compensación deberían ser comparados con los procedimientos establecidos. Realizar las entrevistas y la revisión de documentos para determinar si los controles se aplican de manera consistente y apropiada. La prueba de conformidad solamente se ejecuta en relación a los procedimientos que se han categorizado como efectivos.

Flujograma 5
PASO 4
PRUEBA SUSTANTIVA



FUENTE: www.isaca.org

- El objetivo de este paso es conducir las pruebas de datos necesarios para proveer evidencias a la gerencia sobre la garantía o no de que los objetivos de negocio son logrados. Resultados deseados de este paso:

- No existen indicadores de control establecidos.
- Los indicadores de control han sido evaluados y no son satisfactorios.
- Las pruebas de conformidad indican que los indicadores de control no han sido apropiadamente ni consistentemente aplicados.

3.6 Modelos de madurez (confiabilidad)

Gráfica 8
Calificación de madurez
2007

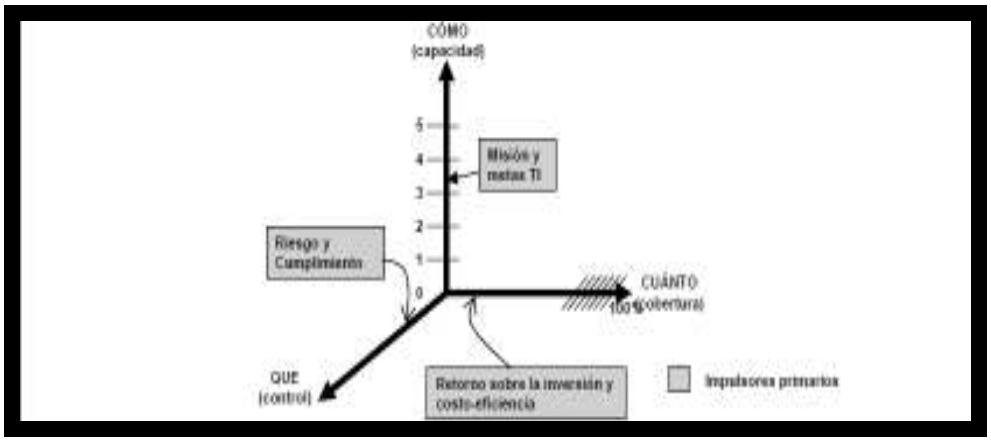
FUENTE: www.isaca.org

“El modelo de madurez es una forma de medir qué tan bien están desarrollados los procesos administrativos, estos es, qué tan capaces son en realidad. Qué tan bien desarrollado o capaces deberían ser, principalmente dependen de las metas TI y en las necesidades de la organización subyacentes a las cuales sirven de base. Cuánta de esa capacidad es realmente utilizada actualmente para retornar la inversión deseada en una organización. Por ejemplo, habrá procesos y sistemas críticos que requieren de una mayor administración de la seguridad que otros que son menos críticos. Por otro lado, el grado de sofisticación de los controles que se requiere aplicar en un proceso está más definido por el apetito de riesgo de una entidad y por los requerimientos aplicables.

Las escalas de modelo de madurez ayudarán a los profesionales a explicarle a la administración dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran. El nivel de madurez correcto estará influenciado por los objetivos de una entidad, por el ambiente operativo y por las prácticas de la organización. Específicamente, el nivel de madurez en la administración se basará en la dependencia que tenga la entidad en TI, en su sofisticación tecnológica y, lo más importante, en el valor de su información.”(4:19)

3.7 Apéndices

Gráfica 9
Las tres dimensiones de la madurez
2007



FUENTE: www.isaca.org

3.7.1 Métricas de control

Gráfica 10
Modelo genérico de madurez
2007

0 No Existente- Carencia completa de cualquier proceso reconocible. La organización no ha reconocido siquiera que existe un problema a resolver.

1 Inicial- Existe evidencia que la organización ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienen a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estádar, y se deja la responsabilidad al individuo. Existe un algo grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado-Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado-Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

FUENTE: www.isaca.org

3.7.2 Modelos de madurez: Información adicional

Tabla 7
Atributos de la madurez
2007

CONCIENCIA Y COMUNICACIÓN	POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS	HERRAMIENTAS Y AUTOMATIZACIÓN	HABILIDADES Y EXPERIENCIA	RESPONSABILIDAD Y RENDICIÓN DE CUENTAS	ESTABLECIMIENTO Y MEDICIÓN DE METAS
1 Surge el reconocimiento de la necesidad del proceso Existe comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y prácticas Los procesos y prácticas no están definidos.	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de herramientas	No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.	No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.	Las metas no están claras y no existen mediciones.
2 Existe conciencia de la necesidad de actuar. La gerencia comunica los problemas generales.	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir documentación y entendimiento informal de políticas y procedimientos.	Existen enfoque comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Pueden haberse adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.	Se identifican los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo. Con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.	Existen algunas metas; se establecen algunas mediciones financieras pero sólo las conoce la alta dirección. Hay monitoreo inconsistente en áreas aisladas.
3 Existe el entendimiento de la necesidad de actuar. La gerencia es más formal y estructurada en su comunicación.	Surge el uso de buenas prácticas. Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave.	Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso. Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado.	Se definen y documentan los requerimientos y habilidades para todas las áreas. Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.	Las responsabilidades y la rendición de cuentas sobre los procesos están definidas y se ha identificado a los dueños de los procesos del negocio o entidad. Es poco probable que el dueño del proceso tenga la autoridad plena.	Se establecen algunas mediciones y metas de efectividad, pero no se comunican, y existe una relación clara con las metas del negocio. Surgen los procesos de medición pero no se aplican de modo consistente. Se adoptan ideas nuevas.

FUENTE: www.isaca.org

CONCIENCIA Y COMUNICACIÓN	POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS	HERRAMIENTAS Y AUTOMATIZACIÓN	HABILIDADES Y EXPERIENCIA	RESPONSABILIDAD Y RENDICIÓN DE CUENTAS	ESTABLECIMIENTO Y MEDICIÓN DE METAS
4 Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.	El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento.	Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.	Los requeriemientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta que se comparta el conocimiento.	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar su responsabilidad. Existe una cultura de recompensas que activa la acción positiva.	La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balanced scorecard de TI en algunas áreas, con excepciones conocidas por la gerencia y se está estandarizando el ambiente.
5 Existe un entendimiento avanzado y a futuro de los requerimientos. Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas integradas de comunicación	Se aplican las mejores prácticas y estándares externos. La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejora extremo a extremo.	Se usan juegos de herramientas estandarizados a lo largo de la organización. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herramientas para dar soporte a la mejora de los procesos y automáticamente detectar excepciones a los controles	La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizaciones claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas. Compartir el conocimiento es una cultura empresarial, y se están desarrollando sistemas basados en el conocimiento. Expertos externo líderes industriales se emplean como guía.	Los dueños de los procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistente.	Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio por la aplicación global del balanced scorecard de TI. La dirección notas las excepciones de forma global y consistente y el análisis de causas raiz.

FUENTE: www.isaca.org

CAPÍTULO IV
ESTABLECIMIENTO DE UN SISTEMA DE CONTROL INTERNO BASADO EN COBIT, EN EL ÁREA DE INFORMÁTICA DE LA CLÍNICA DE ENFERMEDADES INFECCIOSAS, HOSPITAL ROOSEVELT
(CASO PRÁCTICO)

4.1 Antecedentes de la organización

4.1.1 Flujograma operativo de la Clínica de Enfermedades infecciosas Hospital Roosevelt

Presenta el recorrido de tres tipos de pacientes de la Clínica. Pacientes en verde realizan todo el recorrido en las mañanas. Pacientes en color naranja los atienden por la tarde sin extracción de sangre, sólo si el médico lo pide y los pacientes en blanco ingresan en la mañana sin extracción de sangre, sólo si el médico lo requiere.

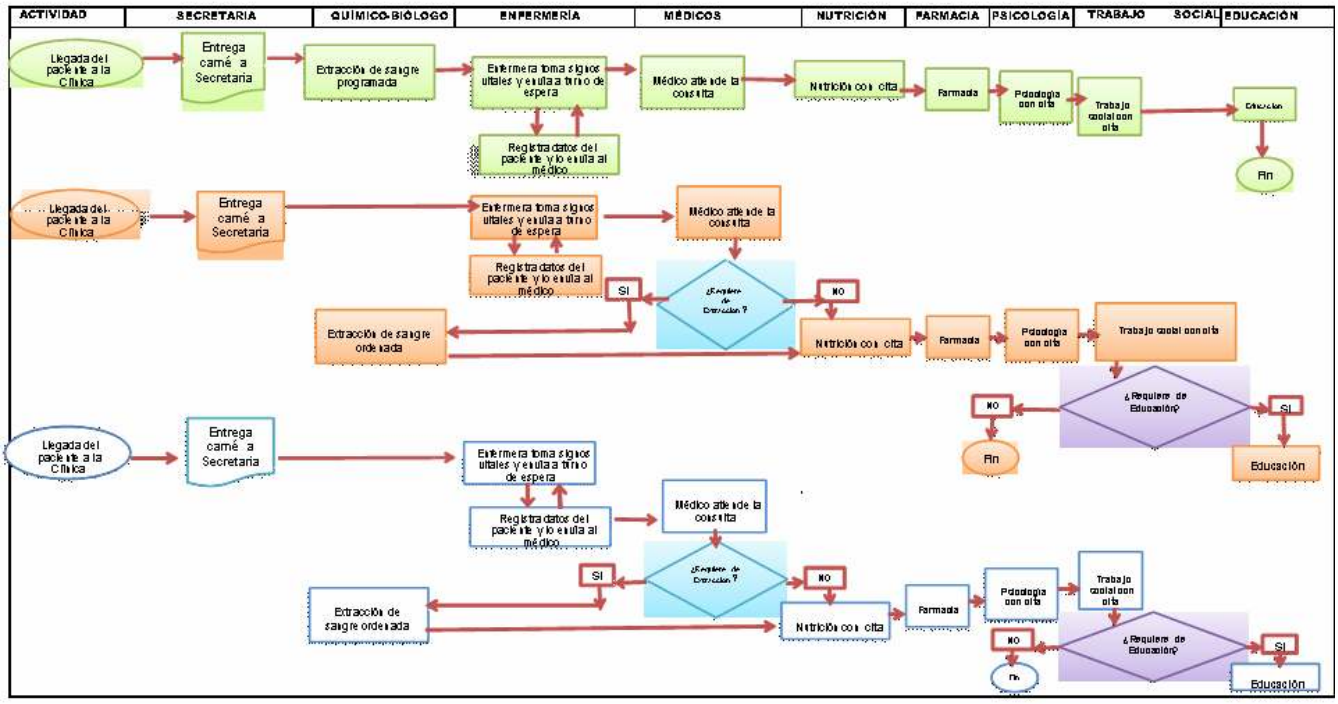
Las actividades se clasifican de la siguiente manera:

1. Llegada del paciente
2. Entrega de carné a secretaria
3. Pacientes en verde pasan a extracción
4. Pacientes en naranja y blanco pasan a signos vitales y esperan al médico
5. Pacientes en verde pasan con médico
6. Pacientes en naranja y blanco pasan a extracción si el médico lo requiere
7. Pacientes pasan a evaluación en el área de nutrición
8. Pacientes pasan a farmacia a recoger medicamentos
9. Pacientes asisten al área de psicología para evaluación
10. Pacientes pasan a trabajo social para recibir asistencia

11. Pacientes en verde pasan a educación, pacientes en naranja y blanco si lo necesitan.

Se atienden pacientes sin cita: hasta un número de 10 en la mañana y 10 en la tarde, éstos su recorrido no es completo, pueden ir al Médico sin cita, Nutrición sin cita, Psicología sin cita, Trabajo Social sin cita y siempre pasan a Farmacia. A continuación se presenta el flujograma con las distintas rutas, según color:

Flujograma 6
Flujograma operativo de la Clínica de Enfermedades infecciosas Hospital Roosevelt, Febrero 2010



Fuente: Elaboración propia, Clínica de Enfermedades Infecciosas, Hospital Roosevelt

Actualmente en la Clínica de enfermedades infecciosas no poseen un área de informática establecida como tal, no existen políticas de seguridad informática; por ejemplo claves de acceso a los sistemas, aunque poseen un inventario de 49 computadoras de escritorio y portátiles no hay un gobierno en TI. Están interesados en la creación de una arquitectura en TI; desarrollar un sistema de red, donde la mayoría de procesos del flujograma se automaticen, creación de la historia clínica electrónica, para médicos, psicólogos, nutrición y

es aquí donde el modelo COBIT, cubre muy bien sus expectativas, para el área de informática como para la entidad; que ayude a desarrollar mejor las actividades en la clínica en beneficio de los pacientes que son tratados en la misma.

Además del flujograma operativo se cita al recurso humano de la Clínica, que se desea entre al nuevo sistema en red basado en COBIT.

- Jefe de la Clínica
- Residentes post-grado de Enfermedades infecciosas
- Médico Pediatra
- Médico encargado de Tuberculosis
- Médico Epidemiólogo
- Enfermería Consulta Externa
- Personal enfermería pediatría
- Personal de Consejería Área de maternidad
- Área de Archivo *
- Digitadoras
- Área de nutrición
- Área de trabajo social
- Área de psicología
- Área de laboratorio
- Área de farmacia Almacén

POSEE SISTEMA DE INVENTARIO

- Personal de Microbiología

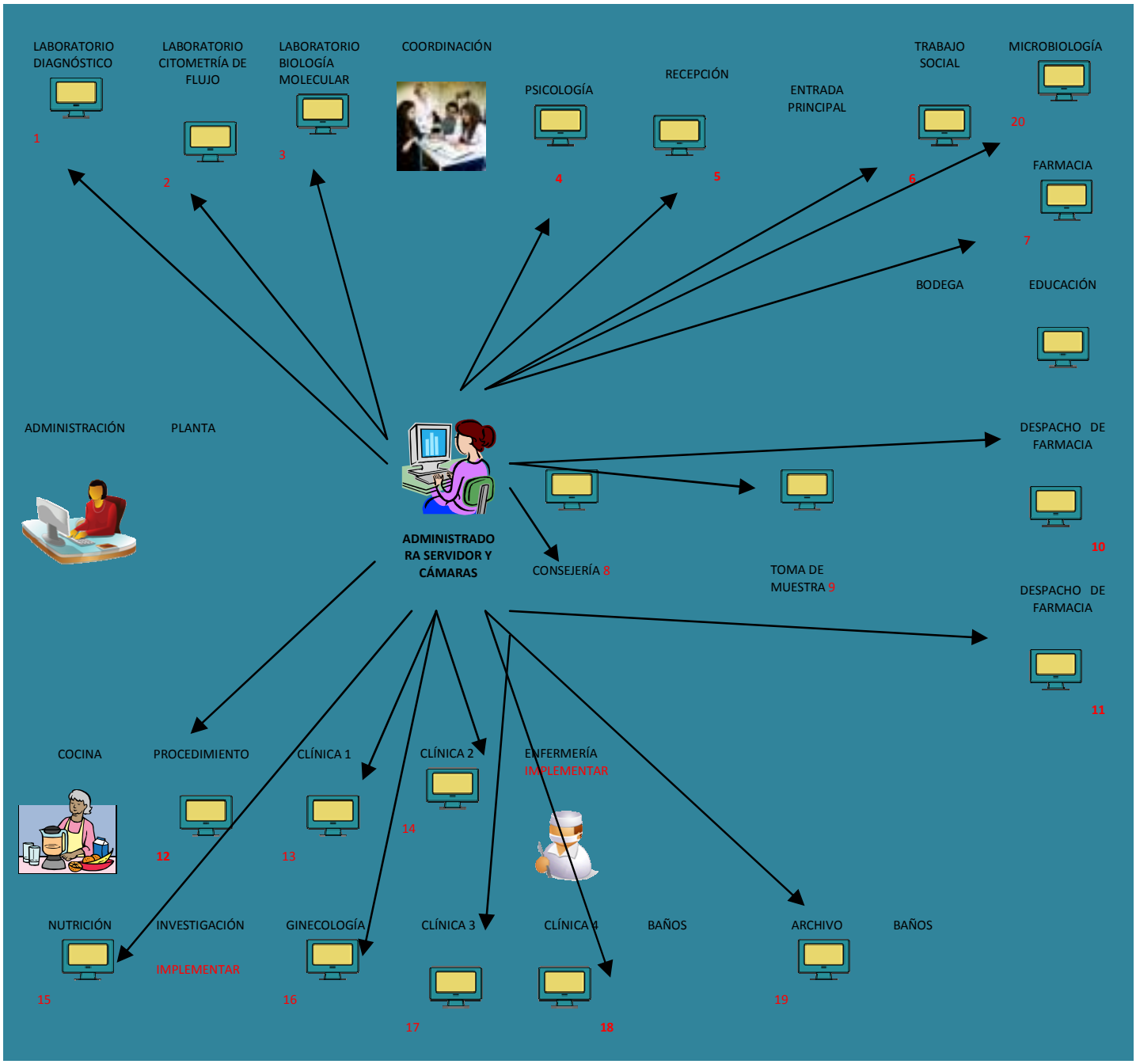
Entrar en arquitectura Red-COBIT

* FACTOR PRIMARIO porque la documentación que se encuentra aquí, se digitalizará como respaldo a la historia clínica electrónica en formato PDF.

4.2 Planeación y Organización de la arquitectura de la información

4.2.1 Mapa de la unidad de análisis, modelo de conexión de la red

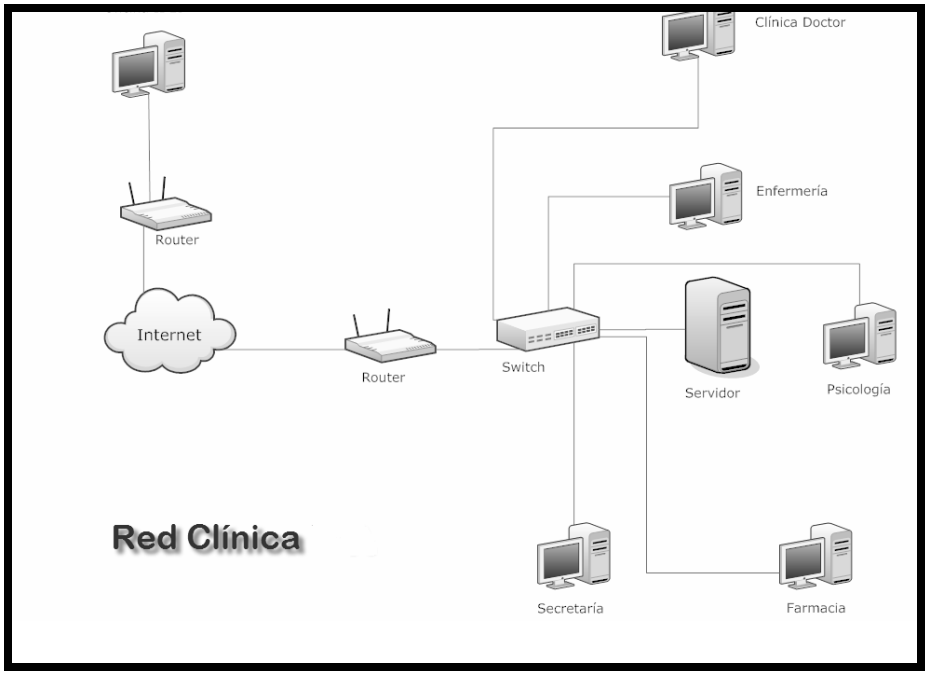
Gráfica 11
Clínica Enfermedades Infecciosas –Red- Administrador y Clientes/usuarios
Febrero 2010



ELABORACIÓN PROPIA, FEBRERO 2010

A continuación se dan imágenes de la infraestructura de aplicación a la medida, de conexiones y cableado de acuerdo al modelo para entrar en red. Para llegar a estas conclusiones en esta arquitectura tecnológica el auditor se auxilia de la Norma Internacional de Auditoría, NIA 620 “Uso del Trabajo de un Experto”, que en este caso fueron varios expertos. Se tomaron en cuenta las recomendaciones de los creadores del programa INTEGRA: el programador Joshua Letona Diemecke y Doctor Juan Carlos Romero. Se visitaron las instalaciones de la Clínica Isaac Cohen Alcahé, TB, Quetzaltenango donde está instalada la aplicación y funciona bajo este modelo de conexión, (***estándar de comparación,*** técnica de ***benchmarking)*****.** Además se consultó con dos proveedores calificados en el área de tecnología como MÉTRICA y SERVICIOS INFORMÁTICOS GLOBALES, éstos últimos dedicados a servicios de Telemedicina.

Figura 8
Diseño de conexión en red
Febrero 2010



ELABORACIÓN PROPIA-MODELOS DE CONEXIÓN

4.2.2 Módulos de gestión (INTEGRA)

Es una aplicación a la medida en un ambiente cliente-servidor que consta de ocho módulos básicos:

1. Gestión y reporte médicos
2. Gestión y reportes de farmacia
3. Gestión y reportes de nutrición
4. Gestión y reportes de Psicología
5. Estudio Socio Económico
6. Gestión y reportes de tránsito de muestras de laboratorio
7. Supervisión de Administradores
8. Control de citas y asistencia de secretaria

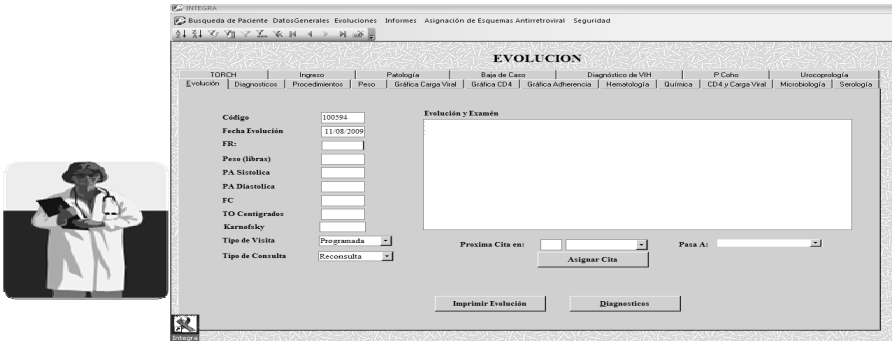
Cada módulo tiene acceso restringido y sólo pueden ingresar a un rubro en particular las personas para eso designadas (**segregación de funciones**), de esta manera se protege la información con fines médico legales y con fines de auditoría. En el manejo interdisciplinario de un paciente diversos integrantes de un mismo equipo necesitan acceso a la información que otros grupos generan y de hecho es factible en esta aplicación, pero no puede ser modificada dicha información presentada como "consulta" para otras personas o grupos. Luego de ingresar un registro no será posible modificarlo por los usuarios no administradores. Todo error en el ingreso de datos necesita ser reportado y evaluado por el/los administradores para considerar su corrección.

La aplicación funciona en red interna en que múltiples computadoras alimentan la base contenida en un servidor central, cuyo manejo y mantenimiento está a cargo de las personas designadas como administradores. Los archivos de respaldo se ha planificado para realizarse de forma diaria y en discos que se deberán archivar de forma cronológica y con colaboración estrecha entre el administrador y la oficina central de administración de cada área de gestión.

En condiciones de funcionamiento normal de una clínica multidisciplinaria el paciente deberá realizar el flujo por todas las dependencias que requiera únicamente con su carné de identificación en la mano. Todas las clínicas y dependencias tendrán acceso al servidor central y a un programa que permita identificar y extraer el expediente del paciente correspondiente ya sea por su código, nombre o apellido.

- **GESTIÓN Y REPORTES MÉDICOS** MÓDULO 1 (MANUAL)

Figura 9
Historia clínica electrónica



Captura de pantalla, historia clínica electrónica (INTEGRA)

Captura de pantalla, Datos Generales de Pacientes (INTEGRA)

Beneficios:

- ✓ Registro con letra perfectamente legible
- ✓ Aumento de velocidad en el registro del mismo
- ✓ Se previene la pérdida de hojas sueltas dentro del expediente

Los diagnósticos se ingresan una sola vez, en caso de diagnóstico crónico que se trabajará en el seguimiento de múltiples visitas, no necesita ser reescrito en cada consulta.

- **GESTIÓN Y REPORTES DE FARMACIA** MÓDULO 2 (MANUAL)

- **Ingreso de medicamentos al Inventario**

Los químicos farmacéuticos y técnicos tendrán acceso a un módulo en que podrán ingresar medicamentos al inventario de la clínica, **siendo esa la única instancia en que tendrán que escribir el nombre del medicamento**. Durante el ingreso de medicamentos al inventario pueden agregar al lote, fecha de vencimiento, factura y proyecto o fuente a donde pertenecen.

Figura 10
Hoja electrónica de registro de medicamentos

Captura de pantalla, Inventario General por movimiento (INTEGRA)

- **Despacho de medicamentos**

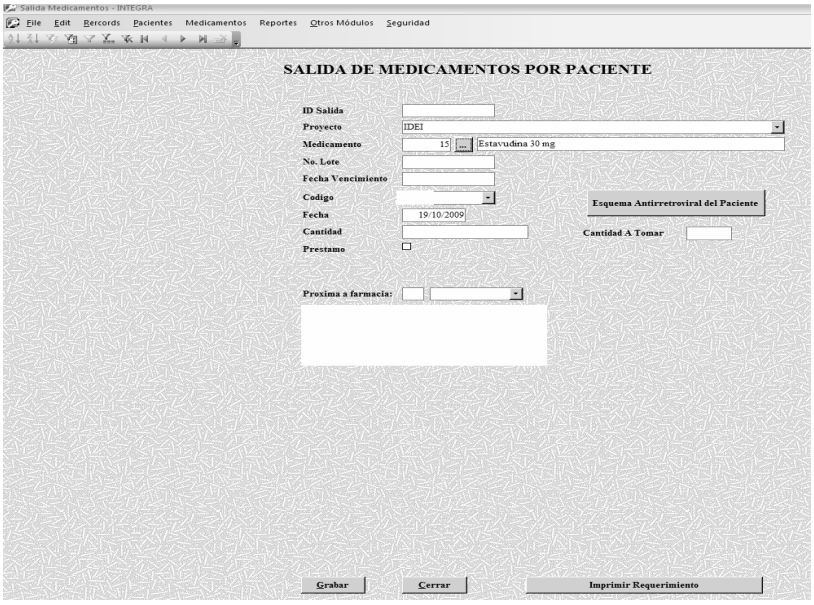
Despacho individual el usuario tendrá acceso al buscador de pacientes y elegido el paciente pasará a una pantalla de resumen de medicamentos activos del paciente con

dosis y vías de administración, al oprimir un botón localizado a la par de cada medicamento podrá realizar un despacho individual. Inmediatamente después se abre una pantalla que les permite elegir de qué proyecto, lote y caducidad será egresado el medicamento. Este despacho no requiere reescritura lo que disminuye el riesgo de errores de transcripción, se despachará únicamente los medicamentos activos para cada paciente y no permitirá el despacho duplicado del mismo medicamento para el mismo paciente durante el mismo día, para evitar la duplicidad de egresos accidentales.

Figura 11
Hoja electrónica de búsqueda de paciente

Captura de pantalla, Búsqueda Pacientes (INTEGRA)

Figura 12
Hoja electrónica del registro de salida de medicamento por paciente



Captura de pantalla, Salida de medicamentos por paciente (INTEGRA)

- **Despacho No individual**

  - ✓ El programa considera la salida de medicamentos a otros proyectos o clínica satélite a los cuales se les podía despachar en cantidades grandes.

- **Manejo de Esquemas antirretrovirales**

  - ✓ El farmacéutico asignará el código de esquemas antirretroviral correspondiente a la combinación que el médico haya prescrito y dará seguimiento a todo cambio indicado ya sea por razones médicas, disponibilidad o fallecimiento.

- **Adherencia**

  - ✓ En la pantalla de despacho de medicamentos el farmacéutico ingresará siempre en una variable la cantidad de pastillas que debería traer de regreso el paciente en la próxima cita, en función de la cantidad entregada y dosis.

  - ✓ En las citas de seguimiento se ingresará cuántas pastillas trajo de regreso y el programa automáticamente calculará el porcentaje de adherencia el cual también estará disponible de forma gráfica para el médico y psicólogo.

Figura 13
Hoja electrónica de selección de medicamentos

Captura de pantalla, Selección de medicamentos (INTEGRA)

- El farmacéutico y técnico de farmacia tendrán acceso a las citas con otras dependencias para el paciente individual y también la nómina general de citas para planificar de forma racional la próxima evaluación del paciente durante el despacho.

- **Reportes**

  Existe una pantalla de reportes de farmacia que necesita se ingrese un rango de fechas para realizar los reportes, de tal forma que el usuario puede escoger libremente si el informe es de un día, una semana, mes o trimestre de trabajo.

  - ✓ Inventario General de medicamentos independiente de su origen o caducidad
  - ✓ Inventario de medicamentos por proyecto
  - ✓ Inventario de medicamentos por caducidad
  - ✓ Reporte detallado movimientos en el inventario por fecha
  - ✓ Reporte de adherencia numérico y gráfico
  - ✓ Reporte de tratamientos antirretrovirales donde se detalla las razones si es que se conoce
  - ✓ Reporte de préstamos entre proyectos que detalla por medicamentos y fechas, a quien le adeudan los diferentes proyectos.
  - ✓ Reporte de inventario de donaciones de medicamentos.

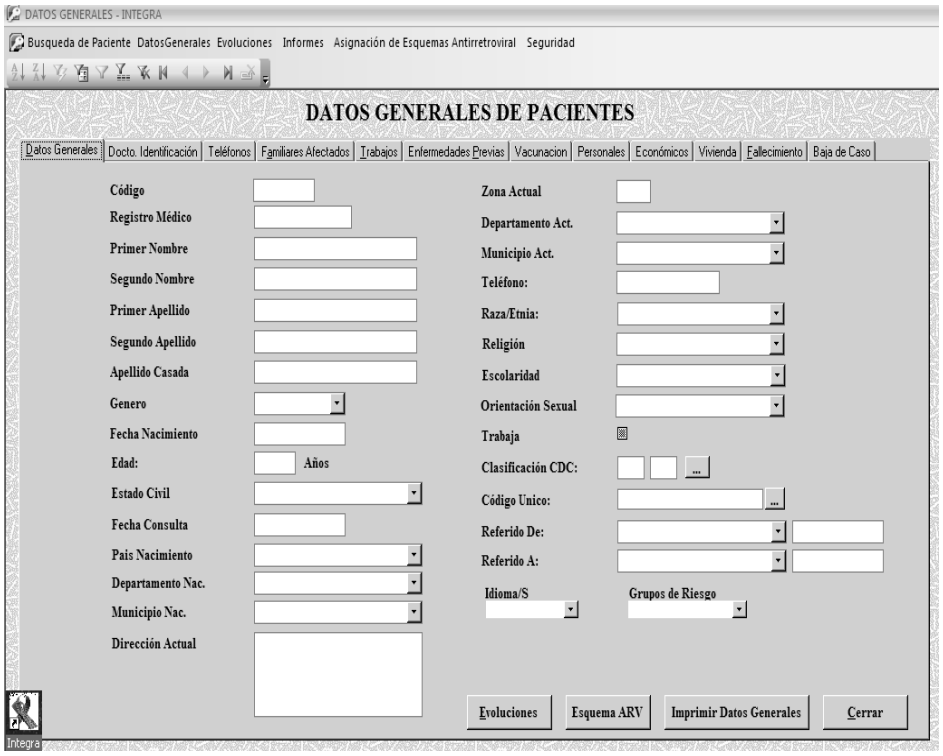
Este módulo reviste gran importancia por razones del monto del presupuesto que se maneja en esta área, aproximadamente traduciéndolo en quetzales unos Q 15,000,000.00 a Q 20,000,000.00 en medicamentos por año.

- **GESTIÓN Y REPORTES DE NUTRICIÓN** MÓDULO 3 (MANUAL)

  - Los nutricionistas tendrán acceso al buscador de pacientes y luego de elegir el paciente indicado pasarán a una pantalla de múltiples pestañas que les permitirá realizar registros de hábitos nutricionales,

mediciones antropométricas, composición corporal, diagnósticos antropométricos y nutricionales y por último intervenciones dietética. Todos los registros están disponibles en retrospectiva y se presentará además gráficas de la progresión del peso y composición corporal.

Figura 14
Hoja electrónica de búsqueda del paciente y datos generales



Captura de pantalla, Datos Generales de Pacientes (INTEGRA)

Figura 15
Historia clínica electrónica de nutrición

Captura de pantalla, Historia Clínica de Nutrición (INTEGRA)

- ✓ El nutricionista tendrá acceso a las citas con otras dependencias para el paciente individual y también la nómina general de citas para planificar de forma racional la próxima evaluación del paciente en consulta.

- ✓ Los reportes de nutrición requieren del ingreso de un rango de fechas para el análisis y son los siguientes:

    - Pacientes evaluados distribuidos por sexo y edad
    - Distribución de los pacientes por sexo y diagnóstico nutricional
    - Distribución de los pacientes por sexo y diagnóstico antropométrico
    - Distribución de los pacientes según intervención o tratamiento nutricional.

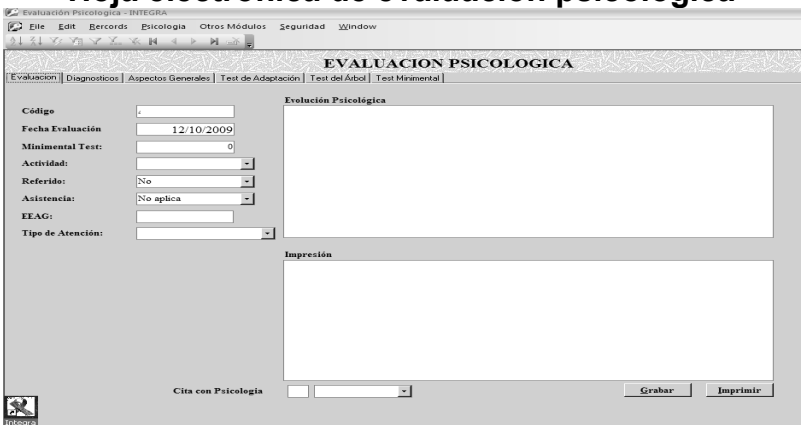
- ➢ **GESTIÓN Y REPORTES DE PSICOLOGÍA** MÓDULO 4 (MANUAL)

Expediente electrónico puede registrar los eventos subjetivos en texto libre, pero tiene variables en que registrará los diagnósticos, puntuación de las escalas de evaluación del desempeño cognitivo, actividades individuales y/o grupales, referencia a otros proyectos y el cumplimiento en asistir a dichas referencias. Al igual que en el

expediente médico: los diagnósticos se ingresan una sola vez y se encontrará activo en todas las subsecuentes visitas a menos que se omita o modifique. También existe un botón que permite tener acceso a todos los diagnósticos activos o inactivos del paciente.

- El psicólogo tendrá acceso a leer las evoluciones médicas más no acceso a modificarlas.
- El psicólogo tendrá acceso a las citas con otras dependencias para paciente individual y también la nómina general de citas para planificar de forma racional la próxima evaluación del paciente en consulta.
- Reportes: requieren del ingreso de un rango de fechas
    - Pacientes evaluados distribuidos por sexo
    - Reporte de pacientes distribuidos por diagnóstico
    - Reporte de pacientes distribuidos por actividades y referencias
- Reporte de adherencia a otros centros donde fue referido cada paciente.

Figura 16
Hoja electrónica de evaluación psicológica



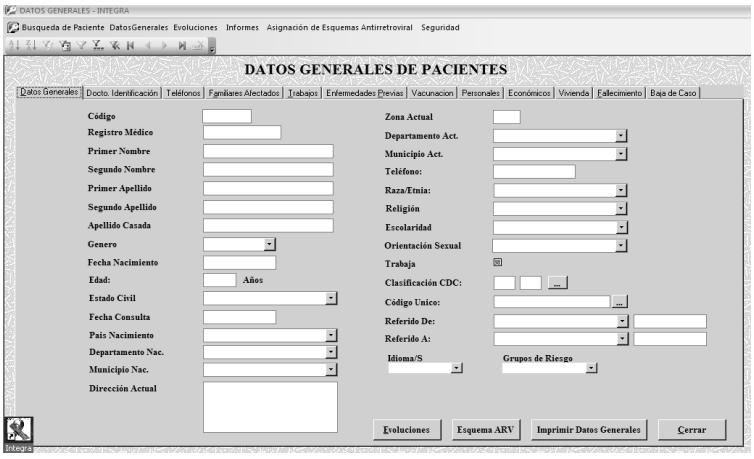
Captura de pantalla, Historia Clínica de Psicología (INTEGRA)

- **GESTIÓN DE TRABAJO SOCIAL (ESTUDIO SOCIO ECONÓMICO)** MÓDULO 5 (MANUAL)

  El/la trabajador social podrá ingresar el estudio socioeconómico basal del paciente y este estará disponible a manera de consulta no modificable para el resto de dependencias, la boleta del ingreso de dicho estudio social es completamente electrónica y estrechamente ligada a los datos generales del paciente los cuales se llenan cuando el paciente asiste a la clínica por vez primera.

El/la trabajador social podrá ingresar el estudio socioeconómico basal del paciente y este estará disponible a manera de consulta no modificable para el resto de dependencias, la boleta del ingreso de dicho estudio social es completamente electrónica y estrechamente ligada a los datos generales del paciente los cuales se llenan cuando el paciente asiste a la clínica por vez primera.

Figura 17
Hoja electrónica de datos generales del paciente



Captura de pantalla, Datos Generales de Pacientes (INTEGRA)

Figura 18
Hoja electrónica de evaluación del Área de Trabajo Social

Captura de pantalla, Ficha de Evaluación, Trabajo Social (INTEGRA)

- Gestión y reportes de tránsito de Muestras de Laboratorio MÓDULO 6 (MANUAL)

- El área donde se centra la toma de muestras y recepción de resultados también tendrá un módulo con buscador de paciente que permite el registro de la toma de cada diferente prueba con sólo oprimir un botón que le asigna la fecha de envío y deja marcado como pendiente el informe hasta el momento en que ingrese el resultado correspondiente.

- Todos los resultados ingresados a la base de datos aparecerán automáticamente en las pestañas correspondientes para los médicos y nutricionistas a manera de datos a consultar no modificable.

- Reportes (previo rango de fechas a elegirse libremente)

  - ✓ Reporte de pruebas de laboratorio realizadas
  - ✓ Reporte de pruebas entregada
  - ✓ Reporte de informes pendientes de ingresar al sistema
  - ✓ Listado de pruebas pendientes de ingresar al sistema por distribuidas por fecha, código y nombre de pacientes.

Figura 19
Hoja electrónica de búsqueda paciente y registro de exámenes de Laboratorio

Captura de pantalla, Búsqueda Pacientes (INTEGRA)

➢ Supervisión de Administradores MÓDULO 7 (MANUAL) Comienza con 1 Administrador y 19 Clientes

- El administrador tendrá acceso a todas las instancias del programa con la finalidad de evaluar la veracidad de los datos ingresados, detectar errores en el ingreso de los mismos y depuración oportuna de los mismos. Requiere conocimientos básicos en manejo de paquetes Excel y Access.
- Tendrán acceso a las tablas matriz para modificar sus contenidos según las necesidades de la Clínica.

- Cada vez que una persona ingresa con su usuario y palabra clave todo dato que registre dejará un rastro electrónico de dicho ingreso con fecha y hora de dicho registro con fines de auditoría. El administrador realizará gestión de nuevos reportes o cambios a realizarse a la base de datos con anuencia y apoyo de desarrolladores durante el período de validación e incorporación oficial del programa en todas las dependencias de la clínica.

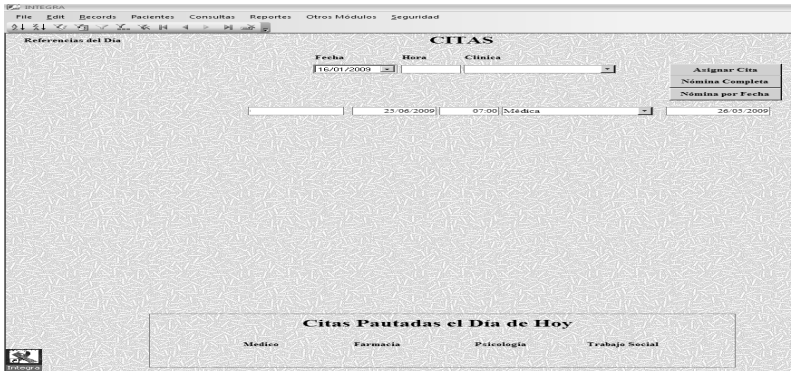

Llegada del paciente Total grupos 248

Actualmente pueden atender 50 pacientes con cita, sin cita 10 en la mañana; se toman como excepciones, se atienden hasta 3 en la tarde sin cita.


Gestión Secretaria MÓDULO 8 ENTREGA CARNÉ

MEDIR TIEMPOS: La persona se registra aproximadamente en 2 o 3 minutos

Figura 20
Hoja electrónica de control de citas



Captura de pantalla, Control de Citas (INTEGRA)

Control de citas y Asistencia: Tendrá acceso a las nóminas de citas de todas las dependencias de la clínica, se asegurará que todas juntas no sobrepasen el mínimo aceptado total para atención general para no sobrecargar

determinadas fechas. Llevará el Control de personas esperadas para cada día y podrá crear una impresión de todas las personas que asistieron a la clínica el mismo día disgregadas por dependencia. Color verde mañana y extracción sangre, anaranjado tarde sin extracción y sin color mañana, sin extracción.

4.2.3 Requerimientos de Hardware y Software, Topología de red

SERVIDOR HARDWARE

Tabla 8
Requerimientos de hardware del servidor
Febrero 2010

	Mínimo	Recomendado
Procesador	600 MHz Pentium III	1 Ghz o superior
Memoria	512 MB	1 GB o mas
Disco Duro	20 GB	2 discos duros de 80 GB (o más) con RAID 1.
Drive	CD-ROM ó DVD-ROM	
Video	Adaptador de video Súper VGA (1,024x768) o mayor resolución	
Tarjeta de Red	Ethernet 10 mbps	Ethernet 100/1000 mbps
Fuente de poder	1 fuente de poder	2 fuentes de poder para redundancia
Otros dispositivos	Mouse, teclado, UPS	2 UPS, 1 para cada fuente de poder.

Fuente: Elaboración propia, basado en las necesidades para operar INTEGRA

Actualmente se cuenta con un servidor HP PROLIANT ML 350 G5 con procesador Intel Xeon QUAD CORE E5310 1.6 Ghz., 8 MB Cache, memoria ram de 1 GB, 2 discos duros de 72 GB con quemadora de DVD, controlador de red (controlador integrado HP NC3773i. Multifunción Gigabit 10/100/1000 WOL).

SOFTWARE

Tabla 9
Requerimientos de software del servidor
Febrero 2010

Sistema Operativo	Microsoft Windows 2000 Server con Service Pack 4 o superior; Windows Server 2003 Standard Edition con Service Pack 1 o superior
RDBMS	Microsoft SQL Server Desktop Edition 7.0 o superior con el ultimo Service Pack (para un máximo de 5 usuarios); Microsoft SQL Server Standard Edition 7.0 o superior con el ultimo Service Pack (el límite es el número de licencias adquiridas)
Antivirus	Se recomienda algún antivirus que sea compatible con los sistemas operativos arriba mencionados.

Fuente: Elaboración propia, basado en las necesidades para operar INTEGRA

❖ CLIENTES HARDWARE

Tabla 10
Requerimientos de hardware para los Clientes/usuarios
Febrero 2010

	Mínimo	Recomendado
Procesador	600 MHz Pentium III	1 Ghz o superior
Memoria	256 MB	512 GB o más
Disco Duro	10 GB	20 GB o más
Drive	CD-ROM ó DVD-ROM	
Video	Adaptador de video Súper VGA (1,024x768) o mayor resolución	
Otros dispositivos	Mouse, teclado	

Fuente: Elaboración propia, basado en las necesidades para operar INTEGRA

SOFTWARE

Tabla 11
Requerimientos de software para los Clientes/usuarios
Febrero 2010

Sistema Operativo	Microsoft Windows 2000 Professional con Service Pack 4 o superior; Windows XP Professional con Service Pack 2 o superior
Office	Microsoft Office 2003 Professional
Antivirus	Se recomienda algún antivirus que sea compatible con los sistemas operativos arriba mencionados.

Fuente: Elaboración propia, basado en las necesidades para operar INTEGRA

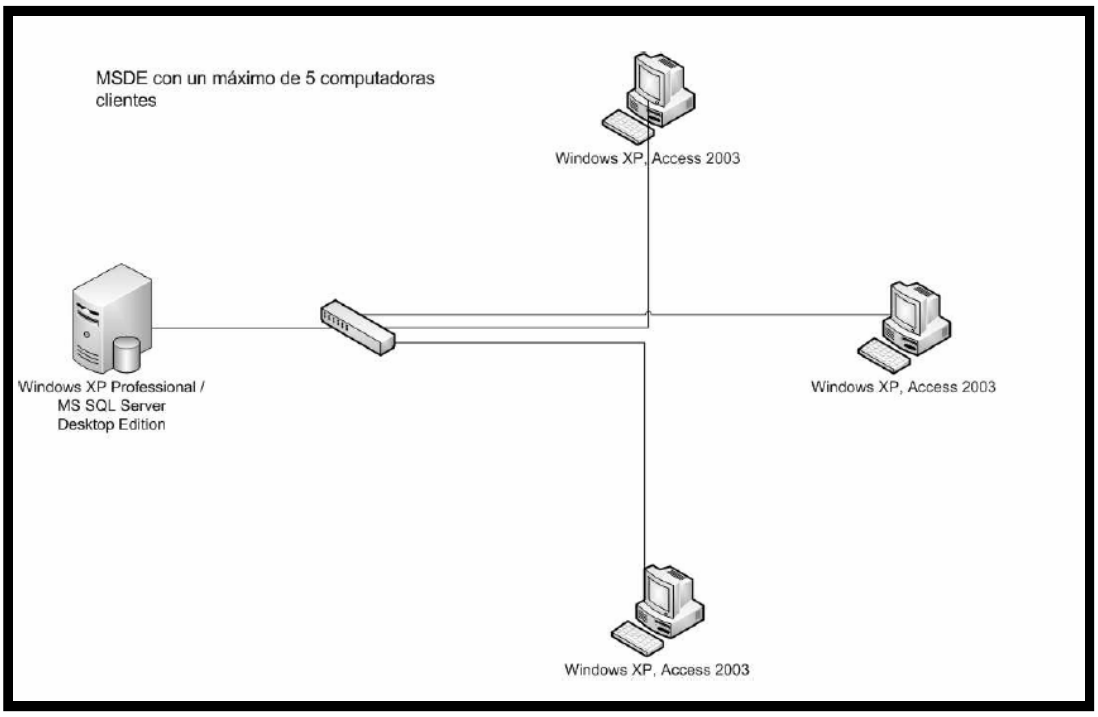
❖ TOPOLOGÍA DE RED

Figura 21

Transferencia de información entre Clientes/usuarios y Administrador

Fuente: INTEGRA

Figura 22
Funcionamiento de Conectividad en base a Microsoft SQL (Lenguaje estándar de comunicación en bases de datos)



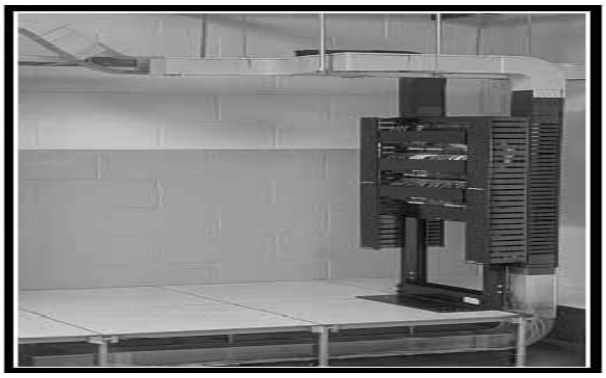
MSDE = Microsoft SQL Server 2000 Desktop Engine. CONECTIVIDAD

❖ CABLEADO

"El cableado se refiere al medio físico a través del cual se interconectan dispositivos de tecnologías de información para formar una red, y el concepto estructurado, se define en los siguientes puntos:

- **Solución Segura**: El cableado se encuentra instalado de tal manera que los usuarios del mismo, tienen acceso a lo que deben de tener y el resto del cableado se encuentra perfectamente protegido.
- **Solución Longeva**: Cuando se instala un cableado estructurado se convierte en parte del edificio, así como lo es la instalación eléctrica, por tanto este tiene que ser igual de funcional que los demás servicios del edificio.

Figura 23
Diseño de un cableado estructurado



Fuente: http://www.guatewireless.org/cableado-de-redes-configuracion-de-colores-del-cable-estructurado-categoria-5e/

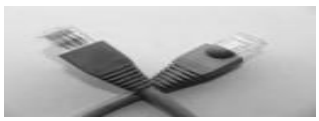
La gran mayoría de los cableados estructurados pueden dar servicio por un período de hasta 20 años, no importando los avances tecnológicos en las computadoras.

- **Modularidad**: Capacidad de integrar varias tecnologías sobre el mismo cableado voz, datos, video.
- **Fácil Administración**: El cableado estructurado se divide en partes manejables que permiten hacerlo confiable y perfectamente administrable, pudiendo así detectar fallas y repararlas fácilmente.

El cableado estructurado en categoría 6 es el tipo de cableado más solicitado hoy en día. El cable UTP (Unshielded Twisted Pair) posee 4 pares bien trenzados entre si. Para que todos los cables funcionen en cualquier red, se sigue un estándar a la hora de hacer las conexiones. Los dos extremos del cable llevan un conector RJ45 con los colores en el orden indicado en la figura.

Figura 24

Interfaz RJ45



Fuente: http://www.guatewireless.org/cableado-de-redes-configuracion-de-colores-del-cable-estructurado-categoria-5e/

El RJ45 es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglíos de **Registered Jack** que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho *pines* o conexiones eléctricas. Es utilizada comúnmente con estándares como **EIA/TIA-568B**, que define la disposición de los pines o wiring pinout.

- **Partes que integran un cableado estructurado**

- **Área de trabajo**: Su nombre lo dice todo, Es el lugar donde se encuentra el personal trabajando con las computadoras, impresoras, etc. En este lugar se instalan los servicios (*nodos de datos, telefonía, energía eléctrica, etc.*).
- **Closet de comunicaciones**: Es el punto donde se concentran todas las conexiones que se necesitan en el área de trabajo.
- **Cableado Horizontal**: Es aquel que viaja desde el área de trabajo hasta el closet de comunicaciones.
- **Closet de Equipo**: En este cuarto se concentran los servidores de la red, el conmutador telefónico, etc. Este puede ser el mismo espacio físico que el del closet de comunicaciones (Racks) y de igual forma debe ser de acceso restringido.
- **Cableado Vertebral (Back Bone)**: Es el medio físico que une 2 redes entre sí. La acometida puede no ser necesaria si no se requiere de servicios que viene de la calle para ser incorporados a la red, o esta puede ser tan pequeña como un simple hoyo en la pared para que pase una línea telefónica. El Back Bone no es necesario a menos de que se deseen unir closets de comunicaciones (Racks).

El cableado horizontal (los puntos 1 y 2) forzosamente tienen que estar considerados en cualquier cableado estructurado por más pequeño que sea. Estos puntos son los mínimos necesarios. El clóset de equipo puede ser tan grande o pequeño como se requiera, puede ser desde un pequeño servidor hasta varios servidores unidos entre sí.

Los puntos 4 y 5, La Acometida y El Cableado Vertebral dependen del tamaño de cableado.

- **Consejos a la hora de instalar y tirar el cable**

Lo primero es hacer un buen cable, utilizar cable categoría 6 STP (apantallado) para evitar ruidos e interferencias, y utilizar la herramienta adecuada. Esto sería lo perfecto para que la red rinda al máximo. Son las mejores condiciones posibles. Después se debe tener en cuenta 2 cosas: La distancia y el ruido eléctrico.

- **Distancia** – Hay que procurar no doblar el cable en exceso, y nunca a menos de 45 grados, no enrosque el cable sobrante ya que habrá pérdidas de señal, al debilitarse por la distancia. En el mejor de los casos, será más lenta la red, en el peor, no habrá comunicación… la distancia del cable no debe de sobrepasar los **90 metros**.
- **Ruido Eléctrico** – Ruido es todo aquello que interfiere en la señal impidiendo o dificultando la comunicación. Todo aparato eléctrico o cable eléctrico cercano al cable de red." (15:1-4)

4.3 Establecimiento de principios y objetivos de la unidad de análisis

El principal principio para la Clínica es: **"para proveer información, la entidad necesita cumplir objetivos".** Los recursos TI necesitan ser manejados por un conjunto de procesos agrupados y bien definidos. El propósito de realizar esta revisión es estudiar la adecuada pero absoluta protección de la información, en este caso todas las bases de datos que se manejan por separado en la clínica, y encontrar una aplicación a la medida que la procese en forma automatizada, pero con objetivos de control de alto nivel, y la respuesta es INTEGRA.

El concepto de confianza razonable sobre este proyecto es que el costo de un sistema de control interno **no debe exceder de los beneficios derivados** y también se

reconoce que la evaluación de estos factores requiere de una adecuada apreciación y buen juicio de la alta administración.

- **HIPÓTESIS**

Desde el punto de vista de las Normas Internacionales de Auditoría bajo el enfoque de la auditoría externa, los procedimientos que el Contador Público y Auditor deberá tomar en cuenta para establecer un sistema de control interno basado en COBIT, que permita concientizar a la alta dirección y trabajadores, superar la resistencia al cambio de la cultura organizacional y cumplir con las exigencias legales, reglamentarias y conflictos en una Clínica de Enfermedades Infecciosas, área de informática del Hospital Roosevelt son:

- ✓ **Planeación y Organización** de la arquitectura de la información
- ✓ **Adquisición e implementación** de infraestructura, programas, aplicaciones y equipo de cómputo a la medida de la entidad
- ✓ **Entrega y Soporte** a los usuarios de los programas cumpliendo con los criterios de la información COBIT
- ✓ **Monitoreo y Evaluación** de que los tres procesos anteriores se cumplan y lleguen a alcanzar una optimización en su nivel de madurez.

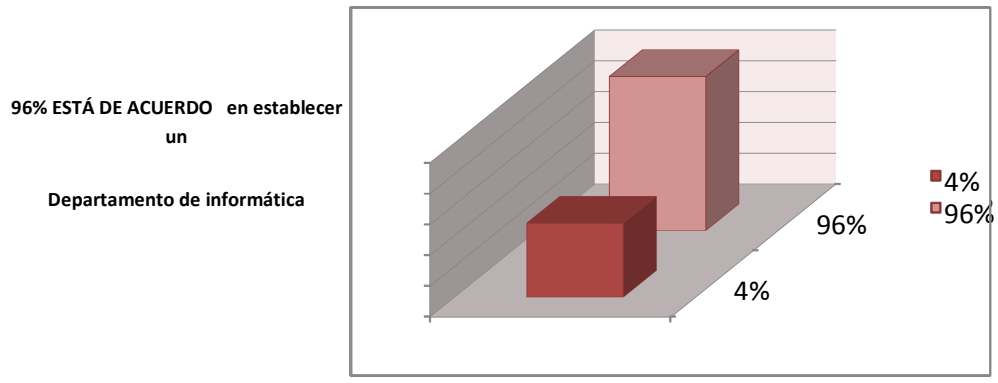
4.4 Identificación de áreas de enfoque

Se realizó un cuestionario para comprender a la entidad y comprobar si tanto administración como empleados estaban convencidos de un establecimiento de controles y así contestaron: El cuestionario se le pasó a 27 personas, de las cuales solamente 20 estarán dentro de la primera fase de automatización. Se presentan las interrogantes más importantes. Esto se hizo para comparar los criterios adquiridos en la visita preliminar, estudio de la documentación, evaluación de las políticas, prácticas de los usuarios, estudio de los procesos y sus responsables, organización y estructura de la Clínica. Se presentan ya graficadas en base a porcentajes estadísticos.

Gráfica 12
Gobierno en TI
Febrero 2010

1. ¿Cree que la Clínica necesita establecer un departamento de informática?

PERSONAS ENTREVISTADAS 26/27 = 96% SI 4% NO



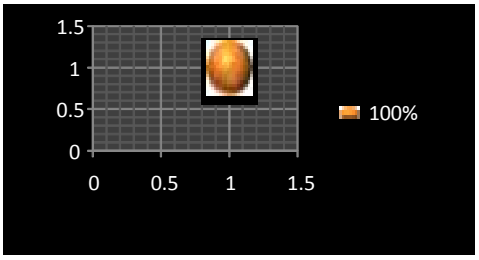
Fuente: Elaboración propia

Gráfica 13
Dominio de Planeación y Organización según COBIT
Febrero 2010

2.. ¿Estaría de acuerdo en planear una arquitectura tecnológica para la Clínica, en razón de automatizar la mayoría de las operaciones de atención al paciente?

27/27 = 100% SI 0/% NO

PERSONAS ENTREVISTADAS 27



Fuente: Elaboración propia

Gráfica 14
Gestión de Seguridad Informática (ISO 27001)
Febrero 2010

4.¿Qué políticas de seguridad deberían implementarse si se crea el departamento de informática?

1. ANTIVIRUS ACTUALIZADO	100%	27
2. CLAVES DE ACCESO	96%	26
3. RESTRICCIÓN DE LA INFORMACIÓN	74%	20
4. Back up automatizado dentro y fuera de la clínica	59%	16
5. Bases de datos no puedan modificarse	92%	25
6. Acceso restringido a sitios de internet	85%	23
7. RESTRINGIR EL USO DE USB	92%	25
8. Utilizar el equipo con fines laborales	74%	20

Fuente: Elaboración propia

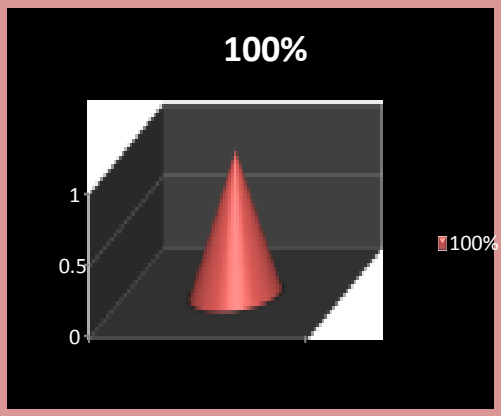
Gráfica 15
Capacitación del recurso humano
Febrero 2010

5. ¿Cree que las personas que trabajan en la clínica deben capacitarse continuamente en el área de informática o con lo que saben es suficiente? SI 27 NO 0

De las 27 personas entrevistadas

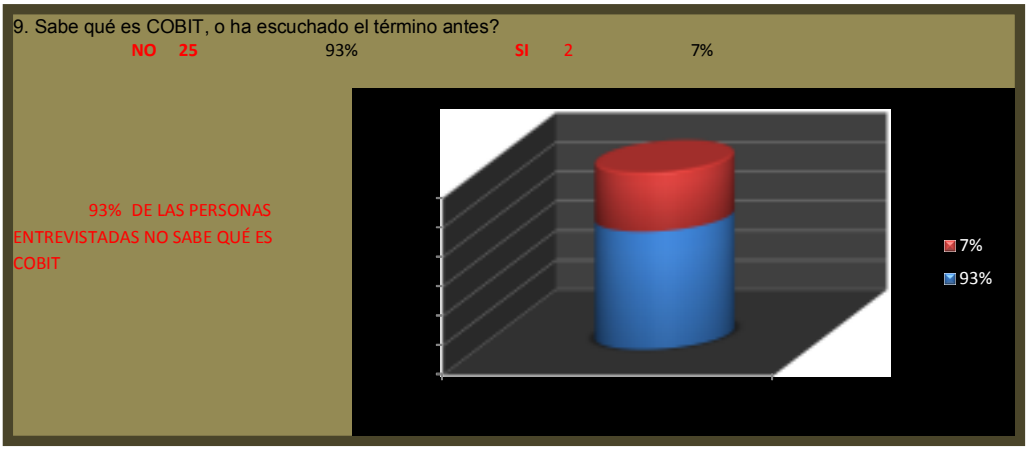
100% está de acuerdo en

Capacitarse.



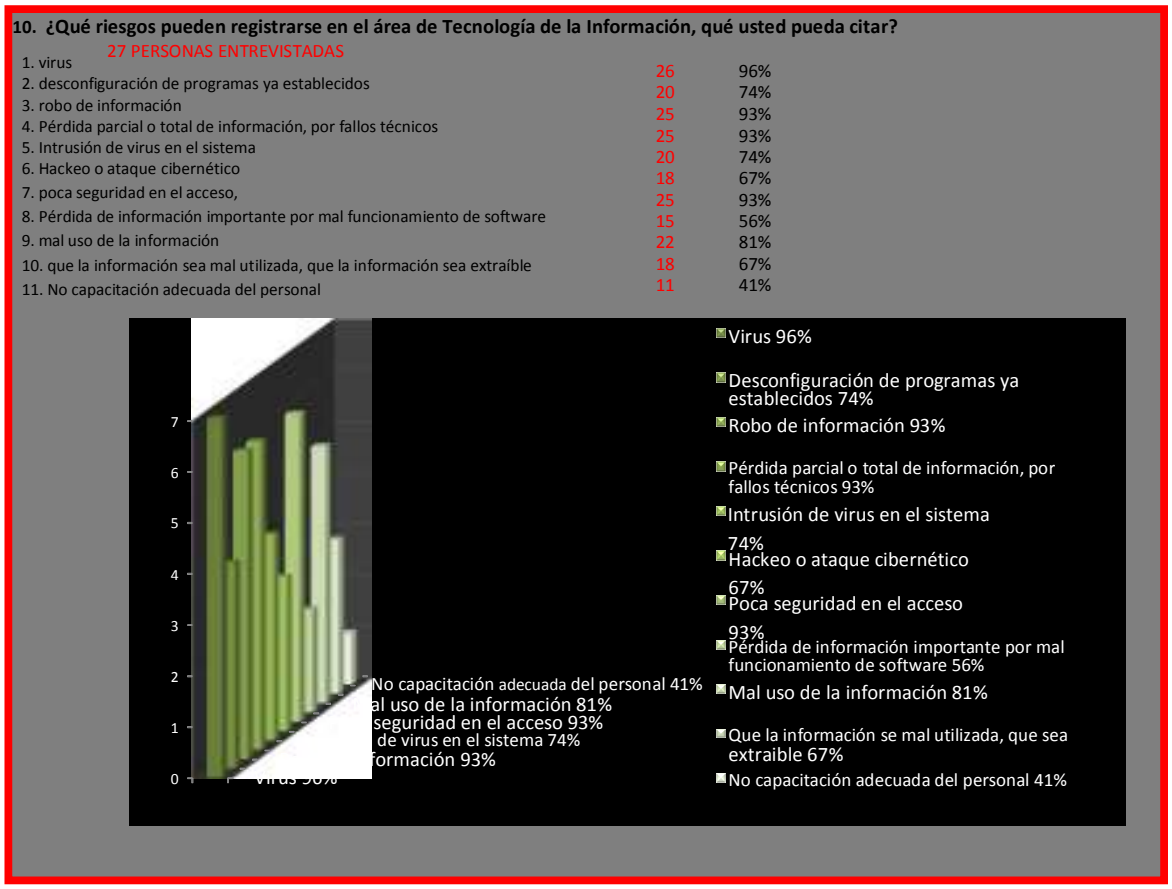
Fuente: Elaboración propia

Gráfica 16
Conocimiento de la existencia de COBIT
Febrero 2010



Fuente: Elaboración propia

Gráfica 17
Identificación de riesgos
Febrero 2010



Fuente: Elaboración propia

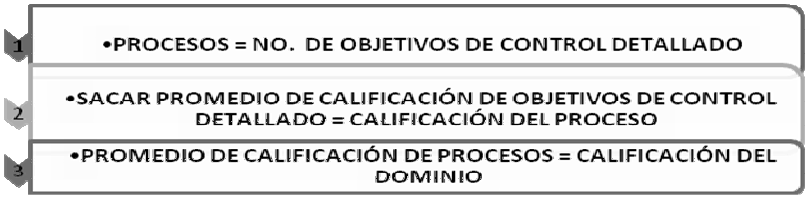
Esto demostró que la administración como los empleados estaban dispuestos a colaborar. Se realizó la primera conferencia para explicar qué significaba seguridad informática, y a qué riesgos estaban expuestos si continuaban como estaban.

Se realizó una primera puntuación de madurez del primer dominio, **Planeación y Organización.** Este dominio cubre las estrategias y las tácticas y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos de la entidad. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Según Normas Internacionales de Auditoría 300 y 315 planeación y entendimiento de la entidad, su entorno y evaluación de riesgos respectivamente, indica que este dominio es clave en cualquier proyecto de establecimiento de control interno.

- **¿Cómo se realiza la calificación de madurez?**

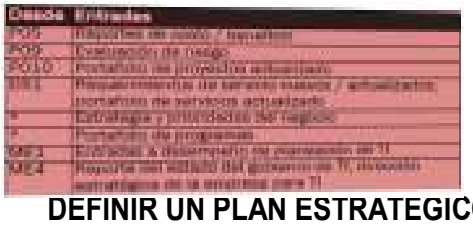
Para que el lector entienda cuando se da la puntuación en madurez, se elabora un ejemplo de orientación en el **dominio Planeación y Organización**, **proceso 1** que se denomina **Planear y Organizar**, que está subdividido en **6 objetivos de control detallado**. Se presentan los distintos papeles que se elaboraron, documentación revisada y observaciones realizadas por el auditor para llegar a la puntuación final de un solo proceso, lo que demostrará que es un trabajo a conciencia el dar una calificación, no es algo al azar. Este dominio se calificó dos veces, porque a criterio del auditor con base en la NIA 300, planeación y 315 entendimiento de la entidad y evaluación de riesgos, este dominio es clave. Especialmente si es una entidad sin controles.

Gráfica 18
¿Cómo se realiza la calificación?
Marzo 2010



Fuente: Elaboración propia

Figura 25
Papel de Trabajo PO1: Planear y Organizar
Marzo 2010



P/T	PO1	
	Auditor	Fecha
Hecho	M.M	12/03/2010
Revisado	AJGB	/03/2010

DEFINIR UN PLAN ESTRATEGICO DE TI

OBJETIVOS DE CONTROL

		No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
PO1.1	Administración del valor de TI						
PO1.2	Alineación de TI con la entidad						
PO1.3	Evaluación del desempeño actual					24/03/2010	
PO1.4	Plan estratégico de TI				24/03/2010		
PO1.5	Planes tácticos de TI					24/03/2010	
PO1.6	Administración del portafolio de TI					24/03/2010	
		0	1		9	12	

TOTAL 9/6 1.5 ˜

Fórmula de la Media.

$X = \frac{\sum X}{n}$ 22/6 = 3.6

Conclusiones

Salidas	Hacia					
Plan estratégico de TI	PO2..PO6	PO8	PO9	AI1	DS1	
Plan táctico de TI	PO2..PO6	PO9	AI1	DS1		
Portafolios de proyectos de TI	PO5	PO6	PO10	AI6		
Portafolio de servicios de TI	PO5	PO6	PO9	DS1		
Estrategia de contratación externa de TI	DS2					
Estrategia de adquisición de TI	AI5					

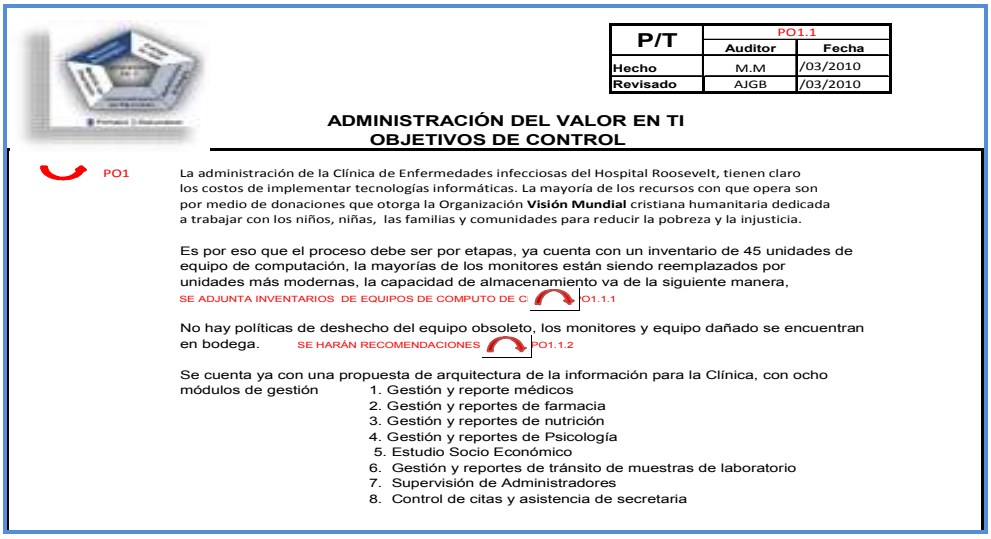
El proceso PO1 ESTÁ EN UN NIVEL DE MADUREZ 2

Este objetivo requiere definir un plan estratégico de TI para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia de la institución y sus prioridades.

Nuevo nivel madurez 4 24/03/2009

Fuente: Elaboración propia

Figura 26
Papel de Trabajo PO1.1: Administración del valor de TI
Marzo 2010



P/T	PO1.1	
	Auditor	Fecha
Hecho	M.M	/03/2010
Revisado	AJGB	/03/2010

ADMINISTRACIÓN DEL VALOR EN TI
OBJETIVOS DE CONTROL

PO1

La administración de la Clínica de Enfermedades infecciosas del Hospital Roosevelt, tienen claro los costos de implementar tecnologías informáticas. La mayoría de los recursos con que opera son por medio de donaciones que otorga la Organización **Visión Mundial** cristiana humanitaria dedicada a trabajar con los niños, niñas, las familias y comunidades para reducir la pobreza y la injusticia.

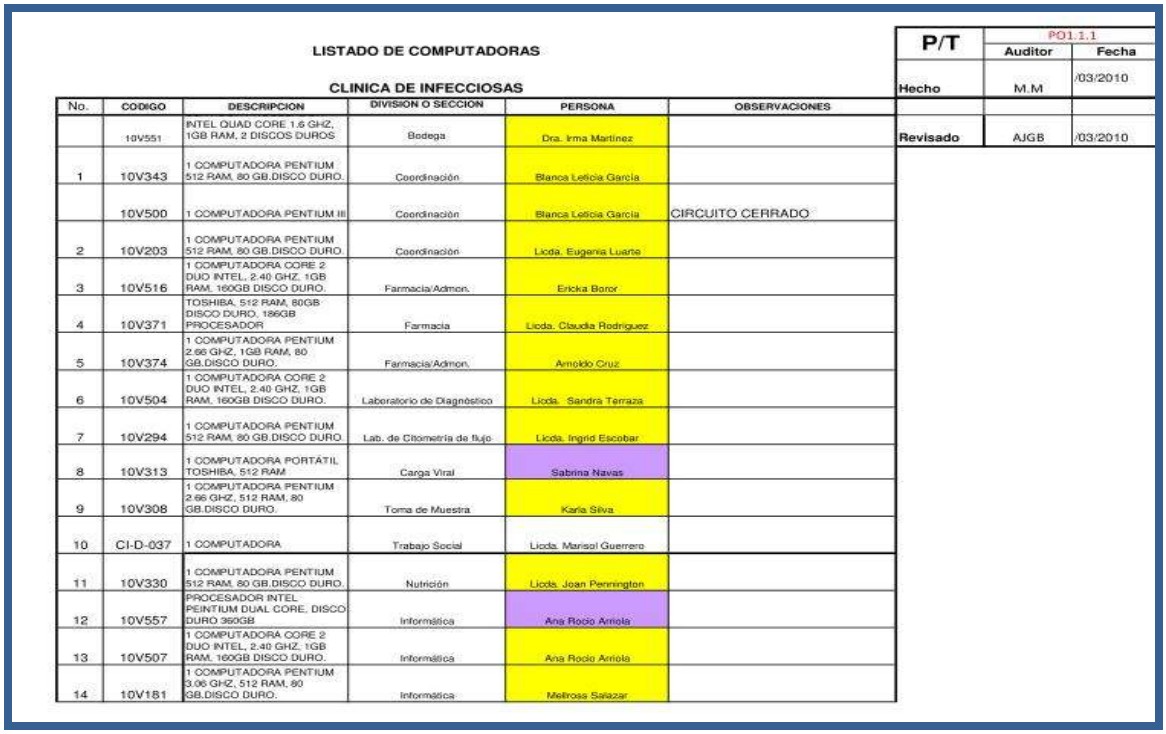
Es por eso que el proceso debe ser por etapas, ya cuenta con un inventario de 45 unidades de equipo de computación, la mayorías de los monitores están siendo reemplazados por unidades más modernas, la capacidad de almacenamiento va de la siguiente manera,
SE ADJUNTA INVENTARIOS DE EQUIPOS DE COMPUTO DE C PO1.1.1

No hay políticas de deshecho del equipo obsoleto, los monitores y equipo dañado se encuentran en bodega. SE HARÁN RECOMENDACIONES PO1.1.2

Se cuenta ya con una propuesta de arquitectura de la información para la Clínica, con ocho módulos de gestión
1. Gestión y reporte médicos
2. Gestión y reportes de farmacia
3. Gestión y reportes de nutrición
4. Gestión y reportes de Psicología
5. Estudio Socio Económico
6. Gestión y reportes de tránsito de muestras de laboratorio
7. Supervisión de Administradores
8. Control de citas y asistencia de secretaria

Fuente: Elaboración propia

Figura 27
Papel de Trabajo PO1.1.1: Inventario de computadoras e impresoras
Marzo 2010

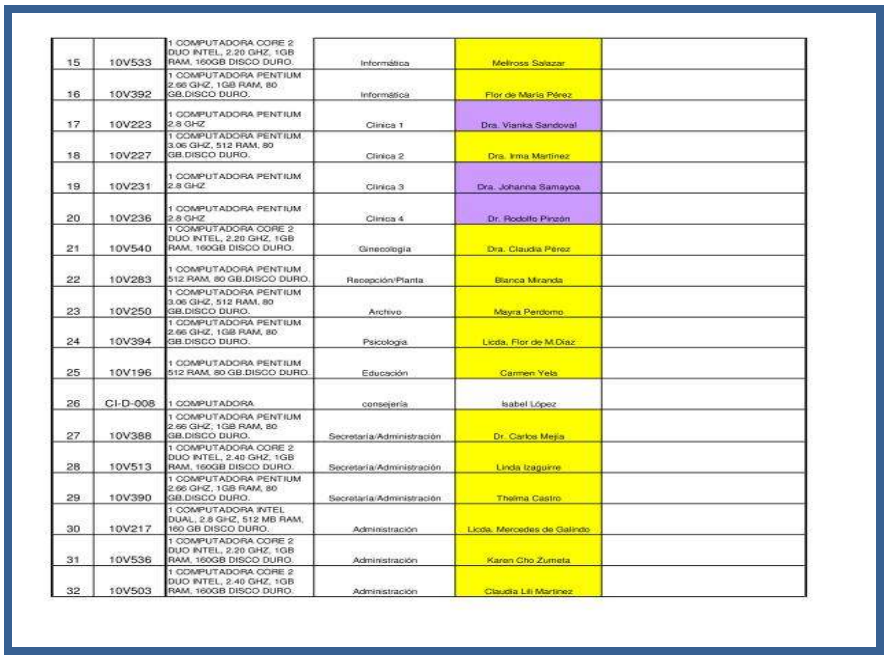


LISTADO DE COMPUTADORAS

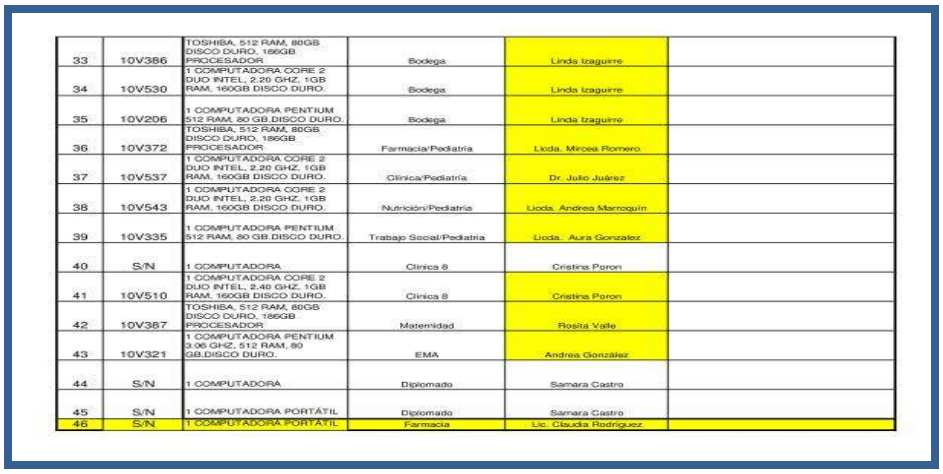
CLINICA DE INFECCIOSAS

P/T	PO1.1.1	
	Auditor	Fecha
Hecho	M.M	/03/2010
Revisado	AJGB	/03/2010

No.	CODIGO	DESCRIPCION	DIVISION O SECCION	PERSONA	OBSERVACIONES
	10V551	INTEL QUAD CORE 1.6 GHZ, 1GB RAM, 2 DISCOS DUROS	Bodega	Dra. Irma Martínez	
1	10V343	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Coordinación	Blanca Leticia García	
	10V500	1 COMPUTADORA PENTIUM III	Coordinación	Blanca Leticia García	CIRCUITO CERRADO
2	10V203	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Coordinación	Licda. Eugenia Luarte	
3	10V516	1 COMPUTADORA CORE 2 DUO INTEL, 2.40 GHZ, 1GB RAM, 160GB DISCO DURO.	Farmacia/Admon.	Ericka Boror	
4	10V371	TOSHIBA, 512 RAM, 80GB DISCO DURO, 186GB PROCESADOR	Farmacia	Licda. Claudia Rodríguez	
5	10V374	1 COMPUTADORA PENTIUM 2.66 GHZ, 1GB RAM, 80 GB.DISCO DURO.	Farmacia/Admon.	Arnoldo Cruz	
6	10V504	1 COMPUTADORA CORE 2 DUO INTEL, 2.40 GHZ, 1GB RAM, 160GB DISCO DURO.	Laboratorio de Diagnóstico	Licda. Sandra Terraza	
7	10V294	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO	Lab. de Citometría de flujo	Licda. Ingrid Escobar	
8	10V313	1 COMPUTADORA PORTÁTIL TOSHIBA, 512 RAM	Carga Viral	Sabrina Navas	
9	10V308	1 COMPUTADORA PENTIUM 2.66 GHZ, 512 RAM, 80 GB.DISCO DURO.	Toma de Muestra	Karla Silva	
10	CI-D-037	1 COMPUTADORA	Trabajo Social	Licda. Marisol Guerrero	
11	10V330	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Nutrición	Licda. Joan Pennington	
12	10V557	PROCESADOR INTEL PEINTIUM DUAL CORE, DISCO DURO 360GB	Informática	Ana Rocio Arriola	
13	10V507	1 COMPUTADORA CORE 2 DUO INTEL, 2.40 GHZ, 1GB RAM, 160GB DISCO DURO.	Informática	Ana Rocio Arriola	
14	10V181	1 COMPUTADORA PENTIUM 3.06 GHZ, 512 RAM, 80 GB.DISCO DURO.	Informática	Melirosa Salazar	



15	10V533	1 COMPUTADORA CORE 2 DUO INTEL, 2.20 GHZ, 1GB RAM, 160GB DISCO DURO.	Informática	Melross Salazar	
16	10V392	1 COMPUTADORA PENTIUM 2.66 GHZ, 1GB RAM, 80 GB.DISCO DURO.	Informática	Flor de María Pérez	
17	10V223	1 COMPUTADORA PENTIUM 2.8 GHZ	Clínica 1	Dra. Vianka Sandoval	
18	10V227	1 COMPUTADORA PENTIUM 3.06 GHZ, 512 RAM, 80 GB.DISCO DURO.	Clínica 2	Dra. Irma Martínez	
19	10V231	1 COMPUTADORA PENTIUM 2.8 GHZ	Clínica 3	Dra. Johanna Samayoa	
20	10V236	1 COMPUTADORA PENTIUM 2.8 GHZ	Clínica 4	Dr. Rodolfo Pinzón	
21	10V540	1 COMPUTADORA CORE 2 DUO INTEL, 2.20 GHZ, 1GB RAM, 160GB DISCO DURO.	Ginecología	Dra. Claudia Pérez	
22	10V283	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Recepción/Planta	Blanca Miranda	
23	10V250	1 COMPUTADORA PENTIUM 3.06 GHZ, 512 RAM, 80 GB.DISCO DURO.	Archivo	Mayra Perdomo	
24	10V394	1 COMPUTADORA PENTIUM 2.66 GHZ, 1GB RAM, 80 GB.DISCO DURO.	Psicología	Licda. Flor de M.Díaz	
25	10V196	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Educación	Carmen Yela	
26	CI-D-008	1 COMPUTADORA	consejería	Isabel López	
27	10V388	1 COMPUTADORA PENTIUM 2.66 GHZ, 1GB RAM, 80 GB.DISCO DURO.	Secretaría/Administración	Dr. Carlos Mejía	
28	10V513	1 COMPUTADORA CORE 2 DUO INTEL, 2.40 GHZ, 1GB RAM, 160GB DISCO DURO.	Secretaría/Administración	Linda Izaguirre	
29	10V390	1 COMPUTADORA PENTIUM 2.66 GHZ, 1GB RAM, 80 GB.DISCO DURO.	Secretaría/Administración	Thelma Castro	
30	10V217	1 COMPUTADORA INTEL DUAL, 2.8 GHZ, 512 MB RAM, 160 GB DISCO DURO.	Administración	Licda. Mercedes de Galindo	
31	10V536	1 COMPUTADORA CORE 2 DUO INTEL, 2.20 GHZ, 1GB RAM, 160GB DISCO DURO.	Administración	Karen Cho Zumeta	
32	10V503	1 COMPUTADORA CORE 2 DUO INTEL, 2.40 GHZ, 1GB RAM, 160GB DISCO DURO.	Administración	Claudia Lil Martínez	



33	10V386	TOSHIBA, 512 RAM, 80GB DISCO DURO, 186GB PROCESADOR	Bodega	Linda Izaguirre	
34	10V530	1 COMPUTADORA CORE 2 DUO INTEL, 2.20 GHZ, 1GB RAM, 160GB DISCO DURO.	Bodega	Linda Izaguirre	
35	10V206	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Bodega	Linda Izaguirre	
36	10V372	TOSHIBA, 512 RAM, 80GB DISCO DURO, 186GB PROCESADOR	Farmacia/Pediatría	Licda. Mircea Romero	
37	10V537	1 COMPUTADORA CORE 2 DUO INTEL, 2.20 GHZ, 1GB RAM, 160GB DISCO DURO.	Clínica/Pediatría	Dr. Julio Juárez	
38	10V543	1 COMPUTADORA CORE 2 DUO INTEL, 2.20 GHZ, 1GB RAM, 160GB DISCO DURO.	Nutrición/Pediatría	Licda. Andrea Marroquín	
39	10V335	1 COMPUTADORA PENTIUM 512 RAM, 80 GB.DISCO DURO.	Trabajo Social/Pediatría	Licda. Aura Gonzalez	
40	S/N	1 COMPUTADORA	Clínica 8	Cristina Poron	
41	10V510	1 COMPUTADORA CORE 2 DUO INTEL, 2.40 GHZ, 1GB RAM, 160GB DISCO DURO.	Clínica 8	Cristina Poron	
42	10V387	TOSHIBA, 512 RAM, 80GB DISCO DURO, 186GB PROCESADOR	Maternidad	Rosita Valle	
43	10V321	1 COMPUTADORA PENTIUM 3.06 GHZ, 512 RAM, 80 GB.DISCO DURO.	EMA	Andrea Gonzalez	
44	S/N	1 COMPUTADORA	Diplomado	Samara Castro	
45	S/N	1 COMPUTADORA PORTÁTIL	Diplomado	Samara Castro	
46	S/N	1 COMPUTADORA PORTÁTIL	Farmacia	Lic. Claudia Rodríguez	

Fuente: Elaboración propia

Dentro de los problemas de inventario; se encontró que no estaban inventariadas 4 computadoras, que ya tenía al menos unos 7 meses de estar en uso, lo mismo con las impresoras.

Fuente: Elaboración propia

El papel PO1.2 Alineación de TI con la entidad, consta del cuestionario que se presentó al principio, donde se realizan una serie de interrogantes a la Administración de la clínica así como a los usuarios (empleados que laboran en la clínica), aquí se puede observar que COBIT, indica que en un dominio se pueden tomar los procesos en orden, pero no es una regla, es a criterio del auditor, tomar el orden que mejor le

parezca, según sea el caso, pero no dejar de tomar en cuenta todos los objetivos de control detallados.

Figura 28
Papel de Trabajo PO1.3: Evaluación del desempeño y la capacidad actual
Marzo 2010

P/T	PO1.3	
	Auditor	Fecha
Hecho	M.M	/03/2010
Revisado	AJGB	/03/2010

Antecedentes al desempeño actual
OBJETIVOS DE CONTROL

ANÁLISIS ESPECIAL EN LA CREACIÓN DE SCI BASADO EN COBIT

SIGNIFICADO- Entendimiento del tema

Gracias a la utilización segura y eficaz de las Tecnologías de Información, las entidades que conforman el Sector Salud tienen posibilidad de participar más activamente en el fortalecimiento de un sistema de sanidad que garantice el bienestar integral de la población. Es por esto que el modelo COBIT proporciona las directrices más concretas para organizar y planificar ambientes TI que sean más seguros y manejen el riesgo de los mismos de la mejor manera posible.

FODA DEL AMBIENTE TI ASOCIADO A COBIT EN EL ÁREA DE SALUD

FORTALEZAS

De aquí que elprofesional de las ciencias de la salud tiene que familiarizarse con vocablos como, por citar algunos, nanomedicina, telemedicina, cibermedicina, cirugía robótica, etc. Historia clínica computarizada y electrónica. Las historias médicas computarizadas se construyen escaneando los documentos basados en papel. Redes y sistemas de información hospitalarios, bases de datos de información médica, bibliotecas virtuales, revistas médicas on-line, protocolos de investigación. Medicina basada en evidencias

OPORTUNIDADES

Hoy en día, Internet y las TI ofrece al Sector Salud la invaluable oportunidad de que todos los actores involucrados en él, pacientes, pacientes, médicos, hospitales, proveedores de diversos servicios de salud, farmacéuticas, laboratorios, investigadores y asociaciones-puedan intercambiar datos e información de manera oportuna y eficaz.

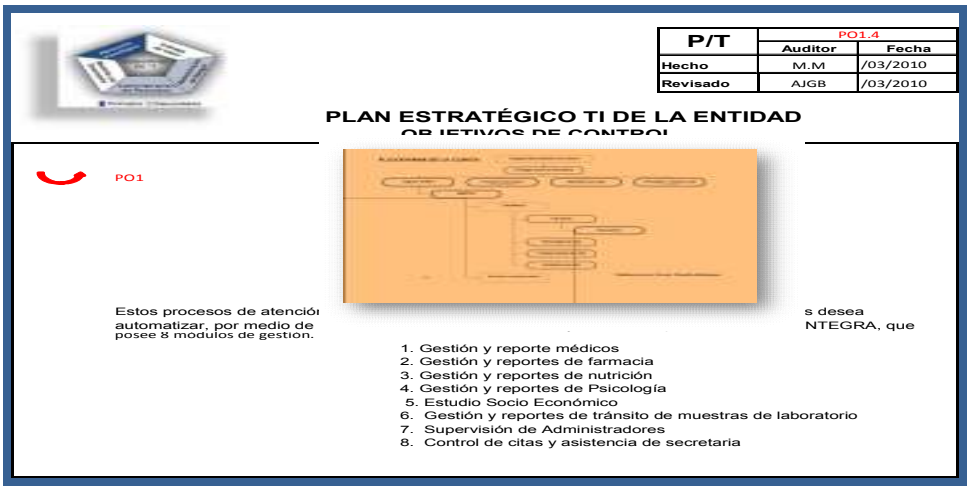
DEBILIDADES

Como ocurre en otros sectores, estos avances surgen de la mano de mayores riesgos conforme aparecen amenazas, aumenta la demanda y los sistemas evolucionan. Estos obliga a las empresas del ramo a mantenerse permanentemente alertas ante intrusiones y posibles focos de vulnerabilidad que filtren información delicada del paciente almacenada en los sistemas TI

AMENAZAS Que no se garantice la confidencialidad, disponibilidad e integridad en términos de TI, que no se mantenga el equilibrio de los recursos humanos, la tecnología, los procesos y procedimientos, que arrojará incumplimiento con la normativa de salud nacional y no acelerará la madurez o confiabilidad en los procesos operativos de TI.

Fuente: Elaboración propia

Figura 29
Papel de Trabajo PO1.4: Plan estratégico TI de la entidad
Marzo 2010



P/T	PO1.4	
	Auditor	Fecha
Hecho	M.M	/03/2010
Revisado	AJGB	/03/2010

PLAN ESTRATÉGICO TI DE LA ENTIDAD
OBJETIVOS DE CONTROL

PO1

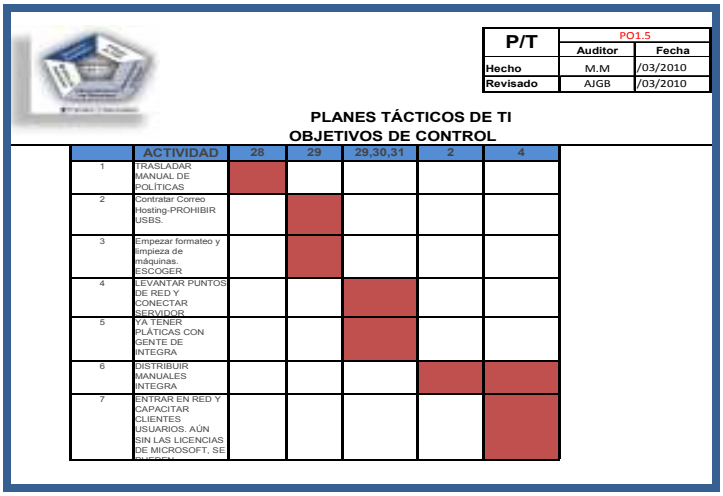
Estos procesos de atenció
automatizar, por medio de
posee 8 modulos de gestion.

s desea
NTEGRA, que

1. Gestión y reporte médicos
2. Gestión y reportes de farmacia
3. Gestión y reportes de nutrición
4. Gestión y reportes de Psicología
5. Estudio Socio Económico
6. Gestión y reportes de tránsito de muestras de laboratorio
7. Supervisión de Administradores
8. Control de citas y asistencia de secretaria

Fuente: Elaboración propia

Figura 30
Papel de Trabajo PO1.5: Planes tácticos de TI
Marzo 2010



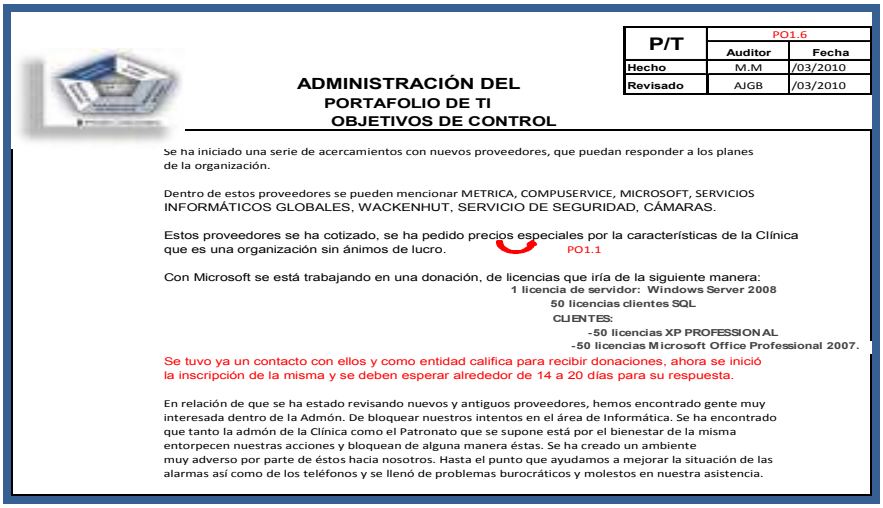
P/T	PO1.5	
	Auditor	Fecha
Hecho	M.M	/03/2010
Revisado	AJGB	/03/2010

PLANES TÁCTICOS DE TI
OBJETIVOS DE CONTROL

	ACTIVIDAD	28	29	29,30,31	2	4
1	TRASLADAR MANUAL DE POLÍTICAS					
2	Contratar Correo Hosting-PROHIBIR USBS.					
3	Empezar formateo y limpieza de máquinas. ESCOGER					
4	LEVANTAR PUNTOS DE RED Y CONECTAR SERVIDOR					
5	YA TENER PLÁTICAS CON GENTE DE INTEGRA					
6	DISTRIBUIR MANUALES INTEGRA					
7	ENTRAR EN RED Y CAPACITAR CLIENTES USUARIOS. AÚN SIN LAS LICENCIAS DE MICROSOFT, SE					

Fuente: Elaboración propia

Figura 31
Papel de Trabajo PO1.6: Portafolio de TI
Marzo 2010



P/T	PO1.6	
	Auditor	Fecha
Hecho	M.M	/03/2010
Revisado	AJGB	/03/2010

ADMINISTRACIÓN DEL
PORTAFOLIO DE TI
OBJETIVOS DE CONTROL

Se ha iniciado una serie de acercamientos con nuevos proveedores, que puedan responder a los planes de la organización.

Dentro de estos proveedores se pueden mencionar METRICA, COMPUSERVICE, MICROSOFT, SERVICIOS INFORMÁTICOS GLOBALES, WACKENHUT, SERVICIO DE SEGURIDAD, CÁMARAS.

Estos proveedores se ha cotizado, se ha pedido precios especiales por la características de la Clínica que es una organización sin ánimos de lucro. PO1.1

Con Microsoft se está trabajando en una donación, de licencias que iría de la siguiente manera:
1 licencia de servidor: Windows Server 2008
50 licencias clientes SQL
CLIENTES:
-50 licencias XP PROFESSIONAL
-50 licencias Microsoft Office Professional 2007.

Se tuvo ya un contacto con ellos y como entidad califica para recibir donaciones, ahora se inició la inscripción de la misma y se deben esperar alrededor de 14 a 20 días para su respuesta.

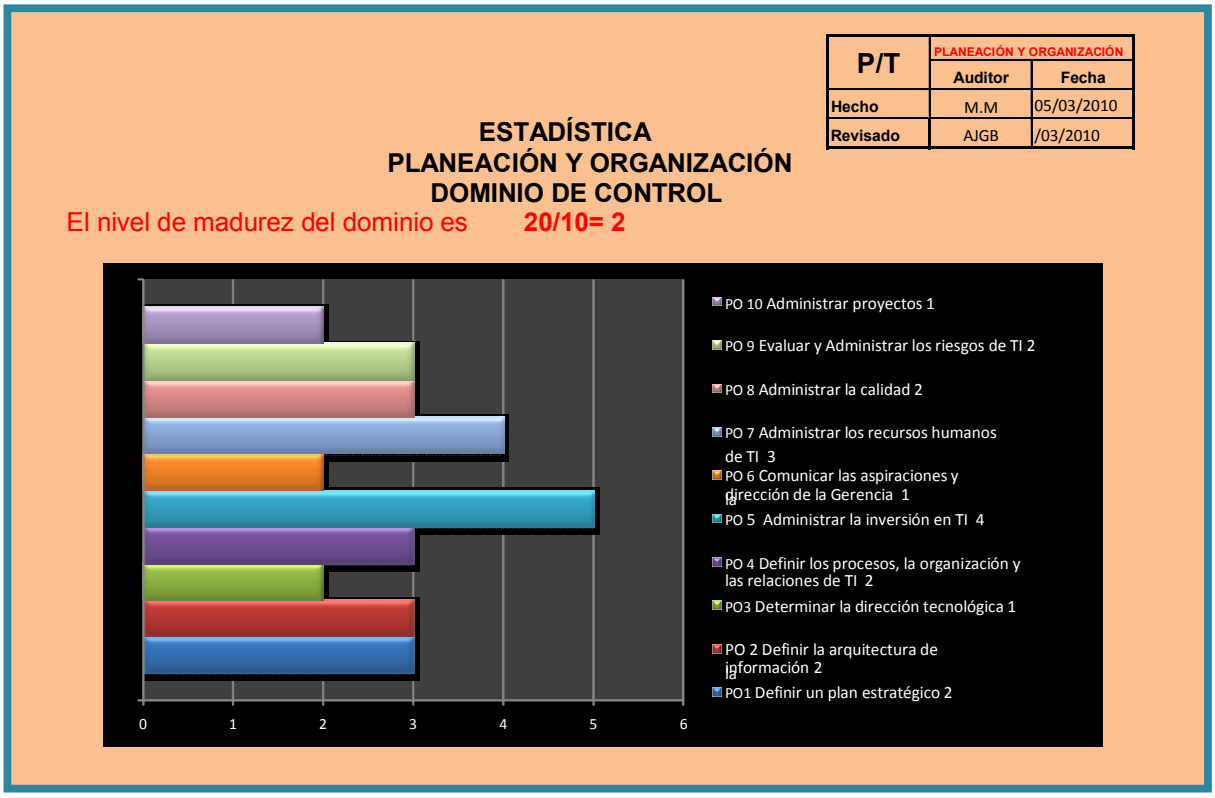
En relación de que se ha estado revisando nuevos y antiguos proveedores, hemos encontrado gente muy interesada dentro de la Admón. De bloquear nuestros intentos en el área de Informática. Se ha encontrado que tanto la admón de la Clínica como el Patronato que se supone está por el bienestar de la misma entorpecen nuestras acciones y bloquean de alguna manera éstas. Se ha creado un ambiente muy adverso por parte de éstos hacia nosotros. Hasta el punto que ayudamos a mejorar la situación de las alarmas así como de los teléfonos y se llenó de problemas burocráticos y molestos en nuestra asistencia.

Fuente: Elaboración propia

Como puede observarse este sólo fue un proceso de **10** que contiene el **Dominio Planeación y Organización,** en total posee **74 objetivos** de control detallado, el siguiente **Dominio Adquisición e implementación** son **40 objetivos**, **Entregar y dar soporte 71 objetivos** y Monitoreo y Evaluación **25**. Este ejemplo se da para dejar evidencia suficiente y competente, que cada calificación conlleva un estudio exhaustivo

de varios criterios a tomar en cuenta para dar cada puntuación. El total de **objetivos** a calificar son **210**, **34** procesos y **4 dominios.**

Gráfica 19
Primera calificación de madurez del Dominio Planeación y Organización
Marzo 2010



Fuente: Elaboración propia

- **Planeamiento y Organización: El nivel de madurez del dominio es 2**

  Los procesos siguen un patrón regular, no hay entrenamiento o comunicación formal de procedimientos estándar. Se dejan responsabilidades al individuo. Existe conciencia de la necesidad de controles y la administración comunica los problemas en forma general. Las políticas, estándares y procedimientos surgen como similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual, lo que hacen que los procesos se realicen repetitivamente, puede existir alguna documentación y entendimiento informal de políticas y procedimientos. Existen enfoques

comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Poseen ciertas herramientas que pueden haberse adquirido por proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse. Se identifican los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha. Los individuos asumen su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de la responsabilidad cuando ocurren problemas y una **cultura de culpas tiende a existir**. Existen algunas metas; se establecen algunas mediciones financieras pero sólo las conoce la alta dirección. Hay monitoreo inconsistente en áreas aisladas.

- **Debilidades de control interno informadas a la administración**

Debilidad 1

Existe una unidad de Informática, pero no funciona como encargada del ambiente TI

Condición

La unidad de informática es realmente el sitio donde se encuentran los digitadores de las distintas bases de datos que se manejan, pero nadie con funciones ni conocimientos para administrar las TIC.

Criterio

De acuerdo a COBIT, la complejidad de las TIC, deben administrarse y desarrollarse con personas capacitadas, es decir la creación de un gobierno en TI que trasmita los conocimientos a los demás usuarios.

Causa

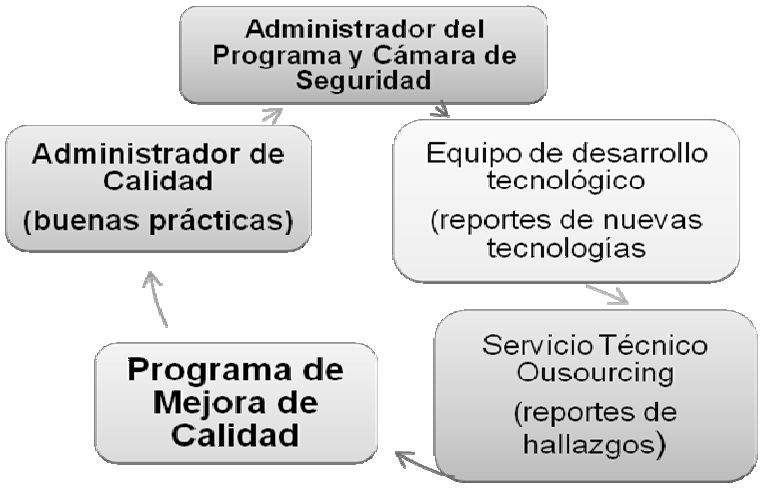
Confundir lo que es un área de informática con un área de digitación.

Efecto

No se cuenta con personal capacitado para administrar al menos el equipo de computación y de impresión de la clínica, por esta causa se manda equipo a la unidad de informática del Hospital Roosevelt, que no es lo más adecuado como servicio de asistencia técnica.

Recomendación: Organigrama de relación de no jerarquía con consultas e información al Jefe de la Clínica.

Gráfica 20
Organigrama de relación sugerido para Gobierno en TI
Marzo 2010



Fuente: Elaboración propia

Además de esta organización es importante el establecimiento de un **Consejo de Arquitectura de TI.** Un grupo de personas que administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicio, y mecanismos de aplicación.

Debilidad 2

Equipo de computación, discos de instalación sin codificación de inventario

Condición

Se identificó equipo de computación y discos de instalación sin codificación de inventario, además que de 49 equipos de computación solamente aparecen 12 discos de instalación, lo cual no permite su localización física para efectos de control.

Criterio

De acuerdo a la Sección II: del **Manual de Normas y Procedimientos Administrativos y Financieros para las Unidades Ejecutoras (Sub-receptores) del proyecto:** Los activos adquiridos por el Receptor Principal o la Unidad Ejecutora, en el marco del acuerdo suscrito, deben registrarse en el libro de inventarios de Activos Fijos. Deben contener código de inventario, fecha de ingreso (o baja) del inventario. Descripción del artículo (marca, color, serie, modelo). Ubicación (persona y departamento al que asignado el bien). Datos de compra (número de factura, proveedor, costo). Datos del seguro (número de póliza, vigencia y compañía aseguradora). Información sobre bajas (motivo y documento que respalda la baja.

Causa

La persona que lleva inventarios, no los administra de la forma que el manual indica, se encuentran equipos de computación sin indicación de serial, capacidades de hardware como disco duro, memoria RAM; determinación si es un equipo portátil o de escritorio y los 12 discos de instalación que se encontraron no tenían ningún código que correspondiera al código de máquina.

Efecto

Dificultad para localizar físicamente el activo además de que se hace difícil el formateo de una máquina si no hay discos de instalación.

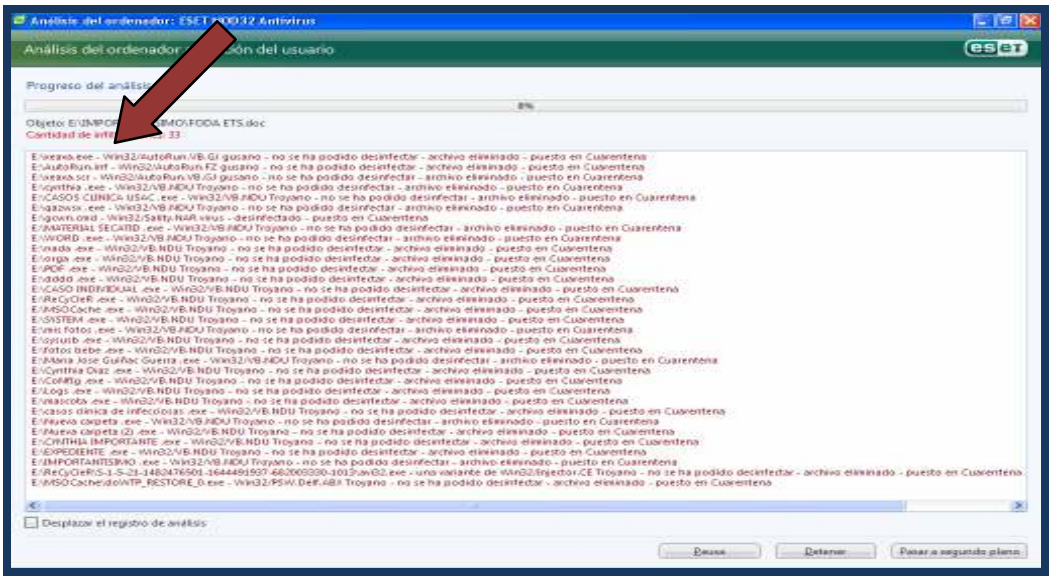
Recomendación

Actualización de inventarios por lo menos en forma bimensual, Identificar los bienes que no poseen códigos con etiquetas perdurables.

- **Riesgos detectados dentro de la Clínica son los siguientes**

  - Alto grado de contaminación de los equipos por medio de USB, los usuarios no tienen el cuidado de limpiarlas antes de usarlas, con la solución de seguridad. Se han encontrado los virus informáticos más peligrosos en el mundo. Win32. I love you, por mencionar algunos.

Figura 32
Análisis de un dispositivo de almacenamiento USB por medio de una solución de seguridad
Marzo 2010



Captura de Pantalla de las memorias USB, se encuentran muy contaminadas un total de 33 virus encontrados, lo resaltado en rojo es parte de las amenazas detectadas EN UN SÓLO DISPOSITIVO

  - Hay equipos que se han encontrado en riesgo físico, por ejemplo un CPU, utilizado como escritorio, donde se encontró una bandeja de hierro con muchos papeles, esto puede dañar seriamente un equipo.

  - Personas que no quieren cambios, y tratan de bloquear el establecimiento de controles.

  - Pueden ocurrir pérdidas o robos de equipos, por falta de cámaras de seguridad en las áreas donde se encuentran los mismos.

- Facilidad de introducirse al equipo de un usuario por falta de claves de acceso.
- Se ha encontrado niños jugando con los equipos de las clínicas, por falta de precaución de cerrar las puertas de acceso a las mismas.
- No existe licenciamiento, hay que verificar. Si no son licencias, puede haber bloqueos y pérdidas en las bases de datos.
- No existe políticas preventivas, por ejemplo, servicios a los equipos, sino solamente correctivos, cuando el equipo ya muestra daños.
- Hay equipos que se encuentran muy alejados de la clínica, lo que hace difícil que su utilización y seguridad sean adecuadamente monitoreados y evaluados.
- En el área de Toma de Muestra se detectó una licencia pirata.
- No se crean Back ups

➢ **Sugerencias**

- Restringir el uso de unidades de almacenamiento USB, por contaminación, quitar físicamente acceso. Datos deben enviarse vía correo de dominio.
- No bajar música, o videos, acrecienta el tráfico en red
- Remover aplicaciones como Nero, Messenger, juegos en línea, páginas de adultos, contienen malware que puede bloquear programas o dar acceso a la dirección IP del usuario, contaminan el sistema.

- Explicar a los clientes/usuarios, que a pesar de que existen soluciones de seguridad no son infalibles, deben ser proactivos en administrar su estación.
- No bajar imágenes, ocupan mucho espacio en el disco duro
- Crear claves de acceso seguras y debe ser cambiadas cada x meses
- Equipos deben usarse exclusivamente para trabajar, concientizar a los usuarios, que no son propiedad de ellos, su mantenimiento es costoso y la reparación más.
- Deben crearse manuales de procedimientos para seguridad física y lógica de los mismos.
- Pedir a los usuarios que se capaciten constantemente.
- Crear Back ups semanales, mensuales, lo determina la alta dirección
- Mantenerlos en una Caja de Seguridad de un Banco.
- Crear un hosting de correo y página internet, con un registro de dominio, que administre archivo y prácticas de usuarios. Sin estar dentro del Servidor. El correo electrónico, es una fuente de contaminación, por lo tanto debe quedar fuera del servidor.

4.5 Evaluación de guías y modelos aplicables mediante objetivos de control

Se informó en una reunión a la Administración sobre lo anteriormente detectado y se acordó elaborar guías de trabajo y buscar modelos que se adaptaran a la Clínica y comenzar la elaboración de un **Manual de Políticas de Seguridad Informática**

(Anexo). Además la Administración de la Clínica se reunió con sus coordinadores de área y giró órdenes que las personas removieran archivos personales, música, imágenes, trabajos de la universidad y que por favor no bajaran archivos de cadenas que se enviaban a través del correo electrónico. Tomaron la decisión que el software a la medida para automatizar la Clínica era INTEGRA, una aplicación desarrollada por el Doctor Juan Carlos Romero y el programador Joshua Letona Diemecke, que está integrado por 8 módulos de gestión. Se solicitó una donación de licencias a Microsoft, puesto que la Clínica no contaba con los fondos necesarios para esto, **se encuentra en trámite**. Se acordó revisar las capacidades de hardware, tanto servidor como computadoras, el cableado, para poder realizar una conexión en línea de 19 clientes y un administrador sin problemas.

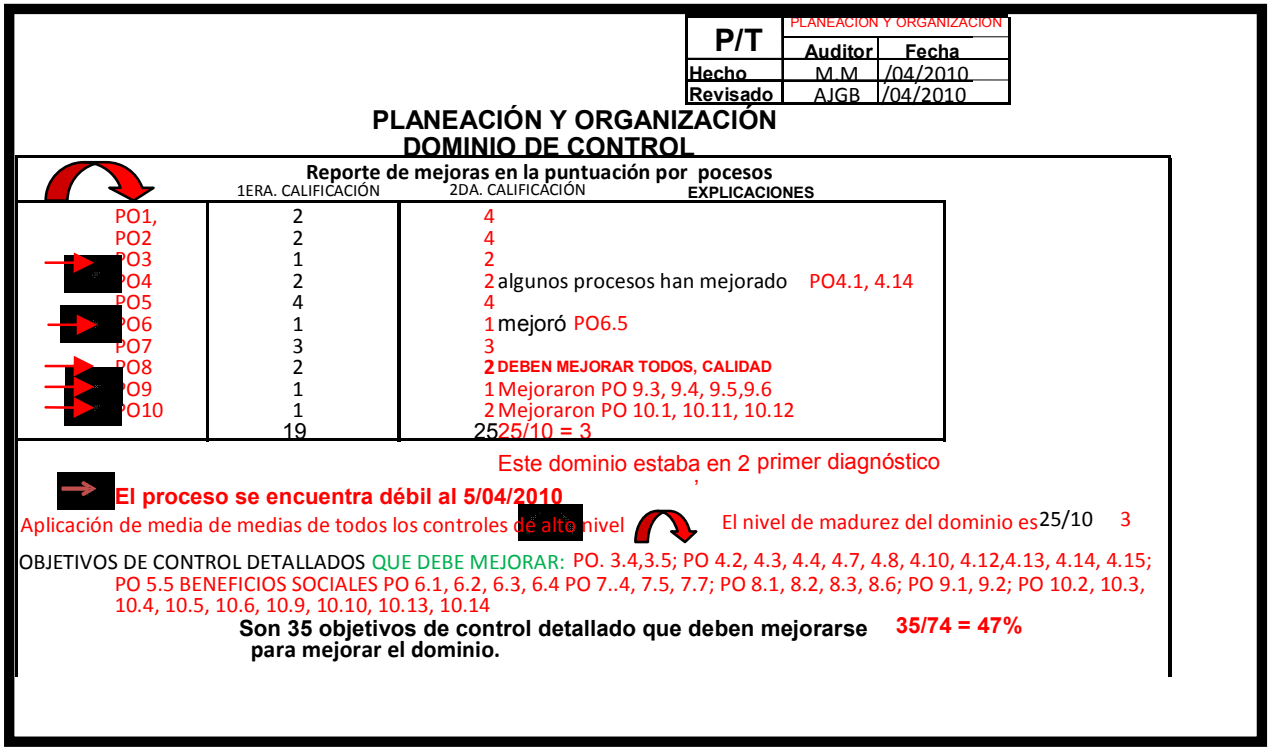
Se volvió a evaluar el dominio Planeación y Organización y como resultado de lo anteriormente expuesto de nivel 2 de madurez pasaron a 3.

Gráfica 21
Segunda calificación de madurez del Dominio Planeación y Organización
Abril 2010

Fuente: Elaboración propia

- **¿Qué quiere decir lo anterior?**

Figura 33
Cédula Centralizadora del dominio Planeación y Organización: papel de trabajo comparativo de calificaciones de madurez
Abril 2010



Fuente: Elaboración propia

La administración de la clínica en base a recomendaciones empieza a cuidar de procesos críticos de TI, se identifica con base en impulsores de valor y riesgo. Se realiza un análisis detallado para identificar requisitos de control y la causa raíz de las brechas, así como para desarrollar oportunidades de mejora. Además se empiezan a utilizar herramientas, se realizan entrevistas para apoyar el análisis y garantizar que los dueños de los procesos de TI son realmente los dueños e impulsan al proceso de evaluación y mejora. Empiezan los controles y se documentan ya en forma adecuada. Se evalúa la efectividad operativa de forma periódica y existen todavía problemas. Aunque la administración de la Clínica puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Entre estos se pueden citar, que ya hay empleados resistiéndose

a los cambios y que trata de convencer a otros de no acatar órdenes, algunos coordinadores de área no colaboran sino más bien obstaculizan. El caso más palpable es la persona encargada de la Administración de la Clínica, que dentro de sus funciones especifica que debe involucrarse con este tipo de operaciones, como colaborar con el establecimiento de controles, la actitud es de mantenerse a puerta cerrada y esto conlleva que no es posible realizar las necesidades de la entidad, puesto que a distancia esta persona es imposible que pueda enterarse de lo que está sucediendo, como consecuencia lejos de colaborar se convierte en un obstáculo y muy negativo a la Clínica.

4.6 Planificación de las mejoras de control

Entre los planes para llegar a un mejor nivel de madurez en el establecimiento de Controles se acordó lo siguiente, siempre con el auxilio de expertos como se mencionó anteriormente.

- **Preparación de Hardware**

Hacer Back ups de archivos de cada PC, en un disco duro portátil que se convierte el Back up general de la clínica, el cual debe mantenerse fuera de la institución en la cajilla de seguridad de un banco, un formateo de la computadora, particionar el disco duro en dos partes (una de sistema, la segunda datos); reinstalación de Windows y programas, regresar archivos del back up, analizando qué archivos son de trabajo y eliminando lo superfluo, reinstalación de antivirus, **bloquear puertos USB y otros puertos de acceso e integrar la red.**

Este método es importante para guardar los archivos, tomando en cuenta posibles fallas de sistema e infecciones de virus. Para mantenimientos posteriores es más sencillo restaurar sistemas caídos o con errores sin perder tiempo en restaurar archivos, el mantenimiento básico lleva 45 minutos en cambio este procedimiento

en cada PC dura alrededor de 4 horas. **Este Proceso será la primera prueba de controles para medición de prevención de riesgos así como reacción del personal de la Clínica, de un nivel 0 de control a un nivel 3 de control.**

- **MEJORAS SERVIDOR**

Considerando el número de Clientes/Usuarios, se elevará la memoria del servidor a 4 GB de RAM y se agregará otro disco duro de 72 GB, lo que dará una capacidad de 216 GB. Es importante que si el sistema de intercambio de datos se presenta lento, puede instalarse físicamente otro procesador para mejorar la velocidad.

SOFTWARE SERVIDOR

Se tomó la decisión de trabajar con Windows Server 2003 Enterprise Edition y después upgrade a Windows Server 2008, y como RDBMS Microsoft SQL Server 2008 Enterprise con crecimiento ilimitado de clientes y Antivirus, NOD 32 versión 3.0621.0. Esto con base a pruebas en la Clínica Isaac Cohen Alcahé, TB, Quetzaltenango.

Figura 34
Modelo de Servidor

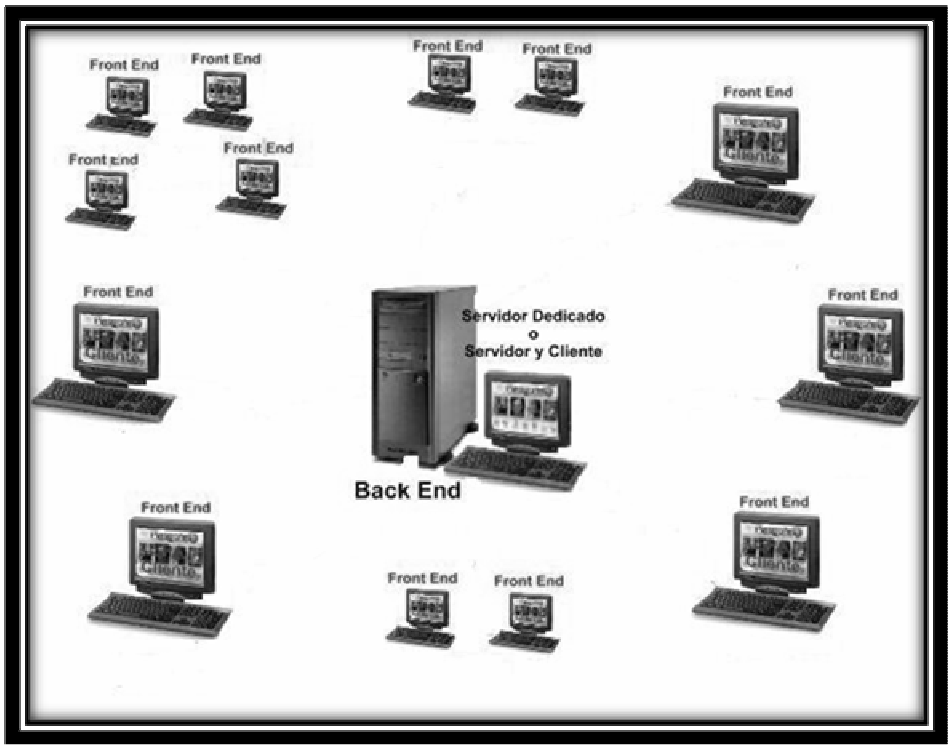
- **CLIENTES HARDWARE**

Del inventario de 49 computadoras, se comprobó que el 61% son adecuadas para cumplir con los requerimientos para entrar en red; tanto en capacidad de disco duro como de Memoria RAM. Es recomendable que el restante 39% se lleve a 1 GB de RAM.

SOFTWARE

Para los clientes se tomó la decisión de Windows XP Professional con Service Pack 3, Microsoft Office 2003 Professional upgrade a Microsoft Office 2007 Professional y antivirus NOD 32 versión 3.0621.0.

Figura 35
Modelo de Red Servidor (Administrador) y Clientes (usuarios)



MODELO DE RED= SERVIDOR Y CLIENTES

- **Cableado**

Actualmente se encuentra en la unidad de informática el centro de cableado, no se encuentran en rack que organice de forma segura y permita una mejor administración de la distribución del cableado; existe un switch de 16 puertos que no se da abasto con los puntos que se necesitan en todas las áreas donde se requiere tener acceso a la red, es más en las oficinas de farmacia, se colocó un switch de 8 puertos para poder redistribuir la señal lo cual no es recomendable, pues genera problemas de rendimiento en la red. El cableado actual no es certificado, lo que no permite seguridad

y no garantiza la señal de red, se deberá hacer el cableado respectivo desde el switch principal en el Rack de datos. Esto con base a recomendaciones tanto de MÉTRICA, como de SERVICIOS INFORMÁTICOS GLOBALES, expertos en el tema de redes certificadas.

Figura 36
Vistas del cableado actual en la Clínica de Enfermedades Infecciosas, Hospital Roosevelt, Abril 2010

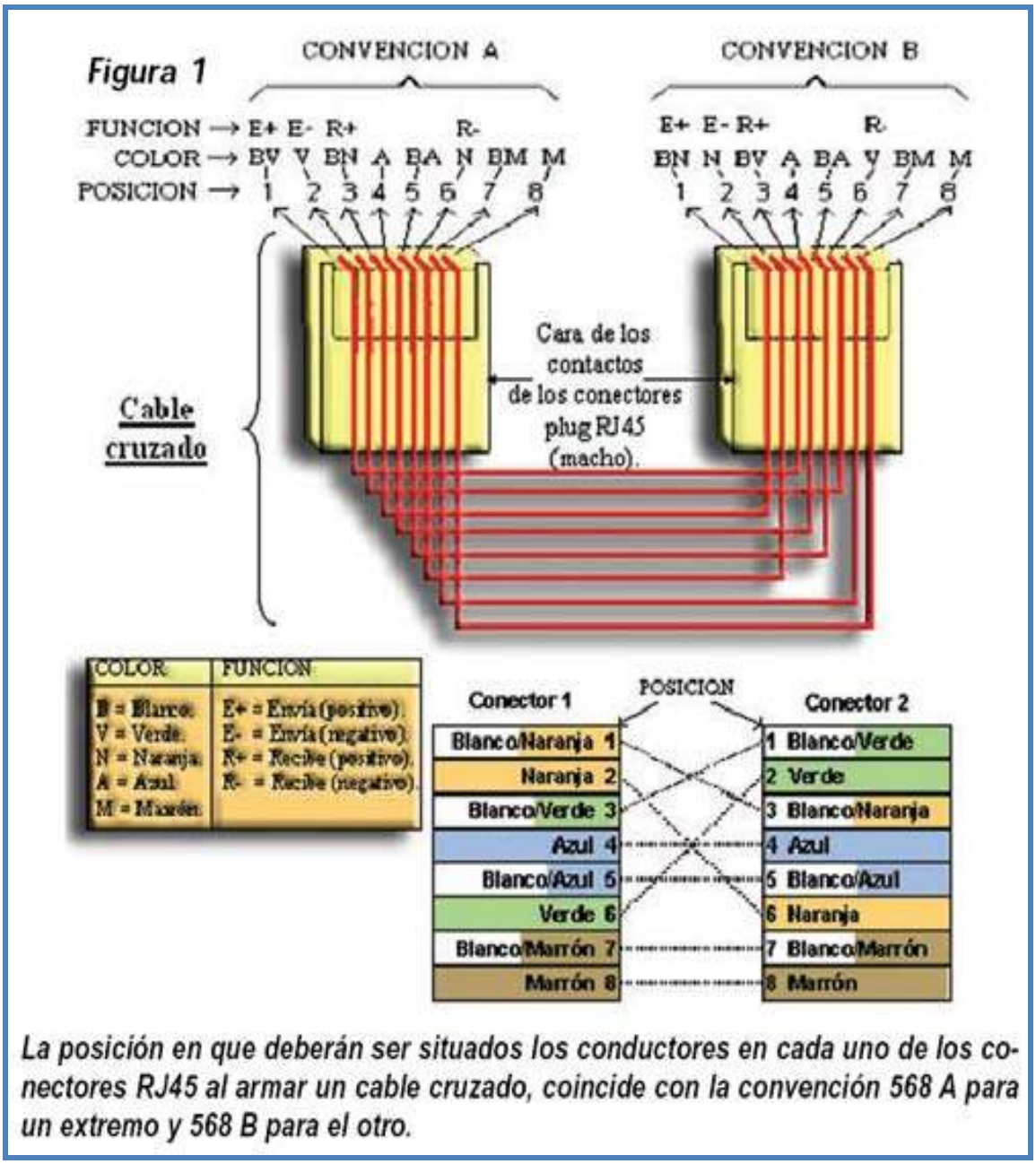
Fuente: Clínica de Enfermedades Infecciosas

- ✓ **Mejoras**

Colocar un Rack que permita realizar la distribución del cableado por medio de un switch de 24 puertos mínimo, se tiene como proyecto poner a funcionar el servidor

HP ML350, como controlador de dominio una estructura física es necesaria y obligatoria. Es recomendable eliminar cualquier otro switch que esté redistribuyendo la señal de red, si se necesitan nuevos puntos de red, se deberá hacer el cableado respectivo desde el switch principal en el rack de datos. Se deberá agregar doce (12) nuevos puntos de red, en estas áreas es necesario realizar el cableado respectivo, siempre que parta del rack de datos y realizar prueba de verificación de puntos de red.

Gráfica 22
Modelo de cableado estructurado y sus certificaciones
Abril 2010



La posición en que deberán ser situados los conductores en cada uno de los conectores RJ45 al armar un cable cruzado, coincide con la convención 568 A para un extremo y 568 B para el otro.

fuente: http://www.guatewireless.org/cableado-de-redes-configuracion-de-colores-del-cable-estructurado-categoria-5e/

Tabla 12
Situación de los puntos de red en la Clínica de Enfermedades Infecciosas, Hospital Roosevelt, Abril 2010

ÁREA	PUNTOS DE RED	
	EXISTEN	FALTAN
Laboratorio de Diagnóstico	1	
Laboratorio de Citometría de flujo	1	
Laboratorio de Biología Molecular	1	
Coordinación	3	
Psicología	1	1
Trabajo Social	0	1
Recepción	1	
Coordinación de Farmacia	0	2
Administración	3	
Secretaria de administración	3	
Digitación	5	
Consejería clínica 8	0	2
Toma de muestras	1	
Despacho de Farmacia A	1	
Procedimientos	0	1
Clínica 1	1	
Clínica 2	2	
Enfermería	0	1
Despacho de Farmacia B	0	1
Nutrición	0	1
Investigación	1	
Ginecología	1	
Clínica 3	1	
Clínica 4	1	
Archivo	1	
Educación	0	1
Laboratorio de Microbiología	0	1
TOTAL	29	12

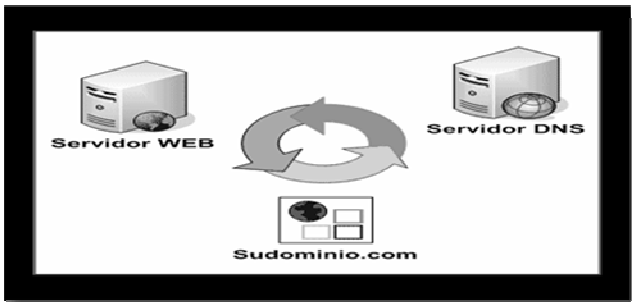
Fuente: Elaboración propia

- **Servicio de hosting para transmisión de datos que reemplaza a Memoria USB**

Características

Nombre del dominio	**@clinicainfecciosashr.com.gt**
Espacio de almacenamiento	80 GB
Transferencia Mensual	1 TB
Estadísticas del sitio Web	Si
Alta Disponibilidad del servidor	Si
Sistema Operativo	MS Windows Server 2008
Servidor Web	Apache 2 IIS 7.0
Seguridad Firewall	Si
Panel de control del Sitio	Si
Soporte	24x7
Características de E-mail	
Cuentas de E-mail	500 cuentas.
Almacenamiento E-mail	3 GB
Acceso Web Mail	Si
MS Exchange Premium E-mail	Expansión

Figura 37
Modelo de dominio



- ✓ **Ventajas del Correo de Dominio**

- La administración de correos es fuera de la oficina
- Se evita el gasto de contar con un servidor de correo dentro de la red
- Se puede configurar Microsoft Outlook para su uso en cada máquina
- Se puede acceder desde cualquier lugar remotamente al correo por medio de webmail.
- Se utilizan servidores localizados en el exterior con todas sus políticas de seguridad a la medida.

4.7 Supervisión y Monitoreo de la primera prueba de controles para medición de prevención de riesgos así como reacción del personal de la Clínica, de un nivel 0 de control a un nivel 3 de control.

De las propuestas en la planificación la totalidad de las mismas fueron aceptadas y aquí comenzó el trabajo de supervisar y darle seguimiento que se cumplieran en su totalidad.

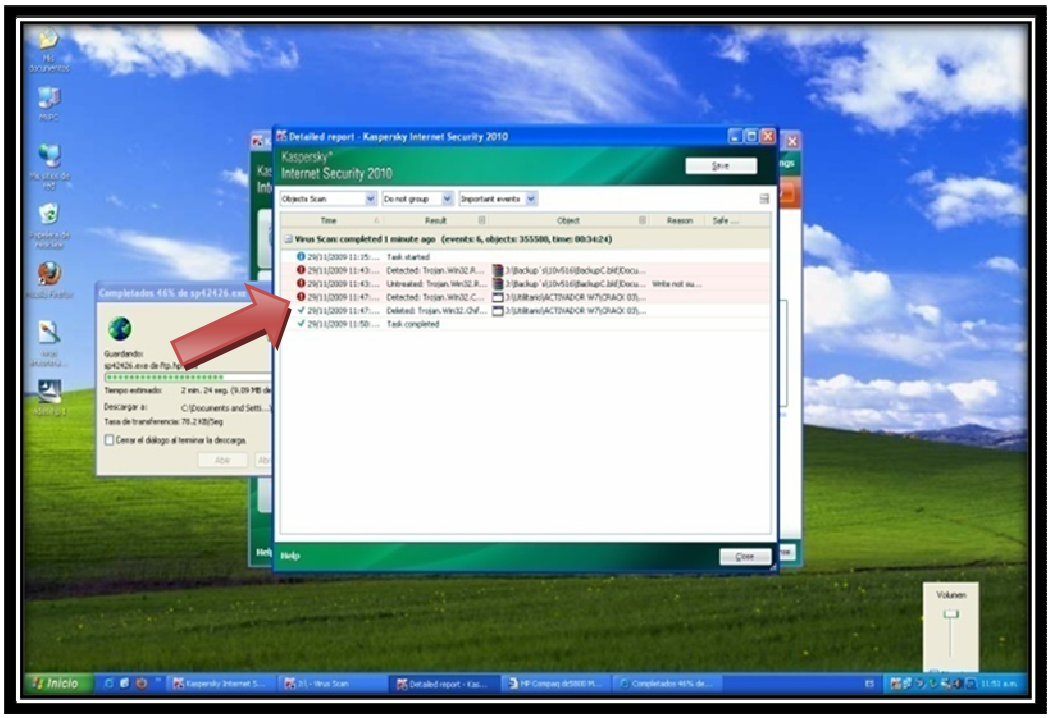
- **Primera prueba de Controles**

Se empezó a realizar el formateo y limpieza de máquinas, cuyo objetivo consistió en la preparación de las mismas para entrar en red, se procedió a la partición de disco, para poder elaborar un back up automático en caso de cualquier infección por virus así como desperfecto físico. Se realizó una limpieza física del equipo que consiste en eliminar polvo que es el mayor enemigo de estos equipos.

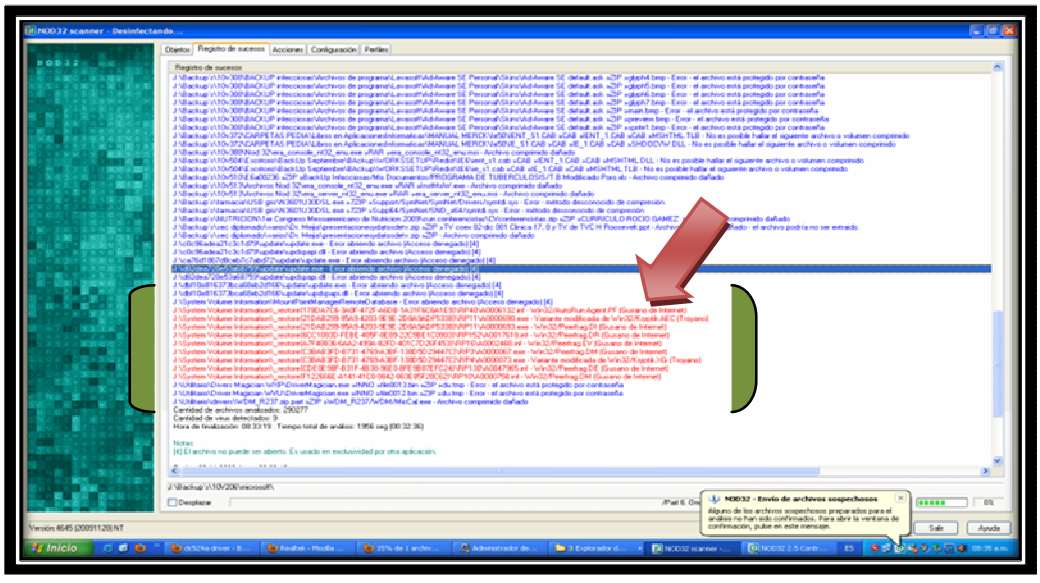
- ✓ Se encontró alta concentración de polvo y parece ser que algunos usuarios se liman las uñas encima del teclado dejando rastros de uñas que provoca que las teclas se traben, así como el polvillo de la lima de uñas que es dañino para el mismo

- ✓ En cuanto a los hallazgos que se encontraron en relación a posibles amenazas, existe una alta contaminación por virus a pesar que varias máquinas habían sido limpiadas con anterioridad, la problemática persiste. Esto sirvió como medición para evaluar riesgos y confirmar la necesidad de cerrar entradas usb y otros puertos de acceso.

Figura 38
Detección de infección por virus en archivos de los usuarios
Abril 2010



Capturas de pantalla de las infecciones por virus



Capturas de pantalla de análisis de solución de seguridad de los diferentes equipos, resaltado en rojo amenazas detectadas

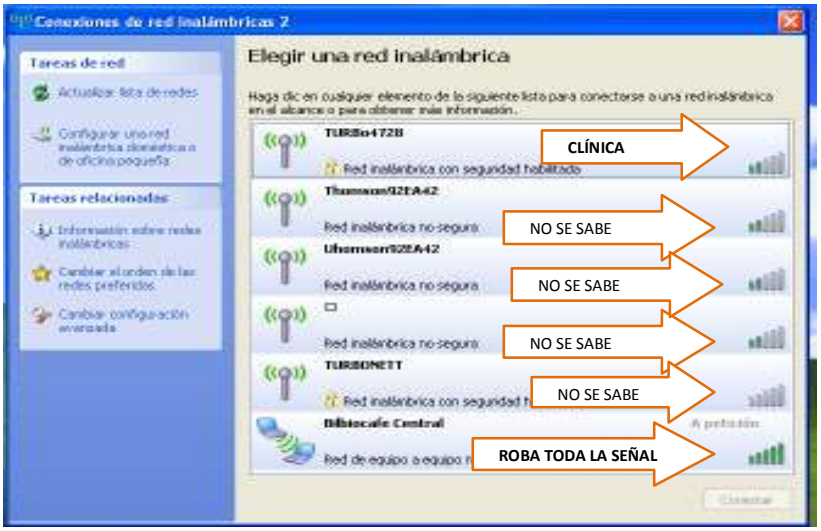
➢ REPORTE DE VIRUS MÁS COMUNES ENCONTRADOS EN LOS EQUIPOS

Virus Scan: completed 2 minutes ago (events: 6, objects: 355580, time: 00:34:24)
03/2010 11:15:39 a.m. Task started
03/2010 11:43:38 a.m. Detected:
Trojan.Win32.RaMag.a:\Backup´s\10v516\BackupC.bkf/Documents_and_Settings\Usuario\Configuraci_n_local\Archivos_temporales_de_Internet\Content.IE5\IJEFG5OJ\help[1].rar

03/2010 11:43:38 a.m. UNTREATED:
Trojan.Win32.RaMag.aJ:\Backup´s\10v516\BackupC.bkf/Documents_and_Settings\Usuario\Configuraci_n_local\Archivos_temporales_de_Internet\Content.IE5\IJEFG5OJ\help[1].rar Write not supported
03/2010 11:47:27 a.m. Detected: Trojan.Win32.Chifrax.aJ:\Utilitario\ACTIVADOR W7\CRACK 03\Windows 7 Activator.EXE/Win7.exe
03/2010 11:47:52 a.m. Deleted: Trojan.Win32.Chifrax.aJ:\Utilitario\ACTIVADOR W7\CRACK 03\Windows 7 Activator.EXE
03/2010 11:50:03 a.m. TASK COMPLETED

- Se encontró vulnerabilidades en el sistema de internet, donde alguien a distancia o cerca de la Clínica está robando la señal para beneficio propio, en este caso bajar música o películas, provocando pérdidas de señal. El sistema está tan vulnerable que cualquier persona con habilidades puede ingresar en el mismo y robar información de las cuentas de correo así como de la información de trabajo, lo cual sucedió y se describe en forma más específica a continuación.

Figura 39
Red inalámbrica de la Clínica con intrusiones
Abril 2010

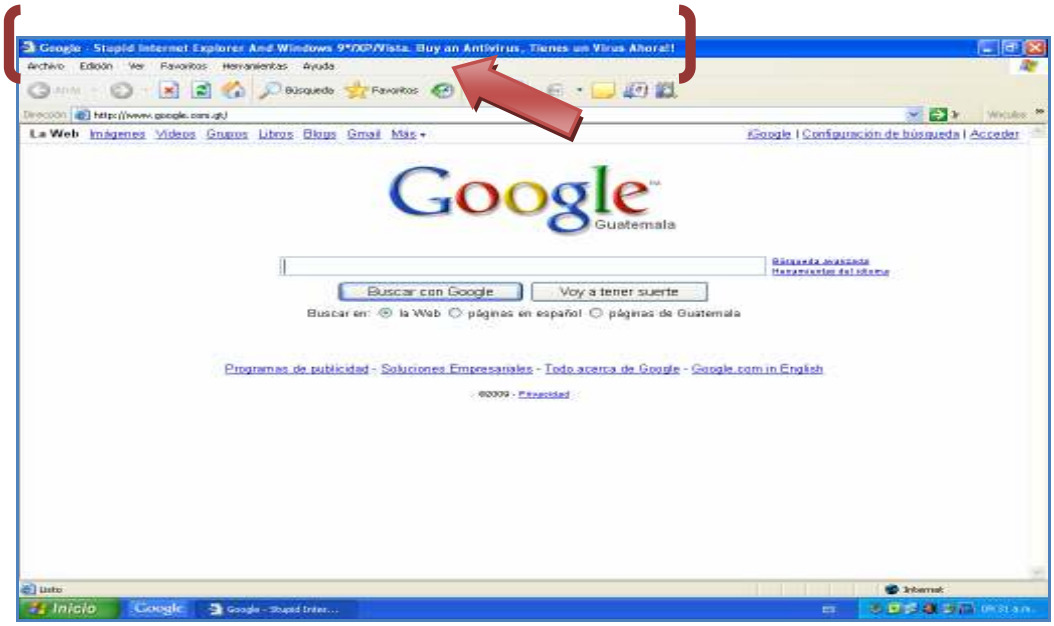


Captura de pantalla del robo de señal, vulnerabilidad en el sistema de internet, señal inalámbrica

Captura de pantalla del robo de señal, vulnerabilidad en el sistema de internet, señal inalámbrica

En esta segunda imagen al momento de actualizar la lista de redes todas las demás se borran sólo se encuentran la red de TURBO4728 y Bilbiocafe Central, en esta misma se observa que la red de TURBO4728 no se encuentra con mayor señal y la de Bilbiocafe Central tiene toda la señal tomada.

Figura 40
Intrusión de un pirata cibernético en computadora de usuario
Abril 2010



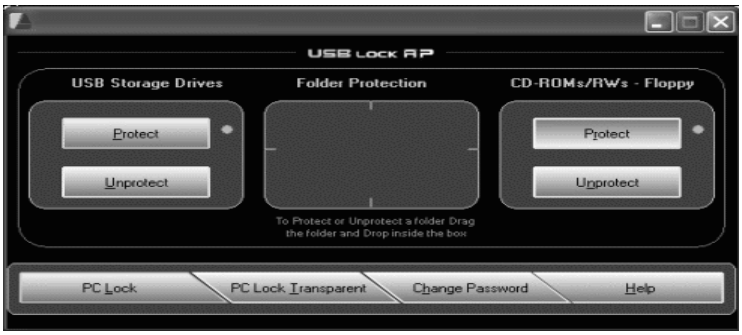
Captura de pantalla de intrusión de pirata Cibernético en la Computadora de un usuario en la Clínica

Esta imagen demuestra que en el navegador, el pirata cibernético dejó un mensaje donde había ingresado al computador de un usuario de la Clínica, dando como resultado que robó la cuenta del mismo y después la usó para cometer un fraude. Escribió a los contactos del usuario que se encontraba en problemas y que le enviaran dinero a una dirección en el extranjero, muchos de los contactos estuvieron a punto de caer en la trampa, pero contactaron al usuario y se comprobó la falsedad del mensaje. El usuario perdió toda su información, y el correo fue bloqueado. La señal inalámbrica es una debilidad para los sistemas en red se recomienda bloquearla y para ingresar debe poseer una clave de acceso segura, esto se puede realizar por medio del proveedor de internet.

- ✓ Otro reporte, tiene que ver con la respuesta de colaboración de las personas que laboran en la Clínica, 90% de las personas entregaron sus máquinas a tiempo, y dos personas reportaron desconocer del proceso, esta fue una Digitadora y la otra la Encargada de Recursos humanos, no realizaron back ups, por lo tanto se perdieron bases de datos de las respectivas áreas.

- **Cierre de puertos USB y otros puertos de acceso: Imágenes del programa USB LOCK AP 2.5 y de IM LOCK: restricciones de navegación e instalación de programas**

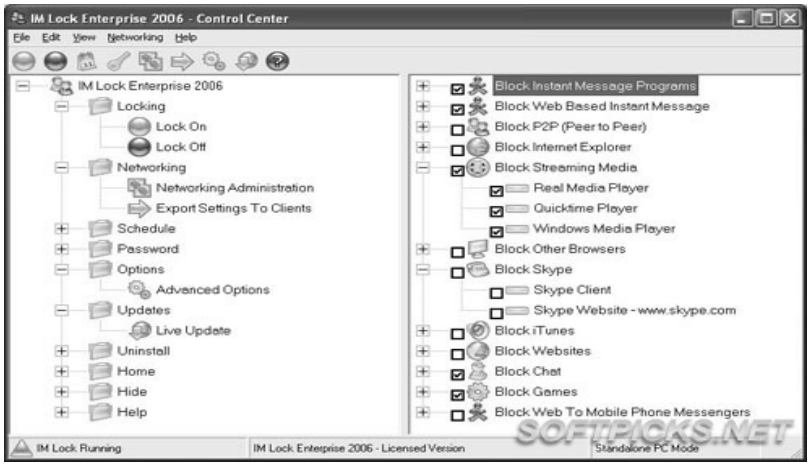
Figura 41
Vista del programa



Captura de pantalla de la aplicación USB LOCK AP

Previene la pérdida de información debido al uso no autorizado de discos removibles USB (Flash sticks, I-Pods, mp3, mp4), CD-ROM, CD-RWs,y Floppy." INFORMACIÓN USB LOCK AP (Auto-Protect); permite prevenir el uso de dispositivos USB removibles, CD-ROM y unidad de disquetes; sin bloquear impresoras USB, cámaras o el ratón. También ofrece protección de carpetas mediante el método de arrastrar y soltar, sin cambiar la ubicación de las mismas. Además permite la función de bloquear el ordenador (transparente) siendo posible ver el lo que está en el monitor. * Interfaz protegida por contraseña encriptada.

Figura 42
Vistas de la Aplicación IM Lock Professional-Control Panel



Capturas de pantalla de la aplicación IM LOCK Enterprise

IM LOCK Enterprise es una utilidad para bloquear páginas web y aplicaciones a las que no se quiere que accedan los usuarios, bloquea desde programas de mensajería instantánea, tipo MSN Messenger, páginas de chat, juegos basados en web y páginas de correo electrónico como Hotmail, Gmail, Yahoo Mail, etc. Por defecto, también bloquea páginas como Flickr o YouTube, aunque es la entidad la que decidirá qué bloquea y qué no. Eso sí, no podrá añadir a mano páginas ni programas a bloquear **(no está disponible en la versión "Home").**

4.7.1 Estado del Entorno de Control Interno en base al Dominio Adquisición e Implementación después de la primera prueba de controles.

En este dominio el enfoque hacia los requerimientos de riesgo y control es ad hoc y desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están concientes de sus responsabilidades, por ejemplo en elección de proveedores, software, y hardware, que sea el más adecuado. Todavía hay que insistir en la elección de los mismos, no hay consultas sobre qué compra es mejor, siguen con conocimientos intuitivos.

- **Establecimiento de Control Interno: Sugerencia**

Debe existir la conciencia de la necesidad de evaluar lo que se necesita en términos de controles TI. Cuando se llevan a cabo, son solamente de forma ad hoc, a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente y no planean. Las metas no están claras y no existen las mediciones, con respecto a qué recursos se necesitan en el ambiente TI. La administración de la Clínica establece como solución a la medida la aplicación INTEGRA; pero no es convencimiento de todos, alguno se inclinan por el programa MANGUA, ejemplo en el área de los Químicos-Biólogos; debe existir unidad de pensamiento. La mayoría de personas que laboran en la Clínica tienen un conocimiento muy bajo sobre plataformas de sistemas operativos o suites de trabajo, lo que hace difícil que este dominio tenga una mejor calificación de madurez. En las compras de equipo de cómputo, no se dejan llevar por calidad y especificaciones de trabajo sino por precio, que a veces resulta no ser bajo sino más bien alto dentro del mercado. La situación que se encontró con el

cableado es un ejemplo, al momento de instalar los puntos de red que se necesitaban se determinaron deficiencias en el mismo, pues no era certificado lo que generó problemas de conectividad así como el problema de licenciamiento. Se recomienda que un Consejo de Arquitectura, con la gente más preparada en Tecnología de la Información entre a tomar decisiones sobre las compras de hardware, instalaciones de cableados, seguridad física y lógica del sistema de la Clínica, esto debe realizarse de forma inmediata.

Figura 43
Papel de trabajo: Cédula centralizadora del dominio Adquirir e implementar
Abril 2010

P/T	ADQUIRIR E IMPLEMENTAR	
	Auditor	Fecha
Hecho	M.M	/04/2010
Revisado	AJGB	/04/2010

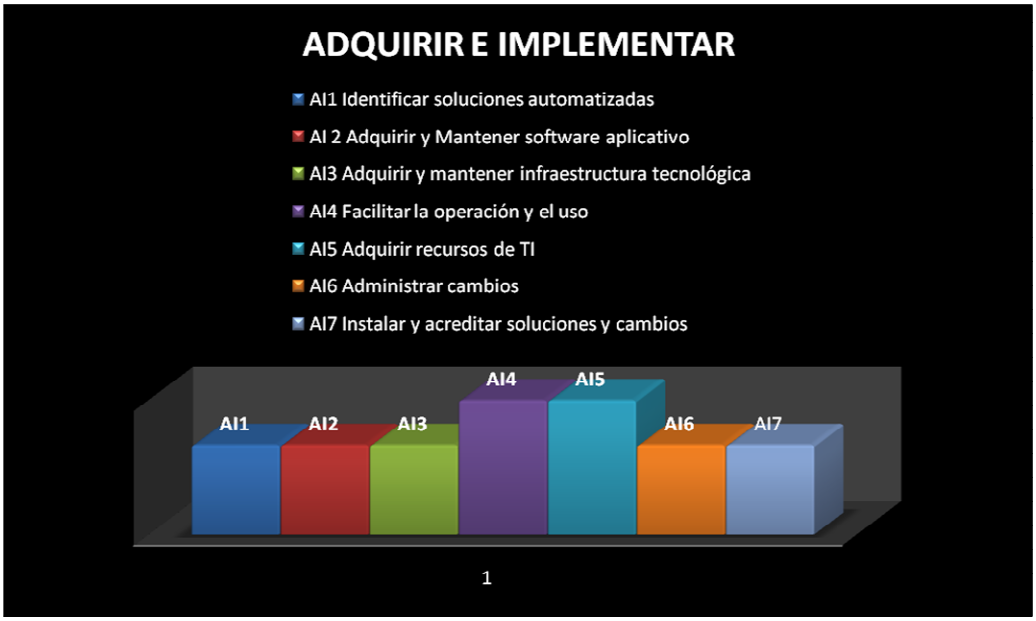
ADQUISICIÓN E IMPLEMENTACIÓN
DOMINIO DE CONTROL

	No. Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
AI1 Identificar soluciones automatizadas						
AI2 Adquirir y mantener software aplicativo						
AI3 Adquirir y mantener infraestructura tecnológica						
AI4 Facilitar la operación y el uso						
AI5 Adquirir recursos de TI						
AI6 Administrar cambios						
AI7 Instalar y acreditar soluciones y cambios						

promedio total = 1

Fuente: Elaboración propia

Gráfica 23
Calificación del dominio Adquirir e Implementar
Abril 2010



Fuente: Elaboración propia. Nivel de Madurez 1

4.7.2 Estado del Entorno de Control Interno en base al Dominio Entregar y dar Soporte después de la primera prueba de controles.

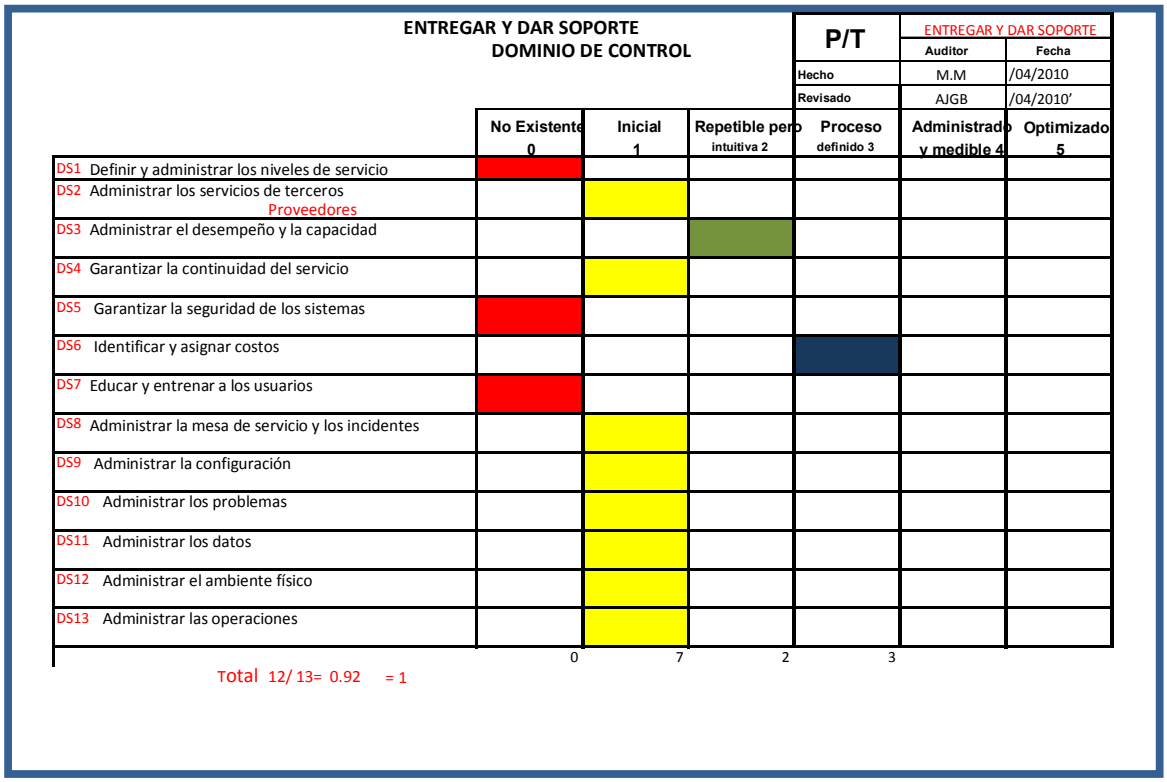
En este dominio el enfoque hacia los requerimientos de riesgo y control está en el mismo nivel que Adquisición e Implementación ad hoc y desorganizado. No se identifican las deficiencias. Los empleados no están concientes de sus responsabilidades, en cuanto al área de selección de proveedores, no hay planes de contingencia en caso de incidentes, la sombra de echarle la culpa aparece en el ambiente de control, haciendo parecer que sin controles todo caminaba perfectamente.

- **Establecimiento de Control Interno: Sugerencia**

Debe existir la conciencia de la necesidad de evaluar lo que se necesita en términos de controles TI en este dominio. Cuando se llevan a cabo, son solamente de forma ad hoc, a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente y no planean. Las metas no están claras y no existen las mediciones, en este caso se menciona la problemática de no saber analizar sobre qué

bases elegir proveedores de tecnología, se encuentra que muchas de las compras son sugeridas, no hay independencia de criterio ni conocimiento sobre lo que más conviene a la clínica, no hay una creación de estándares sobre quiénes deben ser elegidos dentro de una base de datos de proveedores, en la cual debe considerarse estabilidad del negocio, garantías de conocimiento por parte del proveedor. En el momento de un cambio de no control a control, la administración enfrenta problemas, no puede dar respuesta inmediata, por la apatía que algunas personas, que desean que todo siga como estaba; lo que logra es generar dudas en los demás. Administración de datos es deficiente a la hora de perder información, no existen respaldos de esa base, y hay dueños de procesos que se paralizan. La operatoria se puede ver comprometida fácilmente por cualquier incidente no hay preparación para enfrentarlos.

Figura 44
Papel de trabajo: Cédula centralizadora del dominio Entregar y dar Soporte
Abril 2010



ENTREGAR Y DAR SOPORTE
DOMINIO DE CONTROL

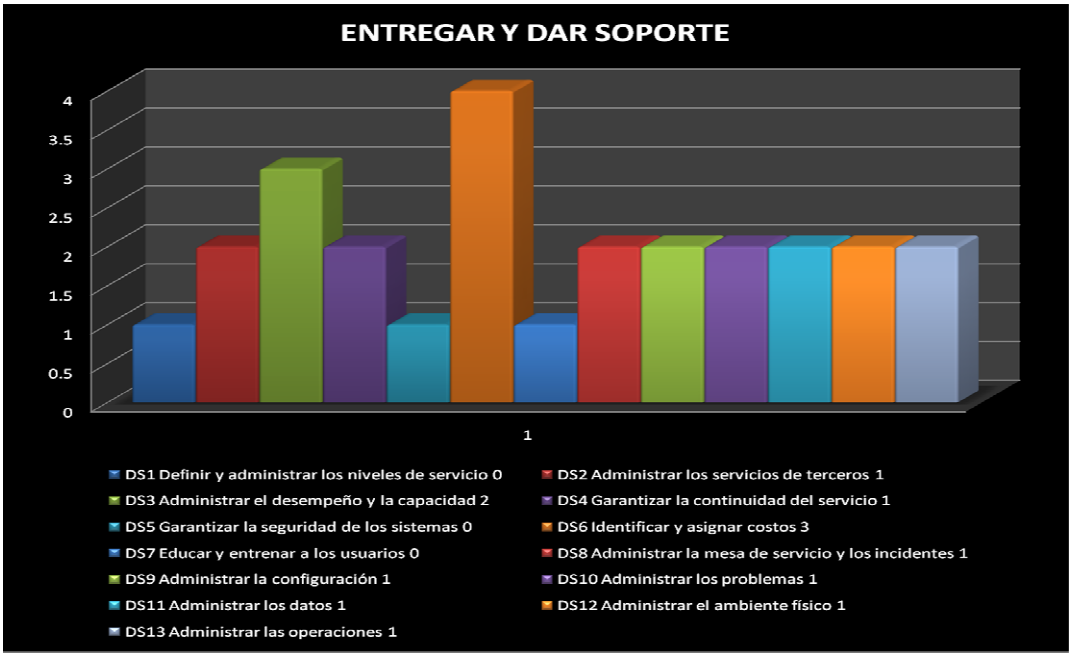
P/T	ENTREGAR Y DAR SOPORTE	
	Auditor	Fecha
Hecho	M.M	/04/2010
Revisado	AJGB	/04/2010'

	No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
DS1 Definir y administrar los niveles de servicio						
DS2 Administrar los servicios de terceros Proveedores						
DS3 Administrar el desempeño y la capacidad						
DS4 Garantizar la continuidad del servicio						
DS5 Garantizar la seguridad de los sistemas						
DS6 Identificar y asignar costos						
DS7 Educar y entrenar a los usuarios						
DS8 Administrar la mesa de servicio y los incidentes						
DS9 Administrar la configuración						
DS10 Administrar los problemas						
DS11 Administrar los datos						
DS12 Administrar el ambiente físico						
DS13 Administrar las operaciones						
	0	7	2	3		

Total 12/ 13= 0.92 = 1

Fuente: Elaboración propia

Gráfica 24
Calificación del dominio Entregar y Dar Soporte
Abril 2010



Fuente: Elaboración propia. Nivel de Madurez 1

4.7.3 Métricas de Control

La primera prueba de control, que se puede denomina como **Fase I del establecimiento de controles,** demostró que no hay suficiente nivel de madurez en los dominios Adquisición e Implementación como el de Entregar y dar Soporte, ahora por medio del dominio Monitoreo y Evaluación se podrá comprobar si la Administración sigue adelante con los controles, o no hay convencimiento, los retiran y buscan otros. Este proceso define indicadores de desempeño relevantes, reportes sistemáticos y oportunos, toma de medidas expeditas cuando existan desviaciones. Este dará como resultado garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas. Se comparará el desempeño con las metas acordadas e iniciar medidas correctivas, se mide con la satisfacción de la administración, número de acciones de mejoramiento impulsadas por las actividades de monitoreo. Porcentaje de procesos críticos monitoreados.

Es importante tomar en cuenta que en un establecimiento de controles, la responsable de implementarlos es la Administración y los auditores solamente colaboran en diseñar el mejor modelo que se adapte a la organización. El auditor sugiere, por eso éste se enfrenta a los siguientes retos:

- Concientizar a la Alta Dirección

- Resistencia en la modificación de la cultura organizacional: Concientizar a los trabajadores sobre su obligación de conocer y aplicar la normativa en materia de seguridad informática **(MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA), (MANUAL DE SELECCIÓN DE PROVEEDORES); (MANUALES DE APLICACIÓN A LA MEDIDA).** Esto logra un cambio favorable en la cultura organizacional.

- Atender a las exigencia legales, reglamentares y los conflictos entre las propias leyes/reglamentos como las estrategias de la organización.

- ✓ Sobre el primer reto se recibió una copia de una comunicación del Jefe de la Clínica sobre la primera Fase de establecimiento de controles a todos los empleados de la Clínica, el cual decía textualmente:

"Como todos han sido testigo en las últimas dos semanas se terminó el formateo de las computadoras, así como el bloqueo de funciones específicas como memorias USB y de uso de CD en las computadoras. Se repartió hace un poco más de dos semanas el normativo de seguridad informática, del cual dado que no hubo observaciones, está vigente desde hace una semana. El cual se espera que todos lo observemos de manera estricta. Es importante que el personal a cargo de su área, SIN EXCUSA, lo

cumpla, pues la inversión realizada en tiempo, dinero y trabajo ha sido muy importante. RECUERDEN QUE NO SE PUEDE GUARDAR BACK-UPS en el escritorio y todo debe ser almacenado en MIS DOCUMEMTOS. LAS COMPUTADORAS QUE ESTÉN EN LÍNEA CON EL SISTEMA HOSTING (dirección electrónica específica de cada persona individual de la clínica, para uso como INTRANET, será instalada en los próximos días, para lo cual NO ME GUSTARÍA saber que tengamos excusas de que nadie sabía lo que había que hacer. Auditorías NO PROGRAMADAS se harán en los equipos para evaluar el cumplimiento normativo, el cual les pido comuniquen al personal a su cargo los próximos días."

Doctor Carlos Mejía Villatoro
Jefe Unidad de Enfermedades Infecciosas y
Coordinador de Post-grado de Enfermedades infecciosas
Hospital Roosevelt

Derivado de lo anterior se pudo obtener un mayor convencimiento en seguir adelante con los controles y de establecerlos lo que promueve una mejor calificación en el dominio de Monitoreo y Evaluación, empiezan a corregir lo que está mal, y tener una meta sobre objetivos claros de control el cual los llevará al éxito de una administración de red con menor número de riesgos en incidentes.

- ✓ Segundo reto elaborar un **Manual de elección de proveedores (Anexo)**, cualidades y calificaciones de un buen proveedor en el área de tecnología de la información. Cumplir y utilizar correctamente los otros manuales. Esto mejorará los dominios de Adquisición e implementación como el Entregar y Dar Soporte.

- ✓ El tercer reto de aprobarse la donación de licencias por parte de MICROSOFT que tiene una valuación de US$ 44,818.00 (Q 371,989.40) el cumplimiento con este objetivo llevaría a la institución tanto en el Dominio Planeación y Organización,

como Adquisición e implementación a subir automáticamente un punto más en la madurez del respectivo dominio.

- ✓ El último reto a citar es que si los usuarios cumplen con guardar toda la información en **mis documentos,** automáticamente se está realizando con éxito el back up debido al proceso de partición de disco, cualquier problema de contaminación o fallas de hardware, ya no existen riesgos de pérdidas de datos y el formateo es más fácil.

4.7.4 Cuadro de rendimiento de Control del dominio Monitoreo y Evaluación

Figura 45
Papel de trabajo: Cédula centralizadora del dominio Monitorear y Evaluar
Abril 2010

P/T	MONITOREAR Y EVALUAR	
	Auditor	Fecha
Hecho	M.M	/04/2010
Revisado	AJGB	/04/2010

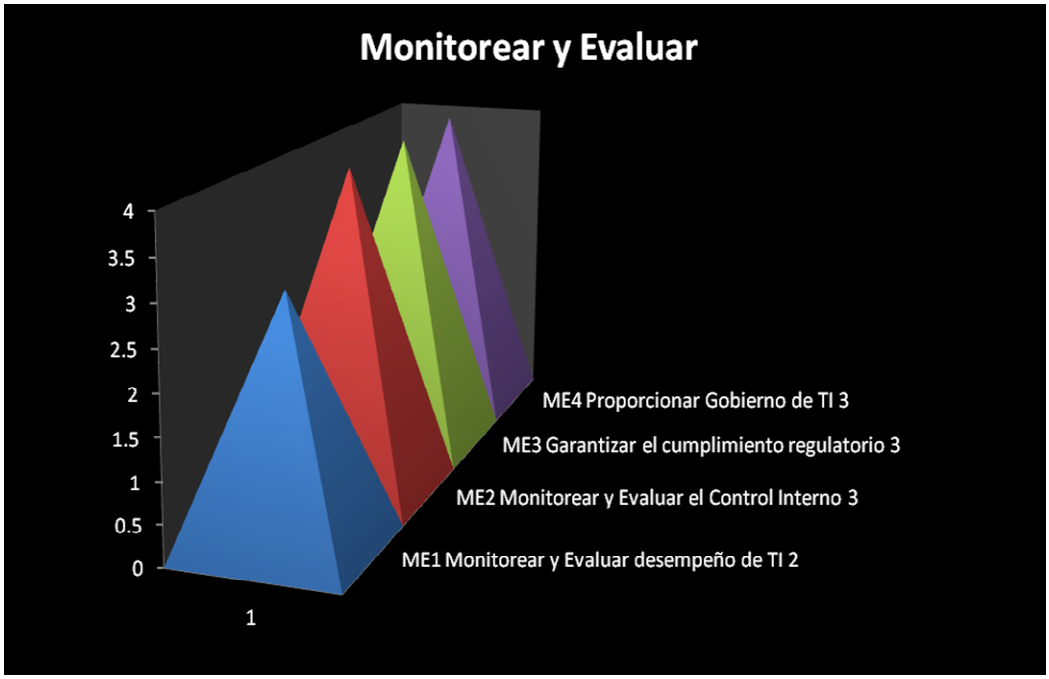
MONITOREAR Y EVALUAR
DOMINIO DE CONTROL

	No Existente 0	Inicial 1	Repetible pero intuitiva 2	Proceso definido 3	Administrado y medible 4	Optimizado 5
ME1 Monitorear y Evaluar el Desempeño de TI						
ME2 Monitorear y Evaluar el Control Interno						
ME3 Garantizar el Cumplimiento Regulatorio						
ME4 Proporcionar Gobierno de TI						

total del Dominio = 3

Fuente: Elaboración propia

Gráfica 25
Calificación del dominio Monitorear y Evaluar
Abril 2010



Fuente: Elaboración propia. Nivel de Madurez 3

- **¿Qué significa para la Entidad esta calificación de madurez?**

Es importante analizar que dos dominios dieron una calificación de madurez muy baja, **AI Y DS: 1** inicial, en cambio si se analiza **PO así como ME en un nivel 3**, existió una planeación de prueba de controles, durante dos semanas la Administración se encuentra más convencida de lo que se implementó como modelo de control. El objetivo era llevar todos los dominios a nivel de madurez 4, pero esto es difícil para una entidad que apenas empieza con controles, pero que va por buen camino. COBIT 4.1, indica que debe proceder a establecer controles en orden, pero pueden existir dominios con mejores calificaciones que otros. Es importante resaltar el buen ambiente de control y concientización en un porcentaje importante de personas que laboran en la Clínica. Sugiere que las direcciones que se han tomado son las correctas, cada vez más personas, comprobarán el beneficio de la seguridad informática así como su relevancia. Nivel 3 de madurez en Monitoreo y Evaluación, la Administración entiende la necesidad de tomar control de su información, la gerencia es más formal y

estructurada, ya se tomó la iniciativa de traer alguien más capacitado en informática y comenzar a convertir Informática en lo que debe ser un Gobierno en TI, que reporte a la Jefatura de la Clínica. Existe un convencimiento de buenas prácticas, los procesos, políticas y procedimientos cada vez más se definen y documentan para todas las actividades clave. Existen ya planes para el uso y estandarización de las herramientas para automatizar el proceso. Se definen y documentan los requerimientos y habilidades para todas las áreas. Existen planes de entrenamiento de los usuarios formal pero todavía se basan en iniciativas individuales. La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los dueños de los procesos de la organización. No existe una autoridad plena para el dueño del proceso. Se empiezan aportar ideas extras al **Manual de Políticas de Seguridad (ver Anexos);** como la persona que tenga que realizar una conferencia y su presentación es en Power Point, la mandará por correo electrónico para ser analizada por la solución de seguridad de la entidad, previo a presentación.

4.8 Análisis beneficio económico de acuerdo con COBIT 4.1: ALINEACIÓN DE COSTOS TI. PO5 Administrar la Inversión de las TIC

Tabla 13
Reporte de gastos según clasificación de cuentas
Abril 2010

CÓDIGOS			DESCRIPCIÓN		
CATEGORÍA	CUENTA	SUBCUENTA		COSTOS	DONACIÓN
02	000	000000	INFRAESTRUCTURA Y EQUIPOS GASTOS MAYORES US$1000.00		
02	811	811000	INFRAESTRUCTURA Y EQUIPOS MAYORES		
02	811	811004	Software y Licencias de Computación		
			1 licencia SQL Svr Standard Edition 2008 Spanish- 1 processor ; 1 Windows Svr Ent 2003 R2 w/SP2 32bit/x64 Spanish 50 licencias Office Professional Plus 2007/Win 32-Spanish 50 licencias y 50 licencias Windows XP Professional w/SP3 32 bit Spanish.	US$ 44,818.00	↔
02	811	811002	Equipo de Computación e Informática		
			Servidor HP Proliant ML 350 1.6 GHz, 8MB Cache, memoria RAM de 1 GB, 2		

			discos duros de 72 GB con quemadora de DVD, controlador de red (controlador integrado HP NC 373i Multifunción Gigabit 10/100/1000 WOL)	**US$ 2,100.00 COMPRADO EN 2008**	
			Programa INTEGRA, Software a la medida	**US$ 6,100.00**	pendiente de instalación
03	**000**	**000000**	**CAPACITACIÓN**		
03	802	802003	Honorarios por Consultorías		
			300 Horas Hombre de trabajo en supervisión y asesoría informática, costo Q 150.00 HH (US$ 20.00)	**US$ 6,000.00**	↔
02	812	812000	**INFRAESTRUCTURA Y EQUIPOS MENORES GASTOS MENORES S$1000.00**		
02	812	812001	Equipo de Computación		
			1 disco duro portátil de 1TB capacidad, marca I-Omega	**US$ 211.00**	
			Disco duro HP de 72 GB y dos memorias RAM de 1 GB y 2GB, respectivamente marca HP	**US$ 812.00**	**Pendiente disco duro de 72 GB**
02	812	812003	Software y Licencias de Computación		
			Servicio Hosting con dominio para 1 año	**US$ 446.00**	**Pendiente de instalación**
08	840	840000	**GASTOS ADMINISTRATIVOS DE LOCAL**		
08	840	840004	Reparaciones y mantenimiento de Local		
			Formateo de computadoras e incluye Back Ups, reinstalación de software, antivirus	**US$ 950.00**	
			12 cableados de punta de red y 1 switch de 24 puertos	**US$ 430.00**	
			Prueba de verificación de puntos de red (incluye conectores y dados de conexión)	**US$ 140.00**	
			Mejoras de Cableado por fallas del actual		
			Opción A: un solo switch de 48 puertos, cambio de cable con protección marcas económicas	**US$ 2,050.00**	**A considerar**
			Opción B: un solo switch de 48 puertos, cambio de cable con protección marca Dell	**US$ 3,374.00**	**A considerar**
			Opción C: Con marcas de cable estructurado	**US$ 5422.00**	**A considerar**

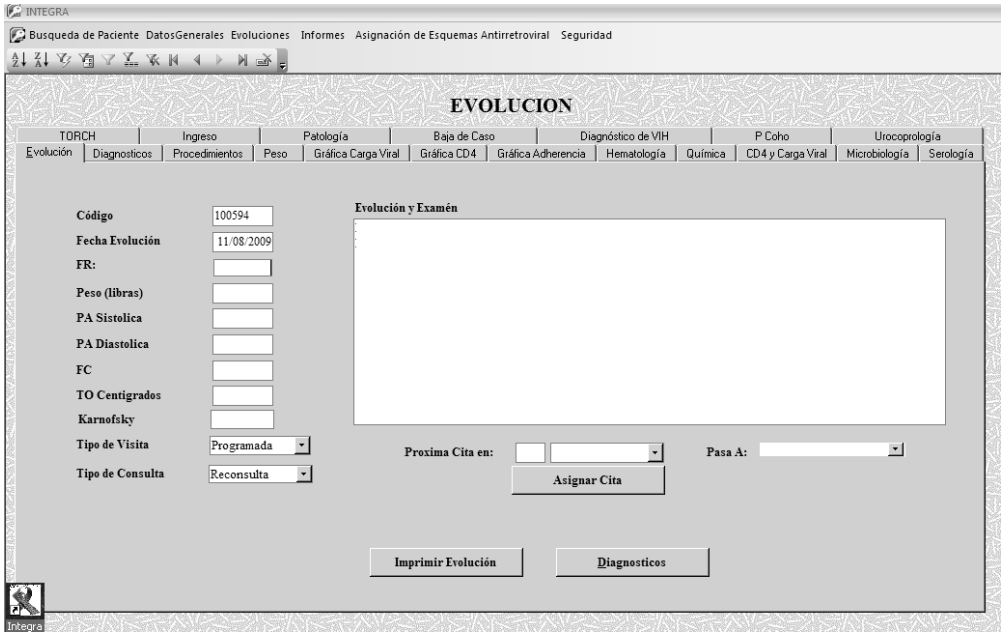
Fuente: Elaboración propia

Se pudo manejar el proyecto con donaciones, porque esta entidad posee un techo en su presupuesto por lo cual aplica a recibir las mismas y se buscaron las opciones de mejoras de la gestión de seguridad sin un exagerado gasto para la institución la cual opera para beneficio de la salud en el país. Se utilizó el modelo de presupuesto del Proyecto.

4.9 Propuesta de mejoras para la administración de calidad del programa INTEGRA.

- **GESTIÓN Y REPORTES MÉDICOS** MÓDULO 1

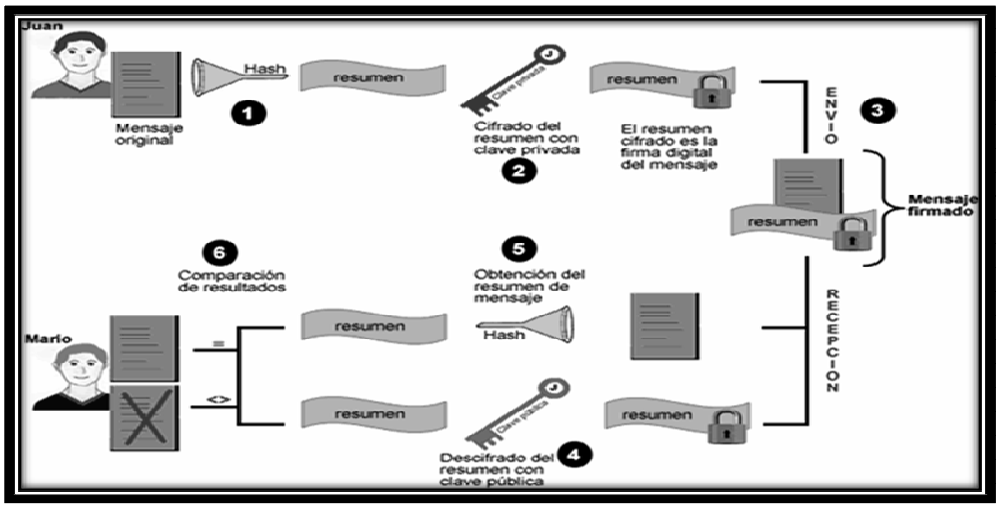
Figura 46
Historia Clínica Electrónica



Captura de pantalla, historia clínica electrónica (INTEGRA)

IMPLEMENTACIÓN: INCORPORAR BASES DE DATOS DE DIGITACIÓN, ESCANEAR ARCHIVOS PDF, RESPALDO DE LA HISTORIA CLÍNICA ELECTRÓNICA E INTEGRAR IMÁGENES COMO RADIOGRAFÍAS. IMPLEMENTAR FIRMA DIGITAL.

- **Modelo de firma electrónica encriptada para los médicos**



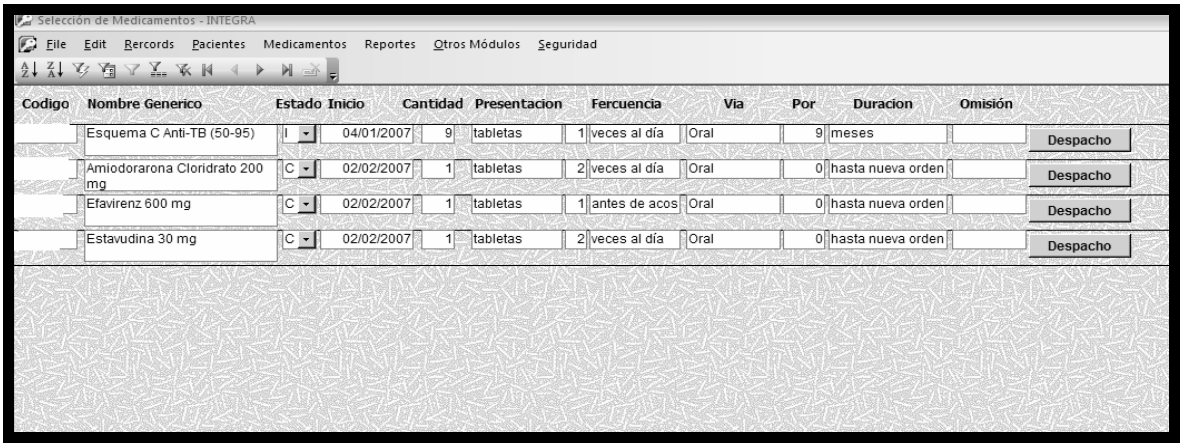
FUENTE: ***Decreto 47-2008, Ley para el reconocimiento de las comunicaciones y firmas electrónicas, publicado en el Diario Centroamérica el 23 de Septiembre 2008.***

SIGNOS VITALES: NO HAY AUTOMATIZACIÓN, PAPELETAS SE ENVÍAN A MÉDICO. DEBE ENTRAR EN BASE DE DATOS Y ENVIARSE AUTOMÁTICO, NO PAPELES. NECESITA IMPLEMENTARSE DENTRO DE INTEGRA. SIGNOS VITALES PRESIÓN ARTERIAL, FRECUENCIA CARDÍACA, TEMPERATURA Y PESO. EXISTE SOFTWARE QUE PUEDE AUTOMATIZAR ESTA ACTIVIDAD.

- **GESTIÓN Y REPORTES DE FARMACIA** MÓDULO 2 (MANUAL)

Este programa no permitirá el despacho duplicado del mismo medicamento para el mismo paciente durante el mismo día., para evitar la duplicidad de egresos accidentales. Pero debe existir un código que pueda dar un cierto número de excepciones en caso de que pacientes sean asaltados, este código de acceso lo tiene el administrador del programa.

Figura 47
Hoja electrónica de selección de medicamentos



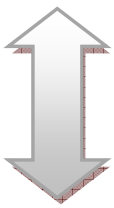
Captura de pantalla, Selección de medicamentos (INTEGRA)

IMPLEMENTACIÓN DE FIRMA BIOMÉTRICA DEL PACIENTE CUANDO RECIBE MEDICAMENTO (HUELLA DIGITAL).

Figura 48
Modelo firma biométrica

FUENTE: ***Decreto 47-2008, Ley para el reconocimiento de las comunicaciones y firmas electrónicas, publicado en el Diario Centroamérica el 23 de Septiembre 2008***

- **Gestión Secretaria**



IMPLEMENTACIÓN HUELLA DIGITAL = NO CARNET/SIN PAPEL

- Gestión y reportes de tránsito de Muestras de Laboratorio MÓDULO 6

MÁQUINA ROCHE, INTEGRARLA A LA RED PARA QUE PRODUZCA REPORTES

CONCLUSIONES

1. La investigación de las prácticas de gestión de TI en la Clínica de Enfermedades Infecciosas ha revelado que no optimizan su inversión en TI. El factor diferenciador para conseguirlo radica en la participación de la administración en dichas decisiones lo que aportará un valor real a la inversión en TI al tiempo que sirven para evitar desastres relacionados con las TIC. Se debe diferenciar entre decisiones estratégicas y operacionales, y dichas decisiones deben estar alineadas con los planes estratégicos y operacionales de la organización, y es allí donde cobra valor el utilizar COBIT como herramienta guía.

2. La Clínica de Enfermedades Infecciosas toma en cuenta ahora que hay numerosos cambios en TI y en la construcción de redes que hacen énfasis en la necesidad de manejar mejor los riesgos relacionados con las TIC. La dependencia de la información electrónica y de los sistemas de TI es esencial para respaldar procesos críticos de la entidad. Las organizaciones exitosas necesitan manejar mejor la compleja tecnología que predomina en toda su estructura para responder rápida y seguramente a las necesidades de la entidad. Además, el entorno regulador está exigiendo un control más estricto sobre la información.

3. La Clínica de Enfermedades Infecciosas comienza a cumplir con requerimientos de calidad, de confianza y de seguridad, tanto para su información, como para sus activos. La Administración optimiza el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus objetivos como lo es automatizar las operaciones de atención al paciente, la administración entiende el estado de sus propios sistemas de TI y decide el nivel de seguridad y control que deben proveer estos sistemas. Aceptan que poseen dominios débiles en madurez, que deben lograr una optimización o como se conoce alcanzar las Buenas Prácticas en el área de tecnología.

4. El proceso de implantación de gobierno de TI asiste a los diferentes niveles en este caso a la Clínica de Enfermedades Infecciosas con una detallada hoja de ruta que le ayuda en la implementación de sus necesidades de Gobierno TI usando COBIT. Identifica qué componentes de COBIT deben ser mejorados desde las necesidades iniciales hasta la implantación de la solución. La hoja de ruta presenta un proyecto que puede ser largo y que requiere prácticas estrictas de gestión de proyectos.

RECOMENDACIONES

1. Que la Clínica de Enfermedades Infecciosas se comprometa a continuar mejorando la seguridad informática de la organización, y que un Consejo de Arquitectura de la Información, con la gente más preparada en Tecnología entre a tomar decisiones sobre las compras de hardware, instalaciones de cableados, seguridad física y lógica del sistema de la Clínica, esto debe realizarse de forma inmediata.

2. La Clínica de Enfermedades Infecciosas que tiene como objetivo entrar en red debe hacer énfasis en la necesidad de manejar los riesgos relacionados, se demostró mediante la primera prueba de controles lo comprometida que estaba la seguridad de datos de la clínica, expuesta a posibles robos por parte de empleados u otros. Deben asignarse claves de acceso a los equipos, pero con copia a la alta dirección, donde se cambien periodicamente. Todo esto a favor del rendimiento de la red que pronto piensan poner en funcionamiento; pero lo más importante en beneficio de los pacientes de la clínica para la salvaguarda de la información de los mismos.

3. Que la administración de la Clínica en el cumplimiento de calidad en la gestión de seguridad informática implemente el **Manual de Selección de Proveedores (Anexo).** Esto en beneficio de los recursos de TI, que adquiera de ahora en adelante, cumplir con estándares bien definidos para elección de los mismos, mantener la infraestructura de seguridad así como una capacitación constante de los usuarios, para que los recursos sean utilizados de la manera correcta, esto hará que los dominios **Adquisición e Implementación así como Entrega y Soporte** eleven el nivel de madurez que se necesita.

4. La Clínica de Enfermedades Infecciosas desde ahora y para siempre debe tomar como su hoja de ruta en la gestión de TI, lo siguiente: Identificar sus necesidades, analizar dichas necesidades, planearlas e implementarlas, siempre acompañadas por objetivos de control que le proporciona COBIT, como herramienta guía. Esto puede dar la sensación de que tomará mucho tiempo, pero es mejor lo planificado y analizado, que lo intuitivo, como se estaba realizando anteriormente en la inversión de TI.

BIBLIOGRAFÍA

1. Coopers & Lybrand e Instituto de Auditores Internos de España. Los Nuevos Conceptos de Control Interno (Informe COSO), Ediciones Díaz de Santos, S.A., Madrid 1997 407pp.

2. Federación Latinoamericana de Auditores Internos, El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial, 2004. 126pp.

3. Instituto Mexicano de Contadores Públicos, AC. NORMAS INTERNACIONALES DE AUDITORÍA. Novena edición, octubre de 2007.

4. IT Governance Institute, **"COBIT 4.1 Control Objectives, Management Guidelines and Maturity Models".** (Quinta Edición, Estados Unidos de América, 2007). 196pp.

5. IT Governance Institute, **"COBIT 4.0 Control Objectives, Management Guidelines and Maturity Models".** (Cuarta Edición, Estados Unidos de América, 2005). 207pp.

6. IT Governance Institute, **"COBIT 3.0 Control Objectives, Management Guidelines and Maturity Models".** (Tercera Edición, Estados Unidos de América, 1998). 215pp.

7. IT Governance Institute, **"COBIT Mapping".** (Segunda Edición, Estados Unidos de América, 2005). 15pp.

8. Muñoz Razo, Carlos. **Auditoría en Sistemas Computacionales.** 2ª Edición México. Editorial Pearson, S.A. 2002 776pp.

9. Murdick Robert y Munson Jhon. **Sistemas de Información Administrativa.** 2ª Edición México. Editorial Prentice-Hall, S.A. 2002 796pp.

10. Piattini, Mario Gerardo; Del Peso, Emilio. **Auditoría Informática: Un enfoque práctico**. 3ª Edición. España. Editorial Alfa-Omega. 1998. 605pp.

11. Root, Steven. Beyond COSO: Internal control to enhance corporate governance. John Wiley & Sons. New York, NY. 2000. 352pp.

12. The Committee of Sponsoring Organizations of the Treadway Commission (COSO II), Enterprise Risk Management Framework – Exposure Draft for Public Comment (July 2003). 319pp.

13. Whittington, O. Ray, 1948-, **Auditoría: Un Enfoque Integral** / O. Ray Whittington, Kurt Pany, 12a edición, Santafé de Bógota: Irwin; McGraw-Hill, 2000, Colombia, 2000. 247pp.

WEBGRAFÍA

14. http://www.borrmart.es/articulo_redseguridad.php?id=1145 4pp.
15. http://www.guatewireless.org/cableado-de-redes-configuracion-de-colores-del-cable-estructurado-categoria-5e/ 5pp
16. http://www. inei.gob.pe/web/metodologias/attach/lib605/DOC4-4.htm
17. http://www.isaca.org
18. http://www.iso27000.es/sgsi.html#section2d 17pp.

ANEXOS

ANEXO 1
GLOSARIO

Glosario de términos de ambientes TI

Algoritmo:

Procedimiento o conjunto de procedimientos que describen una asociación de datos lógicos destinados a la resolución de un problema. Los algoritmos permiten automatizar tareas.

Aplicación:

Aunque se suele utilizar indistintamente como sinónimo genérico de “programa” es necesario subrayar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

Archivo de datos:

Cualquier archivo creado dentro de una aplicación: por ejemplo, un documento creado por un procesador de textos, una hoja de cálculo, una base de datos o un gráfico. También denominado documento.

Archivo de programa:

Archivo ejecutable que inicia una aplicación o programa. Los archivos de programa tienen las extensiones EXE, PIF, COM o BAT.

Archivo de revisión de auditoría:

Involucra módulos incrustados en una aplicación que monitorea continuamente el sistema de transacciones. Recolecta la información en archivos especiales que puede examinar el auditor

Archivos log:

Archivo de texto que almacena generalmente datos sobre procesos determinados. Para entendernos, es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

Auditor:

Persona que efectúa una auditoría

Auditoría:

Examen de las operaciones de una empresa por especialistas ajenos a ella y con objetivos de evaluar la situación de la misma.

Bases de Datos:

Colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacionar es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a éstos.

Bitácoras:

Es como el "diario" de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlos y ver qué es lo que ha sucedido en cada momento.

CAAT:

Técnicas de Auditoría Asistidas por Computadora, son herramientas (software) que ayudan al auditor a facilitar sus tareas.

Captura de Pantalla (*SnapShots)*:

Es una fotografía interna al sistema, es decir a la memoria, lo que permite obtener resultados intermedios en diferentes momentos de un proceso o conseguir valores temporales de una variable. Se activa mediante ciertas condiciones preestablecidas. Permite al auditor rastrear los datos y evaluar los algoritmos aplicados a los datos

C.I.M.S:

Certified Information Security Manager. Certificación para la Administración de la Seguridad de la Información

C.I.S.A:

Certified Information Security Auditor. Certificación en Auditor en Sistemas de Información

Cliente:

Cliente o 'programa cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Cliente-Servidor:

Se denomina así al binomio consistente en un programa cliente que consigue datos de otro llamado servidor sin tener que estar obligatoriamente ubicados en el mismo ordenador. Esta técnica de consulta 'remota' se utiliza frecuentemente en redes como “Internet”.

Confidencialidad:

Se refiere a que la información solo puede ser conocida por individuos autorizados.

Costo:

Desembolso en efectivo o en especie por algún beneficio.

Costos de inversión (largo plazo):

Esto es equipo de cómputo, hardware, software.

Costos de oportunidad:

Son los costos que se derivan de hacer una cosa en lugar de otra.

Costos estimados:

Son los cálculos anticipados de los gastos que predominarán en el futuro (mano de obra, material, etc); dentro de un período dado, con la intención de pronosticar un costo total.

Criptografía:

Ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

Datos:

Término general para la información procesada por un ordenador.

Dirección IP:

Dirección numérica obligatoria de un dominio 'Internet'. Está compuesta por cuatro cifras (de 0 a 255) decimales separadas por puntos. Por ejemplo: 194.179.52.25 corresponde a la dirección IP de “ctv.es”

Disco Duro:

Un disco duro o disco rígido (en inglés *hard disk drive*) es un dispositivo no volátil, que conserva la información aun con la pérdida de energía, que emplea un sistema de grabación magnética digital. Dentro de la carcasa hay una serie de platos metálicos apilados girando a gran velocidad. Sobre los platos se sitúan los cabezales encargados de leer o escribir los impulsos magnéticos.

Disco Duro Portátil:

Es un disco duro que es fácilmente transportable de un lado a otro. Puede ser desde un micro-disco hasta un disco duro normal de sobremesa con una carcasa adaptadora. Las conexiones más habituales son USB 2.0 y Firewire, menos las SCSI y las SATA. Estas últimas no estaban concebidas para uso externo pero dada su longitud del cable permitida y su capacidad Hot-plug, no es difícil usarlas de este modo.

Estándar de comparación (*Benchmarking*):

Técnica de auditoría informática en la cual se realiza el proceso continuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líderes en la industria.

Factibilidad:

Es la disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas, sirve para recopilar datos relevantes sobre el desarrollo de un proyecto y en base a ello tomar la mejor decisión.

- **Gobernabilidad de TI:**

Hardware:

Conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como el teclado, el Mouse, las unidades de disco y el monitor.

I.S.A.C.A:

Information Systems Audit and Control Association. Asociación de Auditoría y Control de Sistemas de Información.

Integridad:

La habilidad de determinar que la información recibida es la misma que la información enviada.

Internet:

Interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente.

IP:

Acrónimo de Internet. Es el protocolo que facilita la comunicación entre ordenadores conectados a la red Internet. Cada ordenador en Internet tiene una dirección IP única, que le identifica dentro de la red y permite su localización para posibilitar la comunicación.

ISO:

(Organización Internacional para la Normalización) Organización de carácter voluntario fundada en 1946 que es responsable de la creación de estándares internacionales en muchas arreas, incluyendo la informática y las comunicaciones. Esta formada por las organizaciones de normalización de sus 89 países miembro

Lenguaje:

En informática, conjunto de caracteres e instrucciones utilizadas para escribir programas de ordenador.

Memoria RAM:

La RAM es un medio físico que almacena temporalmente toda la lógica del ordenador: el sistema operativo, los programas que se están ejecutando y otros datos para su funcionamiento.

Memoria USB:

Es un pequeño dispositivo de almacenamiento que utiliza memoria flash para guardar la información que puede requerir y no necesita baterías (pilas). Son resistentes a los rasguños (externos) al polvo, y algunos al agua –que han afectado a las formas previas de almacenamiento portátil-, como los disquetes, discos compactos y los DVD.

Metodología:

Conjunto de métodos utilizados en la investigación científica

Microsoft Corporation:

Es una empresa multinacional estadounidense, fundada en 1975 por Bill Gates y Paul Allen. Dedicada al sector de la informática. Con sede en Redmond, Washington, Estados Unidos. Microsoft desarrolla, fabrica, licencia y produce software y equipos electrónicos. Siendo sus productos más usados el sistema operativo Microsoft Windows y la suite Microsoft Office**.**

Norma:

Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

Papeles de trabajo:

Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor.

Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Parámetro:

Valor especificado para conseguir los resultados deseados. En comunicaciones existe tal cantidad de parámetros que suelen ofuscar a los usuarios noveles: bits por segundo, bits de datos, bits de parada, paridad, etc. Información que se añade al comando que inicia una determinada aplicación. Un parámetro puede ser un nombre de archivo o cualquier tipo de información de hasta 62 caracteres de largo. Vea también Opción.

Password:

Conocida también como “clave de acceso.” Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto que se utiliza para que una persona no pueda usurpar la identidad de otra.

Procedimiento:

Método o sistema estructurado para la ejecución de actividades

Procedimiento en computación:

Una subrutina o subprograma, como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

Procesamiento de datos:

Conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipuleo y tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.

Procesamiento por lotes:

Archivo de texto que contiene comandos MS-DOS. Cuando se ejecuta un programa de procesamiento por lotes, MS-DOS ejecuta cada uno de los

comandos del archivo, tal como si se hubiesen escrito directamente 1 continuación del símbolo de MS-DOS.

Proceso:

Conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

Programa:

Secuencia de instrucciones que obliga al ordenador a realizar una tarea determinada.

Programa cliente:

Programa cliente o simplemente 'cliente' es aquel programa que permite conectarse a un determinado sistema, servicio o red.

Programa emergente:

Programa residente cargado en la memoria, que no es visible hasta que se presione una determinada combinación de teclas o hasta que tenga lugar un determinado hecho, tal como la recepción de un mensaje.

Programas de administración del sistema:

Herramientas de productividad sofisticadas que son típicamente parte de los sistemas operativos sofisticados, por ejemplo software para recuperación de datos o software para comparación de códigos. Como en el caso anterior estas herramientas no son específicamente diseñadas para usos de auditoría y deben ser utilizadas con cuidado

Programas de utilería:

Son usados por la entidad para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría y, por lo tanto, pueden no contener características tales como conteo automático de registros o totales de control

RDBMS:

Es un Sistema Administrador de Bases de Datos Relacionales. Proporcionan un mecanismo de vistas que permite que cada usuario tenga su propia vista o visión de la base de datos. El lenguaje de definición de datos permite definir vistas como subconjuntos de la base de datos.

Red:

Servicio de comunicación de datos entre ordenadores. Conocido también por su denominación inglesa: “network”. Se dice que una red está débilmente conectada cuando la red no mantiene conexiones permanentes entre los ordenadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

Repositorio:

Donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros

Rutinas de auditoría embebidas en programas de aplicación:

Módulos especiales de recolección de información incluidos en la aplicación y diseñados con fines específicos.

Servidor o server:

Ordenador que ejecuta uno o más programas simultáneamente con el fin de distribuir información a los ordenadores que se conecten con el para dicho fin. Vocablo más conocido bajo su denominación inglesa “server.”

Sintaxis:

Como en las lenguas humanas, la sintaxis es el conjunto de reglas estructurales que gobiernan el uso del lenguaje en el ordenador.

Sistema de información:

Se denomina Sistema de Información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

Software:

Componentes inmateriales del ordenador: programas, sistemas operativos, etc.

Software aplicado:

Programas escritos para la realización de tareas especiales, como el procesador de palabras o listas de correspondencia.

Software de sistemas:

Secciones de códigos que llevan a cabo tareas administrativas dentro del ordenador o ayudan en la escritura de otros programas, pero que no se usan para realizar la tarea que se quiere que ejecute el ordenador.

Software para un propósito específico o diseñado a la medida:

Son programas de computadora diseñados para desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar programas existentes en la entidad en su estado original o modificado porque puede ser más eficiente que desarrollar programas independientes.

SQL:

Es un lenguaje estándar de comunicación, (*Structured Query Language*) con bases de datos, normalizado que permite trabajar con cualquier tipo de lenguaje (ASP o PHP) en combinación con cualquier tipo de base de datos (MS Access, SQL Server, MySQL). Posee dos características muy apreciadas. Por una parte, presenta una potencia

y versatilidad notables que contrasta, con su accesibilidad de aprendizaje.

TI:

Tecnologías de Información

TIC:

Tecnologías de Información y Comunicación

Técnica:

La técnica es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad

Técnicas:

Conjunto de procedimientos de una ciencia los cuales nos ayudan a solucionar problemas.

Técnica de observación (*Tunning*):

Medidas encaminadas a la evaluación del comportamiento del sistema en su conjunto. Afinar la configuración de hardware y software para optimizar su rendimiento

UNIX:

Potente y complejo sistema operativo multiproceso/multitarea y multiusuario orientado a comunicaciones y gran devorador de 'RAM'. Fue creado en 1969 por Ken Thompson y Dennis Ritchie (de la empresa norteamericana 'AT&T Laboratories') coincidiendo con el nacimiento de 'Internet'.

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

POLÍTICAS DE SEGURIDAD INFORMÁTICA

CLÍNICA DE ENFERMEDADES INFECCIOSAS

El Manual de Control Interno Informático constituye una norma de cumplimiento obligatorio, en el cual se indican los requisitos mínimos de Control Interno informático a implementar por la Clínica de Enfermedades Infecciosas. Este manual formará parte del conjunto de manuales que se desarrollarán en el departamento de informática.

El manual se encuentra redactado y clasificado según las medidas de control que deben ser aplicadas en las diversas áreas de actividad relacionada con la Tecnología de la información. Las áreas definidas a efectos del Manual de Control Informático son los siguientes:

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos de la entidad. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. **(Revisar cada 6 meses a 1 año)**

Tabla de Resumen

Dominio	PROCESO	7 Criterios de Información en la Identidad								Recursos de TI			
		Efectividad	Eficiencia	Confidencialid.	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Planeación y Organización													
PO1	Definir un Plan Estratégico de TI	P	S							✓	✓	✓	✓
PO2	Definir la Arquitectura de Información	S	p	S	p					✓	✓		
PO3	Determinar la dirección tecnológica	P	p							✓		✓	
PO4	Definir los procesos, organización y relaciones de TI	P	p										✓
PO5	Administrar la Inversión en TI	P	P					S		✓		✓	✓
PO6	Comunicar las aspiraciones y la dirección de la gerencia	P					S				✓		✓
PO7	Administrar Recursos Humanos de TI	P	P										✓
PO8	Administrar la calidad	P	P		S			S		✓	✓	✓	
PO9	Evaluar y administrar los riesgos de TI	S	S	P	P	P	S	S		✓	✓	✓	✓
PO10	Administrar proyectos	P	P							✓		✓	✓

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos de la

entidad. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos de la organización. **(De acuerdo a los cambios en planeación y organización se revisará)**

Tabla de Resumen

Dominio	PROCESO	7 Criterios de Información en la Identidad							Recursos de TI			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Información	Infraestructura	Personas
Adquisición e Implementación												
AI1	Identificar Soluciones automatizadas	P	S						✓		✓	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S			S	✓			
AI3	Adquirir y Mantener Arquitectura de TI	S	P		S	S					✓	
AI4	Facilitar la operación y el uso	P	P		S	S	S	S	✓		✓	✓
AI5	Adquirir recursos de TI	S	P			S			✓	✓	✓	✓
AI6	Administrar Cambios	P	P		P	P		S	✓	✓	✓	✓
AI7	Instalar y acreditar soluciones y cambios	P	S		S	S			✓	✓	✓	✓

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas. **(CONTROLES CONSTANTES)**

Tabla de Resumen

Dominio	PROCESO	7 Criterios de Información en la Identidad							Recursos de TI			
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumpl	Confiabilidad	Aplicaciones	Información	Infraestructura	Personas
Servicios y Soporte												
DS1	Definir niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S	✓	✓	✓	✓
DS3	Administrar Desempeño y Capacidad	P	P			S			✓		✓	
DS4	Asegurar Servicio Continuo	P	S			P			✓	✓	✓	✓
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S	✓	✓	✓	✓
DS6	Identificar y Asignar Costos		P					P	✓	✓	✓	✓
DS7	Capacitar Usuarios	P	S									✓
DS8	Administrar la mesa de servicio y los incidentes	P	P						✓			✓
DS9	Administrar la Configuración	P	S			S		S	✓	✓	✓	
DS10	Administrar Problemas e Incidentes	P	P			S			✓	✓	✓	✓
DS11	Administrar Datos				P			P		✓		
DS12	Administrar Instalaciones				P	P					✓	
DS13	Administrar Operaciones	P	P		S	S			✓	✓	✓	✓

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. **(CONTROL CONSTANTE)**

Tabla de Resumen

Dominio	PROCESO	7 Criterios de Información en la Identidad								Recursos de TI			
		Efectividad	Eficiencia	Confidenci	Integridad	Disponibili	Cumplimie	Confiabilid		Aplicacion	Informaci	Infraestruct	Personas
Monitoreo													
ME1	Monitorear y evaluar el desempeño de TI	P	P	S	S	S	S	S		✓	✓	✓	✓
ME2	Monitorear y evaluar el control interno	P	P	S	S	S	S	S		✓	✓	✓	✓
ME3	Garantizar el cumplimiento regulatorio						p	S		✓	✓	✓	✓
ME4	Proporcionar gobierno de TI	P	P	S	S	S	S	S		✓	✓	✓	✓

NOTA: Este dominio debe ser supervisión basada en los riesgos que pueden generar las mismas TI.

JUSTIFICACIÓN DEL MANUAL

La creciente complejidad de las TI, la dependencia de ellas por parte de la organización y las expectativas que la alta dirección de estas últimas tiene respecto de las citadas tecnologías, conducen a la necesidad de contar con un marco genérico de control, gestión y gobierno de TI –independiente de la tecnología- que garantice que se alcanzarán los objetivos de la organización; reduciendo riesgos derivados de las propias TI y en ese contexto aparece este manual de políticas de seguridad.

La información o datos actualmente constituye un activo de gran valor y su administración y resguardo seguro, es y debe ser prioridad primordial en la clínica. En apoyo a las premisas anteriores pone a disposición de sus colaboradores equipo de cómputo para el buen desarrollo de sus diferentes actividades dentro de la organización y fuera de ella cuando sea el caso.

Por lo tanto el equipo de cómputo deberá utilizarse como herramienta de apoyo a labores desarrolladas en LA CLÍNICA y será de uso exclusivo de los usuarios de LA CLÍNICA. El uso adecuado del equipo computacional será responsabilidad del usuario, por lo que cualquier daño que se haga o sufra el equipo o alguno de sus componentes (monitor, teclado, Mouse, CPU, bocinas) será evaluado por los responsables del área de tecnología de Información, y de ser necesario, el usuario se hará acreedor a una sanción administrativa.

SEGURIDAD INFORMÁTICA

1. OPERATORIA

A.- DE LOS EQUIPOS DE ESCRITORIO Y DEL EQUIPO PORTÁTIL

- No se permite guardar archivos ajenos a los intereses de LA CLÍNICA en los perfiles móviles o en carpetas del servidor.
    - No utilizar los equipos computacionales como máquinas de juegos; esto incluye utilizar software de juegos o el acceso a servicios que impliquen el uso de juegos interactivos.
    - No utilizar el equipo para desarrollar programas o proyectos ajenos al interés de LA CLÍNICA, sin previa autorización.
    - No utilizar el acceso al servidor para guardar archivos tipo video o imágenes, sin previa autorización.
    - No utilizar el acceso al servidor para guardar archivos tipo sonido “música”.
    - No se permite modificar la configuración del equipo (Red, Internet, Correo)
    - No se permite extraer materiales de consumo del equipo computacional.
    - No se permite instalar software cuya licencia de uso lo prohíba y no este autorizado por el área de Tecnología de la Información.
    - No se debe alterar el software instalado en los equipos.
    - No utilizar los equipos computacionales para acceder a servicios locales o remotos a los que el usuario no tenga autorización explícita, o en su uso, intentar violar la seguridad de acceso de cualquier equipo computacional.
    - No llevar a cabo acciones que puedan interferir con la operación normal de los equipos computacionales o de comunicación electrónica de LA CLÍNICA.
    - No extraer equipo computacional o sus partes de LA CLÍNICA sin previa autorización.

- No se permite utilizar claves de acceso de otros usuarios, o permitir que otros usuarios utilicen la propia.

  - No se permite enviar mensajes a otros usuarios de manera anónima.
  - No utilizar los equipos como medio de comunicación interactiva sin previa autorización.
  - Toda unidad de USB o almacenamiento externo que sea utilizado, deberá ser verificado, para asegurar que no esté contaminado con algún virus informático.
  - No se permite mezclar los archivos de la oficina con sus documentos personales

B.- DEL USO DE INTERNET

- No se permite descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando equipo de cómputo de LA CLÍNICA.
- No se permite el uso de cualquier sistema de información de LA CLÍNICA para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material obsceno.
- No usar las comunicaciones electrónicas para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- No usar las comunicaciones electrónicas para adueñarse del trabajo de otros individuos, o de alguna manera apropiarse de trabajo ajeno.
- No se permite transportar o almacenar material con derechos de propiedad o material nocivo usando la red de LA CLÍNICA.
- Es terminante prohibido violar cualquier ley o regulación nacional respecto al uso de sistemas de información.
- No se permite la instalación y uso de programas de intercambio como Kazaa, Kazaa Lite, Emule, Messenger, Nero, Ares, etc.

- No se permite la instalación de programas que necesiten una licencia del fabricante sin solicitar permiso al departamento de Tecnología de Información.

- No se permite visitar sitios relacionados con violencia, sexo o hackers.
- Evitar aceptar programas de auto instalación sin previa consulta al área de Tecnología de la información.
- No se permite descargar archivos de gran volumen sin autorización previa.

C.- DEL CORREO ELECTRÓNICO

- No utilizar una identidad diferente a la propia, ya sea de otro usuario o ficticia, para enviar mensajes vía electrónica con propósitos malsanos.
- Evitar programas o al envío de e-mail que consuman uso excesivo de tiempo de CPU o espacio de almacenamiento.
- Evitar el seguimiento a las cadenas de correos.
- Enviar correos con archivos de más de 5 MB de tamaño [internamente]
- Enviar correos con archivos de mas de 2.5 MB de tamaño [externamente, de ser necesario solicitar Autorización]
- No enviar información importante o confidencial si no está seguro que la persona que recibirá la información está disponible o tiene espacio suficiente de recepción.
- No usar el correo electrónico para uso personal.
- No utilizar el correo de LA CLÍNICA para crear cadenas de correos.
- No utilizar el correo electrónico interno para hacer trámites de cualquier tipo.
- No utilizar el correo interno para enviar presentaciones, o archivos que no son de interés de la oficina (PowerPoint, chistes, fotos, etc.).
- No abrir archivos adjuntos que contengan las extensiones (exe, bat, rar, ini, bin, cfg, com,zip)
- No abrir correos de personas que son desconocidas para el usuario.
- El buzón de correo no debe de exceder de los 100 MB para los usuarios vía Web y 200 MB para los que tienen el correo localmente en sus estaciones de trabajo.
- No enviar archivos con las extensiones (exe, bat, rar, ini, bin, cfg, com).

- No responder e-mails donde aparezcan más de un destinatario (ejemplo: correo@otrapersona.com fulanito@la Empresamp.com) para evitar que las direcciones de LA EMPRESA sean leídas por personas ajenas a la oficina.
- No trasladar su contraseña a otro usuario.

2. SISTEMA OPERATIVO Y APLICACIONES AUTORIZADAS

- Para conservar un estándar en cuanto al sistema operativo y las aplicaciones de oficina que se deberán utilizar en los equipos de cómputo, se establecen Windows XP y Office 2003 Professional.
- Se adoptará la utilización de nuevas versiones tanto de sistema operativo como de office, hasta que se considere la estabilización de los sistemas en cuanto a su funcionamiento y operatividad.
- De tomarse la decisión de realizar up grade de sistema operativo o de office, éste será realizado única y exclusivamente por el responsable de sistemas, quien registrará las licencias autorizadas correspondientes.
- Otros programas o aplicaciones como convertidores de archivos a formato PDF, diseño, e impresión, serán instalados y configurados por el responsable de sistemas, entre estos:
  - Antivirus
  - Anti Spyware
  - Visio
  - Project
  - Agenda Electrónica
  - Adobe Reader
  - Mozila FIRE Fox

3. CONSIDERACIONES IMPORTANTES PARA LOS BACK-UPS

- Se realizará un bac-kup general de los archivos de las carpetas más importantes del servidor, por lo menos dos veces por semana.
- El usuario será el responsable de sacar back-up de los correos electrónicos que crea convenientes y ubicarlos en las carpetas para su respaldo respectivo.

- Toda la información que el usuario trabaje y que pertenezca a LA CLÍNICA, deberá ser guardada en las carpetas correspondientes en la red para su respectivo respaldo.

4. SUGERENCIAS PARA EVITAR CONTAMINACIÓN POR VIRUS

- Las máquinas están programadas para hacer actualización del antivirus y una búsqueda de archivos contaminados diariamente.
- El departamento de Tecnología de Información revisará periódicamente que esto se esté realizando correctamente.
- Revisar todos y cada uno de los discos que se introduzcan en la computadora. (USB, Diskettes, discos etc.)
- Proteger contra escritura los archivos que contengan información que no se desee modificar.
- Hacer copias o respaldo de programas y datos importantes.
- Cada vez que se transfiera un archivo desde o hacia Internet se debe tener la precaución de revisarlo contra virus.
- El antivirus detectará cuando ingresen a sus correos, archivos contaminados y los eliminará automáticamente, dejando un mensaje de aviso al respecto.
- Si tiene acceso a Internet utilice el programa Moxila FIRE Fox que es más seguro para navegar.
- Evite ingresar a páginas de Hackers o creadores de programas maliciosos.
- Cuando utilice motores de búsqueda de información (Google, etc.) tenga sumo cuidado con los accesos encontrados, pues le pueden llevar a un sitio no deseado y peligroso.
- Cualquier mensaje o alerta que no comprenda comunicarse con el administrador del sistema inmediatamente.

5. ADQUISICIÓN DE EQUIPO DE CÓMPUTO

- Para la cotización del equipo el interesado debe contar con la autorización por parte del director correspondiente del área de trabajo.
- Considerar las Políticas para el Uso del Equipo e Infraestructura Tecnológica de la firma, al momento de seleccionar el equipo a comprar.

- Presentar las proformas o cotizaciones (mínimo 5) al director del área de trabajo para definir la que más convenga a los intereses tanto de la CLÍNICA como del interesado.
- Asesorarse con el departamento de sistemas por cualquier duda o consideración que fuere necesario.
- Autorizada la compra, el interesado debe asegurarse que el proveedor le proporcione la factura y constancia de la garantía del equipo, al momento de realizar la transacción de compra.
- Para que el departamento de sistemas realice la configuración respectiva en el equipo de cómputo para su utilización en la red, se debe presentar fotocopia de la factura del equipo y fotocopia del formato "Autorización compra equipo computo" firmado de autorizado.
- Con los documentos anteriormente presentados y el equipo, el departamento de sistemas procederá a realizar la revisión de la máquina de acuerdo a las Políticas para el Uso del Equipo e Infraestructura Tecnológica, y a la configuración e instalación de

  aplicaciones necesarias para su uso en la red de LA CLÍNICA.

- **El Consejo de Arquitectura tecnológica debe evaluar cada 6 meses a 1 año a sus proveedores y considerar nuevos, que puedan ser más beneficiosos en los planes de la clínica.**

6. CUIDADO DEL EQUIPO CÓMPUTO Y OTROS

- Es terminante prohibido utilizar los CPU, IMPRESORAS Y EQUIPOS PORTÁTILES, como equipos de reposo de ornamentos (peluches, bandejas de metal, loncheras, bolsas, etc.) Estos equipos son frágiles, recordar producen calor, por lo que se exponen a sobrecalentamiento si algo se encuentra encima de los mismos.
- En cuanto a los recursos de la clínica lo vayan permitiendo es importante que los sistemas y concretamente el servidor y equipo de cámaras deben de mantenerse en sitios con unidades de aire acondicionado.

MANUAL DE ELECCIÓN DE PROVEEDORES

MANUAL DE ELECCIÓN DE PROVEEDORES

El Manual de Elección de Proveedores constituye una norma de cumplimiento obligatorio, en el cual se indican los requisitos mínimos de Control Interno sobre cómo elegir proveedores en el área de tecnología a implementar por la Clínica de Enfermedades Infecciosas. Este manual formará parte del conjunto de manuales que se desarrollarán en el departamento de informática.

El manual se encuentra redactado y clasificado según las medidas de control que deben ser aplicadas en las diversas áreas de actividad relacionada con la Tecnología de la información. Las áreas definidas a efectos del Manual son las siguientes:

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos de la entidad. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos de la organización. **(De acuerdo a los cambios en planeación y organización se revisará)**

Tabla de Resumen

		7 Criterios de Información en la Identidad								Recursos de TI			
Dominio	**PROCESO**	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Adquisición e Implementación													
AI1	Identificar Soluciones automatizadas	P	S							✓		✓	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S			S		✓			
AI3	Adquirir y Mantener Arquitectura de TI	S	P		S	S						✓	
AI4	Facilitar la operación y el uso	P	P		S	S	S	S		✓		✓	✓
AI5	Adquirir recursos de TI	S	P			S				✓	✓	✓	✓
AI6	Administrar Cambios	P	P		P	P		S		✓	✓	✓	✓
AI7	Instalar y acreditar soluciones y cambios	P	S		S	S				✓	✓	✓	✓

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte

del servicio a los usuarios, la administración de los datos y de las instalaciones operativas. **(CONTROLES CONSTANTES)**

Tabla de Resumen

		7 Criterios de Información en la Identidad								Recursos de TI			
Dominio	**PROCESO**	Efectividad	Eficiencia	Confidencialida	Integridad	Disponibilidad	Cumplimiento	Confiabilidad		Aplicaciones	Información	Infraestructura	Personas
Servicios y Soporte													
DS1	Definir niveles de servicio	P	P	S	S	S	S	S		✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S		✓	✓	✓	✓
DS3	Administrar Desempeño y Capacidad	P	P			S				✓		✓	
DS4	Asegurar Servicio Continuo	P	S			P				✓	✓	✓	✓
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S		✓	✓	✓	✓
DS6	Identificar y Asignar Costos		P					P		✓	✓	✓	✓
DS7	Capacitar Usuarios	P	S										✓
DS8	Administrar la mesa de servicio y los incidentes	P	P							✓			✓
DS9	Administrar la Configuración	P	S			S		S		✓	✓	✓	
DS10	Administrar Problemas e Incidentes	P	P			S				✓	✓	✓	✓
DS11	Administrar Datos				P			P			✓		
DS12	Administrar Instalaciones				P	P						✓	
DS13	Administrar Operaciones	P	P		S	S				✓	✓	✓	✓

JUSTIFICACIÓN DEL MANUAL

La creciente complejidad de las TI, la dependencia de ellas por parte de la organización y las expectativas que la alta dirección de estas últimas tiene respecto de las citadas tecnologías, conducen a la necesidad de contar con un marco genérico de control, gestión y gobierno de TI –independiente de la tecnología- que garantice que se alcanzarán los objetivos de la organización; reduciendo riesgos derivados de las propias TI y en ese contexto aparece este Manual de Elección de proveedores.

Una vez que una empresa opta por seguir el camino de elegir productos específicos para ambientes TI debe tomar en consideración varias calidades para elegir proveedores de TIC. Pero si bien el costo es una preocupación y aun cuando fuera el motivo principal para elegir el producto en primer lugar – eso no significa que deba ser la única inquietud cuando se trata de elegir un proveedor. Existen otros factores críticos que determinarán si una adquisición de hardware o de software en particular tendrá o no éxito.

Por esta razón se elabora el presente manual como un reforzamiento en las políticas de adquisiciones que ya existen en el Manual de Normas y Procedimientos Administrativos y Financieros para las Unidades Ejecutoras en este caso la Clínica de Enfermedades Infecciosas del Hospital Roosevelt.

1. Cualidades que hay que buscar en un proveedor

- **Liderazgo en la industria:** a las empresas con frecuencia les preocupa tanto la estabilidad financiera de los posibles proveedores de tecnología de la información como las características de los productos mismos. Las empresas necesitan elegir una compañía que sea líder en su segmento del mercado, una que posea una trayectoria comprobada brindando productos y servicios de valor a sus clientes, que cuente con una amplia base instalada de usuarios, y un conjunto de proveedores de software independientes (ISV), socios de hardware y trabajadores capacitados en el mercado lo más extenso posible.

- **Productos de calidad superior:** además de la clase de garantía de calidad, pruebas y depuración que existe en la comunidad, los proveedores líderes realizarán pruebas y controles de garantía de calidad internos exhaustivos, y participarán en programas de certificación que garanticen la compatibilidad con otros productos de hardware y software. Para muchos clientes, la disponibilidad de resultados de rendimiento auditados constituye un criterio relevante que debe ser tomado en cuenta durante la evaluación del producto y el ciclo de compra.

- **La seguridad:** también es un punto crucial: algunos proveedores han demostrado a lo largo del tiempo su capacidad de proveer un código de calidad superior, con menos errores y fallas en la seguridad, que otros distribuidores.

- **Soporte estelar:** uno de los aspectos clave que distinguen a las versiones libres del software de código abierto de las versiones comerciales es la calidad del soporte. Elija a un proveedor que tenga reputación de brindar un soporte de primer nivel como parte de su solución empresarial. Las compañías líderes ofrecerán distintos niveles de soporte – inclusive la cobertura 24x7x365 – y deberían incluir un nivel de mesa de ayuda y opciones de escalación

adecuados para mantener el funcionamiento de aplicaciones que son fundamentales para la misión de la empresa.

- **Amplio ecosistema**: El valor de cualquier sistema informático depende en última instancia de las aplicaciones que corren en él. Uno de los principales elementos diferenciadores de los proveedores líderes es la cantidad de certificaciones que hayan logrado en el mundo informático.

Elija a un proveedor de tecnología que tenga el conjunto más amplio de socios de hardware y software cuyos productos hayan sido certificados para funcionar con sus productos. Disponibilidad de profesionales capacitados. Una preocupación esencial de muchos gerentes de TI es si van a poder encontrar miembros del personal con experiencia para dar soporte. Se trata de una consideración válida. Elija a un proveedor que cuente con la mayor población de empleados y contratistas/consultores potenciales con las habilidades necesarias. Independencia de la versión y arquitectura. Busque un proveedor con un esquema flexible de precios, que permita a los clientes ejecutar cualquier versión del software y transferirlo a distintas arquitecturas y sistemas físicos. Protección legal. Periódicamente surgen en la industria controversias sobre la situación legal del software debido a las posibles violaciones del derecho de autor y de marcas comerciales. Busque un proveedor que indemnice a los clientes contra cualquier problema legal que pudiera surgir.

2. ADQUISICIÓN DE EQUIPO DE CÓMPUTO y SOLUCIONES DE SOFTWARE

- Para la cotización del equipo o programa de software el interesado debe contar con la autorización por parte del director correspondiente del área de trabajo.
- Considerar las Políticas para el Uso del Equipo e Infraestructura Tecnológica de la firma, al momento de seleccionar el equipo a comprar o programa de software.
- Presentar las proformas o cotizaciones (mínimo 5) al director del área de trabajo para definir la que más convenga a los intereses tanto de la CLÍNICA como del interesado.
- Asesorarse con el departamento de sistemas por cualquier duda o consideración que fuere necesario.
- Autorizada la compra, el interesado debe asegurarse que el proveedor le proporcione la factura y constancia de la garantía del equipo o del software al momento de realizar la transacción de compra.
- Para que el departamento de sistemas realice la configuración respectiva en el equipo de cómputo o programa de software para su utilización en la red, se debe presentar fotocopia de la factura del equipo y fotocopia del formato o características del software “Autorización compra equipo computo o programa de software” firmado de autorizado.
- Con los documentos anteriormente presentados y el equipo o programa de software, el departamento de sistemas procederá a realizar la revisión de la máquina o prueba de software de acuerdo a las Políticas para el Uso del Equipo e Infraestructura Tecnológica, y a la configuración e instalación de aplicaciones necesarias para su uso en la red de LA CLÍNICA.

- **El Consejo de Arquitectura tecnológica debe evaluar cada 6 meses a 1 año a sus proveedores y considerar nuevos, que puedan ser más beneficiosos en los planes de la clínica.**