ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

AUDITORÍA DEL SISTEMA INFORMÁTICO DEL HOSPITAL DEL SUR "ENRIQUE GARCÉS"

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

AUTORES:

PABLO FERNANDO DEL HIERRO CADENA
pablofer999@hotmail.com

FREDDY MAURICIO TRUJILLO BAZANTE
cruger0077@hotmail.com

DIRECTOR:

ING. JAIME NARANJO
jaime.naranjo@epn.edu.ec

QUITO, ENERO 2012

DECLARACIÓN

Nosotros, Pablo Fernando Del Hierro Cadena, Freddy Mauricio Trujillo Bazante, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Pablo F. Del Hierro C.	Freddy M. Trujillo B.

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Pablo Fernando Del Hierro Cadena, Freddy Mauricio Trujillo Bazante, bajo mi supervisión

Jaime Naranjo, MSC. ING.

Director del Proyecto

DEDICATORIA

A mi abuelita Julia, que más que darme la vida, ha dado su vida por hacer que la mía tenga el rumbo que ahora tiene.

A mi tío, Carlos que desde el cielo a cuidado de mi, para poder alcanzar todo lo que me he propuesto en mi vida.

A mi padre Arturo y mi madre Estela por ser la fuerza constante que me sostiene en el día a día.

A mis hermanos Carlos y Cristina que han sido un ejemplo a lo largo de mi vida para enfocarme en mis metas.

A mi hermana Lucia, que es el espejo de lo que soy y lo que algún día seré.

A Vicente, Luis, Stalin, Guillermo, Felipe, Andrés, y Francisco, que han sido como mis hermanos, y que me han apoyado en mis locuras y mis aciertos.

A V. G. y A. que han sido tres estrellas brillantes en mi vida, y que con su afecto me han demostrado que para que en la vida haya alegría también debe existir la tristeza.

A mis profesores y maestros, que han sido la luz a lo largo del camino.

Y finalmente falta dedicar esto a mis amigos y compañeros, con los cuales he compartido gran parte de mi vida y con los cuales he aprendido a diferencia lo bueno de lo malo.

Así que este trabajo va dedicado a todas las personas que han estado a lo largo de mi existencia, gracias a todos.

Pablo Fernando Del Hierro C.

El hastió, la pereza y el conformismo, son las virtudes de un mediocre, y los defectos de un hombre. P.F

DEDICATORIA

Quiero dedicar este trabajo, que representa el último paso de lo que al principio se veía muy distante, y tras 5 años de esfuerzo es ahora un hecho.

A mis padres María del Carmen y Freddy, quienes me apoyaron a lo largo de este camino y me ayudaron a que se convierta en rumbo.

A mis hermanos Belén, Michelle y Carlos, que con paciencia supieron ayudarme de la mejor manera que pudieron.

A María Belén, mi novia, que estuvo ahí en los buenos y malos momentos y con su apoyo incondicional supo llenarme de aliento y ganas de seguir adelante.

A mis tíos Juan Carlos y Xavier, que con su ejemplo y consejos supieron guiar mi camino y me ayudaron a lograr mi objetivo.

A mi abuelita Heralda, que con su cariño y comprensión me ayudó a seguir adelante sin mirar atrás.

A toda mi familia, que siempre estuvo ahí cuando necesitaba unas palabras de aliento.

A mis amigos, compañeros y profesores, con los que compartimos grandes momentos y alegrías a lo largo de estos años, que me dejaron grandes enseñanzas.

A todos ellos, ya que sin ustedes, este proyecto no hubiese podido ser.

Freddy Mauricio Trujillo B .

AGRADECIMIENTO

Queremos agradecer a cada uno de nuestros profesores, que nos han brindado enseñas tanto para nuestra vida profesional, como personal, y que han sido la base para desarrollar nuestras virtudes y capacidades.

Agradecemos al Ingeniero Jaime Naranjo, que a más que ser nuestro profesor y tutor ha sido un amigo, que nos ha brindado su confianza, compartido sus experiencias, otorGrado las pautas y herramientas necesarias para desarrollar y concluir con este trabajo.

Agradecemos a nuestras familias por el apoyo incondicional, por las enseñanzas en valores, y sobre todo por el cariño brindado a lo largo de toda nuestra vida.

Agradecemos a nuestros amigos y compañeros, por formar parte de nuestra vida con amistades sinceras y duraderas.

Pablo y Mauricio.

CONTENIDO

1. CAPITULO 1:.....1

2. DESCRIPCIÓN DEL PROYECTO.....1

1.1 . ALCANCE DEL PROYECTO 1

1.2. CARACTERIZACIÓN DE LA EMPRESA 1

1.2.1. DESCRIPCIÓN DE LA EMPRESA. 1

1.2.2 NATURALEZA DE LA EMPRESA..... 3

1.2.3 OBJETIVOS ESTRATÉGICOS 4

1.2.4 DIAGRAMA ORGÁNICO FUNCIONAL DEL HOSPITAL “ENRIQUE GARCÉS”..... 5

1.2 SELECCIÓN DE LA METODOLOGÍA 6

1.2.1 TABLA COMPARATIVA DE METODOLOGÍAS 7

2. CAPÍTULO 2:.....12

EJECUCIÓN DE LA AUDITORÍA.....12

2.1. PLANIFICACIÓN DE AUDITORÍA 12

2.2. SITUACIÓN ACTUAL DEL ÁREA DE SISTEMAS..... 13

2.2.1. NIVEL DE DECISIÓN DE LA UNIDAD INFORMÁTICA 13

2.2.2. ESTRUCTURA DE LA UNIDAD INFORMÁTICA..... 13

2.2.3. FUNCIONES 14

2.2.5. INVENTARIO DE HARDWARE 16

2.2.6. INVENTARIO DE SOFTWARE 16

2.2.7. TOPOLOGÍA DE RED..... 18

2.2.8. SEGURIDADES 21

2.3. REALIZACIÓN DE LA AUDITORÍA..... 23

2.3.1. PROCESOS DEL DOMINIO DE PLANEACIÓN Y ORGANIZACIÓN. 26

2.3.1.1. PO1 Definir un Plan Estratégico De TI 26

2.3.1.2. PO2 Definición de la Arquitectura de Información 33

2.3.1.3. PO3 Determinación de la Dirección Tecnológica 40

2.3.1.4. PO4 Definición de la Organización y de las Relaciones De Ti 46

2.3.1.5. PO6 Comunicación de los objetivos y de las aspiraciones de la gerencia 55

2.3.1.6. PO9 Análisis de riesgos 61

2.3.1.7. Resumen del Dominio Planeación y Organización 69

2.3.2. PROCESOS DEL DOMINIO DE ADQUIRIR E IMPLEMENTAR 71

2.3.2.1. AI2 Adquisición y mantenimiento de software de aplicación 71

2.3.2.2. AI3 Adquisición y mantenimiento de la infraestructura tecnológica 78

2.3.2.3. AI4 Desarrollo y mantenimiento de procedimientos 84

2.3.2.4. AI5 Instalación y acreditación de sistemas 90

2.3.2.5. Resumen del Dominio Adquirir e Implementar 97

2.3.3. PROCESOS DEL DOMINIO ENTREGA Y SOPORTE 99

2.3.3.1. DS1 Definición y administración de niveles de servicio 99

2.3.3.2. DS4 Asegurar el servicio continuo 106

2.3.3.3. DS5 Garantizar la seguridad de sistemas 115

2.3.3.4. DS7 Educación y entrenamiento de usuarios 125

2.3.3.5. DS8 Apoyo y asistencia para los clientes 132

2.3.3.6. DS10 Administración de problemas e incidentes 139

2.3.3.7. DS12 Administración de instalaciones 146

2.3.3.8. Resumen del Dominio Entregar y dar Soporte 154

2.3.4. PROCESOS DEL DOMINIO MONITOREO 155

2.3.4.1. M1 Monitoreo de los procesos 155

2.3.4.2. Resumen del Dominio Monitoreo y Evaluación 161

3. CAPÍTULO 3:.....162

ANÁLISIS DE RESULTADOS 162

3.1. ANÁLISIS DE RESULTADOS..... 162

3.2. INFORME PRELIMINAR..... 163

3.2.1. Presentación del informe preliminar..... 163

3.2.2. Consideraciones previas..... 163

3.3. INFORME TÉCNICO..... 172

3.3.1. Alcance y justificación de la auditoria 172

Alcance 172

Justificación 172

Objetivos propuestos de la auditoria 173

Metodología COBIT 173

3.4. INFORME EJECUTIVO..... 188

4. CAPÍTULO 4:.....191

CONCLUSIONES Y RECOMENDACIONES.....191

4.1. CONCLUSIONES..... 191

4.2. RECOMENDACIONES 192

4.3. BIBLIOGRAFÍA 193

ANEXOS.....194

ANEXO 1 195

Metodología COBIT, Objetivos de Control y Directrices 195

ANEXO 2 202

Encuesta realizada a empleados de la unidad de TI, como a usuarios claves en el Hospital “Enrique Garcés”..... 202

GRAFICAS DE LAS PREGUNTAS CUANTIFICABLES DE LA ENCUESTA..... 206

ANEXO 3 218

Información del Hospital “Enrique Garcés” 218

INDICE DE FIGURAS

Figura 1.1: Logotipo Hospital General “Enrique Garcés” 2

Figura 1.2: Diagrama Orgánico Funcional Hospital General “Enrique Garcés”..... 5

Figura 2.1 Estructura Orgánica Interna de la UI 13

Figura 2.2: Topología de red del Hospital Genera "Enrique Garcés" 19

Figura 2.3: Leyenda Topología de Red Hospital Genera "Enrique Garcés" 20

INDICE DE TABLAS

Tabla 1.1: Tabla Comparativa de Metodologías. 10

Tabla 2.1 Tabla de cruce de actividades 12

Tabla 2.2: Inventario de hardware HEG 16

Tabla 2.3: Inventario de software HEG 17

Tabla 2.3: Tabla Resumen PO1 29

Tabla 2.4: Modelo de Madurez PO1 31

Tabla 2.5: Estrategias a corto y largo plazo PO1 32

Tabla 2.6: Tabla Resumen PO2 35

Tabla 2.7: Modelo de Madurez PO2 38

Tabla 2.8: Estrategias a corto y largo plazo PO2 39

Tabla 2.9: Tabla Resumen PO3 41

Tabla 2.10 Modelo de Madurez PO3 44

Tabla 2.11 Estrategias a corto y largo plazo PO3 45

Tabla 2.12: Tabla Resumen PO4 51

Tabla 2.13 Modelo de madurez PO4 53

Tabla2.14: Estrategias a corto y largo plazo PO4 54

Tabla 2.15: Tabla resumen PO6 57

Tabla 2.16: Modelo de madurez PO6 59

Tabla 2.17 Estrategias a corto y largo plazo PO6 60

Tabla 2.18 Tabla de resumen PO9 64

Tabla 2.19 Modelo madurez PO9 67

Tabla 2.20: Estrategias a corto y largo plazo PO9 68

Tabla 2.21: Tabla Resumen AI2 74

Tabla 2.22: Modelo Madurez Al2 76

Tabla 2.213 Estrategias a corto y largo plazo AI2 77

Tabla 2.24: Tabla Resumen AI3 80

Tabla 2.25: Modelo Madurez AI3 82

Tabla 2.16: Estrategias a corto y largo plazo AI3 83

Tabla 2.26: Tabla resumen AI4 85

Tabla 2.27: Modelo Madurez AI4 88

Tabla 2.28: Estrategias a corto y largo plazo AI4 89

Tabla 2.29: Tabla Resumen AI5 93

Tabla 2.30: Modelo de Madurez AI5 95

Tabla 2.31: Estrategias a corto y largo plazo AI5 96

Tabla 2.32: Tabla Resumen DS1 102

Tabla 2.33: Modelo de Madurez DS1 104

Tabla 2.34: Estrategias a corto y largo plazo DS1 105

Tabla 2.35 Tabla Resumen DS4 110

Tabla 2.36 Modelo de Madurez DS4 113

Tabla 2.38: Estrategias a corto y largo plazo DS4 114

Tabla 2.39: Tabla Resumen DS5 119

Tabla 2.40 Modelo de Madurez DS5 122

Tabla 2.41: Estrategias a corto y largo plazo DS5 124

Tabla 2.42: Tabla Resumen DS7 127

Tabla 2.43: Modelo de Madurez DS7 130

Tabla 2.44 Estrategias a corto y largo plazo DS7 131

Tabla 2.45: Tabla Resumen DS8 135

Tabla 2.46 Modelo de Madurez DS8 137

Tabla 2.47: Estrategias a corto y largo plazo DS8 138

Tabla 2.48: Tabla Resumen DS10 142

Tabla 2.49 Modelo de Madurez DS10 144

Tabla 2 Estrategias a corto y largo plazo DS10 145

Tabla 2.51:3 Tabla Resumen DS12 149

Tabla 2.52: Modelo de Madurez DS12 152

Tabla 2.53: Estrategias a corto y largo plazo DS12 153

Tabla 2.54: Tabla Resumen M1 157

Tabla 2.55: Modelo de Madurez M1 159

Tabla 2.56: Estrategias a corto y largo plazo M1 160

Tabla 3.1 Tabla Grado de Madurez PO1 164

Tabla 3.2 Tabla Grado de Madurez PO2 165

Tabla 3.3 Tabla Grado de Madurez PO3 165

Tabla 3.4 Tabla Grado de Madurez PO4 166

Tabla 3.5 Tabla Grado de Madurez PO6 166

Tabla 3.6 Tabla Grado de Madurez PO9 166

Tabla 3.7 Tabla Grado de Madurez AI2 167

Tabla 3.8 Tabla Grado de Madurez AI3 167

Tabla 3.9 Tabla Grado de Madurez AI4 168

Tabla 3.10 Tabla Grado de Madurez AI5 168

Tabla 3.11 Tabla Grado de Madurez DS1..... 168

Tabla 3.12 Tabla Grado de Madurez DS4..... 169

Tabla 3.13 Tabla Grado de Madurez DS5..... 169

Tabla 3.14 Tabla Grado de Madurez DS7..... 170

Tabla 3.15 Tabla Grado de Madurez DS8..... 170

Tabla 3.16 Tabla Grado de Madurez DS10..... 170

Tabla 3.17 Tabla Grado de Madurez DS12..... 171

Tabla 3.18 Tabla Grado de Madurez M1..... 171

Tabla 3.19 Tabla Grado de Madurez PO1 174

Tabla 3.20 Tabla Grado de Madurez PO2 175

Tabla 3.21 Tabla Grado de Madurez PO3 176

Tabla 3.22 Tabla Grado de Madurez PO4 177

Tabla 3.23 Tabla Grado de Madurez PO6 177

Tabla 3.24 Tabla Grado de Madurez PO9 178

Tabla 3.25 Tabla Grado de Madurez AI2 179

Tabla 3.26 Tabla Grado de Madurez AI3 180

Tabla 3.27 Tabla Grado de Madurez AI4 180

Tabla 3.28 Tabla Grado de Madurez AI5 181

Tabla 3.29 Tabla Grado de Madurez DS1..... 182

Tabla 3.30 Tabla Grado de Madurez DS4 183

Tabla 3.31 Tabla Grado de Madurez DS5 183

Tabla 3.32 Tabla Grado de Madurez DS7 184

Tabla 3.33 Tabla Grado de Madurez DS8 185

Tabla 3.34 Tabla Grado de Madurez DS10 185

Tabla 3.35 Tabla Grado de Madurez DS12 186

Tabla 3.36 Tabla Grado de Madurez M1 186

Tabla 3.37: Tabla resumen de Grados de Madurez 189

Tabla 3.38: Tabla Grado de Madurez 189

RESUMEN

El presente proyecto de titulación está compuesto de cuatro capítulos, y anexos, los cuales tienen como principal objetivo mostrar los resultados obtenidos de la auditoría, utilizando el marco de trabajo y las directrices de auditoría propuestas por COBIT, realizada a la unidad informática del Hospital General “Enrique Garcés”.

El Capítulo I presenta una descripción tanto del alcance del proyecto como la descripción de la unidad informática del Hospital General “Enrique Garcés”, su ubicación dentro del hospital, características principales y nivel de decisión. Además este capítulo cuenta con un análisis que se realizó para determinar cuál sería la metodología más adecuada para realizar la presente auditoria.

El Capítulo II detalla una visión de la situación actual del área informática del Hospital General Enrique Garcés, y de la planificación y realización de la auditoria, en donde se seleccionaran los procesos más adecuados propuestos por COBIT que se ajusten a la situación actual de la unidad de TI, en donde se evaluará, medirá el modelo de madurez, y se realizará recomendaciones a mediano y largo plazo de cada uno de ellos.

El Capítulo III se presentará los resultados de la auditoria a través de un conjunto de informes que serán entregados tanto a la parte gerencial como a la unidad de TI del Hospital General Enrique Garcés, en donde se mostrará el análisis de los resultados, y se entregará las conclusiones finales por cada proceso evaluado.

Finalmente, en el Capítulo IV se presentan las conclusiones y recomendaciones del Proyecto.

INTRODUCCIÓN

Dentro de cualquier institución para mejorar siempre hay que ser evaluado, es por ello que la auditoria es una herramienta que nos permite conocer las debilidades para mejorarlas, y nuestras fortalezas para que estas se vuelvan el puntal para un buen funcionamiento de una empresa.

Esta es la razón por la cual se ha realizado una auditoria a la unidad informática del Hospital General “Enrique Garcés”, para así conocer sus fortalezas y debilidades, y así entrar en un proceso de mejora continua que brinde innumerables beneficios a todos sus trabajadores.

Se analizarán los resultados obtenidos por la auditoria, para en base de ellos poder entregar las conclusiones y recomendaciones de cada proceso evaluado, obteniendo una base para que la unidad de TI comience un plan de mejora que ayude a satisfacer las necesidades que el hospital demande.

Con los informes que se obtendrán de esta auditoría, se podrán tener acciones correctivas, y crear planes a futuro para mitigar ciertos riesgos que pueda tener tanto el hospital como la unidad de TI.

CAPITULO 1:

DESCRIPCIÓN DEL PROYECTO

1.1 . ALCANCE DEL PROYECTO

Este proyecto está orientado a realizar una auditoría al área informática del Hospital General “Enrique Garcés”, y se enfocará en su sistema informático, se trabajará sobre sus servidores, su estructura y topología de red, el área informática y los elementos alrededor de la misma.

Este proyecto comienza con la descripción de los procesos del hospital, para proceder luego con la realización de la auditoria del sistema informático, tomando en cuenta sus servidores y PC’s, utilizando una metodología adecuada, que se adapte y permita evaluar el desempeño del área informática del hospital.

Además se evaluarán los procesos involucrados en el área de TI, y se entregarán las conclusiones respectivas.

Hay que aclarar que no nos involucraremos con el área de desarrollo de software del hospital y las metodologías que utilicen para la creación de aplicaciones, ni con el mantenimiento de equipos y de servidores.

1.2. CARACTERIZACIÓN DE LA EMPRESA

1.2.1. DESCRIPCIÓN DE LA EMPRESA.

Nombre:

Hospital General “Enrique Garcés”

Ubicación:

Chilibulo S/N Y Av. Enrique Garcés

Línea de negocio:

Servicios médicos, Hospital

Categoría:

Tipo A, es decir es un hospital apto para encargase de cualquier emergencia médica, además de poder seguir con cualquier tratamiento, y dar seguimiento a las enfermedades de sus pacientes. [1]

Logotipo:

Figura 1.1: Logotipo Hospital General "Enrique Garcés" [2]

Misión

"Prestar servicios de salud de tipo ambulatoria, de internamiento y de emergencia en actividades de prevención, diagnóstico, tratamiento, recuperación y rehabilitación; de manera permanente y oportuna a la población que demande sus servicios; enmarcados en los principios constitucionales, para lograr el mayor grado de satisfacción de las necesidades y expectativas de salud de los (as) usuarios (as). Es además un hospital docente y de investigación" [3]

Visión

"Al 2013 será un hospital que proporcione atención de salud integral, que sustente su gestión en la capacidad resolutiva de segundo nivel. En la gestión

[1] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[2] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[3] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"

administrativa por procesos en la administración efectiva de los sistemas de información y en el mejoramiento continuo."[4]

1.2.2 NATURALEZA DE LA EMPRESA

El Hospital General "Enrique Garcés", es una unidad operativa del Ministerio de Salud Pública del Ecuador, ubicado en el sector sur del Distrito Metropolitano de Quito, en la Provincia de Pichincha, que provee atención de salud de tipo ambulatorio en consulta externa, y de recuperación de la salud con internamiento en Hospitalización, en las cuatro especialidades básicas de la medicina moderna; Medicina Interna, Cirugía, Pediatría y Gíneco - Obstetricia y en varias subespecialidades. Apoyadas todas ellas en servicios auxiliares de diagnóstico y tratamiento que funcionan las 24 horas del día y los 365 días del año. Es además Hospital en el que se desarrollan actividades docentes y de investigación en ciencias de la salud. [5]

De acuerdo al esquema planteado por el Ministerio de Salud Pública, por su complejidad está en el segundo nivel de atención, constituyéndose en el hospital de referencia de la zona sur de la provincia de Pichincha y de las provincias centrales del país."[6]

Este es uno de los hospitales públicos más importantes de Quito, que se encarga de atender una gran cantidad de pacientes del sur de la ciudad por lo que posee 340 camas y atiende en promedio a 40.000 personas al año. Cuenta con áreas de gineco-obstetricia, medicina interna, terapia intensiva, área de quemados, emergencia, cuidado a pacientes con VIH, ecosonografía, entre otras. [7]

Además debemos comentar que el hospital en los últimos años se encuentra automatizando ciertos procesos, con ayuda de la unidad informática, que es un

---

[4] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[5] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[6] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[7] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"

área bien definida y se encuentra como soporte técnico para las aplicaciones que se utilizan en el hospital. [8]

1.2.3 OBJETIVOS ESTRATÉGICOS

- Contribuir al mejoramiento del nivel de salud de la comunidad y por ende al desarrollo socioeconómico de la misma.[9]
- Ofrecer a sus usuarios, atención de salud con altos estándares de calidad, en forma eficiente, eficaz y oportuna, con equidad, universalidad y solidaridad, enfatizando la movilidad y la participación comunitaria, mediante un trabajo multidisciplinario, intersectorial, intercultural.[10]
- Contribuir al desarrollo técnico, administrativo y científico en la prestación de los servicios de salud."[11]

[8] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[9] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[10] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"
[11] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"

1.2.4 DIAGRAMA ORGÁNICO FUNCIONAL DEL HOSPITAL "ENRIQUE GARCÉS"

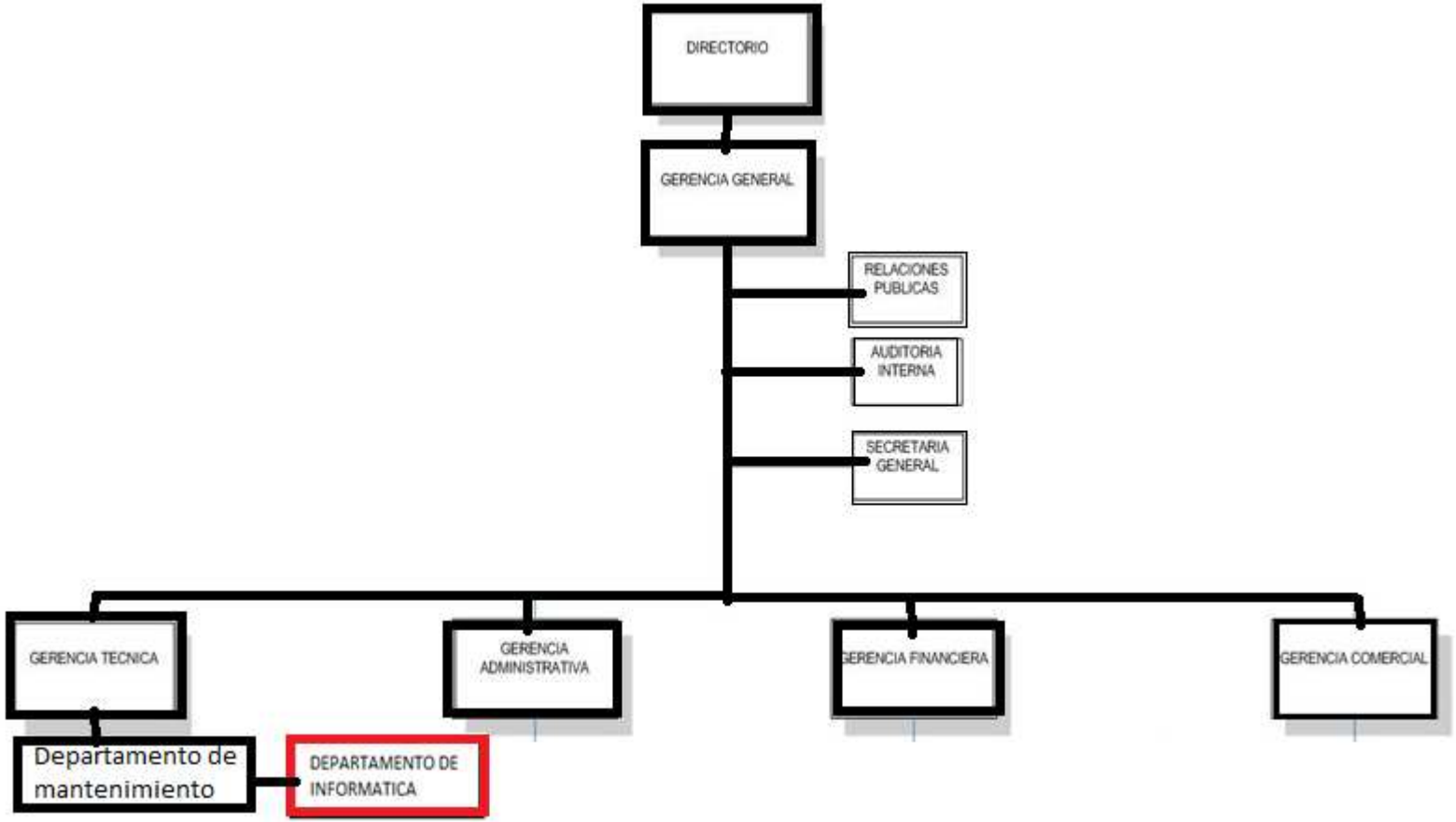


Figura 1.2: Diagrama Orgánico Funcional Hospital General "Enrique Garcés"

1.2 SELECCIÓN DE LA METODOLOGÍA

Uno de los pasos más importantes dentro de la realización de esta auditoría es la selección de la metodología. Puesto que dependiendo de la metodología seleccionada podremos evaluar de una mejor manera los procesos del área informática del hospital e identificar sus necesidades y requerimientos. A continuación definiremos algunas de las metodologías utilizadas en auditorias informáticas para poder escoger la que mejor se ajuste a las necesidades del Hospital General "Enrique Garcés".

"COBIT (Control Objectives for Information and related Technology), según sus siglas en español Objetivos de Control para la Información y Tecnologías relacionadas. Es una metodología originada como un marco para las tecnologías de la información (TI) y el gobierno de TI, que se orienta directamente sobre el control de las actividades gerenciales, lo que hace que esté enteramente relacionado con todo lo referente a tecnologías de la información." [12]

"ITIL (Information Technology Infrastructure Library), según sus siglas en español Biblioteca de Infraestructura de Tecnologías de Información, es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma; en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI" [13]

"Metodología R.O.A (RISK ORIENTED APPROACH), Está formuladasç por recomendaciones de plan de trabajo y de todo el proceso que se debe seguir. También se define el objetivo de la misma, que habrá que describirlo en el memorando de apertura al auditado. La metodología está basada en la minimización de los riesgos, que se conseguirá en función de que existan los

[12] Tomado de http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_información
[13] Tomado de http://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

controles y de que éstos funcionen. En consecuencia el auditor deberá revisar estos controles y su funcionamiento.”[14]

1.2.1 TABLA COMPARATIVA DE METODOLOGÍAS

	COBIT	**ITIL**	**ROA**
Autores	Los creadores de COBIT son ISACA (Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (IT Governance Institute).	Los creadores de ITIL, son la CCTA (Central Computer and Telecommunications Agency) actualmente como la OGC (Office of Government Commerce).	Los creadores de la metodología ROA es Arthur Andersen.

[14] Tomado de http://es.wikipedia.org/wiki/Capability_Maturity_Model_Integration

Alcance	COBIT tiene como alcance la auditoría de sistemas de información, además de su control y su contribución en beneficio del negocio, manteniéndose alineados con el gobierno de tecnologías de información.	ITIL está más orientado a la prestación de servicios, de una manera sistematizada, con el establecimiento de planes y estrategias para la gestión operativa de infraestructura de TI.	Esta pretende ser un sistema sencillo y fiable de conocer la situación general del sistema de información de una empresa, así como definir el estado del control de dichos sistemas tomando como control la definición de la ISAACA.

Elementos de la metodología	COBIT está dispuesto de la siguiente manera: 4 dominos, 34 procesos y 210 objetivos de control	Los elementos de ITIL son cinco libros, donde se encuentran los temas para consolidar el modelo de "ciclo de vida del servicio".	La metodología utilizada es la Evaluacion de Resgos (ROA Risk Oriented Approach) recomendada por ISACA. Esta evaluación de riesgos se desarrolla sobre determinadas áreas de aplicación y bajo técnicas de Checklist (cuestionarios) adaptados a cada entorno especifico; deberá tenerse en cuenta que determinados controles se repetirían en diversas áreas de riesgo

Orientación	Está alineado directamente con el gobierno control y la auditoria de sistemas informáticos.	Está orientado con la prestación y el mantenimiento de servicios de TI.	Está orientado al análisis de riegos que posee el sistema informático de TI. Esta guía va orientada a las Pequeñas y Medianas empresas, y dentro de las mismas, a los responsables de los sistemas de informacion, gerentes directivos o auditores.

Tabla 1.1: Tabla Comparativa de Metodologías.

Después de este análisis previo, hemos decidido utilizar la metodología de COBIT, que nos parece la más adecuada para poder identificar de mejor manera las necesidades de la unidad de TI del Hospital General “Enrique Garcés”. Existen varias versiones del marco de trabajo COBIT como la 4.1, la cual será utilizada en este trabajo de auditoría.

Las razones por la cuales se utilizará COBIT, son principalmente, porque incluye dentro de la metodología prácticas alineadas con las decisiones gerenciales y de gobierno de tecnología. Además de que COBIT está orientado para la auditoría de sistemas informáticos y el control de actividades gerenciales. Es necesario resaltar que los auditores pueden desenvolverse de mejor manera ya que existen las guías y directrices con las actividades que se deben realizar para identificar el nivel de madurez de los procesos implementados por el área de Ti de la empresa.

Además con la utilización de COBIT se pude mantener un marco de control interno, que puede ser útil para que la unidad de TI pueda mejorar en la

prestación de sus servicios, con lo cual se brindará un valor agregado al trabajo realizado dentro de la unidad de TI.

CAPÍTULO 2:

EJECUCIÓN DE LA AUDITORÍA

2.1. PLANIFICACIÓN DE AUDITORÍA

La planificación de la auditoria que se realizará al Hospital General “Enrique Garcés”, se la examinará en conjunto con el área de TI del mismo, y si es necesario con otras áreas del hospital que interactúa con el área de TI.

Se aplicarán técnicas de trabajo tales como:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Entrevistas.

Y herramientas tales como:

- Cuestionarios.
- Estándares del marco de trabajo de COBIT.

	Semana													
Actividad	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**
Conocimiento de la Situación Actual del Área de Sistemas														
Elaboración del Plan de Auditoría														
Puesta en marcha del plan de auditoría														
Evaluación y Análisis de Pruebas Realizadas														
Elaboración de Informes														
Informe Preliminar														
Informe Técnico														
Informe Ejecutivo														
Informe Final														

Tabla 2.1 Tabla de cruce de actividades

2.2. SITUACIÓN ACTUAL DEL ÁREA DE SISTEMAS

2.2.1. NIVEL DE DECISIÓN DE LA UNIDAD INFORMÁTICA

La unidad informática tiene un nivel de decisión de asistente del departamento de mantenimiento, es decir que se encuentra subrogado a este departamento. Esto hace que la unidad informática no cumpla en con un rol muy importante en la toma de decisiones gerenciales del hospital, sino más bien que la unidad esté orientada al soporte de usuarios y de aplicaciones.

Esto hace que las decisiones de la unidad informática no sean tomadas en cuenta, ya que no posee los elementos necesarios para desenvolverse libremente y tomar decisiones importantes en el manejo y planeación de las tecnologías de información del hospital.

2.2.2. ESTRUCTURA DE LA UNIDAD INFORMÁTICA

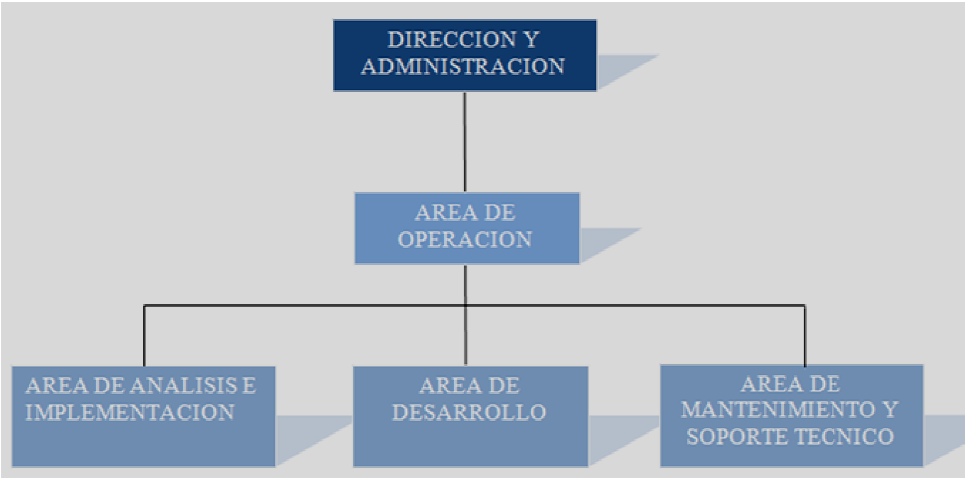


Figura 2.1 Estructura Orgánica Interna de la UI [15]

El Departamento de Sistemas es la unidad encargada de gestionar el apoyo informático a las actividades del Hospital General “Enrique Garcés”, mediante el diseño, coordinación, implementación y operación de las bases de datos institucionales y de la red institucional de computación, informática y central telefónica. Así mismo presta asesoramiento y apoyo a las diferentes unidades, servicios y departamentos del Hospital Enrique Garcés. [16]

Desde su creación el Departamento de Sistema no cuenta con una estructura organizacional definida así como también con personal que soporte la gran

[15] ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO DE SISTEMAS
[16] ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO DE SISTEMAS

demanda de usuarios, software, hardware e información existente en el hospital. [17]

2.2.3. FUNCIONES

Dentro del Hospital Enrique Garcés, el Departamento de Sistemas cumple diversas funciones que justificarán los puestos de trabajo establecidos, los cuáles se engloban a través de los siguientes:

- ✓ **Explotación de sistemas o aplicaciones.** La explotación u operación de un sistema informático o aplicación informática, utilización y aprovechamiento de los sistemas implementados y a desarrollarse. Previsión de fechas de realización de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema, supervisión de trabajos, etc.
- ✓ **Soporte técnico a usuarios.** El soporte, tanto para los usuarios como para el propio departamento, se ocupa de seleccionar, instalar y mantener el sistema operativo adecuado del diseño y control de la estructura de la base de datos, la gestión de los equipos de la red de datos y de voz, el estudio y evaluación de las necesidades y rendimientos del sistema y, por último, la ayuda directa a usuarios.
- ✓ **Gestión y Administración del propio centro de procesamiento de datos. Las** funciones de gestión y administración de un centro de procesamiento de datos engloban operaciones de supervisión, planificación y control de proyectos, seguridad de las instalaciones y equipos, gestión de manejos de cuentas de usuario y gestión de los propios recursos tecnológicos y humanos.

2.2.4. ÁREAS

Área de dirección y administración

Este es el encargado de administrar los suplementos del software, así como el responsable de monitorear cada área del departamento de sistemas, los requerimientos que para su buen desempeño sean necesarios, área encargada de organizar todas las funciones de las áreas del departamento.

[17] ESTRUCTURA ORGÁNICA DEL DEPARTAMENTO DE SISTEMAS

Área de operación

Esta área se encarga de brindar los servicios requeridos para el proceso de datos, como son: preparar los datos y suministros necesarios para el departamento de sistemas, manejar de archivo y documentación de las diferentes áreas, preparar de documentos del departamento y sus áreas.

Área de análisis e implementación

Esta área tiene la tarea de establecer un flujo de información eficiente a través de toda la institución con la realización de análisis de requerimientos informáticos tecnológicos mediante la utilización del tiempo suficiente para el estudio y la proposición de soluciones de los problemas planteando diferentes alternativas y el control de calidad de las mismas.

Área de desarrollo

Esta área se encarga del desarrollo de sistemas en la institución y la implementación de los mismos en coordinación con el área de Análisis, además se encargará del monitoreo continuo de los sistemas instalados en la institución, sus funciones son:

- Construir soluciones integrales (aplicaciones) a las necesidades de información de los usuarios.
- Usar las técnicas de construcción de sistemas de información orientadas netamente a la productividad del personal y a la satisfacción plena del usuario.
- Construir equipos de trabajo con la participación del usuario y del personal técnico de acuerdo a metodologías establecidas.
- Mantener informado al área de Dirección y Administración de los avances, atrasos y problemas que se presentan rutinariamente.

- **Área de mantenimiento y soporte técnico**

Área responsable de la gestión del hardware y del software dentro de las instalaciones del Hospital Enrique Garcés, entendiendo por gestión: estrategia, planificación, instalación, backups (Respaldo de información) y mantenimiento. Algunas funciones principales generales que realiza esta área son:

- Planificar la modificación e instalación de nuevo software y hardware.
- Evaluar los nuevos paquetes de software y nuevos productos de hardware.

- Dar el soporte técnico necesario para el desarrollo de nuevos proyectos, evaluando el impacto de los nuevos proyectos en el sistema instalado.
- Asegurar la disponibilidad del sistema, y la coordinación necesaria para la resolución de los problemas técnicos en su área.
- Administrar, organizar y operar todos los recursos del Centro de Cómputo y Comunicaciones de la Institución.
- Las demás que le asigne el Área de Dirección y Administración.

2.2.5. INVENTARIO DE HARDWARE

A continuación se especifica un listado del hardware que posee el Hospital General "Enrique Garcés":

Servidores	Nro.	Especificación
Servidor Web	1	Intel Core i3 2GB RAM 500 GB Disco Duro Windows 7
Servidor de Directorio Activo y DNS	1	Servidor HP Proligh ML350 Intel Xeon Processor 2.8 GHz 2GB RAM 350 GB Disco Duro Windows Server 2003 Standard
Servidor de Aplicaciones y DNS	1	Intel Core i3 2GB RAM 500 GB Disco Duro Linux Ubuntu Server 10.04
Clientes	**Nro.**	**Especificación**
Intel Pentium 4	148	3.2 GHz, 2 GB RAM
Portátiles	5	2.2 GHz, 2 GB RAM

Tabla 2.2: Inventario de hardware HEG

2.2.6. INVENTARIO DE SOFTWARE

A continuación, se menciona el tipo de software que es utilizado como infraestructura de software y los sistemas desarrollados para el funcionamiento del hospital. [18]

[18] EntreGrado por la Unidad de TI

Software	N°Licencias
Adobe Acrobat 5.0	6
Microsoft SQL Server 2005	2
Nero	5
Windows Xp service pack 2	110
Windows Xp service pack 3	12
Windows vista versión 6.1	5
Microsoft® Windows Vista Business	23
Microsoft® Windows Server® 2008	40
OpenOffice 2.4	4

Tabla 2.3: Inventario de software HEG

2.2.7. TOPOLOGÍA DE RED

La topología de red que posee el Hospital Enrique Garcés es una topología mixta que se encuentra dividida en dos partes, una para el área interna de sistemas, la planta baja y el primer piso, la cual es una topología tipo árbol con 3 switches principales dispuestos en cascada, y para el resto del hospital (del segundo al noveno piso) una topología en estrella. El tipo de cableado que se utiliza para las conexiones internas del hospital es cable par trenzado UTP Categoría 5e y UTP Categoría 6.

Esto hace que la topología sea compleja de analizar, lo que se ve reflejado en el diagrama de red de la figura 2.2 que se mostrará más adelante, es así que para la realización de esta tesis nos referiremos a la topología como una topología en árbol. Ya que es la topología que más se ajusta al diagrama de red del hospital.

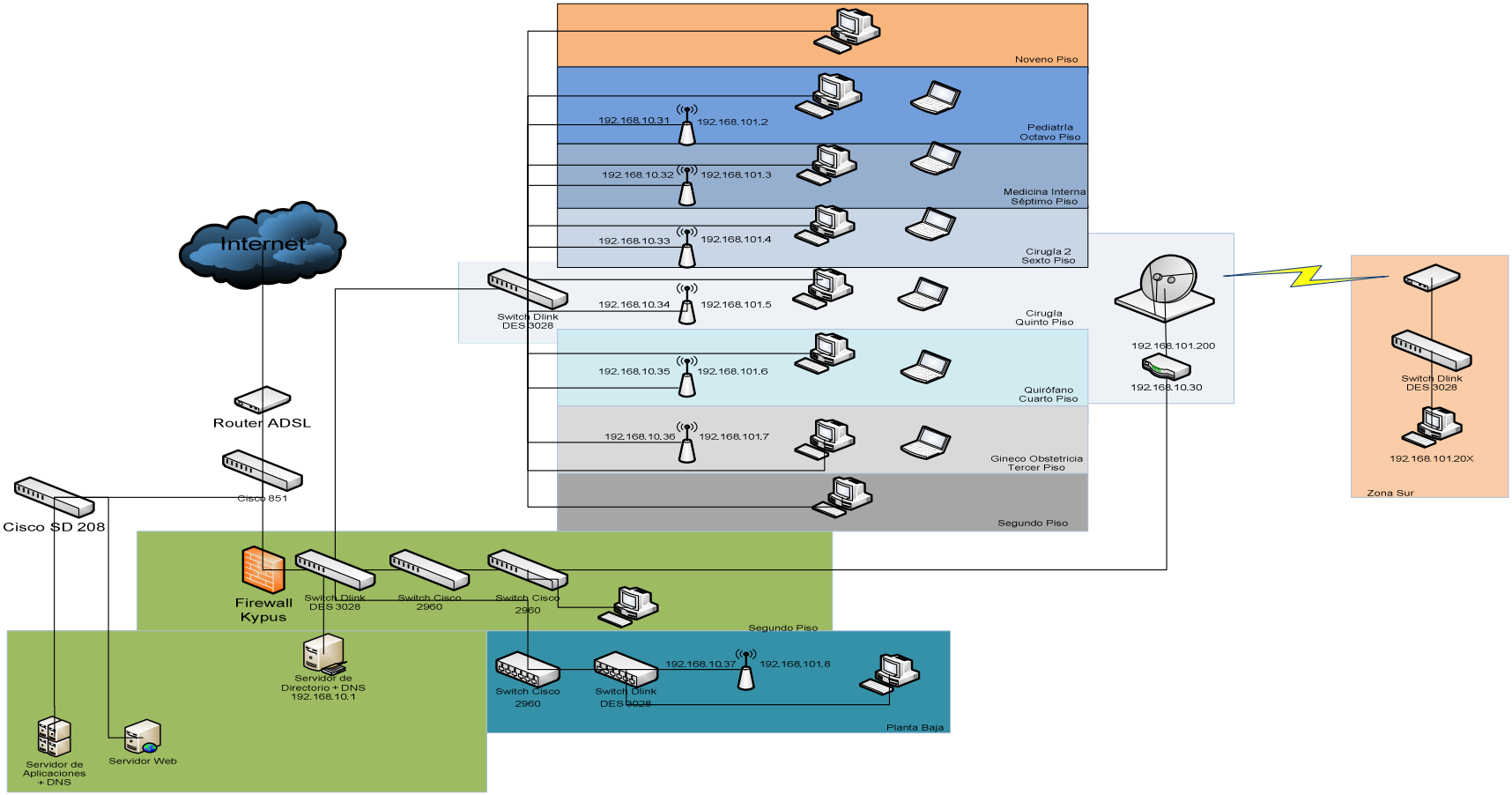


Figura 2.2: Topología de red del Hospital Genera "Enrique Garcés" [19]

[19] Realizado por Del Hierro Pablo y Trujillo Mauricio

Leyenda

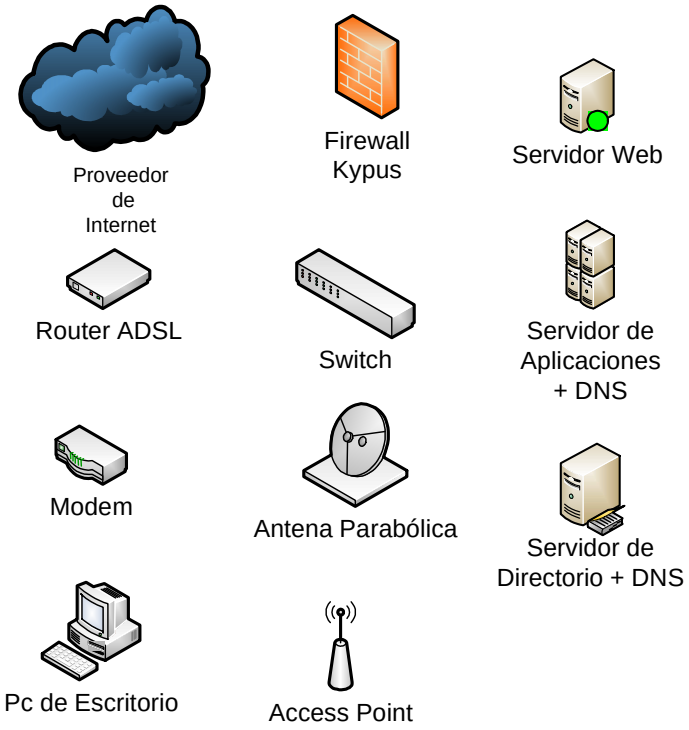


Figura 2.3: Leyenda Topología de Red Hospital Genera "Enrique Garcés" [20]

[20] Realizado por Del Hierro Pablo y Trujillo Mauricio

2.2.8. SEGURIDADES

2.2.8.1. Seguridad Física

Todas las instalaciones deberían tener al menos una puerta de escape, y deben estar ubicadas dentro del edifico.

En el Hospital General “Enrique Garcés” se ha implementado en varias medidas de seguridad digital y control, mediante la implementación de cámaras de vigilancia en las principales áreas del hospital, con las cuales se controla el ingreso de personas no deseadas y el trabajo del personal.

También se cuenta con personal de seguridad a toda hora con cambios de turno que varían durante la semana.

Por otro lado se pudo constatar que los servidores se encuentran en un cuarto frio, que no posee las medidas suficientes de seguridad. Este cuarto de servidores se encuentra dentro de la unidad de TI del hospital, y para su ingreso posee una puerta corrediza sin seguros la cual no garantiza el acceso de personal no autorizado.

Como seguridad el área de TI posee una sobrepuerta metálica con candado y una puerta de madera con chapa normal, que se abre solamente desde adentro o con las llaves respectivas. No se lleva un control adecuado de las personas que ingresan al área de TI.

Los empleados de la unidad informática, al igual que todo el hospital, cuentan con procedimientos a seguir en caso de emergencia debido a accidentes o desastres naturales. El hospital cuenta con rutas físicas de escape señaladas adecuadamente.

2.2.8.2. Seguridad Lógica

La seguridad lógica del Hospital General “Enrique Garcés” maneja perfiles de usuario, que son administrados por la unidad de TI a través del servidor de directorio activo (Active Directory), permitiendo el acceso a los computadores del hospital al personal autorizado, por medio de un usuario y contraseña otorgando solamente las opciones y privilegios correspondientes a su perfil.

Para acceso a la red del hospital e Internet, por medio de los puntos de acceso inalámbricos se requiere de la contraseña correspondiente, la cual es administrada por la unidad de TI, así como el tipo de seguridad de la señal inalámbrica.

Administración de cuentas de usuario

El responsable del área de mantenimiento y soporte técnico de la unidad informática es el encargado de asignar las cuentas de usuario al personal del hospital con acceso a computadoras, estas cuentas y contraseñas son personales e intransferibles y sin ellas no se puede acceder a un equipo del hospital.

Para la autenticación de los usuarios se dispone de un número máximo de intentos para acceder con una cuenta, caso contrario el equipo procede a bloquearse por un tiempo determinado.

Almacenamiento de los respaldos

No se realizan respaldos periódicos tanto de la información del área de TI como la de las otras áreas del hospital, los respaldos se los realizan de forma reactiva cuando se necesita formatear o reemplazar un equipo.

Política para generar respaldos

No se maneja una política para generar respaldos, estos se generan de forma manual por parte de los empleados de la unidad de TI.

2.3. REALIZACIÓN DE LA AUDITORÍA

En esta sección se analizarán los dominios, procesos y objetivos de control planteados por la metodología COBIT que han sido seleccionados con la ayuda del tutor para la evaluación de la unidad de TI del Hospital General “Enrique Garcés”. Debido al tamaño de la unidad de TI no se pueden evaluar todos los procesos y objetivos de control, solamente los detallados a continuación:

Planear y Organizar

1. PO1 Definir un plan estratégico de TI
    a. PO1.2 Alineación de TI con el Negocio
    b. PO1.3 Evaluación del Desempeño y la Capacidad Actual
    c. PO1.4 Plan Estratégico de TI
2. PO2 Definir la arquitectura de la información
    a. PO2.1 Modelo de Arquitectura de Información Empresarial
    b. PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
    c. PO2.4 Administración de Integridad
3. PO3 Determinar la dirección tecnológica
    a. PO3.1 Planeación de la Dirección Tecnológica
    b. PO3.2 Plan de Infraestructura Tecnológica
4. PO4 Definir los procesos, organización y relaciones de la TI
    a. PO4.4 Ubicación Organizacional de la Función de TI
    b. PO4.5 Estructura Organizacional
    c. PO4.6 Establecimiento de Roles y Responsabilidades
    d. PO4.12 Personal de TI
    e. PO4.14 Políticas y Procedimientos para Personal Contratado
    f. PO4.15 Relaciones
5. PO6 Comunicar las aspiraciones de la dirección de la gerencia
    a. PO6.3 Administración de Políticas para TI
    b. PO6.4 Implantación de Políticas de TI
    c. PO6.5 Comunicación de los Objetivos y la Dirección de TI
6. PO9 Evaluar y administrar los riesgos de TI
    a. PO9.3 Identificación de Eventos
    b. PO9.4 Evaluación de Riesgos de TI
    c. PO9.5 Respuesta a los Riesgos

Adquirir e Implementar

1. AI2 Adquirir y mantener software aplicativo
    a. AI2.4 Seguridad y Disponibilidad de las Aplicaciones
    b. AI2.5 Configuración e Implantación de Software Aplicativo Adquirido
    c. AI2.7 Desarrollo de Software Aplicativo
    d. AI2.10 Mantenimiento de Software Aplicativo
2. AI3 Adquirir y mantener infraestructura tecnológica
    a. AI3.1 Plan de Adquisición de Infraestructura Tecnológica
    b. AI3.3 Mantenimiento de la Infraestructura
3. AI5 Adquirir recurso de TI / Adquirir y mantener arquitectura tecnológica
    a. AI5.3 Selección de Proveedores
    b. AI5.4 Adquisición de Recursos de TI

Entregar y dar soporte

1. DS1 Definir y administrar los niveles de servicio
    a. DS1.2 Definición de Servicios
    b. DS1.3 Acuerdos de Niveles de Servicio
    c. DS1.4 Acuerdos de Niveles de Operación
2. DS5 Garantizar la seguridad de los sistemas
    a. DS5.2 Plan de Seguridad de TI
    b. DS5.4 Administración de Cuentas del Usuario
    c. DS5.9 Prevención, Detección y Corrección de Software Malicioso
    d. DS5.10 Seguridad de la Red
3. DS7 Educar y entrenar a los usuarios
    a. DS7.1 Identificación de Necesidades de Entrenamiento y Educación
    b. DS7.2 Impartición de Entrenamiento y Educación
    c. DS8 Administrar la mesa de servicio y los incidentes
4. DS10 Administrar los problemas / Administrar Problemas e incidentes
    a. DS10.1 Identificación y Clasificación de Problemas
    b. DS10.2 Rastreo y Resolución de Problemas
    c. DS10.3 Cierre de Problemas
5. DS12 Administrar el ambiente físico / Administrar Instalaciones
    a. DS12.2 Medidas de Seguridad Física
    b. DS12.3 Acceso Físico

Monitorear y Evaluar

1. ME1 Monitorear y Evaluar el Desempeño de TI / Monitorear los procesos
    a. ME1.4 Evaluación del Desempeño
    b. ME1.6 Acciones Correctivas
2. ME4 Proporcionar Gobierno de TI / Evaluar lo adecuado del control Interno.
    a. ME4.2 Alineamiento Estratégico
    b. ME4.4 Administración de Recursos
    c. ME4.5 Administración de Riesgos
    d. ME4.6 Medición del Desempeño

Esta información ha sido obtenida en base a entrevistas, encuestas, observaciones y con la ayuda del tutor de la tesis. Con el soporte de las guías y directrices brindadas por COBIT para realizar la auditoria.

2.3.1. PROCESOS DEL DOMINIO DE PLANEACIÓN Y ORGANIZACIÓN.

2.3.1.1. PO1 Definir un Plan Estratégico De TI

Guías de auditoria

Considerando si:

Las políticas y procedimientos de negocios de la función de servicios de información siguen un enfoque de planeación estructurado. Se ha establecido una metodología para formular y modificar los planes y que cubre, como mínimo:

- Misión y las metas de la organización
- Iniciativas de tecnología de información para soportar la misión y las metas de la organización
- Inversión óptima de las inversiones en tecnología de información actuales y futuras

Existen planes de tecnología de información a corto y largo plazo, están actualizados, están dirigidos adecuadamente a toda la empresa, su misión y funciones clave de negocios.

Los propietarios de procesos y la Gerencia llevan a cabo revisiones y aprobaciones formales a los planes de TI.

La ausencia de planeación a largo plazo para los sistemas de información y la estructura que lo soporta resulta en sistemas que no soportan los objetivos de la empresa ni los procesos del negocio, o no proveen integridad, seguridad y control apropiados.

Probando que:

Las minutas de las reuniones del comité de Planeación/dirección de la función de servicios de información reflejan el proceso de planeación.

Los entregables de la metodología de planeación existen según lo indicado.

Los planes a corto y largo plazo de tecnología de información son consistentes con los planes a corto y largo plazo de la organización, así como con los requerimientos de ésta.

Se han modificado los planes para reflejar condiciones cambiantes.

Los planes a largo plazo de tecnología de información son traducidos periódicamente en planes a corto plazo.

Existen tareas para implementar los planes.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO1.2 Alineación de TI con el Negocio	Entrevista al gerente de servicios generales. Entrevista al director de TI. Entrevista a una secretaria del hospital.	Orgánico Funcional del Hospital General "Enrique Garcés". Orgánico Funcional del área de TI. Presentación del nuevo sistema de seguridad y de consulta de pacientes.	El área de TI está en proceso de adaptación de algunos procesos directamente alineados con el negocio. El área de TI está aportando con herramientas que facilitan procesos del negocio del hospital.
PO1.3 Evaluación del Desempeño y la Capacidad Actual	Entrevista al director de TI. Entrevista con un médico del hospital. Entrevista a una secretaria del hospital.	Orgánico Funcional del Hospital General "Enrique Garcés".	El área de TI está considerada como un área que cumple su trabajo adecuadamente según las entrevistas realizadas. Se tiene un déficit de personal para cubrir con todas las tareas que el hospital demanda.

			No se tiene una metodología para resolver problemas dentro del hospital.
PO1.4 Plan Estratégico de TI	Entrevista al director de TI. Entrevista a un empleado de soporte técnico.	Orgánico Funcional del Hospital General "Enrique Garcés". Orgánico Funcional del área de TI.	No existe un plan estratégico informático dentro del hospital.

Tabla 2.3: Tabla Resumen PO1

Dominio: Planeación y Organización				
Proceso: PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.	√		**Grado de Madurez** El proceso de definir un plan estratégico de TI se encuentra en un nivel 1. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se ha establecido un plan estratégico para la unidad de TI que permita tener las políticas claras y que cubra todas las necesidades requeridas.
Nivel 1	La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requerimiento de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.	√		
Nivel 2	La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.		√	
Nivel 3	Una política define cómo y cuándo realizar la planeación estratégica de TI. La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Sin embargo, se otorga discrecionalidad a gerentes individuales específicos con respecto a la implantación del proceso, y no existen procedimientos para analizar el proceso. La estrategia general de TI incluye una definición consistente de los riesgos que la			

	organización está dispuesta a tomar como innovador o como seguidor. Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías. La planeación estratégica de TI se discute en reuniones de la dirección del negocio			
Nivel 4	La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La planeación estratégica de TI es una función administrativa definida con responsabilidades de alto nivel. La dirección puede monitorear el proceso estratégico de TI, tomar decisiones informadas con base en el plan y medir su efectividad. La planeación de TI de corto y largo plazo sucede y se distribuye en forma de cascada hacia la organización, y las actualizaciones se realizan según son necesarias. La estrategia de TI y la estrategia organizacional se vuelven cada vez más coordinadas al abordar procesos de negocio y capacidades de valor agreGrado y al apalancar el uso de aplicaciones y tecnologías por medio de la re-ingeniería de procesos de negocio. Existen procesos bien definidos para determinar el uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas			
Nivel 5	La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Las consideraciones de riesgo y de valor agreGrado se actualizan de modo constante en el proceso de planeación estratégica de TI. Se desarrollan planes realistas a largo plazo de TI y se actualizan de manera constante para reflejar los cambiantes avances tecnológicos y el progreso relacionado al negocio. Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia. El plan estratégico especifica cómo los nuevos avances tecnológicos pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.			

Tabla 2.4: Modelo de Madurez PO1

COBIT plantea para el PO1 la necesidad de cumplir con los siguientes objetivos de control:

1. TI como parte del Plan a largo y corto plazo
2. Plan a largo plazo de TI
3. Plan a largo plazo de TI - Enfoque y Estructura
4. Cambios al Plan a largo plazo de TI
5. Planeación a corto plazo para la Función de Servicios de Información
6. Comunicación de los planes de TI
7. Monitoreo y evaluación de los planes de TI.
8. Evaluación de los sistemas existentes

El PO1 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Definir un plan estratégico a corto plazo que se ajuste directamente con la línea del negocio, y que sea discutido en las reuniones de dirección como un punto importante dentro de la agenda, para con ello tener una correcta estrategia dentro del área de TI. • Una vez creado un plan estratégico para la unidad de TI, se debe comenzar a identificar los riegos a los cuales está sujeta la unidad dentro del hospital. • Se recomienda también, que una vez creado este plan estratégico, se dé a conocer a todos los empleados del hospital, para que estos conozcan cuales son las responsabilidades que tiene la unidad de TI.
Estrategias a largo plazo	• Crear un plan estratégico a largo plazo, en donde se consideren los objetivos del negocio, la definición del área de TI y su ubicación dentro del hospital, además que se tome en cuenta infraestructura, inventario y soluciones tecnológicas que el área tenga que plantear. • Se recomienda tener una comunicación más directa con la dirección y gerencia del hospital, para llevar un mejor control y monitoreo de los planes y acciones de la unidad de TI. Al igual que manejar un política clara dentro del plan estratégico para la unidad. • Ubicar a la unidad de TI dentro del hospital como una unidad asesora, no como parte del departamento de mantenimiento, para que así pueda alinearse con el negocio de mejor manera.

Tabla 2.5: Estrategias a corto y largo plazo PO1

2.3.1.2. PO2 Definición de la Arquitectura de Información

Guías de auditoria

Considerando si:

Las políticas y procedimientos de la función de los servicios de información se enfocan al desarrollo y mantenimiento del diccionario de datos.

Se utiliza algún proceso para mantener actualizados el diccionario de datos y las reglas de sintaxis de datos.

Se utiliza algún medio para distribuir el diccionario de datos para asegurar que éste sea accesible para las áreas de desarrollo y que los cambios se reflejen inmediatamente

Los estándares definen la clasificación "default" para los activos de datos que no contienen un identificador de clasificación.

Probando que:

La evaluación del impacto de cualquier modificación realizada al diccionario de datos y cualquier cambio realizado al diccionario de datos para asegurar que éstos han sido comunicados efectivamente.

La documentación del diccionario de datos sea adecuada para confirmar que ésta define los atributos de datos y los niveles de seguridad para cada elemento de datos.

Cada clasificación de datos defina claramente:

- Quién puede tener acceso
- Quién es responsable de determinar el nivel de acceso apropiado
- La aprobación específica requerida para el acceso
- Los requerimientos especiales para el acceso (por ejemplo, acuerdo de confidencialidad o no revelación)

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO2.1 Modelo de Arquitectura de Información Empresarial	Entrevista al director de TI. Dirección de la función de servicios de información.	No existen documentos de la arquitectura de la información.	No existe un modelo de la arquitectura de la información del Hospital General “Enrique Garcés”. No se ha definido la arquitectura que el hospital va a manejar para la información.
PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos	Entrevista líder de TI Gerencia de la función de servicios de información.	No existen documentos acerca del diccionario de datos.	No se tiene ningún diccionario de datos o de reglas de sintaxis de datos. No se encuentra especificado en ningún lugar los detalles de los datos de información.

PO2.4 Administración de Integridad	Entrevista líder de TI Dirección de la función de servicios de información.	No existen procedimientos ni reglas para garantizar la integridad y consistencia de la información.	No se tienen ningún control para asegurar la integridad y la consistencia de la información.

Tabla 2.6: Tabla Resumen PO2

Dominio: Planeación y Organización				
Proceso: PO2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.	√		**Grado de Madurez** El proceso de definición de la arquitectura de información se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se maneja la información como una arquitectura, lo que hace que esta no se encuentre estandarizada, ni se reconozca su importancia.
Nivel 1	La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.		√	
Nivel 2	Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas. Los requerimientos tácticos impulsan el desarrollo de los componentes de la arquitectura de la información por parte de los individuos.			
Nivel 3	La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera			

	consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información. Las herramientas automatizadas se empiezan a utilizar, aunque los procesos y reglas son definidos por los proveedores de software de bases de datos. Un plan formal de entrenamiento ha sido desarrollado, pero el entrenamiento formal se basa en iniciativas individuales.			
Nivel 4	Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. La responsabilidad sobre el desempeño del proceso de desarrollo de la arquitectura se refuerza y se mide el éxito de la arquitectura de información. Las herramientas automatizadas de soporte están ampliamente generalizadas, pero todavía no están integradas. Se han identificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es proactivo y se enfoca en resolver necesidades futuras del negocio. La organización de administración de datos está activamente involucrada en todos los esfuerzos de desarrollo de las aplicaciones, para garantizar la consistencia. Un repositorio automatizado está totalmente implementado. Se encuentran en implantación modelos de datos más complejos para aprovechar el contenido informativo de las bases de datos. Los sistemas de información ejecutiva y los sistemas de soporte a la toma de decisiones aprovechan la información existente.			
Nivel 5	La arquitectura de información es reforzada de forma consistente a todos los niveles. El valor de la arquitectura de la información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio. La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información			

	incluyendo un proceso de mejora continua. La estrategia para el aprovechamiento de la información por medio de tecnologías de bodega de datos y minería de datos está bien definida. La arquitectura de la información se encuentra en mejora continua y toma en cuenta información no tradicional sobre los procesos, organizaciones y sistemas.			

Tabla 2.7: Modelo de Madurez PO2

COBIT plantea para el PO2 la necesidad de cumplir con los siguientes objetivos de control.

1. Modelo de la Arquitectura de Información
2. Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación
3. Esquema de Clasificación de Datos
4. Niveles de Seguridad

El PO2 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Definir un modelo de la arquitectura de la información, un diccionario de datos y reglas de sintaxis para que sea manejados por todos los usuarios. • Crear y comunicar un esquema de datos estándar para todos los usuarios. • Establecer procedimientos formales para la clasificación y estructura de la información, para que la misma esté bien organizada.
Estrategias a largo plazo	• Crear un repositorio de datos automatizado, en el cual se encuentren los datos bajo las reglas del diccionario de datos, manteniendo a su vez también las reglas de sintaxis de los mismos. • Crear procesos y procedimientos que mantengan actualizado el diccionario de datos y las reglas de sintaxis. • Mantener la consistencia e integridad de la información en todo momento. • Crear estándares para los valores que se necesiten poner por defecto para acoplarse al diccionario de datos.

Tabla 2.8: Estrategias a corto y largo plazo PO2

2.3.1.3. PO3 Determinación de la Dirección Tecnológica

Guías de auditoria

Considerando si:

Existe un proceso para la creación y la actualización regular del plan de infraestructura tecnológica, que confirme que los cambios propuestos estén siendo examinados primero para evaluar los costos y riesgos inherentes, y que la aprobación de la Gerencia se obtenga antes de realizar cualquier cambio al plan.

El plan de infraestructura tecnológica está siendo comparado contra los planes a largo y corto plazo de tecnología de información.

La administración de la función de los servicios de información evalúa tecnologías de vanguardia e incorpora tecnologías apropiadas a la infraestructura de servicios de información actual.

Los planes de adquisición de hardware y software suelen satisfacer las necesidades identificadas en el plan de infraestructura tecnológica y si éstos son aprobados apropiadamente.

Probando que:

La administración de la función de servicios de información comprende y utiliza el plan de infraestructura tecnológica.

Se hayan realizado cambios al plan de infraestructura tecnológica para identificar los costos y riesgos asociados, y que dichos cambios reflejen las modificaciones a los planes a largo y corto plazo de tecnología de información.

El plan de adquisición de hardware y software cumple con los planes a largo y corto plazo de tecnología de información, reflejando las necesidades identificadas en el plan de infraestructura tecnológica.

El acceso permitido sea consistente con los niveles de seguridad definidos en las políticas y procedimientos de la función de servicios de información, y que se haya obtenido la autorización apropiada para el acceso.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO3.1 Planeación de la Dirección Tecnológica	Entrevista al gerente de servicios generales. Entrevista al director de TI.	Orgánico Funcional del Hospital General “Enrique Garcés”.	No se tiene un plan sobre cuál es la dirección tecnológica alineada con el negocio y las estrategias de TI.
PO3.2 Plan de Infraestructura Tecnológica	Entrevista al gerente de servicios generales. Entrevista al director de TI.	Presupuesto 2011 para el área informática.	No se tiene un presupuesto para la adquisición de recursos tecnológicos, esto se lo hace en base a los requerimientos del día a día. No se tiene un plan de infraestructura tecnológica ni acuerdos para contingencias.

Tabla 2.9: Tabla Resumen PO3

Dominio: Planeación y Organización				
Proceso: PO3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento de que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.	√		**Grado de Madurez.** El proceso de determinación de la dirección tecnológica se encuentra en un nivel 1. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" se reconoce la importancia de una correcta dirección tecnológica, sin embargo la adquisición e implementación de tecnologías se lo hace sin planificación.
Nivel 1	La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.	√		
Nivel 2	Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de los cambios tecnológicos se delega a individuos que siguen procesos intuitivos, aunque similares. Las personas obtienen sus habilidades sobre planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. Están surgiendo técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.		√	

Nivel 3	La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional. Los proveedores clave se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos, de forma consistente con la dirección de la organización.			
Nivel 4	La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidades necesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentes se toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica ha sido asignado. El proceso para desarrollar el plan de infraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. La estrategia de recursos humanos está alineada con la dirección tecnológica, para garantizar que el equipo de TI pueda administrar los cambios tecnológicos. Los planes de migración para la introducción de nuevas tecnologías están definidos. Los recursos externos y las asociaciones se aprovechan para tener acceso a la experiencia y a las habilidades necesarias. La dirección ha evaluado la aceptación del riesgo de usar la tecnología como líder, o rezagarse en su uso, para desarrollar nuevas oportunidades de negocio o eficiencias operativas.			
Nivel 5	Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas			

	industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avances industriales e internacionales, en lugar de estar orientada por los proveedores de tecnología. El impacto potencial de los cambios tecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe una aprobación ejecutiva formal para el cambio de la dirección tecnológica o para adoptar una nueva. La entidad cuenta con un plan robusto de infraestructura tecnológica que refleja los requerimientos del negocio, es sensible a los cambios en el ambiente del negocio y puede reflejar los cambios en éste. Existe un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica. Las mejores prácticas de la industria se usan de forma amplia para determinar la dirección técnica.			

Tabla 2.10 Modelo de Madurez PO3

COBIT plantea para el PO3 la necesidad de cumplir con los siguientes objetivos de control.

1. Planeación de la Infraestructura Tecnológica
2. Monitoreo de Tendencias y Regulaciones Futuras
3. Contingencias en la Infraestructura Tecnológica
4. Planes de Adquisición de Hardware y Software
5. Estándares de Tecnología

El PO3 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Determinar un presupuesto, para crear una infraestructura tecnológica sólida y que se ajuste a las necesidades y requerimientos del hospital. • Difundir por parte de la unidad de TI la importancia de contar con una infraestructura sólida, para atender a los usuarios de una mejor manera. • Realizar capacitaciones para que los usuarios pueda aprovechar las ventajas que las herramientas tecnológicas les brindan.
Estrategias a largo plazo	• Crear un plan de dirección tecnológica a largo plazo en el cual se revisen y evalúen los riegos y problemas de la unidad tecnológica. • Crear y revisar planes de adquisición y renovación, para la infraestructura tecnológica. • Establecer procesos para conocer las tendencias tecnológicas de acuerdo con el sector hospitalario y utilizar esta información en la elaboración del plan de infraestructura tecnológica.

Tabla 2.11 Estrategias a corto y largo plazo PO3

2.3.1.4. PO4 Definición de la Organización y de las Relaciones De Ti

Guías de auditoria

Considerando si:

Las políticas y las comunicaciones de la Gerencia aseguran la independencia y la autoridad de la función de los servicios de información.

Se han definido e identificado la calidad de miembro, los roles y las responsabilidades del comité de planeación/dirección de TI.

Los estatutos del comité de planeación/dirección de TI alinean las metas del comité con los objetivos y los planes a largo y corto plazo de la organización y con los objetivos y planes a largo y corto plazo de TI.

Las políticas consideran la necesidad de evaluar y modificar la estructura organizacional para satisfacer objetivos y circunstancias cambiantes.

Existen procesos e indicadores de desempeño para determinar la efectividad y aceptación de TI.

La Gerencia se asegura que los roles y responsabilidades se cumplen.

Existen políticas que determinen los roles y responsabilidades para todo el personal dentro de la organización con res-pecto a sistemas de información, control interno y seguridad.

Existen políticas y funciones de aseguramiento de la calidad.

La función de aseguramiento de la calidad cuenta con la independencia suficiente con respecto al personal de desarrollo de sistemas y con una asignación de personal y experiencia adecuados para llevar a cabo sus responsabilidades.

Existen procedimientos establecidos dentro del aseguramiento de la calidad para programar15 recursos y asegurar el cumplimiento de las pruebas y aprobación del aseguramiento de la calidad antes de que se implementen nuevos sistemas o cambios a los sistemas.

El oficial de seguridad de la información comprende adecuadamente sus funciones y responsabilidades y si éstas han mostrado consistencia con respecto a la política de seguridad de la información de la organización.

Existen procedimientos para revisar y mantener cambios en la propiedad de los datos y los sistemas regularmente.

Existen políticas y procedimientos en TI para controlar las actividades de consultores y demás personal por contrato, asegurando así la protección de los activos de la organización.

Existen procedimientos aplicables a los contratos de TI y son adecuados y consistentes con las políticas de adquisición de la organización.

Probando que:

La dirección de TI supervisa la función de servicios de información y sus actividades y determina acciones para resolver puntos pendientes.

La jerarquía de reporte es apropiada para TI.

La efectividad de la ubicación de TI dentro de la organización para facilitar una relación de socios con la alta Gerencia.

La gerencia de TI comprende cuáles son los procesos utilizados para monitorear, medir y reportar el desempeño de TI.

La utilización de indicadores clave para evaluar el desempeño.

Las acciones realizadas por la administración en cuanto a cualquier variación significativa con respecto a los niveles de desempeño esperados.

La administración de usuarios/propietarios evalúa la capacidad de respuesta y la habilidad de TI para proporcionar soluciones de tecnología de información que satisfagan las necesidades de usuarios/propietarios.

La Gerencia de TI conoce sus funciones y responsabilidades.

Aseguramiento de la calidad se involucra en la prueba y aprobación de los planes de proyectos de TI.

El mantenimiento de la competencia del personal de tecnología de información.

Descripciones de puestos de trabajo apropiadas, para la adecuación y la claridad de las responsabilidades, autoridad y criterios de desempeño.

Los términos de los contratos sean consistentes con los estándares normales para contratos de la organización y que los términos y condiciones contractuales estándar hayan sido revisados y evaluados por un consultor legal, que haya sido contratado para tal fin.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO4.4 Ubicación Organizacional de la Función de TI	Entrevista al gerente de servicios generales. Entrevista al director de TI.	Orgánico Funcional del Hospital General “Enrique Garcés”. Orgánico Funcional del área de TI.	El área de sistemas está ubicada como un sub departamento del área de mantenimiento. El área de TI no tiene un nivel de asesor como debería dentro del hospital. Las acciones que realice el área de TI tienen que ser informadas al departamento de mantenimiento.
PO4.5 Estructura Organizacional	Entrevista al gerente de servicios generales.	Orgánico Funcional del Hospital General “Enrique Garcés”.	Se tiene asignada el área de influencia del departamento de TI.

		Orgánico Funcional del área de TI.	
PO4.6 Establecimiento de Roles y Responsabilidades	Entrevista al gerente de servicios generales. Entrevista al director de TI.	Orgánico Funcional del área de TI.	Se tiene bien definidos los roles del personal del área de TI. Existe una sobrecarga de responsabilidades para los empleados del área de TI, lo cual dificulta su trabajo.
PO4.12 Personal de TI	Entrevista al director de TI.	Orgánico Funcional del área de TI.	Falta personal en el área de TI para brindar soporte y acciones rápidas para las necesidades del hospital. No se evalúan los requerimientos de personal de forma regular o con la existencia de cambios

			importantes.
PO4.14 Políticas y Procedimientos para Personal Contratado	Entrevista al director de TI. Entrevista a un empleado de soporte técnico.	Orgánico Funcional del área de TI.	No existen procedimientos que regulen en cumplimiento de las políticas del hospital para el personal de TI.
PO4.15 Relaciones	Entrevista al director de TI. Entrevista a una secretaria del hospital. Entrevista a un empleado de soporte técnico.	Orgánico Funcional del área de TI. Acuerdos de nivel de calidad del servicio impuesto por el hospital.	Las relaciones del departamento de TI con otras áreas son cordiales, y se las realiza por teléfono en su mayoría.

Tabla 2.12: Tabla Resumen PO4

Dominio: Planeación y Organización				
Proceso: PO4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE TI				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.	√		**Grado de Madurez.** El proceso de definición de la organización y de las relaciones de TI se encuentra en un nivel 1. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" se encuentran definida las actividades y funciones del área de TI, pero no está organizada para responder de forma táctica a las necesidades de los clientes.
Nivel 1	Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. TI se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizadas ni reforzadas.	√		
Nivel 2	La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores.		√	
Nivel 3	Existen roles y responsabilidades definidos para la organización de TI y para terceros. La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno. Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores.			

	La organización de TI está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. Existe una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades está definida e implantada.			
Nivel 4	La organización de TI responde de forma proactiva al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas. Se han aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implementar y monitorear la organización deseada y las relaciones. Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional. El equilibrio entre las habilidades y los recursos disponibles internamente, y los que se requieren de organizaciones externas están definidos y reforzados. La estructura organizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesos estratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.			
Nivel 5	La estructura organizacional de TI es flexible y adaptable. Se ponen en funcionamiento las mejores prácticas de la industria. Existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI. La tecnología se aprovecha para apoyar la complejidad y distribución geográfica de la organización. Un proceso de mejora continua existe y está implantado.			

Tabla 2.13 Modelo de madurez PO4

COBIT plantea para el PO4 la necesidad de cumplir con los siguientes objetivos de control.

1. Comité de planeación o dirección de la función de servicios de información
2. Ubicación de los servicios de información en la organización
3. Revisión de Logros Organizacionales
4. Roles y Responsabilidades
5. Responsabilidad del aseguramiento de calidad
6. Responsabilidad de la Seguridad Lógica y Física
7. Propiedad y Custodia
8. Propiedad sobre Datos y Sistemas
9. Supervisión
10. Segregación de Funciones
11. Asignación de Personal para Tecnología de Información
12. Descripción de Puestos de trabajo para el Personal de TI
13. Personal Clave de Tecnología de Información
14. Políticas y Procedimientos para el personal por contrato
15. Relaciones

El PO4 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Crear un documento en donde se especifiquen las funciones y responsabilidades de todos los empleados del área de TI, y que el mismo sea difundido, en todo el hospital. • Crear un documento en el cual consten todos los logros institucionales, y cuáles son las metas a futuro. • Creación y difusión de las políticas que deben regir a los empleados del área de TI.
Estrategias a largo plazo	• Mejorar las relaciones y comunicaciones entre el área de TI y el personal administrativo. • Supervisar las acciones realizadas por los empleados para verificar que estén cumpliendo con sus obligaciones. • Crear políticas que asegure la calidad del servicio brindado por la unidad de TI

Tabla2.14: Estrategias a corto y largo plazo PO4

2.3.1.5. PO6 Comunicación de los objetivos y de las aspiraciones de la gerencia

Guías de auditoria

Considerando si:

Las políticas y procedimientos de la organización crean un marco referencial y un programa de concientización, prestando atención específica a la tecnología de información, propiciando un ambiente de control positivo y considerando aspectos como:

- Integridad
- valores éticos
- código de conducta
- seguridad y control interno
- competencia del personal
- filosofía y estilo operativo de la administración
- responsabilidad, atención y dirección proporcionadas por el consejo directivo o su equivalente

Existen políticas y procedimientos organizacionales para asegurar que los recursos adecuados y apropiados son asignados para implementar las políticas de la organización de manera oportuna.

Existen procedimientos apropiados para asegurar que el personal comprende las políticas y procedimientos implementados, y que se cumple con dichas políticas y procedimientos.

Las políticas y procedimientos de la función de servicios de información definen, documentan y mantienen una filosofía de políticas y objetivos formales que rigen la calidad de los sistemas y servicios producidos, y que éstos son consistentes con la filosofía, políticas y objetivos de la organización.

La Gerencia ha aceptado la responsabilidad total sobre el desarrollo de un marco referencial para el enfoque general de seguridad y control interno.

Existen políticas sobre asuntos específicos para documentar las decisiones administrativas sobre actividades particulares, aplicaciones, sistemas o tecnologías.

Probando que:

Los esfuerzos de la administración para fomentar un control positivo cubren los aspectos clave tales como: integridad, valores éticos, código de conducta, seguridad y control interno, competencia del personal, filosofía y estilo operativo de la administración, y responsabilidad, atención y dirección proporcionados.

Existe el compromiso de la administración en cuanto a los recursos para formular, desarrollar, documentar, promulgar y controlar políticas que cubren el ambiente de control interno.

La propiedad y habilidad para adaptarse a condiciones cambiantes de las revisiones regulares de estándares, directivas, políticas y procedimientos por parte de la administración.

La administración de la función de servicios de información y el personal de desarrollo y operaciones determinan la filosofía de calidad y su política relacionada, y que los procedimientos y objetivos son comprendidos y cumplidos por todos los niveles dentro de la función de servicios de información.

Los procesos de medición de la calidad aseguran que los objetivos de la organización sean alcanzados.

La documentación del sistema seleccionado confirma que las decisiones administrativas del sistema específico han sido documenta-das y aprobadas de acuerdo con las políticas y procedimientos organizacionales.

La documentación del sistema seleccionado confirma que las decisiones administrativas con respecto a actividades, sistemas de aplicación o tecnologías particulares han sido aprobadas por la Gerencia.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO6.3 Administración de Políticas para TI	Entrevista al gerente de servicios generales.	No existen documentos donde se establezcan las políticas para TI.	Las políticas del área de TI, se las maneja directamente por disposiciones de entes superiores. No se elaboran políticas que apoyen la estrategia del área de TI.
PO6.5 Comunicación de los Objetivos y la Dirección de TI	Entrevista al director de TI.	Orgánico Funcional de área de TI.	Los objetivos se los transmite de manera directa o a través de comunicados escritos a las diferentes dependencias del hospital, pero estos no siempre son comunicados a los interesados apropiados.

Tabla 2.15: Tabla resumen PO6

Dominio: Planeación y Organización				
Proceso: PO6 COMUNICACIÓN DE LOS OBJETIVOS Y DE LAS ASPIRACIONES DE LA GERENCIA				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	La gerencia no ha establecido un ambiente positivo de control de información. No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.	√		**Grado de Madurez.** El proceso de comunicación de los objetivos y aspiraciones de la gerencia se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se ha establecido un mecanismo de comunicación de políticas y objetivos de la gerencia; y no se tiene un control sobre los mismos.
Nivel 1	La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.		√	
Nivel 2	La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales. La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción de gerentes y áreas de negocio individuales. La calidad se reconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales. El entrenamiento se realiza de forma individual, según se requiera.			
Nivel 3	La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son			

	razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.			
Nivel 4	La gerencia asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad y asigna suficientes recursos para mantener el ambiente en línea con los cambios significativos. Se ha establecido un ambiente de control de información positivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen y comunican, y forman un componente de buenas prácticas internas. Se ha establecido un marco de trabajo para la implantación y las verificaciones subsiguientes de cumplimiento.			
Nivel 5	El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora. Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación. El monitoreo, la auto-evaluación y las verificaciones de cumplimiento están extendidas en la organización. La tecnología se usa para mantener bases de conocimiento de políticas y de concienciación y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado en computadora.			

Tabla 2.16: Modelo de madurez PO6

COBIT plantea para el PO6 la necesidad de cumplir con los siguientes objetivos de control.

1. Ambiente Positivo de Control de la Información
2. Responsabilidad de la Gerencia en cuanto a Políticas
3. Comunicación de las Políticas de la Organización
4. Recursos para la Implementación de Políticas
5. Mantenimiento de Políticas
6. Cumplimiento de Políticas, Procedimientos y Estándares
7. Compromiso con la Calidad
8. Política sobre el Marco Referencial para la Seguridad y el Control Interno
9. Derechos de la Propiedad Intelectual
10. Políticas para Situaciones Específicas

El PO6 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Definir claramente la misión y visón del área de TI, darla a conocer a todos los empleados. • Dar a conocer las metas, objetivos, y aspiraciones del hospital, para que los empleados sean más participativos y proactivos en el cumplimiento de las mismas. • Diseñar un plan de trabajo en donde los empleados tengan roles específicos en el cumplimiento de las metas propuestas por la dirección.
Estrategias a largo plazo	• Crear políticas, procedimientos y estándares sobre los objetivos del hospital, los cuales deben ser difundidos en todas las áreas, y deben estar alineados con los planes estratégicos. • Definir códigos de moral y ética que se apliquen en el hospital para que no exista conflictos entre empleados. • Crear una comisión que se encargue del control del cumplimiento de políticas, procedimientos y estándares. • Crear un documento donde consten las políticas sobre los derechos de propiedad intelectual de los sistemas creados en el hospital. • Crear políticas para documentar decisiones administrativas sobre actividades particulares, aplicaciones, sistemas o tecnologías.

Tabla 2.17 Estrategias a corto y largo plazo PO6

2.3.1.6. PO9 Análisis de riesgos

Guías de auditoria

Considerando si:

Existe un marco referencial para la evaluación sistemática de riesgos, incorporando los riesgos de información relevantes para el logro de los objetivos de la organización y formando una base para determinar la forma en la que los riesgos deben ser manejados a un nivel aceptable.

Los objetivos de toda la organización están incluidos en el proceso de identificación de riesgos.

Los procedimientos para el monitoreo de cambios en la actividad de procesamiento de sistemas determinan que los riesgos y exposición de los sistemas son ajustados oportunamente.

El personal asignado a evaluación de riesgos está adecuadamente calificado

Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones.

Se utilizan cálculos y otros métodos en la medición de riesgos, amenazas y exposiciones

Existen propuestas cualitativas y/o cuantitativas formales para seleccionar las medidas de control que maximicen el retorno de la inversión

Existe un balance entre las medidas de detección, prevención, corrección y recuperación utilizadas

Probando que:

Se cumple con el marco referencial de evaluación de riesgos en cuanto a que las evaluaciones de riesgos con actualiza-das regularmente para reducir el riesgo a un nivel aceptable.

La documentación de evaluación de riesgos cumple con el marco referencial de evaluación de riesgos y su documentación es preparada y mantenida apropiadamente.

Los escenarios de riesgo versus los controles están documentados, actualizados y comunicados al personal apropiado.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO9.3 Identificación de Eventos	Entrevista a un empleado del área de TI. Entrevista a una secretaria del hospital.	No existen documentos en donde se identifiquen los riesgos del área de TI.	Los riesgos de área de TI son identificados de manera reactiva, primero suceden para saber que se debe realizar como acción correctiva.
PO9.4 Evaluación de Riesgos de TI	Entrevista al director de TI.	No existen documentos en donde se evalúen los riesgos del área de TI.	No se evalúan los riesgos, solo se intenta mitigarlos. No se evalúa el impacto de los riegos.
PO9.5 Respuesta a los Riesgos	Entrevista a un empleado del área de TI. Entrevista a una secretaria	No existen documentos en donde se propongan las respuestas a los riesgos del área de TI.	Las respuestas a los riesgos son reactivas y de ser posible inmediatas, pero no están programadas por lo que

	del hospital.		pueden resultar ineficientes e inadecuadas.

Tabla 2.18 Tabla de resumen PO9

Dominio: Planeación y Organización				
Proceso: PO9 EVALUACIÓN / ANALISIS DE RIESGOS				
	Niveles de los Modelos de Madurez	**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.	√		**Grado de Madurez.** El proceso de evaluación / análisis de riesgos se encuentra en un nivel 0. **Objetivos no Cumplidos** El área de TI del Hospital General "Enrique Garcés" no toma en cuenta los riesgos, ni los evalúa o genera planes de respuesta a los mismos.
Nivel 1	Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan rara vez a gerentes específicos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.		√	
Nivel 2	Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.			

Nivel 3	Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos consideran las responsabilidades de administración de riesgos.		
Nivel 4	La evaluación y administración de riesgos son procedimientos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con TI. La gerencia puede monitorear la posición de riesgo y tomar decisiones informadas respecto a la exposición que está dispuesta a aceptar. Todos los riesgos identificados tienen un dueño nombrado, y la alta dirección, así como la gerencia de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar. La gerencia de TI ha elaborado medidas estándar para evaluar el riesgo y para definir las proporciones riesgo/retorno. La gerencia presupuesta un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular. Se establece una base de datos de administración de riesgos, y parte del proceso de administración de riesgos se empieza a automatizar. La gerencia de TI considera las estrategias de mitigación de riesgo.		

Nivel 5	La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detecta y actúa cuando se toman decisiones grandes de inversión o de operación de TI, sin considerar el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.			

Tabla 2.19 Modelo madurez PO9

COBIT plantea para el PO9 la necesidad de cumplir con los siguientes objetivos de control.

1. Evaluación del Riesgo del Negocio
2. Enfoque de Evaluación de Riesgos
3. Identificación de Riesgos
4. Medición de Riesgos
5. Plan de Acción contra Riesgos
6. Aceptación de Riesgos
7. Selección de seguridades o salvaguardas
8. Compromiso con el análisis o evaluación de riesgos

El PO9 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Identificar los riegos generales y los específicos de cada proyecto existentes dentro de área de TI. • Realizar una evaluación de todos los riesgos que estén presentes, asignando el control de cada uno de ellos a los responsables del servicio. • Realizar una evaluación de los impactos de riesgos y como afectarían al normal funcionamiento de hospital. • Crear planes de contingencia para sanear estos riegos, y evitar que la continuidad del negocio se vea afectada.
Estrategias a largo plazo	• Crear planes de acción a largo plazo para sanear los riegos con la menor afección en cuanto a costo y tiempo posible. • Crear un comité que se encargue de dar seguimiento y controlar los riesgos que puedan aparecer dentro del área de TI. • Crear balance entre las medidas de detección, prevención, corrección y recuperación utilizadas • Supervisar las acciones realizadas por los empleados para disminuir la cantidad de incidentes generados.

Tabla 2.20: Estrategias a corto y largo plazo PO9

2.3.1.7. Resumen del Dominio Planeación y Organización

Dentro de la evaluación del Hospital General “Enrique Garcés” y específicamente dentro del dominio de planeación y organización que nos plantea COBIT, nos encontramos con un panorama poco favorable para la unidad de TI. Es así que cada uno de los procesos evaluados dentro de este dominio oscilan entre el nivel 0 de madurez que es el grado más bajo, hasta un nivel 2, que es un nivel medio bajo.

Se nota en los procesos tales como definir un plan estratégico de TI o Definir la arquitectura de la información, que la falta de comunicación entre la unidad de TI y el director del Hospital General “Enrique Garcés“, lo que afecta directamente el funcionamiento de la unidad ya que no se tienen políticas claras de funcionamiento, además que al no contar con un plan estratégico acorde al negocio y que se alinea con el funcionamiento del departamento informático, no se puede tener una adecuada organización y planeación dentro de la unidad de TI.

Por otra parte la ubicación del departamento de TI, como un sub departamento del departamento de mantenimiento hace que no pueda formar parte de las decisiones importantes dentro del hospital, y favorezca a la falta de planes a largo plazo para la unidad de TI. Se le ha quitado importancia a esta área, lo que se nota directamente con la seguridad que tiene el área de TI, por lo que se deben plantear mayores y mejores medidas de seguridad ya que se maneja información sensible.

No existe un plan estratégico acorde con la importancia del área, lo que se demuestra con la insuficiente capacitación que se brinda a sus empleados, y la falta de personal del área de TI, esto se ve reflejado en las encuestas que se realizaron a diferentes empleados del hospital. Además el manejo que se le da a los problemas es empírico y no se cuenta con una base de conocimientos que permita resolver estos problemas de una manera más adecuada y proactiva.

Para este dominio dentro del área de TI se deben realizar varias reformas, las que permitan tener un mejor desempeño y ayuden a mejor la calidad de

servicio a través de ciertos aspectos que se deben mejorar, empezando por la ubicación correcta del área de TI dentro de la empresa además de tener un plan estratégico que esté acorde a las necesidades y obligaciones del área.

Cabe recalcar que este domino es la base fundamental para que la unidad de TI pueda desarrollarse a futuro y pueda tener mantener una mejor relación con el área administrativa y se logre ofrecer un servicio de calidad.

2.3.2. PROCESOS DEL DOMINIO DE ADQUIRIR E IMPLEMENTAR

2.3.2.1. AI2 Adquisición y mantenimiento de software de aplicación

Guías de auditoria

Considerando si:

Las políticas y procedimientos aseguran:

- La metodología del ciclo de vida de desarrollo de sistemas de la organización aplica tanto para el desarrollo de nuevos sistemas como para modificaciones mayores a sistemas existentes y participación del usuario
- El vínculo con el usuario al crear las especificaciones de diseño y al verificar éstas contra los requerimientos del usuario
- Se preparan especificaciones detalladas de programas para cada proyecto de desarrollo o modificación de información, y que estas especificaciones concuerdan con las especificaciones del diseño del sistema
- Se especifican los mecanismos adecuados para la recolección y captura de datos para cada proyecto nuevo o modificado de desarrollo de sistemas
- existen mecanismos adecuados para la definición y documentación de las interfaces internas y externas para cada proyecto de desarrollo o modificación de sistemas
- Existen mecanismos adecuados para la definición y documentación de los requerimientos de procesamiento para cada nuevo proyecto de desarrollo o modificación de sistemas
- Existen mecanismos adecuados para la definición y documentación de los requerimientos de salida para cada nuevo proyecto de desarrollo o modificación de sistemas
- Los programas de aplicación contienen definiciones que verifican rutinariamente las tareas llevadas a cabo por el software para ayudar a asegurar la integridad en la recuperación de la información a través de roll-back u otros procesos similares

La metodología de ciclo de vida de desarrollo de sistemas requiere la evaluación de los aspectos básicos de seguridad y con-trol interno de un sistema nuevo a ser desarrollado o modificado, junto con el diseño conceptual del sistema, con el fin de integrar los conceptos de seguridad en el diseño lo más pronto posible

La metodología del ciclo de vida de desarrollo de sistemas requiere que los aspectos de seguridad lógica y de las aplicaciones sean considerados e

incluidos en el diseño de nuevos sistemas o modificaciones de sistemas existentes

La evaluación de los aspectos de control internos y de seguridad está basada en un buen marco referencial

Probando que:

La participación del usuario en el proceso de ciclo de vida de desarrollo de sistemas es significativa

Los usuarios clave de los sistemas están involucrados en el proceso del diseño del sistema

Existen los procedimientos de aprobación del diseño para asegurar que la programación del sistema no se inicie hasta que se hayan obtenido las aprobaciones correspondientes

Se documenten las interfaces internas y externas

Los requerimientos de procesamiento forman parte de las especificaciones del diseño

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
AI2.4 Seguridad y Disponibilidad de las Aplicaciones	Entrevista al director de TI.	No existen documentos acerca de la seguridad de las aplicaciones.	No se tiene un seguimiento sobre la seguridad de las aplicaciones y los requerimientos de seguridad.
AI2.5 Configuración e Implantación de Software Aplicativo Adquirido	Entrevista al director de TI.	No se tiene documentos de respaldo de adquisición de software.	No se configura el software adquirido en relación con los objetivos del negocio.
AI2.7 Desarrollo de Software Aplicativo	Entrevista al director de TI.	No se tienen documentos de desarrollo de software aplicativo. No existen manuales del software desarrollado.	Se utilizan metodologías agiles de desarrollo para las aplicaciones pero no se garantiza que el software es desarrollado de acuerdo con todas las especificaciones de estas metodologías.

AI2.10 Mantenimiento de Software Aplicativo	Entrevista al director de TI.	No se tienen documentos sobre planes preventivos de manteniendo de software.	No se realizan mantenimientos preventivos del software, las respuestas a incidentes son reactivas.

Tabla 2.21: Tabla Resumen AI2

Dominio: Adquisición e Implementación				
Proceso: AI2 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN				
	Niveles de los Modelos de Madurez	**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.	√		**Grado de Madurez.** El proceso de adquisición y mantenimiento de software aplicativo se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se ha establecido un plan de adquisición y mantenimiento de software aplicativo, a pesar de que se reconozca la importancia del mismo.
Nivel 1	Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición y mantenimientos de software aplicativo varían de un proyecto a otro. Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.		√	
Nivel 2	Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro de la operación de TI. El mantenimiento es a menudo problemático y se resiente cuando se pierde el conocimiento interno de la organización. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo		√	

Nivel 3	Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia de TI y del negocio. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que se salten pasos. Las actividades de mantenimiento se planean, programan y coordinan			
Nivel 4	Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación. Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones. Han evolucionado prácticas y procedimientos para ajustarlos a la medida de la organización, los utilizan todo el personal y son apropiados para la mayoría de los requerimientos de aplicación.			
Nivel 5	Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base en componentes, con aplicaciones predefinidas y estandarizadas que corresponden a las necesidades del negocio. El enfoque se extiende para toda la empresa. La metodología de adquisición y mantenimiento presenta un buen avance y permite un posicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantes del negocio. La metodología de adquisición e implantación de software aplicativo ha sido sujeta a mejora continua y se soporta con bases de datos internas y externas que contienen materiales de referencia y las mejores prácticas. La metodología produce documentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento.			

Tabla 2.22: Modelo Madurez AI2

COBIT plantea para el AI2 la necesidad de cumplir con los siguientes objetivos de control.

1. Métodos de Diseño
2. Cambios Significativos a Sistemas Actuales
3. Aprobación del Diseño
4. Definición y Documentación de Requerimientos de Archivos
5. Especificaciones de Programas
6. Diseño para la Recopilación de Datos Fuente
7. Definición y Documentación de Requerimientos de Entrada de Datos
8. Definición de Interfaces
9. Interface Usuario - Máquina
10. Definición y Documentación de Requerimientos de Procesamiento
11. Definición y Documentación de Requerimientos de Salida de Datos
12. Controles
13. Disponibilidad como Factor Clave de Diseño
14. Definiciones de TI sobre Integridad para el Software de Programas de Aplicación
15. Pruebas de Software de Aplicación
16. Materiales de Consulta y Soporte para Usuario
17. Reevaluación del Diseño del Sistema

El AI2 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Realizar un documento con los requerimientos y las especificaciones del software necesario para que el negocio pueda funcionar de forma normal. • Realizar pruebas con el software aplicativo para verificar si es el correcto y cubre las necesidades del hospital. • Realizar manuales de usuario que permitan aprovechar todas las potencialidades del software adquirido, y que este pueda ser utilizado de la mejor manera.
Estrategias a largo plazo	• Realizar pruebas funcionales continuas al software aplicativo del hospital. • Hacer cumplir las políticas de seguridad de la empresa en el software instalado. • Supervisar las acciones que son realizadas por los empleados en el software instalado. • Realizar una evaluación del sistema actual para conocer sus fortalezas y debilidades

Tabla 2.213 Estrategias a corto y largo plazo AI2

2.3.2.2. AI3 Adquisición y mantenimiento de la infraestructura tecnológica

Guías de auditoria

Considerando si:

Existen políticas y procedimientos que aseguran que:

- Se prepara un plan de evaluación formal para evaluar el nuevo hardware y software en cuanto a cualquier impacto sobre el desempeño global del sistema
- La posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de in-formación operativa está limitada
- La preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema
- Se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema

Existen políticas y procedimientos para el mantenimiento preventivo de hardware (tanto el operado por la función de servicios de información como por las funciones de los usuarios afectados) para reducir la frecuencia y el impacto de las fallas de desempeño

Se cumple con los pasos y la frecuencia de mantenimiento preventivo prescritos por el proveedor para cada dispositivo de hardware operado por la función de servicios de información y los usuarios afectados se adhieren a ellos.

Existen políticas y técnicas para monitorear el uso de los utilitarios del sistema

Probando que:

Existen las declaraciones de aseguramiento de la integridad del software del sistema entregados por los proveedores para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema.

La evaluación del desempeño trae como resultado la comparación con los requerimientos del sistema.

Existe un proceso formal aprobado de evaluación del desempeño.

El calendario de mantenimiento preventivo asegura que el mantenimiento de hardware programado no tendrá ningún impacto negativo sobre aplicaciones críticas o sensitivas.

El mantenimiento programado asegura que no ha sido planeado para períodos pico de carga de trabajo y que la función de servicios de información y las operaciones de los grupos de usuarios afectados son suficientemente flexibles para adaptar el mantenimiento preventivo rutinario planeado.

El software del sistema es instalado y mantenido de acuerdo con el marco referencial de adquisición y mantenimiento para la infraestructura de tecnología.

Todos los passwords o contraseñas de instalación del software del sistema proporcionados por los proveedores fue-ron cambiados al momento de la instalación

Todos los cambios al software del sistema fueron controlados de acuerdo con los procedimientos de administración.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
AI3.1 Plan de Adquisición de Infraestructura Tecnológica	Entrevista al líder de TI.	No existen documentos de respaldo del plan de adquisición de infraestructura tecnológica.	La adquisición de infraestructura del hospital se la realiza por pedidos para satisfacer necesidades.
AI3.3 Mantenimiento de la Infraestructura	Entrevista al líder de TI.	No existen ni documentos de mantenimiento para la infraestructura tecnológica.	No se tienen planes preventivos de mantenimiento. Los mantenimientos son reactivos en toda la infraestructura tecnológica y se los realiza al presentarse un inconveniente.

Tabla 2.24: Tabla Resumen AI3

Dominio: Adquisición e Implementación				
Proceso: AI3 ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.	√		**Grado de Madurez.** El proceso de adquisición y mantenimiento de la infraestructura tecnológica se encuentra en un nivel 0. **Objetivos no Cumplidos** El Hospital General "Enrique Garcés" no reconoce la administración de la infraestructura tecnológica, no existen planes de adquisición y mantenimiento de la infraestructura.
Nivel 1	Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.		√	
Nivel 2	No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.			
Nivel 3	Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa			

	y coordina el mantenimiento. Existen ambientes separados para prueba y producción.			
Nivel 4	Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.			
Nivel 5	El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología. Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración. Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización. Con un alto nivel de conciencia se pueden identificar los medios óptimos para mejorar el desempeño en forma preventiva, incluyendo el considerar la opción de contratar servicios externos. La infraestructura de TI se entiende como el apoyo clave para impulsar el uso de TI.			

Tabla 2.25: Modelo Madurez AI3

COBIT plantea para el AI3 la necesidad de cumplir con los siguientes objetivos de control.

1. Evaluación de Nuevo Hardware y Software
2. Mantenimiento Preventivo para Hardware
3. Seguridad del Software del Sistema
4. Instalación del Software del Sistema
5. Mantenimiento del Software del Sistema
6. Controles de Cambios para el Software del Sistema
7. Uso y Monitoreo de los Utilitarios del Sistema

El AI3 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Realizar evaluaciones periódicas en hardware y software, tanto en equipos nuevos como en equipos antiguos. • Crear un plan de mantenimientos preventivos, y tratar de evitar los mantenimientos reactivos para asegurar la continuidad del negocio. • Crear un plan para instalación de software original en todas las maquinas con lo cual se asegurar tener todos los equipos en regla.
Estrategias a largo plazo	• Crear políticas de seguridad en todos los equipos, para evitar perdida o mala utilización de los mismos. • Controlar que el inventario este correcto, y que todos los equipos se encuentren en buen estado. • Crear una aplicación que lleve el inventario de los pasivos que tenga el hospital, y que esto sea verificado constantemente.

Tabla 2.16: Estrategias a corto y largo plazo AI3

2.3.2.3. AI4 Desarrollo y mantenimiento de procedimientos

Guías de auditoria

Considerando si:

Los requerimientos operativos fueron determinados con estadísticas históricas de desempeño, disponibles, e información proporcionada por el usuario con respecto a incrementos/decrementos esperados

El nivel de servicio y las expectativas de desempeño están suficientemente detallados para permitir el seguimiento, la emisión de reportes y las oportunidades de mejora

Los requerimientos operativos y los niveles de servicio están determinados utilizando tanto desempeño histórico y ajustes de usuario como mediciones o "benchmarks" de la industria

Los niveles de servicio y requerimientos de procesamiento son un paso integral en la planeación de nuevos sistemas

Probando que:

Existen manuales de entrenamiento para todos los sistemas existentes y nuevos y son satisfactorios para los usuarios, reflejando el uso del sistema en la práctica diaria

Los manuales de usuario incluyen, pero no se limitan a:

- Resumen de los sistemas y del ambiente
- Explicación de todas la entradas, programas, salidas e integración de todos los sistemas con otros sistemas
- Explicación de todas las pantallas de entrada y despliegue de datos
- Explicación de todos y cada uno de los mensaje de error y la respuesta apropiada

Se llevan a cabo el mantenimiento continuo de la documentación de aplicación, manuales de operación y de usuario y el entrenamiento respectivo, si aplica

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
AI4.1 Plan para Soluciones de Operación	Entrevista con un médico del hospital.	No existen documentos que respalden el plan para soluciones de operación.	No se tienen planes ni documentos, donde consten las soluciones de operación.
AI4.2 Transferencia de Conocimiento a la Gerencia del Negocio	Entrevista a un empleado del área de TI.	No existen documentos para la transferencia de conocimiento a la gerencia del negocio.	No se realiza una correcta transferencia de conocimiento entre el área de TI y la gerencia del hospital.
AI4.4 Transferencia de Conocimiento al Personal de Operaciones y Soporte	Entrevista a un empleado del área de TI.	No existen documentos para la transferencia de conocimiento al personal de operaciones y soporte.	No se realiza una correcta transferencia de conocimiento al personal de operaciones y soporte.

Tabla 2.26: Tabla resumen AI4

Dominio: Adquisición e Implementación				
Proceso: AI4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS				
	Niveles de los Modelos de Madurez	**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento. Los únicos materiales existentes son aquellos que se suministran con los productos que se adquieren.	√		**Grado de Madurez.** El proceso de desarrollo y mantenimiento de procedimientos se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se producen manuales de usuario ni de operación en el área de TI.
Nivel 1	Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.		√	
Nivel 2	Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.			

Nivel 3	Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.		
Nivel 4	Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas y las unidades de negocio, de manera que se pueden observar los procesos desde una perspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfaces. Existen controles para garantizar que se adhieren los estándares y que se desarrollan y mantienen procedimientos para todos los procesos. La retroalimentación del negocio y del usuario sobre la documentación y el entrenamiento se recopila y evalúa como parte de un proceso continuo de mejora. Los materiales de documentación y entrenamiento se encuentran generalmente a un buen nivel, predecible, de confiabilidad y disponibilidad. Se implanta un proceso emergente para el uso de documentación y administración automatizada de procedimiento. El desarrollo automatizado de procedimientos se integra cada vez más con el desarrollo de sistemas		

	aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega de documentación, materiales y programas de entrenamiento.			
Nivel 5	El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante que se mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, flujo de trabajo y tecnologías de distribución, que los hacen accesibles y fáciles de mantener. El material de documentación y entrenamiento se actualiza para reflejar los cambios en la organización, en la operación y en el software. Tanto el desarrollo de materiales de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones de proceso del negocio, siendo así un apoyo a los requerimientos de toda la organización y no tan sólo procedimientos orientados a TI.			

Tabla 2.27: Modelo Madurez AI4

COBIT plantea para el AI4 la necesidad de cumplir con los siguientes objetivos de control-

1. Requerimientos Operacionales y Niveles de Servicios
2. Manual de Procedimientos para el Usuario
3. Manual de Operaciones
4. Materiales de Entrenamiento

El AI4 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deben manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Se recomienda la creación de acuerdos de nivel de servicio, para establecer políticas de funcionamiento del área de TI. • Crear manuales de usuario para las aplicaciones utilizadas por el personal, y difundirlos a todos los empleados del hospital. • Establecer políticas de capacitación del área de TI para los usuarios con relación a aspectos ofimáticos y de sistemas utilizados.
Estrategias a largo plazo	• Crear políticas de documentación del área de TI para todos los sistemas que la misma maneje. • Crear un repositorio documental para que cualquier usuario tenga acceso a información que necesite o requiera sobre el uso de un software o un sistema.

Tabla 2.28: Estrategias a corto y largo plazo AI4

2.3.2.4. AI5 Instalación y acreditación de sistemas

Guías de auditoria

Considerando si:

Existen políticas y procedimientos relacionados con el proceso de ciclo de vida de desarrollo de sistemas.

Existe una metodología formal de ciclo de vida de desarrollo de sistemas; para la instalación y acreditación de sistemas, incluyendo, pero no limitándose a, un enfoque en fases sobre: entrenamiento, adecuación del desempeño, plan de conversión, pruebas de programas, grupos de programas (unidades) y del sistema total, un plan de pruebas prototipo o paralelo, pruebas de aceptación, pruebas y acreditación de seguridad, pruebas operativas, controles de cambio, revisión y modificación de implementación y post-implementación.

Se lleva a cabo el entrenamiento de usuarios como parte de cada tentativa de desarrollo.

El proceso de aseguramiento de la calidad incluye la migración independiente de desarrollo a las librerías de producción y la suficiencia de la aceptación requerida de los usuarios y grupos de operación

Probando que:

Se ha incluido en todas las tentativas de desarrollo de nuevos sistemas un plan formal para el entrenamiento de usuarios

El personal está consciente, comprende y tiene conocimiento de la necesidad de controles formales de desarrollo de sistemas y entrenamiento de usuarios para cada instalación e implementación de desarrollo

La conciencia, comprensión y conocimiento de usuarios seleccionados con respecto a sus responsabilidades en el diseño, aprobación, pruebas, entrenamiento, conversión y proceso de implementación es conocida y considerada

Se da seguimiento a los costos reales del sistema comparados con los costos estimados, y al desempeño real contra el esperado de los sistemas nuevos o modificados

Existe un plan de pruebas que cubre todas las áreas de recursos de sistemas de información: software de aplicación, instalaciones, tecnología y usuarios.

Los usuarios comprenden todas las fases y responsabilidades en el desarrollo de sistemas, incluyendo:

- Especificaciones de diseño, incluyendo iteraciones durante el ciclo de desarrollo.
- Análisis costo/beneficio y estudio de factibilidad.
- Aprobación en cada paso del proceso de desarrollo del sistema.
- Aprobación y aceptación del sistema a través del ciclo de desarrollo.
- Aprobación final y aceptación del sistema.
- Evaluación de la suficiencia del entrenamiento recibido para sistemas recientemente entregados y liberados.

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
AI5.1 Entrenamiento	Entrevista a un empleado del área de TI.	No existen documentos de respaldo de entrenamiento.	El entrenamiento que se les ha dado a los usuarios de los sistemas informáticos del hospital ha sido escaso y en muchos casos no ha existido.
AI5.3 Plan de Implementación	Entrevista al director de TI. Entrevista a un empleado del área de TI.	No existen documentos de respaldo sobre planes de implementación.	Los planes para la implementación de software desarrollado no se encuentran documentados ni se lleva un control de fechas y objetivos.
AI5.6 Planes y estrategias de pruebas	Entrevista al director de TI. Entrevista a un empleado del área de TI.	No existen documentos de respaldo de planes y estrategias de pruebas.	Las pruebas realizadas al software desarrollado en el hospital no son realizadas en base a planes y estrategias

			definidas
AI5.7 Pruebas de Cambios	Entrevista al director de TI.	No existen documentos de respaldo de pruebas de cambios.	Las pruebas realizadas al realizar un cambio en un sistema o software en el hospital no se rigen a planes y estrategias definidas.

Tabla 2.29: Tabla Resumen AI5

Dominio: Adquisición e Implementación				
Proceso: AI5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	Hay una ausencia completa de procesos formales de instalación o acreditación y ni la gerencia ni el personal de TI reconocen la necesidad de verificar que las soluciones se ajustan para el propósito deseado.	√		**Grado de Madurez.** El proceso de instalación y acreditación de sistemas se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no existen criterios para estandarizar el software, ni existen procesos de instalación del mismo. Al igual que no se tiene procesos para migración de sistemas.
Nivel 1	Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares y los enfoques que se toman varían. La acreditación formal y la autorización son raras o no existentes.		√	
Nivel 2	Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología. Los equipos individuales de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.		√	
Nivel 3	Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto. El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales. La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación.		√	

Nivel 4	Los procedimientos son formales y se desarrollan para ser organizados y prácticos con ambientes de prueba definidos y con procedimientos de acreditación. En la práctica, todos los cambios mayores de sistemas siguen este enfoque formal. La evaluación de la satisfacción a los requerimientos del usuario es estándar y medible, y produce mediciones que la gerencia puede revisar y analizar de forma efectiva. La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, aún con niveles razonables de problemas posteriores a la implantación. La automatización del proceso es ad hoc y depende del proyecto. Es posible que la gerencia esté satisfecha con el nivel actual de eficiencia a pesar de la ausencia de una evaluación posterior a la implantación. El sistema de prueba refleja adecuadamente el ambiente de producción. La prueba de stress para los nuevos sistemas y la prueba de regresión para sistemas existentes se aplican para proyectos mayores.		**√**	
Nivel 5	Los procesos de instalación y acreditación se han refinado a un nivel de buena práctica, con base en los resultados de mejora continua y refinamiento. Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente de entrenamiento, pruebas y transición a producción para los nuevos sistemas. Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción. La acreditación toma lugar regularmente sin repetición de trabajos, y los problemas posteriores a la implantación se limitan normalmente a correcciones menores. Las revisiones posteriores a la implantación son estándar, y las lecciones aprendidas se canalizan nuevamente hacia el proceso para asegurar el mejoramiento continuo de la calidad. Las pruebas de stress para los nuevos sistemas y las pruebas de regresión para sistemas modificados se aplican en forma consistente.		**√**	

Tabla 2.30: Modelo de Madurez AI5

COBIT plantea para el AI5 la necesidad de cumplir con los siguientes objetivos de control.

1. Entrenamiento
2. Adecuación del Desempeño del Software de Aplicación
3. Plan de Implementación
4. Conversión del sistema
5. Conversión de datos
6. Planes y estrategias de pruebas
7. Pruebas a los Cambios
8. Desempeño y criterios de pruebas en paralelo/piloto
9. Prueba de Aceptación Final
10. Pruebas y Acreditación de la Seguridad
11. Prueba Operacional
12. Promoción a Producción
13. Evaluación del cumplimiento de los Requerimientos del Usuario
14. Revisión Gerencial Post – Implementación

El AI5 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Crear criterios para estandarizar la instalación de software y para la migración de datos. • Establecer una base de software instalado en cada máquina. • Crear un plan para instalación de software original en todas las maquinas.
Estrategias a largo plazo	• Realizar cursos de capacitación a usuarios y personal de TI con relación al software del hospital. • Realización de pruebas en el software instalado para saber si el mismo cubre las necesidades del hospital. • Obtener infraestructura para realizar pruebas y mediciones sobre el desempeño. • Crear planes de implementación e instalación de software nuevo, para evitar cualquier contratiempo.

Tabla 2.31: Estrategias a corto y largo plazo AI5

2.3.2.5. Resumen del Dominio Adquirir e Implementar

En la evaluación general del dominio de adquirir e implementar del Hospital General “Enrique Garcés”, que nos plantea COBIT, nos encontramos con una evaluación que se refleja en los resultados de las evaluaciones de los procesos de este dominio que oscilan entre los niveles 0 y 1 de los respectivos niveles de madures de COBIT. Lo cual nos hace pensar en que se deben realizar correcciones para mejorar la unidad de TI.

Para este dominio se puede notar que los procesos evaluados, si bien es cierto que tienen grandes falencias, también tiene un mayor control puesto que no solo dependen de la unidad de TI, sino también del departamento de mantenimiento, que incluye la bodega, despacho e inventario de los equipos. Con lo cual se tiene un control más exhaustivo para con el hardware del hospital, sin dejar de lado el software.

Dentro de lo que encontramos en estos procesos y con la ayuda de las encuestas y levantamiento de información que se realizó en el hospital, se puede decir que los mantenimientos que se realizan son reactivos, mientras que los mantenimientos preventivos son nulos debido a la falta de personal que se tiene dentro de la unidad de TI, esto complica enormemente el trabajo que se realiza, puesto que las 3 personas que se encuentran en la unidad de TI tienen que dar abasto para todas las necesidades del hospital.

Esto también se ve reflejado en el proceso de adquisición de software y hardware, ya que no se tiene un control completo, sino más bien esto se hace dependiendo de las necesidades que aparezcan en el hospital, sin embargo esto nos muestra otro problema cuando ocurren incidentes ya que no se dispone de repuestos para poder solventar este incidente y pasan días hasta que se le pueda dar una solución al problema.

El nivel de madurez de adquisición de hardware y software que maneja el hospital es bajo, que se tiene un número limitado de cotizaciones y productos para solucionar los contratiempos que surgen. Esto es algo que se debería cambiar, ya que si bien es cierto una vez adquirido el producto se tiene un mejor control de a quién pertenece y de que no desaparezca, se debe tener

siempre varias cotizaciones para poder comparar precios, características y utilidades para realizar una mejor compra.

Para este dominio dentro del área de TI se debe realizar varias reformas, las que cuales permitan tener un mejor desempeño y ayuden a mejorar la calidad de servicio a través de aspectos concretos que permitan que la unidad de TI esté preparada en los inconvenientes que surjan, tanto como de hardware como de software, y mantener a los usuarios satisfechos con el trabajo de la unidad.

2.3.3. PROCESOS DEL DOMINIO ENTREGA Y SOPORTE

2.3.3.1. DS1 Definición y administración de niveles de servicio

Guías de auditoria

Considerando si:

Se identifica por política un proceso de acuerdo de nivel de servicio

La participación en el proceso por parte del usuario se requiere para la creación y modificación de acuerdos

Están definidas las responsabilidades de usuarios y proveedores

La administración monitorea y emite reportes sobre el logro de los criterios de desempeño de servicio especificados y sobre todos los problemas encontrados

Los acuerdos de nivel de servicio incluyen, pero no se limitan a contar con:

- Definición de servicio
- Costo del servicio
- Nivel de servicio mínimo cuantificable
- Nivel de soporte por parte de la función de servicios de información
- Disponibilidad, confiabilidad y capacidad de crecimiento
- Plan de continuidad
- Requerimientos de seguridad
- Procedimientos de cambio para cualquier parte del acuerdo
- Acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio
- Revisión/renovación/no renovación del período efectivo y del nuevo período
- Contenido y frecuencia del reporte de desempeño y pago de servicios
- Cargos son realistas comparados contra la historia, la industria y las buenas prácticas
- Cálculo de cargos
- Compromiso de mejoras al servicio

Probando que:

Para una muestra de acuerdos de nivel de servicio pasados y en proceso, el contenido incluye:

- Definición del servicio

- Costo del servicio
- Nivel de servicio mínimo cuantificable
- Nivel de soporte por parte de la función de servicios de información
- Disponibilidad, confiabilidad y capacidad de crecimiento
- Procedimiento de cambios para cualquier parte del acuerdo
- Plan de continuidad en caso de desastre/contingencia
- Requerimientos de seguridad
- Acuerdo por escrito y formalmente aprobado entre el proveedor y el usuario del servicio
- Revisión/renovación/no renovación del período efectivo y nuevo período
- Contenido y la frecuencia del reporte de desempeño y el pago de servicios
- Cargos son realistas comparados con la historia, la industria y las buenas prácticas
- Cálculos de cargos
- Compromiso de mejoras al servicio
- Aprobación formal por parte de usuarios y proveedores

Los usuarios apropiados están conscientes, tienen conocimiento y comprenden los procesos y procedimientos del acuerdo de nivel de servicio

El nivel de satisfacción del usuario en cuanto al proceso y acuerdos reales del nivel de servicio actuales es suficiente

El servicio proporciona registros para asegurar razones para un bajo desempeño y para asegurar que existe un programa para la mejora del desempeño

La precisión de los cargos reales concuerda con el contenido del acuerdo

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS1.1 Marco de Referencia para los acuerdos de Nivel de Servicio	Entrevista al director de TI. Entrevista usuarios claves de los servicios de TI.	No existen documentos de respaldo para el marco de referencia de los acuerdos de nivel de servicio.	No se encuentran definidos acuerdos de nivel de servicio para los servicios brindados por el departamento de TI del hospital.
DS1.2 Aspectos sobre los Acuerdos de Nivel de Servicio	Entrevista a un empleado de soporte técnico.	No existen documentos de respaldo sobre los acuerdos de nivel de servicio.	Los servicios ofrecidos por el departamento de TI no cuentan con: definición de servicio, costo del servicio, nivel de servicio mínimo cuantificable, nivel de soporte por parte de la función de servicios de información, disponibilidad, confiabilidad y capacidad de crecimiento ni plan de

			continuidad.
DS1.3 Procedimientos de desempeño	Entrevista al director de TI. Entrevista con un médico del hospital. Entrevista a un empleado de soporte técnico.	No existen documentos de respaldo de los procedimientos a realizarse con respecto a los servicios.	Los servicios ofrecidos por el departamento de TI no cuentan con los procedimientos a realizarse dependiendo del servicio y el nivel del mismo.

Tabla 2.32: Tabla Resumen DS1

Dominio: Entregar y Soporte				
Proceso: DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	La gerencia no reconoce la necesidad de un proceso para definir los niveles de servicio. La responsabilidad y la rendición de cuentas sobre el monitoreo no está asignada.	√		**Grado de Madurez.** El proceso de definir y administrar los niveles de servicio se encuentra en un nivel 1. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no existen acuerdos de nivel de servicio y tampoco se tiene conciencia de la necesidad de estos.
Nivel 1	Hay conciencia de la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas sobre para la definición y la administración de servicios no está definida. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa. La notificación es informal, infrecuente e inconsistente.	√		
Nivel 2	Los niveles de servicio están acordados pero son informales y no están revisados. Los reportes de los niveles de servicio están incompletos y pueden ser irrelevantes o engañosos para los clientes. Los reportes de los niveles de servicio dependen, en forma individual, de las habilidades y la iniciativa de los administradores. Está designado un coordinador de niveles de servicio con responsabilidades definidas, pero con autoridad limitada. Si existe un proceso para el cumplimiento de los acuerdos de niveles de servicio es voluntario y no está implementado.		√	
Nivel 3	Las responsabilidades están bien definidas pero con autoridad discrecional. El proceso de desarrollo del acuerdo de niveles de servicio está en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción de cliente. Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar. Las deficiencias en los niveles de servicio están identificadas pero los procedimientos para resolver las deficiencias son informales. Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado. Los niveles de		√	

	servicio están acordados pero pueden no responder a las necesidades del negocio.			
Nivel 4	Aumenta la definición de los niveles de servicio en la fase de definición de requerimientos del sistema y se incorporan en el diseño de la aplicación y de los ambientes de operación. La satisfacción del cliente es medida y valorada de forma rutinaria. Las medidas de desempeño reflejan las necesidades del cliente, en lugar de las metas de TI. Las medidas para la valoración de los niveles de servicio se vuelven estandarizadas y reflejan los estándares de la industria. Los criterios para la definición de los niveles de servicio están basados en la criticidad del negocio e incluyen consideraciones de disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad. Cuando no se cumplen los niveles de servicio, se llevan a cabos análisis causa-raíz de manera rutinaria. El proceso de reporte para monitorear los niveles de servicio se vuelve cada vez más automatizado. Los riesgos operativos y financieros asociados con la falta de cumplimiento de los niveles de servicio, están definidos y se entienden claramente. Se implementa y mantiene un sistema formal de medición de los KPIs y los KGIs.		**√**	
Nivel 5	Los niveles de servicio son continuamente reevaluados para asegurar la alineación de TI y los objetivos del negocio, mientras se toma ventaja de la tecnología incluyendo le relación costo-beneficio. Todos los procesos de administración de niveles de servicio están sujetos a mejora continua. Los niveles de satisfacción del cliente son administrados y monitoreados de manera continua. Los niveles de servicio esperados reflejan metas estratégicas de las unidades de negocio y son evaluadas contra las normas de la industria. La administración de TI tiene los recursos y la asignación de responsabilidades necesarias para cumplir con los objetivos de niveles de servicio y la compensación está estructurada para brindar incentivos por cumplir con dichos objetivos. La alta gerencia monitorea los KPIs y los KGIs como parte de un proceso de mejora continua.		**√**	

Tabla 2.33: Modelo de Madurez DS1

COBIT plantea para el DS1 la necesidad de cumplir con los siguientes objetivos de control.

1. Marco de Referencia para los acuerdos de Nivel de Servicio
2. Aspectos sobre los Acuerdos de Nivel de Servicio
3. Procedimientos de desempeño
4. Monitoreo y Reporte
5. Revisión de Convenios y Contratos de Nivel de Servicio
6. Elementos sujetos a Cargo
7. Programa de Mejoramiento del Servicio

El DS1 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Crear un marco referencial para acuerdos de nivel de servicio. • Crear un conjunto de procedimientos de desempeño dentro de la unidad de TI para saber cómo actuar ante un incidente. • Crear un documento con convenios y contratos de nivel de servicios tanto para la unidad de TI, como para servicios contratados.
Estrategias a largo plazo	• Dotar de la infraestructura adecuada y el personal suficiente para que los acuerdos de nivel de servicios se puedan cumplir. • Crear un programa de mejoramiento del servicio de la unidad de TI, en donde se indiquen los medidores de los mismos.

Tabla 2.34: Estrategias a corto y largo plazo DS1

2.3.3.2. DS4 Asegurar el servicio continuo

Guías de auditoria

Considerando si:

Las políticas organizacionales requieren de un marco referencial de continuidad y de un plan como parte de los requerimientos normales de operación tanto para la función de servicios de información como para todas las organizaciones dependientes de los recursos de sistemas de información

Las políticas y procedimientos de la función de servicios de información requieren de:

- una filosofía y un marco referencial consistentes en relación con el desarrollo de un plan de continuidad
- una priorización de las aplicaciones con respecto a los tiempos de recuperación y regreso a la operación normal
- una evaluación de riesgos y la consideración de seguros por pérdidas del negocio en situaciones de continuidad para la función de servicios de información, así como para los usuarios de los recursos
- una determinación de funciones y responsabilidades específicas con respecto a la planeación de continuidad con pruebas, mantenimiento y requerimientos de actualización específicos
- un acuerdo de contrato formal con los proveedores que prestan servicios en el evento de requerirse la recuperación, incluyendo instalaciones o relaciones de respaldo, anticipándose a una necesidad real
- la inclusión de los siguientes puntos como contenido mínimo en cada plan de continuidad:
  - Procedimientos de emergencia para garantizar la seguridad de todos los miembros del personal afectados
  - Funciones y responsabilidades de la función de servicios de información, de los proveedores que prestan servicios de recuperación, de los usuarios de los servicios y del personal administrativo de soporte
  - Un marco referencial de recuperación consistente con un plan de continuidad a largo plazo
  - Una lista de los recursos de sistemas que requieren alternativas (hardware, periféricos, software)
  - Una lista de las aplicaciones priorizadas de mayor a menor, de los tiempos de recuperación requeridos y de las normas de desempeño esperadas

- Funciones administrativas para comunicar y proporcionar servicios de soporte tales como beneficios, nómina, comunicación externa, seguimiento de costos, etc. en el evento de requerirse la recuperación
- Escenarios de desastre varios, desde las pérdidas mínimas hasta la pérdida total de la capacidad y respuesta a cada una en suficiente detalle para llevar a cabo una ejecución paso a paso.
- La identificación de equipo específico y necesidades de suministros tales como impresoras de alta velocidad, firmas, formatos, equipo de comunicación, teléfonos, etc., así como de una fuente y otras fuentes alternativas definidas
- El entrenamiento, concientización y el conocimiento de las funciones individuales y de equipo en el plan continuidad
- La programación de pruebas, los resultados de la última prueba y las acciones correctivas llevadas a cabo tomando como base la(s) prueba(s) anterior(es)
- El detalle de los proveedores de servicios contratados, de los servicios y de la expectativas de respuesta
- La información logística de la localización de recursos claves, incluyendo el centro de cómputo de respaldo para la recuperación de sistemas operativos, aplicaciones, archivos de datos, manuales de operación y documentación de programas/sistema/usuarios
- Los nombres, direcciones, números de teléfono/ "localizadores" (pagers) actuales del personal clave
- La inclusión de los planes de reconstrucción para la recuperación en la ubicación original de todos los sistemas y recursos
- Las alternativas de reanudación del negocio para todos los usuarios estableciendo sitios de trabajo alternativo, una vez que los recursos de sistemas de información estén disponibles (por ejemplo, el sistema ha sido recuperado en el sitio alterno pero el edificio de los usuarios sufrió un incendio y no está disponible)

Probando que:

Existen planes de continuidad, que éste es actual y que es comprendido por todas las partes afectadas

Se ha proporcionado a todas las partes involucradas un plan regular de entrenamiento de continuidad

Se han seguido todas las políticas y procedimientos relacionados con el desarrollo del plan

El contenido del plan tiene como base el contenido descrito anteriormente, y que:

- los objetivos del plan de contingencia han sido alcanzados
- se ha seleccionado a las personas apropiadas para llevar a cabo funciones de liderazgo
- el plan ha recibido las revisiones y aprobaciones apropiadas por parte de la administración
- el plan ha sido probado recientemente y que éste trabajó de acuerdo con lo esperado, o que cualquier deficiencia encontrada trajo como resultado la aplicación de correcciones al plan
- existe un vínculo entre el plan de continuidad y el plan de negocios de la organización
- los procedimientos manuales alternativos son documentados y probados como parte de la prueba global

Se han dado el entrenamiento y la concientización de los usuarios y del personal de la función de servicios de información en cuanto a funciones, tareas y responsabilidades específicas dentro del plan

Las relaciones y tiempos del proveedor contratado son consistentes con las expectativas y necesidades del usuario

El contenido del sitio de respaldo está actualizado y es suficiente con respecto a los procedimientos normales de rotación en el sitio alterno (off-site)

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS4.2 Estrategia y Filosofía del Plan de Continuidad de TI	Entrevista al director de TI.	No existen documentos de respaldo de la estrategia y filosofía de plan de continuidad de TI.	No existen políticas y procedimientos generales para la organización con relación a la planeación de recuperación / seguridad.
DS4.3 Contenido del Plan de Continuidad de TI	Entrevista al director de TI. Entrevista a un empleado del área de TI.	No existen documentos de respaldo del plan de continuidad.	No existen planes de continuidad de los servicios brindados por el departamento de TI. Los procedimientos que se realizan en el caso de un incidente no se basan en políticas establecidas.
DS4.8 Distribución del Plan de Continuidad de TI	Entrevista a un empleado del área de TI. Entrevista al gerente de	No existen documentos de respaldo del plan de continuidad.	No se han realizado pruebas del plan de continuidad por parte de los usuarios relacionados con la continuidad

	servicios generales.		y recuperación del negocio.
DS4.10 Recursos críticos de TI	Entrevista al director de TI. Entrevista al gerente de servicios generales.	No existen documentos de respaldo del plan de continuidad ni los recursos críticos	No se encuentran totalmente identificados los recursos críticos de TI, y no se tienen planes de recuperación / seguridad para estos recursos. No existe una metodología para la priorización de aplicaciones y recursos.
DS4.12 Almacenamiento de respaldos en el sitio alterno	Entrevista al director de TI. Entrevista a un empleado del área de TI.	No existen documentos de respaldo sobre el almacenamiento de respaldos.	No se realizan respaldos en un medio externo a la organización.

Tabla 2.35 Tabla Resumen DS4

Dominio: Entrega y Soporte				
Proceso: DS4 ASEGURAR EL SERVICIO CONTINUO				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.	√		**Grado de Madurez.** El proceso de asegurar el servicio continuo se encuentra en un nivel 1. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se tiene un plan formal para garantizar la continuidad del servicio.
Nivel 1	Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.	√		
Nivel 2	Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.		√	
Nivel 3	La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas			

	de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir entrenamiento para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.			
Nivel 4	Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda entrenamiento formal y obligatorio sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.			
Nivel 5	Los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de			

	disponibilidad y la continua planeación de la continuidad están totalmente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirán como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática. La gerencia ajusta la planeación de continuidad como respuesta a los KGIs y KPIs			

Tabla 2.36 Modelo de Madurez DS4

COBIT plantea para el DS4 la necesidad de cumplir con los siguientes objetivos de control.

1. Marco de Referencia para Continuidad (recuperación en caso de desastres) de TI
2. Estrategia y Filosofía del Plan de Continuidad de TI
3. Contenido del Plan de Continuidad de TI
4. Reducción de los Requerimientos de la Continuidad de TI
5. Mantenimiento del Plan de Continuidad de TI
6. Prueba del Plan de Continuidad de TI
7. Capacitación para el Plan de Continuidad de TI
8. Distribución del Plan de Continuidad de TI
9. Procedimientos de Respaldo del Procesamiento Alterno en el Departamento Usuario
10. Recursos críticos de TI
11. Respaldo del Sitio y del Hardware
12. Almacenamiento de respaldos en el sitio alterno
13. Procedimientos de Involucramiento

El DS4 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Asignar responsabilidades para los elementos críticos del hospital; que permitan garantizar la continuidad del servicio. • Realizar respaldos periódicos de la información crítica, además de contar con los suficientes repuestos de hardware para cualquier incidente. • Crear un plan de continuidad, basado en los lineamientos del negocio y los acuerdos de nivel de servicio.
Estrategias a largo plazo	• Alinear el plan de continuidad de TI con el plan continuidad del negocio, incluir procedimientos alternativos y medidas de emergencia. • Crear políticas que involucren a los usuarios, y difundir dichas políticas para que los usuarios tengan procedimientos para seguir ante un incidente. • Tener un plan de aseguramiento de la continuidad, con relación a eventos naturales y que estén fuera de las manos del control de la unidad de TI.

Tabla 2.38: Estrategias a corto y largo plazo DS4

2.3.3.3. DS5 Garantizar la seguridad de sistemas

Guías de auditoria

Considerando si:

Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte.

Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.

Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.

Se cuenta con perfiles de seguridad de usuario que representen —los menos accesos requeridos y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación.

El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.

Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir:

- intentos no autorizados de acceso al sistema (sign on)
- intentos no autorizados de acceso a los recursos del sistema
- intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad
- privilegios de acceso a recursos por ID de usuario
- modificaciones autorizadas a las definiciones y reglas de seguridad
- accesos autorizados a los recursos (seleccionados por usuario o recurso)
- cambio de estatus de la seguridad del sistema
- accesos a las tablas de parámetros de seguridad del sistema operativo

Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión.

Existen estándares de administración de llaves criptográfica tanto para la actividad centralizada como para la de los usuarios.

Los controles de cambios al software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de sistemas.

Probando que:

TI cumple con los estándares de seguridad relacionados con:

- autenticación y acceso
- administración de perfiles de usuario y clasificación de la seguridad de datos
- reportes y revisión gerencial de las violaciones e incidentes de seguridad
- estándares de administración de llaves criptográficas
- Detección, resolución y comunicación sobre virus
- clasificación y propiedad de datos

Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema

Existen procedimientos para el acceso externo de recursos del sistema, por ejemplo, “logon”, “ID”, ”password” o contraseña y “dial back”.

Se lleva un inventario de los dispositivos de acceso al sistema para verificar su suficiencia.

Los parámetros de seguridad del sistema operativo tienen como base estándares locales/del proveedor.

Las prácticas de administración de seguridad de la red son comunicadas, comprendidas e impuestas.

Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad

Existen procedimientos de “logon” vigentes para sistemas, usuarios y para el acceso de proveedores externos.

Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes

Existen llaves secretas para la transmisión

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS5.1 Manejo de las Medidas de Seguridad	Entrevista al gerente de servicios generales.	No existen documentos de respaldo del manejo de medidas de seguridad.	No existen políticas y procedimientos de TI relacionados con la seguridad y acceso a los sistemas de información. Las medidas tomadas para el control de acceso y seguridad no se encuentran definidas.
DS5.4 Administración de Cuentas de Usuario	Entrevista a un empleado del área de TI.	Documentos generados por el servidor de Active Directory.	La administración de cuentas de usuario se lo realiza a través de un servicio de directorio, pero este servicio no cuenta con políticas y procedimientos establecidos.

DS5.19 Prevención, Detección y Corrección del Software Dañino	Entrevista al director de TI.	Inventario de software del Hospital General “Enrique Garcés”	No se realiza un mantenimiento preventivo, se lleva un control de cambios de software pero sin procedimientos de control establecidos.
DS5.20 Arquitectura de Firewalls y Conexiones con las Redes Públicas	Entrevista a un empleado del área de TI.	Topología de la red del Hospital General “Enrique Garcés”	No se encuentran definidos los procesos de administración de acceso y restricción del firewall de la organización, se lleva un control de acceso por medio del firewall pero sin reportes de violaciones a la seguridad y procedimientos de revisión administrativa

Tabla 2.39: Tabla Resumen DS5

Dominio: Entrega y Soporte				
Proceso: DS5 GARANTIZAR LA SEGURIDAD DE SISTEMAS				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.	√		**Grado de Madurez.** El proceso de garantizar la seguridad en los sistemas se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se generan reportes de seguridad de los sistemas implantados, no se cuenta con la infraestructura adecuada para realizar estos controles.
Nivel 1	La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.		√	
Nivel 2	Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. El entrenamiento sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como			

	parte de su propia disciplina.			
Nivel 3	Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe entrenamiento en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.			
Nivel 4	Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están liGrados con los objetivos del negocio. El entrenamiento sobre seguridad se imparte tanto para TI como para el negocio. El entrenamiento sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.			
Nivel 5	La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada			

	con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIs para ajustar el plan de seguridad en un proceso de mejora continua.			

Tabla 2.40 Modelo de Madurez DS5

COBIT plantea para el DS5 la necesidad de cumplir con los siguientes objetivos de control.

1. Manejo de las Medidas de Seguridad
2. Identificación, Autenticación y Acceso
3. Seguridad de Acceso a Datos en Línea
4. Administración de Cuentas de Usuario
5. Revisión Gerencial de Cuentas de Usuario
6. Control de Usuario de las Cuentas de Usuario
7. Vigilancia de Seguridad
8. Clasificación de Datos
9. Administración Centralizada de Identificación y Derechos de Acceso
10. Reportes de Actividades de Violación y Seguridad
11. Manejo de Incidentes
12. Re-acreditación
13. Contrapartes confiables
14. Autorización de Transacción
15. No Rechazo
16. Ruta Confiable
17. Protección de las Funciones de Seguridad
18. Administración de Llaves Criptográficas
19. Prevención, Detección y Corrección del Software Dañino
20. Arquitectura de Firewalls y Conexiones con las Redes Públicas
21. Protección del Valor Electrónico

El DS5 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Tener un plan de administración centralizada de identificación y derechos de acceso de los usuarios, evitando posibles problemas con accesos no autorizados. • Crear políticas de autorización para realizar transacciones, en base a los lineamientos del negocio y supervisadas por el director del área de TI. • Crear un repositorio de información para el manejo de incidentes. • Revisar las seguridades físicas dentro de la unidad de TI y analizar si son las suficientes para controlar y salvaguardar la información que allí se tiene.

Estrategias a largo plazo	• Mantener políticas de seguridad para todos los equipos del hospital, para evitar perdida o mala utilización de los mismos. • Establecer políticas de uso y monitoreo del software instalado en cada máquina. • Supervisar que las políticas de seguridad estén siendo cumplidas por todos los empleados.

Tabla 2.41: Estrategias a corto y largo plazo DS5

2.3.3.4. DS7 Educación y entrenamiento de usuarios

Guías de auditoria

Considerando si:

Existen políticas y procedimientos relacionados con una concientización continua de seguridad y controles

Se cuenta con un programa de educación/entrenamiento enfocado a los principios de seguridad y control de los sistemas de información

Los nuevos empleados tienen conocimiento y conciencia de la responsabilidad de seguridad y control con respecto a la utilización y la custodia de los recursos de TI

Se cuenta con políticas y procedimientos vigentes relacionados con entrenamiento y si éstos están actualizados con respecto a la configuración técnica de los recursos de TI

Existe disponibilidad de oportunidades y frecuencia de entrenamiento interno, considerando también la asistencia de los empleados

Existe disponibilidad de oportunidades y frecuencia de entrenamiento técnico externo, considerando también la asistencia de los empleados

Si una función de entrenamiento es analizada con base en las necesidades de entrenamiento del personal con respecto a seguridad y controles, trasladando estas necesidades en oportunidades de entrenamiento interno o externo

Se requiere a todos los empleados asistir a entrenamientos de conciencia de control y seguridad continuamente, los cuales incluirían, sin limitarse a:

- principios generales de seguridad de sistemas
- conducta ética de TI
- prácticas de seguridad para la protección contra daños ocasionados por fallas que afecten la disponibilidad, confidencialidad, integridad y desempeño de las funciones en una forma segura

- existen las responsabilidades asociadas con la custodia y utilización de los recursos de TI
- la seguridad de la información y los sistemas de información cuando se utilizan en un sitio alterno/externo

Probando que:

Los nuevos empleados tienen conciencia y conocimiento de la seguridad, controles y responsabilidades fiduciarias de poseer y utilizar recursos de TI

Las responsabilidades de los empleados con respecto a la confidencialidad, integridad, disponibilidad, confiabilidad y seguridad de todos los recursos de TI son comunicadas continuamente

Un grupo de la función de TI es formalmente responsable del entrenamiento para el personal de TI, sobre concientización en seguridad y control y mantenimiento de programas de educación continua para certificaciones profesionales

Se considera continuamente la evaluación de las necesidades de entrenamiento para empleados

El desarrollo o la participación en los programas de entrenamiento relacionados con seguridad y controles es parte de los requerimientos de entrenamiento

Existen programas de entrenamiento vigentes para concientizar a los nuevos y antiguos empleados en seguridad

Los acuerdos de confidencialidad y conflicto de intereses son firmados por todos los empleados

No faltan estatutos de confidencialidad y conflicto de intereses para empleados

No faltan evaluaciones de necesidades de entrenamiento para empleados

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS7.1 Identificación de necesidades de entrenamiento	Entrevista a un empleado del área de TI. Entrevista al director de TI.	No existen documentos de respaldo de identificación de necesidades de entrenamiento.	Se identifican las necesidades de capacitación pero no siempre son atendidas.
DS7.2 Organización de Entrenamiento	Entrevista al director de TI. Entrevista al gerente de servicios generales.	No existen documentos de respaldo de organización de entrenamiento.	No existen políticas y procedimientos de entrenamiento y la planeación de estos eventos se lo hace sin procedimientos definidos.
DS7.3 Entrenamiento sobre principios y conciencia de Seguridad	Entrevista a un empleado del área de TI.	No existen documentos de respaldo sobre entrenamiento sobre principios y conciencia de seguridad.	No existen procedimientos de un concientización continua sobre principios de seguridad y control de los sistemas de información.

Tabla 2.42: Tabla Resumen DS7

Dominio: Entregar y Soporte				
Proceso: DS7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	Hay una total falta de programas de entrenamiento y educación. La organización no reconoce que hay un problema a ser atendido respecto al entrenamiento y no hay comunicación sobre el problema.	√		**Grado de Madurez.** El proceso de educación y entrenamiento de usuarios se encuentra en un nivel 0. **Objetivos no Cumplidos** El Hospital General "Enrique Garcés" no ha establecido un plan de capacitación o educación a los empleados, quienes reciben capacitaciones esporádicas o pagadas por ellos mismos que no son suficientes.
Nivel 1	Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre la seguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.		√	
Nivel 2	Hay conciencia sobre la necesidad de un programa de entrenamiento y educación, y sobre los procesos asociados a lo largo de toda la organización. El entrenamiento está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se han desarrollado hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores, cubriendo los mismos temas de materias con diferentes puntos de vista. Algunas de las clases abordan los temas de conducta ética y de conciencia sobre prácticas y actividades de seguridad en los sistemas. Hay una gran dependencia del conocimiento de los individuos. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.			
Nivel 3	El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades			

	de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento y educación son monitoreados, pero no todas las desviaciones son susceptibles de detección por parte de la gerencia. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.			
Nivel 4	Hay un programa completo de entrenamiento y educación que produce resultados medibles. Las responsabilidades son claras y se establece la propiedad sobre los procesos. El entrenamiento y la educación son componentes de los planes de carrera de los empleados. La gerencia apoya y asiste a sesiones de entrenamiento y de educación. Todos los empleados reciben entrenamiento sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. Todos los empleados reciben el nivel apropiado de entrenamiento sobre prácticas de seguridad en los sistemas para proteger contra daños originados por fallas que afecten la disponibilidad, la confidencialidad y la integridad. La gerencia monitorea el cumplimiento por medio de revisión constante y actualización del programa y de los procesos de entrenamiento. Los procesos están en vía de mejora y fomentan las mejores prácticas internas.			
Nivel 5	El entrenamiento y la educación dan como resultado la mejora del desempeño individual. El entrenamiento y la educación son componentes críticos de los planes de carrera de los empleados. Se asignan suficientes presupuestos, recursos, instalaciones e instructores para los programas de entrenamiento y educación. Los procesos se afinan y están en continua mejora, tomando ventaja de las mejores prácticas externas y de modelos de madurez de otras organizaciones. Todos los problemas y desviaciones se analizan para identificar las causas de raíz, se identifican y llevan a cabo acciones de forma expedita. Hay una actitud positiva con respecto a la conducta ética y respecto a los principios de			

	seguridad en los sistemas. TI se utiliza de manera amplia, integral y óptima para automatizar y brindar herramientas para los programas de entrenamiento y educación. Se utilizan expertos externos en entrenamiento y se utilizan benchmarks del mercado como orientación.			

Tabla 2.43: Modelo de Madurez DS7

COBIT plantea para el DS7 la necesidad de cumplir con los siguientes objetivos de control.

1. Identificación de necesidades de entrenamiento.
2. Organización de entrenamiento.
3. Entrenamiento sobre principios y conciencia de Seguridad.

El DS7 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deben manejar estrategias a corto y largo plazo, que de acuerdo a la metodología de COBIT se recomienda lo siguiente:

Estrategias a corto plazo	• Crear planes de capacitación para usuarios sobre el software instalado.
Estrategias a largo plazo	• Crear un plan de organización de capacitaciones y entrenamientos para usuarios. • Crear planes de capacitación a usuarios sobre principio y conciencia de seguridad.

Tabla 2.44 Estrategias a corto y largo plazo DS7

2.3.3.5. DS8 Apoyo y asistencia para los clientes

Guías de auditoria

Considerando si:

La naturaleza de la función del Help Desk (por ejemplo, la forma en las solicitudes de ayuda son procesadas y la asistencia es proporcionada) es efectiva

Existen instalaciones vigentes, divisiones o departamentos que lleven a cabo la función de Help Desk, así como personal o posiciones responsables del Help Desk

El nivel de documentación para las actividades del Help Desk es adecuado y está actualizado

Existe un proceso real para registrar solicitudes de servicios y si se hace uso de dicha bitácora

El proceso para el escalamiento de preguntas y la intervención de la administración para su solución son suficientes

El período de tiempo para atender las solicitudes recibidas es adecuado

Existen los procedimientos para el seguimiento de tendencias y reportes de las actividades del Help Desk

Se identifican y ejecutan formalmente iniciativas de mejora de desempeño

Se alcanzan y se cumple con los acuerdos de nivel de servicio y los estándares de desempeño

El nivel de satisfacción del usuario periódicamente se revisa y se reporta

Probando que:

Las políticas y procedimientos son actuales y precisos en relación con las actividades del Help Desk

Los compromisos de nivel de servicio son conservados y que las variaciones son explicadas

Las solicitudes de servicio son atendidas de una forma oportuna

El análisis y reporte de tendencias asegura que los reportes:

- son emitidos y que se toman las medidas necesarias para mejorar el servicio
- incluyen problemas específicos, análisis de tendencias y tiempos de respuesta
- son enviados a las personas responsables con la autoridad para resolver los problemas

Se obtienen para una muestra de solicitudes de ayuda, confirmación de la precisión, oportunidad y suficiencia de la respuesta

Las encuestas sobre el nivel de satisfacción del usuario existen y se trabaja con ellas

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS8.1 Help Desk	Entrevista al director de TI. Entrevista usuarios claves de los servicios de TI.	No existen documentos de respaldo de Help Desk.	Las solicitudes a Help Desk son procesadas, aunque no se cuenta con procedimientos definidos para hacerlo. La asistencia brindada a los usuarios es efectiva, pero no siempre el periodo de tiempo es adecuado
DS8.2 Registro de consultas del cliente	Entrevista a un empleado de soporte técnico. Entrevista a un empleado del área de TI.	No existen documentos de respaldo de consultas del cliente.	Las consultas de los clientes son atendidas, pero no existe un proceso real para registrar las solicitudes de servicios ni se lleva una bitácora.
DS8.4 Monitoreo de atención a	Entrevista a un empleado de	No existen documentos de respaldo de monitoreo a	No se mide el nivel de satisfacción de los usuarios

clientes	soporte técnico. Entrevista a un empleado del área de TI.	clientes.	periódicamente

Tabla 2.45: Tabla Resumen DS8

Dominio: Entrega y Soporte				
Proceso: DS8 APOYO Y ASISTENCIA PARA LOS CLIENTES				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No hay soporte para resolver problemas y preguntas de los usuarios. Hay una completa falta de procesos para la administración de incidentes. La organización no reconoce que hay un problema que atender.	√		**Grado de Madurez.** El proceso de Apoyo y asistencia para los clientes se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no existe una mesa de servicios para resolver preguntas de clientes directamente.
Nivel 1	La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan.		√	
Nivel 2	Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación sobre procedimientos estándar y la responsabilidad es delegada al individuo.			
Nivel 3	Se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes. Los procedimientos se estandarizan y documentan, pero se lleva acabo entrenamiento informal. Se deja la responsabilidad al individuo de conseguir entrenamiento y de seguir los estándares. Se desarrollan guías de usuario y preguntas frecuentes (FAQs), pero los individuos deben encontrarlas y puede ser que no las sigan. Las consultas y los incidentes se rastrean de forma manual y se monitorean de forma individual, pero no existe un sistema formal de reporte. No se mide la respuesta oportuna a las consultas e incidentes y los			

	incidentes pueden quedar sin resolución. Los usuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes.			
Nivel 4	En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está entrenado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.			
Nivel 5	El proceso de administración de incidentes y la función de mesa de servicio están bien organizados y establecidos y se llevan a cabo con un enfoque de servicio al cliente ya que son expertos, enfocados al cliente y útiles. Los KPIs y KGIs son medidos y reportados sistemáticamente. Una amplia y extensa cantidad de preguntas frecuentes son parte integral de la base de conocimientos. Existen a disposición del usuario, herramientas para llevar a cabo autodiagnósticos y para resolver incidentes. La asesoría es consistente y los incidentes se resuelven de forma rápida dentro de un proceso estructurado de escalamiento. La gerencia utiliza una herramienta integrada para obtener estadísticas de desempeño del proceso de administración de incidentes y de la función de mesa de servicio. Los procesos han sido afinados al nivel de las mejores prácticas de la industria, con base en los resultados del análisis de los KPIs y KGIs, de la mejora continua y de benchmarking con otras organizaciones.			

Tabla 2.46 Modelo de Madurez DS8

COBIT plantea para el DS8 la necesidad de cumplir con los siguientes objetivos de control.

1. Help Desk
2. Registro de consultas del cliente
3. Escalamiento de consultas del cliente
4. Monitoreo de atención a clientes
5. Análisis y reporte de tendencias

El DS8 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Establecer un servicio de help desk encargado de resolver incidentes menores que no necesiten de la presencia de un especialista. • Establecer políticas de escalamiento de incidentes en caso de no poder ser resueltos en el nivel inferior.
Estrategias a largo plazo	• Crear políticas de monitoreo a clientes para consultar su nivel de satisfacción. • Crear reportes de problemas resueltos y no resueltos y analizar sus resultados.

Tabla 2.47: Estrategias a corto y largo plazo DS8

2.3.3.6. DS10 Administración de problemas e incidentes

Guías de auditoria

Considerando si:

Existe un proceso de manejo de problemas que asegure que todos los eventos operacionales que no son parte de las operaciones estándar son registrados, analizados y resueltos de manera oportuna, y que se generan reportes de incidentes para problemas significativos

Existen procedimientos de manejo de problemas para:

- definir e implementar un sistema de administración de problemas
- registrar, analizar y resolver de manera oportuna todos los eventos no-estándar
- establecer reportes de incidentes para los eventos críticos y la emisión de reportes para usuarios
- identificar tipos de problemas y metodología de priorización que permitan una variedad de soluciones toman-do el riesgo como base
- definir controles lógicos y físicos de la información de manejo de problemas
- distribuir salidas sobre la base de —necesidad de conocer
- seguir las tendencias de los problemas para maximizar recursos y reducir la rotación
- recolectar entradas de datos precisas, actuales, consistentes y utilizables para la emisión de reportes
- notificar al nivel apropiado de administración sobre los escalamientos y concientización
- determinar si la administración evalúa periódicamente el proceso de manejo de problemas en cuanto a una mayor efectividad y eficiencia
- asegurar la suficiencia de los seguimientos de auditoría para los problemas de sistemas
- asegurar la integración entre los cambios, la disponibilidad, los sistemas y el personal de administración de la configuración

Probando que:

Una muestra seleccionada de salidas de procesos cumple con los procedimientos establecidos relacionados con:

- problemas no-críticos
- problemas críticos/ de alta prioridad que requieren escalamiento
- el reporte de los requerimientos, el contenido, la exactitud, distribución y acciones tomadas
- Satisfacción del usuario con el proceso del manejo de problemas y sus resultados

Vía entrevistas, el conocimiento y la conciencia del proceso de manejo de problemas

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS10.1 Sistema de administración de Problemas	Entrevista a un empleado de soporte técnico. Entrevista al director de TI.	No existen documentos de respaldo del sistema de administración de problemas.	No existe un proceso de manejo de problemas que asegure que todos los eventos sean registrados, analizados y resueltos de maneara oportuna.
DS10.2 Escalamiento de Problemas	Entrevista a un empleado de soporte técnico.	No existen documentos de respaldo del escalamiento de problemas.	No existen procedimientos establecidos para el escalonamiento de problemas, este procedimiento se lo hace de acuerdo al criterio del personal de TI a cargo.
DS10.3 Seguimiento de Problemas y Pistas de	Entrevista a un empleado del área de TI.	No existen documentos de respaldo de seguimiento de	No se realiza seguimiento de los problemas resueltos o inconclusos, ni se hace un

Auditoría	Entrevista a un empleado de soporte técnico.	problemas.	seguimiento de pistas de auditoría.

Tabla 2.48: Tabla Resumen DS10

Dominio: Entrega y Soporte				
Proceso: DS10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.	√		**Grado de Madurez.** El proceso de administración de problemas e incidentes se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se cuenta con una administración de problemas e incidentes, no se tiene una mesa de atención a clientes, ni políticas o procedimientos para la administración de problemas.
Nivel 1	Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.		√	
Nivel 2	Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.			
Nivel 3	Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y entrenamiento. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y			

	proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.			
Nivel 4	El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramente establecidas. Los métodos y los procedimientos son documentados, comunicados y medidos para evaluar su efectividad. La mayoría de los problemas están identificados, registrados y reportados, y su solución ha iniciado. El conocimiento y la experiencia se cultivan, mantienen y desarrollan hacia un nivel más alto a medida que la función es vista como un activo y una gran contribución al logro de las metas de TI y a la mejora de los servicios de TI. La administración de problemas está bien integrada con los procesos interrelacionados, tales como administración de incidentes, de cambios, y de configuración, y ayuda a los clientes para administrar información, instalaciones y operaciones. Se han acordado los KPIs y KGIs para el proceso de administración de problemas.			
Nivel 5	El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.			

Tabla 2.49 Modelo de Madurez DS10

COBIT plantea para el DS10 la necesidad de cumplir con los siguientes objetivos de control.

1. Sistema de administración de Problemas
2. Escalamiento de Problemas
3. Seguimiento de Problemas y Pistas de Auditoría
4. Autorizaciones de acceso temporales y de emergencia
5. Prioridades para procesamiento de emergencia

El DS12 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se debería manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Crear una mesa de atención a clientes, que maneje un sistema de administración de problemas. • Establecer políticas de escalamiento de problemas. Evitando así gastos innecesarios para la empresa.
Estrategias a largo plazo	• Definir prioridades para mitigar riesgos, y reconocer incidentes. • Realizar un seguimiento de problemas y pistas de auditoría.

Tabla 2 Estrategias a corto y largo plazo DS10

2.3.3.7. DS12 Administración de instalaciones

Guías de auditoria

Considerando si:

La localización de las instalaciones no es obvia externamente, se encuentra en el área u organización menos accesible, y si el acceso es limitado al menor número de personas

Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para emplea-dos, proveedores, equipo y personal de mantenimiento de las instalaciones

Los procedimientos y prácticas de administración de llave (“Key”) y lectora de tarjetas (“card reader”) son adecuados, incluyendo la actualización y revisión continua tomando como base una “menor necesidad de acceso”

Las políticas de acceso y autorización de entrada/salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles

Se llevan a cabo revisiones periódicas de los perfiles de acceso, incluyendo revisiones administrativas

Existen y se llevan a cabo los procesos de revocación, respuesta y escalamiento en caso de violaciones a la seguridad

Existe el proceso de “signage” con respecto a la no identificación de áreas sensibles, y si es consistente con los requerimientos de seguro, código de construcción local y regulatorios

Las medidas de control de seguridad y acceso incluyen a los dispositivos de información portátiles utilizados fuera del sitio

Se lleva a cabo una revisión de los registros de visitantes, asignación de pases, escolta, persona responsable del visitan-te, bitácora para asegurar tanto los

registros de entradas como de salidas y el conocimiento de la recepcionista con respecto a los procedimientos de seguridad

Se lleva a cabo una revisión de los procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma, así como las respuestas esperadas en los distintos escenarios para los diferentes niveles de emergencias ambientales

Se lleva a cabo una revisión de los procedimientos de control de aire acondicionado, ventilación, humedad y las respuestas esperadas en los distintos escenarios de pérdida o extremos no anticipados

Probando que:

El personal tiene conciencia y comprende la necesidad de seguridad y controles

Los armarios cableados están físicamente protegidos con el acceso posible autorizado y el cableado se encuentra bajo tierra o conductos protegidos tanto como sea posible

El proceso de “signage” identifica rutas de emergencia y qué hacer en caso de una emergencia o violación a la seguridad

Los directorios de teléfono en otras partes de la instalación no identifican localidades sensibles

La bitácora de visitantes sigue apropiadamente los procedimientos de seguridad

Existen los procedimientos de identificación requeridos para cualquier acceso dentro o fuera vía observación

Las puertas, ventanas, elevadores, ventilas y ductos o cualquier otro modo de acceso están identificados

El personal de las instalaciones rota turnos y toma vacaciones y descansos apropiados

Existen los procedimientos de mantenimiento y registro para un desempeño de trabajo oportuno

Las variaciones de las políticas y procedimientos en las operaciones de los turnos segundo y tercero son reportadas

Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones

No se almacenan útiles peligrosos

Existe el seguimiento de auditoría de control de acceso sobre software de seguridad o reportes clave de administración

Se ha dado seguimiento a toda emergencia ocurrida en el pasado o a su documentación

El personal con acceso son empleados reales

Se llevan a cabo verificaciones de suficiencia de administración clave de acceso

Se otorga una educación en seguridad física y conciencia de seguridad

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS12.1 Seguridad Física	Entrevista a un empleado del área de TI.	No existen documentos de respaldo sobre la seguridad física.	Las instalaciones se encuentran en un área menos accesible al público en general, pero no se tienen procedimientos de acceso lógico y físico para empleados.
DS12.2 Bajo Perfil de las Instalaciones de Tecnología de Información	Entrevista al director de TI. Entrevista a un empleado de soporte técnico.	No existen documentos de respaldo sobre el bajo perfil de las instalaciones de TI.	No se poseen políticas y procedimientos relacionados con el plan de las instalaciones, la seguridad física y lógica, acceso y salida.

Tabla 2.51:3 Tabla Resumen DS12

Dominio: Entrega y Soporte				
Proceso: DS12 Administración de instalaciones				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.	√		**Grado de Madurez.** El proceso de administración de instalaciones se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se reconoce la importancia de la seguridad sobre las instalaciones y la creación de ambientes que permitan desempeñar de manera correcta las actividades.
Nivel 1	La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.		√	
Nivel 2	Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.			
Nivel 3	Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no			

	son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.			
Nivel 4	Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.			
Nivel 5	Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente cómputo de la organización. Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.). Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan sin operadores humanos. Los KPIs y KGIs se miden regularmente. Los programas de mantenimiento preventivo fomentan un estricto apego a los horarios y se aplican pruebas regulares a los equipos sensibles. Las estrategias de instalaciones y de estándares están alineadas con las metas de			

	disponibilidad de los servicios de TI y están integradas con la administración de crisis y con la planeación de continuidad del negocio. La gerencia revisa y optimiza las instalaciones utilizando los KPIs y KGIs de manera continua, capitalizando oportunidades para mejorar la contribución al negocio.			

Tabla 2.52: Modelo de Madurez DS12

COBIT plantea para el DS12 la necesidad de cumplir con los siguientes objetivos de control.

1. Seguridad Física
2. Bajo Perfil de las Instalaciones de Tecnología de Información
3. Escolta de Visitantes
4. Salud y Seguridad del Personal
5. Protección contra Factores Ambientales
6. Suministro Ininterrumpido de Energía

El DS12 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 2, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Establecer políticas de seguridades físicas que puedan ayudar a mantener un mejor control sobre el hardware y la información. • Establecer políticas para protección contra factores ambientales.
Estrategias a largo plazo	• Establecer políticas de prevención de incidentes externos.

Tabla 2.53: Estrategias a corto y largo plazo DS12

2.3.3.8. Resumen del Dominio Entregar y dar Soporte

Para el dominio de entregar y dar soporte, dentro de la evaluación del Hospital General “Enrique Garcés” que nos plantea COBIT, la evaluación arroja los siguientes resultados: las evaluaciones no son buenas, ya que los niveles de madurez se encuentran en promedio en un nivel de madurez de 1 que es bajo, esto obedece a diferentes razones, entre las principales que podemos encontrar son: La falta de personal, la falta de planificación para un control, la poca o nula capacitación que se les da a los usuarios, procesos que no son manejados de la manera adecuada y desembocan en que el dominio de entrega y de dar soporte no tenga un buen nivel de madurez.

La falta de recursos asignados al área de TI es otro factor importante para que no se pueda realizar un trabajo que solvente todas las necesidades que tiene el hospital. No se puede garantizar la continuidad del servicio y se realiza poca o nada de previsión de inconvenientes lo cual dificulta el trabajo de la unidad de TI. No se cuenta con acuerdos de nivel de servicio los cuales deberían ser implementados para establecer si la unidad cumple o no con lo establecido.

Otro factor determinante para los resultados de estas evaluaciones es el ambiente físico en el que se maneja el área de TI, y los equipos insuficientes con los que cuenta para realizar su trabajo. Dentro del ambiente físico se deben realizar varias adecuaciones, para que se puedan desenvolver de mejor manera las actividades cotidianas.

Dentro del ambiente físico, se deben implementar mejores políticas de seguridad, y se debe tener un plan de contingencia para salvaguardar la información que el área de TI maneja. Una vez que se tengan solventadas estas necesidades, la capacitación a los usuarios es otro factor importante, para la reducción de los incidentes generados.

Finalmente, la unidad de TI debe abrir una mesa de servicio y de control de incidentes para poder garantizar la continuidad en el servicio, un manejo adecuado de incidentes, llevar u control de satisfacción de clientes y poder realizar escalamientos de problemas en base a procedimientos establecidos.

2.3.4. PROCESOS DEL DOMINIO MONITOREO

2.3.4.1. M1 Monitoreo de los procesos

Guías de auditoria

Considerando si:

Los datos identificados para monitorear los recursos de TI son apropiados

Se usan indicadores clave del desempeño y/o factores críticos de éxito para medir el desempeño de TI en comparación con los niveles deseables.

Los reportes internos de la utilización de los recursos de TI (gente, instalaciones, aplicaciones, tecnología y datos) son adecuados.

Existe una revisión administrativa de los reportes de desempeño de los recursos de TI

Existen controles de monitoreo para proporcionar una retroalimentación confiable y útil de manera oportuna

La respuesta de la organización a las recomendaciones de mejoramiento de control de calidad, auditoría interna y auditoría externa es apropiada

Existen iniciativas y resultados de mejoramiento del desempeño deseado

Se está dando el desempeño organizacional en comparación con las metas establecidas dentro de la organización

Existe análisis sobre satisfacción del usuario

Probando que:

Existen reportes de monitoreo del desempeño de los datos

Existe revisión administrativa de los reportes de monitoreo del desempeño e iniciativas de acciones correctivas

Los empleados están conscientes y comprenden las políticas y procedimientos relativos al monitoreo del desempeño

La calidad y el contenido de los reportes internos se relacionan con:

- La recolección de datos de monitoreo del desempeño
- El análisis de los datos de monitoreo del desempeño
- El análisis de los datos del desempeño de los recursos
- Las acciones administrativas sobre problemas del desempeño
- El análisis de encuestas de satisfacción de los usuarios

La alta administración está satisfecha con los reportes sobre el monitoreo del desempeño

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
M1.2 Evaluar el Desempeño	Entrevista al director de TI. Entrevista al gerente de servicios generales.	No existen documentos de respaldo de la evaluación de desempeño.	No se evalúa el desempeño del departamento de TI, ni se mide la satisfacción del cliente.
M1.3 Evaluar la Satisfacción del Cliente	Entrevista al director de TI. Entrevista a una secretaria del hospital.	No existen documentos de respaldo de la satisfacción del cliente.	La satisfacción de los clientes del departamento de TI es alta, a pesar de no llevarse un control al momento de brindar soporte y mantenimiento.

Tabla 2.54: Tabla Resumen M1

Dominio: Monitoreo				
Proceso: M1 MONITOREO DE LOS PROCESOS				
Niveles de los Modelos de Madurez		**Cumple**	**No Cumple**	**Observaciones**
Nivel 0	La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de forma independiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de los procesos no se reconoce.	√		**Grado de Madurez.** El proceso de monitoreo de procesos se encuentra en un nivel 0. **Objetivos no Cumplidos** En el Hospital General "Enrique Garcés" no se ha realizado levantamiento de procesos para realizar un monitoreo.
Nivel 1	La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.		√	
Nivel 2	Se han identificado algunas mediciones básicas a ser monitoreadas. Los métodos y las técnicas de recolección y evaluación existen, pero los procesos no se han adoptado en toda la organización. La interpretación de los resultados del monitoreo se basa en la experiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.			
Nivel 3	La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico.			

	Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se han definido, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de satisfacción del cliente y los niveles de servicio están definidas. Se ha definido un marco de trabajo para medir el desempeño.			
Nivel 4	La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechan en toda la organización para recolectar y monitorear la información operativa de las aplicaciones, sistemas y procesos. La gerencia puede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas. Las mediciones de la función de TI están alienadas con las metas de toda la organización.			
Nivel 5	Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos, tales como el Balanced Scorecard. El monitoreo de los procesos y el rediseño continuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización.			

Tabla 2.55: Modelo de Madurez M1

COBIT plantea para el M1 la necesidad de cumplir con los siguientes objetivos de control.

1. Recolectar Datos de Monitoreo
2. Evaluar el Desempeño
3. Evaluar la Satisfacción del Cliente
4. Reporte Administrativo

El M1 debería tener algunos cambios para que pueda ascender a un nivel de madurez de 1, para lo cual se deberían manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT, se recomiendan las siguientes:

Estrategias a corto plazo	• Recolectar información sobre el desempeño del personal de TI y la satisfacción de los clientes del área. • Establecer procedimientos para la creación de reportes de desempeño del personal de área de TI. • Establecer procedimientos para la creación de reportes de satisfacción de los clientes de área de TI.
Estrategias a largo plazo	• Analizar los resultados de los reportes de desempeño del personal de área de TI para la toma de decisiones. • Analizar los resultados de los reportes de satisfacción de los clientes del área de TI para la toma de decisiones.

Tabla 2.56: Estrategias a corto y largo plazo M1

2.3.4.2. Resumen del Dominio Monitoreo y Evaluación

El dominio de monitoreo y evaluación en general se encuentra en un nivel de madurez 0 puesto que si bien es cierto se busca que la satisfacción del cliente sea alta, no se tiene formularios de control ni datos históricos que puedan corroborar que se esté realizando un buen trabajo.

No se realizan reportes administrativos para evaluar el desempeño de la unidad de TI, al igual que no se tiene un proceso de recolección de datos de la satisfacción de los clientes de área de TI con los servicios que este ofrece, es por ello que se necesita mejorar en varios aspectos, para que el nivel de madurez de este dominio mejore.

Finalmente, se tiene como observación, que el monitoreo y la evaluación dentro de la unidad de TI del hospital necesita mejorar notablemente, ya que en base de este proceso se puede demostrar la eficiencia de la unidad de TI ante la gerencia del hospital, lo que lo convierte en una prioridad para el ascenso de la unidad de TI.

CAPÍTULO 3:

ANÁLISIS DE RESULTADOS

3.1. ANÁLISIS DE RESULTADOS

A continuación se detallara el informe preliminar, y los informes finales técnico y ejecutivo, que estarán dirigidos al líder de la unidad de TI así como al director del Hospital “Enrique Garcés”, y demás de empleados que estén interesados en los resultados obtenidos de la auditoria basada en la metodología de COBIT.

Estos informes tendrán en común las conclusiones y recomendaciones que son elaborados en base de la auditoria y evaluación de cada uno de los procesos que corresponden a cada dominio, propuestos por COBIT, y que serán aplicados a la unidad de TI del Hospital General “Enrique Garcés”

3.2. INFORME PRELIMINAR

Con el objeto de realizar ciertos afinamientos a la auditoria nos vemos en la necesidad de escribir un informe preliminar el cual nos permitirá recolectar las observaciones necesarias para poder presentar un informe final con todos los puntos de vista, tanto de los evaluadores así como el de la dirección del hospital y de la unidad de TI

3.2.1. Presentación del informe preliminar

Quito, 5 de enero del 2012

Ing. Carlos Chancusig

Líder de la Unidad de TI del

Hospital “Enrique Garcés”

El motivo de la presente carta, es agradecerle por la colaboración brindada a lo largo del trabajo realizado por los estudiantes de la Escuela Politécnica Nacional. Además de la atención prestada para que los estudiantes puedan desenvolver las actividades requeridas para la práctica.

Además tiene como objetivo poner a su consideración los resultados obtenidos en la auditoría realizada a la unidad de TI.

3.2.2. Consideraciones previas.

“El Hospital general Enrique Garcés”, es una unidad operativa del Ministerio de Salud Pública del Ecuador, ubicado en el sector sur del Distrito Metropolitano de Quito, en la Provincia de Pichincha, que provee atención de salud de tipo ambulatorio en consulta externa, y de recuperación de la salud con internamiento

en Hospitalización, en las cuatro especialidades básicas de la medicina moderna; Medicina Interna, Cirugía, Pediatría y Gíneco - Obstetricia y en varias subespecialidades. Apoyadas todas ellas en servicios auxiliares de diagnóstico y tratamiento que funcionan las 24 horas del día y los 365 días del año. Es además Hospital en el que se desarrollan actividades docentes y de investigación en ciencias de la salud. [21]

El área de TI del hospital Enrique Garcés, en sus objetivos no coincide con los objetivos de la Informática del hospital del Sur, Además no se atienden de la mejor manera de las peticiones de cambios de los usuarios.

El Departamento de Sistemas es la unidad encargada de gestionar el apoyo informático a las actividades del Hospital Enrique Garcés, mediante el diseño, coordinación, implementación y operación de las bases de datos institucionales y de la red institucional de computación, informática y central telefónica. Así mismo presta asesoramiento y apoyo a las diferentes unidades, servicios y departamentos del Hospital Enrique Garcés.

Dicho esto en cada uno de los procesos de cada dominio se realizó las siguientes observaciones.

PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI	**Grado de Madurez** Nivel 1
Observaciones Realizadas:	
En el hospital "Enrique Garcés" no se ha establecido un plan estratégico para la unidad de TI que permita tener las políticas claras y que cubra todas las necesidades que el hospital requiera. Además, se nos indicó que el hospital tiene un plan estratégico general, pero para el área de sistemas no se cuenta con un plan estratégico que le permita definir todas sus tareas a realizar.	

Tabla 3.1 Tabla Grado de Madurez PO1

[21] REGLAMENTO ORGANICO FUNCIONAL HOSPITAL GENERAL "ENRIQUE GARCES"

PO2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
En el hospital "Enrique Garcés" no se maneja un plan para la arquitectura de la información, lo que hace que la información no se encuentre estandarizada, ni se reconozca la importancia de este aspecto. En el hospital también se nos indico que no se tiene un diccionario de datos, y que se encuentran en una migración de información, ya con ciertos estándares, pero no son suficientes para los que nos plantea COBIT	

Tabla 3.2 Tabla Grado de Madurez PO2

PO3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA	**Grado de Madurez** Nivel 1
Observaciones Realizadas:	
No se tiene un plan sobre cuál es la dirección tecnológica alineada con el negocio y las estrategias de TI. No se tiene un presupuesto para la adquisición de recursos tecnológicos, esto se lo hace en base a los requerimientos del día a día. No se tiene un plan de infraestructura tecnológica ni acuerdos para contingencias.	

Tabla 3.3 Tabla Grado de Madurez PO3

PO4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE TI	**Grado de Madurez** Nivel 1
Observaciones Realizadas:	
El área de sistemas está ubicada como un sub departamento del área de mantenimiento. El área de TI no tiene un nivel de asesor como debería dentro del hospital.	

Las acciones que realice el área de TI tienen que ser informadas al departamento de mantenimiento. Se tiene asignada el área de influencia del departamento de TI.

Tabla 3.4 Tabla Grado de Madurez PO4

PO6 COMUNICACIÓN DE LOS OBJETIVOS Y DE LAS ASPIRACIONES DE LA GERENCIA	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
Las políticas del área de TI, se las maneja directamente por disposiciones de entes superiores. No se elaboran políticas que apoyen la estrategia del área de TI. Los objetivos se los transmite de manera directa o a través de comunicados escritos a las diferentes dependencias del hospital, pero estos no siempre son comunicados a los interesados apropiados	

Tabla 3.5 Tabla Grado de Madurez PO6

PO9 EVALUACIÓN / ANALISIS DE RIESGOS	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
En el hospital “Enrique Garcés” no tiene políticas claras de mitigación de riesgos, los cuales son tratados de una manera reactiva, ocasionando que algunos objetivos del hospital no sean cumplidos. Los riesgos se los identifica de manera reactiva, es decir suceden para saber que se debe realizar como acción correctiva. Se tiene el expertis de cada uno de los integrantes del área de TI para resolver diferentes problemas que se presentan.	

Tabla 3.6 Tabla Grado de Madurez PO9

AI2 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
No se tiene un seguimiento sobre la seguridad de las aplicaciones y los requerimientos de seguridad. Se utilizan metodologías agiles de desarrollo para las aplicaciones pero no se garantiza que el software es desarrollado de acuerdo con todas las especificaciones de estas metodologías. No se configura el software adquirido en relación con los objetivos del negocio.	

Tabla 3.7 Tabla Grado de Madurez AI2

AI3 ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
En el hospital "Enrique Garcés" tiene como proceso reactivo el de adquirir la infraestructura tecnológica, debido a que no se posee ningún plan de contingencias, y trata solo de solucionar las contingencias a corto plazo. La adquisición de infraestructura nueva del hospital se la realiza por pedidos o por satisfacer nuevas necesidades, estas compras se las realizan siempre y cuando todavía se tenga presupuesto para las compras.	

Tabla 3.8 Tabla Grado de Madurez AI3

AI4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
No se tienen planes ni documentos, donde consten las soluciones de operación. No se realiza una correcta transferencia de conocimiento entre el área de TI y la	

gerencia del hospital. No se realiza una correcta transferencia de conocimiento al personal de operaciones y soporte.

Tabla 3.9 Tabla Grado de Madurez AI4

AI5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
En el hospital "Enrique Garcés" no existen criterios para estandarizar el software, ni existen procesos de instalación del mismo. Al igual que no se tiene procesos para migración de sistemas. Los planes para la implementación de software desarrollado no se encuentran documentados ni se lleva un control de fechas y objetivos.	

Tabla 3.10 Tabla Grado de Madurez AI5

DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	**Grado de Madurez** Nivel 1
Observaciones Realizadas:	
En el hospital "Enrique Garcés" posee un acuerdo de nivel de servicios. Además que se tiene una manera informal y reactiva de solucionar problemas, y las notificaciones de que se a realizado un servicio también es informal. Los servicios ofrecidos por el departamento de TI no cuentan con: definición de servicio, costo del servicio, nivel de servicio mínimo cuantificable, nivel de soporte por parte de la función de servicios de información, disponibilidad, confiabilidad y capacidad de crecimiento ni plan de continuidad	

Tabla 3.11 Tabla Grado de Madurez DS1

DS4 ASEGURAR EL SERVICIO CONTINUO	**Grado de Madurez**

	Nivel 1
Observaciones Realizadas:	
En el hospital "Enrique Garcés" no se tiene un plan formal para garantizar la continuidad del servicio, sino más bien se tiene elementos reactivos ante cualquier eventualidad. Además que el asigna miento de responsabilidades es muy limitada con relación al mantenimiento de equipos. No se encuentran totalmente identificados los recursos críticos de TI, y no se tienen planes de recuperación / seguridad para estos recursos. No existe una metodología para la priorización de aplicaciones y recursos.	

Tabla 3.12 Tabla Grado de Madurez DS4

DS5 GARANTIZAR LA SEGURIDAD DE SISTEMAS	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
El entrenamiento que se les ha dado a los usuarios de los sistemas informáticos del hospital ha sido escaso y en muchos casos no ha existido. Los planes para la implementación de software desarrollado no se encuentran documentados ni se lleva un control de fechas y objetivos. Las pruebas realizadas al software desarrollado en el hospital no son realizadas en base a planes y estrategias definidas Las pruebas realizadas al realizar un cambio en un sistema o software en el hospital no se rigen a planes y estrategias definidas.	

Tabla 3.13 Tabla Grado de Madurez DS5

DS7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
El hospital "Enrique Garcés" no ha establecido un plan de capacitación o educación a empleados los cuales reciben capacitaciones esporádicas o pagadas por ellos mismos, las cuales no son suficientes para estar actualizadas. No existen procedimientos de un concientización continua sobre principios de seguridad y control de los sistemas de información.	

Tabla 3.14 Tabla Grado de Madurez DS7

DS8 APOYO Y ASISTENCIA PARA LOS CLIENTES	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
El hospital "Enrique Garcés" no posee un mesa de servicios para resolver preguntas de clientes directamente Además en la unidad de TI, no hay personal que se dedique a esto específicamente. Las solicitudes a Help Desk son procesadas, aunque no se cuenta con procedimientos definidos para hacerlo. La asistencia brindada a los usuarios es efectiva, pero no siempre el periodo de tiempo es adecuado	

Tabla 3.15 Tabla Grado de Madurez DS8

DS10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
El hospital "Enrique Garcés" no cuenta con administración de problemas e incidentes, no se tiene una mesa de atención a clientes, y no se tiene una forma clara de administrar problemas. No existen procedimientos establecidos para el escalonamiento de problemas, este procedimiento se lo hace de acuerdo al criterio del personal de TI a cargo.	

Tabla 3.16 Tabla Grado de Madurez DS10

DS12 ADMINISTRACIÓN DE INSTALACIONES	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
En el hospital "Enrique Garcés" no se reconoce la importancia de la seguridad sobre las instalaciones y la creación de ambientes que permitan desempeñar de manera	

correcta las actividades. Las instalaciones se encuentran en un área menos accesible al público en general, pero no se tienen procedimientos de acceso lógico y físico para empleados.

Tabla 3.17 Tabla Grado de Madurez DS12

M1 MONITOREO DE LOS PROCESOS	**Grado de Madurez** Nivel 0
Observaciones Realizadas:	
En el hospital “Enrique Garcés” no se ha realizado levantamiento de procesos para realizar un monitoreo. La satisfacción de los clientes del departamento de TI es alta, a pesar de no llevarse un control al momento de brindar soporte y mantenimiento. No se evalúa el desempeño del departamento de TI, ni se mide la satisfacción del cliente.	

Tabla 3.18 Tabla Grado de Madurez M1

3.3. INFORME TÉCNICO

3.3.1. Alcance y justificación de la auditoria

Alcance

Este proyecto está orientado a realizar una auditoría al área de informática del Hospital Enrique Garcés, y se enfocara en su sistema informático, es decir se trabajará sobre sus servidores, su estructura de red, la topología de red, y los elementos que estén alrededor del área de informática.

Este proyecto comienza con la descripción de los procesos del hospital, para proceder luego con la realización de la auditoria del Sistema Informático, tomando en cuenta sus servidores y PC's, y la realización de la caracterización de la carga de trabajo, usando herramientas que permitan realizar estas mediciones.

Además realizará mediciones sobre estos equipos, y se entregarán las conclusiones respectivas.

Hay que aclarar que no nos involucraremos con el área de desarrollo del hospital, ni con sus metodologías que estén utilizando al crear aplicaciones para el hospital, no con el mantenimiento de equipos ni de servidores para mejorar el desempeño de los mismos.

Justificación

Actualmente el hospital se encuentra con tiempos de respuesta altos, porque el sistema no está desempeñando adecuadamente su papel. Esto se traduce en una mala atención al paciente, o en una atención inoportuna, además que se observa en el hospital pérdida de tiempo en la ejecución de los servicios de atención médica.

El proyecto tiene el afán de ayudar a la comunidad, a través de un hospital público, haciendo una auditoria del Sistema Informático, para aumentar su eficiencia y brindar un mejor servicio.

Objetivos propuestos de la auditoria

OBJETIVO GENERAL

Realizar la auditoria del Sistema Informático del Hospital del Sur “Enrique Garcés”.

OBJETIVOS ESPECÍFICOS

- Determinar falencias de Hardware y Software en el Sistema Informático del Hospital del Sur “Enrique Garcés”.
- Determinar los elementos críticos dentro del Sistema Informático.
- Mejorar la gestión de TI y redes en el Hospital del Sur.

Metodología COBIT

“COBIT (Control Objectives for Information and related Technology), Objetivos de Control para la información y Tecnologías relacionadas. Es una metodología originada como un marco creado por ISACA para la tecnología de la información (TI) y de Gobierno de TI, que se orienta directamente sobre el control de las actividades gerenciales, lo que hace que este enteramente relacionado con todo lo referente a tecnologías de la información.”

Las razones por la cuales se utilizará COBIT, son principalmente, porque incluye dentro de la metodología practicas en tecnología alineadas con las decisiones gerenciales y de gobierno de tecnología. Además de que COBIT está directamente dirigido a los administradores y gerentes de tecnología. Cabe resaltar que los auditores pueden desenvolverse de mejor manera ya que existes las guías y directrices con todas las actividades que se deben realizar para verificar si se encuentra en el camino correcto para la consecución del objetivo de la auditoria, además que se identifican los riesgos y procesos que no se están desempeñando de manera correcta.

Además con la utilización de COBIT puede mantener un marco de control interno, que puede ser útil para que la unidad de TI pueda mejorar en la prestación de sus servicios, con lo cual se brindará un valor agreGrado al trabajo realizado dentro de la unidad de TI. Finalmente utilizaremos COBIT ya que se tiene cierto expertis académico previo a la realización de esta tesis.

PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI	**Grado de Madurez** Nivel 1
Conclusión Final	
El Hospital "Enrique Garcés" no cuenta con un plan estratégico orientado a la unidad de TI que le permita establecer cuáles son sus obligaciones y responsabilidades, el cual también debería contener los objetivos que debe de cumplir el área informática, que deben ser orientados a la línea de negocio	
Recomendaciones Finales	
• Definir un plan estratégico a corto plazo que se ajuste directamente con la línea del negocio, y que sea discutido en las reuniones de dirección como un punto importante dentro de la agenda, para con ello tener una correcta estrategia dentro del área de TI. • Una vez creado un plan estratégico para la unidad de TI, se debe comenzar a identificar los riegos a los cuales está sujeta la unidad dentro del hospital. • Crear un plan estratégico a largo plazo, en donde se consideren los objetivos del negocio, la definición del área de TI y su ubicación dentro del hospital, además que se tome en cuenta infraestructura, inventario y soluciones tecnológicas que el área tenga que plantear. • Se recomienda tener una comunicación más directa con la dirección y gerencia del hospital, para llevar un mejor control y monitoreo de los planes y acciones de la unidad de TI. Al igual que manejar un política clara dentro del plan estratégico para la unidad.	

Tabla 3.19 Tabla Grado de Madurez PO1

PO2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN	**Grado de Madurez** Nivel 0
Conclusión Final	
La unidad de TI no posee documentos, ni planes para definir un arquitectura de información, lo que ocasiona que no existan estándares para el ingreso de información, que se ve reflejada en la poca comunicación entre los miembros de TI.	
Recomendaciones Finales	
• Definir un modelo de la arquitectura de la información, un diccionario de datos y reglas de sintaxis para que sea manejados por todos los usuarios. • Crear y comunicar un esquema de datos estándar para todos los usuarios. • Crear procesos y procedimientos que mantengan actualizado el diccionario de datos y las reglas de sintaxis. • Mantener la consistencia e integridad de la información en todo momento. • Crear estándares para los valores que se necesiten poner por defecto para acoplarse al diccionario de datos	

Tabla 3.20 Tabla Grado de Madurez PO2

PO3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA	**Grado de Madurez** Nivel 1
Conclusión Final	
No se tiene bien definida la dirección que debe tener la unidad de TI con relación a la dirección tecnológica, además que no se cuenta con un plan de adquisición con la infraestructura tecnológica.	
Recomendaciones Finales	
• Determinar un presupuesto, para crear una infraestructura tecnológica	

solida y que se ajuste a las necesidades y requerimientos del hospital.

- Difundir por parte de la unidad de TI la importancia de contar con una infraestructura solida, para atender a los usuarios de una mejor manera.
- Realizar un levantamiento de requerimientos con relación a la estructura necesaria, el mismo que debe ser enviado a la dirección para solventar los problemas mas importantes con relación a la infraestructura.
- Crear un plan de dirección tecnológica a largo plazo en el cual se revisen todos los riegos, eventualidades y problemas que la dirección tecnológica pueda tener.
- Crear y revisar planes de adquisición, para las compras que se deban realizar.
- Crear políticas de adquisición de materiales, no solo para cubrir eventualidades, sino también para tener reservas de equipos que puedan ser usados ante cualquier inconveniente.
- Realizar un presupuesto para la unidad de TI que sea acorde con las necesidades, y las posibles necesidades, para mantener una bodega con repuestos, y stock necesario para cubrir las diferentes necesidades.

Tabla 3.21 Tabla Grado de Madurez PO3

PO4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE TI	**Grado de Madurez** Nivel 1
Conclusión Final	
No se tiene documentos en la dirección en donde se tenga definida bien las funciones para cada departamento, sin embargo la unidad de TI si posee un documento en donde se delega a cada uno de sus empleados sus funciones.	
Recomendaciones Finales	
• Crear un documento en donde se especifiquen las funciones y responsabilidades de todos los empleados, y que el mismo sea difundido, en todo el hospital. • Crear un documento en el cual consten todos los logros institucionales, y cuáles son las metas a futuro. • Creación de políticas que rijan al personal por contrato dentro del hospital.	

• Dar a conocer las responsabilidades del nivel directivo, y de la dirección, para conocer con quien se debe reunir el líder de la unidad de TI • Mejorar las relaciones y comunicaciones entre el área de TI y el personal administrativo. • Ubicar el personal clave de la unidad de TI en comités y reuniones de la dirección.

Tabla 3.22 Tabla Grado de Madurez PO4

PO6 COMUNICACIÓN DE LOS OBJETIVOS Y DE LAS ASPIRACIONES DE LA GERENCIA	**Grado de Madurez** Nivel 0
Conclusión Final	
La dirección del hospital no tiene la mejor comunicación con el departamento de TI, ya que este no se encuentra en un nivel asesor de decisión dentro del hospital que le permita alinearse de mejor manera con los objetivos del negocio.	
Recomendaciones Finales	
• Crear políticas, procedimientos y estándares sobre los objetivos del hospital, los cuales deben ser difundidos en todos el hospital, los mismos que deben estar alineados con las políticas de los planes estratégicos. • Dar a conocer las metas, objetivos, y aspiraciones que el hospital tiene, para que los empleados sean más participativos y proactivos con dichas metas. • Definir claramente la misión y visón del hospital, y además dar a conocer a todos los empleados, para que sepan hacia donde se enrumba el hospital. • Definir códigos de moral y ética que se apliquen en el hospital para que no exista conflictos entre empleados. • Crear un plan de seguridad aplicable a todas las aéreas del hospital en donde la unidad de TI tenga influencia. • Crear un repositorio de datos donde ser tenga las políticas de situaciones especificas para poder ser controladas • Crear una comisión que se encargue del control del cumplimiento de políticas, procedimientos y estándares.	

Tabla 3.23 Tabla Grado de Madurez PO6

PO9 EVALUACIÓN / ANALISIS DE RIESGOS	**Grado de Madurez** Nivel 0
Conclusión Final	
Reconocer e identificar los riesgos para que estos puedan ser evaluados y analizados dentro del hospital y que impacto pueden tener los mismos sobre la continuidad del negocio.	
Recomendaciones Finales	
• Realizar una evaluación de todos los riegos que estén presentes dentro del hospital, asignando el control de cada uno de ellos a los respectivos líderes del departamento. • Realizar una evaluación de los impactos de estos riesgos y como afectarían al normal funcionamiento de hospital. • Crear planes de accione contra riegos que se puedan ser previstos desde el análisis de los riesgos. • Comunicar a los empleados cuales son los riesgos que el hospital pueda tener, para que con la ayuda de los propios empleados estos puedan ser atenuados o minorados. • Crear un comité que se encargue de dar seguimiento y controlar a los riesgos que puedan aparecer en el transcurso de cualquier eventualidad.	

Tabla 3.24 Tabla Grado de Madurez PO9

AI2 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tienen procesos para la creación, diseño y especificaciones para el mantenimiento de software, además que no se tienen procesos definidos para la adquisición de los mismos.	

Recomendaciones Finales
• Realizar un documento con todos los requerimientos y las especificaciones de los programas necesarios para asegurar la continuidad del negocio. • Realizar pruebas con el software aplicativo para verificar si es el correcto y cubre todas las necesidades del hospital, y si es el necesario para cubrir todas las actividades que son necesarias dentro del hospital. • Realizar pruebas funcionales continuas al software aplicativo del hospital. • Hacer cumplir las políticas de seguridad de la empresa en el software instalado. • Supervisar las acciones que son realizadas por los empleados en el software instalado. • Realizar una evaluación del sistema actual para conocer sus fortalezas y debilidades

Tabla 3.25 Tabla Grado de Madurez AI2

AI3 ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tienen planes ni procesos para la adquisición de tecnología, con lo cual no se le puede dar el seguimiento adecuado, a pesar de que tenga un inventario de los pasivos de la empresa.	
Recomendaciones Finales	
• Realizar evaluaciones periódicas en hardware y software, tanto en equipos nuevos como en equipos antiguos. • Crear un plan de mantenimientos preventivos, y tratar de evitar los mantenimientos reactivos para asegurar la continuidad del negocio. • Crear un plan para instalación de software original en todas las maquinas con lo cual se asegurar tener todos los equipos en regla. • Crear políticas de seguridad en todos los equipos, para evitar perdida o mala utilización de los mismos. • Controlar que el inventario este correcto, y que todos los equipos se	

encuentren en buen estado. • Establecer políticas de uso y monitoreo del software instalado en cada máquina. • Supervisar las acciones que son realizadas por los empleados con relación al hardware y al software que este a su cargo.

Tabla 3.26 Tabla Grado de Madurez AI3

AI4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tienen planes para levantar procedimientos, y con los cual no se puede definir ni mantener los procesos existentes en el hospital, con lo cual no se puede general la documentación necesaria tanto para usuarios como para operadores.	
Recomendaciones Finales	
• Se recomienda la creación de acuerdos de nivel de servicio, para establecer políticas de funcionamiento del área de TI • Crear manuales de usuario para las aplicaciones que son usadas por todo el personal, los mismos que deben ser difundidos a todos los empleados del hospital. • Establecer políticas de capacitación del área de TI para los usuarios con relación a aspectos ofimáticos y de sistemas que los mismos ocupen. • Crear políticas de documentación que maneje el área de TI para todos los sistemas que la misma maneje. • Realizar un rediseño de los procesos del hospital de ser requeridos para así tener un mejor control sobre los mismos además de tener un mejor desempeño en el trabajo. • Crear procesos administrativos que permitan ubicar de mejor manera a las necesidades del hospital para ser tratadas según su importancia. • Crear un repositorio documental para que cualquier usuario tenga acceso a información que necesite o requiera.	

Tabla 3.27 Tabla Grado de Madurez AI4

AI5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	**Grado de Madurez**

	Nivel 0
Conclusión Final	
No se tiene criterios para estandarización ni existen procesos de instalación y acreditación de sistemas, además que no se tiene metodologías para la instalación al igual que para la migración de sistemas. Al igual que no se cuenta con una arquitectura ni con un diccionario de datos.	
Recomendaciones Finales	
• Crear criterios para estandarizar la instalación de software y para la migración de datos. • Establecer una metodología de instalación de datos, además de establecer una base de software instalado en cada máquina. • Crear un plan para instalación de software original en todas las maquinas. • Realizar cursos de capacitación a usuarios y personal de TI con relación al software instalado. • Tener un tiempo de prueba con todo software instalado para saber si el mismo cubre las necesidades del hospital. • Tener infraestructura para tener un ambiente de pruebas, y realizar mediciones sobre el desempeño. • Crear planes de implementación e instalación de software nuevo, para evitar cualquier contratiempo.	

Tabla 3.28 Tabla Grado de Madurez AI5

DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	**Grado de Madurez** Nivel 0
Conclusión Final	
El hospital no se tiene un documento que tenga los acuerdos de nivel de servicio, esto hace que estos acuerdos sean muy informales y no se tenga los elementos para ejercer un mejor control sobre la unidad de TI	

Recomendaciones Finales
• Crear un marco referencial para un acuerdo de nivel de servicios. • Crear un conjunto de procedimientos de desempeño dentro de la unidad de TI para saber cómo actuar ante cualquier eventualidad. • Crear un programa de mejoramiento del servicio ofrecido por la unidad de TI, en donde se indiquen medidores de los mismos. • Establecer condiciones de nivel de servicios que la unidad de TI deba cumplir con respecto de todas las necesidades que el hospital tenga. • Dotar de la infraestructura adecuada además del personal suficiente para que estos acuerdos de nivel de servicios puedan ser cumplidos. • Crear un documento con convenios y contratos de nivel de servicios tanto para la unidad de TI, como para los servicios contratados

Tabla 3.29 Tabla Grado de Madurez DS1

DS4 ASEGURAR EL SERVICIO CONTINUO	**Grado de Madurez** Nivel 1
Conclusión Final	
No se tiene planes para asegurar la continuidad del servicio, por lo cual la mayoría de acciones que se realizan en el departamento de TI no son formales, y hace falta asignar las responsabilidades más formalmente.	
Recomendaciones Finales	
• Asignar responsabilidades de manera formal a cada empleado de la unidad de TI, para elementos críticos dentro del hospital, que permita garantizar la continuidad del servicio. • Realizar respaldos periódicos de la información critica, además de contar con el suficiente stock de hardware por cualquier eventualidad. • Crear un plan de continuidad, y realizar pruebas con este plan para verificar su valides. • Contar con un plan de continuidad de TI que este alineado al plan de continuidad del negocio, en el cual se incluyan procedimientos alternativos y medidas de emergencia. • Dotar de la infraestructura adecuada para que se pueda cumplir con este plan de continuidad en caso de una falla, o cualquier eventualidad que se pueda	

presentar. • Crear políticas que involucren a los usuarios, y difundir dichas políticas para que ante cualquier eventualidad los mismos usuarios sepan que hacer. • Realizar capacitaciones del plan de continuidad con los usuarios para que estos puedan saber cómo reaccionar ante cualquier eventualidad.

Tabla 3.30 Tabla Grado de Madurez DS4

DS5 GARANTIZAR LA SEGURIDAD DE SISTEMAS	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tienen maneras formales de controlar la seguridad, tales como reportes o informes de seguridad.	
Recomendaciones Finales	
• Tener un plan de administración centralizada de identificación y derechos de acceso para cada usuario, evitando asi posible problemas con accesos no autorizados. • Crear políticas de autorización para realizar transacciones, las mismas que deben ser verificadas por el respectivo líder de la unidad de TI. • Tener un repositorio de manejo de incidentes, el mismo que es necesario para seguir un procedimiento en cada incidente, a través de rutas confiables que no pongan en riesgo la información sensible del hospital • Crear políticas de seguridad en todos los equipos, para evitar perdida o mala utilización de los mismos. • Establecer políticas de uso y monitoreo del software instalado en cada máquina. • Supervisar que las políticas de seguridad estén siendo cumplidas por todos los empleados. • Tener el suficiente personal para que no existan problemas de seguridad en el área de TI	

Tabla 3.31 Tabla Grado de Madurez DS5

DS7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tiene planes de capacitación y entrenamiento para los usuarios del hospital	
Recomendaciones Finales	
• Tener planes de capacitación para usuarios sobre software instalado. • Crear un plan de organización de capacitaciones y entrenamientos para usuarios	

Tabla 3.32 Tabla Grado de Madurez DS7

DS8 APOYO Y ASISTENCIA PARA LOS CLIENTES	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tiene una forma formal de dar asistencia a los clientes, y el soporte brindado por la unidad de TI no es suficiente para cubrir todas las necesidades que el hospital tiene.	
Recomendaciones Finales	
• Crear un help desk encargado de resolver problemas menores y que no	

necesiten de la presencia de un especialista • Crear escalamiento de problemas si son necesarios. • Crear políticas de monitoreo a clientes para consultar su nivel de satisfacción. • Crear reportes de problemas resueltos y análisis de los mismos.

Tabla 3.33 Tabla Grado de Madurez DS8

DS10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tienen un encargado de administrar problemas, y no se tiene un plan de comunicación de la solución de problemas.	
Recomendaciones Finales	
• Crear una mesa de atención a clientes, que maneje un sistema de administración de problemas. • Tener una política de escalamiento de problemas. Evitando así gastos innecesarios para la empresa. • Crear políticas de seguridad en todos los equipos, para evitar perdida o mala utilización de los mismos. • Definir prioridades para mitigar riesgos, y reconocer incidentes.	

Tabla 3.34 Tabla Grado de Madurez DS10

DS12 ADMINISTRACIÓN DE INSTALACIONES	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tienen documentos que ayuden con la administración del ambiente físico, además que no se tienen estándares para la seguridad física, es así que se	

necesita mejorar en varios aspectos de la infraestructura.
Recomendaciones Finales
• Establecer políticas de seguridades físicas que puedan ayudar a mantener un mejor control sobre el hardware y la información. • Establecer una política para protección contra factores ambientales. • Crear políticas de seguridad en todos los equipos, para evitar daños, además de mantener salud y seguridad personal • Establecer políticas de prevención de incidentes externos • Creación de programas para protección contra eventos naturales.

Tabla 3.35 Tabla Grado de Madurez DS12

M1 MONITOREO DE LOS PROCESOS	**Grado de Madurez** Nivel 0
Conclusión Final	
No se tiene procesos de monitoreo formales, que permitan controlar y medir el desempeño de la unidad de TI.	
Recomendaciones Finales	
• Se recomienda que la empresa debe contar con reportes e informes útiles y oportunos para poder evaluar el desempeño de la misma. • Definir los indicadores de los reportes, para que estos puedan ser ubicados en los reportes y ser socializados con todo el personal. • Crear políticas de elaboración de reportes e informes para mantener un control constante.	

Tabla 3.36 Tabla Grado de Madurez M1

Como muestran los resultados el nivel de madurez de cada uno de los procesos evaluados se encuentran en nivel 1 o 0, lo cual es muy bajo, por tanto se deben realizar varios correctivos, crear planes y estructuras para poder definir claramente los objetivos que el hospital tenga para que los mismos sean alineados con los objetivos de la unidad de TI.

3.4. INFORME EJECUTIVO

El presente informe está enfocado a entregar los resultados de los procesos evaluados referentes a los cuatro dominios que plantea COBIT, que se basa en el nivel de madurez de cada uno de ellos, de la siguiente manera:

PO1 DEFINIR UN PLAN ESTRATÉGICO DE TI	**Grado de Madurez** Uno
PO2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN	**Grado de Madurez** Cero
PO3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA	**Grado de Madurez** Uno
PO4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE TI	**Grado de Madurez** Uno
PO6 COMUNICACIÓN DE LOS OBJETIVOS Y DE LAS ASPIRACIONES DE LA GERENCIA	**Grado de Madurez** Cero
PO9 EVALUACIÓN / ANALISIS DE RIESGOS	**Grado de Madurez** Cero
AI2 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN	**Grado de Madurez** Cero
AI3 ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA	**Grado de Madurez** Cero
AI4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS	**Grado de Madurez** Cero
AI5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS	**Grado de Madurez** Cero
DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	**Grado de Madurez** Uno
DS4 ASEGURAR EL SERVICIO CONTINUO	**Grado de Madurez** Uno
DS5 GARANTIZAR LA SEGURIDAD DE SISTEMAS	**Grado de Madurez** Cero
DS7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS	**Grado de Madurez** Cero
DS8 APOYO Y ASISTENCIA PARA LOS CLIENTES	**Grado de Madurez** Cero
DS10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES	**Grado de Madurez** Cero
DS12 ADMINISTRACIÓN DE INSTALACIONES	**Grado de Madurez** Cero
M1 MONITOREO DE LOS PROCESOS	**Grado de Madurez**

	Cero

Tabla 3.37: Tabla resumen de Grados de Madurez

Los indicadores que se tienen de los niveles de madurez son los siguientes

Cero	No se tiene controles ni procesos administrativos en lo absoluto
Uno	Se reconoce un proceso pero es desorganizado
Dos	Se tiene procesos levantados y se planea estrategias
Tres	Se crean documentos de los procesos
Cuatro	Se tiene control sobre los procesos y su forma de aplicación.
Cinco	Se tienen buenas prácticas, planes y estrategias, en donde se automatizan los procesos

Tabla 3.38: Tabla Grado de Madurez

Como muestra los resultados el nivel de madurez de cada uno de los procesos evaluados se encuentran en nivel 1 o 0, lo cual es muy bajo, por tanto se deben realizar varios correctivos, y crear planes y estructuras para poder definir claramente los objetivos que el hospital tenga para que los mismos sean alineados con los objetivos de la unidad de TI.

Dentro de la auditoria se tiene 7 aspectos a ser evaluados los cuales son: eficiencia, eficacia, confidencialidad, integridad, disponibilidad, cumplimiento, confiablidad. Los cuales son evaluados dependiendo del nivel de madurez que tenga cada proceso, y se pueden evaluar en base de las recomendaciones que se realizaron en cada uno de los procesos.

Esta auditoría se realiza con el afán de plantear mejoras, para que sean adoptadas por la dirección, con lo cual se beneficie todo el hospital.

CAPÍTULO 4:

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

- Esta auditoría podrá ayudar a determinar los procesos que la unidad de TI debe implementar, determinar la criticidad de los mismos y así tomar medidas correctivas que permitan mejorar el desempeño de la unidad y lograr como objetivo el buen funcionamiento del hospital a través del aseguramiento de la continuidad de los servicios.

- La metodología COBIT a través de su marco de referencia y guías de auditoría nos proporciono las herramientas necesarias para determinar la situación actual de los procesos de la unidad de TI del Hospital General “Enrique Garcés” y realizar recomendaciones a corto y largo plazo para tomar acciones correctivas, con lo cual la dirección de TI priorice los procesos y las estrategias para mejorar el desempeño de la unidad dentro del hospital.

- Los procesos evaluados en el área de TI del Hospital General “Enrique Garcés” obtuvieron como resultados un nivel de madurez entre 0 y 1, demostrando un bajo nivel de madurez general de la unidad. Se pudieron dar recomendaciones que mejorarán el desempeño de las actividades de la unidad y permitirán elevar el grado de madurez de estos procesos y el grado de madurez general.

- Esta auditoría tiene un nivel de complejidad medio-alto y se logró gracias a la apertura de la unidad de TI del hospital: entregándonos la información solicitada, autorizándonos a la realización de encuestas y entrevistas para la recolección de información, permitiéndonos el acceso a las distintas dependencias del hospital; la apertura del tutor de tesis: solventando dudas, proponiendo material de consulta y con revisiones periódicas de nuestro trabajo.

4.2. RECOMENDACIONES

- Se recomienda utilizar esta auditoría como una guía para realizar correcciones a los procesos de la unidad de TI de Hospital General “Enrique Garcés”.

- Se recomienda ubicar al área de TI del hospital a un nivel asesor que le permitan: participar en la toma de decisiones, brindar los servicios tecnológicos requeridos por el hospital y asesorar a los demás departamentos con lo referente a tecnología.

- Se recomienda a la dirección del Hospital General “Enrique Garcés” poner mayor énfasis en los procesos cuyos resultados arrojaron un nivel de madurez cero, utilizar las recomendaciones a corto y largo plazo planteadas para cada proceso y mantener controles periódicos que permitan la evaluación y monitoreo de los procesos de la unidad de TI para asegurar una mejora continua de la unidad.

- Se recomienda al departamento financiero asignar un presupuesto en coordinación con el director de la unidad de TI, acorde con las necesidades del área y del hospital.

Se recomienda mejorar la comunicación del área de TI con la parte administrativa para coordinar acciones de mejora en los servicios provistos al hospital.

4.3. BIBLIOGRAFÍA

1. HERNÁNDEZ, Enrique. “Auditoría Informática, Un Enfoque Metodológico”. CECSA. Primera Edición. México 1985.
2. PIATTINI, Mario. “Auditoría de Tecnologías y Sistemas de Información”. Ra-Ma.
3. Comité Directivo de COBIT e IT Governance Institute (2000), COBIT. “Directrices de Auditoría”. Tercera Edición, Illinois USA.
4. ECHENIQUE, García José Antonio. “Auditoría en Informática”, McGraw – Hill. España. 1990.
5. FERRRARI DOMENICO, Prentice Hall, Computer Systems Performance Evaluation.
6. INTOSAI, “Methodological recommendations for information systems audit”. http://www.intosaiitaudit.org/16th_ISCITA_lith.pdf. 16-12-2010.
7. ISACA, “Capacity management for more efficient IT”. http://www.baselinemag.com/c/a/IT-Management/Capacity-Management-For-More-Efficient-IT-605424/. 16-12-2010.
8. PIATINI, Mario. DEL PESO, Emilio. “Metodología de una Auditoría”. http:www.itson.mx/METODOLOGIA%20DE%20LA%20AUDITORIA%20INFORMATICA_PIATTINI%20Y%20DEL%20PESO.doc. 16-12-2010
9. JAMES, Hall. “Information System Auditing and Assurance”. http://www.swlearning.com/accounting/hall/ais_4e/study_notes/ch17.pdf. 16-12-2010
10. National State Auditors Association. “Management Planning Guide for Information Systems Security Auditing”. http://www.gao.gov/special.pubs/mgmtpln.pdf. 16-12-2010.

ANEXOS

ANEXO 1

Metodología COBIT, Objetivos de Control y Directrices

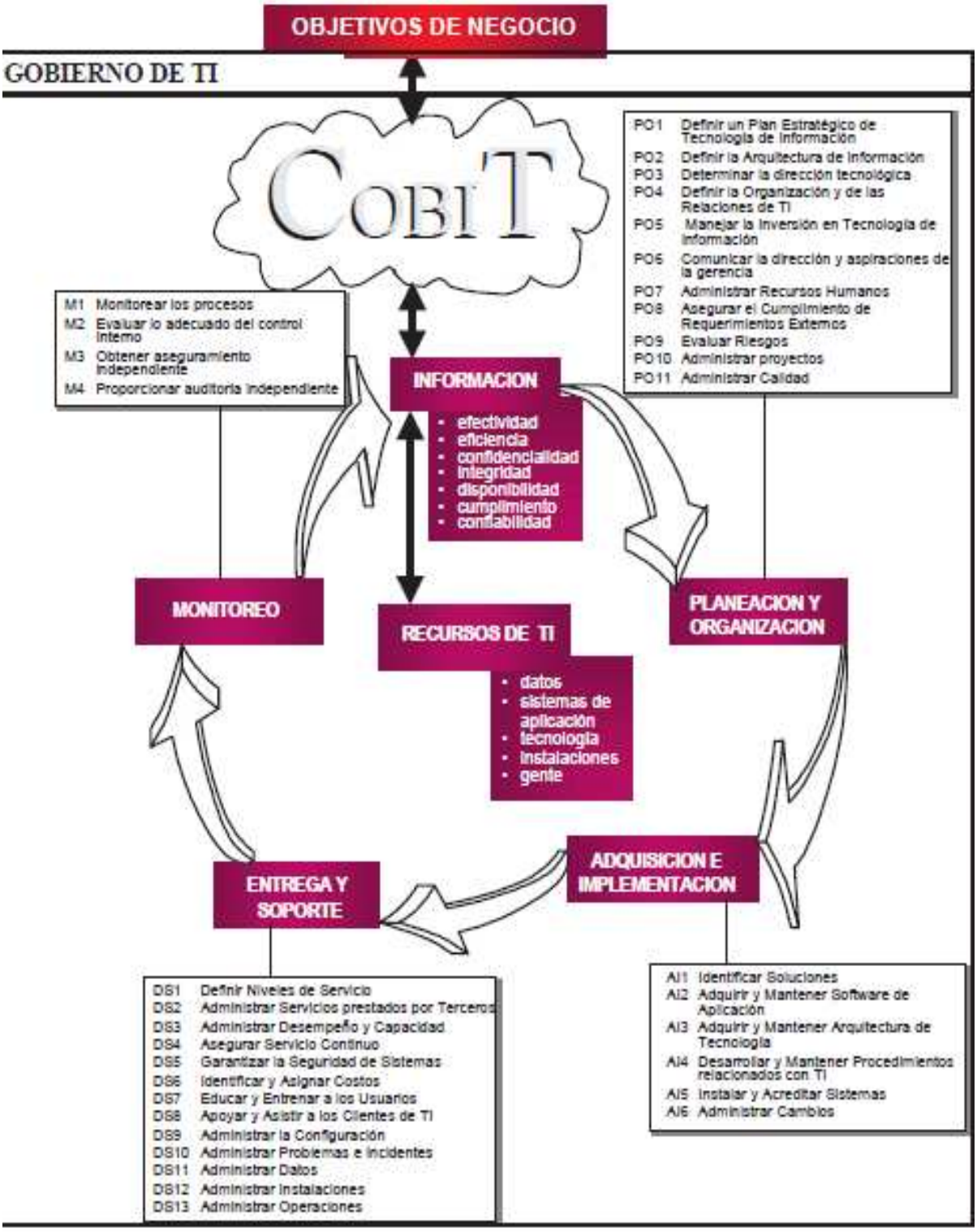
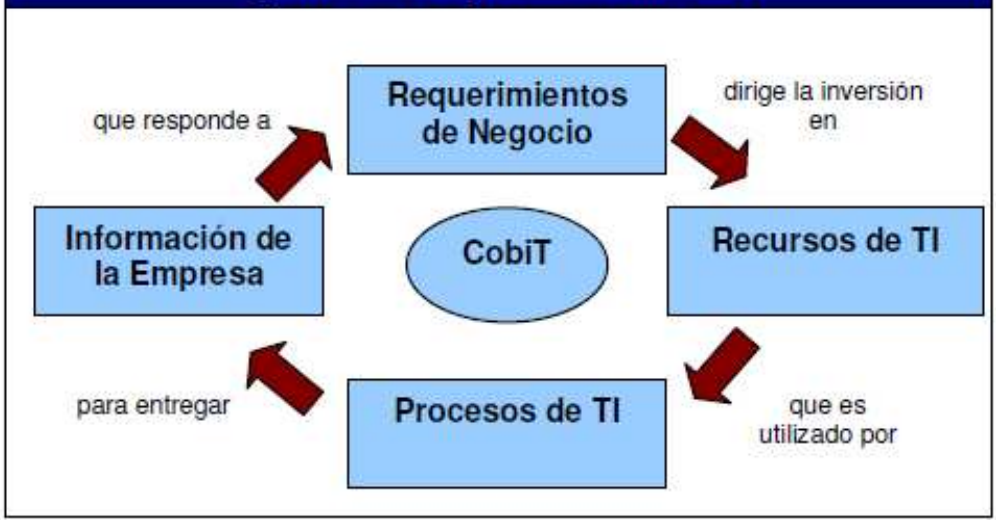

OBJETIVOS DE NEGOCIO
GOBIERNO DE TI
CobiT
PO1 Definir un Plan Estratégico de Tecnología de Información
PO2 Definir la Arquitectura de Información
PO3 Determinar la dirección tecnológica
PO4 Definir la Organización y de las Relaciones de TI
PO5 Manejar la Inversión en Tecnología de Información
PO6 Comunicar la dirección y aspiraciones de la gerencia
PO7 Administrar Recursos Humanos
PO8 Asegurar el Cumplimiento de Requerimientos Externos
PO9 Evaluar Riesgos
PO10 Administrar proyectos
PO11 Administrar Calidad
M1 Monitorear los procesos
M2 Evaluar lo adecuado del control interno
M3 Obtener aseguramiento independiente
M4 Proporcionar auditoría independiente
INFORMACION
efectividad
eficiencia
confidencialidad
integridad
disponibilidad
cumplimiento
confiabilidad
MONITOREO
RECURSOS DE TI
datos
sistemas de aplicación
tecnología
instalaciones
gente
PLANEACION Y ORGANIZACION
ADQUISICION E IMPLEMENTACION
ENTREGA Y SOPORTE
DS1 Definir Niveles de Servicio
DS2 Administrar Servicios prestados por Terceros
DS3 Administrar Desempeño y Capacidad
DS4 Asegurar Servicio Continuo
DS5 Garantizar la Seguridad de Sistemas
DS6 Identificar y Asignar Costos
DS7 Educar y Entrenar a los Usuarios
DS8 Apoyar y Asistir a los Clientes de TI
DS9 Administrar la Configuración
DS10 Administrar Problemas e Incidentes
DS11 Administrar Datos
DS12 Administrar Instalaciones
DS13 Administrar Operaciones
AI1 Identificar Soluciones
AI2 Adquirir y Mantener Software de Aplicación
AI3 Adquirir y Mantener Arquitectura de Tecnología
AI4 Desarrollar y Mantener Procedimientos relacionados con TI
AI5 Instalar y Acreditar Sistemas
AI6 Administrar Cambios

Figura 5 – Principio Básico de COBIT



La siguiente tabla proporciona un resumen de los dominios y procesos de COBIT, además de cómo están evaluados, y sobretodo no ayudará a conocer cuáles son los procesos aplicables a nuestra auditoria.

Dominio	Proceso	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimento	Confiabilidad	Aplicaciones	Información	Instalaciones	Personas
Planeación y Organización												
PO1	Definir un plan estratégico de TI	P	S	-	-	-	-	-	√	√	√	√
PO2	Definir la arquitectura de la información	S	P	S	P	-	-	-	√	√		
PO3	Determinar la dirección tecnológica	P	P	-	-	-	-	-	√		√	
PO4	Definir los procesos, organización y relaciones de la TI	P	P	-	-	-	-	-				√
PO6	Comunicar las	P	P	-	-	-	-	S		√		√

	aspiraciones de la dirección de la gerencia											
PO9	Evaluar y administrar los riesgos de TI	P	-	-	-	-	-	S	√	√	√	√

Adquirir e Implementar.

AI2	Adquirir y mantener software aplicativo	P	P		S			S	√			
AI3	Adquirir y mantener infraestructura tecnológica	S	P		S	S					√	
AI4	Facilitar la operación y el uso	P	P	S	S	S	S	S	√		√	√
AI5	Adquirir recurso de TI	S	P				S		√	√	√	√
AI7	Instalar y acreditar soluciones y	P	S		S	S			√	√	√	√

	cambios											

Entregar y dar Soporte.

DS1	Definir y administrar los niveles de servicio	P	P	S	S	S	S	S	√	√	√	√
DS4	Garantizar la continuidad del servicio	P	S			P			√	√	√	√
DS5	Garantizar la seguridad de los sistemas			P	P	S	S	S	√	√	√	√
DS7	Educar y entrenar a los usuarios	P	S									√
DS8	Administrar la mesa de servicio y los incidentes	P	P						√			√
DS10	Administrar los problemas	P	P			S			√	√	√	√
DS12	Administrar el ambiente				P	P					√	

	físico											

Monitorear y Evaluar.

ME1	Monitorear y Evaluar el Desempeño de TI	P	P	S	S	S	S	√	√	√	√
ME4	Proporcionar Gobierno de TI	P	P	S	S	S	S	√	√	√	√

ANEXO 2

Encuesta realizada a empleados de la unidad de TI, como a usuarios claves en el Hospital “Enrique Garcés”

Preguntas de la encuesta y entrevista.

1. ¿Existe dentro de la empresa un área de informática?
2. ¿Se ha nombrado un gerente para esta área?
3. ¿Está identificada dicha área dentro del organigrama general de la empresa?
4. ¿Se tiene un organigrama específico de dicha área?
5. ¿Existe un manual de organización y funciones aplicables a dicha área y el personal lo conoce?
6. ¿Están delimitadas las funciones de cada integrante del área de informática?
7. ¿Cada empleado del área de informática conoce la persona ante la que tiene que rendir cuentas de su labor?
8. ¿Los gerentes y otros funcionarios de nivel superior pueden dar órdenes directas a cualquier empleado del área de informática?
9. ¿Cada empleado del área de informática es especialista en aspectos distintos de programación?
10. ASPECTOS RELACIONADOS AL HARDWARE
11. ¿En alguna ocasión se ha extraviado algún periférico (bocinas, audífonos, teclado, mouse, teclado numérico, etc.) de una computadora?
12. Si hay vigilante, ¿Revisa éste que los empleados no lleven artículos que no son de su propiedad?
13. ¿En alguna ocasión le han quemado discos o guardada información en los equipos de la entidad?
14. ¿Cada componente de su computadora y periféricos tiene la numeración respectiva del inventario?

ASPECTOS RELACIONADOS AL SOFTWARE

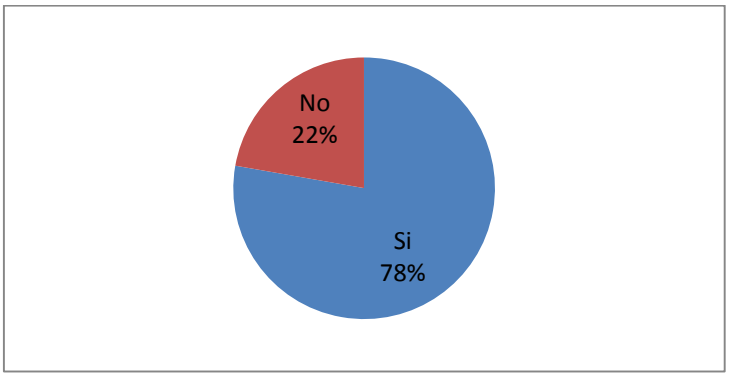
15. ¿Se utilizan programas como el Office de Microsoft u otros programas para los que la empresa haya comprado las licencias correspondientes?
16. ¿Los empleados pueden utilizar el equipo informático de la entidad para elaborar documentos o diseños para uso personal?
17. ¿Hay una persona nombrada como responsable de resguardar el software comprado por la empresa?
18. ¿Para el resguardo de los diversos discos de programas, se tiene un archivadero adecuado?
19. ¿El software comprado por la entidad le facilita su trabajo?
20. ¿Los programas antes mencionados son justo lo que necesita para sus actividades laborales?
21. ¿Existen programas diseñados y elaborados por el área de informática, con los procedimientos específicos para las actividades que la entidad desarrolla?

22. ¿Los programas fueron creados bajo estricta normas de seguridad para evitar que puedan ser revendidos a otras empresas que se dediquen a la misma actividad económica?
23. ¿Los diversos software se guardan en un lugar libre de humedad o con calor excesivo?
24. ¿Las capacitaciones recibidas, a que aspectos han sido enfocadas?_____
25. ¿Se ha capacitado en su momento a los usuarios de los sistemas informáticos?
26. ASPECTOS RELACIONADOS A LA SEGURIDAD
27. ¿Considera usted que hay demasiada humedad o excesivo calor, lo cual pueda deteriorar los computadores?
28. ¿Le han dado clave para ingresar al sistema?
29. ¿La clave que ha recibido le da acceso a documentos y archivos con base en la autoridad que tiene dentro de la empresa?
30. ¿Alguna vez su equipo no ha funcionado y al verificar algún accesorio ha estado desconectado?
31. ¿El acceso a Internet es para todos los empleados?
32. ¿Alguna vez al insertar su contraseña el sistema le ha dado mensaje de error y aun cuando lo escribe correctamente, el mensaje se ha repetido?
33. ¿Existe un plan estratégico informático
34. ¿Se realiza un presupuesto y se lo asigna a la unidad informática
35. ¿Con que tipo de seguridades físicas y lógicas cuenta la información de la empresa
36. ¿Existe capacitación de los usuarios de los sistemas informáticos
37. ¿Hay mantenimiento de software y hardware
38. ¿Qué piensa del funcionamiento de los sistemas informáticos
39. ¿Existe planes de contingencia para el área informática
40. ¿Cuáles son las políticas del departamento de tecnología y como se las comunica a los demás departamentos
41. ¿Cuáles son los riesgos que han identificado y como se los mitiga
42. ¿Cómo se realiza la adquisición de la infraestructura tecnológica?
43. ¿Cómo se garantiza la continuidad de los servicios y existen planes de mitigación?
44. ¿La computadora que utiliza funciona?
45. ¿Para enviar sus documentos a los otros empleados de la empresa lo hace mediante?
46. ¿Cuánto tiempo ha perdido en el último año por fallas de hardware?
47. ¿Qué actividades tiene permitidas en su oficina?
48. ¿Cuántas veces ha recibido su computadora un mantenimiento preventivo?
49. ¿Puede recuperar sus datos si por alguna falla se borran?
50. ¿La red está siempre disponible?
51. ¿Existe soporte técnico en la empresa?

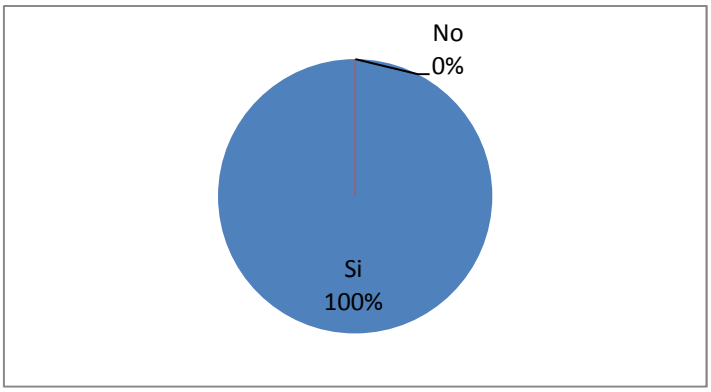
52. ¿Cuándo usted requiere un cambio de los sistemas computacional sigue un procedimiento definido?

GRAFICAS DE LAS PREGUNTAS CUANTIFICABLES DE LA ENCUESTA

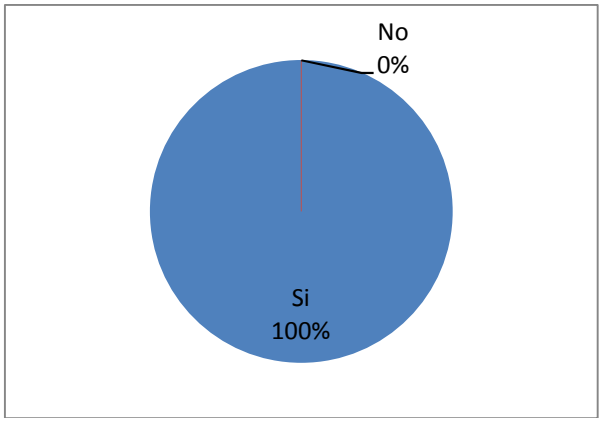
Si hay vigilante, ¿Revisa éste que los empleados no lleven artículos que no son de su propiedad?



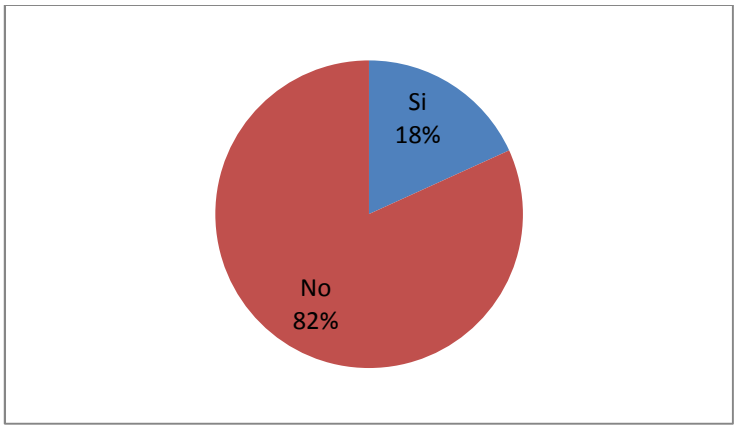
¿En alguna ocasión le han quemado discos o guardada información en los equipos de la entidad?



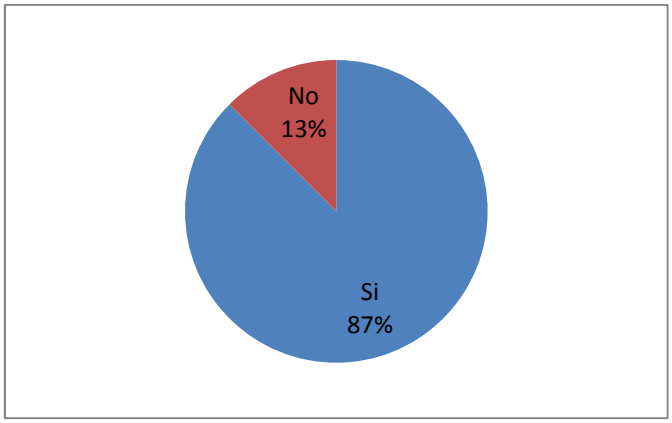
¿Cada componente de su computadora y periféricos tiene la numeración respectiva del inventario?



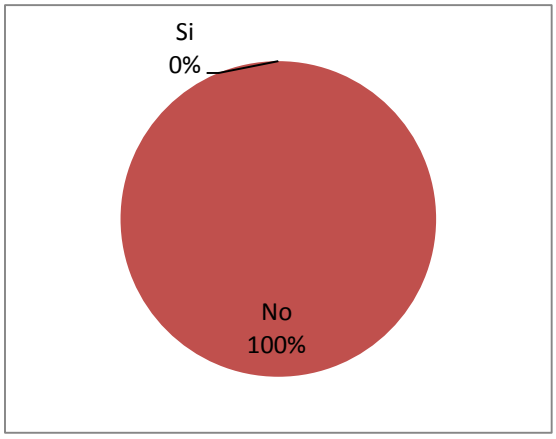
¿Los programas fueron creados bajo estricta normas de seguridad para evitar que puedan ser revendidos a otras empresas que se dediquen a la misma actividad económica?



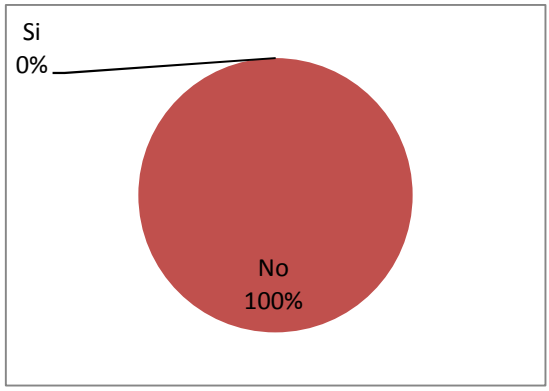
¿Se utilizan programas como el Office de Microsoft u otros programas para los que la empresa haya comprado las licencias correspondientes?



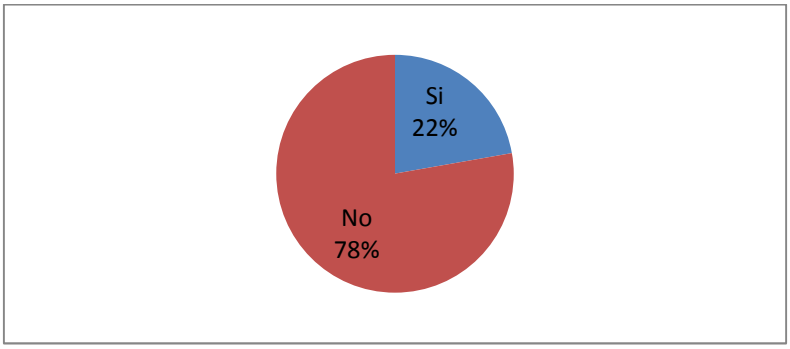
¿Los empleados pueden utilizar el equipo informático de la entidad para elaborar documentos o diseños para uso personal?



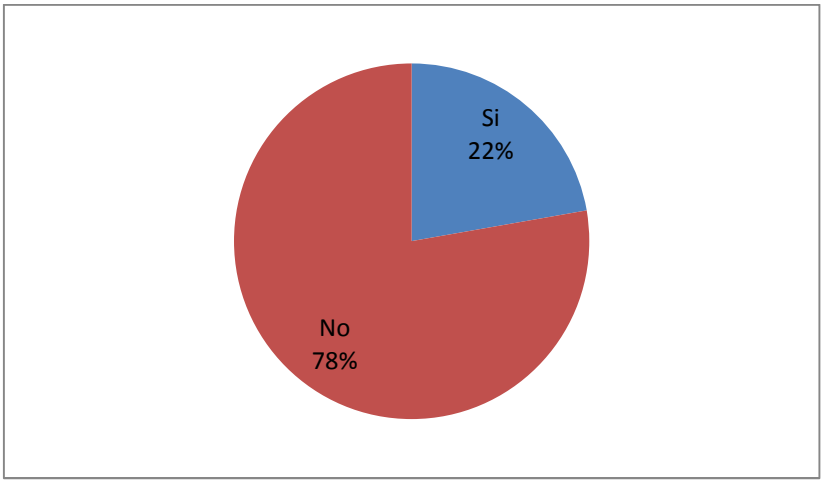
¿Para el resguardo de los diversos discos de programas, se tiene un archivadero adecuado?



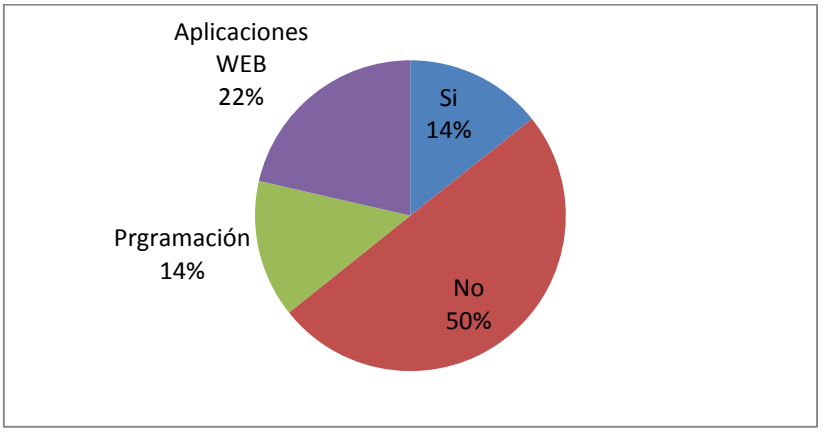
¿El software comprado por la entidad le facilita su trabajo?



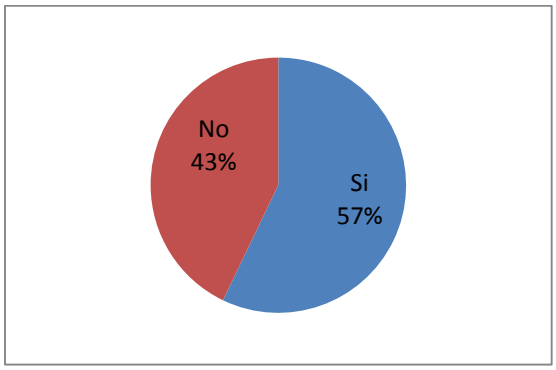
¿Los diversos software se guardan en un lugar libre de humedad o con calor excesivo?



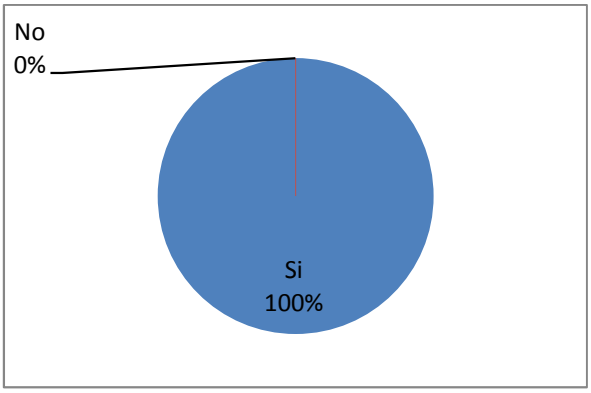
¿Las capacitaciones recibidas, a que aspectos han sido enfocadas?



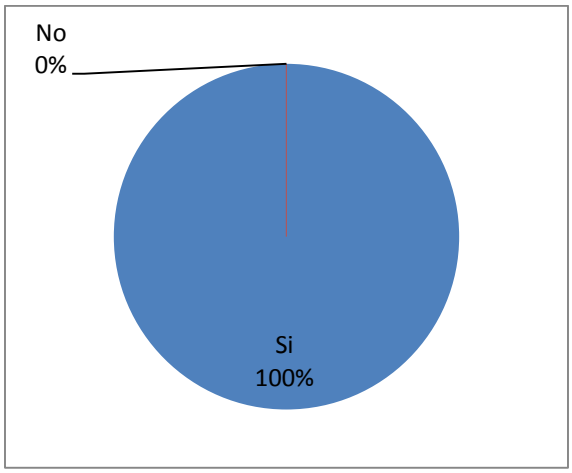
¿Se ha capacitado en su momento a los usuarios de los sistemas informáticos?



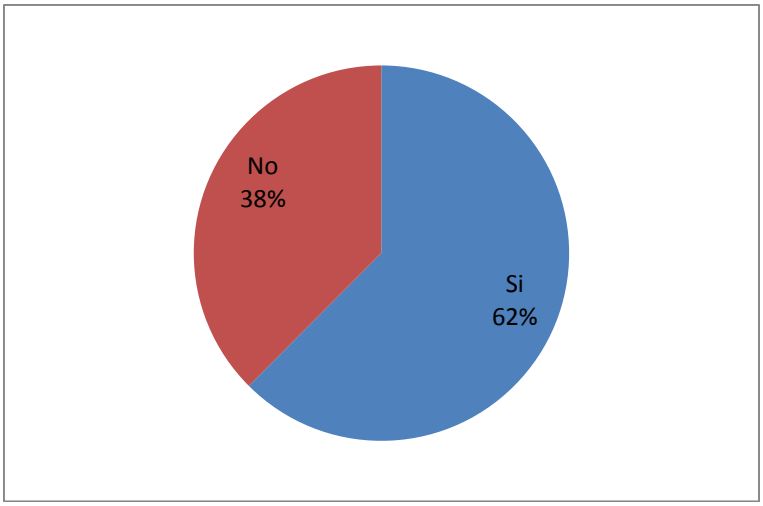
¿Le han dado clave para ingresar al sistema?



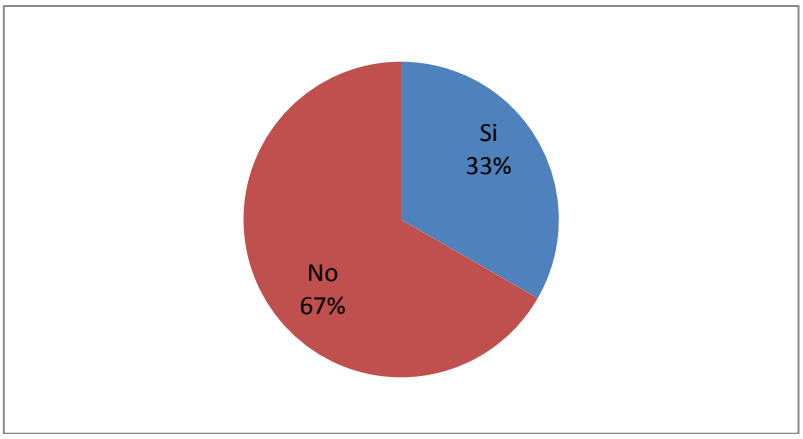
¿La clave que ha recibido le da acceso a documentos y archivos con base en la autoridad que tiene dentro de la empresa?



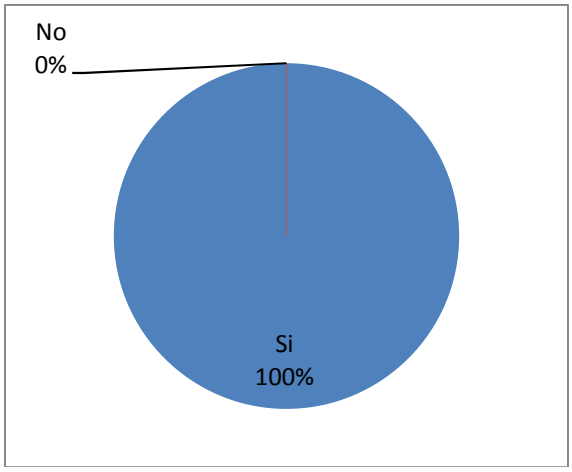
¿El acceso a Internet es para todos los empleados?



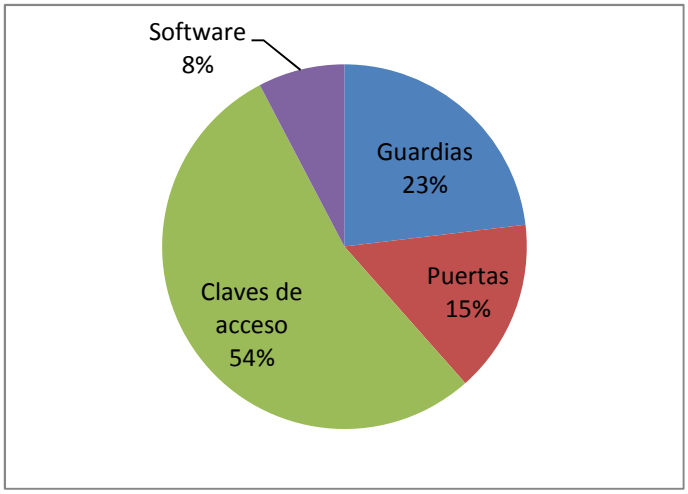
¿Existe un plan estratégico informático?



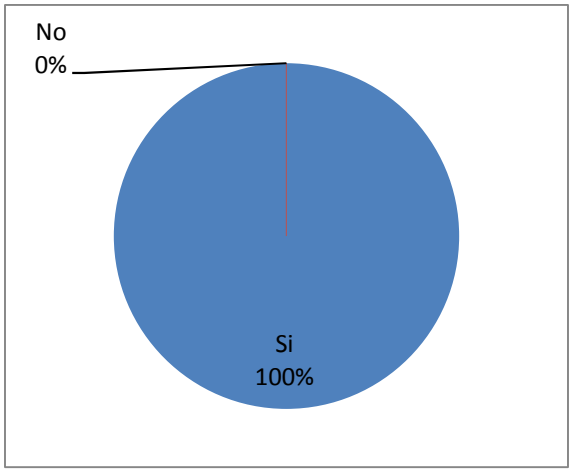
¿Se realiza un presupuesto y se lo asigna a la unidad informática?



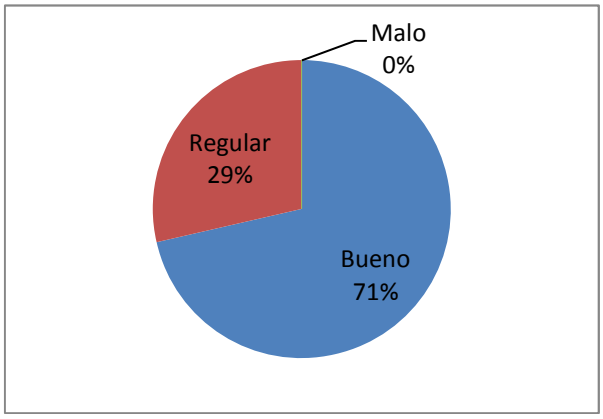
¿Con que tipo de seguridades físicas y lógicas cuenta la información de la empresa?



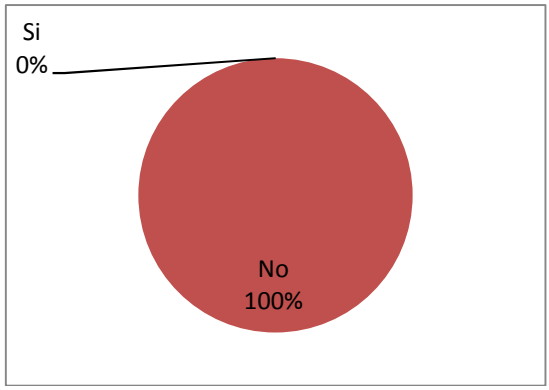
¿Hay mantenimiento de software y hardware?



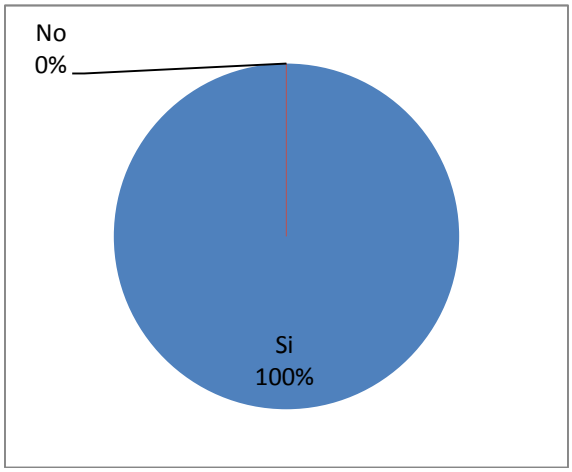
¿Qué piensa del funcionamiento de los sistemas informáticos?



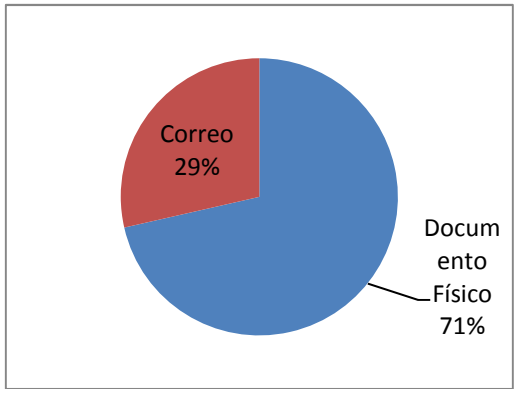
¿Existe planes de contingencia para el área informática?



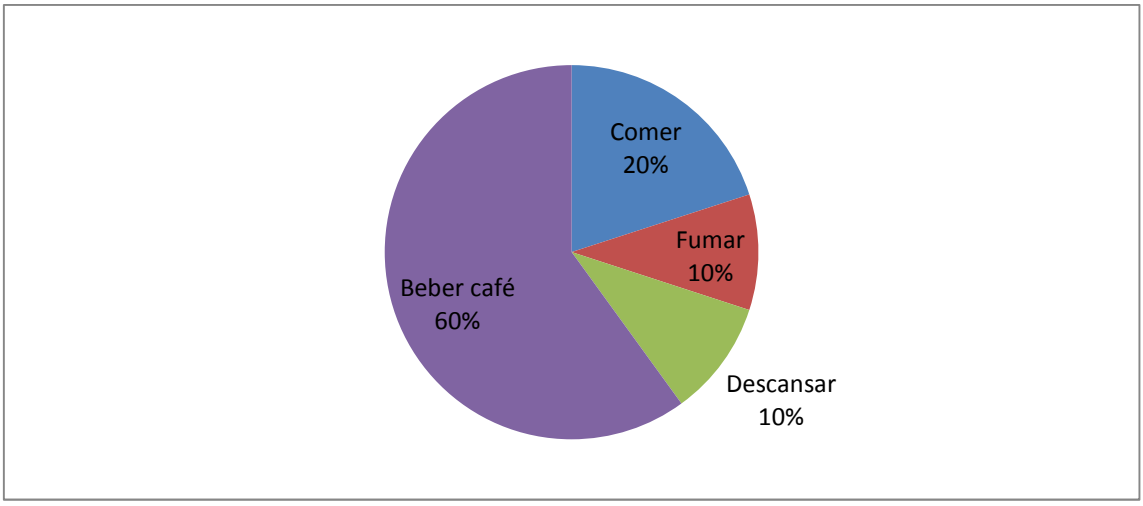
¿La computadora que utiliza funciona?



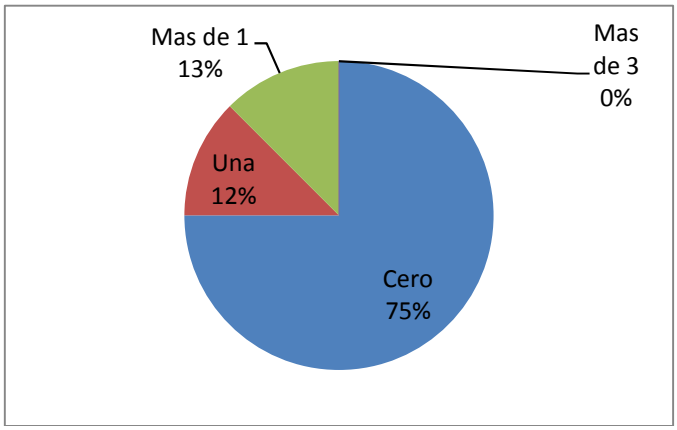
¿Para enviar sus documentos a los otros empleados de la empresa lo hace mediante?



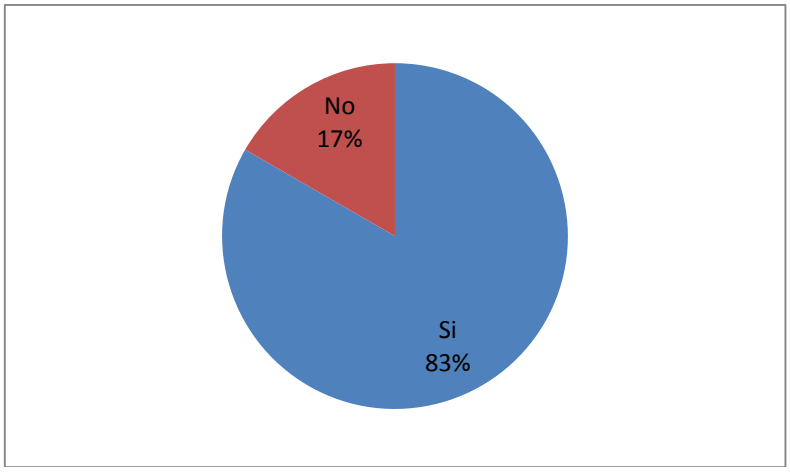
¿Qué actividades tiene permitidas en su oficina?



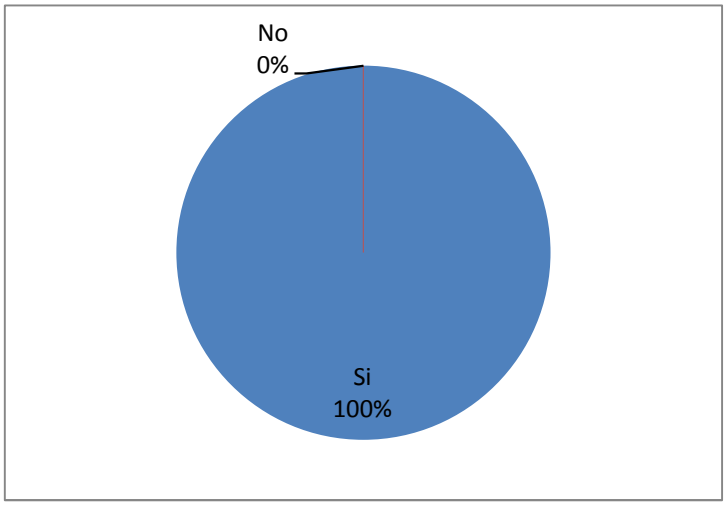
¿Cuántas veces ha recibido su computadora un mantenimiento preventivo?



¿La red está siempre disponible?



¿Existe soporte técnico en la empresa?



ANEXO 3

Información del Hospital “Enrique Garcés”

Orgánico Funcional del Hospital “Enrique Garcés”

ORGANICO FUNCIONAL HEG

a) PROCESOS GOBERNANTES
a.1.).- Gestión estratégica Hospitalaria – Dirección del Hospital
a.2.).- Gestión técnica Hospitalaria – Subdirección Médica

b) PROCESOS HABILITANTES DE ASESORIA
b.1).- Consejo Técnico
b.2).- Asesoría Jurídica
b.3).- Calificación de la oferta y la demanda
b.4).- Comité de Participación Social
b.5).- Comunicación Social
b.6).- Comité de Historia Clínica

b.7).- Comité de Farmacología

b.8).- Comité de Auditoría Médica

b.9).- Comité de Enfermedades Nosocomiales

b.10). Comité de Contrataciones pública

b.11).- Comité de Docencia e Investigación

b.12).- Comité de Muerte Materna

b.13).- Comité Operativo de Emergencia
b.14).- Comité de SOAT

b.15).- Comité de Bioética

b.16).- Comité de Higiene y Seguridad del Trabajo

b.16.1) Subcomité de Desechos Hospitalarios

PROCESOS HABILITANTES DE APOYO

GESTION DE DESARROLLO ORGANIZACIONAL
c.1).- Gestión de Recursos Humanos

c.2).- Gestión de Desarrollo Organizacional
c.2.1).- Gestión financiera
c.2.1.1).- Presupuesto y Contabilidad
c.2.1.2).- Administración de caja
c.2.2).- Gestión de Servicios Institucionales
c.2.2.1).- Servicios generales
c.2.2.1.1.-) Limpieza
c.2.2.1.2.-) Información y Central Telefónica
c.2.2.1.3.-) Seguridad y Transporte
c.2.2.2).- Mantenimiento
c.2.2.1.2.-) Almacén Central y Proveeduría

c.2.2.1.3.-) Gestión informática
c.2.2.1.4.-) Gestión SOAT
c.2.2.1.5.-) Gestión de Comunicación

2.3).- Hotelería

PROCESOS QUE OTORGAN VALOR AGREGRADO
d.1).- Servicios de apoyo
d.1.1).- Servicios auxiliares del diagnóstico
d.1.1.1).- Imagenología
d.1.1.2).- Laboratorio clínico
d.1.1.3).- Laboratorio de patología
d.1.1.4).- Endoscopía (digestiva, bronquial, laparoscopía)
d.1.1.5).- Electro diagnóstico (electrocardiografía, Electroencefalografía)
d.1.2).- Servicios auxiliares del tratamiento
d.1.2.1).- Unidad de cuidados intensivos
d.1.2.2).- Centro Quirúrgico
d.1.2.3).- Centro Obstétrico
d.1.2.4).- Rehabilitación y fisioterapia
d.1.2.5).- Farmacia
d.1.2.6).- Estomatología
d.1.3).- Gestión de enfermería en los servicios de:
d.1.3.1).- Consulta Externa
d.1.3.2).- Emergencia
d.1.3.3).- Hospitalización
d.1.3.4).- Centro Obstétrico
d.1.3.5).- Neonatología
d.1.3.6).- Quirófanos
d.1.3.7).- Central de esterilización
d.1.3.8).- Cuidados Intensivos
d.1.3.9).- Endoscopía, Electrocardiografía y electrocencefalografía
d.1.3.10).- Dispensario Anexo al IESS
d.1.4).- Trabajo Social
d.1.5).- Estadística y archivos clínicos
d.2).- Nutrición y dietética
d.3).- Aseguramiento de la calidad
d.3.1).- Garantía de la calidad
d.3.2).- Control y mejoramiento de procesos
d.3.3).- Salud Ocupacional

a).- Servicios Médicos de todas las especialidades ejecutados en:
a.1).- Consulta externa
a.1.1).- Todas las especialidades de atención
a.1.2).- Inmunizaciones
a.1.3).- Curaciones
a.2).- Hospitalización
a.2.1).- Medicina Interna
a.2.2).- Cirugía
a.2.3).- Pediatría
a.2.4).- Ginecología y Obstetricia
a.3).- Emergencia
a.3.1).- Especialidades Médicas (Pediatría, Ginecología y Obstetricia, Medicina Interna, Cirugía)
a.3.2).- Observación

b).- Servicios de Apoyo
b.1).- Gestión de enfermería en los servicios de:
b.1.1).- Consulta externa
b.1.2).- Hospitalización
b.1.3).- Emergencia
b.1.3).- Centro Obstétrico
b.1.4).- Neonatología
b.1.5).- Quirófanos
b.1.6).- Central de Esterilización
b.1.7).- Cuidados Intensivos
b.1.8).- Lavandería y ropería
b.1.9).- Endoscopía, Electrocardiografía y Electroencefalografía
b.1.10).- Dispensario Anexo del IESS
b.2).- Apoyo al Diagnóstico
b.2.1).- Imagenología
b.2.2).- Laboratorio clínico
b.2.3).- Patología
b.2.4).- Endoscopía
b.2.5).- Electrocardiografía
b.2.6).- Electroencefalografía
b.3).- Apoyo al Tratamiento
b.3.1).- Unidad de cuidados intensivos
b.3.2).- Centro Quirúrgico
b.3.3).- Centro Obstétrico
b.3.4).- Rehabilitación
b.3.5).- Estomatología
b.3.6).- Anestesiología
b.3.7).- Neonatología
b.3.8).- Epidemiología
b.4).- Salud Ocupacional
b.5).- Trabajo Social
b.6).- Estadística y Archivos clínicos
c.- Aseguramiento de la calidad
c.1).- Garantía de la calidad
c.2).- Control y mejoramiento de procesos
c.3).- Fundación “Dr. Enrique Garcés”

Orgánico funcional de la unidad de TI

HOSPITAL ENRIQUE GARCÉS

GESTIÓN INFORMÁTICA

PROPUESTA:

ESTRUCTURA ORGANIZACIONAL
PLANEACIÓN DEL PERSONAL

Antecedentes:

El Departamento de Sistemas es la unidad encargada de gestionar el apoyo informático a las actividades del Hospital Enrique Garcés, mediante el diseño, coordinación, implementación y operación de las bases de datos institucionales y de la red institucional de computación, informática y central telefónica. Así mismo presta asesoramiento y apoyo a las diferentes unidades, servicios y departamentos del Hospital Enrique Garcés.

Desde su creación el Departamento de Sistema no cuenta con una estructura organizacional definida así como también con personal que soporte la gran demanda de usuarios, software, hardware e información existente en el hospital.

Considerando:

Que la informática y los sistemas de información constituyen factores críticos de éxito para alcanzar lo propuesto en los diferentes planes operativo y estratégicos del Hospital Enrique Garcés, en su camino de alcanzar las mentas planteadas en la misma,

Se propone:

La creación el Orgánico Estructural del Departamento de Sistemas tomando en cuenta las siguientes áreas que conformarán el mismo detalladas a continuación:

ÁREAS

Dentro del Hospital Enrique Garcés, el Departamento de Sistemas cumple diversas funciones que justificarán los puestos de trabajo establecidos, los cuáles se engloban a través de los siguientes:

- Explotación de sistemas o aplicaciones. La explotación u operación de un sistema informático o aplicación informática, utilización y aprovechamiento de los sistemas implementados y a desarrollarse. Previsión de fechas de realización de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema, supervisión de trabajos, etc.

- Soporte técnico a usuarios. El soporte, tanto para los usuarios como para el propio departamento, se ocupa de seleccionar, instalar y mantener el sistema operativo adecuado del diseño y control de la estructura de la base de datos, la gestión de los equipos de la red de datos y de voz, el estudio y evaluación de las necesidades y rendimientos del sistema y, por último, la ayuda directa a usuarios.

- Gestión y Administración del propio centro de procesamiento de datos. Las funciones de gestión y administración de un centro de procesamiento de datos engloban operaciones de supervisión, planificación y control de proyectos, seguridad de las instalaciones y equipos, gestión de manejos de cuentas de usuario y gestión de los propios recursos tecnológicos y humanos.

AREAS QUE CONFORMAN EL DEPARTAMENTO DE SISTEMAS

ÁREA DE DIRECCION Y ADMINISTRACION

Este es el encargado de administrar los suplementos del software, así como el responsable de monitorear cada área del departamento de sistemas, los requerimientos que para su buen desempeño sean necesarios, área encargada de organizar todas las funciones de las áreas del departamento. Sus funciones son:

- Proponer su Plan Operativo, Presupuesto y demás documentos de gestión administrativa;
- Elaborar el Plan Informático de la Institución, Plan de Contingencias y demás instrumentos que garanticen el desarrollo informático institucional en función de la orientación estratégica institucional;
- Apoyar y propiciar la modernización institucional mediante el uso y aplicación racional de las tecnologías de información vigentes;
- Desarrollar acciones para la optimización continua de los procesos y procedimientos de la Institución;
- Elaborar normas, procedimientos y demás instrumentos de normativa institucional interna, verificando y evaluando su aplicación y actualización sistemática;
- Editar, concordar, actualizar y difundir los documentos de gestión institucional a fin de garantizar su coherencia, armonía y formalidad;
- Planear, investigar y determinar, en coordinación con las áreas usuarias, los requerimientos de sistematización y tecnología informática, así como la asignación de recursos informáticos;
- Analizar, diseñar, desarrollar e implementar las aplicaciones computarizadas correspondientes a los diferentes aspectos de la gestión administrativa y operativa del Hospital Enrique Garcés;
- Supervisar el desarrollo e implementación de proyectos informáticos que sean encargados a terceros;
- Administrar las redes locales y/o remotas, así como las diferentes bases de datos de la Institución;
- Evaluar periódicamente la eficiencia del software y hardware para determinar la factibilidad de aplicación de nuevas tecnologías;
- Proporcionar información para el Programa de Capacitación del Personal en materia de su competencia;

ÁREA DE OPERACIÓN

Esta área se encarga de brindar los servicios requeridos para el proceso de datos, como son:

- Preparar los datos y suministros necesarios para el departamento de sistemas.
- Manejo de archivo y documentación de las diferentes áreas.
- Preparación de documentos del departamento y sus áreas.
- Manejo equipos periféricos como impresoras, scanner, etc.
- Dar soporte a los usuarios que tengan problemas mínimos en sus equipos.
- Documentar las actividades diarias.
- Coordinación y comunicación entre el Área de Dirección y las demás áreas que conforman el Departamento de Sistemas.
- Los suministros empleados y cualquier condición anormal que se presente.
- Brindar apoyo a la realización de documento como Word, Excel y Power Point.
- Control de La Central Telefónica:

✓ Funcionamiento de las líneas externas e internas,
✓ Control de acceso a las líneas externas,
✓ Control de acceso con claves de usuarios,
✓ Control del Servicio Telefónico en caso de daños en comunicaciones entre extensiones.
✓ Reportes o avisos de daños graves de La Central Telefónica al Técnico de ALCATEL.
✓ Reportes de llamadas de las líneas externas.

- Digitalización de reglamentos, manuales, informes técnicos y documentos administrativos.
- Las demás que le asigne el Área de Dirección y Administración.

ÁREA DE ANALISIS E IMPLEMENTACION

Esta área tiene la tarea de establecer un flujo de información eficiente a través de toda la institución con la realización de análisis de requerimientos informáticos tecnológicos mediante la utilización del tiempo suficiente para el estudio y la proposición de soluciones de los problemas planteando diferentes alternativas y el control de calidad de las mismas.

Las funciones de esta área son:

- Planear, investigar y determinar, en coordinación con las áreas, los requerimientos de sistematización y tecnología informática, así como la asignación de recursos informáticos.
- Planificar, analizar, diseñar, desarrollar e implementar las aplicaciones computarizadas requeridas para facilitar la gestión administrativa y operativa de la Institución en coordinación con el área de desarrollo.
- Realizar el mantenimiento de las aplicaciones que sean desarrolladas en la Institución.
- Mantener actualizada la documentación de las aplicaciones que sean desarrolladas en la Institución.
- Desarrollar y actualizar periódicamente el modelo de datos lógico y físico de toda la Institución.
- Modelar y proponer el diseño de los procesos de la Institución a fin de normar, estandarizar y facilitar la informatización de dichos procesos.
- Definir la estrategia de implementación de los cambios o rediseños de los procesos que se vean afectados por la incorporación de tecnologías de información.
- Desarrollar y actualizar el modelo conceptual de datos de la Institución.
- Elaborar normas, procedimientos y demás instrumentos de normativa institucional interna, verificando y evaluando su aplicación y actualización sistemática.
- Editar, concordar, actualizar y difundir los documentos de gestión institucional interna, a fin de garantizar su coherencia, armonía y formalidad.
- Mantener actualizada la documentación de los procesos de la Institución.
- Mantener informado al área de Dirección y Administración de los avances, atrasos y problemas que se presentan rutinariamente.
- Elaborar los términos de referencia y los criterios de evaluación técnica para el desarrollo de proyectos de sistemas que sean encargados a terceros.
- Supervisar el desarrollo e implementación de proyectos informáticos que sean encargados a terceros.
- Definir la metodología y estándares de desarrollo de las aplicaciones para la Institución.

- Apoyar al Área de Dirección y Administración en la elaboración del Planeamiento Estratégico Informático y en la elaboración del Plan de Contingencias.
- Capacitar al personal usuario en la utilización de los nuevos sistemas desarrollados en la Institución.
- Participar en la formulación del Plan Operativo Anual del Departamento de sistemas.
- Solicitar apoyo al área de Operación.
- Las demás que le asigne el Área de Dirección y Administración.

AREA DE DESARROLLO

Esta área se encarga del desarrollo de sistemas en la institución y la implementación de los mismos en coordinación con el área de Análisis, además se encargará del monitoreo continuo de los sistemas instalados en la institución, sus funciones son:

- Construir soluciones integrales (aplicaciones) a las necesidades de información de los usuarios.
- Usar las técnicas de construcción de sistemas de información orientadas netamente a la productividad del personal y a la satisfacción plena del usuario.
- Construir equipos de trabajo con la participación del usuario y del personal técnico de acuerdo a metodologías establecidas.
- Mantener informado al área de Dirección y Administración de los avances, atrasos y problemas que se presentan rutinariamente.
- Mantener programas de capacitación para el personal técnico y usuarios.
- Establecer un flujo de información eficiente a través de toda la organización.
- Realizar el estudio y la proposición de soluciones de problemas informáticos, plantación de diferentes alternativas.
- Elaboración de los programas que se ejecutan en las computadoras, modificar los existentes de ser necesario y vigilar que todos los procesos se ejecuten correctamente.

- Programar las especificaciones de los sistemas realizados por en el analistas y las transforman en programas eficientes y bien documentados para la institución.

- Coordinar con las áreas de sistemas y usuarios la implantación de las aplicaciones.
- Diseñar los planes de calidad de las aplicaciones y garantizar su cumplimiento.
- Validar los nuevos procedimientos y políticas a seguir por las implementaciones de los proyectos liberados.
- Probar los productos y servicios a implementar antes de ser liberados al usuario final.
- Elaborar conjuntamente con el área de Programación o Desarrollo, los planes de capacitación de los nuevos usuarios.
- Coordinar la presentación de las nuevas aplicaciones a los usuarios.
- Supervisar el cumplimiento de los sistemas con la normatividad establecida.
- Solicitar apoyo al área de Operación.
- Las demás que le asigne el Área de Dirección y Administración.

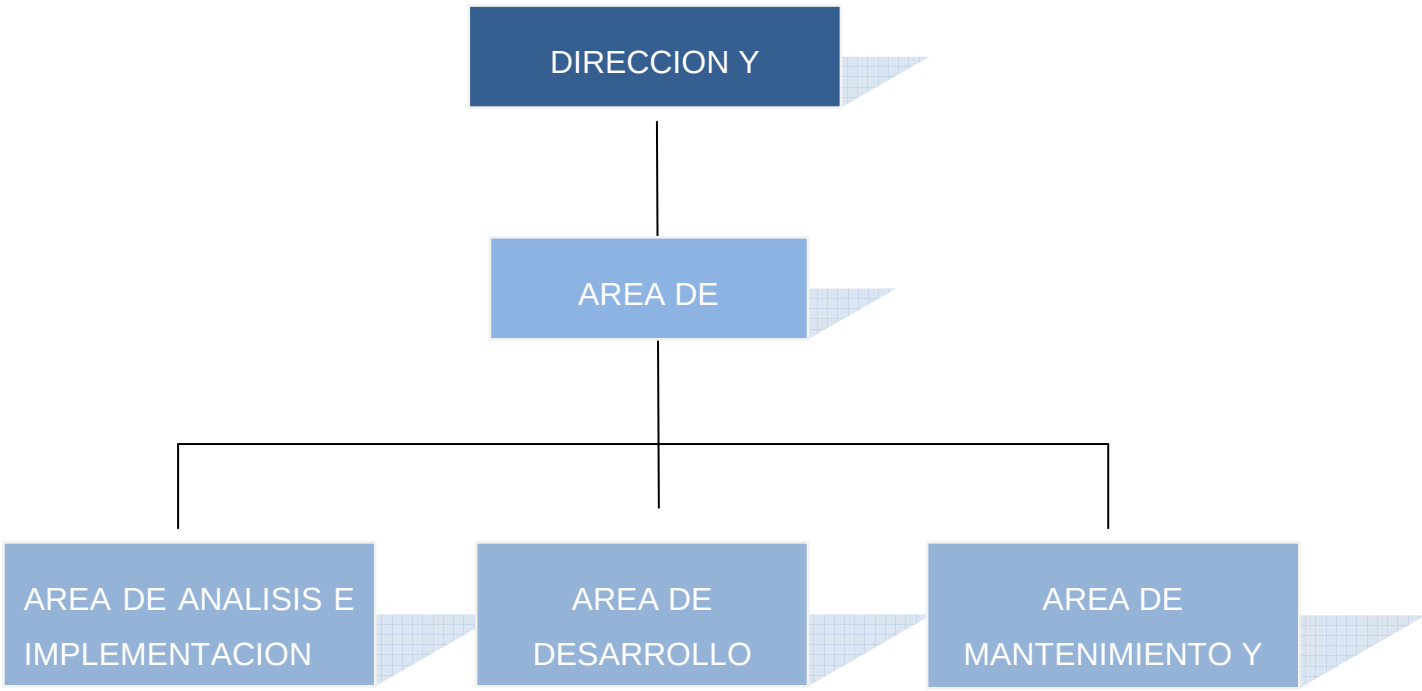
ÁREA DE MANTENIMIENTO Y SOPORTE TÉCNICO

Área responsable de la gestión del hardware y del software dentro de las instalaciones del Hospital Enrique Garcés, entendiendo por gestión: estrategia, planificación, instalación, backups (Respaldo de información) y mantenimiento. Algunas funciones principales generales que realiza esta área son:

- Planificar la modificación e instalación de nuevo software y hardware.
- Evaluar los nuevos paquetes de software y nuevos productos de hardware.
- Dar el soporte técnico necesario para el desarrollo de nuevos proyectos, evaluando el impacto de los nuevos proyectos en el sistema instalado.
- Asegurar la disponibilidad del sistema, y la coordinación necesaria para la resolución de los problemas técnicos en su área.
- Realizar la coordinación con los técnicos del proveedor con el fin de resolver los problemas técnicos y garantizar la instalación de los productos.
- Proponer las notas técnicas y recomendaciones para el uso óptimo de los sistemas instalados.
- Participar en el diseño de la Arquitectura de Sistemas.
- Realización, vigilancia y control de respaldos de los sistemas e información que posee el hospital periódicamente.
- Dirigir, evaluar y controlar el funcionamiento de los equipos de cómputo, servidores de aplicación, base de datos, web y comunicaciones, de la red de la Institución.

- Planificar, dirigir, controlar y ejecutar las actividades de instalación, mantenimiento y optimización de los sistemas operativos, del manejador de base de datos, del software de base y de las comunicaciones.
- Configurar, administrar y supervisar las redes locales y/o remotas, equipos periféricos, así como las diferentes bases de datos de la Institución.
- Elaborar periódicamente informes y estadísticas del sistema de red, software y hardware.
- Apoyar al área de Dirección y Administración de sistemas en la elaboración del Planeamiento Estratégico Informático y en la elaboración del Plan de Contingencias.
- Elaborar y ejecutar el plan de mantenimiento preventivo y correctivo de los equipos de cómputo de la Institución.
- Brindar y registrar el soporte técnico y ayuda en el puesto de trabajo a los usuarios de la Institución.
- Realizar periódicamente las copias de respaldo de los datos de la institución y del sistema.
- Programar, monitorear y controlar la Central Telefónica de la Institución con apoyo del área de operación.
- Administrar, organizar y operar todos los recursos del Centro de Cómputo y Comunicaciones de la Institución.
- Las demás que le asigne el Área de Dirección y Administración.

ORGANICO ESTRUCTURAL DEL DEPARTAMENTO DE SISTEMAS



Inventario proporcionado por la unidad de TI

CODIGO DE EQUIPO	HOST DE EQUIPO	IP EQUIPO	NUMERO DE PUNTO
P1_1	SERVGEN1	192.168.10.151	11
P1_10	emergencia2	192.168.10.85	6
P1_11	Estadistica_Em	192.168.10.185	
P1_12	emergencia1	192.168.10.84	8
P1_13	emergencia4	192.168.10.59	9
P1_14	tesoreria1	192.168.10.160	20
P1_15	tesoreria2	192.168.10.161	20
P1_16	recaudacion3	192.168.10.137	20
P1_17	enfermeria1	192.168.10.87	5
P1_18	paquetes1	192.168.10.181	7
P1_19	RRHH1	192.168.10.141	16
P1_2	ALIMENTACION1	192.168.10.67	17
P1_20	RRHH2	192.168.10.143	
P1_21	RRHH3	192.168.10.144	
P1_22	RRHH4	192.168.10.145	
P1_23	RRHH5	192.168.10.146	
P1_24	RRHH6	192.168.10.147	
P1_25	RRHH8	192.168.10.193	
P1_26	RRHH7	192.168.10.173	
P1_27	Sub_adm2	192.168.10.150	18
P1_28	COM_ADQ1	192.168.10.73	19
P1_29	Sub_adm1	192.168.10.156	19
P1_3	alimentacion3	192.168.10.68	
P1_30	financiero10	192.168.10.78	19

P1_31	financiero9	192.168.10.79	19
P1_32	Direccion_secre	192.168.10.130	21
P1_33	RgistroDir	192.168.10.148	21
P1_34	financiro11	192.168.10.169	24
P1_35	financiero	192.168.10.174	6
P1_36	financiro6	192.168.10.109	
P1_37	financiero7	192.168.10.110	24
P1_38	financiero-HP	192.168.10.233	
P1_39	financiero3	192.168.10.106	22
P1_4	alimentacion2	192.168.10.66	26
P1_40	financiero4	192.168.10.107	4
P1_41	financiero1	192.168.10.104	24
P1_42	financiero5	192.168.10.108	
P1_43	Comp_publ4	192.168.10.72	26
P1_44	financiero2	192.168.10.105	26
P1_45	Comp_pub2	192.168.10.136	26
P1_46	Comp_publ3	192.168.10.223	26
P1_47	Comp_publ1	192.168.10.135	26
P1_48	triaje_em	192.168.10.217	
P1_49			
P1_5	alimentacion	192.168.10.216	29
P1_50			
P1_51			
P1_6	Mirian-Pc	192.168.10.187	3
P1_7		192.168.10.224	3
P1_8	Planificacion2	192.168.10.134	3
P1_9	TRAB_SOC3	192.168.10.175	
P2-1	Tomografo	192.168.10.187	
P2-10	Con_ext1	192.168.10.77	
P2-11	Oftalmologia	192.168.10.196	25

P2-12	TRAB_SOC1	192.168.10.162	22
P2-13	TRAB_SOC2	192.168.10.163	22
P2-14	rehabilit_1	192.168.10.139	23
P2-15	rehabilit_2	192.168.10.140	8
P2-16	REHABILITACION5	192.168.10.141	
P2-17	Laboratorio3	192.168.10.11	6
P2-2	Sistemas45539B		
P2-3	Imagen1	192.168.10.143	2
P2-4	Imageneologia	192.168.10.27	
P2-5	Patologia	192.168.10.159	7
P2-6	lab secre		
P2-7	Catalina_1	192.168.10.124	
P2-8			
P2-9	Xtratech	192.168.10.184	
P3-1	neonatologia3	192.168.10.127	
P3-2	neo3	192.168.10.126	
P3-3	neonatologia1	192.168.10.125	
P3-4	ginecologia1	192.168.10.141	3
P3-5	cent_obst	192.168.10.175	
P4-1	gine4_1	192.168.10.198	
P4-2	anestesiologia2	192.168.10.140	3
P4-3	anestesiologia1	192.168.10.69	1
P5-1	Uci2	192.168.10.168	3
P5-2	Uci1	192.168.10.167	2
P6-1	Endoscopia1	192.168.10.170	
P6-2			
P6-3			
P6-4			
P6-5	Traumatologia	192.168.10.164	2
P6-6	Traumatologia2	192.168.10.165	

P7-1	MED_INT1	192.168.10.200	
P7-2	MED_INT2	192.168.10.204	
P7-3	MED_INT4	192.168.10.222	
P7-4	infectologia3	192.168.10.116	1
P7-5	Infectologia2	192.168.10.115	
P8-1	pediatria1	192.168.10.132	4
P8-2	pediatria2	192.168.10.111	
P8-3	docencia1	192.168.10.82	
P9-1	Salud Mental 1		
P9-2	S.Mental2	192.168.10.149	
PB-1	pchome	192.168.10.90	
PB-10	estadistica11.heg.gov.ec	192.168.10.91	24
PB-11	estadistica-p/4	192.168.10.202	26
PB-12	estadistica-v5.heg.gov.ec	192.168.10.203	27
PB-13	estadistica-t6	192.168.10.204	
PB-14	estadistica-t7	192.168.10.205	14
PB-15	estadistica-t8	192.168.10.89	
PB-16	estadistica-v6	192.168.10.99	
PB-17	estadistica-t10	192.168.10.100	
PB-18	estadistica-5.heg.gov.ec	192.168.10.26	
PB-19	user-pc	192.168.10.122	
PB-2	Mario Meneses	192.168.10.93	
PB-20			
PB-21	matenimiento3.heg.gov.ec	192.168.10.120	
PB-22	patrcio-pc	192.168.10.121	
PB-23	soat1.heg.gov.ec	192.168.10.155	
PB-24	financiero 8		
PB-25	soat4.heg.gov.ec	192.168.10.161	
PB-26	soat2.heg.gov.ec	192.168.10.221	
PB-27	soat3.heg.gov.ec	192.168.10.121	

PB-28	com-social2.heg.gov.ec	192.168.10.74	
PB-29	com-social1.heg.gov.ec	192.168.10.76	
PB-3	est-HEG	192.168.10.96	
PB-30	patologiat3.heg.gov.ec	192.168.10.191	4
PB-31	pchome	192.168.10.189	
PB-32	patologia1.heg.gov.ec	192.168.10.129	
PB-33	patologia.heg.gov.ec	192.168.10.180	
PB-34	patologia5.heg.gov.ec	192.168.10.195	
PB-35	patologia7.heg.gov.ec	192.168.10.128	
PB-36	sistemas	192.168.10.186	
PB-37	farmacia2.heg.gov.ec	192.168.10.102	
PB-38	farmacia3.heg.gov.ec	192.168.10.103	
PB-39	farmacia1.heg.gov.ec	192.168.10.101	
PB-4	estadistica4	192.168.10.95	
PB-40	farmaciav1.heg.gov.ec	192.168.10.58	
PB-41			
PB-42	farmaciav3.heg.gov.ec	192.168.10.57	
PB-43	farmaciav4.heg.gov.ec	192.168.10.60	
PB-44			
PB-45	almacen8.heg.gov.ec	192.168.10.157	
PB-46	almacen5.heg.gov.ec	192.168.10.63	
PB-47	almacen4.heg.gov.ec	192.168.10.64	
PB-48	almacen3.heg.gov.ec	192.168.10.65	17
PB-49	almacen2.heg.gov.ec	192.168.10.162	
PB-5	pchome	192.168.10.94	
PB-50	almacen1.heg.gov.ec	192.168.10.61	17
PB-51	lavanderiaheg.gov.ec	192.168.10.229	
PB-6	estadistica6.HEG.gov.ec	192.168.10.97	
PB-7	Irag-HEG	127.0.0.1	
PB-8	est_turnos3	192.168.10.55	

PB-9	heg-D9595E6A637	192.168.10.201	23
ZS-1	ClinicaSecre	192.168.101.201	
ZS-2	Infectologia1	192.168.101.202	
ZS-3	Clinica VIH	192.168.101.203	
ZS-4	sala_de_acogida		
ZS-5	pcchome_eec269f5	192.168.101.208	
ZS-6	com_des1	192.168.101.1	
ZS-7	Disp_IESS	192.168.101.209	
ZS-8	pcchome_9ecbbe18	192.168.101.210	