DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL
TÍTULO DE MAGÍSTER EN AUDITORÍA Y EVALUACIÓN DE SISTEMAS TECNOLÓGICOS

TEMA:
PLAN DE CONTINGENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DEL HOSPITAL IESS ZAMORA

AUTORA: ABAD CONDE, CESILIA

DIRECTOR: Msc. ING. DÍAZ RODRÍGUEZ, OSWALDO

SANGOLQUÍ

2015

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***PLAN DE CONTINGENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DEL HOSPITAL IESS ZAMORA***" realizado por la señorita ***Ing. CESILIA ABAD CONDE***, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a la señorita ***Ing. CESILIA ABAD CONDE*** para que lo sustente públicamente.

Sangolquí, 09 de diciembre del 2015

MSc.ING. OSWALDO DÍAZ RODRIGUEZ

DIRECTOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

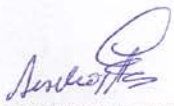
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

AUTORÍA DE RESPONSABILIDAD

Yo, ***CESILIA ABAD CONDE***, con cédula de identidad N° 1103850994, declaro que este trabajo de titulación ***"PLAN DE CONTINGENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DEL HOSPITAL IESS ZAMORA"*** ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 09 de diciembre del 2015



Ing. CESILIA ABAD CONDE

C.C. 1103850994

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

AUTORIZACIÓN

Yo, ***CESILIA ABAD CONDE***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación **"PLAN DE CONTINGENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DEL HOSPITAL IESS ZAMORA"** cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 09 de diciembre del 2015

Ing. CESILIA ABAD CONDE

C.C. 1103850994

DEDICATORIA

Dedico este trabajo a mis padres, Lauro Abad e Imelda Conde quienes con su mejor esfuerzo y ejemplo me dieron la oportunidad de una formación personal y profesional y ser quien soy, a Eduardo Rodríguez por ser la persona que Dios puso en mi camino para hacer mis sueños realidad.

Cesilia Abad Conde

AGRADECIMIENTO

Al Director de proyecto y tesis Ing. Oswaldo Rodríguez por sus conocimientos impartidos durante todo el desarrollo del presente trabajo.

Al Dr. Galo Vivanco y personal del hospital por las facilidades prestadas para la obtención de la información.

Al Ing. Mario Rom por brindarme sus conocimientos en beneficio de ésta maestría.

A Eduardo Rodríguez Paz por estar siempre a mi lado y compartir juntos la mejor etapa de nuestra vida.

Cesilia Abad Conde

ÍNDICE DE CONTENIDO

CAPÍTULO II

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El Instituto Ecuatoriano de Seguridad Social es una entidad, cuya organización se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia. Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del sistema nacional de Seguridad Social, teniendo como misión de proteger a la población urbana y rural, con relación de dependencia laboral o sin ella, contra las contingencias de enfermedad, maternidad, riesgos del trabajo, discapacidad, cesantía, invalidez, vejez y muerte, en los términos que consagra la Ley de Seguridad Social. En el 2007 el IESS implementó la Dirección de Desarrollo Institucional, con la finalidad de mejorar los procesos de TI mediante la aplicación de nuevos estándares para gestionar la seguridad de la información, como gestión de riesgos (serie ISO/IEC 27.000), y desarrollo de un modelo de madurez de la seguridad de la información tanto a nivel de usuarios internos, externos y en los servicios que presta el IESS en las Direcciones Provinciales, Hospitales y Unidades Medicas. Adicionalmente se implementa un sistema médico en todas las Unidades y Hospitales, dando origen a la creación de la Unidad de Tecnología en el Hospital IESS Zamora, adquieriendo nuevos equipos de comunicación, servidores, estaciones de trabajo y asignación de roles al personal del Área, bajo los estándares establecidos por la DNTI. Hasta la presente fecha no se ha evaluado los procesos de TI, por lo tanto es necesario evaluar dichos procesos aplicando la metodología COBIT 4.1 para medir el nivel de cumplimiento y prever los riesgos en los puntos más vulnerables. Finalmente se elaborará el informe de la auditoria con sus respectivas observaciones y recomendaciones para ser entregado a la máxima autoridad del Hospital.

PALABRAS CLAVES:
COBIT
ISO
DNTI
ISO/IEC 27.000

ABSTRACT

The Ecuadorian Institute of Social Security is an entity whose organization is based on the principles of solidarity, obligation, universality, equity, efficiency, subsidiarity and adequacy. It is responsible for implementing the system of General Mandatory Insurance is part of the national social security system, with the mission of protecting the urban and rural population, labor relationship or not, the contingencies of sickness, maternity, risk labor, disability, unemployment, invalidity, old age and death, under the terms enshrined in the Social Security Act. In 2007, the IESS implemented the Institutional Development, in order to improve IT processes through the application of new standards to manage information security as risk management (ISO series / IEC 27,000), and development of a maturity model of information security at the level of internal, external and the services provided by the IESS in the Provincial, Hospitals and Medical Units users. Additionally a medical system is implemented in all Units and Hospitals, giving rise to the creation of the Technology Unit in Hospital IESS Zamora, new communications equipment, servers, workstations and assigning roles to staff area under standards set by the DDI. To date it has not been evaluated IT processes, therefore it is necessary to evaluate these processes by applying the COBIT 4.1 methodology to measure the level of compliance and provide risks in the most vulnerable points. Finally, the audit report with their respective observations and recommendations to be delivered to the highest authority of the Hospital will be developed.

KEYWORDS:
COBIT
ISO
DDI
ISO / IEC 27000

CAPÍTULO I

1. DESCRIPCIÓN DEL PROYECTO

1.1 . Alcance del Proyecto

Del previo análisis realizado en los procesos del Área de TI del Hospital del IESS Zamora, se determinó que es prioritario realizar una Evaluación de los Puntos vulnerables del Área de TI para evitar los posibles riesgos en las aplicaciones y activos de información estableciendo y con ello poder determinar los puntos críticos de la Unidad.

Este proyecto comienza con la descripción de los procesos del hospital, para proceder luego con la realización de la evaluación del sistema informático, tomando en cuenta equipos de comunicación, estaciones de trabajo y software instalado, utilizando una metodología adecuada, que se adapte y permita evaluar el desempeño del área informática del hospital.

1.2. Caracterización de la Organización

1.2.1. Descripción de la Organización

Nombre:

Hospital del Día “IESS Zamora”

Ubicación:

Provincia Zamora Chinchipe, Cantón Zamora

Línea de negocio:

Consulta Externa, Quirófano, Emergencia y Hospitalización

Categoría:

Nivel II, es decir, es un hospital apto para atender Emergencias, Consulta Externa, Quirófano, Ecu 911 y Hospitalización.

Logotipo:

1.3 Antecedentes

El Instituto Ecuatoriano de Seguridad Social es una entidad, cuya organización y funcionamiento se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia. Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del sistema nacional de Seguridad Social.

a. Año 1928: Caja de Pensiones

Decreto Ejecutivo Nº 018 publicado en el Registro Oficial Nº 591 del 13 de marzo de 1928. El gobierno del doctor Isidro Ayora Cueva, mediante Decreto Nº 018, del 8 de marzo de 1928, creó la Caja de Jubilaciones y Montepío Civil, Retiro y Montepío Militares, Ahorro y Cooperativa, institución de crédito con personería jurídica, organizada que de conformidad con la Ley se denominó Caja de Pensiones

La Ley consagró a la Caja de Pensiones como entidad aseguradora con patrimonio propio, diferenciado de los bienes del Estado, con aplicación en el sector laboral público y privado.

Su objetivo fue conceder a los empleados públicos, civiles y militares, los beneficios de Jubilación, Montepío Civil y Fondo Mortuorio. En octubre de 1928, estos beneficios se extendieron a los empleados bancarios (POA, Dirección Provincial de Pichincha, 2014).

En octubre de 1935 mediante Decreto Supremo No. 12 se dictó la Ley del Seguro Social Obligatorio y se crea el Instituto Nacional de Previsión, órgano superior del Seguro Social que comenzó a desarrollar sus actividades el 1º de mayo de 1936. Su finalidad fue establecer la práctica del Seguro Social Obligatorio, fomentar el Seguro Voluntario y ejercer el Patronato del Indio y del Montubio.

En la misma fecha inició su labor el Servicio Médico del Seguro Social como una sección del Instituto.

c. Año 1937: Caja del Seguro Social

En febrero de 1937 se reformó la Ley del Seguro Social Obligatorio y se incorporó el seguro de enfermedad entre los beneficios para los afiliados. En

julio de ese año, se creó el Departamento Médico, por acuerdo del Instituto Nacional de Previsión.

En marzo de ese año, el Ejecutivo aprobó los Estatutos de la Caja del Seguro de Empleados Privados y Obreros, elaborado por el Instituto Nacional de Previsión. Nació así la Caja del Seguro Social, cuyo funcionamiento administrativo comenzó con carácter autónomo desde el 10 de julio de 1937 (POA, Dirección Provincial de Pichincha, 2014).

d. Años 1942 a 1963

El 14 de julio de 1942, mediante el Decreto No. 1179, se expidió la Ley del Seguro Social Obligatorio. Los Estatutos de la Caja del Seguro se promulgaron en enero de 1944, con lo cual se afianza el sistema del Seguro Social en el país.

En diciembre de 1949, por resolución del Instituto Nacional de Previsión, se dotó de autonomía al Departamento Médico, pero manteniéndose bajo la dirección del Consejo de Administración de la Caja del Seguro, con financiamiento, contabilidad, inversiones y gastos administrativos propios.

Las reformas a la Ley del Seguro Social Obligatorio de julio de 1958 imprimieron equilibrio financiero a la Caja y la ubicaron en nivel de igualdad con la de Pensiones, en lo referente a cuantías de prestaciones y beneficios (POA, Dirección Provincial de Pichincha, 2014).

e. Año 1.963: Fusión de las cajas: caja nacional del seguro social

En septiembre de 1963, mediante el Decreto Supremo No. 517 se fusionó la Caja de Pensiones con la Caja del Seguro para formar la Caja Nacional del Seguro Social. Esta Institución y el Departamento Médico quedaron bajo la supervisión del ex -Instituto Nacional de Previsión.

En 1964 se establecieron el Seguro de Riesgos del Trabajo, el Seguro Artesanal, el Seguro de Profesionales, el Seguro de Trabajadores Domésticos y, en 1966, el Seguro del Clero Secular.

En 1968, estudios realizados con la asistencia de técnicos nacionales y extranjeros, determinaron "la inexcusable necesidad de replantear los principios rectores adoptados treinta años atrás en los campos actuariales, administrativo, y prestación de servicios", lo que se tradujo en la expedición

del Código de Seguridad Social , para convertirlo en "instrumento de desarrollo y aplicación del principio de Justicia Social, sustentado en las orientaciones filosóficas universalmente aceptadas en todo régimen de Seguridad Social: el bien común sobre la base de la Solidaridad, la Universalidad y la Obligatoriedad". El Código de Seguridad Social tuvo corta vigencia.

En agosto de l968, con el asesoramiento de la Organización Iberoamericana de Seguridad Social, se inició un plan piloto del Seguro Social Campesino.

El 29 de junio de 1970 se suprimió el Instituto Nacional de Previsión (POA, Dirección Provincial de Pichincha, 2014).

f. Año 1970: Instituto Ecuatoriano de Seguridad Social

Mediante Decreto Supremo Nº 40 del 25 de julio de 1970 y publicado en el Registro Oficial Nº 15 del 10 de julio de 1970 se transformó la Caja Nacional del Seguro Social en el Instituto Ecuatoriano de Seguridad Social .

El 20 de noviembre de 1981, por Decreto Legislativo se dictó la Ley de Extensión del Seguro Social Campesino.

En l986 se estableció el Seguro Obligatorio del Trabajador Agrícola, el Seguro Voluntario y el Fondo de Seguridad Social Marginal a favor de la población con ingresos inferiores al salario mínimo vital.

El Congreso Nacional, en l987, integró el Consejo Superior en forma tripartita y paritaria, con representación del Ejecutivo, empleadores y asegurados; estableció la obligación de que consten en el Presupuesto General del Estado las partidas correspondientes al pago de las obligaciones del Estado.

La Asamblea Nacional, reunida en l998 para reformar la Constitución Política de la República, consagró la permanencia del IESS como única institución autónoma, responsable de la aplicación del Seguro General Obligatorio.

El IESS, según lo determina la vigente Ley del Seguro Social Obligatorio, se mantiene como entidad autónoma, con personería jurídica, recursos propios y distintos de los del Fisco.

El 30 de noviembre del 2001, en el Registro Oficial N° 465 se publica la LEY DE SEGURIDAD SOCIAL, que contiene 308 artículos, 23 disposiciones transitorias, una disposición especial única, una disposición general.

1.3.1 Hospital del IESS Zamora

De acuerdo al Plan Operativo Anual 2014 (POA, 2014), del Hospital IESS Zamora, provee los servicios de Consulta externa, Emergencia y Hospitalización que comprende: especialidades de atención al afiliado, Emergencia las 24 horas, Rayos X, Laboratorio y Quirófano. El funcionamiento de los servicios consiste en que el afiliado llama al Call Center, solicita la cita con el médico de su requerimiento, donde existe un sistema de atención médica denominado Aplication System/400 (AS/400), desarrollado en Report Program Generator (RPG), siendo necesario indicar que es un emulador, ya que el servidor de bases de datos está centralizado en la ciudad de Quito; en las instalaciones existen equipos de comunicación para empaquetar esta información, como son router, switch y un servidor en red hat, cubriendo el área de telecomunicaciones. Además, todas las estaciones de trabajo tienen un usuario bajo un dominio.

1.3.2 Visión y Misión del Hospital IESS Zamora

a. Visión

Un Centro de Atención Ambulatoria prestador de servicios de salud con enfoque individual, familiar, comunitario y en red plural, de calidad y prestigio garantizados por la eficiencia, efectividad y calidez de sus servicios; acorde al avance de la ciencia, tecnología y profesionalización del talento humano, en función de las necesidades de los usuarios para mejorar su salud y calidad de vida; logrando altos niveles de competitividad y desarrollo local, regional y nacional (Reglamento Oficial del IESS Zamora, 2008).

b. Misión

Proveer una atención de salud con calidad, calidez y eficacia constituyendo una organización que ofrece servicios de salud integral a la población urbana y rural, a través de equipos multidisciplinarios permanentemente capacitados y calificados con tecnología de punta variada

y renovada, aplicando acciones de promoción, prevención, recuperación y rehabilitación, en los servicios de: Clínica, cirugía del día, Ginecología, pediatría, fisiatría, medicina general, urgencias, odontología, cuidado materno infantil y auxiliares de diagnóstico (laboratorio, imagenología, farmacia), para impulsar ambientes y estilos de vida saludables (Reglamento Oficial del IESS Zamora, 2008).

1.3.3 Estructura Organizacional. La estructura organizacional del Hospital del IESS Zamora se implementó en el año 2015, como consta en la figura 1

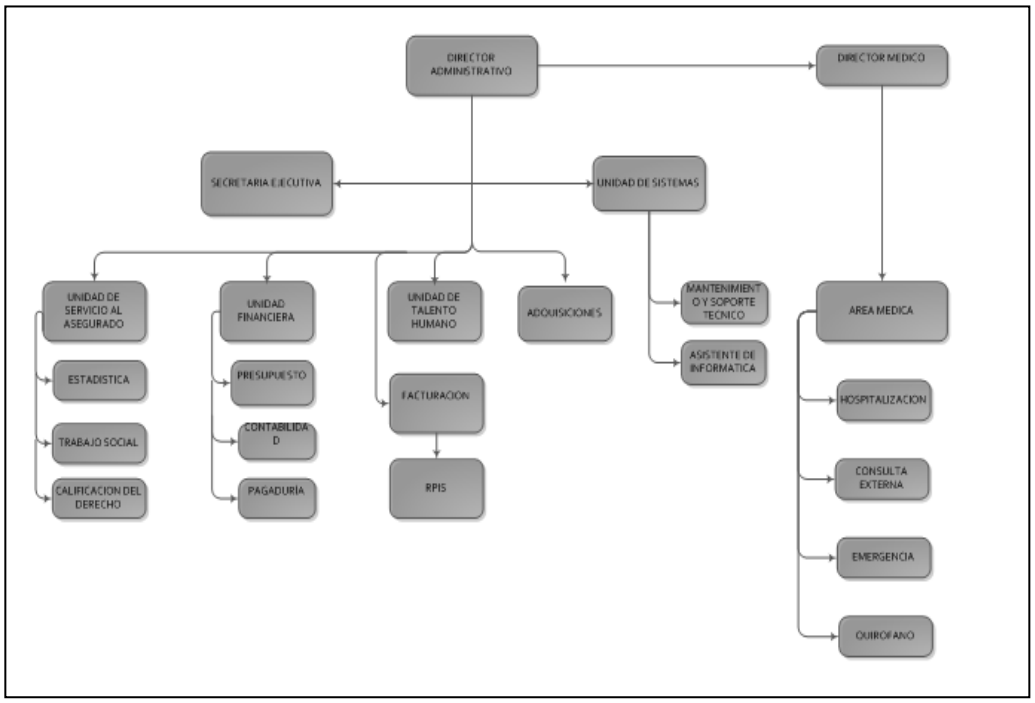


Figura 1 Organigrama del Hospital IESS Zamora

1.4 Identificación de Problemas

1.4.1 A nivel del estado de salud

a. Falta de protocolos de diagnóstico y tratamiento de patologías.
b. Capacidad resolutiva incompleta por el nivel de complejidad.
c. Falta de coordinación y comunicación entre las unidades médicas.
d. Funcionamiento inadecuado del sistema de referencia y contra referencia
e. Inadecuado manejo estadístico.

1.4.2 A nivel de la gestión.

a. Tiempo de espera prolongado en procesos adquisitivos.

b. Falta de interconectividad informática en red interna y externa.

c. Automatización de procesos.

d. Ausencia de un manual de funciones

1.4.3 A nivel de la inversión.

a. Falta de capacitación al usuario interno.

b. Inadecuada ejecución del POA Y PAC.

c. Falta de concienciación y cooperación en el cumplimiento de funciones específicas.

1.4.4 Equipamiento y tecnología del Hospital IESS Zamora

El equipamiento requerido es indispensable para mejorar el funcionamiento de la mayoría de servicios; consientes que la tecnología ayuda en el diagnóstico oportuno, se propone mejorar el equipo médico existente, algunos han terminado su vida útil, como en laboratorio, fisiatría, RX y se propone adquirir equipos nuevos acorde al avance tecnológico y bajo la propuesta del área correspondiente. Siguiendo los lineamientos institucionales y las necesidades de los usuarios se obtendrá el equipamiento adecuado.

Se propone renovar y dotar de suficiente instrumental médico y odontológico a las diferentes Unidades del Hospital y así como innovar el equipo médico menor de Consulta Externa e implementación de mobiliarios y equipos de oficina para los diferentes servicios.

1.5 Procesos Técnicos Administrativos

a. De acuerdo a la Reforma y Fortalecimiento de los Servicios de Salud (RFSA, 2014) del IESS, exige que los procesos de producción y servicios sean más eficientes y eficaces, toda vez que la propuesta institucional para el año 2014 sea de Equilibrio Financiero, a través del fortalecimiento de los siguientes procesos:

b. Técnico administrativo de facturación, Costos de servicios, Análisis financiero y presupuestario y análisis de servicios de costo elevado, en

procura de impulsar acciones para disminuirlos, particularmente de Consulta externa y otros que pudiesen presentarse.

c. Manejo y Control mensual de kardex, egreso y saldo de fármacos, insumos, materiales y biomateriales por servicio y Unidad, lo que permitirá un abastecimiento oportuno, de acuerdo al perfil epidemiológico.

d. Inventarios de Bodega, Farmacia; así como el arqueo permanente de estos departamentos; y, levantamiento de activos fijos, como herramienta de gestión e inversión de la Dirección.

e. Información estadística, bioestadística, de la Unidad y del AS/400 de producción y estadística del sistema de vigilancia epidemiológica para tener información veraz y única, para la toma de decisiones Gerenciales.

f. Abastecimiento y Compras públicas, acorde a la Ley Organica del Sistema Nacional de Contratación Pública (LOSNCP,2013).

g. Mejoramiento continuo de la calidad, a través de la vigencia de comités de trabajo con reuniones periódicas (mensuales) con la gerencia en procura de solución a quejas y denuncias del servicio

h. Socialización de Procesos internos, logros alcanzados, metas propuesta y avance de indicadores de gestión con el personal operativo del centro a través de reuniones de trabajo, para construir un equipo de trabajo participativo de mantenimiento preventivo y correctivo del equipamiento médico e informático existente, e implementar un plan de contingencia ante eventualidades.

1.6 Automatización del Hospital

Con la finalidad de optimizar recursos se utiliza el AS/400 para la atención médica para los costos de la unidad se utiliza el sistema denominado Winsing, Facturación son básicos para el funcionamiento del Hospital y se constituyen en una herramienta de apoyo muy importante en la gestión y financiamiento de los diversos servicios.

Y ante la adquisición de Equipos médicos de alta tecnología (RX/laboratorio, especialidades médicas, Fisiatría, Quirófano), es pertinente la adquisición de Generadores de Energía.

El apoyo Técnico Informático para la U. médica debe subdividirse en un área de mantenimiento de equipos y redes informáticas y otra área de asesoría y control, capacitación y administración de los Programas informáticos.

1.6.1 Naturaleza de la Organización

Área bien definida y se encuentra como soporte técnico para las aplicaciones que se utilizan en el hospital.

1.6.1.1 Objetivos Estratégicos

a. Compromiso y voluntad para asumir nuevos roles y competencias, compartiendo las experiencias.
b. Posicionamiento institucional, con actitud propositiva en el cumplimiento de Reglamentos e Instructivos.
c. Transparencia en los procesos de Dirección y gestión, procesos internos de producción y entrega de servicios, implementado el mejoramiento continuo y garantía de calidad de atención en salud.
d. Fortalecimiento de los procesos de entrega de servicios, producción, facturación y costos de las unidades del Centro y cumplimiento del sistema de referencia y contrarreferencia.
e. Optimización de la Gestión financiera y RRHH en gerencia de servicios de salud, planificación y pensamiento estratégico, atención medica integral y medicina familiar; así como el abastecimiento y adquisición para el centro a través de Compras públicas.

1.7 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 señalamos algunas de las metodologías utilizadas en auditorias informáticas para poder escoger la que mejor se ajuste a las necesidades del Hospital del Día “IESS Zamora”:

a. COBIT 4.1 (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 sumamente relacionado con todo lo referente a tecnologías de la Información" (IT Governance Institute*. COBIT, 2010).*

b. 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" (Zamora, Carlos. ITIL, 2005).

c. Metodología R.O.A (RISK ORIENTED APPROACH), "Está formulada 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 controles y de que éstos funcionen. En consecuencia el auditor deberá revisar estos controles y su funcionamiento"

1.7.1 Comparación de las metodologías. Con la finalidad de establecer la función de cada una de las metodologías, se ha realizado una tabla comparativa que se señala a continuación:

Tabla 1.
Comparación de metodologías COBIT 4.1, ITIL, ROA

	COBIT 4.1	ITIL	ROA
Autores	Los creadores de COBIT 4.1 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.
Alcance	COBIT 4.1 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 Organización, así como definir el estado del control de dichos sistemas tomando como control la definición de la ISAACA.
Elementos de la Metodología	COBIT 4.1 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

Fuente: (IT Governance Institute. *COBIT, 2010,* ITIL, 2005).

Después de este análisis previo, la metodología a utilizar es COBIT 4.1, que es la más adecuada para poder identificar los riegos y

vulnerabilidades de la unidad de TI del Hospital del Día “IESS Zamora”. 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 4.1, son principalmente, porque incluye dentro de la metodología prácticas alineadas con las decisiones gerenciales y de gobierno de tecnología. Además COBIT 4.1 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 del Hospital.

Además con la utilización de COBIT 4.1 se 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 agregado al trabajo realizado dentro de la unidad de TI.

CAPÍTULO II

2. EJECUCIÓN DE LA AUDITORÍA

2.1 Planificación de la Auditoría

La planificación de la auditoria que se realizó al Hospital del Día “IESS Zamora”, 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 4.1

2.2. Situación actual del Área de Sistemas

2.2.1. Nivel de decisión de la unidad de 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.

2.2.2 Estructura de la Unidad de Informática. La estructura de la Unidad de Informática del Hospital IESS ZAMORA que gestiona, controla los procesos del Área de TI se esquematiza en la figura 2.

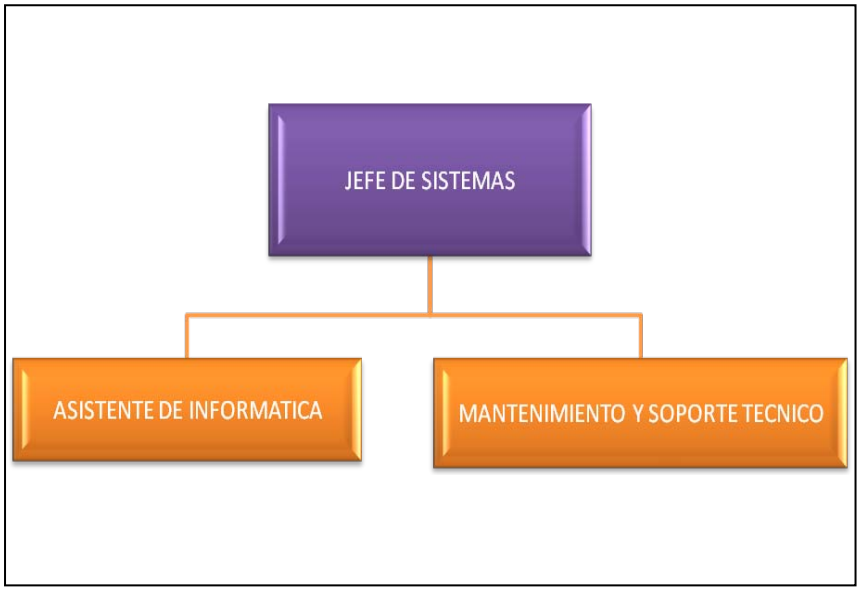


Figura 2 Estructura de TI

El Departamento de Sistemas es la unidad encargada de gestionar el apoyo informático a las actividades del Hospital del Día "IESS Zamora", 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 Áreas, Servicios, departamentos y Anexos del Hospital del Día "IESS Zamora". Desde su creación el Departamento de Sistemas no cuenta con un modelo organizacional que defina los procesos, control de activos, gestión de riesgos e incidentes, para salvaguardar la información, así como también con personal que soporte la gran demanda de usuarios, software, hardware e información existente en el hospital.

2.2.3 Funciones

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 internos y externos, 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. Á reas

a. Área de dirección o Jefe de Sistemas

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.

b. Asistente de Sistemas

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.

c. Mantenimiento y soporte técnico

Área responsable de la gestión del hardware y del software dentro de las instalaciones del Hospital del Día “IESS Zamora”, 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.

2.2.5 Inventario de Hardware. A continuación en la tabla 2 se especifica un listado del hardware que posee el Hospital IESS Zamora:

Tabla 2
Inventario de HW del Hospital IESS Zamora

CODIGO INSTITUCIONAL	TIPO	MARCA	CANTIDAD
169920000000	PCs de Escritorio	DELL	72
	Laptop	HP	10
	Impresoras	EPSON, CANON, HP, XEROX	10
	Fax		2
	Escáner	HP	5
	Copiadora	RICOH	2
	Dispositivos de Almacenamiento	SAMSUNG	15
	Infocus	CANON	5
	Pantalla Eléctrica		
	Servidor	HP	2
	Switch	3com 5500	4
	Router	3com V6000	1

Fuente: (POA Hospital IESS Zamora, 2015)

2.2.6. Inventario de Software. En la tabla 3 , se menciona el tipo de software que es utilizado en el Hospital IESS Zamora.

Tabla 3
Inventario de SW del Hospital IESS Zamora

CODIGO INSTITUCIONAL	TIPO
169920000000	Sistema Operativo
	Antivirus
	Paquete Office
	Aplicativos de Contabilidad
	Aplicativos de Presupuesto
	Aplicativos del Área Medica

Fuente: (POA Hospital IESS Zamora, 2015)

2.2.7. Inventario de Activos. En la figura 3, se detalla los activos de Información que se utiliza en el Hospital IESS Zamora

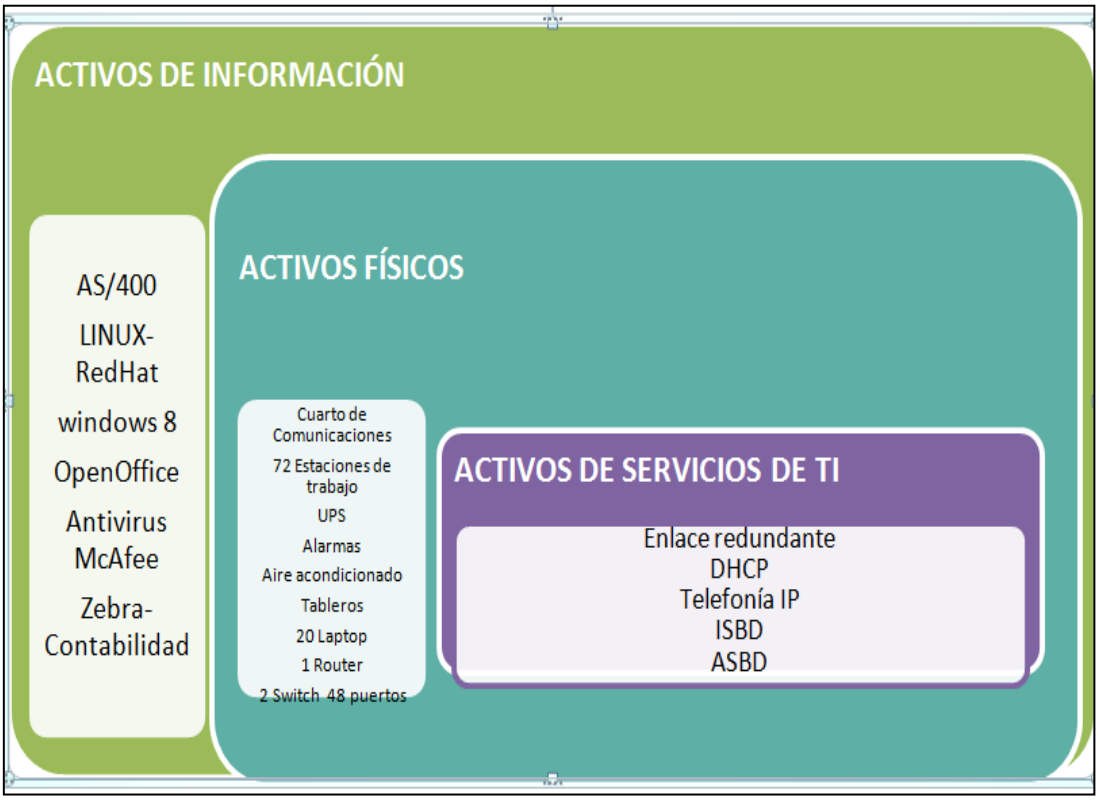


Figura 3 Inventario de Activos de Información del Hospital IESS Zamora

2.2.7. TOPOLOGÍA DE RED

La topología de red que posee el IESS es una topología mixta como se presenta en la figura 4.

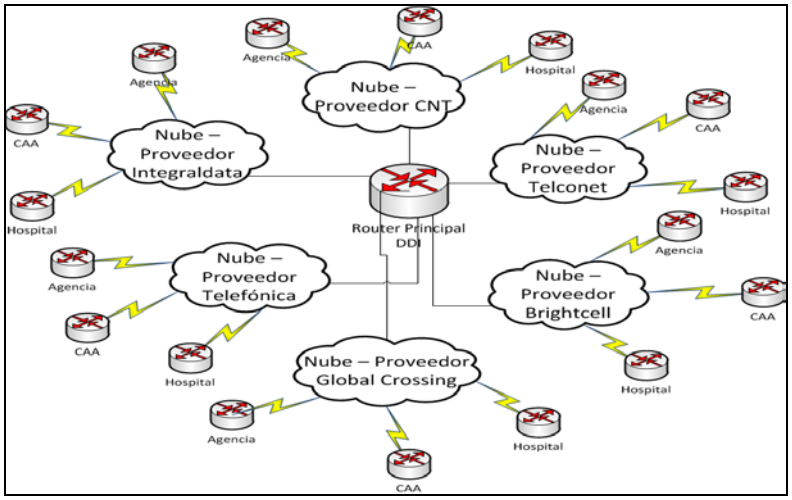


Figura 4 Topología de Red del IESS

Los enlaces de Comunicación que se han implementado a nivel del IESS se presenta en la tabla 4.

Tabla 4
Enlaces de Comunicación del IESS

Dependencias	Enlaces Actuales
Unidades Administrativas	63
Unidades Administrativas de Salud	4
Hospitales	22
Centros de Atención Ambulatoria	32
Unidades de Atención Ambulatoria	44
Seguro Social Campesino	12
Enlaces de Internet (Principal y Backup)	4
Enlaces de Replica (Principal y Backup)	4
Enlaces Backup	34 (entre Hospitales I,II,III y CAA's) 4 (Unidades Administrativas)

Fuente: (Dirección general del IESS)

La arquitectura que se ha implementado en el IESS a nivel nacional se muestra en la figura 5.

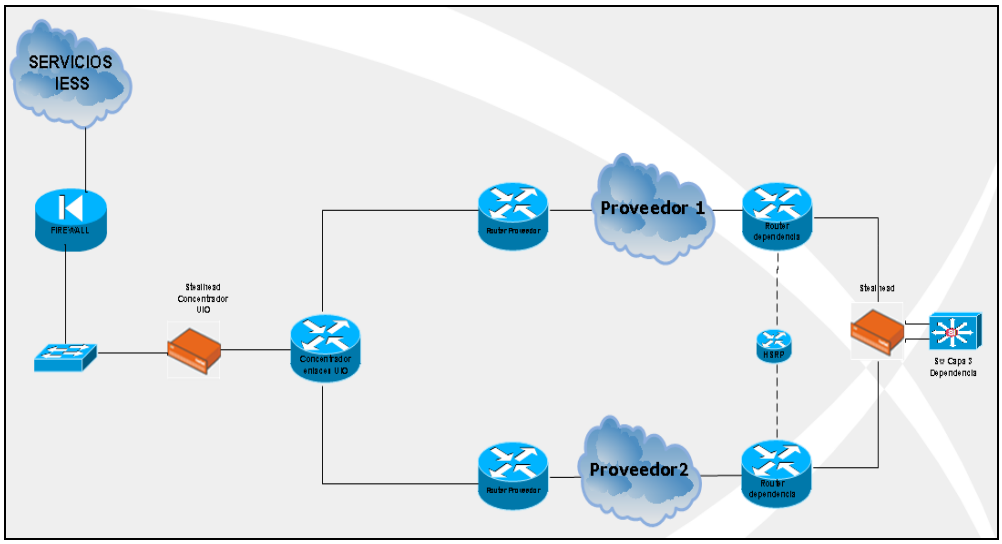


Figura 5 Arquitectura de TI del IESS

2.2.8 Seguridades

2.2.8.1 Seguridad Física

En el Hospital del Día “IESS Zamora”, se ha implementado 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 las 24 horas.

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 metálica con chapa normal sin seguros la cual no garantiza el acceso de personal no autorizado.

2.2.8.2. Seguridad Lógica

La seguridad lógica del Hospital del Día “IESS Zamora” maneja perfiles de usuario, que son administrados por la unidad de TI a través del servidor de directorio activo 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.

Sin embargo no existe una matriz de perfiles de usuario y políticas de seguridad establecidas a nivel local.

a. Administración de cuentas de usuario

El Asistente de informática es el encargado de 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.

b. 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.

c. 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 4.1 que han sido seleccionados 65 items de los cuatro procesos, con la ayuda del tutor para la evaluación de la unidad de TI del Hospital del Día “IESS Zamora”. 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 (26 priorizados)

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 Organizacional

b. PO2.2 Diccionario de Datos Organizacional 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 (11 priorizados)

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 (20 priorizados)

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 (8 priorizados)

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

2.3.1. Procesos del Dominio de Planeación y Organización

2.3.1.1. PO1 Definir un Plan Estratégico de TI

GUÍA PARA LA AUDITORIA

Las políticas y procedimientos del Área de TI deben seguir un enfoque de planeación estructurado como se muestra en la tabla 5. Se ha establecido una metodología para formular y modificar los planes y que cubre, como mínimo:

Misión y las metas de la Unidad

Iniciativas de tecnología de información para soportar la misión y las metas de la Unidad

Análisis costo/beneficio de las adquisiciones de tecnología.

Los dueños de los procesos y la alta Gerencia deben llevar a cabo revisiones periódicas de los planes de TI.

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

Tabla 5
Estrategia a corto y largo plazo PO1

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO1.2 Alineación de TI con la Unidad	Entrevista a la alta gerencia. Entrevista al responsable del proceso de TI. Entrevista a una secretaria del hospital.	Orgánico Funcional del Hospital del Día "IESS Zamora". 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 responsable del proceso de TI. Entrevista con un médico del hospital. Entrevista a una secretaria del hospital.	Orgánico Funcional del Hospital del Día "IESS Zamora".	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.

Fuente: (IT Governance Institute*. COBIT, 2010,* ITIL, 2005)

Tabla 6

PO1. Definir un Plan Estratégico

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 de la Unidad.		X	Grado de Madurez El proceso de definir un plan estratégico de TI se encuentra en un nivel 1. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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	El jefe de TI conoce la necesidad de una planeación estratégica 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.		X	
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.		X	
Nivel 3	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.		X	
Nivel 4	La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La dirección puede monitorear el proceso estratégico de TI, tomar decisiones informadas con base en el plan y medir su efectividad.		X	
Nivel 5	La planeación estratégica de TI es un proceso documentado y da como resultado un valor observable de negocios por medio de las inversiones en TI.		X	

Fuente: (IT Governance Institute. *COBIT, 2010,* ITIL, 2005)

COBIT 4.1 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 deben manejar estrategias a corto y largo plazo de acuerdo a la metodología de COBIT 4.1, como se muestra en la tabla 7.

Tabla 7
Estrategias a corto y largo plazo PO2

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,
Estrategias a largo plazo	Crear un plan estratégico a largo plazo, en donde se consideren los objetivos del Hospital, 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. 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.

Fuente: (IT Governance Institute*. COBIT, 2010,* ITIL, 2005)

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.

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 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.

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)

Tabla 8
PO2.1 Modelo de Arquitectura de Información Organizacional

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO2.1 Modelo de Arquitectura de Información Organizaciona	Entrevista al responsable del proceso 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 del Día “IESS Zamora”. No se ha definido la arquitectura que el hospital va a manejar para la información.

Fuente: (IT Governance Institute. *COBIT, 2010,* ITIL, 2005)

Tabla 9
Po2 Definición de la Arquitectura de Información

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.		X	Grado de Madurez El proceso de definición de la arquitectura de información se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" no se maneja la información como una arquitectura, lo que hace que esta no se encuentre estandarizada, ni se reconozca su importancia en el área administrativa y médica.
Nivel 1	Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.	X		
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.	X		
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.	X		
Nivel 4	Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. El proceso de definición de la arquitectura de información es proactivo y se enfoca en resolver necesidades futuras del negocio.		X	
Nivel 5	La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la unidad en el desarrollo y mantenimiento de la arquitectura de información		X	

Fuente: (IT Governance Institute*. COBIT, 2010,* ITIL, 2005)

COBIT 4.1 plantea para el PO2 la necesidad de cumplir con los siguientes objetivos de control.

a. Modelo de la Arquitectura de Información

b. Diccionario de Datos y Reglas de Sintaxis de Datos de la Unidad

c. Esquema de Clasificación de Datos

d. 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 4.1, se recomiendan las siguientes de acuerdo a la tabla :

Tabla 10

Estrategias a corto y largo plazo PO2

Estrategias a corto plazo	Definir un modelo de la arquitectura de la información, un diccionario de datos y reglas de sintaxis para que sea manejado por todos los usuarios. Crear y comunicar un esquema de datos estándar para todos los usuarios. Establecer procedimientos formales para la clasificación y
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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 han 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.

Tabla 11
PO3 Planeación de la Dirección Tecnológica

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 responsable del	Orgánico Funcional del Hospital del Día “IESS Zamora””.	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 responsable del proceso de TI.	Presupuesto 2015 para el área 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 12
Modelo de Madurez P03

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. Se evidencia falta de entendimiento de que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.		X	Grado de Madurez. El proceso de determinación de la dirección tecnológica se encuentra en un nivel 1. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.	X		
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 personas que siguen procesos intuitivos, aunque similares.		X	
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.	X		
Nivel 4	La dirección garantiza el desarrollo del plan de infraestructura tecnológica. 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.		X	
Nivel 5	Existe una función de investigación que revisa las tecnologías emergentes y evolutivas 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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el PO3 la necesidad de cumplir con los siguientes objetivos de control.

a. Planeación de la Infraestructura Tecnológica
b. Monitoreo de Tendencias y Regulaciones Futuras
c. Contingencias en la Infraestructura Tecnológica
d. Planes de Adquisición de Hardware y Software
e. 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 4.1, se recomiendan las siguientes:

Tabla 13
Estrategias a corto y largo plazo PO3

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 puedan aprovechar las ventajas que las herramientas tecnológicas les brinda.
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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 trabajo, 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 del Hospital 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 respecto 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 Jefe 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 programar recursos y asegurar el cumplimiento de las antes de que se implementen nuevos sistemas o cambios a los sistemas.

El analista de sistemas 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 el flujo de información, 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 determinan 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 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.

El Jefe 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.

Los términos de los contratos sean consistentes con los estándares normales acordes a la organización y los términos y condiciones contractuales estándar son revisadas y evaluadas por un comité de Adquisiciones.

Tabla 14
PO4 Definición de la organización y de las relaciones de TI

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
PO4.4 Ubicación Organizacional de la Función de TI	Entrevista al Jefe de servicios generales. Entrevista al responsable del proceso de TI.	Orgánico Funcional del Hospital del Día "IESS Zamora". Orgánico Funcional del área de TI.	El área de sistemas está ubicada como un sub departamento del área de adquisiciones. Las acciones que realice el área de TI tienen que ser informadas al departamento de adquisiciones y Facturación.
PO4.5 Estructura Organizacional	Entrevista al gerente de servicios generales.	Orgánico Funcional del Hospital del Día "IESS Zamora".Orgánico Funcional del áreade TI.	Se tiene asignada el área de influencia del departamento de TI.
PO4.6 Establecimiento de Roles y Responsabilidades	Entrevista al gerente de servicios generales. Entrevista al responsable del proceso 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 responsable del proceso de TI.	Orgánico Funcional del área de TI.	Faltan controles en el flujo de información de la Unidad. No se evalúan los requerimientos de personal de forma regular o con la existencia de cambios importantes.
PO4.15 Relaciones	Entrevista al responsable del proceso 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 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

- Ubicación de los servicios de información en la organización
- Revisión de Logros Organizacionales
- Roles y Responsabilidades
- Responsabilidad del aseguramiento de calidad
- Responsabilidad de la Seguridad Lógica y Física
- Propiedad y Custodia
- Propiedad sobre Datos y Sistemas
- Supervisión
- Segregación de Funciones
- Asignación de Personal para Tecnología de Información
- Descripción de Puestos de trabajo para el Personal de TI
- Personal Clave de Tecnología de Información
- Políticas y Procedimientos para el personal por contrato
- 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 4.1, se recomiendan las siguientes:

Tabla 15
Estrategias a corto y largo plazo PO4

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. 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

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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.

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 documentadas 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.

Tabla 16
PO6 Comunicación de los objetivos de 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 nivel central. 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 responsable del proceso de TI.	Orgánico Funcional de área de TI.	Los objetivos se los transmite de manera directa mediante una asamblea general.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el PO6 la necesidad de cumplir con los siguientes objetivos de control.

- Ambiente Positivo de Control de la Información
- Responsabilidad de la Gerencia en cuanto a Políticas
- Comunicación de las Políticas de la Organización
- Recursos para la Implementación de Políticas
- Mantenimiento de Políticas

- Cumplimiento de Políticas, Procedimientos y Estándares
- Compromiso con la Calidad
- Política sobre el Marco Referencial para la Seguridad y el Control Interno
- Derechos de la Propiedad Intelectual
- 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 4.1, se recomiendan las siguientes:

Tabla 17.
Estrategias a corto y largo plazo PO6

Estrategias a corto plazo	Definir claramente la misión y visón del área de TI, darla a conocer a todos los empleados. 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 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 actualizaciones regulares 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.

Tabla 18
PO9 Análisis de riesgos

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 responsable del proceso de TI.	No existen documentos en donde se evalúen los riesgos del área de TI.	No se evalúan los riesgos, solo se trata de 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 del hospital.	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 pueden resultar ineficientes e inadecuadas.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 19
Modelo de Madurez 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.		X	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 del Día "IESS Zamora" 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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 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 4.1, se recomiendan las siguientes:

Tabla 20
Estrategias a corto y largo plazo PO9

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 del impacto de riesgos y como afectarían al normal funcionamiento de hospital. Crear planes de contingencia para prever estos riegos, y asegurar la continuidad del negocio.
Estrategias a largo plazo	Crear planes de acción a largo plazo para evitar 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

2.3.1.7. Resumen del Dominio Planeación y Organización

Dentro de la evaluación del Hospital del Día “IESS Zamora” y específicamente dentro del dominio de planeación y organización que nos plantea COBIT 4.1, 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, no se cuenta con perfiles de usuario de acuerdo al rol que desempeñan, 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 disminuido 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 al personal 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 mejorar 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 Organización 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

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

Tabla 21
AI2 Adquisición y mantenimiento de software de aplicación

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
AI2.4 Seguridad y Disponibilidad de las Aplicaciones	Entrevista al responsable del proceso 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	Entrevista al responsable del proceso 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 responsable del proceso 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 22
Nivel de Madurez 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.		X	Grado de Madurez. El proceso de adquisición y mantenimiento de software aplicativo se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.		X	
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.		X	
Nivel 3	Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Las actividades de mantenimiento se planean, programan y coordinan		X	
Nivel 4	Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones.	X		
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 La metodología produce documentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento.	X		

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el AI2 la necesidad de cumplir con los siguientes objetivos de control.

- Métodos de Diseño
- Cambios Significativos a Sistemas Actuales
- Aprobación del Diseño
- Definición y Documentación de Requerimientos de Archivos
- Especificaciones de Programas
- Diseño para la Recopilación de Datos Fuente
- Definición y Documentación de Requerimientos de Entrada de Datos
- Definición de Interfaces
- Interface Usuario - Máquina
- Definición y Documentación de Requerimientos de Procesamiento
- Definición y Documentación de Requerimientos de Salida de Datos
- Controles
- Disponibilidad como Factor Clave de Diseño
- Definiciones de TI sobre Integridad para el Software de Programas de Aplicación
- Pruebas de Software de Aplicación
- Materiales de Consulta y Soporte para Usuario
- 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 4.1, se recomiendan las siguientes:

Tabla 23
Estrategias a corto y largo plazo AI2

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 Organización 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

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 información 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 fueron cambiados al momento de la instalación

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

Tabla 24
Tabla Resumen AI3

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

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 25
Modelo de Madurez AI3

Dominio: Adquisición e Implementación				
Proceso: AI3 ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLOGICA				
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.	X		Grado de Madurez. El proceso de adquisición y mantenimiento de la infraestructura tecnológica se encuentra en un nivel 0. Objetivos no Cumplidos El Hospital del Día "IESS Zamora" 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 La actividad de mantenimiento reacciona a necesidades de corto plazo.		X	
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.		X	
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.		X	
Nivel 4	Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio.	X		
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. La infraestructura de TI se entiende como el apoyo clave para impulsar el uso de TI.	X		

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el AI3 la necesidad de cumplir con los siguientes objetivos de control.

- Evaluación de Nuevo Hardware y Software
- Mantenimiento Preventivo para Hardware
- Seguridad del Software del Sistema
- Instalación del Software del Sistema
- Mantenimiento del Software del Sistema
- Controles de Cambios para el Software del Sistema
- 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 4.1, se recomiendan las siguientes:

Tabla 26
Estrategias a corto y largo plazo AI3

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 de información. 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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.

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 las 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 mensajes 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

Tabla 27
AI4 Desarrollo y mantenimiento de procedimientos

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 28
Modelo de Madurez 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.		X	Grado de Madurez. El proceso de desarrollo y mantenimiento de procedimientos se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" no se producen manuales de usuario ni de operación en el área de TI.
Nivel 1	Mucha de la documentación y muchos de los procedimientos ya caducaron.		X	
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.		X	
Nivel 3	Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. 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.		X	
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.	X		
Nivel 5	El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos.	X		

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el AI4 la necesidad de cumplir con los siguientes objetivos de control.

- Requerimientos Operacionales y Niveles de Servicios
- Manual de Procedimientos para el Usuario
- Manual de Operaciones
- 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 4.1, se recomiendan las siguientes:

Tabla 29
Estrategias a corto y largo plazo AI4

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 pos 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.

Tabla 30
AI5 Instalación y acreditación de sistemas

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
AI5.3 Plan de Implementación	Entrevista al responsable del proceso 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 responsable del proceso 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

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 31
Modelo de Madurez 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.	X		Grado de Madurez. El proceso de instalación y acreditación de sistemas se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.	X		
Nivel 2	Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología.	X		
Nivel 3	Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación.		X	
Nivel 4	Los procedimientos son formales y se desarrollan para ser organizados y prácticos con ambientes de prueba definidos y con procedimientos de acreditación.		X	
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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el AI5 la necesidad de cumplir con los siguientes objetivos de control.

- Entrenamiento
- Adecuación del Desempeño del Software de Aplicación
- Plan de Implementación
- Conversión del sistema
- Conversión de datos
- Planes y estrategias de pruebas
- Pruebas a los Cambios
- Desempeño y criterios de pruebas en paralelo/piloto
- Prueba de Aceptación Final
- Pruebas y Acreditación de la Seguridad
- Prueba Operacional
- Promoción a Producción
- Evaluación del cumplimiento de los Requerimientos del Usuario
- Revisión Gerencial Pos 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 4.1, se recomiendan las siguientes:

Tabla 32
Estrategias a corto y largo plazo AI5

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

2.3.2.5. Resumen del Dominio Adquirir e Implementar

En la evaluación general del dominio de adquirir e implementar del Hospital del Día “IESS Zamora”, que nos plantea COBIT 4.1, 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 4.1. 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

Tabla 33
DS1 Definición y administración de niveles de servicio

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 responsable del proceso 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 usuario 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 y capacidad de crecimiento.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 34
Modelo de Madurez 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.		X	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 del Día "IESS Zamora" 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.		X	
Nivel 2	Los niveles de servicio están acordados pero son informales y no están revisados.		X	
Nivel 3	Las responsabilidades están bien definidas pero con autoridad discrecional.		X	
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.	X		
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.	X		

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS1 la necesidad de cumplir con los siguientes objetivos de control.

- Marco de Referencia para los acuerdos de Nivel de Servicio

- Aspectos sobre los Acuerdos de Nivel de Servicio
- Procedimientos de desempeño
- Monitoreo y Reporte
- Revisión de Convenios y Contratos de Nivel de Servicio
- Elementos sujetos a Cargo
- 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 4.1, se recomiendan las siguientes:

Tabla 35
Estrategias a corto y largo plazo DS1

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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:

Filosofía y un marco referencial consistentes en relación con el desarrollo de un plan de continuidad

Priorización de las aplicaciones con respecto a los tiempos de recuperación y regreso a la operación normal

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

Determinación de funciones y responsabilidades específicas con respecto a la planeación de continuidad con pruebas, mantenimiento y requerimientos de actualización específicos

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

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

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

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)

Tabla 36
DS4 Asegurar el servicio continuo

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 responsable del proceso 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 responsable del proceso 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 37
Modelo de Madurez DS4

Dominio: Entregar 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			Grado de Madurez. El proceso de asegurar el servicio continuo se encuentra en un nivel 1. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.		X	
Nivel 2	Se asigna la responsabilidad para mantener la continuidad del servicio. 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.	X		
Nivel 3	La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas	X		
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.		X	
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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS4 la necesidad de cumplir con los siguientes objetivos de control.

- Marco de Referencia para Continuidad (recuperación en caso de desastres) de TI
- Estrategia y Filosofía del Plan de Continuidad de TI
- Contenido del Plan de Continuidad de TI
- Reducción de los Requerimientos de la Continuidad de TI
- Mantenimiento del Plan de Continuidad de TI
- Prueba del Plan de Continuidad de TI
- Capacitación para el Plan de Continuidad de TI
- Distribución del Plan de Continuidad de TI
- Procedimientos de Respaldo del Procesamiento Alterno en el departamento Usuario
- Recursos críticos de TI

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 4.1, se recomiendan las siguientes:

Tabla 38
Resumen DS4

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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.

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

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:

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, usuario y password.

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 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

Tabla 39
DS5 Garantizar la seguridad de sistemas

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 .	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	Entrevista al responsable del proceso de TI.	Inventario de software del Hospital del Día “IESS Zamora”	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 del Día “IESS Zamora”	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

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 40
Modelo de Madurez DS5

Dominio: Entregar y Soporte				
Proceso: DS5 GARANTIZAR LA SEGURIDAD DE SISTEMAS				
Niveles de los Modelos de Madurez		Cumple	No cumple	Observaciones
Nivel 0	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.		X	Grado de Madurez. El proceso de garantizar la seguridad en los sistemas se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.		X	
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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS5 la necesidad de cumplir con los siguientes objetivos de control.

- Manejo de las Medidas de Seguridad
- Identificación, Autenticación y Acceso
- Seguridad de Acceso a Datos en Línea
- Administración de Cuentas de Usuario
- Revisión Gerencial de Cuentas de Usuario

- Control de Usuario de las Cuentas de Usuario
- Vigilancia de Seguridad
- Clasificación de Datos
- Administración Centralizada de Identificación y Derechos de Acceso
- Reportes de Actividades de Violación y Seguridad
- Manejo de Incidentes
- Re-acreditación
- Contrapartes confiables
- Autorización de Transacción
- No Rechazo
- Ruta Confiable
- Protección de las Funciones de Seguridad
- Administración de Llaves Criptográficas
- Prevención, Detección y Corrección del Software Dañino
- Arquitectura de Firewalls y Conexiones con las Redes Públicas
- Protección del Valor Electrónico

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

Tabla 41
DS7 Educación y entrenamiento de usuarios

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 responsable del proceso 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 responsable del proceso 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 42
Modelo de Madurez 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.		X	Grado de Madurez. El proceso de educación y entrenamiento de usuarios se encuentra en un nivel 0. Objetivos no Cumplidos El Hospital del Día "IESS Zamora" 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.		X	
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.		X	
Nivel 3	El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento.		X	
Nivel 4	Hay un programa completo de entrenamiento y educación que produce resultados medibles. El entrenamiento y la educación son componentes de los planes de carrera de los empleados.	X		
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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS7 la necesidad de cumplir con los siguientes objetivos de control.

- Identificación de necesidades de entrenamiento.
- Organización de entrenamiento.
- 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 4.1 se recomienda lo siguiente:

Tabla 43
Resumen DS7

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

2.3.3.5. DS8 Apoyo y asistencia para los usuarios

Guías de auditoria

Considerando si:

La naturaleza de la función del Help Desk 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

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

Tabla 44
DS8 Apoyo y asistencia para los usuarios

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
DS8.1 Help Desk	Entrevista al responsable del proceso 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 usuarios 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 Clientes	Entrevista a un empleado de soporte técnico. Entrevista a un empleado del área	No existen documentos de respaldo de monitoreo a clientes	No se mide el nivel de satisfacción de los usuarios periodicamente

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 45
Modelo de madurez DS8

Dominio: Entregar y Soporte				
Proceso: DS8 APOYO Y ASISTENCIA PARA LOS USUARIOS				
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.		X	Grado de Madurez. El proceso de Apoyo y asistencia para los usuarios se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día “IESS Zamora” 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.		X	
Nivel 2	Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes.		X	
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. Se deja la responsabilidad al individuo de conseguir entrenamiento y de seguir los estándares. 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. Losusuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes.		X	
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.			
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.	X		

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS8 la necesidad de cumplir con los siguientes objetivos de control.

- Help Desk
- Registro de consultas del cliente
- Escalamiento de consultas del cliente
- Monitoreo de atención a clientes
- 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 4.1, se recomiendan las siguientes:

Tabla 46
Resumen DS8

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 tomando 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

Pproblemas 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

Tabla 47
DS10 Administración de problemas e incidentes

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 responsable del proceso 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 Auditoría	Entrevista a un empleado del área de TI. Entrevista a un empleado de soporte técnico.	No existen documentos de respaldo de seguimiento de problemas	No se realiza seguimiento de los problemas resueltos o inconclusos, ni se hace un seguimiento de pistas de auditoría.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 48
Modelo de Madurez DS10

Dominio: Entregar 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.		X	Grado de Madurez. El proceso de administración de problemas e incidentes se encuentra en un nivel 0 Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.		X	
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.		X	
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.	X		
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.	X		
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.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS10 la necesidad de cumplir con los siguientes objetivos de control.

- Sistema de administración de Problemas
- Escalamiento de Problemas

- Seguimiento de Problemas y Pistas de Auditoría
- Autorizaciones de acceso temporal y de emergencia
- 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 4.1, se recomiendan las siguientes:

Tabla 49
Resumen DS12

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 Organización.
Estrategias a largo plazo	Definir prioridades para mitigar riesgos, y reconocer incidentes. Realizar un seguimiento de problemas y pistas de auditoría.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 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 empleados, proveedores, equipo y personal de mantenimiento de las instalaciones

Los procedimientos y prácticas de administración de llave y lectora de tarjetas 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

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 visitante, 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 de 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

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

Tabla 50
DS12 Administración de instalaciones

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 responsable del proceso 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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 51
Modelo de Madurez DS12

Dominio: Entregar 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.		X	Grado de Madurez. El proceso de administración de instalaciones se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.		X	
Nivel 2	Los controles ambientales se implementan y monitorean por parte del personal de operaciones.		X	
Nivel 3	Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado.	X		
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.		X	
Nivel 5	Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente cómputo de la organización.		X	

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el DS12 la necesidad de cumplir con los siguientes objetivos de control.

- Seguridad Física
- Bajo Perfil de las Instalaciones de Tecnología de Información
- Escolta de Visitantes
- Salud y Seguridad del Personal

- Protección contra Factores Ambientales
- 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 4.1, se recomiendan las siguientes:

Tabla 52
Resumen DS12

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.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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 del Día “IESS Zamora” que nos plantea COBIT 4.1, 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 inexistencia de controles en los sistemas de información, 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 la infraestructura que se encuentra 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 (talento humano, 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.

Tabla 53
M1 Monitoreo de los procesos

Objetivos de Control	Pruebas realizadas	Documentos de respaldo	Resultados de la evaluación
M1.2 Evaluar el Desempeño	Entrevista al responsable del proceso de TI. Entrevista al gerente de servicios	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 responsable del proceso de TI. Entrevista a una secretaria del hospital.	No existen documentos de respaldo de la satisfacción del cliente.	La satisfacción de los usuarios del departamento de TI es alta, a pesar de no llevarse un control al momento de brindar soporte y mantenimiento.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

Tabla 54
Modelo de Madurez 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.		X	Grado de Madurez. El proceso de monitoreo de procesos se encuentra en un nivel 0. Objetivos no Cumplidos En el Hospital del Día "IESS Zamora" 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.		X	
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.		X	
Nivel 3	La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo.		X	
Nivel 4	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	X		
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.	X		

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

COBIT 4.1 plantea para el M1 la necesidad de cumplir con los siguientes objetivos de control.

- Recolectar Datos de Monitoreo
- Evaluar el Desempeño
- Evaluar la Satisfacción del Cliente

- 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 4.1, se recomiendan las siguientes:

Tabla 55
Resumen M1

Estrategias a corto plazo	Recolectar información sobre el desempeño del personal de TI y la satisfacción de los usuarios 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 usuarios 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 usuarios del área de TI para la toma de decisiones.

Fuente: (IT Governance Institute. COBIT, 2010, ITIL, 2005)

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.

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 y de nivel de complejidad dl Hospital.

INFORME FINAL DE AUDITORÍA

1. En la evaluación general del dominio de adquirir e implementar del Hospital del Día “IESS Zamora”, que nos plantea COBIT 4.1, aporta un resultado que oscilan entre los niveles 0 y 1 de los respectivos niveles de madures de COBIT 4.1. Lo cual nos hace pensar en que se deben realizar correcciones para mejorar la unidad de TI.

2. Para este dominio se puede notar que los procesos evaluados, tienen 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, evidenciándose un control más exhaustivo para con el hardware del hospital, sin dejar de lado el software.

3. 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.

4. 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 demuestra otro problema cuando ocurren incidentes ya que no se dispone de repuestos para poder solventar este incidente.

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

6. 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.

7. Para el dominio de entregar y dar soporte, dentro de la evaluación del Hospital del Día “IESS Zamora” que nos plantea COBIT 4.1, 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 inexistencia de controles en los sistemas de información, 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.

8. 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.

9. Otro factor determinante para los resultados de estas evaluaciones es la infraestructura que se encuentra 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.

10. 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.

11. 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 un control de satisfacción de usuarios internos y externos para realizar escalamientos de problemas en base a procedimientos establecidos.

12. 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.

13. 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 usuarios 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.

14. 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 y de nivel de complejidad del Hospital.

CONCLUSIONES

Luego de realizar el proceso investigativo, se sintetizan las siguientes conclusiones, que engloban todos los hechos observados durante el desarrollo de los momentos del proyecto:

- Se logró conocer el contexto tecnológico actual de la Entidad en relación a los conceptos de vulnerabilidad de la información y alineamiento estratégico, con el fin de establecer criterios de seguridad de la información.

- COBIT 4.1 contiene cuatro componentes como guías de auditoría; la primera nos guía en la obtención del entendimiento de los procesos del negocio, la segunda son preguntas que conllevan a la evaluación de la empresa por medio de su comparación con la tercera parte que es la que contiene respuestas y una última parte, nos permite comprobar el riesgo de la empresa, en el caso de no cumplir con los objetivos de control; todo esto nos permite realizar una auditoría de manera general para TI; durante el desarrollo de este proyecto, se ha determinado que las guías de auditoría de COBIT son las más apropiadas para determinar los riesgos que posee una Entidad.

- Mediante un marco de referencia de COBIT, se ha podido evaluar como diagnosticar los procesos de TI en el Hospital del IESS Zamora. También se ha determinado cada uno de los criterios de información, con este estudio se ha dado un conjunto de directrices las cuales pueden alinear el TI con el negocio, se identificó riesgos, gestionar recursos y medir el desempeño, como los niveles de madurez en cada uno de los procesos.

- El usar una metodología de control cualquiera que sea planteada es muy importante tomar en cuenta la colaboración y predisposición de los involucrados, ya que cualquier control que se

implemente únicamente tendrá efecto el momento en que la gente tome conciencia de la importancia y contribución que se promete a su desempeño.

RECOMENDACIONES

Una vez indicadas las conclusiones, se indican las respectivas recomendaciones, relacionadas a aspectos propositivos y de generación de mejora continua en la organización investigada.

- En el Hospital del Día IESS Zamora de acuerdo a la auditoria aplicada, se recomienda mantener un monitoreo global de TI, tomando como punto de partida el marco de trabajo descrito en este proyecto, para iniciar acciones correctivas en base a la evaluación periódica del desempeño de los procesos contra las metas, y para mantener niveles óptimos de seguridad, calidad y eficiencia.

- Para mejorar los procesos de TI El estándar COBIT ofrece una completa guía de alto nivel para la definición y evaluación de los procesos de negocios relacionados con TI. Asimismo, provee prácticas enfocadas al mejoramiento del control de los objetivos claves para una mejor implementación del gobierno de TI.

- Es necesario considerar los objetivos de control para poder llegar a una meta, pasando por políticas, procedimientos, prácticas y estructuras organizadas para proveer un aseguramiento más razonable, esto en conjunto con una información oportuna y condensada.

BIBLIOGRAFÍA

- Auditoría de Sistemas. (2013). Obtenido de (Echenique García, 2001) http://www.auditoriasistemas.com
- Bethancourt, L. (2004). POLÍTICAS TI. Venezuela: 4ta.
- Datamation Management and Technology. (Noviembre de 2013). Obtenido de Marco de Referenc (Solis, 2007)ia COBIT: http:// datamation.cubika.com
- Echenique García, J. (2001). *Auditoría en Informática.* México: 2da. Ed.
- Guidelines. (Octubre de 2008). *Governance Institute*. Obtenido de http://www.isaca.org
- A., G. (2013). Objetivos de Control para la Información, CISA. USA: 2da.
- Guidelines. (Octubre de 2008). Governance Institute. Obtenido de http://www.isaca.org Institute, G. (2013). COBIT. USA: 3ra.
- Institute, G. (2007). COBIT 4.1. USA: EXECUTIVE SUMMARY FRAMEWORK, 4ta.
- Solis, G. A. (2007). Systems Audit and Control Association. USA: 4ta.