



UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

**CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E
INFORMÁTICOS**

TEMA:

**MANUAL TÉCNICO DE PROCESOS BASADO EN NORMATIVA
INTERNACIONAL PARA LA GESTIÓN DE RIESGOS INFORMÁTICOS EN
EL DEPARTAMENTO DE SISTEMAS DEL HOSPITAL PROVINCIAL
DOCENTE AMBATO**

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

SUBLÍNEA DE INVESTIGACIÓN: Administrativas Informáticas

AUTOR: Santiago Fabián Chuncha Benalcázar

TUTOR: Ing. Mg. Galo Mauricio López Sevilla

**AMBATO – ECUADOR
2014**

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación sobre el tema: **“Manual Técnico de Procesos Basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato”**, del señor Santiago Fabián Chuncha Benalcázar, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para obtener el título terminal de tercer nivel de la Universidad Técnica de Ambato.

Ambato Agosto, 2014

EL TUTOR

.....
Ing. Galo Mauricio López Sevilla

AUTORÍA

El presente trabajo de investigación titulado: “**Manual Técnico de Procesos Basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato**”, es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato Agosto, 2014

.....
Santiago Fabián Chuncha Benalcázar
CC: 1803369311

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Jaime Ruiz, Ing. Renato Urvina, revisó y aprobó el Informe Final del trabajo de graduación titulado **“Manual Técnico de Procesos Basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato”**, presentado por la señor Santiago Fabián Chuncha Benalcázar de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

.....

Ing. Mg. José Vicente Morales Lozada

PRESIDENTE DEL TRIBUNAL

.....

Ing. Mg. Jaime Bolívar Ruiz Banda

DOCENTE CALIFICADOR

.....

Ing. Mg. Klever Renato Urvina Barrionuevo

DOCENTE CALIFICADOR

DEDICATORIA

Agradezco de todo corazón a mis padres y abuelos, reciban esta dedicación como un homenaje a su grandeza por brindarme siempre su apoyo incondicional en cada momento de mi vida.

A mis hermanos, familiares, compañeros de carrera y amigos quienes me han brindado su apoyo para lograr alcanzar esta meta; prometo no defraudarlos nunca, por creer en mí solo me resta decirles Muchas Gracias.

Santiago Fabián Chuncha Benalcázar

AGRADECIMIENTO

A Dios en primer lugar por darme la vida, Bendecirme, porque solo por su gracia y amor me ha permitido terminar una más de mis metas, sólo con su ayuda y guía.

También quiero expresar mis agradecimientos a la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato y a mis maestros por sus sabios conocimientos que encaminaron al desarrollo exitoso de mi vida estudiantil.

Santiago Fabián Chuncha Benalcázar

PÁGINAS PRELIMINARES

Portada.....	i
Aprobación del Tutor.....	ii
Autoría de Tesis.....	iii
Aprobación de la Comisión Calificadora.....	iv
Dedicatoria.....	v
Agradecimiento.....	vi
Índice de Contenidos.....	vii
Índice de Tablas.....	xi
Índice de Figuras.....	xiii
Resumen Ejecutivo.....	xv
Summary.....	xvi
Introducción.....	xvii

ÍNDICE DE CONTENIDOS

CAPITULO I EL PROBLEMA DE INVESTIGACIÓN

1.1 TEMA	1
1.2 PLANTEAMIENTO DEL PROBLEMA.....	1
1.3 DELIMITACIÓN DE CONTENIDOS.....	2
1.4 JUSTIFICACIÓN	3
1.5 OBJETIVOS	4
1.5.1 Objetivo General.....	4
1.5.2 Objetivos Específicos	4

CAPITULO II MARCO TEÓRICO

2.1	MARCO TEÓRICO	5
2.1.1	Seguridad Informática.....	5
2.1.2	Sistema de Seguridad Informática	6
2.1.2.1	Riesgos Informáticos.....	6
2.1.2.2	Gestión de Riesgos Informáticos.....	6
2.1.2.3	Análisis de Riesgos Informáticos.....	7
2.1.3	Matriz de análisis de riesgo	7
2.1.3.1	Parámetros para elaborar una matriz de riesgos.....	9
2.1.4	Procedimiento de Seguridad.....	12
2.1.5	Políticas de seguridad	13
2.1.6	Políticas de Administración.....	13
2.1.7	Plan de seguridad.....	13
2.1.8	Normativas Internacionales	14
2.1.8.1	Normativa ISO/IEC 17799:2005	14
2.1.8.2	Normativa Serie ISO 27000.....	17
2.1.8.3	Normativa ISO/IEC 27001	20
2.1.8.4	Cobit	25
2.1.8.5	Itil	36
2.1.9	Modelo de Madurez.....	39

CAPITULO III METODOLOGÍA

3.1	MODALIDAD DE LA INVESTIGACIÓN	41
3.1.1	Investigación de Campo	41
3.1.2	Investigación Bibliográfica-Documental	41
3.1.3	Investigación Aplicada	41
3.2	RECOLECCIÓN DE LA INFORMACIÓN	41
3.3	PROCESAMIENTO DE LA INFORMACIÓN.....	41
3.3.1	Análisis e Interpretación de Resultados.....	42
3.4	DESARROLLO DEL PROYECTO	42

CAPITULO IV DESARROLLO DE LA PROPUESTA

4.1. ETAPA 1 - PRÁCTICAS ACTUALES.....	46
4.1.1 Análisis de Procedimientos.....	46
4.1.2 Clasificación de Riesgos.....	49
4.1.3 Reducción de Riesgos.....	55
4.1.4 Control de Riesgos.....	62
4.2. ETAPA 2 - REGLAMENTOS Y POLÍTICAS VIGENTES.....	71
4.2.1 Revisión de Políticas de Administración del Departamento de Sistemas.....	71
4.2.2 Análisis y Delimitación de Áreas Críticas.....	72
4.2.3 Pruebas de Riesgos.....	72
4.3. ETAPA 3 - NORMATIVAS INTERNACIONALES.....	77
4.4. ETAPA 4 - ENTORNO COMPETITIVO.....	83
4.4.1 Establecimiento de Procesos y Funciones del Departamento de Sistemas.....	83
4.4.2 Funciones del Departamento de Sistemas.....	88
4.5. DESARROLLO DEL MANUAL DE PROCESOS.....	92
4.5.1. Manual Técnico de Procesos Organizativos.....	106
4.5.2. Manual Técnico Procesos de Recursos Físicos.....	114
4.5.3. Manual de Procesos Técnicos.....	121
4.5.4. Manual Técnico de Procesos Personales.....	136
4.5.5. Manual Técnico de Procesos contra Acciones Hostiles.....	156
4.5.6. Resumen de análisis actual de procesos.....	162

CAPITULO V EL PROBLEMA DE INVESTIGACIÓN

CAPITULO V.....	173
5.1 CONCLUSIONES.....	173
5.2 RECOMENDACIONES.....	174

BIBLIOGRAFÍA.....	175
GLOSARIO DE TÉRMINOS	180
ANEXOS.....	183

ÍNDICE DE TABLAS

Tabla 2.1 Resumen de Normativa ISO/IEC 17799:2005.....	17
Tabla 2.2 Resumen de Normativa Serie ISO 27000	20
Tabla 4.3 Resumen de Normativa Serie ISO 27001	25
Tabla 2.4 Resumen de Normativa Serie ISO 27001	36
Tabla 2.5 Resumen de Normativa ITIL.....	39
Tabla 4.1 Encuesta de Riesgos en Actos originados por la criminalidad común	49
Tabla 4.2 Encuesta de Riesgos en Sucesos de Origen físico.....	50
Tabla 4.3 Encuesta de Riesgos en Sucesos derivados de decisiones institucionales y	51
Tabla 4.4 Encuesta de Riesgos en los Datos e Información.....	52
Tabla 4.5 Encuesta de Riesgos en Sistemas e Infraestructura.....	53
Tabla 4.6 Encuesta de Riesgos en Personal	54
Tabla 4.7 Comparativa de Normas Internacionales	80
Tabla 4.8 Comparativa de Normativa según sus Fortalezas.....	81
Tabla 4.9 Comparativa de Normativa según sus Debilidades.....	82
Tabla 4.10 Comparativa de Normativa según sus Funciones	82
Tabla 4.11 Comparativa de Normativa según sus Áreas	82
Tabla 4.12 Comparativa de Normativa según su Creador	83
Tabla 4.13 Comparativa de Normativa según su Utilidad	83
Tabla 4.14 Manual de Procesos: Gestionar el marco de gestión de TI – Procesos Organizativos	113
Tabla 4.15 Manual de Procesos: Gestionar la Seguridad – Procesos de Recursos Físicos.....	121
Tabla 4.16 Manual de Procesos: Gestionar la Arquitectura Empresarial – Procesos Técnicos.....	129

Tabla 4.17 Manual de Procesos: Gestionar los servicios de Seguridad – Procesos Técnicos.....	136
Tabla 4.18 Manual de Procesos: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno – Procesos Personales.....	143
Tabla 4.19 Manual de Procesos: Gestionar el marco de gestión de TI – Procesos Personales	150
Tabla 4.20 Manual de Procesos: Gestionar la arquitectura Empresarial – Procesos Personales	156
Tabla 4.21 Manual de Procesos: Gestionar los activos – Procesos contra acciones Hostiles.....	162
Tabla 4.22 Datos Procesos Organizativos	164
Tabla 4.23 Datos Procesos Físicos.....	165
Tabla 4.24 Grado de madurez de Procesos Técnicos	167
Tabla 4.25 Encuesta de Procesos Personales.....	170
Tabla 4.26 Encuesta de Procesos contra Acciones Hostiles	171

ÍNDICE DE FIGURAS

Fig. 2.1 Matriz de Análisis de Riesgo	8
Fig. 2.2 Detalle de la Matriz de Análisis de Riesgo	9
Fig. 4.1 Diagrama de Flujo para elaboración de Matriz de Análisis de Riesgo	48
Fig. 4.2 Matriz de Análisis de Riesgo para Elementos de Información “Datos”	56
Fig. 4.3 Matriz de Análisis de Riesgo para Elementos de Información “Datos”	57
Fig. 4.4 Matriz de Análisis de Riesgo para Elementos de Información “Sistema e Infraestructura”	58
Fig. 4.5 Matriz de Análisis de Riesgo para Elementos de Información “Sistema e Infraestructura”	59
Fig. 4.6 Matriz de Análisis de Riesgo para Elementos de Información “Personal”	60
Fig. 4.7 Matriz de Análisis de Riesgo para Elementos de Información “Personal”	61
Fig. 4.8 Matriz Análisis de Riesgo	63
Fig. 4.9 Matriz Análisis de Riesgo Sistemas e Infraestructura por Negligencia de Usuarios y decisiones Institucionales	63
Fig. 4.10 Matriz Análisis de Riesgo Sistemas e Infraestructura por Criminalidad y Sucesos Físicos	66
Fig. 4.11 Matriz Análisis de Riesgo Datos e Información por	

Negligencia de Usuarios y Decisiones Institucionales.....	68
Fig. 4.12 Matriz Análisis de Riesgo Datos e Información por	
Criminalidad y Sucesos Físicos	69
Fig. 4.13 Matriz Análisis de Personal en todos los Riesgos	70
Fig. 4.14 Encabezado del formato de Control de Trabajo / Equipos	73
Fig. 4.15 Cuerpo del formato de Control de Trabajo / Equipos	74
Fig. 4.16 Pie de página del formato de Control de Trabajo / Equipos	74
Fig. 4.17 Cabecera de formato de Mantenimiento de Equipos	75
Fig. 4.18 Estructura Orgánica – Hospitales Generales, Especializados	
y de Especialidades de 70 camas o más	84
Fig. 4.19 Descripción del Proceso.....	93
Fig. 4.20 Descripción del Proceso.....	93
Fig. 4.21 Descripción del Proceso.....	93
Fig. 4.22 Descripción del Proceso.....	93
Fig. 4.23 Descripción del Proceso.....	94
Fig. 4.24 Descripción del Proceso.....	94
Fig. 4.25 Descripción del Proceso.....	94
Fig. 4.26 Análisis de madurez de procesos Organizativos.....	164
Fig. 4.27 Análisis de madurez de Procesos Físicos.....	166
Fig. 4.28 Análisis de madurez de Procesos Técnicos.....	168
Fig. 4.29 Análisis de madurez de Procesos Personales	170
Fig. 4.30 Análisis de madurez de Procesos contra acciones hostiles	171

RESUMEN EJECUTIVO

El Departamento de Sistemas del Hospital Provincial Docente Ambato es un departamento que se encarga del manejo de procesos, el uso y el aprovechamiento de la Tecnología para alcanzar el desempeño ideal de esta Institución de Salud.

Toda empresa u organización sea esta pública o privada demuestran su eficiencia a través de la forma en que gestionen sus procesos, potenciando cada uno de los departamentos administrativos, en particular el informático, que con los grandes avances tecnológicos son uno de los cuales deben estar permanentemente actualizados y protegidos especialmente ante los diferentes riesgos informáticos esto permite que se pueda cumplir con los objetivos de mediano y largo plazo satisfaciendo los requerimientos de los usuarios tanto internos como externos.

Esta investigación propone el desarrollo de un Manual de Procesos que estará fundamentada bajo una normativa Internacional la cual permitirá organizar, optimizar y agilizar los procesos que el Departamento de Sistemas provee a los demás Departamentos de la Institución.

Existe una clara necesidad de asegurar la información ante eventuales vulnerabilidades que se pueden ver afectadas por amenazas y la mayoría de instituciones no cuentan con planes de seguridad ante los riesgos informáticos, por lo que la investigación propone establecer herramientas para evaluar y controlar los riesgos informáticos en el Hospital Regional Ambato, para contribuir a una mejora continua en esta área.

SUMMARY

The Department of Provincial Teaching Hospital Systems Ambato is a department in charge of managing processes, the use and exploitation of the technology to achieve the ideal performance of the health institution.

Every business or organization whether public or private show their efficiency through the way they manage their processes, enhancing each of the administrative departments, including the computer, with the technological advances are one of which must be permanently updated and specially protected against different computer risk that permits you to meet the objectives of medium and long term to meet the requirements of both internal and external users.

This research proposes the development of a Manual Process - be based on an international standard which allow - organize, optimize and streamline processes Systems Department provides to other departments of the institution.

There is a clear need for secure information against possible vulnerabilities that may be affected by threats and most institutions do not have plans to computer security risks, so research proposes to establish tools to assess and control risks in computer Ambato Regional Hospital, to contribute to continuous improvement in this area.

INTRODUCCIÓN

La presente investigación cuyo tema es, “Manual Técnico de Procesos Basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato”; la misma que está integrada por cinco capítulos que organizan el análisis del tema:

Capítulo I. “El Problema”, este capítulo orienta la contextualización de la problemática que representa los riesgos informáticos para el Hospital regional, que permite organizar un análisis crítico delimitando su alcance, justificando la importancia del tema y planteando los objetivos.

Capítulo II. “Marco Teórico”, comprende los antecedentes investigativos enmarcados por diversas fundamentaciones teóricas para en un marco conceptual y finalmente presentar la propuesta de solución.

Capítulo III. “Metodología”, se presenta el enfoque; la modalidad y el tipo de investigación; la técnica para obtener información, se detalla los pasos a seguir mediante una breve descripción de cómo se desarrollará el proyecto.

Capítulo IV. “Desarrollo de la Propuesta”, en este capítulo se describe todo el proceso que se ha seguido para dar solución al proyecto de investigación, desarrollando los pasos que fueron necesarios para lograr el Objetivo General del Proyecto.

Capítulo V. “Conclusiones y Recomendaciones”, en donde menciona las conclusiones a las que el investigador llega una vez desarrollado el proyecto, así como las recomendaciones pertinentes.

Y por último se encuentra los anexos y referencias correspondientes al trabajo investigativo.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 TEMA

“Manual Técnico de Procesos basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato”

1.2 PLANTEAMIENTO DEL PROBLEMA

En la actualidad la inseguridad de la información y los diversos riesgos Informáticos son una problemática que alcanza a todos los niveles de la sociedad, debido a que el inadecuado control, manejo y administración de dispositivos, medios de transmisión, protocolos de comunicación etc., no se los está realizando bajo estándares y normas internacionales que orienten dichos procesos; la tecnología es el eje principal de la sociedad, economía, y desarrollo de los pueblos pero también se observa cómo el mundo está viviendo una crisis informática.

Grandes países como Estados Unidos de América, Europa, entre otros, han evolucionado tecnológicamente con el fin de prestar mejores y oportunos servicios; pero conjuntamente con este cambio, los fraudes tecnológicos han tomado también un avance para la vulnerabilidad de seguridades por lo que en la actualidad cada vez más organismos están tomando mayores seguridades para prevenir caer ante esta amenaza.

En el Ecuador han existido casos en que el uso inadecuado de conocimientos Informáticos ha permitido vulnerar los sistemas Informáticos, Bases de Datos y Redes de Comunicación; casos que han logrado hacer un gran daño a organizaciones, a la dignidad de las personas y el bien común de la sociedad; el diario ‘Hoy’ en su edición digital menciona que en el Ecuador se producen al menos “Cinco delitos informáticos cada día” entre los principales el phishing, fuga de información, manipulación de programas, manipulación de datos de

entrada y salida, siendo estos datos el mayor bien intangible dentro de una organización; es el riesgo latente en las organizaciones que están implementando nuevas tecnologías, y a la par también aparecen mayores riesgos de ataques contra la confidencialidad de su información [1].

En el departamento de sistemas del Hospital Provincial Docente Ambato, se presenta como problema principal un incremento de riesgos informáticos causado por la falta de un manual técnico de procesos, el mismo que no existe por falta de recursos necesarios para su elaboración; además al no contar con una adecuada gestión de riesgos informáticos tiene vulnerada su información ya que no se cuenta con controles o auditorías por lo que es una necesidad prioritaria planear, implementar, controlar y evaluar los riesgos informáticos.

Mantener una actualizada gestión de procesos, responder a las demandas de la sociedad tecnológica y prevenir la fuga de información es un desafío que incumbe a todos los miembros de una institución desde los directivos hasta sus operativos, ya que mientras más personas comprendan la problemática de la seguridad de la tecnología informática se podrá proteger los recursos ante las amenazas cibernéticas e inseguridad de la información.

1.3 DELIMITACIÓN DE CONTENIDOS

- **Área:** Administrativas Informáticas
- **Línea:** Normas y Estándares
- **Sublíneas:** Normas de Calidad de Unidades Informáticas
Estándares de Calidad
Seguridad de Unidades Informáticas
- **Temporal:** Seis meses a partir de la aprobación
- **Espacial:** La investigación se realizará en el Departamento de Sistemas del Hospital Provincial Docente Ambato.

1.4 JUSTIFICACIÓN

El interés por realizar la investigación se da porque las empresas mantienen falencias respecto a los riesgos informáticos, lo cual significa gestionar integralmente cada una de las operaciones que un sistema tecnológico informático ejecuta dentro de una institución, identificando los puntos críticos de la organización que soportan de alguna manera la estrategia definida y hacer foco en estos; como es el caso del Hospital Provincial Docente Ambato que necesita desarrollar en su departamento de sistemas a partir de un proceso eficiente que le evite el incremento de riesgos informáticos.

Se revisará la teoría referente a la normativa internacional para poder aplicar en la práctica diaria del departamento de sistemas del Hospital Ambato y mantenerse a la vanguardia tecnológica; es novedoso organizar un manual técnico de procesos en seguridad informática porque permitirá que otras instituciones de salud lo tomen de referencia para mejorar la seguridad de la información donde los principales beneficiarios serán el personal del Hospital Docente Ambato, y sus pacientes ya que toda la información que se maneja estará resguardado y bajo procedimientos.

El tema tiene un impacto técnico, económico y teórico importante en tanto que mejorando los procesos de un departamento se puede desplegar mejoras al resto de áreas que dependen de él en la parte técnica, logrando un ahorro de recursos económicos y teórico porque puede ampliar la visión y servir de ejemplo para otras instituciones que estén pasando la misma problemática. Se cuenta con toda la factibilidad técnica, operativa, política para realizar la investigación en tanto existe el conocimiento necesario y el apoyo científico para solucionar la problemática planteada.

1.5 OBJETIVOS

1.5.1 Objetivo General

- Elaborar un Manual Técnico de Procesos basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato

1.5.2 Objetivos Específicos

- Analizar el manejo actual de los procedimientos y detectar los riesgos informáticos existentes en el Departamento de Sistemas del Hospital Provincial Docente Ambato.
- Delimitar y definir las áreas críticas relacionadas con dichos riesgos de fuga o manipulación de información en el Departamento de Sistemas del Hospital Provincial Docente Ambato.
- Investigar la metodología de Normativa Internacional adecuada a las necesidades y recursos disponibles del Hospital Provincial Docente Ambato.
- Establecer los procesos y funciones correspondientes al Departamento de Sistemas del Hospital Provincial Docente Ambato para la elaboración de un Manual Técnico bajo criterios de manejo y aplicación metódica a la que estarán sujetas.
- Diseñar un Manual Técnico de Procesos bajo una Normativa Internacional apegado a la estructura y al manejo de procesos en el Departamento de Sistemas del Hospital Provincial Docente Ambato.

CAPÍTULO II MARCO TEÓRICO

2.1 MARCO TEÓRICO

Antecedentes

Una vez realizado varios análisis para reducir los riesgos informáticos y revisada la problemática de acuerdo con los repositorios de la Universidad Técnica de Ambato se puede anotar investigaciones realizadas.

GUACHI AUCAPIÑA, Tania Verónica en su tema “NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.”; argumenta que no se cuenta con estándares de seguridad informática que ayuden a preservar las propiedades de confidencialidad, integridad y disponibilidad de los sistemas de información y de comunicación ya que dicha información no se encuentra protegida con metodologías estandarizadas y en el mayor de los casos no se cuenta con una función que administre y controle los riesgos informáticos. Recomendando la implantación de la norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación adoptando una metodología para mantener y mejorar la seguridad de la información [2].

2.1.1 Seguridad Informática

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema. La seguridad informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad [3].

Además la seguridad informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada [4].

2.1.2 Sistema de Seguridad Informática

Es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados [3].

La seguridad informática debe garantizar:

- La disponibilidad de los sistemas de información.
- La recuperación rápida y completa de los sistemas de información
- La integridad de la información.
- La confidencialidad de la información [3].

2.1.2.1 Riesgos Informáticos

El riesgo se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños [5].

2.1.2.2 Gestión de Riesgos Informáticos

Es un método formal para investigar los riesgos de un Sistema Informático y recomendar las medidas apropiadas que deberían adaptarse para controlar

estos riesgos. A su vez es una salvaguardia preventiva que intenta buscar otras salvaguardas para proteger el Sistema de Información.

Introduce un enfoque riguroso y consecuente para la investigación de los factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa; señala los riesgos existentes, identificando las amenazas que afectan al sistema informático. [4].

2.1.2.3 Análisis de Riesgos Informáticos

Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Teniendo en cuenta que la explotación de un riesgo causaría daños o pérdidas financieras o administrativas a una empresa u organización, se tiene la necesidad de poder estimar la magnitud del impacto del riesgo a que se encuentra expuesta mediante la aplicación de controles. Dichos controles, para que sean efectivos, deben ser implementados en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo. [6]-[7].

2.1.3 Matriz de análisis de riesgo

La matriz de análisis de riesgo que “constituye en una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que

podieran impactar los resultados y por ende al logro de los objetivos de una organización.” [8]

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como matriz de riesgo. En este documento se muestran los elementos identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgo es indispensable para lograr una correcta administración del riesgo. La administración del riesgo hace referencia a la gestión de los recursos de la organización. Existen diferentes tipos de riesgos como el riesgo residual y riesgo total así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras. La fórmula para determinar el riesgo total es:

$$\text{RT (Riesgo Total)} = \text{Probabilidad} \times \text{Impacto Promedio}$$

A partir de esta fórmula se determina su tratamiento y después de aplicar los controles se puede obtener el riesgo residual [7].

1 = Insignificante (incluido Ninguna)

2 = Baja

3 = Mediana

4 = Alta

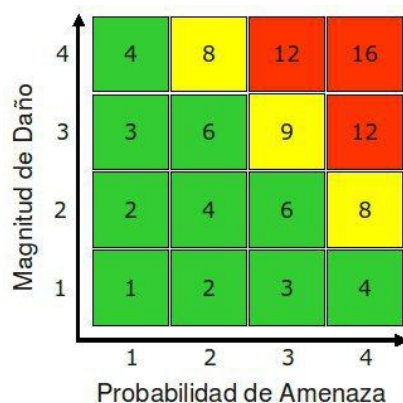





Fig. 2.1 Matriz de Análisis de Riesgo

Elaborado por: http://protejete.wordpress.com/gdr_principal/matriz_riesgo/

“El Riesgo, que es el producto de la multiplicación probabilidad de amenaza por magnitud de daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.” [8]

Bajo Riesgo = 1 – 6 (verde) 

Medio Riesgo = 8 – 9 (amarillo) 

Alto Riesgo = 12 – 16 (rojo) 

Riesgo = Probabilidad de Amenaza * Magnitud de Daño

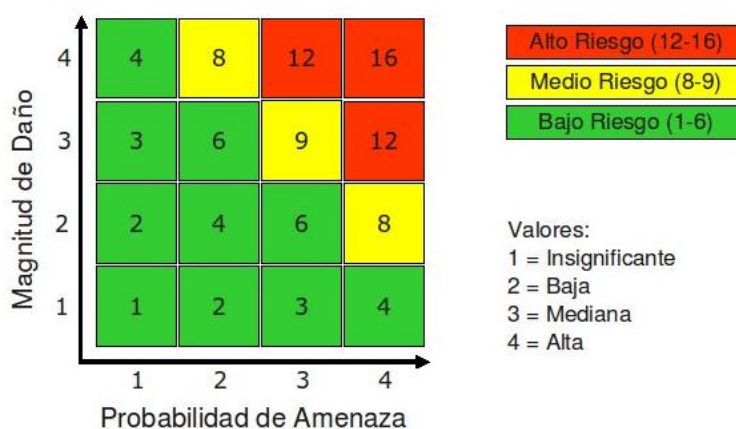


Fig. 2.2 Detalle de la Matriz de Análisis de Riesgo

Elaborado por: http://protejete.wordpress.com/gdr_principal/analisis_riesgo/

“La Matriz contiene una colección de diferentes amenazas y elementos de información. Para llenar la matriz, se estima los valores de la Probabilidad de amenaza por cada amenaza y la magnitud de daño por cada elemento de información.” [8]

2.1.3.1 Parámetros para elaborar una matriz de riesgos

Dentro de los parámetros necesarios para elaborar la matriz de riesgos constan los siguientes:

Amenazas: que “es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos

de un sistema, en el caso de la seguridad informática, los elementos de información.

Generalmente se distingue y divide tres grupos

- **Criminalidad:** son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.
- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.
- **Negligencia y decisiones institucionales:** son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.” [9].

Elementos de Información: “son todos los componentes que contienen, mantienen o guardan información. Dependiendo de la literatura, también son llamados Activos o Recursos.

Son los Activos o Recursos de una institución que se debe que proteger, para evitar su pérdida, modificación o el uso inadecuado de su contenido, para impedir daños para dicha institución y las personas presentes en la información.

Generalmente se distingue y divide tres grupos

- **Datos e Información:** son los datos e informaciones en sí mismo.
- **Sistemas e Infraestructura:** son los componentes donde se mantienen o guardan los datos e informaciones.

- Personal: son todos los individuos que manejan o tienen acceso a los datos e informaciones y son los activos más difíciles de proteger, porque son móviles, pueden cambiar su afiliación y son impredecibles.” [10]

Medidas Personales: Mantienen el alto grado de habilidades, conocimientos y la competitividad en los usuarios, así como la optimización de recursos y manejo de equipos, de forma proactiva y operativa dentro de la Institución.

- Capacitación
- Sensibilización
- Contratación
- Funciones
- Recursos

Medidas Físicas: “Tiene que ver con la protección de los elementos físicos de una empresa u organización, como el hardware y el lugar donde se realizan las actividades sea edificio o habitaciones

- Acceso Físico del Personal
- Instalación Eléctrica
- Temperatura
- Agua
- Sistemas contra incendios
- Seguros
- Factores Externos.” [11]

Medidas Técnicas: “Conservan la integridad de la información (su no alteración, pérdida y robo) y en menor grado la confidencialidad de los datos personales.

- Sistemas de información
- Ficheros locales
- Equipos
- Elementos materiales que tratan los datos

- Inventarios
- Perfiles” [12]

Medidas Organizativas: “Garantizan la confidencialidad, integridad y seguridad de los datos en programas y sistemas informáticos, que se encuentran almacenados físicamente en un determinado dispositivo.

- Procedimientos
- Normas
- Estándares de Seguridad” [12]

Acciones Hostiles: Cuidan y Protegen los bienes físicos e información de la Institución, estas acciones están relacionadas a delitos premeditados (crimen) por personas externas e internas a la Institución como son:

- Robo
- Fraude
- Sabotaje y/o Vandalismo
- Intromisiones no Autorizadas a la Red

2.1.4 Procedimiento de Seguridad

Es la definición detallada de los pasos a ejecutar para llevar a cabo una tarea determinada. Los procedimientos de seguridad permiten aplicar e implantar políticas de seguridad que han sido aprobadas por la organización [5].

Por lo tanto se puede decir que es una expresión gráfica del sistema de seguridad informática, diseñado acorde a la realidad de la institución, constituyendo el documento básico donde se establecen los principios organizativos y funcionales de Seguridad Informática en una Entidad, determinando una serie de pasos para cumplir con una norma o garantizar que en la ejecución de actividades se considerarán determinados aspectos de seguridad. Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. Un procedimiento puede

apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad. [13].

2.1.5 Políticas de seguridad

Es una declaración de intenciones de alto nivel que cubren la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar las responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. [6].

Las políticas de seguridad definen qué se debe proteger en el sistema, mientras que los procedimientos de seguridad describen cómo se debe conseguir dicha protección. En definitiva, si se compara las políticas de seguridad con las leyes en un estado de derecho. Los procedimientos serían el equivalente a los Reglamentos aprobados para desarrollar y poder aplicar las Leyes. [6].

2.1.6 Políticas de Administración

Las Políticas recogen las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por lo tanto, ha de ser aprobada por la dirección. [14]

El objetivo principal de la política es el concientizar a todo el personal de una organización y en particular al involucrado directamente con el sistema de información, la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. [14]

2.1.7 Plan de seguridad

Al momento de documentar las medidas de seguridad actual de la institución se está mencionando de un plan de seguridad; el único objetivo de este plan será proteger o resguardar los activos informáticos de dicha Institución [15]

2.1.8 Normativas Internacionales

“Las normas son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo de la red organizacional. Una norma de seguridad establece unos requisitos que se sustentan en la política y que regulan determinados aspectos de seguridad.”
[16]

2.1.8.1 Normativa ISO/IEC 17799:2005

La ISO/IEC 17799:2005 es una guía de buenas prácticas, pero no especifica los requisitos necesarios que permitan un sistema de certificación necesario para la seguridad de la información.

Comprende a la totalidad de los activos de sistema de información de la organización, como el hardware, el software, la estructura de los datos, y el personal, incluye controles para direccionar una serie de problemas, como la provisión de outsourcing (tercerización) y la gestión de parches.

Provee a las organizaciones mejoras e información en la práctica de seguridad de la información, con acuerdos para la gestión para los proveedores de servicio, dispositivos móviles, tecnologías inalámbricas, códigos virales, con una adecuada administración de recursos humanos.

Factibilidad organizacional

Se utiliza para evaluar, implementar, mantener y administrar la seguridad de la información, busca la confidencialidad, la integridad y disponibilidad de la información para personas autorizadas

Brinda la guía para buenas prácticas, ofrece recomendaciones dirigidas a los responsables de la información, proporciona una base común para desarrollar normas de seguridad, es una norma no certificable, pero que recoge la relación

de controles a aplicar (o al menos, a evaluar) para establecer un Sistema de Gestión de la Seguridad de la Información (SGSI).

Factibilidad técnica

“Esta Norma establece directrices y principios generales para el comienzo, la implantación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización. Los objetivos descritos en esta norma internacional proporcionan una guía general basados en objetivos comúnmente aceptados para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma internacional están diseñados para ser implantados conforme a los requisitos identificados a partir de una evaluación del riesgo. La norma ofrece mejoras novedosas sobre las buenas prácticas en seguridad de la información. Por ejemplo, trata sobre cómo mejorar la gestión de los sistemas de seguridad contratados con empresas externas; los proveedores de servicios y subcontratistas; la mejora de la capacidad de manejo de los indicadores; cómo abordar los problemas de gestión de los parches, los dispositivos móviles, la tecnología inalámbrica y el código móvil malicioso a través de Internet; las mejoras en las buenas prácticas sobre gestión de recursos humanos y otras funciones de nueva aparición.” [17]

Beneficios que se obtiene implantando ISO/IEC 17799:2005

- “Aumento de la seguridad efectiva de los sistemas de información.
- Correcta planificación y gestión de la seguridad.
- Garantías de continuidad del negocio.
- Mejora continua a través del proceso de auditoría interna.
- Incremento de los niveles de confianza de nuestros clientes y partners.
- Aumento del valor comercial y mejora de la imagen de la organización.”

[18]

RESUMEN DE NORMATIVA ISO/IEC 17799:2005

Definición

- Denominado también como ISO 27002
- Guía de buenas practicas
- Es un proceso para evaluar, implementar, mantener y administrar la seguridad de la información.

Características

- Fue desarrollada en 1990 en Inglaterra.
- En 1995 el estándar BS 7799 es oficialmente presentado.
- En el 2000 la organización de estándares internacionales (ISO) incorpora la primera parte de la norma BS 7799 y se rebautizada como ISO 17799.
- También existen otras tales como la ISO 13335 e ISO 15408.
- Consta de 11 secciones.
- 39 objetivos de control.
- La versión 2005 del estándar incluye como secciones principales las siguientes:
 - Política de seguridad de la información.
 - Organización de la seguridad de la información.
 - Gestión de activos de información.
 - Seguridad de los recursos humanos.
 - Seguridad física y ambiental.
 - Gestión de las comunicaciones y operaciones.
 - Control de accesos.
 - Adquisición, desarrollo y mantenimiento de sistemas de información.
 - Gestión de incidentes en la seguridad de la información.
 - Cumplimiento.
 - Gestión de continuidad del negocio.

<p>Objetivos</p> <ul style="list-style-type: none"> • Facilitar una base común para las normas de seguridad. • Fomentar un método de gestión de seguridad, logrando las relaciones de confianza entre las organizaciones.
<p>Alcance</p> <ul style="list-style-type: none"> • Uno de los alcances es el aumento de la seguridad efectiva, evitando riesgos significativos en las empresas, que mejora la planificación y gestión de seguridad, la confianza de los clientes, la imagen de las organizaciones. • Las recomendaciones están dirigidas a todos aquellos responsables de iniciar, implementar y mantener sistemas de seguridad. • Una de las garantías es la preservación de la confidencialidad. • Solo quienes están autorizados por la organización podrán acceder a la información, lo cual evita riesgos informáticos claves como: <ul style="list-style-type: none"> ▪ Uso de información no autorizada ▪ Fraudes informáticos ▪ También preserva la integridad, logrando que la información y metodología implementada en los procesos de la organización sean exactos y completos. ▪ Disponibilidad rápida de la información y sus activos para los usuarios autorizados, cuando la organización lo requiera.

Tabla 2.1 Resumen de Normativa ISO/IEC 17799:2005

Elaborado por: Investigador

2.1.8.2 Normativa Serie ISO 27000

Proviene de la norma BS 7799 de British Standards Institution, facilita que las empresas u organizaciones tengan un conjunto de buenas prácticas para la gestión de la seguridad de la información.

Esta serie define los requisitos para un sistema de gestión de la seguridad de la información (SGSI), a través de tres enfoques, como la confidencialidad, integridad, y disponibilidad, garantizando la selección adecuada y proporcional de controles de seguridad, permite proteger la información, es recomendable para cualquier tipo de organización, pero sobre todo para aquellas que manejen información crítica o información de otras organizaciones.

De la serie la norma ISO 27001 (la principal de la familia) es certificable, puede tardar en su implementación de 6 a 12 meses, siempre dependerá del nivel de seguridad de la información, su alcance, responsables, se requerirá de consultora externa y de capacitación continua.

Una certificación es aquella que ayuda a gestionar los valiosos activos de la información, norma internacional auditable, garantizando la selección de controles de seguridad más adecuados y que permite organizar la seguridad de la información, en cualquier tipo de organización privada, pública, con o sin fines de lucro

Contiene una serie de términos y definiciones que se emplean en todas las normas de la serie, que ayuda a la comprensión para la adecuada implementación, sobre todo para los responsables de los sistemas de seguridad de la información.

Resumen de Normativa Serie ISO 27000
<p>Definición:</p> <ul style="list-style-type: none">• Evolucionada a partir de BS 7799-2.• Es un sistema de gestión de la seguridad de la información (SGSI).• Es conjunto de estándares, es de utilidad para pequeñas, medianas y grandes empresas, desarrollado para la adecuada gestión de la información, mediante un proceso metódico, documentado, en base a objetivos y la evaluación de riesgos.

Características

- La ISO/IEC 27000 provee de una vista general a los estándares de la serie.
- Contiene un glosario de términos utilizados por la serie ISO/IEC 27000.
- Permite la especificación de los principios fundamentales, conceptos, definiciones y vocabulario para la serie ISO/IEC 27000.
- Contenidos:
 - a) Vista general de los estándares ISO/IEC 27000, muestra cómo se usan de manera colectiva para la planeación, implementación, certificación y operativización de los sistemas de administración de seguridad de la información.
 - b) Permite la administración de riesgos, mediante la implementación de procesos exactos y completos.
 - c) Establece definiciones claramente redactadas sobre los temas relacionados con la seguridad de la información, para que los responsables pueden manejarlo sin riesgos, garantizando la confidencialidad y acceso oportuno a la información.
 - d) Está compuesta a grandes rasgos por:
 - ISMS (Information Security Management System).
 - Valoración de Riesgo.
 - Controles.

Beneficios

- Brinda garantía a los controles internos.
- Cumplimiento de requisitos de gestión de la información.
- Permite el respeto a las leyes y normas de aplicación internacionales.
- Información segura garantía para los clientes.
- Identificación, planificación, evaluación y gestión de riesgos.
- Integración con otros sistemas de gestión de la organización.
- Reducción de costes de los procesos internos.
- Mejora de los procesos con un enfoque de gestión.

- Mayor motivación y satisfacción del personal por contar con directrices de trabajo claras.

Tabla 2.2 Resumen de Normativa Serie ISO 27000

Elaborado por: Investigador

2.1.8.3 Normativa ISO/IEC 27001

Tiene base en el estándar BS 7799, pero se la ha reorganizado para alinearse con otras normas internacionales de la serie ISO 27000, pero se incluye nuevos controles haciendo énfasis en las métricas para un adecuado sistema de seguridad de la información y la gestión de incidentes.

Se fundamenta en otras como la serie ISO 13335, ISO/IEC TR 18044:2004, ISO/IEC 17799:2005, y las “Directrices de la OCDE para Sistemas y Redes de Seguridad de la Información – Hacia una cultura de seguridad” que suministran orientación para la implementación de la seguridad de la información.

Es un proceso cíclico, deben implementarse de manera continua garantizando la eficacia del Sistema de Gestión de la Seguridad de la Información (SGSI).

“Los requisitos de la Norma ISO 27001 aportan a un Sistema de Gestión de la Seguridad de la Información (SGSI), consistente en medidas orientadas a proteger la información, indistintamente del formato de la misma, contra cualquier amenaza, de forma que se garantiza en todo momento la continuidad de las actividades de la empresa.

Los Objetivos del SGSI son preservar la:

- Confidencialidad
- Integridad
- Disponibilidad de la Información” [19]

Factibilidad organizacional

Establece objetivos y una metodología para la implementación de seguridad de la información, permite que una organización sea certificada, confirmando que la seguridad de la información se ha planificado, controlado e implementado de la mejor forma posible.

El sistema de seguridad de la norma ISO 27001 tiene cuatro fases, las cuales se implementaran en base a los enfoque de confidencialidad, integridad y disponibilidad de la información, que buscan que solo los usuarios autorizados tengan acceso a la información, mediante una adecuada metodología de procesos internos, logrando reducir los riesgos informáticos.

Las fases son las siguientes:

1. **Planificación:** ayuda a la planeación de la organización básica, define los objetivos de la seguridad de la información, permite escoger los controles adecuados de seguridad.
2. **Implementación:** implica la ejecución de las actividades.
3. **Revisión:** en cambio monitorea el funcionamiento de SGSI mediante los diversos canales y verifica los resultados en el cumplimiento de objetivos, y metas.
4. **Mantenimiento y Mejora:** ayuda a mejorar los incumplimientos detectados.

Beneficios que se obtiene implantando ISO 27001

- “Competitividad. ISO 27001 Asegura los activos de información de forma apropiada, evitando inversiones innecesarias o ineficientes.
- Confianza. Como prueba independiente del uso de prácticas adecuadas de cara a empresas y organizaciones, cliente final, auditores, tribunales, administración etc.

- Ventajas comerciales. ISO 27001, acredita a los clientes que la protección de su información es un objetivo primordial y ofrece garantía del cumplimiento de las obligaciones contractuales.
- Cumplimiento Legal. Es una demostración independiente del cumplimiento normativo que sea aplicable en cada caso
- Imagen. Las empresas certificadas en ISO 27001 mejoran su imagen pudiendo demostrar su compromiso en la mejora continua que esta herramienta proporciona a la organización.
- Reducción de riesgos, mejorando la garantía de continuidad del negocio identificando correctamente las amenazas y debilidades del sistema aplicando los controles adecuados para minimizar los riesgos.” [20]
- Otras de las ventajas de las normas ISO 27001, es el cumplimiento demostrando la rentabilidad de la inversión, debe cumplir con diversas normas sobre protección de datos, privacidad y control de TI.
- Permite brindar una ventaja de comercialización desarrollando un valor agregado a la empresa.
- Mejora en la imagen y relaciones con terceros.
- Mejora en el control de las personas.
- Mejora en la gestión de continuidad del negocio
- Mejora en el registro de incidentes y debilidades.

Factibilidad económica

No se puede establecer un costo general porque variará dependiendo del tipo de empresa, el personal, de la existencia de sistemas de información como se menciona Dejan Kosutic: “el costo total de la implementación dependerá del tamaño de su organización (o del tamaño de la(s) unidad(es) de negocio que se incluirá(n) dentro del alcance de la norma ISO 27001), del grado crítico de la información (por ejemplo, la información de los bancos se considera más crítica y requiere un nivel de protección mayor), de la tecnología que utiliza la organización (por ejemplo, los centros de datos suelen tener mayores costos debido a sus complejos sistemas) y de las disposiciones legales

(generalmente, los sectores públicos y financieros están muy controlados en relación con la seguridad de la información)” [21].

Aunque en su implementación es necesario invertir a los siguientes costos:

- a. Costo de publicaciones y de capacitación
- b. Costo de asistencia externa
- c. Costo de tecnología
- d. Costo del tiempo de los empleados
- e. Costo de la certificación

Resumen de Normativa ISO/IEC 27001
Definición: <ul style="list-style-type: none">• Norma que permite brindar la seguridad de la información.• La única norma internacional auditable.• El ISO 27001:2005 es aceptado para la administración de seguridad.• Permite definir los requisitos para un sistema de gestión de la seguridad de la información (SGSI)
Objetivos <ul style="list-style-type: none">• El objetivo de la norma es gestionar los valiosos activos de la información de una empresa.
Características <ul style="list-style-type: none">• Establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI).• La única norma internacional auditable.• Genera la posibilidad de contar con estándar mejorado e integral en el trayecto de la historia de una empresa.• La norma contiene un catálogo de 133 posibles controles.• Es el estándar más adoptado por las empresas.• Es más flexible.

- Se logra acoplar a los procesos de las organizaciones.
- Los activos necesitan protección, desde la información digital, los activos físicos como computadoras y redes, los documentos de papel.
- Será clave para el desarrollo de competencias del personal para la protección técnica de la información contra los fraudes informáticos.
- Como la norma anterior tiene 3 puntos claves en términos de protección:
 - El primero es la confidencialidad, tendrán acceso a la información solo personas autorizadas.
 - La integridad, protege la precisión, los métodos para los procesos de la información, es decir, permite la protección integral de toda la información de una organización
 - Disponibilidad: Acceso a la información y activos relacionados solo a personas autorizadas cuando se requiere de manera rápida y oportuna

Descripción

- Permite la certificación un sistema de gestión de seguridad, más que solo establecer una norma de buenas prácticas.
- Demuestra que se han tomado las medidas necesarias para la protección adecuada de la información contra accesos y cambio no autorizados
- Adopta una aproximación al proceso de desarrollo, implementación, operación, monitoreo, mantenimiento continuo, revisión, y mejora, en base a la gestión de la seguridad de la información, con una adecuada administración y planificación organizacional.
- La norma ISO 27001 está alineada con otros sistemas de gestión y soporta la implementación y la operación coherente e integrada con normas de gestión relacionadas.
- Está alineada con otros sistemas de gestión relacionados, está en armonía con la ISO 9001 e ISO 14001.
- Pone énfasis en la administración y mejora y continúa procesos para el

<p>sistema de gestión de seguridad.</p> <ul style="list-style-type: none"> • Permite claridad en los requisitos de documentación y registros del sistema de gestión de la información • Logra la implementación de procesos de evaluación y gestión de los riesgos mediante el modelo denominado PDCA, en base a cuatro puntos fundamentales, Planificar, Hacer, Verificar, Actuar.
<p>Documentos de ISO 27001</p> <p>La norma ISO 27001 requiere los siguientes documentos:</p> <ul style="list-style-type: none"> • El alcance del SGSI. • La política del SGSI. • Procedimientos para control de documentación, auditorías internas. • Procedimientos para medidas correctivas y preventivas. • Todos los demás documentos, según los controles aplicables. • Metodología de evaluación de riesgos. • Informe de evaluación de riesgos. • Declaración de aplicabilidad. • Plan de tratamiento del riesgo. • Registros.

Tabla 4.3 Resumen de Normativa Serie ISO 27001

Elaborado por: Investigador

2.1.8.4 Cobit

Cobit acrónimo en inglés de Control Objectives for Information and related Technology y su traducción al español como Objetivos de Control para Tecnología de la Información y Relacionada; fue creada y desarrollada por Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI).

“Cobit es una metodología aceptada mundialmente para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos que éstas

implican. La metodología Cobit se utiliza para planear, implementar, controlar y evaluar el gobierno sobre TIC; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Permite a las empresas aumentar su valor TIC y reducir los riesgos asociados a proyectos tecnológicos. Ello a partir de parámetros generalmente aplicables y aceptados, para mejorar las prácticas de planeación, control y seguridad de las Tecnologías de Información.” [22]

“A la fecha, Cobit tiene cuatro versiones mayores publicadas:

En 1996, la primera edición de Cobit fue publicada. Esta incluía la colección y análisis de fuentes internacionales reconocidas y fue realizada por equipos en Europa, Estados Unidos y Australia.

En 1998, fue publicada la segunda edición; su cambio principal fue la adición de las guías de gestión. Para el año 2000, la tercera edición fue publicada y en el 2003, la versión en línea ya se encontraba disponible en el sitio de ISACA.

Fue posterior al 2003 que el marco de referencia de Cobit fue revisado y mejorado para soportar el incremento del control gerencial, introducir el manejo del desempeño y mayor desarrollo del Gobierno de TI.

En diciembre de 2005, la cuarta edición fue publicada y en Mayo de 2007, se liberó la versión 4.1 que es la que actualmente se maneja.

La versión número 5 de Cobit se liberó en el 2012, esta edición consolidará e integrará los marcos de referencia de Cobit 4.1. Este nuevo marco de referencia viene integrado principalmente del Modelo de Negocios para la Seguridad de la Información y el Marco de Referencia para el Aseguramiento de la Tecnología de la Información.” [23].

El modelo Cobit es el marco aceptado internacionalmente de buenas prácticas para el control de la información TI y los riesgos que conllevan. Cobit se usa para implementar el gobierno de TI y mejorar los controles de TI. De igual

manera, contiene objetivos de control, directrices de aseguramiento, mediciones de desempeño y resultados, factores críticos de éxito y modelos de madurez.

“Cobit es un marco de gestión de TI y un conjunto de herramientas de soporte para el gobierno de TI, que permite a los gerentes cubrir la brecha entre los requisitos de control, los aspectos técnicos y riesgos de negocio.”

Cobit hace viable el desarrollo de una política clara y buenas prácticas para los controles de TI a través de las organizaciones.

Cobit hace énfasis en la conformidad de las regulaciones; ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de Cobit.” [24].

Contextualización

“En el 2011, tres de cada diez empresas en Latino América encuestadas por ISACA, experimentó una brecha de seguridad y 16% ha enfrentado problemas de seguridad en los dispositivos móviles, esto de acuerdo con una encuesta global realizada entre más de 3,700 profesionales de TI que son miembros de ISACA.

Las fugas de datos y los problemas relacionados con los empleados encabezan la lista de los principales problemas de TI que representarán desafíos para la seguridad de la red de una organización. Los resultados de los participantes en América Latina están alineados con las amenazas identificadas en otras partes del mundo. Más del 50% de ellos, actualmente se encuentran utilizando marcos de referencia como Cobit 5, para el gobierno y administración de los activos y servicios de TI de la empresa.

Cobit 5 para la Seguridad de la Información está disponible en ISACA, una asociación global sin fines de lucro integrada por 100,000 profesionales del gobierno de TI.

Cobit 5 ofrece principios, prácticas, herramientas analíticas y modelos globalmente aceptados diseñados para ayudar al negocio y a los líderes de TI a maximizar la confianza, y el valor de la información y los activos tecnológicos de sus empresas. El marco y los documentos relacionados se han descargado más de 70,000 veces en dos meses desde su lanzamiento.” [25].

En 2012, las pérdidas de información y los temas relacionados con los empleados encabezaron la lista de problemas informáticos que muy probablemente presenten un desafío para la seguridad de la red de una organización.

“Las amenazas se clasificaron en el siguiente orden:

- Fuga de información (pérdida o violación) 17%
- Errores involuntarios de empleados 16%
- Incidentes relacionados con dispositivos personales de los empleados 13%
- Computación en la nube 11%
- Ataques cibernéticos 7%
- Piratería externa 5%
- Empleado descontento 5%
- Todas las anteriores 19%

Cobit 5 para la seguridad de la información puede ayudar a las empresas a reducir su perfil de riesgo gestionando la seguridad de manera apropiada. La tecnología de la información y las tecnologías relacionadas son cada vez más centrales para la empresa, pero la seguridad de la información es central para la confianza del interesado, manifestó Christos Dimitriadis, Vicepresidente Internacional de ISACA.” [26]

Cobit 5 se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales:

Principio 1. Satisfacer las Necesidades de las Partes Interesadas. Las empresas existen para crear valor para sus partes interesadas manteniendo el

equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

Cobit 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar Cobit 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Principio 2: Cubrir la Empresa “Extremo a Extremo”. Cobit 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; no se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin; es decir, incluyendo a todo y todos (internos y externos) los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: Aplicar un Marco de Referencia Único Integrado. Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. Cobit 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

Principio 4: Hacer Posible un Enfoque Holístico. Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. Cobit 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y

gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo Cobit 5 define siete categorías de catalizadores:

- Principios, Políticas y Marcos de Trabajo.
- Procesos.
- Estructuras Organizativas.
- Cultura, Ética y Comportamiento.
- Información.
- Servicios, Infraestructuras y Aplicaciones.
- Personas, Habilidades y Competencias.

Principio 5: Separar el Gobierno de la Gestión. El marco de trabajo establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. [27]

Cobit 5, además proporciona un Modelo de Evaluación de Procesos (PAM), basado en la norma internacional ISO/IEC 15504, Information Technology – Process Assessment, permite la mejora de los procesos, proporciona un medio para la medición de desempeño de los procesos del gobierno y la gestión, e identificar el área de mejora.

Tiene relación con normas ISO como la ISO 9001, con la misma se pueden reforzar con los controles de la calidad documental, además también con la ISO/IEC 27001, se pueden implementar de forma independiente o Integrada, contiene una serie de controles de seguridad de la información que se pueden cumplir aplicando este estándar, separa la seguridad de la información en dos procesos: Gestionar la Seguridad y Gestionar la Seguridad de los Servicios de Seguridad.

Este estándar incluye objetivos de control de riesgos y para tener control sobre los riesgos se le puede integrar con ISO 31000 así como el Risk IT (Riesgo de TI), logrando una gestión más efectiva y eficiente los riesgos de TI.

Las ventajas que representa es su flexibilidad en la implementación, cumple con los aspectos de las normas internacionales reconocidas internacionalmente.

Asegura una clara alineación entre las metas y los objetivos del negocio, a la vez con los procesos y actividades dentro de los mismos, establecen los controles para toda la organización, se enfoca en una perspectiva estratégica. Puede llegar a integrar a otros marcos de trabajo o estándares ISO, como ITIL, PMBOK, CMMI, Prince 2, ISO 9001, ISO 20000, ISO 27001, etc.

En la actualidad es obligatorio para toda entidad del sector público el manejo de procesos por lo cual Cobit aporta una serie de estándares que ayudan la definición de las estructuras organizativas:

En el modelo de procesos de Cobit 5 (Procesos Catalizadores), se distingue entre los procesos de gobierno y de gestión, incluyendo conjuntos específicos de prácticas y actividades para cada uno. El modelo de procesos también incluye una matriz RACI que describe las responsabilidades de las diferentes estructuras organizativas y roles en la empresa. “El modelo de procesos describe las entradas y salidas de los distintos procesos basados en prácticas a otros procesos, incluyendo la información intercambiada entre los procesos de gobierno y gestión. La información empleada en evaluar, orientar y supervisar la TI empresarial es intercambiada entre gobierno y gestión tal y como se describe en las entradas y salidas del modelo de procesos.

Cobit 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente se encuentra en una empresa que se relacionan con las actividades de TI, proporciona un modelo de referencia común entendible para las operaciones de TI y los responsables de negocio. El modelo de proceso propuesto es un modelo completo e integral, pero no

constituye el único modelo de procesos posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación particular.

La incorporación de un modelo operacional y un lenguaje común para todas las partes de la empresa involucradas en las actividades de TI, es uno de los pasos más importantes y críticos hacia el buen gobierno. Adicionalmente proporciona un marco para medir y vigilar el rendimiento de TI, proporcionar garantía de TI, comunicarse con los proveedores de servicio e integrar las mejores prácticas de gestión.

El modelo de referencia de procesos de Cobit 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

- GOBIERNO: contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión.
- GESTIÓN: contiene cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar, y proporciona cobertura extremo a extremo de las TI. Estos dominios son una evolución de la estructura de procesos y dominios de Cobit

Los nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

- Alinear, Planificar y Organizar
- Construir, Adquirir e Implementar
- Entregar, dar Servicio y Soporte
- Supervisar, Evaluar y Valorar

Cada dominio contiene un número de procesos. A pesar de que la mayoría de los procesos requieren de actividades de “planificación”, “implementación”, “ejecución” y “supervisión”, bien en el propio proceso, o bien en la cuestión específica a resolver (como p. ej. calidad, seguridad), están situados en dominios de acuerdo con el área más relevante de actividad cuando se

considera la TI a un nivel empresarial. El modelo de referencia de procesos de Cobit 5 es el sucesor del modelo de procesos de Cobit 4.1 e integra también los modelos de procesos de Risk IT y Val IT.” [27].

Beneficios que se obtiene implantando Cobit

- “Mantener la información de alta calidad para apoyar las decisiones de negocio.
- Lograr los objetivos estratégicos y obtener los beneficios de negocio a través del uso efectivo e innovador de TI.
- Lograr la excelencia operativa a través de la aplicación eficaz y fiable de la tecnología.
- Mantener riesgos relacionados con TI a un nivel aceptable.
- Optimizar los servicios y la tecnología de los gastos de TI.
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y políticas establecidas.” [28]

Factibilidad organizacional

Cobit 5 tiene la ventaja de poder implementarse en cualquier tipo de organización, en el caso de las organizaciones públicas, la identificación de los procesos son clave para la consecución de recursos económicos, para gestionar la seguridad de la información que debe ser manejada solo por los usuarios autorizados, actualmente la mayor parte de entidades públicas manejan la transferencia de recursos a través del Internet, lo cual si no se cuenta con adecuado gestión de la información, se pueden presentar riesgos de estafas.

Como se menciona ISACA se puede implementar a cualquier empresa, a todos los modelos de negocios, culturas corporativas, se puede aplicar en entornos corporativos que estén buscando procesos más eficientes.

Factibilidad tecnológica

“Cobit 5 es la última versión del marco de trabajo globalmente aceptado de ISACA, ofreciendo una visión de negocios extensa de la gobernabilidad de TI que refleja el rol central de la tecnología de la información en la creación de valor para las organizaciones. Los principios, prácticas, herramientas de análisis y modelos encontrados en Cobit 5 enmarcan el liderazgo y guía de negocios, TI y expertos en gobernabilidad alrededor del mundo.

Es el único marco de negocio para el gobierno y la gestión de las TI corporativas. Esta versión evolutiva incorpora las últimas ideas en la gestión empresarial y técnicas de gestión, y establece los principios globalmente aceptados, prácticas, herramientas analíticas y modelos para ayudar a aumentar la confianza en el valor de los sistemas de información. Cobit 5 se construye y amplía Cobit 4.1 mediante la integración de otros marcos importantes, normas y recursos, incluyendo Val TI y Risk IT de ISACA e Information Technology Infrastructure Library (ITIL®) y las normas relacionadas de la Organización Internacional de Normalización (ISO).” [28]

Resumen de Normativa COBIT
Definición <ul style="list-style-type: none">• Estandar que apoya las organizaciones en la planeación e implementación de su estrategia de seguridad informática.
Características <ul style="list-style-type: none">• Integra el framework de riesgos anteriormente llamado Risk IT, y• La evolución se denominará Cobit 5 for Risk Management• Cobit 5 incluye un Modelo de Evaluación de Procesos, basado en la norma internacional ISO/IEC 15504, Information Technology – Process Assessment.• Se complementa con guías y publicaciones adicionales, específicas, en temas de riesgos, cumplimiento, aseguramiento, gobierno de TI, etc.• Cobbit ha tenido varias actualizaciones

<ul style="list-style-type: none"> • Ofrece una visión global en la gestión y gobierno • Se establece 34 procesos, en base a los siguientes puntos: <ul style="list-style-type: none"> ▪ Descripción del proceso ▪ Indicadores de información y domino ▪ Objetivos de TI ▪ Objetivos del Proceso ▪ Prácticas Clave ▪ Métricas ▪ Gobierno y recursos de TI
<p>Descripción</p> <ul style="list-style-type: none"> • Organizaciones sin fines de lucro y asociaciones internacionales como ISACA promueven continuamente el uso de mejores prácticas para la seguridad de la información. • Se pueden implementar conjuntamente con Cobit iniciativas ITIL e ISO 27000 • Integra lineamientos sobre gestión de riesgos y seguridad de la información. • El principal valor de Cobit 5 es la diversidad de modelos y estándares específicos a nivel global, para seguridad, riesgos, etc. • El valor agregado del Cobit 5 es no pretender sustituir los frameworks usados en las empresas, sino aportar como el tema de madurez en los procesos de tecnologías de la información. • Desarrolla un marco de gobierno de las tecnologías de la información, para el control integral de tecnologías en toda la organización • Pone énfasis en el cumplimiento regulatorio
<p>Alcance</p> <ul style="list-style-type: none"> • Se orienta a la gerencia de tecnologías de información, pero complementada con adecuada herramientas y capacitación • Esta respalda por una comunidad de expertos en seguridad de

información y tecnologías

- Se encuentra en una evolución constante a la par con las tecnologías de la información
- Mapeado con otros estándares
- Orientado a Procesos, sobre la base de Dominios de Responsabilidad

Tabla 2.4 Resumen de Normativa Serie ISO 27001

Elaborado por: Investigador

2.1.8.5 Itil

Del inglés “Information Technology Infrastructure Library” en español “Biblioteca de Infraestructura de Tecnologías de Información” está orientado para el trabajo de mejores prácticas de servicios de la Tecnológica de Información.

Es un conjunto de procedimientos orientando a instituciones a alcanzar calidad y eficiencia en su operatividad dentro de su institución. Fue desarrollada en los 80's pero fue implantada a mediados de los 90's y fue basado en proceso - modelo de control y gestión de operaciones.

Factibilidad técnica

La gestión de servicios con ITIL tiene su columna vertebral en la función de Service Desk, la cual es el punto único de contacto entre la organización y el usuario o cliente del servicio.

Una de las cualidad técnicas de ITIL es la “Reducción del número de llamadas al Service Desk: Las mejores prácticas de ITIL establecen los procesos necesarios no solo para resolver incidentes, sino para aprender de ellos y lograr tener una base de conocimientos con la que la organización logra una mejora continua minimizando cada vez el número de incidentes y la carga de trabajo del Service Desk” [29], entendiendo que mejora los procesos en las bases de datos de las empresas, por lo cual los clientes ven más satisfechos con el servicio prestado.

Factibilidad organizacional

Su costo es manejable para las empresas, la fase de operaciones alcanza del 70% al 80% del coste y el tiempo, el resto del valor y tiempo se invierte en el desarrollo del producto.

Beneficios que se obtiene implantando ISO 27001

- “Aumento del ratio de resolución de incidencias en primera instancia: Organizando adecuadamente los niveles de escalamiento de incidentes en el Service Desk, se logra maximizar el tiempo de respuesta y resolución desde que se comunica el incidente en el servicio TI hasta su resolución” [29]
- Implantación de cambios más rápida / mejor control de cambios: Se puede gestionar de mejor manera los cambios requeridos en la infraestructura TI, permitiendo la calidad y estabilidad de los servicios.
- Se minimizan los problemas en los cambios y los “malos entendidos, respecto a la organización y el cliente.
- Busca que el servicio sea de alta calidad, fiable, y de costo aceptable para la empresa.

ITIL
Definición <ul style="list-style-type: none">• Es un estándar conocido para la gestión de servicios TI, enfoca a una mejora en la gestión de servicios, fomenta la satisfacción del cliente y del personal de una empresa
Características <ul style="list-style-type: none">• ITIL actúa sobre los procesos, fomenta el conjunto de buenas prácticas para mejorar el servicio que ofrece cualquier empresa• Promueve la mejora continua de la empresa

Descripción

- Se alinean al estándar de calidad ISO 9000, vinculado con el Modelo de Excelencia de la EFQM.
- Desarrolla un enfoque de procesos basado en el triángulo procesos, persona – tecnología, brindando servicios de calidad logrando la satisfacción de las personas, usuarios de los servicios de TI
- Permite la solución rápida de incidentes
- Esa constituido por cinco fases:
 - Estrategia del servicio
 - Gestión del servicio
 - Transición del servicio
 - Operación del servicio
 - Mejora continua del servicio

Alcance

- Estándar mundial de gestión de servicios informáticos
- “Las áreas cubiertas por ITIL en cada documento publicado por la OGC son:
 - Soporte al servicio: asegurar que el cliente (externo o interno) recibe adecuadamente un servicio, que es gestionado además de la mejor forma posible.
 - Entrega del servicio: administración de los servicios de soporte y mantenimiento que se prestan al cliente.
 - Planificación de la implantación: determina las ventajas de implantar ITIL en una determinada organización.
 - Administración de aplicaciones: conjunto de buenas prácticas para la gestión de todo el ciclo de vida de las aplicaciones, centrándose sobre todo en definición de requisitos e implementación de soluciones.
 - Administración de la infraestructura de tecnologías de la información y comunicaciones: gestión de la administración de sistemas como

máquinas, redes o sistemas operativos, entre otros.

- Administración de seguridad: proceso para la implantación de requerimientos de seguridad; relaciona las áreas ITIL de soporte y entrega de servicio.
- Administración de activos de software: pautas necesarias para la gestión del software adquirido y/o de desarrollo propio.
- Entrega de servicios desde un punto de vista de negocio: fidelización de clientes, servicios de externalización y gestión del cambio, entre otros.” [30]

Tabla 2.5 Resumen de Normativa ITIL

Elaborado por: Investigador

2.1.9 Modelo de Madurez

Es una herramienta que permite dividir los clasificar de negocios, y que nos sirve para mejorarlos o para obtener alguna certificación, determinando su desarrollo las cuales evaluarán un determinado proceso; para este análisis utilizaremos la escala de madurez basada en el Capability Maturity Model permite el mejoramiento del desarrollo de productos y servicios, y además es la que ocupa COBIT en respuesta a la necesidad de saber qué hacer de manera eficiente [31].

Las características de cada nivel son:

“0 – No Existente: el proceso no utiliza funcionalidad de un sistema homologado.

1 – Inicial: el proceso está parcialmente implementado en un sistema homologado o usa desarrollos propios habiendo funciones estándares o su uso es inadecuado o no corresponde a una Best Practice.

2 – Repetible: el proceso esta soportado, en gran medida, por la funcionalidad de un sistema homologado pero, no está estandarizado y no tiene gobernabilidad.

3 – Definido: el proceso esta soportado por la funcionalidad de un sistema homologado, no está estandarizado pero, tiene gobernabilidad.

4 – Administrado: el proceso está completamente soportado por la funcionalidad de un sistema homologado tanto en la operación (transacciones) como en la gestión (analytics), los procesos de negocios están estandarizados para las distintas filiales y se cuenta con una gobernabilidad que permite garantizar que los procesos operan de acuerdo a sus diseños y a las normativas (SoX, ISO, etc.)

5 – Optimizado: Los procesos de negocios se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y diseños. Se miden –benchmarking- respecto a cómo operaran en otras organizaciones similares. [31]”

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 MODALIDAD DE LA INVESTIGACIÓN

3.1.1 Investigación de Campo

Se aplica esta modalidad ya que el investigador acudirá al lugar en que se producen los acontecimientos, tomando contacto en forma directa con la realidad, para obtener información de acuerdo con los objetivos del proyecto.

3.1.2 Investigación Bibliográfica-Documental

Debido a que los datos nos llevarán a conocer cuáles son las principales causas para que el problema se mantenga, y esto permitirá tomar contacto de manera directa con el problema y facilitará el establecimiento de objetivos, el acceso a la información, su alcance y objetivos. La investigación se apoyará en fuentes como libros, revistas, artículos actualizados.

3.1.3 Investigación Aplicada

El diseño de un modelo de Manual Técnico de Procesos basado en Normativa Internacional para la Gestión de Riesgos Informáticos en el Departamento de Sistemas del Hospital Provincial Docente Ambato, corresponde a un proyecto de desarrollo para custodiar y resguardar los datos informáticos.

3.2 RECOLECCIÓN DE LA INFORMACIÓN

Las técnicas que se empleará en la presente investigación será: la observación, entrevista, encuesta y la consulta en libros e internet, para describir, explicar el porqué de una determinada situación.

3.3 PROCESAMIENTO DE LA INFORMACIÓN

- Se filtrará la información obtenida que resulte escasa, defectuosa, contradictoria o no pertinente para la investigación.

- Matriz de Riesgos Informáticos.
- Presentación de resultados en cuadros y gráficos estadísticos.

3.3.1 Análisis e Interpretación de Resultados

Se analizarán los resultados, obtenidos en la observación, entrevista y encuestas sobre gestión de riesgos informáticos de forma porcentual para interpretar las mayores tendencias, poder definir los riesgos potenciales y áreas críticas para evitar una posible fuga o manipulación inadecuada de la información.

3.4 DESARROLLO DEL PROYECTO

Las etapas de desarrollo del proyecto de investigación son las siguientes:

ETAPA 1 – PRÁCTICAS ACTUALES

- 1.1 Análisis de procedimientos.
- 1.2 Clasificación de riesgos.
- 1.3 Reducción de riesgos.
- 1.4 Control de riesgos.

ETAPA 2 – REGLAMENTOS Y POLÍTICAS VIGENTES

- 2.1 Revisión de políticas de y administración del departamento de sistemas.
- 2.2 Análisis y delimitación de áreas críticas.
- 2.3 Pruebas de riesgos.

ETAPA 3 – NORMATIVAS INTERNACIONALES

- 3.1 Estudio y análisis de normativas internacionales.

ETAPA 4 – ENTORNO COMPETITIVO

- 4.1 Establecimiento de procesos y funciones del departamento de sistemas.

ETAPA 5 – DESARROLLO DE MANUAL DE PROCESOS

- 5.1 Diseño y elaboración de manual técnico.

Dentro de la primera etapa de análisis actual de los procedimientos se establecerá un diagnóstico de los riesgos informáticos identificando el nivel de riesgo estableciendo los siguientes procedimientos:

- Análisis
- Clasificación
- Reducción
- Control

Esta etapa se realizará mediante observaciones de campo la cual permitirá evaluar todos los potenciales riesgos en los cuales se pueda ver envuelta la información del Hospital Provincial Docente Ambato y el cumplimiento de las políticas de seguridad.

En la segunda etapa se definirá las áreas críticas en donde se encuentran la mayor parte de riesgos potenciales por los que se pueden derivar a una manipulación parcial o total de la información, en base a falencias en la red, inseguridades lógicas, confidencialidad, políticas de accesos, etc., con el fin de delimitar el alcance de la propuesta de solución; estos parámetros se los coordinará conjuntamente con el director del Departamento de Sistemas del Hospital Provincial Docente Ambato.

En la tercera etapa se realizará un estudio de la normativa que se apegue a las necesidades, infraestructura, políticas, tipo de información, servicios, recursos humanos y económicos; es decir el estándar que mejor se apegue a la situación actual del Hospital Provincial Docente Ambato.

En la cuarta etapa se establecerán los procesos y funciones que corresponden a la administración del Departamento de Sistemas del Hospital Provincial Docente Ambato para poder delimitar el gobierno y gestión que abarcará el Manual Técnico de Procesos para que realice, apoye, dirija y pueda llevar el control posterior de implementación y seguimiento a todo el modelo de seguridad de la información.

Finalmente en la quinta etapa se diseñará el manual Técnico bajo una normativa Internacional con los procedimientos, instructivos y registros conjuntamente con el desarrollo de documentos que formalicen cómo se deben realizar las actividades y que información es la que se debe retener como evidencia para dar conformidad a las Políticas de Seguridad Informáticas acorde a las necesidades, áreas preestablecidas y recursos que cuenta el Hospital Provincial Docente Ambato con el fin de mantener una información de alta calidad, alcanzando una excelencia operativa, reduciendo los riesgos relacionados con las Tecnologías Informáticas a un nivel aceptable para poder colaborar de manera óptima y adecuada con el alcance de objetivos y metas de la institución.

CAPITULO IV

DESARROLLO DE LA PROPUESTA

SEGURIDAD DE LA INFORMACIÓN

En la actualidad una de las mayores urgencias y prioridades dentro de cualquier empresa, negocio, institución, etc., es implantar una adecuada gestión de seguridad de los sistemas de información; sin importar el nivel de tecnología que cuenta la Institución; es así, que organizaciones internacionales como ISO, BS, NIST, IEEE, ISACA están en el constante desarrollo y evolución de estándares y mejoras continuas en las metodologías y herramientas que facilitan la gestión de las seguridad de información.

En la actualidad estos estándares se han convertido en obligaciones de cada departamento de Sistemas para de manera conjunta con las demás áreas y departamentos de la institución, alcanzar un control eficiente y certificaciones de calidad que llevarán a la institución a prestar mejores servicios a sus clientes internos y externos.

Más allá de un cumplimiento de estándares que incluso se han convertido en normas legales dentro de cualquier institución; el aplicar estas normas y estándares permite a las organizaciones obtener un beneficio básico que será la gestión objetiva y controlada de uno de sus activos más importantes que es la información. Además de asegurar la información estos procesos ayudan en los resultados de eficiencia y eficacia en los procesos y gestiones del negocio; traduciéndose así en una optimización de recursos dando un mayor beneficio para la empresa dentro de la mejora continua.

En resumidas cuentas la seguridad es un proceso continuo, sujetas a mejoras multidimensionales cuyo fin será permitir a que una organización pueda cumplir su visión, misión y objetivos; implementando sistemas que usen una información integra, objetiva y confiable a todos sus usuarios, para proporcionar mejores resultados en cada uno de los productos que se ofrece al cliente.

4.1. ETAPA 1 - PRÁCTICAS ACTUALES

4.1.1 Análisis de Procedimientos

En el levantamiento de información en el departamento de sistemas se encuentra con una serie de problemáticas que con el paso del tiempo se han expandido en una especie de “efecto domino”; es decir, un conjunto de sucesos continuos en donde las consecuencias de una acción previa incrementaron el daño llegando a afectar elementos exteriores más vulnerables (espacio) y que pueden mantenerse “represados” hasta un punto límite donde su ruptura produce daños (tiempo) desembocando en una problemática mucho más grave y con mayores proporciones.

Este “efecto domino” se ha mantenido latente dentro de la Institución de salud ya que el tratamiento a las distintas problemáticas se los ha realizado de manera reactiva; es decir, que conforme aparece un problema se lo ha solucionado sin dar un tratamiento especializado, preventivo o correctivo y esto ha provocado que el error empiece aparecer continuamente en las actividades cotidianas del departamento de sistemas; es justamente por esta problemática que nace el departamento en 2008 y pocos han sido los avances y mejoras hasta la actualidad, siendo imperceptible algún tipo de variación en sus procesos.

Es un objetivo puntual para el departamento de sistemas del Hospital Provincial Docente Ambato en mejorar la calidad de sus servicios, llegando a equipararse con los demás departamentos de la Institución de Salud; ya que estos trabajan con manuales de procesos establecidos, funcionando de manera adecuada con relación a éste.

Es así como se ha revisado las actividades encomendados mediante documentación en base a contratos que debe realizar el departamento de sistemas y son:

- Realizar el plan e informe de mantenimiento de equipos, seguridad y red.

- Mantenimiento físico de equipos de cómputo.
- Control lógico y de seguridad.
- Plan de mantenimiento de equipos.
- Capacitación y asesoramiento permanente.
- Operación de equipos Informáticos de manera adecuada.
- Llevar documentación electrónica que permitan operar fácilmente archivos, informes, impresos de flujos de información.
- Asesorar y facilitar manejos de los diferentes sistemas.
- Realizar trabajos solicitados.
- Informar sobre bases, resultados y procesos de sistemas.
- Realizar mantenimiento preventivo y correctivo de equipos.
- Reportes de daños y novedades en equipos.
- Programar e implantar sistemas informáticos de acuerdo a las necesidades existentes.
- Complementar funciones con actividades variadas de registros y asesorías en materia informática y las demás que les fueran encomendadas por las autoridades competentes.

Una vez realizado una investigación de campo se ha determinado que las actividades diarias que el departamento de sistemas se limita de manera considerable y limitadas en el menor porcentaje las mencionadas anteriormente; estas actividades son:

- Mantenimiento correctivo de equipos.
- Administración de cuentas de usuario.
- Administración de políticas ethernet.
- Soporte técnico a usuarios.

FLUJOGRAMA PARA ANÁLISIS DE RIESGOS

La metodología aplicada a esta investigación en el análisis de riesgos, así como las herramientas y materiales usados, están basados en la experiencia práctica real obtenida por Markus Erb Ingeniero electrónico, en el proyecto “Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras” financiado por HIVOS Holanda e impartido en Costa Rica en los años 2007 y 2008 [32].

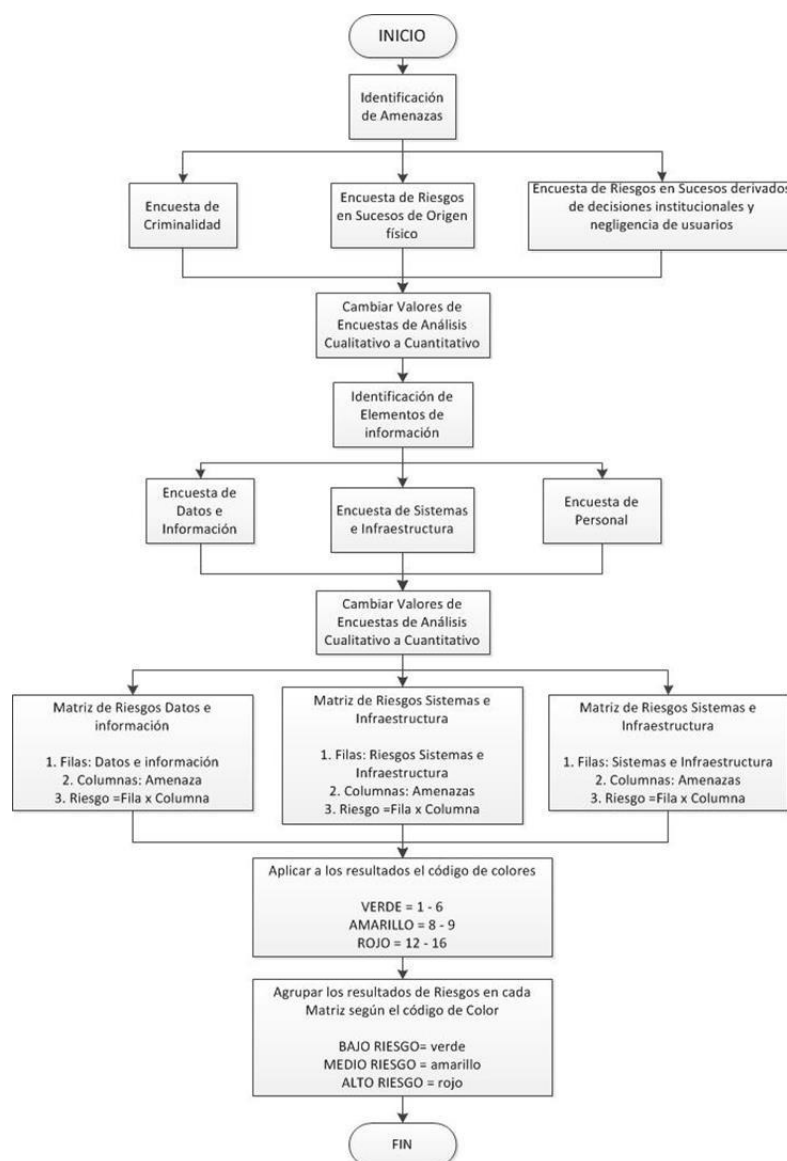


Fig. 4.3 Diagrama de Flujo para elaboración de Matriz de Análisis de Riesgo

Elaborado por: Investigador

4.1.2 Clasificación de Riesgos

Al gestionar de manera eficaz los riesgos informáticos dentro del Hospital Provincial Docente Ambato se ha certificado que la información y los procesos estarán controlados y documentados para su posterior valoración, dando un diagnóstico de la situación que atraviesa la institución y priorizar cuales son las principales causas y las que se deberá dar un pronto tratamiento y corrección.

Los siguientes resultados se han generado en base encuestas realizadas al Director del Departamento de Sistemas Ing. Danilo Naranjo; dichos resultados darán a conocer la realidad de las problemáticas existentes en la actualidad en el Hospital Provincial Docente Ambato dentro del área tecnológica, operativa, estructural, riesgos, información, catastros; dicha encuesta dará a conocer las fortalezas y debilidades de la Institución de Salud.

Actos originados por la criminalidad común				
Tipo de Amenaza o Ataque	Probabilidad de Amenaza			
	Insignificante (Ninguna)	Baja	Mediana	Alta
Actos originados por la criminalidad común				
Allanamiento		X		
Acosamiento civil, fiscal, penal	X			
Orden de secuestro o detención	X			
Sabotaje, ataque físico y/o electrónico			X	
Daños por vandalismo			X	
Fraude y/o estafa	X			
Robo físico de equipos tecnológicos			X	
Robo de información electrónica			X	
Intromisión a red interna				X
Infiltración			X	
Virus / ejecución no autorizado de programas				X
Desciframiento de contraseñas no autorizadas				X
Violación a derechos de autor			X	

Tabla 4.6 Encuesta de Riesgos en Actos originados por la criminalidad común

Elaborado por: Investigador

Suceso de origen físico				
Tipo de Amenaza o Ataque	Probabilidad de Amenaza			
Suceso de origen físico	Insignificante (Ninguna)	Baja	Mediana	Alta
Incendio	X			
Inundación			X	
Sismo		X		
Daños debidos al polvo			X	
Falta de ventilación				X
Electromagnetismo			X	
Sobrecarga eléctrica				X
Falla de corriente (apagones)				X
Falla de sistema / daños en disco duro			X	

Tabla 4.7 Encuesta de Riesgos en Sucesos de Origen físico

Elaborado por: Investigador

Sucesos derivados de decisiones institucionales y negligencia de usuarios				
Tipo de Amenaza o Ataque	Probabilidad de Amenaza			
Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales	Insignificante (Ninguna)	Baja	Mediana	Alta
Falta de inducción, capacitación y concientización sobre riesgos			X	
Mal manejo de sistemas y herramientas Informáticas				X
Utilización de programas no autorizados y/o software 'pirata'				X
Falta de pruebas de software nuevo con datos productivos (Instalación de nuevos programas sin respaldar los datos anteriormente)			X	
Pérdida de datos e información			X	
Infección de sistemas a través de unidades portables sin escaneo				X
Manejo inadecuado de datos críticos				X
Unidades portables con información sin cifrado de datos				X
Transmisión no cifrada de datos críticos				X
Manejo inadecuado de contraseñas				X
Compartir contraseñas o permisos a terceros sin autorización				X

Exposición o extravío de equipo, unidades de almacenamiento, etc.			X	
Sobrepasar autoridades			X	
Falta de definición de perfil, privilegios y restricciones del personal				X
Falta de mantenimiento físico (proceso, repuestos e insumos)			X	
Falta de actualización de software (proceso y recursos)			X	
Fallas en permisos de usuarios (acceso a archivos)			X	
Acceso electrónico no autorizado a sistemas externos			X	
Acceso electrónico no autorizado a sistemas internos			X	
Red cableada expuesta para el acceso no autorizado			X	
Red inalámbrica expuesta al acceso no autorizado			X	
Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)				X
Falta de mecanismos de verificación de normas y reglas				X
Ausencia de documentación				X
Ineficaz control de accesos a usuarios				X
Inexistente bitácora de procesos técnicos				X
Inadecuado control de inventario en los activos tecnológicos			X	
Inexistencia de políticas de seguridad informática				X
Concentración de funciones en una sola persona				X
Falta de personal dentro del departamento de sistemas				X
Falta de capacitación a los usuarios			X	
Falta de capacitación al departamento de sistemas				X
Falta de recursos económicos				X

Tabla 4.8 Encuesta de Riesgos en Sucesos derivados de decisiones institucionales y negligencia de usuarios

Elaborado por: Investigador

Elementos de Información

Datos e Información									
Tipo de Amenaza o Ataque		Clasificación				Magnitud de Daño			
Datos e Información		Confidencial, Privado, Sensitivo	Obligación por ley /Contrato	Costo de recuperación (tiempo, económico, material, imagen)	Insignificante (Ninguna)	Baja	Mediana	Alta	
Documentos institucionales (proyectos, planes, evaluaciones, informes, etc.)		X		X			X		
Finanzas		X					X		
Servicios bancarios									
RR.HH.		X		X				X	
Productos institucionales (investigaciones, folletos, fotos, etc.)									
Correo electrónico									
Bases de datos internos		X		X				X	
Bases de datos externos									
Página web interna (Intranet)									
Página web externa									
Respaldos		X		X			X		
Infraestructura (planos, documentación, etc.)									
Informática (planos, documentación, etc.)									
Base de datos de contraseñas		X							X
Datos e información no institucionales									
Navegación en internet									
Chat interno									
Chat externo									

Tabla 4.9 Encuesta de Riesgos en los Datos e Información

Elaborado por: Investigador

Sistemas e Infraestructura									
Tipo de amenaza o ataque	Clasificación				Magnitud de Daño				
	Acceso exclusivo	Acceso ilimitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Insignificante (Ninguna)	Baja	Mediana	Alta		
Sistemas e Infraestructura									
Equipos de la red cableada		X				X			
Equipos de la red inalámbrica		X				X			
Cortafuegos	X		X				X		
Servidores	X		X				X		
Computadores		X				X			
Computadores Portátiles		X				X			X
Programas de administración Institucional	X		X						
Programas de manejo de proyectos									
Programas de producción de datos									
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)									
Impresoras		X				X			
Memorias portátiles		X				X			
Celulares									
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)									
Vehículos									

Tabla 4.10 Encuesta de Riesgos en Sistemas e Infraestructura

Elaborado por: Investigador

Personal									
Tipo de Amenaza o Ataque	Clasificación					Magnitud de Daño			
	Imagen pública de alto perfil, indispensable para funcionamiento institucional	Perfil medio, experto en su área	Perfil bajo, no indispensable para funcionamiento institucional	Insignificante (Ninguna)	Baja	Mediana	Alta		
Personal									
Junta Directiva									
Dirección / Coordinación									
Administración									
Personal técnico									
Recepción									
Piloto / conductor									
Informática / Soporte técnico interno	X							X	
Soporte técnico externo									
Servicio de limpieza de planta									
Servicio de limpieza externo									
Servicio de mensajería propio									
Servicio de mensajería externo									

Tabla 4.11 Encuesta de Riesgos en Personal

Elaborado por: Investigador

4.1.3 Reducción de Riesgos

Se basa en el método de análisis de riesgo con un grafo de riesgo, usando la fórmula:

$$\text{Riesgo} = \text{Probabilidad de Amenaza} \times \text{Magnitud de Daño.}$$

En base a los resultados brindados por los elementos de Información, ésta se transformará en valores que serán ingresados en una sola matriz de análisis de riesgos, donde se podrá cuantificar los resultados, obteniendo los valores críticos de índice de afectación de cada riesgo por cada área determinada en los elementos de Información y así poder reducir dichos riesgos para la entidad; centrándose en las áreas que poseen menores seguridades y poder hacer frente a posibles ataques externos o internos haciendo que sea más fácilmente identificarlos y clasificarlos para su posterior control.

La siguiente información se encuentra en formatos generados para el análisis de riesgos actuales; en base a encuestas realizadas anteriormente se verifica las áreas vulnerables, visualizadas fácilmente en base a la metodología que Markus Erb provee para su aplicación; así como los correctivos y protecciones necesarias en los elementos tecnológicos de información.

Riesgos para los Elemento de Información “Sistemas e Infraestructura”

Matriz de Análisis de Riesgo			Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																							
			Actos originados por la criminalidad																							
Sistemas e Infraestructura	Clasificación			Sucesos de origen físico																						
	Acceso exclusivo	Acceso limitado	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Dato: 1= Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Allanamiento	Acosamiento civil, fiscal, penal	Orden de secuestro o Detención	Sabotaje, Ataque físico y/o electrónico	Danos por vandalismo	Fraude y/o Estafa	Robo físico de Equipos Tecnológicos	Robo de información electrónica	Intrusión a Red Interna	Infiltración	Virus / Ejecución no autorizado de programas	Descrimentamiento de Contraseñas no autorizadas	Violación a derechos de autor	Incendio	Inundación	Sismo	Danos debidos al polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
					2	1	1	3	3	1	3	3	4	3	4	4	3	1	3	2	3	4	3	4	4	1
Equipos de la red cableada		X		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Equipos de la red inalámbrica				3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Cortafuegos			X	4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Servidores			X	4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Computadores			X	3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Computadores Portátiles			X	3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Programas de administración Institucional		X		4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Programas de manejo de proyectos																										
Programas de producción de datos																										
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)																										
Impresoras			X	3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Memorias portátiles		X		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Celulares																										
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)																										
Vehículos																										

Fig. 4.6 Matriz de Análisis de Riesgo para Elementos de Información “Sistemas e Infraestructura”

Elaborado por: Investigador

Matriz de Análisis de Riesgo	Clasificación	Magnitud de daño: 1 = Bajo 2 = Medio 3 = Alto 4 = Muy Alto	Bucses derivadas por la negligencia de usuarios y decisiones institucionales																																														
			Falta de inducción, capacitación y conciencia sobre riesgos	Mantenimiento de sistemas y herramientas informáticas	Utilización de programas no autorizados y/o software pirata	Falta de pruebas de software	Instalación de nuevos programas	Pérdida de datos e información	Indicadores de sistemas a través de unidades portátiles sin escaneo	Mantención inadecuada de datos	Unidades portátiles con información sin respaldo de datos	Transmisión no cifrada de datos críticos	Mantención inadecuada de contraseñas	Compartir contraseñas o permisos a terceros sin autorización	Exposición o extravío de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de mantenimiento físico (proceso, repuestos e insumos)	Falta de actualización de software (proceso y recursos)	Faltas en permisos de usuarios (acceso a archivos)	Acceso electrónico no autorizado a sistemas externos	Acceso electrónico no autorizado a sistemas internos	Red abierta expuesta para el acceso no autorizado	Red inalámbrica expuesta al acceso no autorizado	Falta de normas y reglas claras	Verificación de normas y reglas	Ausencia de documentación	Interfaz control de accesos a usuarios	Existente historia de procesos técnicos	Inadecuado control de inventario en los activos tecnológicos	Inexistencia de políticas de seguridad informática	Concesión de funciones en una sola persona	Falta de personal dentro del Departamento de sistemas	Falta de capacitación a los Usuarios	Falta de capacitación al Departamento de Sistemas	Falta de Recursos Económicos													
Sistemas e Infraestructura	Acceso exclusivo	3	Falta de inducción, capacitación y conciencia sobre riesgos																																														
			X	Mantenimiento de sistemas y herramientas informáticas																																													
				X	Utilización de programas no autorizados y/o software pirata																																												
					X	Falta de pruebas de software																																											
						X	Instalación de nuevos programas																																										
							X	Pérdida de datos e información																																									
								X	Indicadores de sistemas a través de unidades portátiles sin escaneo																																								
									X	Mantención inadecuada de datos																																							
										X	Unidades portátiles con información sin respaldo de datos																																						
											X	Transmisión no cifrada de datos críticos																																					
X	Mantención inadecuada de contraseñas																																																
	X	Compartir contraseñas o permisos a terceros sin autorización																																															
		X	Exposición o extravío de equipo, unidades de almacenamiento, etc																																														
			X	Sobrepasar autoridades																																													
				X	Falta de definición de perfil, privilegios y restricciones del personal																																												
					X	Falta de mantenimiento físico (proceso, repuestos e insumos)																																											
						X	Falta de actualización de software (proceso y recursos)																																										
							X	Faltas en permisos de usuarios (acceso a archivos)																																									
								X	Acceso electrónico no autorizado a sistemas externos																																								
									X	Acceso electrónico no autorizado a sistemas internos																																							
X										Red abierta expuesta para el acceso no autorizado																																							
	X									Red inalámbrica expuesta al acceso no autorizado																																							
		X								Falta de normas y reglas claras																																							
			X							Verificación de normas y reglas																																							
				X						Ausencia de documentación																																							
					X					Interfaz control de accesos a usuarios																																							
						X				Existente historia de procesos técnicos																																							
							X			Inadecuado control de inventario en los activos tecnológicos																																							
								X		Inexistencia de políticas de seguridad informática																																							
									X	Concesión de funciones en una sola persona																																							
X										Falta de personal dentro del Departamento de sistemas																																							
	X									Falta de capacitación a los Usuarios																																							
		X								Falta de capacitación al Departamento de Sistemas																																							
			X							Falta de Recursos Económicos																																							

Fig. 4.7 Matriz de Análisis de Riesgo para Elementos de Información “Sistema e Infraestructura”

Elaborado por: Investigador

4.1.4 Control de Riesgos

Es necesario después de analizar, clasificar y reducir los riesgos informáticos, tomar medidas destinadas a la protección de procesos operativos y de seguridad, dispositivos de almacenamiento, equipos informáticos, medios de transmisión, comunicación, energía, y todo aquello que pueda provocar pérdida, alteración o acceso no autorizado por parte de algún agente externo o interno a las seguridades actuales y condiciones que maneja el departamento; ya que no son suficientes las medidas que se están aplicando para hacer frente a estos riesgos potenciales en posibles pérdidas de datos.

Además de no existir seguridades suficientes, el mayor daño que se produce en el manejo de información en la actualidad es por una inadecuada administración de normas a usuarios debido a mal manejo de los diferentes sistemas o recursos tecnológicos por lo que se producen pérdida e inconsistencia en la información; es decir, una falta de capacitación en las habilidades, conocimientos y la competitividad en los usuarios, que producen un lento desarrollo proactivo y operativo, reduciendo la productividad de los procesos en la Institución y viéndose afectado directamente el departamento de sistemas al ser el responsable de dar solución a los diferentes problemas e incluso aquellos que no competen dentro de las actividades, procesos y funciones de esta área.

Se procede a realizar el análisis cuantitativo los riesgos Informáticos en el Hospital Provincial Docente Ambato mediante el uso de la matriz de análisis de riesgos en la que se ha realizado un promedio de los valores encontrando que existe el mayor grado de riesgo y amenaza en el área de sistemas e infraestructura de la institución, por sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales; es decir, no existen condiciones internas y externas que impidan el desarrollo del ataque por lo que se debe dar un tratamiento urgente a esta área.

en color AMARILLO que en la matriz se observa que el 100% de áreas y problemas críticos están marcadas y fácilmente reconocibles.

Por lo tanto después de obtener resultados en las matrices analizadas se ha enmarcado los puntos críticos, a los que se tiene que dar un tratamiento especial y necesario para reducir los riesgos que tiene la Institución y los cuales están involucrados dentro del área de Sistemas e Infraestructura y son:

Medidas Personales

- Mal manejo de sistemas y herramientas Informáticas
- Falta de capacitación a los Usuarios
- Falta de capacitación al Departamento de Sistemas
- Infección de sistemas a través de unidades portables sin escaneo
- Manejo inadecuado de contraseñas
- Compartir contraseñas o permisos a terceros sin autorización
- Sobrepasar autoridades
- Concentración de funciones en una sola persona
- Falta de personal dentro del Departamento de Sistemas
- Falta de Recursos Económicos

Medidas Técnicas

- Pérdida de datos e Información
- Manejo inadecuado de datos críticos
- Unidades portables con información sin cifrado de datos
- Transmisión no cifrada de datos críticos
- Falta de pruebas de software nuevo con datos productivos
- Exposición o extravío de equipo, unidades de almacenamiento, etc.
- Acceso electrónico no autorizado a sistemas externos
- Acceso electrónico no autorizado a sistemas internos
- Falta de actualización de software (proceso y recursos)
- Fallas en permisos de usuarios (acceso a archivos)

- Falta de definición de perfil, privilegios y restricciones del personal
- Ineficaz control de accesos a usuarios

Medidas Organizativas

- Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
- Falta de mecanismos de verificación de normas y reglas
- Ausencia de documentación
- Inexistente bitácora de procesos técnicos
- Inexistencia de políticas de seguridad informática
- Utilización de programas no autorizados y/o software 'pirata'
- Red cableada expuesta para el acceso no autorizado
- Red inalámbrica expuesta al acceso no autorizado

El segundo grado de amenaza dentro de los Sistemas e infraestructura es un riesgo en actos originados por la criminalidad común y sucesos de origen físico; también se encuentra en este punto daños en los datos e información que proceden por sucesos derivados de la impericia, negligencia de usuarios y decisiones institucionales; aunque existen condiciones que hacen poco probable un ataque en el corto plazo se deberá considerar que no son suficientes para evitarlo a largo plazo.

Matriz de Análisis de Riesgo				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3 = Mediana, 4 = Alta]																						
Sistemas e Infraestructura	Clasificación			Magnitud de Daño: 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Actos originados por la criminalidad											Sucesos de origen físico										
	Acceso exclusivo	Acceso limitado	Caso de recuperación (tiempo, material, imagen, emocional)		Allanamiento	Acosamiento civil, fiscal, penal	Orden de secuestro o desorden	Sabotaje, ataque físico y/o electrónico	Daños por vandalismo	Fraude y/o Estafa	Robo físico de Equipos Tecnológicos	Robo de información electrónica	Intromisión a Red interna	Infiltración	Virus / Ejecución no autorizada de programas	Desplazamiento de Contraseña no autorizada	Violación a derechos de autor	Incendio	Inundación	Sismo	Daños debidos al polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falta de corriente (apagones)	Falta de sistema / Daño disco duro
Equipos de la red cableada	x			3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Equipos de la red inalámbrica		x		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Corratuques	x		x	4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	15	4
Servidores	x		x	4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Computadores		x		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Computadores Portátiles		x		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Programas de administración institucional	x		x	4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Programas de manejo de proyectos																										
Programas de producción de faxes																										
Programas de comunicación (correo electrónico, chat, llamadas telefónicas, etc.)																										
Impresoras		x	x	3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Memorias portátiles		x		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Celulares																										
Edificio (Oficinas, Recepción, Sala de espera, Sala de reunión, Bodega, etc.)																										
Vehículos																										

Fig. 4.12 Matriz Análisis de Riesgo Sistemas e Infraestructura por Criminalidad y Sucesos Físicos
Elaborado por: Investigador

Bajo el mismo criterio de análisis se ha realizado la clasificación de los riesgos potenciales enmarcándolos en los aspectos generales que se desea tomar un plan de acción para reducir los riesgos y son los siguientes:

Medidas Organizativas

- Violación a derechos de autor
- Virus / Ejecución no autorizado de programas

Acciones Hostiles

- Robo físico de Equipos Tecnológicos
- Allanamiento
- Sabotaje, Ataque físico y/o electrónico
- Robo de información electrónica
- Daños por vandalismo
- Infiltración
- Intromisión a Red interna

- Desciframiento de Contraseñas no autorizadas

Medidas Físicas

- Inundación
- Sismo
- Daños debidos al polvo
- Falta de ventilación
- Electromagnetismo
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Falla de sistema /Daño disco duro

El tercer grado de amenaza son los datos e información que se originan por actos de criminalidad común y por sucesos de origen físico es un problema que se encuentra latente en la Institución que no se lo puede descuidar, ya que la información es un activo intangible demasiado importante dentro de cualquier institución.

Si bien es cierto los datos e información hay que protegerlos de ataques externos e internos; las condiciones actuales de riesgo que corren los datos no son precisamente de origen intencionado, más bien es el resultado de los riesgos que se originan por daños causados por los Sistemas e Infraestructura que no están controlados de una manera adecuada, razones por las cuales se generan complicaciones y pérdida de información en la mayoría de los casos; por lo tanto, para esta área en el análisis de Matriz de Riesgo existen condiciones que hacen lejana la posibilidad de ataques directos, pero que también es necesario protegerla y no descuidarla conforme al crecimiento y evolución de información y datos dentro del Hospital Provincial Docente Ambato, sin antes dar una solución adecuada a las probabilidades de riesgo Alta y mediana.

Matriz de Análisis de Riesgo				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																						
Datos e Información	Clasificación			Actos originados por la criminalidad												Sucesos de origen físico										
	Confidencial, Privado, Sensible	Obligación por ley / Contrato / Convenio	Careo de recuperación (tiempo, económico, material, imagen, profesional)	Magnitud de Daño: 1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto	Atentamiento	Acusamiento civil, fiscal, penal	Orden de secuestro o detención	Robo de cheque físico y/o electrónico	Daños por vandalismo	Fraude y/o Estafa	Robo físico de Equipos Tecnológicos	Robo de información electrónica	Intrusión a Red Interna	Infiltración	Violación no autorizada de programas	Desfibramiento de Contraseñas no autorizadas	Violación a derechos de autor	Incendio	Inundación	Sismo	Daños debidos al polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falla de corriente (apagones)	Falla de sistema / Daño disco duro
Documentos Institucionales (Proyectos, Planes, Evaluaciones, INFORMAS, SIS)	x		x	3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Finanzas	x			3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Servicios bancarios				4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
RR.HH	x	x		4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Productos Institucionales (Investigaciones, Folletos, Fotos, etc.)																										
Correo electrónico																										
Bases de datos internos	x	x		4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Bases de datos externos																										
Página Web interna (Intranet)																										
Página Web externa																										
Respalidos	x	x		3	6	3	3	9	9	3	9	9	12	9	12	12	9	3	9	6	9	12	9	12	12	3
Infraestructura (Planes, Documentación, etc.)																										
Informática (Planes, Documentación, etc.)																										
Base de datos de Contraseñas	x			4	8	4	4	12	12	4	12	12	16	12	16	16	12	4	12	8	12	16	12	16	16	4
Datos e información no institucionales																										
Navegación en Internet																										
Chat interno																										
Chat externo																										

Fig. 4.14 Matriz Análisis de Riesgo Datos e Información por Criminalidad y Sucesos Físicos

Elaborado por: Investigador

Medidas Físicas

- Falta de ventilación
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Electromagnetismo
- Daños debidos al polvo
- Inundación
- Sismo
- Incendio
- Falla de sistema /Daño disco duro

Los riesgos a los que están expuestos los datos e Información por actos originados por criminalidad son:

4.2. ETAPA 2 - REGLAMENTOS Y POLÍTICAS VIGENTES

4.2.1 Revisión de Políticas de Administración del Departamento de Sistemas

En el actual manejo del departamento de sistemas no se cuenta políticas de administración definidas, autorizadas ni estandarizadas por las autoridades, sino que se cuenta con un desarrollo dinámico de los procesos y cambios en los sistemas de información.

Al no contar Políticas de Administración dentro del Departamento de Sistemas no va a existir normas, definiciones, control, responsabilidades en los procesos cotidianos de los usuarios para preservar la información que se maneja dentro del Hospital Provincial Docente Ambato; poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información. Es necesario tener un plan de seguridad que permitan controles lógicos de acceso, manipulación de la información; así también para el control físico de los recursos tecnológicos que dispone la institución.

Las normas que en la actualidad maneja el departamento de sistemas son, en el mayor de los casos lineamientos que se han creado en base a la necesidad que ha existido, para dar solución a diferentes problemáticas a lo largo de la creación del departamento de sistemas en el año 2008; es así que la Dirección Provincial de Salud de Tungurahua y la Contraloría General del Estado al observar esta problemática de falta de procesos, normativas, políticas y manuales de seguridad proporcionó una documentación con información que puede ser usada como anexo para una determinación de estrategias en las directrices para la normalización de procesos y creación de documentos que puedan ayudar a la corrección de estas singularidades en el área de sistemas e Información pero se ha hecho caso omiso debido a la falta de apoyo e interés de las autoridades de la institución.

Este desinterés en parametrizar lineamientos que ayudarán a corregir problemas cotidianos y dar seguridad a la información se debe a que no existe auditorías informáticas periódicas externas o internas; así como la falta de

sanciones a quienes incurran en estas infracciones, por lo que como no existen penalidades a una inadecuada manejo de información o delitos informáticos o recursos tecnológicos se actúa de manera despreocupada a poner un alto a estas irregularidades y errores. Las normas dentro del departamento de sistemas regularán el comportamiento de los usuarios en la administración de recursos tecnológicos así como la información electrónica que utilizan; también ayudará en el control de actividades que los usuarios realizan.

4.2.2 Análisis y Delimitación de Áreas Críticas

Dentro de la administración del departamento de sistemas, las áreas más vulnerables en donde se encuentran los altos factores e índices de riesgo como se observan en las Fig. 14 y Fig.15 de ésta investigación, en donde se encuentra la relación de los datos e información con las áreas que poseen mayor grado de afectación, e importancia; también las que se originan debido a la negligencia de usuarios y decisiones institucionales, riesgos de origen físico y actos originados por criminalidad y estos son:

- Servicios bancarios
- RR.HH.
- Documentos institucionales
- Finanzas
- Bases de datos internos
- Base de datos de Contraseñas

4.2.3 Pruebas de Riesgos

En el análisis de las pruebas de riesgos se puede encontrar cuál es el actual registro de daños, mantenimiento, soporte, y diversas actividades que el departamento de sistemas del Hospital Provincial Docente Ambato intenta llevar, para poder tener un respaldo manual de los diversos soportes realizados hacia los servidores de la Institución.

Es por esta razón que se detallará los formatos actuales como una prueba de riesgo que posee el departamento de sistemas, ya que dicha documentación puede estar expuesta a catastros físicos, pérdida e incluso manipulación que al final sería un riesgo en la información del servicio técnico que se realiza dentro del Hospital Provincial Docente Ambato.

Existe un formato que el director del departamento de sistemas ha elaborado para llevar una bitácora de los diversos soportes técnicos que ha realizado, donde se documenta:

Encabezado

Se encuentra el logo del Ministerio de Salud Pública, y la institución, en este caso Hospital Provincial General Docente Ambato en el lado izquierdo y al lado derecho del encabezado se encuentra el Escudo Nacional del Ecuador.



Fig. 4.16 Encabezado del formato de Control de Trabajo / Equipos

Elaborado por: Departamento de Sistemas del Hospital Provincial Docente Ambato

Cuerpo

Se localiza un titulado “CONTROL DE TRABAJO / EQUIPOS” la Matriz en donde se llevará la documentación de trabajos de Soporte Técnicos que se ha realizado y dentro de esta matriz se encuentra:

- Fecha: Indica cuando se realizó el soporte y la hora.
- Servicio: Se especifica el área al cual corresponde la persona a la que se ha dado el soporte técnico.
- Trabajo Realizado: Es la actividad que se realizó a la persona que requiere para dar solución al problema.
- Nombre: Se indica quién es la persona que solicitó ayuda de soporte Técnico.

- Firma: Se encuentra la rúbrica de la persona que recibió el soporte una vez que el trabajo ha sido corregido; en algunas ocasiones también se solicita el sello del funcionario.

CONTROL DE TRABAJO / EQUIPOS				
FECHA	SERVICIO	TRABAJO REALIZADO	NOMBRE	FIRMA
	Trabajo Visual	Reparación de impresora Epson TX300F	Lety Rosa	
	Obat	Chequeo de examen	Wilson Sandoval	
	Exámen Humano	Uso de Auriculares	Diana Borjas	
17-03-2014 16:30h	Exámen Humano	Recarga de pilas	Lic Ester SANCHEZ	

Fig. 4.17 Cuerpo del formato de Control de Trabajo / Equipos

Elaborado por: Departamento de Sistemas del Hospital Provincial Docente Ambato

Pie de Página

Se encuentra la información del Hospital Regional Docente Ambato como es su dirección y sus teléfonos en su lado derecho y al lado izquierdo una Bandera Nacional del Ecuador.



Fig. 4.18 Pie de página del formato de Control de Trabajo / Equipos

Elaborado por: Departamento de Sistemas del Hospital Provincial Docente Ambato

Una vista general del formato de control de trabajo / equipos es el que consta en el Anexo 2.

El segundo formato que se utiliza dentro del departamento de sistemas del Hospital Provincial Docente Ambato sirve para cuando se desea dar un mantenimiento de equipos para algún departamento; es una especie de “checklist” en la que el Director del departamento señala los trabajos realizados al equipo de cómputo de una lista de actividades que no tienen una regulación directa de por parte de la Institución o de algún organismo que regule esta área, sino que se ha visto la necesidad de instalarlos y limitarlos en el desarrollo del departamento desde su creación, justamente para limitar al funcionario hacer actividades que no competen a sus funciones laborales.

Aunque este formato se lo lleva de manera manual, se encuentran claramente delimitadas dos áreas en la matriz:

En la parte superior se encuentra la cabecera donde el equipo identificado por su número de activo dentro de la Institución. En esta misma área en la parte inferior se encuentra un detalle del equipo con la información que el Director considera necesarias identificar para su reconocimiento posterior

<p> EQUIPO: <i>monitoreo de</i> <i>CD 16 96 43 33 25</i> <i>W-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> </p>	<p> <i>VC 1</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> <i>HP-0111 00 24 97 80 2C 1A</i> </p>																

Fig. 4.19 Cabecera de formato de Mantenimiento de Equipos
Elaborado por: Departamento de Sistemas del Hospital Provincial Docente Ambato

Finalmente se encuentra el cuerpo del Formato donde consta un listado de actividades y que es señalado con un visto o una “X” según al trabajo realizado bajo cada columna de la cabecera. El formato completo lo se lo puede observar en el anexo 3.

Estos son los dos únicos formatos que sobrelleva el departamento de Sistemas para todas sus actividades diarias, siendo un alto grado de riesgo ya que esta información no se encuentra estandarizada ni aceptada por algún organismo regulatorio superior o externo. Además esta documentación no es informada ni enviada a la gerencia de la institución por lo que no existe conocimiento de esta problemática sino que es guardada y no precisamente bajo normas de seguridad adecuadas o digitalizadas para su sustento, simplemente a la espera de que si existiera alguna regulación o auditoría esa documentación sería usada para su sustento.

En el análisis de que surgieron del control de riesgos en la segunda etapa de la investigación, las mismas que fueron delimitadas por su grado de riesgo en el Hospital Provincial Docente Ambato se observa que estos dos formatos no abastece la cantidad de documentación normalizada de respaldo ya que las áreas a ser consideradas son las siguientes:

- Análisis de riesgos de sistemas e infraestructura
- Análisis de riesgo sistemas e infraestructura por criminalidad y sucesos físicos
- Análisis de riesgo datos e información por negligencia de usuarios y decisiones institucionales
- Análisis de riesgo datos e información por criminalidad y sucesos físicos

Estas son las Pruebas de riesgos que observadas dentro de la gestión de riesgos que maneja el departamento de sistemas del Hospital Provincial Docente Ambato y que en cierto modo la estructura de sus formatos han sido viabilizados hacia una adecuada administración de las problemáticas existentes por parte de los funcionarios pero lastimosamente no han sido lo suficientemente adaptados o incluso no se han realizado otros formatos para

documentar la gran cantidad de anomalías y riesgos presentes en toda la infraestructura física, lógica, seguridades, daños, etc., que también se dan en la cotidianidad de la institución.

Si se analiza los formatos se observa que la información recopilada no es la suficiente dentro de sus mismos requerimientos; es el caso de que en algunos documentos se encuentran datos que no son llenos. Por ejemplo:

En el Anexo 2, Anexo 4 y Anexo 5 se puede observar que no constan fechas en la que se realizaron los trabajos; en los mismos anexos en la columna “Nombre” no se encuentra el nombre completo (nombre y apellido) sino solo el apellido del funcionario (en algunos casos), esto puede ser de confusión en el caso de que dos o más funcionarios posean el mismo apellido; en la columna “trabajo realizado” no se especifica la serie o el código que tiene el dispositivo dentro de la institución, ni el modelo del equipo haciendo que dicha información sea necesaria para aplicar garantías en caso de daños totales en el equipo y a lo largo de los anexos que se ha tomado a lazar se encuentra problemáticas de esta índole; cabe destacar que en el anexo 6 se encuentra correctamente los datos ingresados en cada uno de sus requerimientos y esta es la manera en que deberían estar registrados los anexos con falta de información mencionados anteriormente.

4.3. ETAPA 3 - NORMATIVAS INTERNACIONALES

Con relación a la seguridad de la información existen una variedad de normativas internacionales; se ha realizado un cuadro comparativo para el estudio de la normativa que más se apegue a las necesidades de la institución de salud, y son las siguientes:

COMPARATIVA DE NORMAS INTERNACIONALES	
ESTÁNDAR RFC2196	<ul style="list-style-type: none">• Usado en la práctica de la seguridad de la información.• Pone en práctica mediante procedimientos descritos de administración de sistemas.• Debe obligar al cumplimiento de las acciones

	<p>relacionadas mediante herramientas de seguridad.</p> <ul style="list-style-type: none"> • Detecta fugas o errores. • Define claramente las áreas de responsabilidad de los usuarios, administradores y dirección, y tener un uso responsable para toda situación posible.
ESTÁNDAR IT BASELINE PROTECTION MANUAL	<ul style="list-style-type: none"> • El IT Baseline Protection Manual presenta un conjunto de recomendaciones de seguridad, establecidas por la Agencia Federal Alemana para la Seguridad en Tecnología de la Información.
ESTÁNDAR ISO 27001	<ul style="list-style-type: none"> • Su título completo en realidad es BS 7799 -2:2005 (ISO/IEC 27001:2005). • Fue preparado por el JTC 1 y en el subcomité SC 27, IT Security Techniques. La versión que se considerará es la primera edición, de fecha 15 de octubre de 2005. • El conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta son: <ul style="list-style-type: none"> ▪ ISO/IEC 27000 Fundamentals and vocabulary. ▪ ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005). ▪ Publicado el 15 de octubre del 2005. ▪ ISO/IEC 27002 Code of practice for information security management. ▪ Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005. ▪ ISO/IEC 27003 ISMS implementation guidance (en desarrollo). ▪ ISO/IEC 27004 Information security management measurement (en desarrollo). ▪ ISO/IEC 27005 Information security risk management (basado en ISO/IEC 13335

	<ul style="list-style-type: none"> ▪ MICTS Part 2 e incorporado a éste; en desarrollo).
ESTÁNDAR ISO/IEC 17799	<ul style="list-style-type: none"> • Denominado también como ISO 27002. • Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a los responsables, • Implanta y mantener sistemas de gestión de la seguridad de la información.
ESTÁNDAR ISO/IEC 27000:2009	<ul style="list-style-type: none"> • Es parte de una familia en crecimiento de Estándares para Sistemas de Administración de Seguridad de la información (ISMS), • Es un estándar internacional titulado “Tecnología de la Información – Técnicas de Seguridad – Sistemas de Administración de la Seguridad de la Información – Visión general y Vocabulario” • El estándar fue desarrollado por el sub-comité 27 (SC27) del primer Comité Técnico Conjunto (JTC1), de la ISO (International Organization for Standardization) y el IEC (International Electrotechnical Commission)
ESTÁNDAR ISO/IEC 18028-2:2006	<ul style="list-style-type: none"> • Define una arquitectura de seguridad para red, ofreciendo seguridad a redes de extremo a extremo. La arquitectura puede ser aplicada a varias clases de redes donde la seguridad extremo a extremo es una preocupación independiente de la tecnología subyacente de la red • Estándar mundial de facto para la gestión de servicios informáticos de calidad, buscando la satisfacción integral del cliente
ITIL	<ul style="list-style-type: none"> • Estándar mundial de facto para la gestión de servicios informáticos de calidad, buscando la satisfacción integral del cliente.

COBIT 5	<ul style="list-style-type: none"> • Utilizada para el adecuado control de proyectos de tecnología, los flujos de información y los riesgos inherentes a los procesos internos.
----------------	--

Tabla 4.12 Comparativa de Normas Internacionales

Elaborado por: Investigador

Resumen de Análisis de Normativas Internacionales

Se concluye que de todas las normas analizadas, la metodología Cobit es la más aplicable a la estructura del Departamento de sistemas del Hospital Provincial Docente Ambato, porque pone énfasis en los modelos de gestión por procesos, en la actualidad son una necesidad y obligatoriedad en el ámbito estatal a nivel de instituciones públicas.

Cobit no requiere una gran inversión económica, además todo el proceso para su implementación se realiza con la adquisición de la metodología de Implantación.

Aunque al igual que la norma ISO 27001, es difícil calcular el costo de implementación, la ventaja sobre esta radica en que cuenta con recursos electrónicos para su implementación, antes se necesita de ser miembro de ISACA la página web oficial de Cobit, comprar los manuales de capacitación, la búsqueda de asesoría externa, los pasos para su activación, implementación todos tienen un valor, aunque en consideración podrá ser menor a las ISO 27001 que requiere mayor tiempo de inversión, recodificación de procesos, incluso pilotaje antes de su implementación.

Cobit 5 enfoca la seguridad de la información en los procesos de las empresas, lo cual es esencial para garantizar la disminución de riesgos informáticos,

Cobit es útil para las empresas que se encuentran bajo presión, para mantener los riesgos relacionados con el TI a un nivel aceptable, logrando la optimización de costos de la tecnología y los servicios TI; la información es uno de los

valores esenciales en las organizaciones, por lo que su implementación permitirá mejorar la gestión de la información.

La siguiente tabla de resumen está realizada en base a investigación en la web, y a través de una comparativa anterior de cada una de las normativas analizadas y resumidas en un cuadro comparativo en función de Cobit dependiendo de sus características:

FORTALEZAS	
COBIT	<ul style="list-style-type: none"> • Fuerte en controles y métricas de TI • Contemplan ciclos de mejora continua • Se alinea con los otros estándares para mejorar sus debilidades • Cobit no es sólo para auditores, es un marco para todos los usuarios de TI • Ayuda a las Organizaciones a mapear sus procesos de acuerdo a las mejores prácticas recopiladas por ISACA. [33]
ITIL	<ul style="list-style-type: none"> • Fuerte en el desarrollo de procesos • ITIL utiliza un lenguaje más directo que ayuda a la hora de implementarlo. [33]
ISO	<ul style="list-style-type: none"> • Su fortaleza se establece en los controles de seguridad • Establece una valoración de los riesgos a los que se enfrenta una organización en materia de seguridad de la información. [33]

Tabla 4.13 Comparativa de Normativa según sus Fortalezas

Elaborado por: Investigador

DEBILIDADES	
COBIT	<ul style="list-style-type: none"> • No contiene un conjunto detallado de las mejores prácticas orientadas a proceso • Cobit está sobrecargado con un lenguaje de tipo consultoría y en consecuencia es necesario descifrarlo antes de ser aplicado.
ITIL	<ul style="list-style-type: none"> • Limitaciones en el desarrollo de sistema de seguridad • TIL sirve de suplemento a Cobit y no al revés.
ISO	<ul style="list-style-type: none"> • No determina de manera clara como hacer las cosas.

Tabla 4.14 Comparativa de Normativa según sus Debilidades

Elaborado por: Investigador

FUNCIONES	
COBIT	<ul style="list-style-type: none"> • Mapeo de procesos IT.
ITIL	<ul style="list-style-type: none"> • Mapeo de gestión de niveles de servicio de IT.
ISO	<ul style="list-style-type: none"> • Marco de referencia de seguridad de la información.

Tabla 4.15 Comparativa de Normativa según sus Funciones

Elaborado por: Investigador

ÁREAS	
COBIT	<ul style="list-style-type: none"> • 4 procesos y 34 dominios
ITIL	<ul style="list-style-type: none"> • 9 procesos
ISO	<ul style="list-style-type: none"> • 10 dominios

Tabla 4.16 Comparativa de Normativa según sus Áreas

Elaborado por: Investigador

CREADOR	
COBIT	<ul style="list-style-type: none"> • ISACA
ITIL	<ul style="list-style-type: none"> • Ogc
ISO	<ul style="list-style-type: none"> • ISO International Organization for Standardization

Tabla 4.17 Comparativa de Normativa según su Creador
Elaborado por: Investigador

UTILIDAD	
COBIT	<ul style="list-style-type: none"> • Auditoria de sistemas de información • No existe un certificado en las prácticas indicadas por Cobit, aunque ISACA sí ofrece la posibilidad a título personal de obtener certificaciones como: (CISA) Certified Information Systems Auditor (CISM) Certified Information Security Manager (CGEIT) Certified in the Governance of Enterprise IT (CRISC) Certified in Risk and Information Systems Control
ITIL	<ul style="list-style-type: none"> • Gestión de niveles de servicio
ISO	<ul style="list-style-type: none"> • Cumplimiento del estándar de seguridad • Certificación ISO 27001 • ISO 27001

Tabla 4.18 Comparativa de Normativa según su Utilidad
Elaborado por: Investigador

4.4. ETAPA 4 - ENTORNO COMPETITIVO

4.4.1 Establecimiento de Procesos y Funciones del Departamento de Sistemas

En el proceso de análisis, clasificación, reducción y control de riesgos se obtuvieron resultados que brinda una proyección de qué procesos son los que se realiza en el departamento de sistemas con mayor habitualidad, que serán el punto de partida para establecer los procesos actuales.

El departamento de sistemas, deberá estar posicionada dentro de la estructura organizacional del Hospital Provincial Docente Ambato en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades de usuarios; también deberá participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica asegurando la cobertura de servicios a todas las unidades del Hospital Provincial docente Ambato. Esta estructura debe reflejar las necesidades institucionales, y deben ser revisadas periódicamente para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos.

Para esto se parte de la estructura orgánica que el Hospital Provincial Docente Ambato actualmente lleva en su actual implantación y dentro del mismo consta el departamento de sistemas (TICS), para su incidencia en los procesos y funciones dentro de las diferentes áreas de la institución.

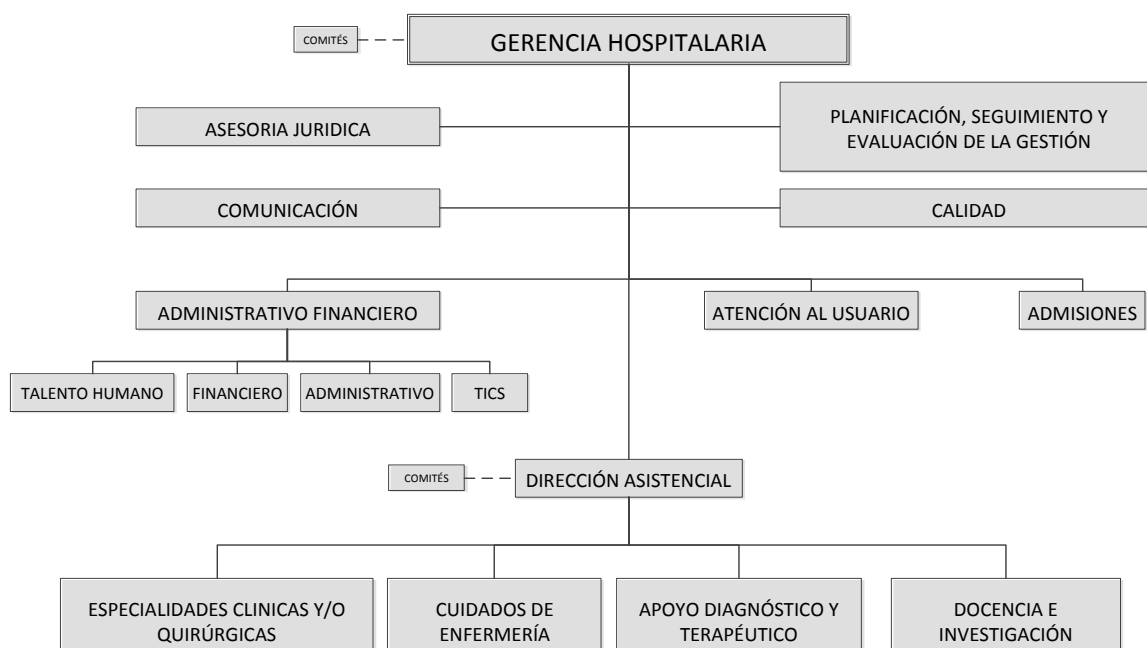


Fig. 4.20 Estructura Orgánica – Hospitales Generales, Especializados y de Especialidades de 70 camas o más

Elaborado por: Provisto por el Departamento de Sistemas del Hospital Provincial Docente Ambato

En el análisis de riesgos se ha podido verificar que las áreas dentro de la institución, se encuentran con un mayor grado de vulnerabilidad y precisamente éstas serán aquellas en las que apremia realizar mayores y mejores medidas de control de seguridad; es por esto que el departamento de sistemas pondrá enfoque a procesos que den solución de dichos riesgos; estos procesos son:

- Procesos Organizativos
- Procesos de recursos Físicos
- Procesos Técnicos
- Procesos Personales
- Procesos contra Acciones Hostiles

Procesos Organizativos

El Departamento de Sistemas definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en el Hospital Provincial Docente Ambato; estos se actualizarán permanentemente incluyendo las tareas, responsables de su ejecución, procesos de excepción, el enfoque de cumplimiento y el control de procesos que han sido normalizados, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Será necesario que se establezca procedimientos de comunicación, difusión y coordinación entre las funciones del Departamento de Sistemas y las funciones propias de la organización.

Es necesario realizar controles bajo estándares y/o normativas Internacionales para su mejor administración y seguridad, encaminando a un adecuado servicio de calidad que presta el departamento de Sistemas. [34]

Procesos de Recursos Físicos

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará

como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario.

El departamento de sistemas elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia.

Es de vital importancia tomar en cuenta que las instalaciones físicas adecuadas incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros. [34]

Procesos Técnicos

El Departamento de Sistemas definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

Se definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos. El Departamento de Sistemas presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

Será necesario implementar y administrar seguridades a nivel de hardware, realizando un monitoreo de seguridad y acciones correctivas sobre las vulnerabilidades o inconvenientes de seguridad identificados, a fin de que los bienes tecnológicos informáticos se encuentren protegidos ante cualquier tipo de amenaza .

Es necesario definir, aprobar y difundir procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen por lo que es preciso tener seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas, cuentas de usuario y servicios de tecnología de información de la entidad; también efectuar revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.

Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales. Será necesario medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.
[34]

Procesos Personales

El plan de capacitación estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño institucional.

La asignación de funciones y sus respectivas responsabilidades avalarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro del departamento de sistemas la supervisión de roles y funciones del personal dentro de cada área, para gestionar un adecuado rendimiento y

evaluar las posibilidades de reubicación e incorporación de nuevo personal. [34]

Procesos Contra Acciones Hostiles

Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables para poder controlar el robo, sabotaje vandalismo que existe por personas externas y de ser el caso internas hacia estos bienes.

El Departamento de Sistemas debe realizar una revisión de la red y de los usuarios que acceden a ésta, para poder identificar las intromisiones no autorizadas a la red. [34]

4.4.2 Funciones del Departamento de Sistemas

Es necesario segregar funciones dentro del personal del departamento de sistemas aun siendo el caso de que una sola persona administre todas las áreas; ya que así se podrá visualizar de mejor manera la importancia de que dicho personal es necesario incrementar para poder alcanzar las metas y objetivos trazados dentro del departamento dando el soporte debido a todos los usuarios de la Institución.

Será de un análisis conjunto con las máximas autoridades, personal de Talento Humano y el Director del Departamento de Sistemas lograr alcanzar la implementación de estos perfiles con personal calificado en estas áreas dando paso al cumplimiento de funciones que son:

Jefe de Sistemas:

- Dirigir y supervisar al personal del departamento de sistemas.
- Brindar un funcionamiento adecuado y oportuno de los sistemas informáticos de la Institución.

- Realizar soporte técnico y capacitación a las áreas usuarias en todos los sistemas automatizados de la Institución.
- Coordinar y supervisar el desarrollo de los sistemas informáticos de la Institución.
- Administrar las bases de datos, sistemas operativos y seguridades lógicas y físicas.
- Vigilar permanentemente que exista una adecuada comunicación y correcto funcionamiento de la red informática y de comunicaciones.
- Implementar políticas de control y seguridad de la información y de los equipos.
- Implantar normas de control de calidad de la información que se procesa.
- Recomendar estrategias de inversión en equipos electrónicos y manejo de las informaciones en términos de calidad-costo-beneficio.
- Coordinar y supervisar el mantenimiento preventivo de equipos de la entidad.
- Supervisar el uso correcto de los equipos y software instalado, revisa que los manuales de usuario estén correctamente elaborados y actualizados.
- Elaborar, ejecutar y difundir los planes de contingencias y/o de emergencias.
- Participar en la elaboración y ejecución de planes operativos, plan de contingencia del departamento de sistemas.
- Establecer los requerimientos informáticos de hardware y software de la Institución en coordinación con los otros departamentos y áreas.
- Elaborar información adicional requerida por los organismos de control.
- Verificar el cumplimiento de los contratos vigentes respecto a su área.
- Realizar labores solicitadas por su Jefe inmediato superior o gerencia general.
- Supervisar las innovaciones tecnológicas viables para los requerimientos de la Institución.

- Definir la estructura organizacional de su departamento y las funciones del equipo humano bajo su dirección y recomendar los cambios en la organización de su departamento cuando lo amerite.
- Proporcionar la disponibilidad de los datos mediante un procedimiento de respaldo en caso de fallas humanas o de los sistemas.
- Coordinar el entrenamiento y desarrollo del personal bajo su supervisión.
- Mantener los controles internos inherentes al departamento en forma que pueda ser auditado.
- Supervisar que la institución cuente con los reportes gerenciales necesarios y requeridos de los sistemas en producción.

Asistente de Sistemas:

- Coordinar y dirigir el proceso de desarrollo, mantenimiento e implementación de sistemas con mejoras y adecuaciones que satisfagan las necesidades actuales y futuras de operación de la Institución.
- Codificar, revisar y probar los programas diseñados.
- Validar con el usuario si los programas desarrollados cumplen con los requerimientos planteados, a través de pruebas y coordinar las mejoras y/o modificaciones de programas existentes.
- Ayudar a los usuarios en sus necesidades diarias, en relación al manejo de los sistemas.
- Analizar y priorizar las solicitudes de mantenimiento a los sistemas en producción y soporte técnico al equipo computacional requeridas por las áreas usuarias.
- Documentar los programas y aplicaciones que conforman los sistemas de la Institución.
- Realizar soporte continuo y entrenamiento a los usuarios de todos los departamentos de la Institución.
- Realizar el mantenimiento de software y Hardware y demás aplicaciones.

- Garantizar el proceso de instalación y mantenimiento de equipos (PC, UPS, impresoras, terminales, disco duro, etc.) con el fin de que se realice según los requerimientos de los usuarios y atendiendo a estándares de calidad.
- Generar reportes para el óptimo desempeño de los roles de los usuarios.
- Realizar otras labores relacionadas al cargo solicitadas por su jefe inmediato superior o por la Gerencia General.
- Administrar las redes y comunicaciones en todos sus aspectos de la Institución; tanto LAN como WAN.

Asistente de Soporte Técnico.

- Coordinar y dirigir el proceso de desarrollo, mantenimiento e implementación de sistemas con mejoras y adecuaciones que satisfagan las necesidades actuales y futuras de operación de la Institución.
- Codificar, revisar y probar los programas diseñados.
- Validar con el usuario si los programas desarrollados cumplen con los requerimientos planteados, a través de pruebas y coordinar las mejoras y/o modificaciones de programas existentes.
- Ayudar a los usuarios en sus necesidades diarias, en relación al manejo de los sistemas.
- Revisar, analizar y priorizar las solicitudes de mantenimiento a los sistemas en producción y soporte técnico al equipo computacional requeridas por las áreas usuarias.
- Documentar los programas y aplicaciones que conforman los sistemas de la Institución.
- Brindar soporte continuo y entrenamiento a los usuarios de todos los departamentos de la Institución.
- Custodiar la instalación y mantenimiento de software y Hardware y demás aplicaciones.
- Llevar un inventario de los equipos de computación.

- Garantizar el proceso de instalación y mantenimiento de equipos (PC, UPS, impresoras, terminales, disco duro, etc.) con el fin de que se realice según los requerimientos de los usuarios y atendiendo a estándares de calidad.
- Realizar las actividades necesarias cuando se reciba reportes de gestión acerca de eventualidades con los servicios que presta el área.
- Administrar los servicios de Internet e Intranet de la Institución, controlar los accesos y usuarios de toda la Institución.
- Ejecutar y controlar todos los respaldos de la información de los distintos equipos.
- Controlar el buen uso de los equipos y aplicación de Normativas.
- Asesorar permanentemente a los usuarios en el uso correcto de los equipos

4.5. DESARROLLO DEL MANUAL DE PROCESOS

Para poder entender la aplicación de COBIT se debe partir que éste se divide en tres procesos que son: dominios, procesos y actividades.

Para desarrollar un manual de procesos hay que comprender que la misión de COBIT es “investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento” [35].

El objetivo de COBIT 5 es proveer un enfoque de buenas prácticas a la hora de implementar un GEIT basado en un ciclo de vida de mejora continua que debe adaptarse a las necesidades específicas de la empresa. [36].

En el siguiente esquema se aprecia la metodología del Manual de Procesos a desarrollar en base a la descripción de procesos que la Normativa COBIT 5 establece para su aplicación; esto, para cada uno de los 37 procesos que COBIT 5 establece, a diferencia de COBIT 4.1 que son 34 procesos que ofrece

esta versión, ayudando a una mejor estructuración del formato para cada manual de procesos realizado.

Descripción del proceso:

DESCRIPCIÓN DEL PROCESO.

DS5 Garantizar la Seguridad de los Sistemas

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

Fig. 4.21 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Indicadores del proceso:

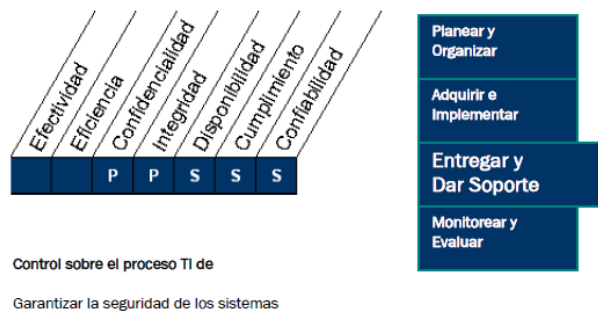


Fig. 4.22 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Objetivos de TI:

Que satisfice el requerimiento del negocio de TI para

Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad

Fig. 4.23 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Objetivos del proceso:

Enfocándose en

La definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad

Fig. 4.24 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Prácticas clave:

Se logra con

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular

Fig. 4.25 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Métricas:

Y se mide con

- El número de incidentes que dañan la reputación con el público
- El número de sistemas donde no se cumplen los requerimientos de seguridad
- El número de de violaciones en la segregación de tareas

Fig. 4.26 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Gobierno y recursos de TI:

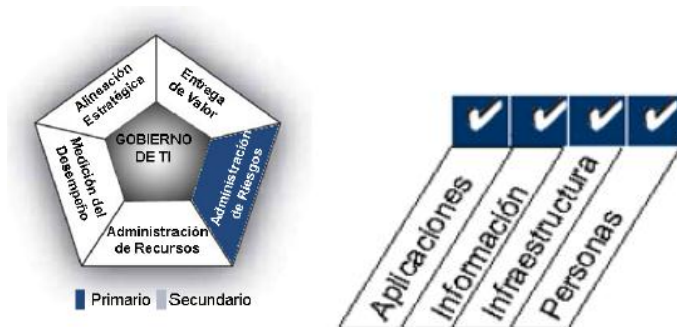


Fig. 4.27 Descripción del Proceso

Elaborado por: www.isaca.org/Knowledge-Center/.../COBIT5-and-InfoSec-Spanish.ppt Pág. 9

Finalmente se puede indicar que COBIT 5 es una metodología que ha sufrido cambios desde su aparición hasta la actualidad, y busca organizar, controlar desde todo tipo de vista las funciones, operaciones de las instituciones públicas, privadas, agrupadas en procesos o no, con el objetivo que puedan alcanzar sus metas.

“Definición” (campo opcional)

“QUÉ”, son los requerimientos que preceden a la acción de mejora (marco de referencia) que los “ejecutivos” (autoridades, encargados, directores, etc.), [35] deben cubrir estas necesidades:

- Brindar un enfoque de negocios que permita la alineación entre las metas de negocio y de TI.
- Establecer una orientación a procesos para definir el alcance y el grado de cobertura, con una estructura definida que permita una fácil navegación en el contenido.
- Ser generalmente aceptable al ser consistente con las mejores prácticas y estándares de TI aceptados, y que sea independiente de tecnologías específicas.
- Proporcionar un lenguaje común, con un juego de términos y definiciones que sean comprensibles en general para todos los Interesados.
- Ayudar a satisfacer requerimientos regulatorios, al ser consistente con estándares de gobierno corporativo generalmente aceptados (COSO) y con controles de TI esperados por reguladores y auditores externos.

Campos: Código, Dominio y Proceso

Los dominios de gestión tienen como responsabilidad planear, construir, ejecutar y monitorear los riesgos dentro del TI; además agrupa los objetivos de control dentro del desarrollo en el tiempo de inversión del TI. Los dominios de gobierno contienen cinco procesos los cuales se enfocan en el riesgo relacionado con los intereses de terceros y son:

1. Evaluar, Dirigir y Monitorear (EDM)
2. Alinear, Planificar y Organizar (APO)
3. Construcción, Adquisición e Implementación (BAI)

4. Entregar, dar Servicio y Soporte (DSS)
5. Monitorear, Evaluación y Verificación (MEA)

Asegurar que el riesgo de la empresa y la tolerancia sean controlados y que su impacto sea identificado y gestionado con una tolerancia mínima de fallos. COBIT 5 ofrece los 5 Dominios mencionados y 37 procesos descritos en [36] que se relacionan internamente en que se relacionan con las metas de TI; estas son:

Evaluar, Dirigir y Monitorear

1. **EDM01** Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno
2. **EDM02** Asegurar la Entrega de Beneficios
3. **EDM03** Asegurar la Optimización del Riesgo
4. **EDM04** Asegurar la Optimización de los Recursos
5. **EDM05** Asegurar la Transparencia hacia las partes interesadas

Alinear, Planificar y Organizar

6. **APO01** Gestionar el Marco de Gestión de TI
7. **APO02** Gestionar la Estrategia
8. **APO03** Gestionar la Arquitectura Empresarial
9. **APO04** Gestionar la Innovación
10. **APO05** Gestionar el portafolio
11. **APO06** Gestionar el Presupuesto y los Costes
12. **APO07** Gestionar los Recursos Humanos
13. **APO08** Gestionar las Relaciones
14. **APO09** Gestionar los Acuerdos de Servicio
15. **APO10** Gestionar los Proveedores
16. **APO11** Gestionar la Calidad

- 17. **APO12** Gestionar el Riesgo
- 18. **APO13** Gestionar la Seguridad

Construcción, Adquisición e Implementación

- 19. **BAI01** Gestionar los Programas y Proyectos
- 20. **BAI02** Gestionar la Definición de Requisitos
- 21. **BAI03** Gestionar la Identificación y la Construcción de Soluciones
- 22. **BAI04** Gestionar la Disponibilidad y la Capacidad
- 23. **BAI05** Gestionar la introducción de Cambios Organizativos
- 24. **BAI06** Gestionar los Cambios
- 25. **BAI07** Gestionar la Aceptación del Cambio y de la Transición
- 26. **BAI08** Gestionar el Conocimiento
- 27. **BAI09** Gestionar los Activos
- 28. **BAI10** Gestionar la Configuración

Entregar, dar Servicio y Soporte

- 29. **DSS01** Gestionar las Operaciones
- 30. **DSS02** Gestionar las Peticiones y los Incidentes del Servicio
- 31. **DSS03** Gestionar los Problemas
- 32. **DSS04** Gestionar la Continuidad
- 33. **DSS05** Gestionar los Servicios de Seguridad
- 34. **DSS06** Gestionar los Controles de los Procesos del Negocio

Monitorear, Evaluación y Verificación

- 35. **MEA01** Supervisar, Evaluar y Valorar Rendimiento y Conformidad
- 36. **MEA02** Supervisar, Evaluar y Valorar el Sistema de Control Interno
- 37. **MEA03** Supervisar, Evaluar y Valorar la Conformidad con los
Requerimientos Externos

Campo: Objetivos

En el manual de procesos es necesario especificar un “porqué” de dicho manual, dentro de las necesidades y acorde a la administración de la información que maneja el departamento de sistemas dentro de la Institución; este objetivo especificado en [35], donde se dará a conocer a las Autoridades si la información administrada será capaz de:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse
- Cuento con un manejo juicioso de los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Campos: Justificación y Metodología

La justificación es el enfoque que incorporará las TI con la gerencia para desarrollar estrategias y poder así entregar servicios de forma clara y beneficiosa.

La metodología es la forma cómo el departamento de sistemas aplicará el manual de procesos en conjunto con las altas autoridades de la Institución, también dependerá del correcto y adecuado entendimiento de las capacidades de TI que se dispone actualmente; y la aplicación prioritaria de los requerimientos que se necesita para cuantificar los objetivos planteados.

Campos: Criterios de Información Afectados

En la relación de las metas con los procesos se usará una escala donde “P” indica principal, cuando hay una relación importante y “S” indica secundario, cuando todavía hay un vínculo fuerte, pero menos importante.

Existen seis objetivos de negocio en donde la información deberá adaptarse a criterios de control en donde COBIT menciona [35] a los siguientes:

“Efectividad: tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

Eficiencia: consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.

Confidencialidad: se refiere a la protección de información sensitiva contra revelación no autorizada.

Integridad: está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

Cumplimiento: tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

Confiabilidad: se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.”

Campo: Roles

“Quien” son todos los involucrados internos y externos que proveen o dan servicio a la Institución que tienen necesidades específicas de gobierno y control para alcanzar la calidad de servicio como lo señala en [35] y son:

- Interesados dentro de la empresa que tienen interés en generar valor de las inversiones en TI
- Interesados internos y externos que proporcionan servicios de TI
- Interesados internos y externos con responsabilidades de control/riesgo”

Campo: Recursos

“CÓMO”, para poder alcanzar las metas que la TI busca, se debe hacer uso de personas, infraestructura de tecnología para poder ejecutar la automatización del negocio, para lo cual es necesario que la empresa invierta en recursos necesarios para solventar una capacidad técnica apropiada.

En [35], los recursos que reconoce COBIT son:

Aplicaciones: incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

Información: son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

Infraestructura: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

Personas: son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing (tercerizadores) o contratadas, de acuerdo a como se requieran.

Campo: Indicadores

En los procesos para gestión de TI se dispone de 17 metas relacionadas [37] con la TI:

1. Alineamiento de TI y la estrategia de negocio
2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas
3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI

4. Riesgos de negocio relacionados con las TI gestionados
5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI
6. Transparencia de los costes, beneficios y riesgos de las TI
7. Entrega de servicios de TI de acuerdo a los requisitos del negocio
8. Uso adecuado de aplicaciones, información y soluciones tecnológicas
9. Agilidad de las TI
10. Seguridad de la información, infraestructura de procesamiento y aplicaciones
11. Optimización de activos, recursos y capacidades de las TI
12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.
14. Disponibilidad de información útil y relevante para la toma de decisiones
15. Cumplimiento de las políticas internas por parte de las TI
16. Personal del negocio y de las TI competente y motivado
17. Conocimiento, experiencia e iniciativas para la innovación de negocio

De acuerdo al mapeo entre las Metas relacionadas con las TI de COBIT 5 y los Procesos se tomarán en consideración las metas Relacionadas especificadas los criterios (Principal o Secundario) que se especifican en [37].

Campo: Métricas

Las métricas que define COBIT van de la mano con las metas y están divididas en tres niveles:

1. “Las metas y métricas de TI que definen lo que el negocio espera de TI (lo que el negocio usaría para medir a TI)
2. Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI (cómo sería medido el dueño del proceso de TI)
3. Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas).” [35].

Campo: Prácticas

Cobit 5 proporciona requerimientos necesarios para una gestión y gobierno efectivo los cuales afectarán a cada proceso de forma directa, siendo estos:

- “Declaraciones sobre acciones que proporcionan beneficios, optimizan el nivel de riesgo y el uso de los recursos
- Alineadas con los estándares y buenas prácticas más relevantes y comúnmente aceptadas
- Genéricas y, por tanto, necesitan adaptarse a cada empresa.
- En los procesos se contemplan los roles de las figuras de TI y de negocio (de principio a fin).” [37].

Los directivos del Hospital Provincial Docente Ambato deberán tomar decisiones relativas a las prácticas de gobierno y gestión tomando en cuenta los siguientes aspectos:

- “Seleccionando aquéllas que sean aplicables y, de entre éstas, decidiendo cuáles se implementarán
- Añadiendo y/o adaptando prácticas, cuando sea necesario
- Definiendo y añadiendo prácticas no relacionadas con las TI, para la integración en los procesos de negocio

- Eligiendo cómo implementarlas (frecuencia, ámbito, automatización, etc.)
- Aceptando el riesgo por no implementar aquéllas que podrían ser aplicables” [37].

Campo: Actividades

“Se definen como las ‘directrices para lograr las prácticas de gestión que permitan un gobierno y una gestión satisfactorios de las TI de una empresa’. Las actividades de COBIT 5 proporcionan el cómo, porqué y qué implementar en cada una de las prácticas de gestión y gobierno para mejorar el rendimiento y/o identificar una solución TI y el riesgo en la prestación de los servicios. Este material es de uso por parte de:

- **Equipo de dirección**, proveedores de servicio, usuarios finales y profesionales de las TI que necesiten planificar, construir, ejecutar o supervisar las TI de una empresa.
- **Profesionales de aseguramiento** que deban dar su opinión respecto a las implementaciones existentes, a las propuestas, o respecto a mejoras necesarias.” [37].

El Equipo de Dirección y los profesionales de aseguramiento serán los responsables en hacer cumplir cada una de las actividades que se especifica para lograr las prácticas de gestión de la institución. Las actividades encaminarán a alcanzar las prácticas de gobierno y de gestión; por lo tanto es necesario que las actividades tengan el siguiente enfoque:

“Describen el conjunto necesario y suficiente de pasos relativos a las acciones de una implementación para lograr GP/MP

- Consideran las entradas y salidas del proceso
- Se basan en estándares y buenas prácticas comúnmente aceptadas
- Ayudan a establecer roles y responsabilidades claros

- No son prescriptivas y necesitan adaptarse y desarrollarse en procedimientos específicos y adecuados a la empresa.” [37].

Los manuales a realizarse son aquellos que señalaron un mayor grado de riesgos y han sido establecidos en los procesos del Departamento de Sistemas que son:

- Procesos Organizativos
- Procesos de Recursos Físicos
- Procesos Técnicos
- Procesos Personales
- Procesos contra Acciones Hostiles

En cada uno de ellos se ha efectuado Normas para su tratamiento en las siguientes áreas:

PROCESOS ORGANIZATIVOS:

1. Proceso:

APO01 Gestionar el marco de gestión de TI

Subprocesos:

APO01.03 Mantener los habilitadores del sistema de administración.

APO01.08 Mantener la conformidad con políticas y procedimientos.

PROCESOS DE RECURSOS FÍSICOS:

2. Proceso:

APO13 Gestionar la seguridad.

PROCESOS TÉCNICOS:

3. Proceso:

APO03: Gestionar la arquitectura empresarial.

Subproceso:

APO03.02 Herramientas y automatización.

4. Proceso:

DSS05 Gestionar los servicios de seguridad

PROCESOS PERSONALES:

5. Proceso:

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.

Subprocesos:

EDM01.02 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.

6. Proceso :

APO01 Gestionar el marco de gestión de TI.

Subprocesos:

APO01.02 Establecer roles y responsabilidades.

7. Proceso:

APO03 Gestionar la arquitectura empresarial.

PROCESOS CONTRA ACCIONES HOSTILES:

8. Proceso:

BAI09 Gestionar los activos.

4.5.1. Manual Técnico de Procesos Organizativos

MANUAL TÉCNICO DE PROCESOS ORGANIZATIVOS	
Código	APO
Dominio	Alinear, Planificar y Orientar
Proceso: APO01 Gestionar el marco de gestión de TI Subproceso relacionados: APO01.03 Mantener los habilitadores del sistema de administración. APO01.08 Mantener la conformidad con políticas y procedimientos.	
OBJETIVOS Definir y promulgar apropiadamente los objetivos de gestión y direcciones con respecto a la TI en el Hospital Provincial Docente Ambato. Además de establecer políticas y procedimientos para que los sigan sus gestores y su personal, para asegurar que se logran las metas de la empresa, que se minimiza el riesgo y que se consigue la conformidad.	
JUSTIFICACIÓN En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.	
METODOLOGÍA La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes. Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.	

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados			
Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiabilidad	P
Integridad	P		
Requerimientos de negocio a alcanzar			
Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.			
ROLES			
Dueño		Gerencia Hospitalaria	
Responsable		Departamento de Sistemas (TICS)	
Controlador		Administrativo Financiero	
Clientes		Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.	
Proveedores		Proveedores internos de todos los servicios relacionados y contratistas externos.	
UBICACIÓN			
Ubicación		Ecuador, Ambato, Hospital Provincial Docente Ambato.	
TIEMPO			
Ejecución		Bajo demanda	
Frecuencia		NO APLICABLE	

RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
1) Alineamiento de TI y estrategia de la organización		% de objetivos de TI dentro de la estrategia de negocio que le proporcionan el alineamiento	
2) Cumplimiento y soporte de la TI al cumplimiento de la organización de las leyes y regulaciones externas		% de iniciativas TI dentro del negocio que permiten el cumplimiento y soporte a los requerimientos internos y externos	
3) Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		Efectividad de las decisiones de la dirección ejecutiva sobre el plan táctico de TI	
4) Riesgos propios de la actividad relacionados con las TI gestionados		% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos	
7) Entrega de servicios de TI de acuerdo a los requisitos de la organización		# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa	
9) Agilidad de las TI		Tiempo de los servicios de TI	
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones		# de veces en que el servicio de TI puso en riesgo al negocio	
11) Optimización de activos, recursos y capacidades de las TI		% de activos, recursos y capacidades de las TI disponibles	
12) Capacitación y soporte de procesos de la organización, integrando aplicaciones y tecnología		# de capacitaciones y soporte integradoras de TI	

en procesos organizacionales	
13) Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	# de programas que se ajustan a los requerimientos del negocio
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
15) Cumplimiento de las políticas internas por parte de las TI	# de interrupciones al negocio debidas al servicio de TI
16) Personal de la organización y de las TI competente y motivado	% del personal que no cumplen con las políticas y requisitos del negocio
17) Conocimiento, experiencia e iniciativas para la innovación de la institución	# de acciones de capacitación, desarrollo e innovación relacionadas con las TI
PRÁCTICAS	
Práctica	Descripción
Administración del Valor de TI	Garantizar que el portafolio de inversiones de TI del Hospital Provincial Docente Ambato contenga programas que detallen el grado de complejidad relacionados con la asignación de fondos, los costos, cronogramas, funcionalidad que puedan impactar en los resultados esperados. Establecer además un análisis del riesgo en relación a diferentes escenarios.
Alineación de TI con el Negocio	Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las

	oportunidades que ofrece TI, y sobre qué debe hacer el Hospital Provincial Docente Ambato para capitalizar esas oportunidades.
Evaluación del Desempeño y la Capacidad Actual	Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de la organización, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.
Plan Estratégico de TI	Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la institución (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos.
Planes Tácticos de TI	Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados.
Administración del Portafolio de TI	Administrar de forma activa, junto con el manejo de la institución, el

	portafolio de programas de inversión de TI requerido para lograr objetivos organizacionales, estratégicos, específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.
ACTIVIDADES	
Actividades	Responsables
1) Realizar controles bajo estándares y/o normativas Internacionales para su mejor administración y seguridad, que esto inducirá al adecuado encaminamiento hacia la calidad de servicios que presta el departamento de Sistemas.	Gerencia Hospitalaria
2) Determinar y evaluar la alineación de la administración de riesgos.	Departamento de Sistemas (TICS)
3) Identificar los objetivos internos de TI y establecer el contexto del riesgo.	Departamento de Sistemas (TICS)
4) Priorizar y planear actividades de control.	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
5) Aprobar y asegurar fondos para planes de acción de riesgos.	Administrativo Financiero
6) Mantener y monitorear un plan de acción de riesgos.	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
7) Priorizar y planear actividades de inducción, capacitación y concientización sobre riesgos	Departamento de Sistemas (TICS)
8) Controlar y eliminar la utilización	Departamento de Sistemas (TICS)

de programas no autorizados y/o software 'pirata'	
9) Establecer dentro de la política de seguridad informática el respaldo de la información, que minimice la pérdida de los mismos.	Departamento de Sistemas (TICS)
10) Informar y capacitar a todo los implicado en el uso y manejo de las TI sobre las medidas de seguridad informática, relacionado con el correcto manejo de contraseñas y accesos.	Departamento de Sistemas (TICS)
11) Proteger la Red cableada expuesta	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
12) Análisis de la disponibilidad y necesidad de recursos humanos que intervienen directamente en las TI	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
13) Definir, documentar y difundir las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en el Hospital Provincial Docente Ambato.	Departamento de Sistemas (TICS)
14) Establecer la actualización permanente de las políticas, estándares y procedimientos que regulen las actividades relacionadas con TI, incluyendo las tareas, responsables de su ejecución, procesos de excepción,	Gerencia Hospitalaria, Departamento de Sistemas (TICS)

<p>el enfoque de cumplimiento y el control de procesos que han sido normalizados, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.</p>	
<p>15) Establecer procedimientos de comunicación, difusión y coordinación entre las funciones del Departamento de Sistemas y las funciones propias de la organización.</p>	<p>Gerencia Hospitalaria, Departamento de Sistemas (TICS)</p>
<p>16) Incorporar controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos mediante procedimientos de supervisión de las funciones de tecnología de información midiéndose el cumplimiento de las regulaciones y estándares definidos.</p>	<p>Gerencia Hospitalaria, Departamento de Sistemas (TICS)</p>
<p>17) Desarrollar los Procedimientos, Normas y Estándares de Seguridad que garanticen la confidencialidad, integridad y seguridad de los datos en programas y sistemas informáticos.</p>	<p>Gerencia Hospitalaria</p>
<p>18) Aprobar y establecer las políticas de seguridad informática.</p>	<p>Gerencia Hospitalaria, Departamento de Sistemas (TICS)</p>

Tabla 4.19 Manual de Procesos: Gestionar el marco de gestión de TI – Procesos Organizativos

Elaborado por: Investigador

4.5.2. Manual Técnico Procesos de Recursos Físicos

MANUAL TÉCNICO PROCESOS DE RECURSOS FÍSICOS	
Código	APO
Dominio	Alinear, Planificar y Orientar
Proceso: APO13 Gestionar la seguridad.	
OBJETIVOS Definir y promulgar apropiadamente los objetivos de gestión y direcciones con respecto a la TI. Además contribuirá a alcanzar las metas relacionadas con el soporte de TI, las leyes y regulaciones externas, gestionar los riesgos relacionados con la actividad, en este caso que afecten al Hospital Provincial Docente Ambato, además de garantizar la seguridad de la información, infraestructura y disponibilidad de información útil y relevante para la toma de decisiones.	
JUSTIFICACIÓN En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.	
METODOLOGÍA La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes. Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados. Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS),	

donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiabilidad	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
Responsable	Departamento de Sistemas (TICS)
Controlador	Administrativo Financiero
Clientes	Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.

UBICACIÓN

Ubicación	Ecuador, Ambato, Hospital Provincial Docente Ambato.
-----------	--

TIEMPO

Ejecución	Bajo demanda
Frecuencia	NO APLICABLE

RECURSOS

Recursos de TI que utiliza

Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
2) Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		% de iniciativas TI dentro del negocio que permiten el cumplimiento y soporte a los requerimientos internos y externos	
4) Riesgos de negocio relacionados con las TI gestionados		% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos	
6) Transparencia de los costes, beneficios y riesgos de las TI		Nivel de entendimiento y certeza de los costes, beneficios y riesgos de las TI	
7) Entrega de servicios de TI de acuerdo a los requisitos del negocio		# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa	
8) Uso adecuado de aplicaciones, información y soluciones tecnológicas		% de incumplimiento de los estándares tecnológicos	
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones		# de veces en que el servicio de TI puso en riesgo al negocio	
14) Disponibilidad de información útil y fiable para la toma de decisiones		# ocasiones en que la información no era fiable y puso en riesgo al negocio	
PRÁCTICAS			
Práctica		Descripción	
Administración del Valor de TI		Garantizar que el portafolio de inversiones de TI del Hospital Provincial Docente Ambato contenga programas que detallen el	

	<p>grado de complejidad relacionados con la asignación de fondos, los costos, cronogramas, funcionalidad que puedan impactar en los resultados esperados. Establecer además un análisis del riesgo en relación a diferentes escenarios.</p>
<p>Alineación de TI con el Negocio</p>	<p>Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el Hospital Provincial Docente Ambato para capitalizar esas oportunidades.</p>
<p>Evaluación del Desempeño y la Capacidad Actual</p>	<p>Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de la organización, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.</p>
<p>Plan Estratégico de TI</p>	<p>Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la institución (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos.</p>
<p>Planes Tácticos de TI</p>	<p>Crear un portafolio de planes</p>

	tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados.
Administración del Portafolio de TI	Administrar de forma activa, junto con el manejo de la institución, el portafolio de programas de inversión de TI requerido para lograr objetivos organizacionales, estratégicos, específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.
ACTIVIDADES	
Actividades	Responsables
1) Desarrollar el plan informático estratégico con un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización.	Departamento de Sistemas (TICS)
2) Incluir en el plan informático estratégico un análisis de la situación actual y las propuestas de mejora con la participación de	Departamento de Sistemas (TICS)

<p>todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario.</p>	
<p>3) Elaborar planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia.</p>	<p>Departamento de Sistemas (TICS)</p>
<p>4) Asegurar que los planes operativos de TI asignen los recursos apropiados de la función</p>	<p>Departamento de Sistemas (TICS)</p>

de servicios de tecnología de información a base de lo establecido en su plan estratégico.	
5) Aprobar y asegurar a través del plan estratégico y los planes operativos de TI la asignación de los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico.	Gerencia Hospitalaria
6) Analizar y aprobar por la máxima autoridad de la organización el plan estratégico y los planes operativos de TI, así como el presupuesto asociado a éstos, los cuales serán incorporados al presupuesto anual de la organización.	Gerencia Hospitalaria
7) Monitorear y evaluar trimestralmente el plan estratégico y los planes operativos de TI para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
8) Incluir en las instalaciones físicas adecuadas mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire controlado, disponer de	Gerencia Hospitalaria, Departamento de Sistemas (TICS)

energía acondicionada, esto es estabilizada y polarizada, entre otros.	
--	--

Tabla 4.20 Manual de Procesos: Gestionar la Seguridad – Procesos de Recursos Físicos

Elaborado por: Investigador

4.5.3. Manual de Procesos Técnicos

MANUAL DE PROCESOS TÉCNICOS	
Código	APO
Dominio	Alinear, Planificar y Orientar
<p>Proceso: APO03: Gestionar la arquitectura empresarial.</p> <p>Subproceso relacionado: APO03.02 Herramientas y automatización.</p>	
<p>OBJETIVOS</p> <p>Definir y promulgar apropiadamente las herramientas y automatización de TI relacionadas con la información; servicios, infraestructura y aplicaciones.</p>	
<p>JUSTIFICACIÓN</p> <p>En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.</p>	
<p>METODOLOGÍA</p> <p>La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes.</p>	

Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiabilidad	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
Responsable	Departamento de Sistemas (TICS)
Controlador	Administrativo Financiero
Clientes	Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.

UBICACIÓN

Ubicación	Ecuador, Ambato, Hospital Provincial Docente Ambato.
-----------	--

TIEMPO

Ejecución	Bajo demanda
-----------	--------------

Frecuencia		NO APLICABLE	
RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
1) Alineamiento de TI y estrategia de la organización		% de objetivos de TI dentro de la estrategia de negocio que le proporcionan el alineamiento	
3) Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		Efectividad de las decisiones de la dirección ejecutiva sobre el plan táctico de TI	
4) Riesgos de negocio relacionados con las TI gestionados		% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos	
5) Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI		# de inversiones y servicios relacionados con las TI	
6) Transparencia de los costes, beneficios y riesgos de las TI		Nivel de entendimiento y certeza de los costes, beneficios y riesgos de las TI	
7) Entrega de servicios de TI de acuerdo a los requisitos de la organización.		# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa.	
8) Uso adecuado de aplicaciones, información y soluciones tecnológicas		% de incumplimiento de los estándares tecnológicos.	
9) Agilidad de las TI		Tiempo de los servicios de TI	
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones.		# de veces en que el servicio de TI puso en riesgo al negocio.	

11) Optimización de activos, recursos y capacidades de las TI	% de activos, recursos y capacidades de las TI disponibles
12) Capacitación y soporte de procesos de la organización, integrando aplicaciones y tecnología en procesos organizacionales	# de capacitaciones y soporte integradoras de TI
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
17) Conocimiento, experiencia e iniciativas para la innovación de la institución	# de acciones de capacitación, desarrollo e innovación relacionadas con las TI
PRÁCTICAS	
Práctica	Descripción
Planeación de la Dirección Tecnológica	Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas de la institución. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.
Plan de Infraestructura Tecnológica	Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan

	<p>se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala para inversiones y personal en sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.</p>
<p>Monitoreo de Tendencias y Regulaciones Futuras</p>	<p>Establecer un proceso para monitorear las tendencias ambientales del sector/industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de esas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.</p>
<p>Estándares Tecnológicos</p>	<p>Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección tecnológica, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su</p>

	importancia y riesgo para la institución y en el cumplimiento de los requerimientos externos.
Consejo de Arquitectura de TI	Establecer un comité de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación, y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se vinculan con el PO2 Definir arquitectura de la información.
ACTIVIDADES	
Actividades	Responsables
1) Definir sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.	Departamento de Sistemas (TICS)
2) Definir y ejecutar procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.	Departamento de Sistemas (TICS)
3) Presentar informes periódicos de gestión a la alta dirección, para	Departamento de Sistemas (TICS)

<p>que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.</p>	
<p>4) Establecer mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos mediante un control adecuado de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas.</p>	<p>Gerencia Hospitalaria, Departamento de Sistemas (TICS)</p>
<p>5) Definir los procedimientos de obtención periódica de respaldos en función a un cronograma definido por el Director del Departamento de Sistemas.</p>	<p>Departamento de Sistemas (TICS)</p>
<p>6) Implementar y administrar las seguridades a nivel de hardware, que se debe realizar con el monitoreo de seguridad y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados a fin de que los bienes de TI se encuentren protegidos ante cualquier tipo de amenaza que ponga en riesgo su pérdida, daño o integridad.</p>	<p>Gerencia Hospitalaria, Departamento de Sistemas (TICS)</p>

<p>7) Definir, aprobar y difundir procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos.</p>	<p>Departamento de Sistemas (TICS)</p>
<p>8) Establecer la seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas, cuentas de usuario y servicios de tecnología de información de la entidad; también efectuar revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.</p>	<p>Departamento de Sistemas (TICS)</p>
<p>9) Elaborar un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y</p>	<p>Departamento de Sistemas (TICS)</p>

software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.	
10) Desarrollar medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.	Departamento de Sistemas (TICS)

Tabla 4.21 Manual de Procesos: Gestionar la Arquitectura Empresarial – Procesos Técnicos

Elaborado por: Investigador

MANUAL DE PROCESOS TÉCNICOS	
Código	DSS
Dominio	Entrega, Servicio y Soporte
Proceso: DSS05 Gestionar los servicios de seguridad	
OBJETIVOS Definir y gestionar los servicios de seguridad que permitan establecer las medidas de seguridad físicas adecuadas, controles de acceso, detección de software malicioso, la protección de almacenamiento móvil y/o extraíble y soportes, así como la supervisión de la seguridad.	
JUSTIFICACIÓN En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.	

METODOLOGÍA

La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes. Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiabilidad	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
Responsable	Departamento de Sistemas (TICS)
Controlador	Administrativo Financiero
Clientes	Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.

UBICACIÓN			
Ubicación		Ecuador, Ambato, Hospital Provincial Docente Ambato.	
TIEMPO			
Ejecución		Bajo demanda	
Frecuencia		NO APLICABLE	
RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
1) Alineamiento de TI y estrategia de negocio		% de objetivos de TI dentro de la estrategia de negocio que le proporcionan el alineamiento	
2) Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		% de iniciativas TI dentro del negocio que permiten el cumplimiento y soporte a los requerimientos internos y externos	
4) Riesgos de negocio relacionados con las TI gestionados		% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos	
7) Entrega de servicios de TI de acuerdo a los requisitos del negocio		# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa	
8) Uso adecuado de aplicaciones, información y soluciones tecnológicas		% de incumplimiento de los estándares tecnológicos	
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones		# de veces en que el servicio de TI puso en riesgo al negocio	

11) Optimización de activos, recursos y capacidades de las TI	% de activos, recursos y capacidades de las TI disponibles
12) Capacitación y soporte de procesos de negocio, integrando aplicaciones y tecnología en procesos de negocio	# de capacitaciones y soporte integradoras de TI
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
15) Cumplimiento de las políticas internas por parte de las TI	# de interrupciones al negocio debidas al servicio de TI
PRÁCTICAS	
Práctica	Descripción
Establecimiento de roles y responsabilidades	Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definirían las responsabilidades y rendición de cuentas para alcanzar las necesidades de la institución.
Responsabilidad de Aseguramiento de Calidad de TI	Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA) y proporcionar al grupo de QA sistemas de QA, los controles y la experiencia para comunicarlos. Asegurar que la ubicación organizacional, las responsabilidades y el tamaño del grupo de QA satisfacen los requerimientos de la organización.

<p>Responsabilidad sobre el riesgo, la Seguridad y el Cumplimiento</p>	<p>Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.</p>
<p>Propiedad de Datos y de Sistemas</p>	<p>Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los máximos responsables toman decisiones</p>

	sobre la calificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.
Supervisión	Implementar practicas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.
Segregación de funciones	Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.
Personal de TI	Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente organizacional, operativo o de TI para garantizar que la función de TI cuento con un número suficiente de recursos para soportar

	adecuada y apropiadamente a las metas y objetivos de la institución.
ACTIVIDADES	
Actividades	Responsables
1) Establecer procedimientos de detección y eliminación de virus, recuperación de información, así como el apoyo a los usuarios en operaciones de manejo de paquetes ofimáticos y finalmente mantenimiento de equipos de cómputo.	Departamento de Sistemas (TICS)
2) Desarrollar y aplicar una eficaz bitácora de procesos técnicos.	Departamento de Sistemas (TICS)
3) Establecer un correcto y adecuado Control periódico de Inventario y registro de Equipos Tecnológicos.	Departamento de Sistemas (TICS)
4) Priorizar y planear la contratación auditores internos o externos informáticos que controlen periódicamente a la institución de Salud y por ende al Departamento de Sistemas.	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
5) Aprobar y asegurar una gestión integral de cada operación que la organización realiza, en conjunto a un sistema de TI que podría coordinar las funciones independientemente de quien las realiza.	Gerencia Hospitalaria
6) Desarrollar y establecer políticas y reglamentos internos del	Departamento de Sistemas (TICS)

Departamento de Sistemas con un enfoque amplio de seguridad informática que identifique las garantías o resguardos de la información digitalizada en el Hospital Provincial Docente Ambato.	
7) Establecer el procedimiento correcto del manejo de datos críticos garantizando la transmisión cifrada de los mismos.	Departamento de Sistemas (TICS)
8) Diseñar las pruebas de software nuevo con datos productivos.	Departamento de Sistemas (TICS)

Tabla 4.22 Manual de Procesos: Gestionar los servicios de Seguridad – Procesos Técnicos

Elaborado por: Investigador

4.5.4. Manual Técnico de Procesos Personales

MANUAL DE PROCESOS PERSONALES	
Código	EDM
Dominio	Evaluar, orientar y supervisar
<p>Proceso: EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.</p> <p>Subproceso: EDM01.02 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.</p>	
<p>OBJETIVOS Definir y promulgar apropiadamente los objetivos de gestión y direcciones con respecto a la TI en el Hospital Provincial Docente Ambato. En este caso se relaciona con la cultura, ética y comportamiento; principios, políticas y marcos; estructuras organizativas; y procesos de la institución.</p>	

JUSTIFICACIÓN

En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.

METODOLOGÍA

La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes. Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiabilidad	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incrementen el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
--------------	-----------------------

Responsable	Departamento de Sistemas (TICS)		
Controlador	Administrativo Financiero		
Clientes	Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.		
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.		
UBICACIÓN			
Ubicación	Ecuador, Ambato, Hospital Provincial Docente Ambato.		
TIEMPO			
Ejecución	Bajo demanda		
Frecuencia	NO APLICABLE		
RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
1) Alineamiento de TI y estrategia de la organización		% de objetivos de TI dentro de la estrategia de negocio que le proporcionan el alineamiento	
2) Cumplimiento y soporte de la TI al cumplimiento de la organización de las leyes y regulaciones externas		% de iniciativas TI dentro del negocio que permiten el cumplimiento y soporte a los requerimientos internos y externos	
3) Compromiso de la dirección ejecutiva para tomar decisiones		Efectividad de las decisiones de la dirección ejecutiva sobre el plan	

relacionadas con TI	táctico de TI
4) Riesgos propios de la actividad relacionados con las TI gestionados	% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos
5) Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	# de inversiones y servicios relacionados con las TI
6) Transparencia de los costes, beneficios y riesgos de las TI	Nivel de entendimiento y certeza de los costes, beneficios y riesgos de las TI
7) Entrega de servicios de TI de acuerdo a los requisitos de la organización	# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa
9) Agilidad de las TI	Tiempo de los servicios de TI
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones	# de veces en que el servicio de TI puso en riesgo al negocio
11) Optimización de activos, recursos y capacidades de las TI	% de activos, recursos y capacidades de las TI disponibles
12) Capacitación y soporte de procesos de la organización, integrando aplicaciones y tecnología en procesos organizacionales	# de capacitaciones y soporte integradoras de TI
13) Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	# de programas que se ajustan a los requerimientos del negocio
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
15) Cumplimiento de las políticas	# de interrupciones al negocio

internas por parte de las TI	debidas al servicio de TI
16) Personal de la organización y de las TI competente y motivado	% del personal que no cumplen con las políticas y requisitos del negocio
17) Conocimiento, experiencia e iniciativas para la innovación de la institución	# de acciones de capacitación, desarrollo e innovación relacionadas con las TI
PRÁCTICAS	
Práctica	Descripción
Establecimiento de roles y responsabilidades	Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definirían las responsabilidades y rendición de cuentas para alcanzar las necesidades de la institución.
Responsabilidad de Aseguramiento de Calidad de TI	Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA) y proporcionar al grupo de QA sistemas de QA, los controles y la experiencia para comunicarlos. Asegurar que la ubicación organizacional, las responsabilidades y el tamaño del grupo de QA satisfacen los requerimientos de la organización.
Responsabilidad sobre el riesgo, la Seguridad y el Cumplimiento	Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los

	<p>riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.</p>
Propiedad de Datos y de Sistemas	<p>Proporcionar a la institución los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los máximos representantes toman decisiones sobre la calificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.</p>
Supervisión	<p>Implementar practicas adecuadas de supervisión dentro de la función</p>

	de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.
Segregación de funciones	Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice solo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.
Personal de TI	Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de recursos para soportar adecuada y apropiadamente a las metas y objetivos de la institución.
ACTIVIDADES	
Actividades	Responsables
1) Definir un marco de trabajo para TI	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
2) Establecer organismos y	Departamento de Sistemas (TICS)

estructuras organizacionales apropiadas, que incluya interesados y proveedores	
3) Identificar los responsables de sistemas	Departamento de Sistemas (TICS)
4) Identificar los propietarios y beneficiarios de los datos	Departamento de Sistemas (TICS)
5) Establecer e implantar roles y responsabilidades de TI que incluya la supervisión y segregación de funciones	Departamento de Sistemas (TICS)
6) Identificar y registrar los roles y responsabilidades	Departamento de Sistemas (TICS)

Tabla 4.23 Manual de Procesos: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno – Procesos Personales

Elaborado por: Investigador

MANUAL DE PROCESOS PERSONALES	
Código	APO
Dominio	Alinear, Planificar y Orientar
Proceso: APO01 Gestionar el marco de gestión de TI.	
Subproceso relacionado: APO01.02 Establecer roles y responsabilidades.	
OBJETIVOS Definir y promulgar apropiadamente los objetivos de gestión y direcciones con respecto a la TI, donde se establezcan los roles y responsabilidades de todos los implicados en TI.	
JUSTIFICACIÓN En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos	

relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.

METODOLOGÍA

La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes. Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiability	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
Responsable	Departamento de Sistemas (TICS)
Controlador	Administrativo Financiero

Clientes	Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.		
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.		
UBICACIÓN			
Ubicación	Ecuador, Ambato, Hospital Provincial Docente Ambato.		
TIEMPO			
Ejecución	Bajo demanda		
Frecuencia	NO APLICABLE		
RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
1) Alineamiento de TI y estrategia de negocio		% de objetivos de TI dentro de la estrategia de negocio que le proporcionan el alineamiento	
2) Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		% de iniciativas TI dentro del negocio que permiten el cumplimiento y soporte a los requerimientos internos y externos	
3) Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		Efectividad de las decisiones de la dirección ejecutiva sobre el plan táctico de TI	

4) Riesgos de negocio relacionados con las TI gestionados	% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos
7) Entrega de servicios de TI de acuerdo a los requisitos del negocio	# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa
9) Agilidad de las TI	Tiempo de los servicios de TI
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones	# de veces en que el servicio de TI puso en riesgo al negocio
11) Optimización de activos, recursos y capacidades de las TI	% de activos, recursos y capacidades de las TI disponibles
12) Capacitación y soporte de procesos de negocio, integrando aplicaciones y tecnología en procesos de negocio	# de capacitaciones y soporte integradoras de TI
13) Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	# de programas que se ajustan a los requerimientos del negocio
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
15) Cumplimiento de las políticas internas por parte de las TI	# de interrupciones al negocio debidas al servicio de TI
16) Personal del negocio y de las TI competente y motivado	% del personal que no cumplen con las políticas y requisitos del negocio
17) Conocimiento, experiencia e iniciativas para la innovación de negocio	# de acciones de capacitación, desarrollo e innovación relacionadas con las TI

PRACTICAS	
Practica	Descripción
Administración del Valor de TI	Garantizar que el portafolio de inversiones de TI del Hospital Provincial Docente Ambato contenga programas que detallen el grado de complejidad relacionados con la asignación de fondos, los costos, cronogramas, funcionalidad que puedan impactar en los resultados esperados. Establecer además un análisis del riesgo en relación a diferentes escenarios.
Alineación de TI con el Negocio	Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el Hospital Provincial Docente Ambato para capitalizar esas oportunidades.
Evaluación del Desempeño y la Capacidad Actual	Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de la organización, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.
Plan Estratégico de TI	Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos

	estratégicos de la institución (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos.
Planes Tácticos de TI	Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados.
Administración del Portafolio de TI	Administrar de forma activa, junto con el manejo de la institución, el portafolio de programas de inversión de TI requerido para lograr objetivos organizacionales, estratégicos, específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.
ACTIVIDADES	
Actividades	Responsables
1) Identificar las necesidades de capacitación internas tanto para el personal del Departamento de Sistemas así como también para los usuarios que hacen uso de los	Gerencia Hospitalaria, Departamento de Sistemas (TICS)

<p>servicios de información, las cuales deberán constar en un plan de capacitación informática, estructurada conjuntamente con la unidad de talento humano de la Institución.</p>	
<p>2) Orientar el plan de capacitación a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño institucional.</p>	<p>Gerencia Hospitalaria, Departamento de Sistemas (TICS)</p>
<p>3) Asignar las funciones y sus respectivas responsabilidades garantizando una adecuada segregación, evitando funciones incompatibles.</p>	<p>Departamento de Sistemas (TICS)</p>
<p>4) Realizar la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.</p>	<p>Departamento de Sistemas (TICS)</p>
<p>5) Contemplar en la descripción documentada y aprobada de los puestos de trabajo los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño.</p>	<p>Departamento de Sistemas (TICS)</p>

6) Considerar procedimientos que eliminen la dependencia de personal clave.	Departamento de Sistemas (TICS)
---	---------------------------------

Tabla 4.24 Manual de Procesos: Gestionar el marco de gestión de TI – Procesos Personales

Elaborado por: Investigador

MANUAL DE PROCESOS PERSONALES	
Código	APO
Dominio	Alinear, Planificar y Orientar
Proceso: APO03 Gestionar la arquitectura empresarial.	
OBJETIVOS Definir y promulgar apropiadamente los objetivos de gestión y direcciones con respecto a la TI, relacionados con la información; servicios, infraestructura y aplicaciones como parte de la gestión de la arquitectura organizacional.	
JUSTIFICACIÓN En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.	
METODOLOGÍA La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes.	

Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiabilidad	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
Responsable	Departamento de Sistemas (TICS)
Controlador	Administrativo Financiero
Clientes	Todos los departamentos del Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.

UBICACIÓN

Ubicación	Ecuador, Ambato, Hospital Provincial Docente Ambato.
-----------	--

TIEMPO

Ejecución		Bajo demanda	
Frecuencia		NO APLICABLE	
RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
1) Alineamiento de TI y estrategia de negocio		% de objetivos de TI dentro de la estrategia de negocio que le proporcionan el alineamiento	
3) Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI		Efectividad de las decisiones de la dirección ejecutiva sobre el plan táctico de TI	
4) Riesgos de negocio relacionados con las TI gestionados		% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos	
5) Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI		# de inversiones y servicios relacionados con las TI	
6) Transparencia de los costes, beneficios y riesgos de las TI		Nivel de entendimiento y certeza de los costes, beneficios y riesgos de las TI	
7) Entrega de servicios de TI de acuerdo a los requisitos del negocio		# de plataformas tecnológicas por servicios disponibles a lo largo de toda la empresa	
8) Uso adecuado de aplicaciones, información y soluciones tecnológicas		% de incumplimiento de los estándares tecnológicos	
9) Agilidad de las TI		Tiempo de los servicios de TI	
10) Seguridad de la información,		# de veces en que el servicio de TI	

infraestructura de procesamiento y aplicaciones	puso en riesgo al negocio
11) Optimización de activos, recursos y capacidades de las TI	% de activos, recursos y capacidades de las TI disponibles
12) Capacitación y soporte de procesos de negocio, integrando aplicaciones y tecnología en procesos de negocio	# de capacitaciones y soporte integradoras de TI
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
17) Conocimiento, experiencia e iniciativas para la innovación de negocio	# de acciones de capacitación, desarrollo e innovación relacionadas con las TI
PRACTICAS	
Practica	Descripción
Planeación de la Dirección Tecnológica	Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas de la institución. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.
Plan de Infraestructura Tecnológica	Crear y mantener un plan de

	<p>infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala para inversiones y personal en sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.</p>
<p>Monitoreo de Tendencias y Regulaciones Futuras</p>	<p>Establecer un proceso para monitorear las tendencias ambientales del sector/industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de esas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.</p>
<p>Estándares Tecnológicos</p>	<p>Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección tecnológica, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los</p>

	estándares y las practicas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de los requerimientos externos.
Consejo de Arquitectura de TI	Establecer un comité de arquitectura de TI que proporciones directrices sobre la arquitectura y asesoría sobre su aplicación, y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se vinculan con el PO2 Definir arquitectura de la información.
ACTIVIDADES	
Actividades	Responsables
1) Desarrollar los Procedimientos, Normas y Estándares de Seguridad que garanticen el correcto manejo de sistemas y herramientas Informáticas.	Departamento de Sistemas (TICS)
2) Priorizar y planear capacitación al Departamento de Sistemas y a los Usuarios.	Gerencia Hospitalaria
3) Establecer un procedimiento que controle y evite la infección de sistemas a través de unidades portables sin escaneo.	Departamento de Sistemas (TICS)

4) Capacitar y orientar al personal sobre la importancia del correcto manejo de contraseñas y las consecuencias de compartir las mismas o permisos con terceros sin autorización.	Departamento de Sistemas (TICS)
5) Determinar las necesidades reales de personal que garanticen el correcto desempeño de las actividades dentro del dentro del Departamento de Sistemas.	Gerencia Hospitalaria, Departamento de Sistemas (TICS)
6) Aprobar y asegurar fondos para la contratación adicional de personal, necesario en el Departamento de Sistemas.	Administrativo Financiero

Tabla 4.25 Manual de Procesos: Gestionar la arquitectura Empresarial – Procesos Personales
Elaborado por: Investigador

4.5.5. Manual Técnico de Procesos contra Acciones Hostiles

MANUAL DE PROCESOS CONTRA ACCIONES HOSTILES	
Código	BAI
Dominio	Construir, Adquirir e Implementar
Proceso: BAI09 Gestionar los activos.	
OBJETIVOS Gestionar los activos apropiadamente garantizando la seguridad y mantenimiento de los mismos, identificando, analizando y documentando los riesgos asociados, de acuerdo a los requerimientos de TI del Hospital Provincial Docente Ambato.	
JUSTIFICACIÓN En la actualidad existe la necesidad de generar más valor de las inversiones en la Tecnología y de administrar una gama creciente de riesgos	

relacionados con la Tecnología, para mantener el éxito del negocio. Es por ello que se hace necesario una regulación y legislación cada vez más estricta sobre el uso comercial de la información, asociado al logro de una mayor concientización de la importancia de un ambiente de TI bien gobernado y administrado, en este caso por el Hospital Provincial Docente Ambato.

METODOLOGÍA

La metodología de arquitectura de la información usada en el Hospital Provincial Docente Ambato es la que define el proceso, que comienza con los objetivos de la organización a cargo de los máximos representantes. Esto asegura que los resultados del programa estén estrechamente alineados con los resultados y prioridades esperados.

Este enfoque se desplaza a las operaciones de TI, por lo general bajo el control del director de tecnología en el Departamento de Sistemas (TICS), donde se consideran más detalles sobre el riesgo y objetivos de negocio relacionados con TI. Se establecerán así las prioridades en los esfuerzos de remediación para hacer frente a las áreas de riesgos de TI.

Criterios de Información Afectados

Efectividad	P	Disponibilidad	P
Eficiencia	P	Cumplimiento	P
Confidencialidad	S	Confiability	P
Integridad	P		

Requerimientos de negocio a alcanzar

Elaborar iniciativas óptimas que garanticen el éxito de la institución, que proporcionen a su vez el manejo eficiente de los costes de TI e incremente el valor agregado.

ROLES

Dueño	Gerencia Hospitalaria
Responsable	Departamento de Sistemas (TICS)
Controlador	Administrativo Financiero
Clientes	Todos los departamentos del

	Hospital Provincial Docente Ambato, a través del responsable de cada uno de ellos.		
Proveedores	Proveedores internos de todos los servicios relacionados y contratistas externos.		
UBICACIÓN			
Ubicación	Ecuador, Ambato, Hospital Provincial Docente Ambato.		
TIEMPO			
Ejecución	Bajo demanda		
Frecuencia	NO APLICABLE		
RECURSOS			
Recursos de TI que utiliza			
Gente	X	Instalaciones	X
Aplicaciones	X	Datos	X
Tecnología	X		
INDICADORES			
Metas Relacionadas con TI		Métricas Relacionadas	
2) Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		% de iniciativas TI dentro del negocio que permiten el cumplimiento y soporte a los requerimientos internos y externos	
4) Riesgos de negocio relacionados con las TI gestionados		% de iniciativas adoptadas en el plan táctico de TI que minimizan los efectos de los riesgos	
6) Transparencia de los costes, beneficios y riesgos de las TI		Nivel de entendimiento y certeza de los costes, beneficios y riesgos de las TI	
7) Entrega de servicios de TI de acuerdo a los requisitos del negocio		# de plataformas tecnológicas por servicios disponibles a lo largo de	

	toda la empresa
9) Agilidad de las TI	Tiempo de los servicios de TI
10) Seguridad de la información, infraestructura de procesamiento y aplicaciones	# de veces en que el servicio de TI puso en riesgo al negocio
11) Optimización de activos, recursos y capacidades de las TI	% de activos, recursos y capacidades de las TI disponibles
14) Disponibilidad de información útil y fiable para la toma de decisiones	# ocasiones en que la información no era fiable y puso en riesgo al negocio
15) Cumplimiento de las políticas internas por parte de las TI	# de interrupciones al negocio debidas al servicio de TI
PRACTICAS	
Practica	Descripción
Diseño de Alto Nivel	Traducir los requerimientos de la institución a una especificación de diseño de alto nivel para la adquisición de software teniendo en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización. Tener aprobadas las especificaciones de diseño por gerencia para garantizar que el diseño de alto nivel responde a los requerimientos. Reevaluar cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento.
Diseño Detallado	Preparar el diseño detallado y los requerimientos técnicos del software

	<p>de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Realizar reevaluaciones cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento.</p>
Control y Posibilidad de Auditar las Aplicaciones	<p>Implementar controles dentro de la institución, cuando aplique, relacionados con la aplicación automatizada tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.</p>
Seguridad y Disponibilidad de las Aplicaciones	<p>Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización.</p>
Configuración e Implantación de Software Aplicativo Adquirido	<p>Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio.</p>
Actualizaciones Importantes en Sistemas Existentes	<p>En caso de cambios importantes a los sistemas existentes que resulten en cambios significativos al diseño actual y/o funcionalidad, seguir un</p>

	proceso de desarrollo similar al empleado para el desarrollo de sistemas nuevos.
ACTIVIDADES	
Actividades	Responsables
1) Mantener el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables para poder controlar el robo, sabotaje vandalismo que existe por personas externas y de ser el caso internas hacia estos bienes.	Departamento de Sistemas (TICS)
2) Realizar monitoreo de la red y los usuarios que acceden a esta para poder identificar las intromisiones no autorizadas a la red.	Departamento de Sistemas (TICS)
3) Definir los requerimientos técnicos y funcionales del Hospital Provincial Docente Ambato	Departamento de Sistemas (TICS)
4) Analizar y delimitar las áreas críticas dentro de la institución, que puedan ser afectadas por actos de vandalismo, sabotaje, Ataque físico y/o electrónico	Departamento de Sistemas (TICS)
5) Definir e implementar procedimientos que eviten el ataque a la red interna, en busca de información y contraseñas no autorizadas	Departamento de Sistemas (TICS)

6) Definir claramente la funcionalidad de automatización de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación de TI.	Departamento de Sistemas (TICS)
7) Revisar y aprobar todos los aspectos legales y contractuales que se identifican y direccionan con el software aplicativo desarrollado por terceros.	Departamento de Sistemas (TICS)
8) Desarrollar, Implementar un plan de aseguramiento de calidad del software, que garantice la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.	Departamento de Sistemas (TICS)

Tabla 4.26 Manual de Procesos: Gestionar los activos – Procesos contra acciones Hostiles
Elaborado por: Investigador

4.5.6. Resumen de análisis actual de procesos

Una vez realizado el manual de procesos se verifica la situación actual en base a encuestas realizadas al departamento de sistemas; es así como se obtiene resultados en donde los directivos deberán tomar correcciones del estado actual de los procesos resultantes del análisis riesgos.

Se ha realizado la encuesta al departamento de sistemas, el mismo que después de tabular sus datos se pasó de un análisis cualitativo a un valor cuantitativo en la escala de madurez de un proceso y así poder realizar la

gráfica radial para la verificación actual de los procesos resultantes en el análisis de riesgos que presenta el Hospital Provincial Docente Ambato

Mediante la gráfica de radar observamos el desempeño de los procesos actuales con el desempeño esperado dentro de los indicadores resultantes del análisis de esta investigación; además se puede notar qué se debe dar una mayor cobertura en cada proceso.

PROCESOS ORGANIZATIVOS Gestionar el marco de gestión de TI

No.	INDICADORES	GRADO DE MADUREZ						VALOR
		No existente	Inicial	Repetible	Definido	Administrado	Optimizado	
I.1	Alineamiento de TI y estrategia de la organización.		X					1
I.2	Cumplimiento y soporte de la TI al cumplimiento de la organización de las leyes y regulaciones externas.		X					1
I.3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.		X					1
I.4	Riesgos propios de la actividad relacionados con las TI gestionados.	X						0
I.7	Entrega de servicios de TI de acuerdo a los requisitos de la organización.		X					1
I.9	Agilidad de las TI.			X				2
I.10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.			X				2
I.11	Optimización de activos, recursos y capacidades de las TI.		X					1
I.12	Capacitación y soporte de procesos de la organización, integrando aplicaciones y tecnología en procesos organizacionales.	X						0

I.13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	X						0
I.14	Disponibilidad de información útil y fiable para la toma de decisiones		X					1
I.15	Cumplimiento de las políticas internas por parte de las TI.	X						0
I.16	Personal de la organización y de las TI competente y motivado.		X					1
I.17	Conocimiento, experiencia e iniciativas para la innovación de la institución.			X				2

Tabla 4.27 Datos Procesos Organizativos

Elaborado por: Investigador

Grafica radial de análisis de procesos organizativos

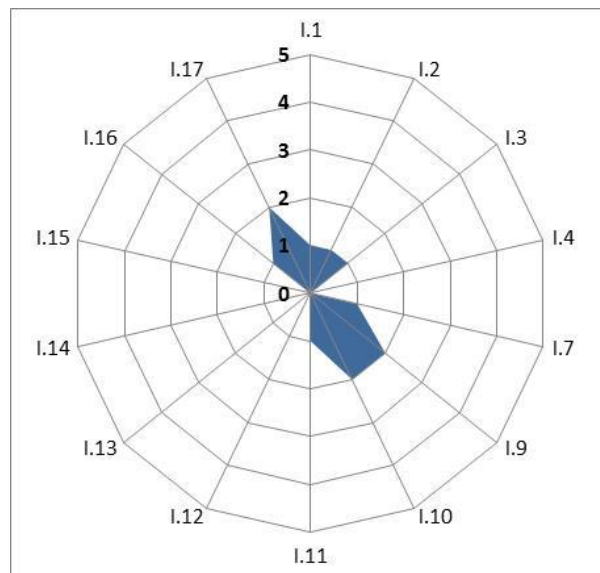


Fig. 4.28 Análisis de madurez de procesos Organizativos

Elaborado por: Investigador

El análisis de la gráfica radial muestra que el estimado desempeño de procesos organizativos actuales no cubre las expectativas del desempeño esperado; es decir que no se cuenta con un adecuado proceso organizativo dentro del Hospital Provincial Docente Ambato.

PROCESOS DE RECURSOS FÍSICOS

Gestionar la seguridad.

No.	INDICADORES	GRADO DE MADUREZ						VALOR
		No existente	Inicial	Repetible	Definido	Administrado	Optimizado	
I.2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.		X					1
I.4	Riesgos de negocio relacionados con las TI gestionados	X						0
I.6	Transparencia de los costes, beneficios y riesgos de las TI	X						0
I.7	Entrega de servicios de TI de acuerdo a los requisitos del negocio		X					1
I.8	Uso adecuado de aplicaciones, información y soluciones tecnológicas		X					1
I.10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			X				2
I.14	Disponibilidad de información útil y fiable para la toma de decisiones		X					1

Tabla 4.28 Datos Procesos Físicos

Elaborado por: Investigador

Grafica radial de análisis de procesos físicos

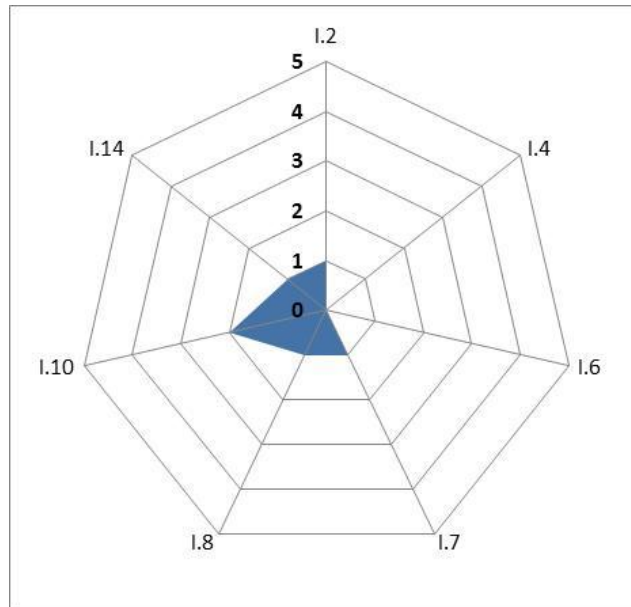


Fig. 4.29 Análisis de madurez de Procesos Físicos

Elaborado por: Investigador

El análisis de la gráfica radial muestra que el estimado desempeño de procesos físicos actuales no cubre las expectativas del desempeño esperado; es decir que no se cuenta con un adecuado proceso físico dentro del Hospital Provincial Docente Ambato.

PROCESOS TÉCNICOS

APO03: Gestionar la arquitectura empresarial

No.	INDICADORES	GRADO DE MADUREZ						VALOR
		No existente	Inicial	Repetible	Definido	Administrado	Optimizado	
I.1	Alineamiento de TI y estrategia de la organización.		X					1
I.2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		X					1
I.3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.		X					1

I.4	Riesgos de negocio relacionados con las TI gestionados.	X						0
I.5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI.	X						0
I.6	Transparencia de los costes, beneficios y riesgos de las TI.	X						0
I.7	Entrega de servicios de TI de acuerdo a los requisitos de la organización.		X					1
I.8	Uso adecuado de aplicaciones, información y soluciones tecnológicas		X					1
I.9	Agilidad de las TI.		X					1
I.10	Seguridad de la información, infraestructura de procesamiento y aplicaciones.		X					2
I.11	Optimización de activos, recursos y capacidades de las TI.		X					1
I.12	Capacitación y soporte de procesos de la organización, integrando aplicaciones y tecnología en procesos organizacionales.	X						0
I.14	Disponibilidad de información útil y fiable para la toma de decisiones.		X					1
I.15	Cumplimiento de las políticas internas por parte de las TI.	X						0
I.17	Conocimiento, experiencia e iniciativas para la innovación de la institución.			X				2

Tabla 4.29 Grado de madurez de Procesos Técnicos

Elaborado por: Investigador

Grafica radial de análisis de procesos técnicos

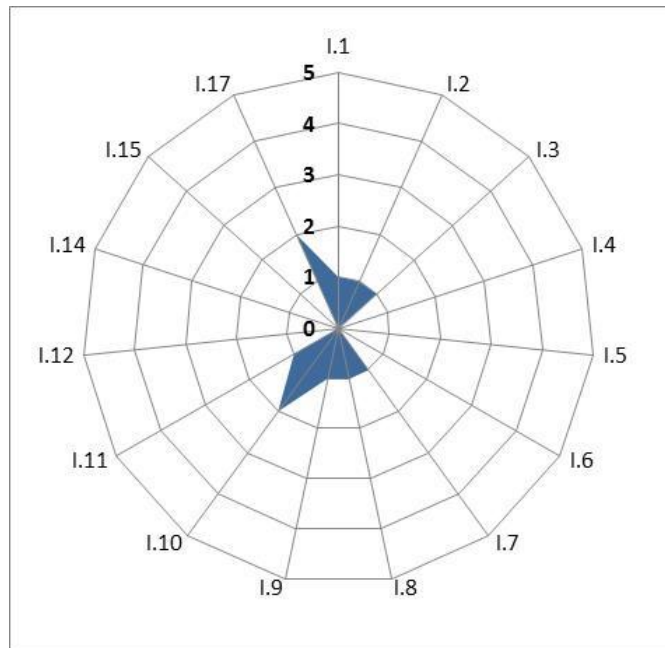


Fig. 4.30 Análisis de madurez de Procesos Técnicos

Elaborado por: Investigador

El análisis de la gráfica radial muestra que el estimado desempeño de procesos técnicos actuales no cubre las expectativas del desempeño esperado; es decir que no se cuenta con un adecuado proceso técnico dentro del Hospital Provincial Docente Ambato.

PROCESOS PERSONALES

EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno

No.	INDICADORES	GRADO DE MADUREZ						VALOR
		No existente	Inicial	Repetible	Definido	Administrado	Optimizado	
I.1	Alineamiento de TI y estrategia de la organización		X					1
I.2	Cumplimiento y soporte de la TI al cumplimiento de la organización de las leyes y regulaciones externas		X					1

I.3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	X						0
I.4	Riesgos propios de la actividad relacionados con las TI gestionados	X						0
I.5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI		X					1
I.6	Transparencia de los costes, beneficios y riesgos de las TI		X					1
I.7	Entrega de servicios de TI de acuerdo a los requisitos de la organización		X					1
I.8	Uso adecuado de aplicaciones, información y soluciones tecnológicas			X				2
I.9	Agilidad de las TI			X				2
I.10	Seguridad de la información, infraestructura de procesamiento y aplicaciones		X					1
I.11	Optimización de activos, recursos y capacidades de las TI		X					1
I.12	Capacitación y soporte de procesos de la organización, integrando aplicaciones y tecnología en procesos organizacionales		X					1
I.13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	X						0
I.14	Disponibilidad de información útil y fiable para la toma de decisiones			X				2
I.15	Cumplimiento de las políticas internas por parte de las TI	X						0
I.16	Personal de la organización y de las TI competente y motivado		X					2

I.17	Conocimiento, experiencia e iniciativas para la innovación de la institución			X				2
------	--	--	--	---	--	--	--	---

Tabla 4.30 Encuesta de Procesos Personales

Elaborado por: Investigador

Grafica radial de análisis de procesos personales

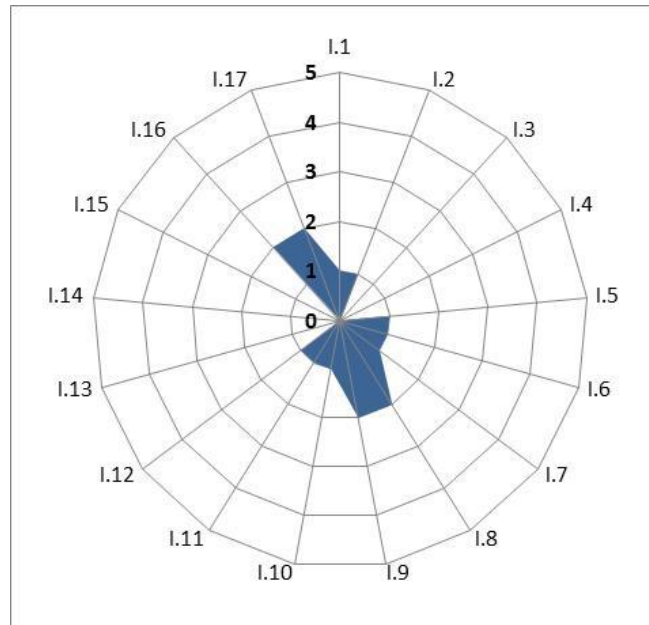


Fig. 4.31 Análisis de madurez de Procesos Personales

Elaborado por: Investigador

El análisis de la gráfica radial muestra que el estimado desempeño de procesos personales actuales no cubre las expectativas del desempeño esperado; es decir que no se cuenta con un adecuado proceso personal dentro del Hospital Provincial Docente Ambato.

PROCESOS CONTRA ACCIONES HOSTILES

BAI09 Gestionar los activos

No.	INDICADOR	GRADO DE MADUREZ						VALOR
		No existente	Inicial	Repetible	Definido	Administrado	Optimizado	
I.2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		X					1

I.4	Riesgos de negocio relacionados con las TI gestionados	X						0
I.6	Transparencia de los costes, beneficios y riesgos de las TI	X						0
I.7	Entrega de servicios de TI de acuerdo a los requisitos del negocio		X					1
I.9	Agilidad de las TI		X					1
I.10	Seguridad de la información, infraestructura de procesamiento y aplicaciones			X				2
I.11	Optimización de activos, recursos y capacidades de las TI		X					1
I.14	Disponibilidad de información útil y fiable para la toma de decisiones		X					1
I.15	Cumplimiento de las políticas internas por parte de las TI	X						0

Tabla 4.31 Encuesta de Procesos contra Acciones Hostiles

Elaborado por: Investigador

Grafica radial de análisis de Acciones hostiles

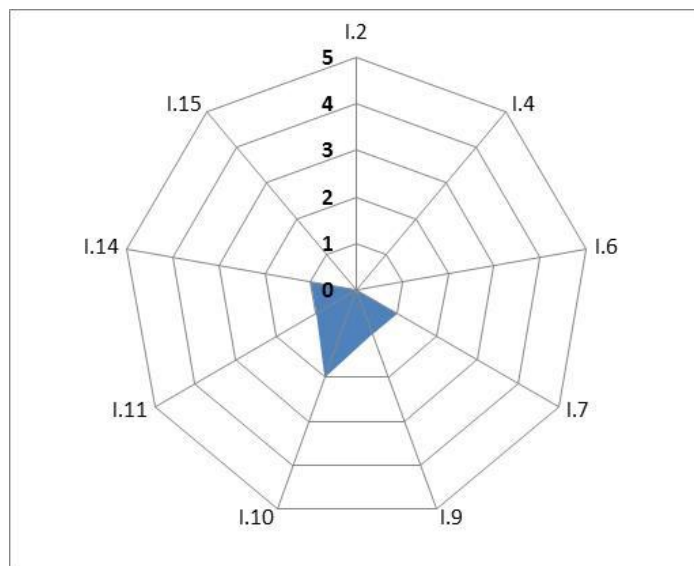


Fig. 4.32 Análisis de madurez de Procesos contra acciones hostiles

Elaborado por: Investigador

El análisis de la gráfica radial muestra que el estimado desempeño de procesos contra acciones hostiles actuales no cubre las expectativas del desempeño esperado; es decir que no se cuenta con un adecuado proceso contra acciones hostiles dentro del Hospital Provincial Docente Ambato.

En resumen podemos citar que existe un grado de madurez muy bajo en los procesos actuales para la reducción y contención de riesgos dentro del departamento de sistemas de la institución de salud, siendo ésta una amenaza tangible por el mayor número de puntos críticos que presentan los resultados de análisis.

CAPITULO V CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El gestionar los riesgos Informáticos en el Hospital Provincial Docente Ambato permitirá disminuir las vulnerabilidades existentes, ya que al no dar un adecuado tratamiento tales riesgos podrán expandirse a los productos y servicios que provee el departamento de sistemas.
- Implementar un proceso de análisis mediante una matriz de riesgos permitió encontrar los puntos críticos en los procesos actuales dentro del departamento de sistemas y reducir de forma considerable los problemas, inseguridades, y riesgos existentes en la Institución.
- El uso de la normativa internacional Cobit 5 en la implementación del manual técnico de procesos podrán incrementar el grado de madurez que tienen los procesos actuales de manera controlada, generando una mayor confianza en la información que dispone la institución de salud.
- La implantación del manual técnico de procesos mejorará la eficiencia y calidad de servicios que presta departamento de sistemas, logrando una optimización de recursos al Hospital Provincial Docente Ambato.
- La organización de las actividades y la delimitación del campo de acción del Departamento de Sistemas dentro del Hospital Provincial Docente Ambato permitirá optimizar la productividad y servicios prestados por el departamento tecnológico.
- Los resultados actuales de los procesos dentro del Hospital Provincial Ambato permite un análisis inicial del trabajo, o un punto de referencia para empezar un cambio en el modelo actual de trabajo de dicha institución.

5.2 RECOMENDACIONES

- Tomando en cuenta las vulnerabilidades y problemáticas existentes, se recomienda dar una solución oportuna a dichas necesidades; esto permitirá una reducción de los riesgos latentes de manera considerable.
- La normativa Cobit 5 se relaciona directamente con la versión Cobit 4.1 y los diferentes productos de la Familia Cobit; es así que se recomienda realizar un análisis de los productos Cobit para su mejor interpretación al momento de implantar el manual técnico de procesos.
- Se recomienda al Director del Departamento de Sistemas en coordinación con los Directivos de la Institución la implantación del manual técnico de procesos de manera gradual, para realizar un control de madurez de procesos en cada etapa, verificando sus resultados finales en un tiempo determinado de análisis.
- Se recomienda realizar una segunda etapa de desarrollo de los Subprocesos que se relacionan directamente con los procesos principales una vez que se haya implantado, desarrollado y administrado el 100% de la aplicación de dichos manuales técnicos para la mejora continua de los procesos y servicios que administra el Departamento de Sistemas.
- Se recomienda establecer las funciones que presta el personal del departamento de sistemas y definir las áreas de trabajo, en donde se podrá tratar adecuadamente los riesgos existentes y controlarlos de manera integral.
- Un análisis progresivo de la implantación a mitad o final de la misma permitirá corregir los procesos mediante auditorías internas o externas y poder alcanzar certificaciones de calidad en la oferta de productos y servicios dentro de una institución.

BIBLIOGRAFÍA

- [1]. Hoy Digital, “Cinco delitos informáticos cada día”
<http://www.hoy.com.ec/noticias-ecuador/cinco-delitos-informaticos-cada-dia-433373.html>
- [2]. T. V. Guachi Aucapiña, “*Norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito San Francisco. Ltda.*”, Repositorio UTA, 2012 [En Línea]. Available: <http://repo.uta.edu.ec/handle/123456789/2361>
- [3]. P, Aguilera. *Seguridad Informática*, 3ª Edición., Editorial EDITEX S.A. Madrid España 2010.
- [4]. C. Heredero. J, López. S. Martín. *Dirección y gestión de los sistemas de información en la empresa* 2da Edición 2006 ESIC EDITORIAL Madrid España.
- [5]. J. Cano, P. C. *Administrando la confidencialidad de la información*. México: Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI), Facultad de Derecho, Universidad de los Andes. (2010).
- [6]. R, Fisher *Seguridad en los Sistemas Informáticos* Ediciones Díaz de Santos S.A 1988 Madrid España.
- [7]. *Procedimientos de Seguridad de la Información Notificación y Respuesta a incidentes. Comisión Nacional de Seguridad - Universidad Nacional de Córdoba*. 2008.

- [8]. Realización de una Matriz de riesgo [Online] Disponible en:
<http://sigweb.cl/biblioteca/MatrizdeRiesgo.pdf>
- [9]. Gestión de Riesgo en la seguridad Informática [Online] Disponible en:
http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/
- [10]. Gestión de Riesgo en la seguridad Informática [Online] Disponible en:
http://protejete.wordpress.com/gdr_principal/elementos_informacion/
- [11]. P. Aguilera, “*Seguridad en el Entorno físico*” in Seguridad Informática, G. Morlanes, Ed. Editex: Madrid, 2010, pp. 30
- [12]. Las medidas de Seguridad en la Protección de Datos [Online] Disponible en:
<http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=323>
- [13]. J, Alonso (2010). *Seguridad Informática* [OnLine]. Disponible en:
http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Políticas_de_seguridad_informtica.pdf.
- [14]. P. Aguilera, “*Introducción a la Seguridad informática*” en Seguridad Informática, G. Morlanes, Ed. Editex: Madrid, 2010, pp. 21
- [15]. Course Technology. *Diccionario de Informática E Internet*, THOMSON Editoriales 2005 pág. 39
- [16]. Normas de las Políticas de seguridad Informática [OnLine]. Disponible en:
<http://seguridadinformaticaufps.wikispaces.com/Normas,+estandares,+Leyes+y+demas+de+las+políticas+de+seguridad.+1150204-159-250-214>
- [17]. AENOR CHILE. (2014). UNE - ISO/IEC 27002:2009. [Online] Disponible en: <http://www.aenorchile.com/nuevas-normas.aspx>

- [18]. Villalón Huerta, A. (Septiembre de 2004). *Códigos de buenas prácticas de seguridad. UNE-ISO/IEC 17799*. El sistema de gestión de seguridad de la información "La nueva norma UNE 71502" [Online] Disponible en: <http://www.shutdown.es/ISO17799.pdf>
- [19]. ISO 27001. Gestión de la Seguridad de la Información [Online]. Disponible en: <http://www.normas-iso.com/iso-27001#>
- [20]. ISO - IEC – 27001 Seguridad de la Información [Online]. Disponible en: STANDARD PARA LA SEGURIDAD DE LA INFORMACIÓN <http://ingertec.com/iso-27001>
- [21]. ¿Cuánto cuesta la implementación de la norma ISO 27001? [Online] Disponible en: <http://blog.iso27001standard.com/es/2011/02/08/cuanto-cuesta-la-implementacion-de-la-norma-iso-27001/>
- [22]. ¿Qué es Cobit? [Online]. Disponible en: <http://www.itera.com.mx/it institute/emails/chile/cobit.htm>
- [23]. Martínez Estébanes, E., & García Cano, J. C. *GOBIERNO DE TI A TRAVÉS DE COBIT 4.1 Y CAMBIOS ESPERADOS EN COBIT 5.0*. Revista ECORFAN , 2 (5). 2011. 109-131.
- [24]. Montaña Orrego, V. *La gestión en la seguridad de la información según Cobit, Itil e Iso 27000*. Revista Pensamiento Americano, 2 (6). 2011. Págs 21-23.
- [25]. ISACA presenta COBIT 5 para Seguridad de la Información [Online] Disponible en: <http://www.pcworld.com.mx/Articulos/23883.htm>

- [26]. ISACA Emite COBIT 5 para la Seguridad de la Información. [Online]
Disponible en:
<http://www.businesswire.com/news/home/20120625005115/es/#.U0wtOlf1Pm8>
- [27]. ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la Empresa*, 5th ed. Rolling Meadows, IL, EEUU: Institute, IT Governance, 2012, pp 31- 33
- [28]. Certificación en Fundamentos de COBIT. [Online] Disponible en:
<http://www.kryteria.com.mx/CU005.aspx>
- [29]. ITIL vs COBIT. [Online] Disponible en: <http://cntec.mx/noticias/41-cat-ultimasnoticias/122-tilvscobit.html>
- [30]. ISO 27000.es. Otros Estándares. [Online] Disponible en:
<http://www.iso27000.es/otros.html>
- [31]. M. Saffirio, *Escala de Madurez – Process Maturity Model*. [Online]
Disponible en: <http://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/>
- [32]. M. Erb, *Gestión de Riesgo en la Seguridad Informática*. [Online]
Disponible en: <http://protejete.wordpress.com/about/#proyecto>
- [33]. Integrando Cobit, ITIL e ISO 27000 como parte del Gobierno de TI. [Online] Disponible en: <http://www.magazcitum.com.mx/wp-content/uploads/2010/07/Integrando-Cobit-ITIL-e-ISO-27001-como-parte-del-Gobierno-de-TI.pdf>
- [34]. D. Naranjo, Hospital Provincial Docente Ambato (private communication), 2014

- [35]. ISACA, *Cobit 4.1*, 41st ed. Rolling Meadows, IL, EEUU: Institute, IT Governace, 2007.
- [36]. ISACA, *COBIT 5 Implementación*, 5th ed. Rolling Meadows, IL, EEUU: Isaca, 2012.
- [37]. ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la Empresa*, 5th ed. Rolling Meadows, IL, EEUU: Institute, IT Governance, 2012

GLOSARIO DE TÉRMINOS

%: Porcentaje (cuantitativo).

#: Número (valor, cantidad).

APO: Alinear, Planificar y Orientar.

ASEGURAMIENTO DE CALIDAD (QA): Una planificada y sistemática patrón de todas las acciones necesarias para proporcionar una adecuada confianza de que un artículo o producto cumple con requisitos técnicos establecidos. (ISO / IEC 24765).

BAI: Construir Adquirir, Implementar.

BITÁCORA: Registra los detalles de la información o de los eventos en un sistema de registro organizado, por lo general se secuenció en el orden en que ocurrieron.

DIRECTOR GENERAL EJECUTIVO: La persona de más alto rango en una empresa.

DSS: Entrega, Servicio y Soporte.

EDM: Evaluar, Orientar y supervisar.

EFQM: modelo de calidad definido por la fundación que lleva dicho nombre: Fundación Europea para la Gestión de la Calidad

GOBIERNO: El método por medio del cual una organización es dirigida, administrada o controlada.

INFRAESTRUCTURA TECNOLÓGICA: Tecnológica, los recursos humanos (HR) y las instalaciones que permitan la transformación y uso de aplicaciones.

MARCO DE CONTROL: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

OBJETIVO DE CONTROL: Una declaración del resultado o propósito que se desea alcanzar al Implementar procedimientos de control en un proceso en particular.

P: Principal.

PLAN ESTRATÉGICO: Proceso de decidir sobre los objetivos de la empresa, en los cambios en los objetivos y las políticas que deben regir su adquisición y uso.

PLAN TÁCTICO DE TI: Un plan de mediano plazo (es decir, de seis a 18 meses) que traduce la dirección del plan estratégico de TI en las iniciativas requeridas, requerimientos de recursos y las maneras en que los recursos y los beneficios serán monitoreados y gestionados.

PORTAFOLIO: Una agrupación de "objetos de interés" (programas de inversión, servicios de TI, los proyectos de TI, otros activos de TI o recursos) dirigido y monitoreado para optimizar el valor de negocio.

PORTAFOLIO DE INVERSIONES: es de interés primordial para Val IT. IT carteras de servicios, proyectos, activos y otros recursos son de interés primordial para COBIT.

RISK IT: brinda una vista completa de extremo a extremo de todos los riesgos relacionados con el uso de TI y un tratamiento similar a fondo de la gestión del riesgo, desde el tono y la cultura en la parte superior , para las cuestiones operativas.

S: Secundario

SERVICE DESK: solución de resolución de problemas y respuesta ante incidentes automatizada para una reparación efectiva y rápida de incidentes de usuario final.

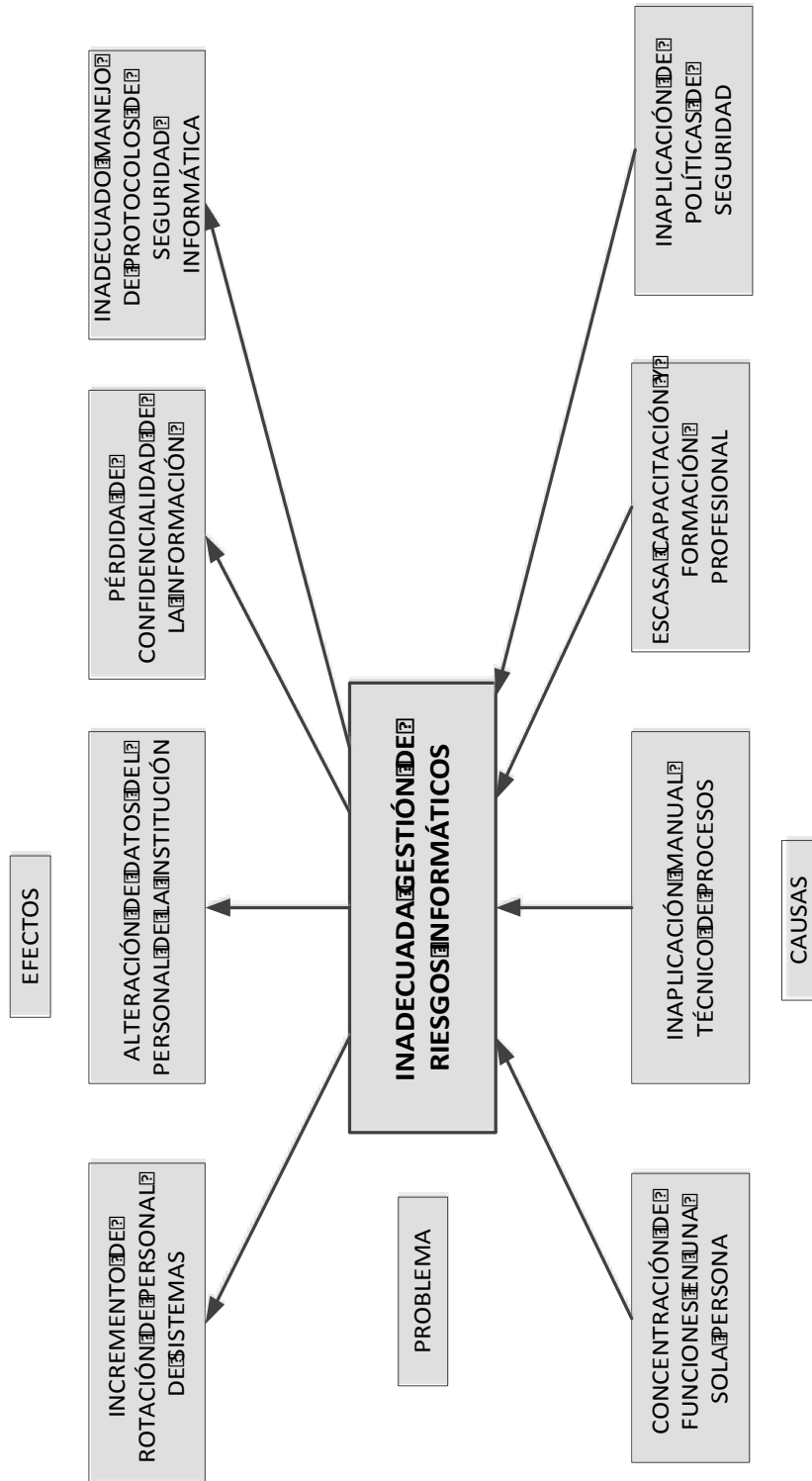
TI: Tecnologías de la información.

TICS: Tecnologías de la Información y Comunicación.

VAL IT: es un framework de gobernabilidad que se puede utilizar para crear valor de negocio de las inversiones en TI

ANEXOS

ANEXO 1: Árbol del Problema



ANEXO 2: Formato de Registro 1

Fuente: Departamento de Sistemas



CONTROL DE TRABAJO / EQUIPOS

FECHA	SERVICIO	TRABAJO REALIZADO	NOMBRE	FIRMA
	Servicios Institucionales	Recepción de tinta	Eugenio Montesdeoca	
	Enfermería	Conexión a internet en Enfermería 1	L AMANOR PARRA	Lic. Flavio PARRA
	Trabajo Social	Conexión a internet en Trabajo Social 3	ANAY ROSAY "	
	Trabajo Humano	Chequeo de imprenta y mouse	Lic SUCUNOTA	
	Jacometría	Reconexión a internet	Jacqueline Sucunota Fonoaudióloga	Jacqueline Sucunota FONOAUDIOLOGA MSP: 39123 CEL: 0998826422

Av. Pasteur y Unidad Nacional - Cashapamba
Teléfonos: 593 (03) 2824309 - 2425782 - 2841858



ANEXO 3: Formato de Registro 2
Fuente: Departamento de Sistemas






	V/C 1	V/C 2	V/C 3	V/C 4	V/C 5	V/C 6	V/C 7	V/C 8	V/C 9	V/C 10	V/C 11	V/C 12	V/C 13	V/C 14	V/C 15	V/C 16	V/C 17	V/C 18	V/C 19	V/C 20
Instalar Windows XP	✓																			
Eliminar componentes innecesarios Windows	✓																			
Etiquetar unidades HDD	✓																			
Habilitar vista de archivos ocultos y extensiones	✓																			
Instalar Drivers:																				
Chipset	✓																			
Video	✓																			
Lan	✓																			
Modem	X																			
Audio	✓																			
Otros	X																			
Office	✓																			
Adobe Reader	✓																			
Mozilla Firefox	✓																			
Flash Player Mozilla	✓																			
Flash Player Explorer	✓																			
Java	✓																			
Winzip	✓																			
WinRar	✓																			
Grabador cds	✓																			
Antivirus	✓																			
Cambiar nombre equipo	✓																			
Cambiar contraseña Administrador	✓																			
Asignar IP	✓																			
Asignar políticas en el servidor	✓																			
Asociar con el Dominio	✓																			
Actualizar Antivirus	✓																			
Borrar usuarios innecesarios	✓																			
VNC Server	✓																			
Agregar Excepciones en el Firewall VNC	✓																			
Configurar programas (office, winrar, adobe, mozilla)	✓																			
Actualizar Windows	✓																			

ANEXO 4: Formato de Control de Trabajos / Equipos 1

Fuente: Departamento de Sistemas



CONTROL DE TRABAJO / EQUIPOS

FECHA	SERVICIO	TRABAJO REALIZADO	NOMBRE	FIRMA
	Imaginería	Recarga de tintas	Dra Paola Ley	
	Dirección Médica	Recarga de tintas	Paulina Morela	
	Gerencia	Revisión de contadores de la impresora	Patly Muro	
	Promesa Acogida	Cheques de impresión	Ricardo Abello	
	Trabajo Social	Recurción a la red interna	Letly Rosas	 12-3-19

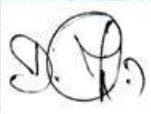






ANEXO 5: Formato de Control de Trabajos / Equipos 2

Fuente: Departamento de Sistemas



CONTROL DE TRABAJO / EQUIPOS

FECHA	SERVICIO	TRABAJO REALIZADO	NOMBRE	FIRMA
	Imaginerología	Recarga de tintas	Dra. Paola López	
	Dirección Médica	Recarga de tintas	Paulina Morela	
	Gerencia	Revisión de contadores de la imprenta	Pauly Nino	
	Prensa Acogida	Cheques de impresión	F. Cabellos	
	Trabajo Social	Reconexión a la red interna	Lilly Rosas	 12-3-19



ANEXO 6: Formato de Control de Trabajos / Equipos 3

Fuente: Departamento de Sistemas



CONTROL DE TRABAJO / EQUIPOS

FECHA	SERVICIO	TRABAJO REALIZADO	NOMBRE	FIRMA
Marzo 24/ 2014	Farmacia	Vaciado del receptáculo de tinta y recarga de tinta	José Vasco	
Marzo 24/ 2014	Dirección Médica	Vaciado del receptáculo de tinta y recarga de tinta	Paulina Moreta	
Marzo 24/ 2014	Órgano Social	Mantenimiento impresora Epson TX 300F	Lety Rosas	
Marzo 24/ 2014	Asesoría Jurídica	Mantenimiento impresora Epson TX 730 y conexión a internet	Martha Hincapié	

