## CARATULA

UNIVERSIDAD INTERNACIONAL DEL ECUADOR

SEDE LOJA

ESCUELA DE INGENIERÍA EN INFORMÁTICA
Y
MULTIMEDIA.

TEMA:

"AUDITORIA DE PRODUCTIVIDAD DEL HARDWARE, SOFTWARE Y TELECOMUNICACIONES TOMANDO COMO REFERENCIA EL MARCO DE TRABAJO DE COBIT 4.0 Y DESARROLLO DE UN SISTEMA WEB PARA EL CONTROL DE LOS RECURSOS DE TECNOLOGÍA DE LA INFORMACIÓN PARA EL HOSPITAL PROVINCIAL GENERAL ISIDRO AYORA DE LA CIUDAD DE LOJA"

*Tesis, previa a la obtención del Título de Ingeniería en Informática y Multimedia.*


AUTORES:

Patricia Soledad Sigüenza Granda

Angel Manuel Naula Maita

DIRECTOR:

Ing. Boris Díaz


LOJA – ECUADOR

2012

# CERTIFICACIÓN

Sr. Ing. Boris Díaz
**DIRECTOR DE TESIS**

**Certifico:**

Que la tesis realizada por **la Sra. Patricia Soledad Siguenza Granda y el Sr. Angel Manuel Naula Maita,** de título **"AUDITORÍA *DE* PRODUCTIVIDAD DEL HARDWARE, SOFTWARE Y TELECOMUNICACIONES TOMANDO COMO REFERENCIA EL MARCO DE TRABAJO DE COBIT 4.0 Y DESARROLLO DE UN SISTEMA WEB PARA EL CONTROL DE LOS RECURSOS DE TECNOLOGÍA DE LA INFORMACIÓN PARA EL HOSPITAL PROVINCIAL GENERAL ISIDRO AYORA DE LA CIUDAD DE LOJA*",*** revisada bajo mi dirección cumple con todos los requisitos académicos establecidos por la Universidad Internacional del Ecuador sede-Loja. Por lo tanto autorizó a su presentación.

Loja, 28 de noviembre del 2011

**Ing Boris Díaz**
**DIRECTOR DE TESIS**

# AUTORÍA

En el presente Proyecto de Tesis, los autores, son los responsables intelectuales, de las observaciones, análisis, opiniones, conclusiones y recomendaciones emitidas en el mismo.

A demás, es importante mencionar que la información de otros autores empleada en el presente trabajo, está debidamente especificada en fuentes de referencia y apartados bibliográficos.

# AGRADECIMIENTO

En primer lugar queremos dar gracias a Dios, por darnos la vida y la oportunidad de culminar con nuestras metas.

A nuestra Universidad Internacional del Ecuador sede Loja, por abrirnos la puerta hacia el conocimiento, es el lugar donde nos instruimos académicamente en el ámbito intelectual y personal.

A la escuela de Informática y Multimedia, a través de su Director, Ing. Bayardo Encarnación, quien a través de su entrega y dedicación, es participe para que la carrera de Informática vaya en ascenso cada día.

A nuestros queridos profesores, que con su profesionalismo nos impartieron el aprendizaje a través de sus conocimientos y experiencias, dejando en algún momento de lado al profesor, para convertirse en el amigo.

A nuestro Director, Ing. Boriz Días, por su apoyo, dedicación y entrega incondicional, en el desarrollo del presente proyecto. Gracias por responder a nuestras inquietudes, siempre que lo hemos requerido.

Al Dr. Daniel Astudillo, ex-director del Hospital Isidro Ayora-Loja, por abrirnos las puertas de la institución y darnos la oportunidad de realizar nuestra investigación.

Al Ing. Mario Cueva, por facilitarnos el ingreso a las instalaciones del centro de cómputo y proporcionarnos la información solicitada para la investigación del proyecto.

A nuestros familiares y amigos que con su apoyo incondicional, durante el proceso, fueron nuestros principales motivadores, para que continuemos hasta la finalización del presente proyecto.

A todos, quienes de una u otra forma nos han colaborado para el desarrollo del proyecto.

## DEDICATORIA

A mí amado Dios por darme la oportunidad de soñar y llegar a la meta.

A la memoria de mi madre Felicia Sigüensa, de quien guardo en mi mente y mi corazón todo su amor y entrega incondicional, gracias por tus consejos y por inculcarme el deseo de superación, donde quiera que estés tengo la plena seguridad de que estas tan feliz como yo por este sueño cumplido, mil gracias mamita desde lo más profundo de mí ser. A mi pequeña Nicolle te amo mi niña con todo mi corazón. A mí esposo Diego gracias por tu amor, apoyo y comprensión. A mis queridos hermanos Daniel, Luis y Karina les dedico este trabajo con todo mi amor, son el motivo de mi inspiración y superación. A mis queridos tíos Germán y Juvencio. A mí querida abuelita María y demás familiares.

A mis amigos que de alguna u otra forma han sido participes de esto.

….Patricia Sigüenza

Primeramente agradezco a Dios por ser el amigo que nunca me fallo y por concederme culminar mi carrera.

A mi madre por ser la mejor madre del mundo ya que con su esfuerzo, enseñanza y consejos me pudo ayudar a que yo pueda cumplir con éxito mi carrera.

A la memoria de mi padre por ser una persona que me enseño a trabajar y por sus buenas enseñanzas para que yo pueda superarme día a día. A mis hermanos Cesar, Hilda, José, Ángela, Laura, Claudia, Susana, Darío, Pablo quienes son los que más quiero y por animarme de una o de otra manera para que yo culmine mis estudios universitarios.

A todos mis familiares porque de una o de otra manera me ayudaron a mi superación personal.

A todos mis amigos los cuales me colaboraron en la culminación de mi tesis especialmente a Romel quien fue partícipe de esto.

Además un profundo agradecimiento a mi hermano quien tuvo que abandonar sus estudios para convertirse en jefe de hogar cuando falto mi padre quien con su responsabilidad y su esfuerzo me ayudo a que yo estudiara y culmine mi carrera universitaria.

….Ángel Naula

# TABLA DE CONTENIDO

# DESCRIPCIÓN DEL TEMA

La presente Auditoría Informática de Productividad de Hardware, Software y Telecomunicaciones tomando como referencia el marco de trabajo de Cobit 4.0, para el Hospital Provincial General Isidro Ayora de la Ciudad de Loja, consiste básicamente en visitar las instalaciones de la institución y recopilar toda la información necesaria de cómo se administra el hardware, software y telecomunicaciones. Para la adquisición de la información se acudirá a la técnica de la entrevista, encuestas, observación directa e indirecta; así como también se solicitara al administrador del Centro de Cómputo ingeniero Mario Cueva toda la documentación de los procesos que se ejecutan dentro del departamento si los tuviere debidamente formalizados y documentados, caso contrario se le pedirá que nos describa el procedimiento que lleva para cumplir con las actividades que le han sido asignadas, luego de tener toda la información recopilada procederemos a: analizar, agrupar, evaluar y recomendar en base a los hallazgos encontrados en el entorno auditado.

Se evaluará si los procesos manejados a nivel informático han sido definidos de manera formal y sino fuere así se establecerá las debidas recomendaciones basadas en el modelo Cobit, además se comprobará la efectividad en los controles existentes e identificará los riesgos que podrían causar problemas en la administración y seguridad del hardware, software y telecomunicaciones.

Luego de identificar las debilidades existentes se comunicará a los auditados mediante un documento escrito donde se detallan: los riesgos, los hallazgos u observaciones, las evidencias encontradas y la matriz de recomendaciones.

Finalmente al determinar la necesidad que tienen las instituciones públicas hoy en día de poder administrar los recursos informáticos que poseen, se ha previsto desarrollar un Sistema Web para el Control de los Recursos de Tecnología de la Información, el mismo que constará: de la parte Web en la que se da a conocer información general del Hospital Isidro Ayora, y la parte de la aplicación de escritorio que servirá de apoyo al administrador

del centro de cómputo, para llevar el registro y control del software, hardware y elementos de telecomunicaciones. Además la aplicación permitirá controlar el mantenimiento del hardware, software y elementos de telecomunicaciones; también constará de un módulo de respaldo de base de datos a través del cual el administrador, creará respaldos de base de datos con extensión .SQL, otra característica importante de nuestra aplicación es que permitirá generar reportes para el usuario, los mismos que facilitarán y ayudarán en la toma de decisiones a los directivos institucionales en lo referente al hardware, software y elementos de telecomunicaciones que posee el hospital.

# HIPÓTESIS

¿Se puede incrementar la Productividad del Hardware, Software y Telecomunicaciones del Hospital Provincial General Isidro Ayora de la ciudad de Loja, aplicando la Auditoría Informática a través de la cual se propone recomendaciones y soluciones que permitan contribuir a la mejora de los procesos existentes?

# INTRODUCCIÓN

En la actualidad, la informática se ha convertido en una herramienta poderosa que colabora de forma rápida y eficiente en la ejecución de las actividades que se llevan dentro de las empresas, organizaciones o instituciones.

Es importante que las empresas pongan más énfasis en el cuidado de los recursos de TI que poseen porque aparte de ahorrar tiempo y dinero, estas tecnologías contribuyen de manera significativa para su desarrollo integral.

Automatizar la información sin lugar a duda hoy por hoy requiere de esfuerzo y dinero, pero es necesario hacerlo si se quiere estar en equilibrio con los adelantos tecnológicos que nos ofrece el mundo. Que empresa o institución por más pequeña que sea no tiene por los menos un equipo de cómputo en el que almacena uno de sus activos más importantes "Información", que podemos decir de las grandes empresas o instituciones que tienen de 20 computadores o más y que a la vez manejan grandes volúmenes de información que les resulta tedioso de manipular, es por esto que las empresas deben definir e implementar procesos idóneos para administrar adecuadamente los recursos de TI que contienen la información, esto por un lado sin olvidar que los recursos tecnológicos cuestan dinero y que hay que cuidarlos para que cumplan con el tiempo de vida útil establecido. Es importante que los procesos para el mantenimiento y cuidado de las TI estén debidamente formalizados para su adecuada ejecución.

Para determinar cómo se llevan los procesos en la administración de las TI se propone la Auditoria Informática, considerada una de las disciplinas más recientes en el ámbito de la informática, que le va a permitir a la institución analizar, evaluar, verificar y recomendar, en los asuntos correspondientes a la planificación, control de eficacia, seguridad y adecuación de los recursos de TI. Así también para automatizar el proceso de administración de los recursos de Tecnología de la Información, se desarrollará una aplicación distribuida cliente servidor.

# ESQUEMA DE METODOLOGÍA DE LA AUDITORÍA

Metodología de la Auditoría de Productividad de Hardware, Software y Elementos de Telecomunicaciones del Hospital General Provincial Isidro Ayora de la Ciudad de Loja.

1. Definición del Alcance y Objetivos de la Auditoría Informática.
2. Estudio Preliminar del Entorno a Auditar
3. Planificación Específica
4. Ejecución del Trabajo
5. Comunicación de Resultados

# ILUSTRACIÓN DEL ESQUEMA DE METODOLOGÍA

## 1. Definición del Alcance y Objetivos de la Auditoría Informática.

Al iniciar una Auditoría Informática es preciso definir el entorno y los límites en que se desarrollará. Cuando el director o líder de un área específica de informática solicita los servicios de un auditor Informático deberá coordinar entre las dos partes para delimitar todo lo que comprendería el análisis y estudio de la auditoría.

El auditor deberá conocer lo que el cliente desea obtener con la auditoría para poder definir su alcance y objetivos.

## 2. Estudio Preliminar del Entorno a Auditar

El propósito esta fase es lograr un conocimiento general del espacio físico donde se desenvuelven los recursos de TI del Hospital Isidro Ayora de la Ciudad de Loja que van hacer auditados.

Se elaborará un plan de estudios de todos los recursos de TI, dependiendo del alcance y de los objetivos propuestos por la auditoría. Se necesitará obtener la información sobre políticas, planes o procedimientos para la gestión de los recursos de hardware, software y elementos de telecomunicaciones; para así poder tener el primer diagnóstico de la parte auditada.

Se investigará las principales actividades del sistema operativo Windows, así como también se determinará cuántos y cuáles son los servidores, pc's, laptops y elementos de telecomunicaciones que trabajan bajo esta plataforma; esto permitirá evaluar la confiablidad y estabilidad necesaria de todos los equipos de la institución.

Se describirá la ubicación geográfica del cuarto de comunicaciones dentro de la institución; así como el cumplimiento de estándares requeridos para la institución.

Es importante realizar el análisis de todos los componentes de hardware, software y elementos de telecomunicaciones, el estado en que se encuentran y funcionamiento de cada uno de ellos; para verificar que sus tareas cumplen con los objetivos para lo cual fueron adquiridos y configurados.

Investigaremos la estructura orgánica de la institución para llegar a cada una de las áreas donde se encuentran recursos de TI y en especial al departamento de Gestión Informática para conocer las relaciones jerárquicas y funcionales, cuyo propósito es determinar cómo se lleva el proceso de creación de cuentas de usuario, asignación de contraseñas, otorgamiento de permisos de acceso, el mantenimiento físico y lógico de las TI; así como su seguridades físicas y lógicas.

Finalmente en esta fase determinaremos el diagnóstico inicial del estado de los recursos de TI, identificando los aspectos críticos más importantes, basándonos en información recolectada durante el desarrollo.

## 3. Planificación Específica

Se realizará una planificación sobre el plan de trabajo, definiendo tareas que se deberá ejecutar, para lo cual se definirán responsables y se elaborara el cronograma de actividades.

## 4. Ejecución del Trabajo

En esta fase, analizaremos las actividades y procesos de la administración de los recursos de TI actualmente, y cómo podemos mejorar la productividad de los mismos, para ello deberemos evaluar la existencia de las actividades y procesos mediante las políticas utilizadas en la administración de los recursos de TI, para garantizar permanentemente la seguridad física y lógica de estos.

Para evaluar los procesos de las TI y el funcionamiento de los mismos hemos creído convenientemente realizar la auditoría informática implementando algunos procesos genéricos de los 3 dominios del marco de trabajo de COBIT. Los dominios de Cobit a ejecutar son: (Ver Anexo 1 Y 2)

- Planear y Organizar
- Adquirir e Implantar
- Entregar y Dar Soporte

Los Objetivos de Control para la Información y la Tecnología Relacionada (COBIT) es el marco referencial que se utiliza para Planear y Organizar, Adquirir e Implantar, Entregar y Dar Soporte, Monitorear y Evaluar el gobierno sobre TI; incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez. El marco de trabajo COBIT es constantemente actualizado, siendo Cobit la última actualización relevante en este estándar internacional; el cual permite a las empresas aumentar su valor TI y reducir los riesgos asociados a proyectos tecnológicos. Ello gracias a que COBIT se estructura a partir de parámetros generalmente aplicables y aceptados, para mejorar las prácticas de planeación, control y seguridad de las Tecnologías de Información.

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- ✓ Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

- ✓ La 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.

- ✓ La 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.

- ✓ Las 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 o contratadas, de acuerdo a como se requieran.

Se evaluara cada uno de los procesos definidos para el departamento de Gestión Informática, enmarcándonos es los tres dominios de Cobit, calificando cada proceso del 0 (No existente) al 5(optimizado) definidos en el modelo de madurez de Cobit.

Para evaluar los riesgos nos enmarcamos en el proceso Cobit, PO9 Evaluar y Administrar los Riesgos de TI, se creará la matriz de riesgo residual para determinar la existencia de controles que ayuden a mitigar de alguna manera el riesgo encontrado. Se podrá establecer la existencia de controles, tomando en cuenta la información que se obtuvo de las entrevistas, encuestas, observación, vídeos e imágenes. Algunos riesgos tendrán cero o más controles.

Para el análisis de información recolectada del HGPIA-Loja, utilizaremos una matriz en donde llevaremos ordenadamente la información. (Ver Anexo 3,"Formato Para Analizar Informacion Recolectada").

Para la identificación de los riesgos, nos basamos en el análisis de las entrevistas, encuestas, observaciones directas, documentos, imágenes y videos obtenidos de la institución. (Ver "Matriz de Identificación de Riesgos")

**Ponderación de riesgos de TI del HPGIA-Loja**

Para la evaluar los riesgos de TI del HPGIA-Loja, estos se calcularán multiplicando la cuantificación del impacto (severidad) por la cuantificación de la probabilidad (ocurrencia) de aparición. Es decir:

## PONDERACIÓN DEL RIESGO= IMPACTO * PROBABILIDAD

La cuantificación del impacto como la de probabilidad se calificara en valores de 1 a 5 como se describe en las siguientes tablas:

El **impacto** es la medida del daño o perjuicio que ocasionaría un riesgo en caso de que se haga realidad.

| Análisis de riesgos Impacto | |
|---|---|
| Muy alto | 5 |
| Alto | 4 |
| Moderado | 3 |
| Bajo | 2 |
| Muy bajo | 1 |

La **probabilidad de ocurrencia** de un riesgo es la estimación de la posibilidad de que este se haga realidad.

| Análisis de riesgos Probabilidad de ocurrencia | |
|---|---|
| Muy probable | 5 |
| Bastante probable | 4 |
| Probable | 3 |
| Poco probable | 2 |
| Improbable | 1 |

Para determinar el nivel de aceptación del riesgo, se tomara como base la siguiente tabla:

| Intervalo [4] | Nivel de Riesgo |
|---|---|
| (1-6.25) | Muy Bajo |
| (7.25-12.50) | Bajo(Aceptable) |
| (13.50-18.75) | Medio(Precauciones) |
| (19.75-25) | Alto(Inaceptable) |

Una vez que los riesgos han sido ponderados se procede a evaluar la "calidad de la gestión", con el fin de determinar cuán eficaces son los controles establecidos por la institución para mitigar los riesgos identificados. En la medida que los controles sean más eficientes y la gestión de riesgos pro-activa, el indicador de riesgo inherente neto tiende a disminuir.

Para valorar la efectividad de los controles se lo hará en base a la siguiente tabla:

| CONTROL | EFECTIVIDAD |
|---|---|
| Destacados | 5 |
| Alto | 4 |
| Medio | 3 |
| Bajo | 2 |
| Ninguno | 1 |

Finalmente, se calcula el "riesgo neto o residual", que es la relación entre el nivel de Riesgo Inherente y el Promedio de Efectividad de los Controles, es decir:

**Riesgo Residual= Nivel de Riesgo Inherente/Promedio de Efectividad de Controles**

**CONTROL**

Consiste en un conjunto de estrategias y procedimientos establecidos para proporcionar una seguridad sensata para poder lograr los objetivos fijados por la institución.

Proceso a través del cual los auditores realizan un esfuerzo sistemático orientado a comparar el rendimiento con los estándares establecidos por las organizaciones, y estar en capacidad de determinar si el desempeño es acorde con las normas. Este proceso incluye, asegurarse de que todos los recursos estén siendo utilizados de la manera más efectiva posible, siempre en función de los objetivos que la organización ha propuesto.

Controlar es influir en lo que sucede con el fin de obtener el resultado deseado. El propósito del control es minimizar y gobernar problemas y riesgos.

La palabra control tiene muchas connotaciones y su significado depende del área en que se aplique; puede ser entendida como:

- ✓ Estrategias, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar que los objetivos empresariales serán alcanzados y que eventos no deseables serán prevenidos, detectados y corregidos.
- ✓ Función administrativo: proceso administrativo, planeación, organización y dirección.
- ✓ Función restrictiva de un sistema para mantener a los participantes dentro de los patrones deseados y evitar cualquier desvío.

**RIESGO**

Son las “amenazas” a las que está sometida el área auditada y los "impactos" que puedan causar cuando se presentan. Son aspectos que pueden encaminar a grandes problemas a una institución, esto obliga a la realización de estrictos controles.

Los riesgos pueden ser de infraestructura, procesos y personal estos se los puede simplificar a continuación:

**Infraestructura**

- ✓ Mecanismos de Seguridad para el Acceso al Centro de Cómputo y a la sala de servidores del HGPIA-Loja.
- ✓ Seguridad Física y lógica de las pc´s, laptops y elemento de telecomunicaciones del HGPIA-Loja.
- ✓ Seguridad Física y lógica de los servidores del HGPIA-Loja.
- ✓ Ausencia de Seguros contra robo para los recursos de TI (pc´s, laptops, servidores y ruteadores) del HGPIA-Loja.
- ✓ Controles de la Temperatura y Humedad del Entorno del Hardware del HGPIA-Loja
- ✓ Destrucción y/o Pérdida de Información relevante para el HGPIA-Loja.
- ✓ Actualización de los Antivirus de los Equipos Informáticas del HGPIA-Loja
- ✓ Inventario actualizado de las partes y/o piezas de los computadores del HGPIA-Loja.
- ✓ Licencias para Instalación y Actualización del software del HGPIA-Loja.
- ✓ Administración de cuentas de usuario de los computadores del HGPIA-Loja.
- ✓ Administración de configuraciones de los servidores.

**Procesos**

- ✓ Inexistencia de los planes para los procesos esenciales de la institución para la productividad de los recursos de TI.
- ✓ Planes para la Contratación del Personal de Informática del HGPIA-Loja
- ✓ Planes de adquisición de recursos de TI para el HGPIA-Loja

- ✓ Planes de continuidad del Negocio del HGPIA-Loja.
- ✓ Planes de mantenimiento físico y lógico de los recursos de TI del HGPIA-Loja.

**Personal**

- ✓ Entrenamiento y capacitación al personal del centro de cómputo en estándares y tecnología de vanguardia.
- ✓ Asignación de funciones formalizadas al personal de gestión informática.
- ✓ Desconocimiento de que hacer para salvaguardar el hardware en el caso de incendios.

### 5. Comunicación de Resultados

En la elaboración del informe final se dará a conocer el alcance, objetivos, tiempo empleado, auditores y destinatarios de la auditoría informática.

Con el desarrollo de todas las fases de la auditoría se podrá emitir el primer borrador del informe, los destinarios del informe serán: el director, el administrador, el administrador del centro de cómputo del HGPIA-Loja y al auditor externo de la Contraloría General del Estado de la Ciudad de Loja, con fecha de entrega a todos los funcionarios antes mencionados y los resultados encontrados con sus respectivas recomendaciones.

En el informe se detallaran los procesos definidos para la presente auditoría con su debida evaluación y recomendación siguiendo el modelo Cobit, cada proceso se evaluará de acuerdo al modelo de madurez y si la criticidad de los procesos está entre el nivel 0 o 1 estos deberán ser tomados muy en cuenta por los directivos y administradores de la institución.

## DESARROLLO DE LA METODOLOGÍA DE AUDITORÍA INFORMÁTICA

A continuación se detalla todo el desarrollo de las fases de la Auditoría Informática.

# FASE 1:

## DEFINICIÓN DEL ALCANCE Y OBJETIVOS DE LA AUDITORÍA

## CONTENIDOS

# 1. DEFINICIÓN DEL ALCANCE Y OBJETIVOS DE LA AUDITORÍA

## 1.1. Alcance

La Auditoría de Productividad de Hardware, Software y Telecomunicaciones tomando como referencia el marco de trabajo de Cobit 4.0, para el Hospital Provincial General Isidro Ayora de la Ciudad de Loja, constituye un proyecto para evaluar y proponer mejores soluciones en los procesos actuales implantados que se encuentren deficientes. Se analizará y evaluará la gestión del hardware, software y elementos de telecomunicaciones existentes en la institución para así poder determinar si cumplen con los controles de seguridad, y si sus características van acorde con los procesos que se les ha asignado.

## 1.2. Objetivos

### *1.2.1 Objetivo General*

- Auditar la Productividad del Hardware, Software y Telecomunicaciones tomando como referencia el marco de trabajo de Cobit 4.0

### *1.2.3 Objetivos Específicos*

- Determinar la situación actual del área Informática del Hospital Isidro Ayora.
- Definir procesos críticos a evaluar mediante la aplicación de matrices de riesgo de la seguridad y productividad.
- Ejecutar la Auditoría Informática aplicando los 3 dominios de COBIT 4.0, tomando de ellos los procesos genéricos que están enfocados a la productividad del hardware, software y telecomunicaciones.
- Elaborar matrices de recomendación para incrementar la productividad del hardware, software y telecomunicaciones.

# FASE 2

## ESTUDIO PRELIMINAR DEL ENTORNO A AUDITAR

## CONTENIDOS

# INTRODUCCIÓN

Esta fase comprende el estudio general de todos los recursos de TI que tiene el HGPIA-Loja, se trata de determinar cuáles son las características físicas y lógicas de los recursos de TI, así como también los respectivos espacios físicos en donde se encuentran los servidores, equipos informáticos y elementos de telecomunicaciones dentro del centro de cómputo del HGPIA-Loja, además se estudia los procesos que se manejan para su administración.

# 2. ESTUDIO PRELIMINAR DEL ENTORNO A AUDITAR

## 2.1. Investigación de recursos de TI (hardware, software y telecomunicaciones) del HGPIA-Loja

### *2.1.1 Hardware*

Son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida, también se conoce al hardware como la parte dura o física del computador. La mayoría de las computadoras están organizadas de la siguiente forma: los dispositivos de entrada (Teclados, Lectores de Tarjetas, Lápices Ópticos, Lectores de Códigos de Barra, Escáner, Mouse, etc.) y salida (Monitor, Impresoras, Plotters, Parlantes, etc.) que permiten la comunicación entre el computador y el usuario.

### *2.1.2 Software*

Es equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.

Tales componentes lógicos incluyen, entre muchos otros, aplicaciones informáticas, el sistema operativo, que básicamente, permite al resto de los programas funcionar adecuadamente, facilitando la interacción con los componentes físicos y el resto de las aplicaciones, proporcionando también una interfaz para el usuario.

### *2.1.3 Telecomunicaciones*

La telecomunicación es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones.

Son importantes las telecomunicaciones dentro de una institución ya que permite recibir un servicio un usuario utilizando un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte, y, por tanto, el usuario requiere de distintos equipos terminales. Por ejemplo, para tener acceso a la red telefónica, el equipo terminal requerido consiste en un aparato telefónico; para recibir el servicio de telefonía celular, el equipo terminal consiste en teléfonos portátiles con receptor y transmisor de radio, etcétera.

## 2.2 Entorno operativo de los recursos TI

### *2.2.1 Organización y ubicación geográfica de los recursos de TI*

Los recursos de TI están distribuidos en los 42 departamentos de Hospital Isidro Ayora, cada coordinador o líder departamental tiene a su cargo una cantidad de equipos para realizar los procesos y tareas asignadas. (Ver Anexo 4 “Estructura Organizacional de la Institución”)

El centro de cómputo del HGPIA-LOJA se encuentra ubicado en el segundo piso de la institución. Dentro del centro de cómputo se halla la sala de servidores y la central telefónica.

En la Sala de Servidores se albergan los 3 servidores y la arquitectura de red con sus componentes.

### *2.2.2 Inventario de hardware, software y elementos de telecomunicaciones*

A continuación detallaremos el inventario de todos los recursos de TI del HGPIA-LOJA.

**Inventario de Hardware**

| PRODUCTO | CANTIDAD | SOFTWARE INSTALADO |
|---|---|---|
| **Servidores**<br>• Servidor de Aplicaciones HP Proliant DL360 G5<br>• Servidor de Aplicaciones IBM 5400<br>• Servidor de Internet IBM | 1<br>1<br>1 | Windows server 2000<br>Windows server 2008<br>Linux |
| **Computadoras** | 171 | Windows XP |
| **Laptops** | 8 | Windows XP |
| **Elementos de telecomunicaciones**<br>• Switch Cisco Catalyst 2900 Series XL, 24 puertos<br>• Ruteador Relay Cisco 3600<br>• Cableado estructurado puntos de voz 95 y puntos de datos de 103, categoría 5.<br>• Edificio nuevo 18 puntos de voz y 30 puntos de datos, categoría 6.<br>• Proveedor Internet CNT<br>• Central Telefónica Alcatel 4400.<br>• UPS-3000 Powerware Prestige. | 3<br>1 | |

**Inventario de Sistemas de información del HGPIA-LOJA**

| PRODUCTO |
| --- |
| 1. Sistema de Control de Recursos Humanos (Programas empleados)<br>2. Sistema de Facturación (Administración de Caja)<br>3. Sistema de Administración de Recursos Humanos (Recursos Humanos).<br>4. Sistema de Cámaras (Servicios Generales).<br>5. Sistema de Control de Activos Fijos (Contabilidad)<br>6. Administración y control de procesos de estadística (Implementándose). |

**Inventario de Software del HGPIA-LOJA**

| PRODUCTO |
| --- |
| **Ofimática:** tiene programas Microsoft Office no licenciados<br><br>**Base de Datos:** Mysql Server versión 3.23.49-nt, SQL Server 2005 (no licenciado).<br><br>**Sistema Operativo pagados:** Windows XP, Windows 2000 Profesional, Windows server 2000, Windows server 2008 (no licenciado).<br><br>**Sistemas Operativos gratuitos:** Fedora 11, Ubuntu. |

### *2.2.3 Función del hardware del HGPIA-Loja*

Es muy importante ya que permite trabajar con toda la información de una forma rápida, detallada y económica, para así ahorrar tiempo y esfuerzos inútiles.

En este sentido, un equipo informático está formado no solo por partes físicas sino también por partes no tangibles.

Todo hardware para un correcto funcionamiento debe tener las siguientes características.

- ✓ Fiabilidad
- ✓ Durabilidad

- ✓ Recambiables
- ✓ Compactar la información
- ✓ Velocidad
- ✓ Compatibilidad
- ✓ Bajo costo

En muchos casos el hardware debe ser de marca y no clones para un correcto funcionamiento y una excelente fiabilidad.

### *2.2.4 Función del software del HGPIA-Loja*

Para que el ordenador sea capaz de procesar la información, no basta solo contar con el hardware. Es necesario disponer, además, de un componente que sea capaz de indicar la unidad central de proceso.

- ✓ Como utilizar los dispositivos
- ✓ Cuando utilizarlos
- ✓ Qué hacer con la información.

Es decir, hacen falta los programas. Al conjunto de programas se denominan software permitiendo de esta manera que el hardware realice la función para lo cual se requiera en el hospital.

### *2.2.5 Función de las telecomunicaciones en el HGPIA-Loja*

Es inevitable que las telecomunicaciones siempre han desempeñado un papel muy importante en las instituciones ya que proporcionan una forma sencilla de comunicación electrónica a distancia, satisfaciendo las necesidades de enlace rápido para la solución de problemas existentes. Mediante los puntos de red, el fax, el internet y los puntos de voz, se puede tener los medios de telecomunicaciones de mayor eficiencia y eficacia para el desarrollo tecnológico de instituciones públicas de nuestro país.

Las comunicaciones siempre serán básicas en los procesos de las instituciones públicas para su desarrollo, en especial para logros técnicos, científicos, que impulsan la debida aplicación de la ciencia en beneficio de la humanidad.

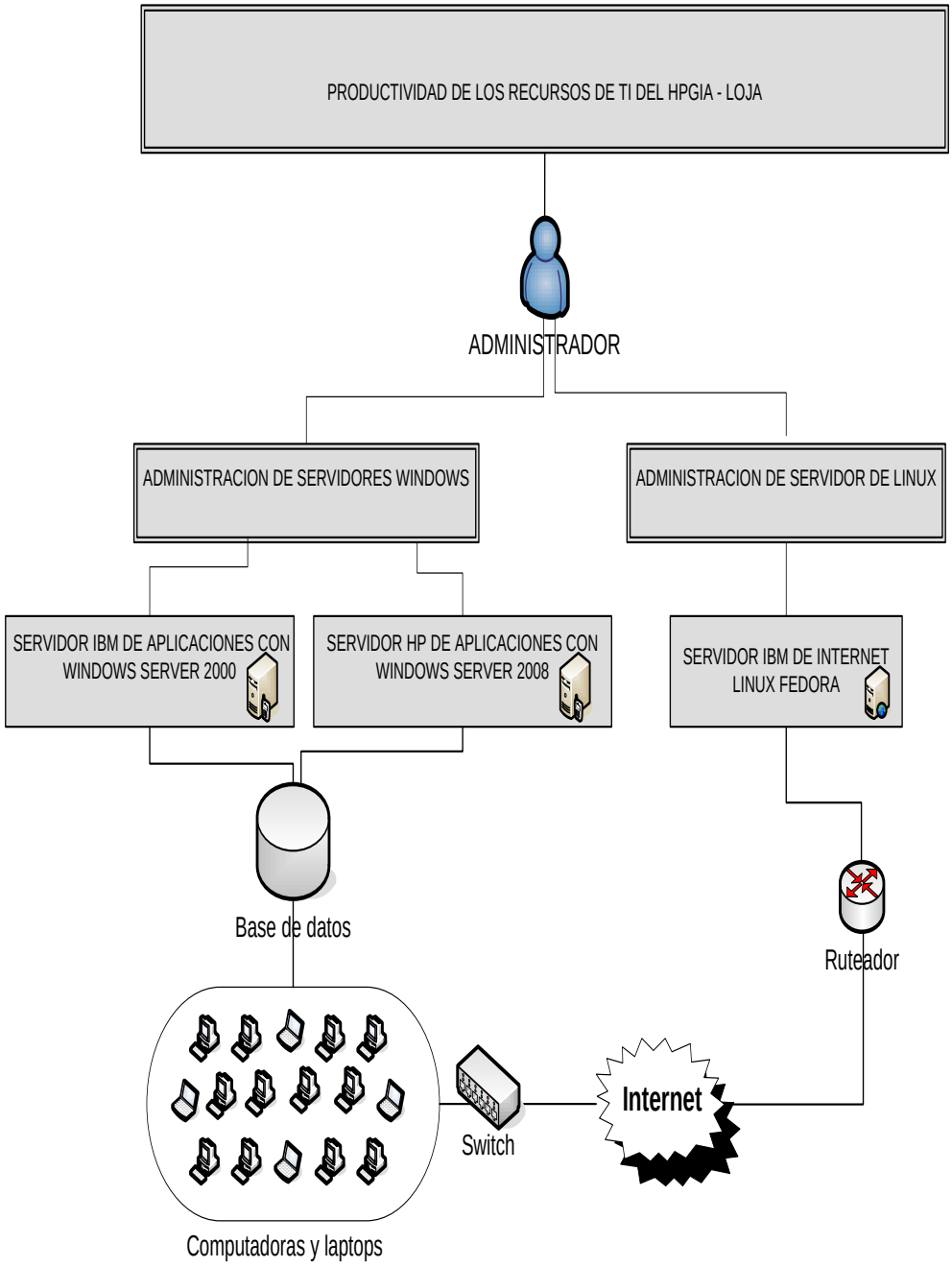
## 2.3. Función del administrador del HGPIA-Loja

### *2.3.1 Objetivos de productividad de los recursos de Ti*

La función del administrador es de brindar servicios a todos los usuarios que manejan un equipo de cómputo, creando espacios de comunicación, atendiendo sugerencias, manteniendo herramientas y el espacio requerido para cada usuario a tiempo y de buena forma, mantener en buen estado los recursos de TI (Hardware, Software y elementos de Telecomunicaciones) del HGPIA-Loja, manteniendo la documentación de todos los recursos de TI, respetando la privacidad de los usuarios y promoviendo el buen uso de los recursos.

Para el administrador del centro de cómputo del HGPIA-Loja, el principal objetivo es la administración de los servidores es decir revisar que todos los servicios que brinda la red funcionen eficientemente. El administrador debe conocer las claves de las cuentas de root de todas las máquinas que administra. Desde esa cuenta puede configurar servicios y establecer políticas que afectaran a todos los usuarios.

### 2.3.2 Organigrama de productividad de los recursos de TI del HGPIA-Loja



## 2.4 Estado actual de los recursos de TI del HGPIA-Loja

### *2.4.1 Diagnóstico Inicial del hardware, software y telecomunicaciones de las pc's, laptops y servidores del HGPIA-Loja*

Los recursos de TI (laptops, pc's, servidores y equipos de telecomunicaciones), que se encuentran en el Hospital General Isidro Ayora de la ciudad de Loja están su mayoría en estado activo.

De acuerdo a la información obtenida de las entrevistas aplicadas a cada uno de los líderes o coordinadores departamentales únicamente 33 computadores cuentan con servicio de Internet, así también 13 computadores están en mal estado, y 29 computadores pertenecen a tecnologías desactualizadas, además se requiere de programas informáticos que ayuden en la ejecución de los procesos que manejan los siguientes departamentos:

| Departamento | Requerimiento del tipo de Software |
|---|---|
| Secretaria de Farmacia | Sistema para Ingreso y Egreso de Recetas medicas |
| Gestión de Emergencia | Sistema Inventario de Medicamentos |
| Calificación de Demanda y Oferta Hospitalaria | Sistema para Control de Producción de Personal |
| Secretaria de Laboratorio Clínico | Sistema para el Control de Registro de Exámenes |

Se tiene planes no formales para la realización de mantenimiento físico y lógico de todos los recursos de TI de la institución por parte del administrador. Además cuentan con bitácoras de todas las actividades que se han realizado diariamente.

De existir algún inconveniente en los recursos de TI, el administrador realizará el seguimiento a la falla, luego realizará el proceso de restauración necesario. En este caso,

para el administrador, los procesos que pueden ser considerados como críticos, son las tareas que se ejecutan a nivel físico y lógico.

Los Sistemas de Información de la institución han sido desarrollados para trabajar en entornos Windows, según el decreto 1014 de la República del Ecuador, establece que toda institución pública debe incorporar software libre para sus sistemas y equipamiento informático.

### *2.4.2 Determinación de los procesos críticos o sensibles de los pc's, laptops y servidores del HGPIA-Loja*

La utilización de los recursos de TI dependerá de un conjunto de procesos por parte del administrador, para garantizar la eficiencia y la confiabilidad de los servicios que se ejecutan en los mismos.

Los procesos de administración primordiales que se realizarán en los recursos de TI de la institución lo detallamos a continuación.

En los servidores Windows, los procesos que el administrador efectúa son:

Servidor de Internet:

- ✓ Control de acceso al servidor.
- ✓ Asignar a máquinas direcciones IP.
- ✓ Mantenimiento físico y lógico preventivo.

Servidor de Aplicaciones:

- ✓ Control de acceso al servidor.
- ✓ Administración del software y aplicaciones.
- ✓ Mantenimiento físico y lógico preventivo.

En las laptops, los procesos que el administrador efectúa son:

Laptops:

- ✓ La administración de cuentas de usuario
- ✓ Administración del hardware y software

- ✓ Mantenimiento físico y lógico correctivo.

En las Pc's, los procesos que el administrador efectúa son:

- ✓ Creación y administración de cuentas de usuario
- ✓ Administración de hardware y software
- ✓ Mantenimiento de físico y lógico correctivo.

En los elementos de telecomunicaciones, los procesos que el administrador efectúa son:

- ✓ Administración de la red
- ✓ Administración de los elementos físicos
- ✓ El mantenimiento físico y lógico correctivo.

Para el administrador el proceso del mantenimiento físico correctivo es considerado como un proceso crítico de todos los recursos de TI; adicional a este, cada recurso tiene procesos que se los puede considerar como críticos, en los cuales se pondrá mayor interés para el desarrollo de nuestra Auditoría Informática.

Los procesos de administración que se llevan en los recursos de TI, son generales para todos ellos, de existir algún problema en los recursos de TI, el administrador realizará el seguimiento a la falla, y luego realizará el proceso de restauración necesario.

# FASE 3

## PLANIFICACIÓN ESPECÍFICA

**CONTENIDOS**

# INTRODUCCIÓN

Las actividades serán planificadas para lograr concordancia entre el trabajo realizado y los objetivos de la auditoría propuestos. Toda la información recolectada de las actividades debe ser probado, razón por la cual será necesario establecer y clasificar los procedimientos de auditoría, logrando de estará manera identificar pertinentemente los rendimientos de administración, si las tuviere.

Esta fase de planificación conlleva a la metodología que se utiliza para realizar la Auditoría Informática, elaborando así un plan de trabajo, utilizando técnicas para la recolección de la información, centrándose en obtener información que sea útil a la hora de evaluar los recursos de TI.

Adicionalmente la distribución del tiempo para el desarrollo de estas actividades será muy importante, según el período estimado de duración de la realización de la auditoría.

# 3. PLANIFICACIÓN ESPECÍFICA

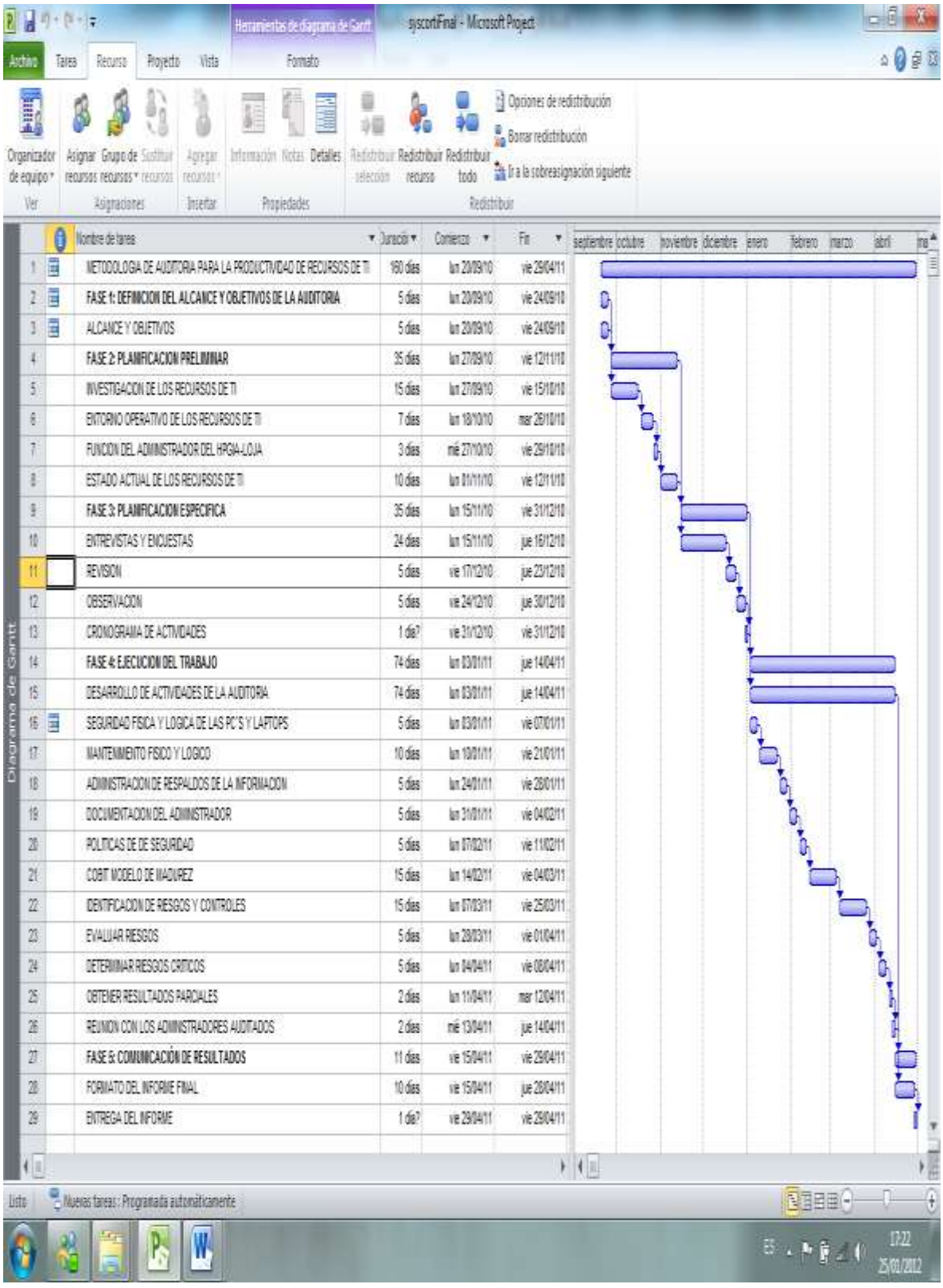
## 3.1 Actividades

Las entrevistas, encuestas, revisiones, observación directa e indirecta son algunas de las técnicas que se utilizaron para el desarrollo de la presente auditoría.

Las actividades de la auditoría están propuestas a evaluar temas como: el proceso de la administración, cumplimiento de políticas, características físicas y el correcto funcionamiento de las laptops, pc's, servidores y elementos de telecomunicaciones, situaciones deficientes, documentación existente, entre otros.

Además hemos sido cuidadosos en la elaboración de las preguntas que fueron empleadas en las técnicas de recopilación de información, cuyo fin era evitar confusiones que produzcan contestaciones ambiguas.

## 3.2 Cronograma de actividades



# FASE 4:

## EJECUCIÓN DEL TRABAJO

## CONTENIDOS

## INTRODUCCIÓN

En la presente fase de la Auditoría Informática, se procederá a desarrollar las actividades planificadas como son: encuestas, entrevistas, etc., aplicadas al administrador del centro de cómputo, líderes departamentales y personal administrativo de la institución; así también se utilizó la técnica de observación, visitando las instalaciones del entorno del equipo informático; además se cuestionó la existencia de documentos que respalden el cumplimiento de la administración de los recursos de TI del Hospital Isidro Ayora de Loja.

En esta fase se analizará y evaluará cada uno de los procesos definidos en la administración de los recursos de TI de la institución, integrados con los procesos del modelo Cobit, así también se identificará la criticidad de cada proceso en base al modelo de madurez de Cobit.

Además se logra obtener toda la información y evidencia necesaria para identificar los posibles riesgos que se pueden presentar en la administración de los recursos de TI del hospital.

Una vez que los riesgos han sido identificados, estos serán analizados y evaluados de tal manera que se pueda emitir las recomendaciones, que ayudaran a mitigar los riesgos, minimizando así el riesgo residual a un nivel aceptable.

Es importante para el desarrollo de esta fase que el auditor siempre tenga a mano su herramienta de trabajo, que consiste en: una cámara digital, grabadora de audio, cuaderno de campo y cámara de vídeo.

# 4. EJECUCIÓN DEL TRABAJO

## 4.1 Procesos que intervienen actualmente en la administración del hardware (pc´s, laptops, servidores), software y elementos de telecomunicaciones del HPGIA-Loja

Para evaluar la eficacia y eficiencia de los procesos que intervienen actualmente en la administración del hardware, software y elementos de telecomunicaciones del hospital Isidro Ayora-Loja, nos hemos basado en la información obtenida de las entrevistas, encuestas, etc.; aplicadas al administrador del centro de cómputo y demás personal administrativo.

### *4.1.1 Seguridad física de las pc´s y laptops*

De la información obtenida de las encuestas, entrevistas y observación directa, se ha podido analizar y evaluar la seguridad física de las pc´s y laptops, se ha identificado los posibles riesgos que pueden afectar la productividad de los equipos.

Para las pc´s, no existe un sello o adhesivo adherido a la caja del CPU, que evite que este sea abierto y sus componentes internos sean extraídos fácilmente por cualquier persona inescrupulosa. Además no existe el respectivo control para garantizar la existencia física de cada equipo, como es el caso en el que los equipos son removidos de un departamento a otro. Por otro lado se encontró equipos que ya han cumplido su tiempo de vida útil y aún no han sido retirados.

Otro aspecto importante encontrado son los accesos no controlados de visitantes a las instalaciones de las pc´s y laptops en especial en el centro de cómputo, dando seguimiento a esta situación se observó que no existe un registro de personas que acceden al entorno de los equipos, además cuando se ausentan los empleados de sus puestos de trabajo, no tienen la precaución de cerrar la puerta, para evitar que los quipos sean robados o mal manipulados.

### 4.1.2 Seguridad lógica de las pc´s y laptops

La seguridad lógica de las pc´s y laptops se lo realiza a través del uso de cuentas de usuario, el 66% de empleados administrativos usan cuentas de usuario de administrador para acceder a los equipos, y un 34% no usa cuentas de usuario para acceder al equipo. Ver información en: (Ver Anexo 3.2, “Formato para Analizar Información Recolectada”).

Las pc´s y laptops tienen instalado software sin sus respectivas licencias, además los antivirus no están actualizados y en algunos equipos se ha procedido a instalar software sin el debido consentimiento del departamento de Informática.

### 4.1.3 Seguridad física de los servidores

La sala de servidores no cuenta con la infraestructura adecuada, están en un cuarto pequeño, cuyas paredes están fabricadas en un 50% con material inflamable (madera), además dentro del cuarto existe gran cantidad de material inflamable (cartón, papel y plástico). Así también hay sillas, cajas y alambres que se prestan para que exista un desorden total (Ver Anexo 9, “Imágenes”).

No existen los respectivos controles para el acceso a la sala de servidores cualquier persona puede entrar y salir fácilmente del lugar, no se lleva un registro o bitácoras de las personas que estuvieron ahí, es más ni siquiera se mantiene la puerta de la sala de servidores debidamente cerrada y con llave.

Los servidores no están colocados en armarios adecuados, están ubicados casi en el piso, haciéndolos vulnerables al polvo, humedad del suelo y manipulación inadecuada de personas no autorizadas o incluso del mismo personal.

### 4.1.4 Seguridad lógica de los servidores

El acceso lógico a los servidores se lo realiza con una cuenta de usuario administrador, la única persona que tiene autorización para acceder a los equipos es el administrador del centro de cómputo. Debido a que los servidores no cuentan con sus respectivas licencias, y no se actualiza los parches estos equipos están expuestos a vulnerabilidades de

infección de virus como el gusano Zotop que es de muy fácil propagación y manda a reiniciar el sistema operativo, la entrada de este es por el puerto TCP/445 en el Servidor de Aplicaciones HP Proliant DL360 G5, asi también se puede producir la ejecución remota de aplicaciones para usuarios no autorizados. Lo mismo sucedería con el servidor IBM 5400 con Windows Server 2008.

### *4.1.5 Seguridad física de los elementos de telecomunicaciones*

Para los elementos de telecomunicaciones no existe una sala adecuada, el espacio donde están colocados es reducido, el cableado no cumple con estándares establecidos, no está ordenado ni debidamente etiquetado. El panel donde se encuentra el cableado de central telefónica, está lleno de polvo y bichos, no se puede identificar fácilmente a que punto de voz pertenecen cada cable puesto que no están debidamente etiquetados.

### *4.1.6 Seguridad lógica de los elementos de telecomunicaciones*

La seguridad lógica de los elementos de telecomunicaciones y las tecnologías de protección han de implementar las medidas y controles que permitan prevenir y gestionar el riesgo de amenazas y han de ayudar a crear procesos automatizados encaminados a disponer de información sobre eventos completos, útiles y de calidad en el momento que sea requerido y que, además, permitan la implantación de mecanismos para la extracción, preservación y conservación de evidencias y registros de utilización de las infraestructuras.

### *4.1.7 Software de la institución*

Los sistemas informáticos que posee la institución, han sido desarrollados para trabajar en entornos Windows, si se aplica el decreto presidencial 1014, estos sistemas quedarían rezagados puesto que han sido desarrollados bajo tecnologías no portables, lo mismo sucedería con las herramientas de ofimática, sistemas operativos, sistemas de base de datos y programas antivirus para entornos Windows. La información sobre Software de la Institución la podemos encontrar en (Ver Anexo 3.2,"Formato para Analizar Información Recolectada").

### 4.1.8 Mantenimiento físico y lógico del hardware

El mantenimiento físico del hardware y elementos de telecomunicaciones no se lo realiza en base a un plan de mantenimiento preventivo, este se lo realiza únicamente cuando los equipos han sufrido algún daño o falla. Así también el mantenimiento lógico de los equipos no se lo realiza en forma periódica, este se lo hace únicamente cuando los equipos han sufrido alteraciones en su funcionamiento.

### 4.1.9 Administración de respaldos de la información

La información de respaldos es sin lugar a duda uno de los elementos más importantes en la administración de los pc's, laptops y servidores, pues si se presenta algún daño en los equipos, con los respaldos se puede recuperar y reconstruir, los datos y archivos dañados o eliminados. La información sobre los respaldos de la información la podemos encontrar en (Ver Anexo 3.2, "Pregunta 9"). Los datos nos indican que no se administran lo respaldos de la información que se manejan en los departamentos de la institución, es importante llevar un procedimiento para asegurar la adecuada administración de los respaldos de la información.

### 4.1.10 Documentación del administrador

El administrador no posee la documentación de los equipos asignados a su cargo, así como también de los procesos y subprocesos del centro de cómputo. Mediante entrevistas y oficios dirigidos al administrador, solicitando documentación de los procedimientos que llevan, se pudo determinar que no existen procedimientos establecidos formalmente para ejecutar de manera eficiente cada uno de las actividades que se realizan en el centro de cómputo.

### *4.1.11 Políticas de seguridad*

El Hospital Isidro Ayora no cuenta con políticas de seguridad a nivel informática, estas no se encuentran definidas, no obstante en base a la información recopilada se ha logrado determinar que si es importante poner en marcha la creación de estas políticas.

## 4.2 COBIT modelo de madurez

Actualmente el director y administradores de la institución son los responsables de la governancia de las TI. Para ello deben definir un plan de negocio que les permita obtener un nivel óptimo en la administración y controles de las tecnologías de TI.

El modelo de madurez está diseñado como perfil de proceso de TI, a los que una empresa lo reconocería como estados actuales o futuros, estos modelos no han sido diseñados como limitantes en los que si no se cumple con los niveles previos no se puede avanzar hacia el siguiente nivel.

Se ha evaluado cada uno de los procesos definidos para esta auditoría con una escala de medición creciente de 0(no existente) a 5(optimizado).

La ventaja es que es relativamente fácil para la dirección ubicarse a sí misma en una escala y de esta forma saber que es los que se puede hacer si se quiere una mejora.

A continuación se muestra la tabla de modelo de madurez genérica a usarse en la auditoria. Ver Tabla 1

| | |
|---|---|
| **0 No Existente** | Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver. |
| **1 Inicial** | Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad-hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado. |

| | |
|---|---|
| **2 Repetible** | Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables. |
| **3 Definido** | Los procedimientos se han estandarizado y documentado, y se han difundido a través del entendimiento. Sin embargo, se deja al individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes. |
| **4 Administrado** | Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada. |
| **5 Optimizado** | Los procesos se han definido hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que las empresas se adapten de manera rápida. |

**Tabla1. Modelo Genérico de Madurez**
**Fuente:** Documento Cobit 4.0

A continuación se detalla el porqué del nivel de madurez definido:

### *Dominio Planear y Organizar*

#### PO1 DEFINIR UN PLAN ESTRATEGICO DE TI

El HPGIA, no tiene definido un plan estratégico, no se toma en cuenta el beneficio que le pueden brindar las TI, para ofrecer un servicio de calidad a los pacientes que acuden todos los días a esta institución.

Se recomienda crear el plan estratégico el cual es importante para la administración y dirección de los recursos de TI, con esta planificación el HPGIA y el departamento de gestión informática son los responsables directos de que los proyectos e investigaciones se realicen de forma óptima, para satisfacción de todos.

**PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN**

La arquitectura de la información no se encuentra definida en el HGPIA, el administrador lleva la documentación como él piensa que es conveniente y la archiva.

El HGPIA, no cuenta con un diccionario corporativo de datos que contenga las reglas de sintaxis de los datos de la institución, por lo tanto no se cuenta con información segura y confiable, que ayude para la toma de decisiones gerenciales.

**PO9 EVALUAR Y ADMINISTRAR RIESGOS DE TI**

No existe una evaluación y administración de riesgos en el departamento de gestión Informática ni siquiera se le da la importancia en el caso de que alguna eventualidad sucediera, no se podrá determinar el impacto que puede ocasionar sobre las metas del negocio sino no se definen los controles que ayuden a mitigarlos.

Las TI están expuestas a todo tipo de amenaza, en el caso de que estas sucedieran, no se le puede dar respuesta de forma inmediata, y esto puede afectar a las funciones del departamento y al rendimiento de otros departamentos.

### *Adquirir e Implantar*

**AI1 IDENTIFICAR SOLUCIONES AUTOMATIZADAS**

Para identificar soluciones automatizadas el departamento de gestión informática no ha desarrollado metodologías que permitan garantizar el buen levantamiento de requerimientos, que satisfagan de forma efectiva y eficiente el uso de soluciones automatizadas, además no hay estudios de factibilidad que permitan examinar la

posibilidad de implantar los requerimientos levantados. Este proceso se tiende a hacer de manera informal por parte del administrador del centro de cómputo.

**AI2 ADQUIRIR Y MANTENER EL SOFTWARE APLICATIVO**

Si bien este es uno de los procesos que debe ejecutar el administrador del centro de cómputo conjunto con el administrador general y el director de HPGIA, para adquirir y mantener el software aplicativo, esto no se hace en base a un estudio de adquisición del software, simplemente se ve las necesidades superfluas de los departamentos a nivel de requerimientos y procede a la adquisición, tal es el caso que en alguna ocasión se había comprado software que no satisfacía las necesidades del departamento que lo solicito, y simplemente nunca se lo uso.

Además el administrador no da mantenimiento al software ya que en la mayoría el software es desarrollado por estudiantes egresados de las distintas universidades de Loja y a nivel de departamento no se ejecuta el proceso de mantenimiento de software aplicativo.

**AI3 ADQUIRIR Y MANTENER LA INFRAESTRUCTURA TECNOLÓGICA**

La institución no cuenta con un plan de adquisición de tecnológica para controlar los procesos de adquirir, implantar y actualizar la infraestructura tecnológica.

Los cambios en la infraestructura tecnológica se hacen a medida que se necesite ya sea por actualización de nuevos equipos o por la implementación de nuevo software aplicativo para la institución, el mantenimiento de los equipos de TI se lo hace únicamente cuando se presentan daños o fallas en los equipos, no se da mantenimiento preventivo con la debida planificación de un calendario de trabajo.

**AI4 FACILITAR LA OPERACIÒN Y EL USO**

En el departamento de gestión informática no existe un manual de políticas, que sirva como guía para el buen y fácil uso de las TI, en el departamento que usan software

aplicativo existe poco dominio de la herramienta de software implantado, originando pérdida de tiempo porque aparecen nuevas dudas con respecto al uso del software por parte del usuario. Muchas veces se entrega manuales de usuario pero este no llega a todos los usuarios que manejan el sistema y hay algunos usuarios que ni siquiera saben de la existencia de los manuales.

**AI5 ADQUIRIR RECURSOS DE TI**

La adquisición de recursos de TI se hace en base a los lineamientos de adquisición de compras públicas del HPGIA, para esto el departamento de proveeduría selecciona al proveedor, evaluando el costo, calidad, cumplimiento de requerimientos específicos, licencias de software y la legalidad del proveedor.

### *Entregar y Dar Soporte*

**DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.**

Se tiene conciencia de la formalización de acuerdos internos y externos en línea con los requerimientos y capacidad de entrega, este proceso se ejecuta informalmente no hay un plan de rendición de cuentas con respecto a los niveles de servicio.

**DS3 ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD**

No existe una administración del desempeño y capacidad de las TI, el usuario es a veces el que tiene que solucionar problemas que tiene a su alcance, como no existe un plan para monitorear el desempeño, cuando los usuarios no pueden solucionar el problema se procede a llamar al administrador del centro de cómputo quien es el encargado de solucionarlo.

**DS11 ADMINISTRAR LOS DATOS**

Los datos no se administran de forma eficiente, cada departamento es el dueño de su información, la gran mayoría no tiene la buena costumbre de crear un respaldo de la información que es crítica, simplemente los datos se almacenan en el disco duro de cada

máquina. El administrador lo que hace es crear una copia diaria de respaldo del servidor de aplicaciones, porque en este se encuentran las bases de datos del software de aplicación, por el resto de departamentos él no se preocupa de la administración de los datos.

La administración de los datos del HPGIA no está definida de manera formal, para su recuperación, almacenamiento y procesamiento. En la siguiente tabla se muestra la calificación de cada proceso Cobit luego de su evaluación:

| REPORTE DE NIVELES DE MADUREZ | | |
|---|---|---|
| | **Proceso** | **Grado de Madurez** |
| **DOMINIO PLANEAR Y ORGANIZAR** | | |
| P01 | Definir un plan estratégico | 1 |
| P02 | Definir la arquitectura de la información | 1 |
| P09 | Evaluar y administrar riesgos de TI | 0 |
| **DOMINIO ADQUIRIR E IMPLANTAR** | | |
| AI1 | Identificar soluciones automatizadas | 1 |
| AI2 | Adquirir y mantener Software aplicativo | 1 |
| AI3 | Adquirir y mantener infraestructura tecnológica | 1 |
| AI4 | Facilitar la operación y el uso | 1 |
| AI5 | Adquirir recursos de TI | 4 |
| **DOMINIO ENTREGAR Y DAR SOPORTE** | | |
| DS1 | Definir y administrar los niveles de servicio | 1 |
| DS7 | Administrar el desempeño y la capacidad | 1 |
| DS11 | Administrar los datos | 1 |

**Tabla2. Resultado de los niveles de Madurez**

### 4.3. Evaluación y administración de riesgos de TI del HGPIA-Loja, siguiendo el modelo COBIT

Para el proceso de evaluación y administración de riesgos de TI del Hospital Isidro Ayora, siguiendo el modelo Cobit se definen las siguientes fases:

- ✓ Identificación de Riesgos de TI
- ✓ Evaluación de Riesgos de TI
- ✓ Respuesta a los riesgos de TI

### *4.3.1 Identificación de riesgos de TI*

Para la identificación de los riesgos, nos basamos en el análisis de las entrevistas, encuestas, observaciones directas, documentos, imágenes y videos obtenidos de la institución. (Ver Anexo 3.2 para la interpretación de las entrevistas, Anexo 3.3 para la interpretación de las encuestas y Anexo 9 para imágenes del Centro de Cómputo del HGPIA-LOJA).

**Listado de posibles de Riesgos**

**MATRIZ DE IDENTIFICACIÓN DE RIESGOS**

| Cod_Riesgo | Riesgo |
|---|---|
| **De Infraestructura** | |
| **R01** | **Falta de Mecanismos de Seguridad para el Acceso al Centro de Cómputo del HGPIA-Loja.** |
| **R02** | **La Falta de Seguridad Física de las pc's y laptops del HGPIA-Loja.** |
| **R03** | **La Falta de Seguridad Física para el Servidor de Internet y de Aplicaciones del HGPIA-Loja.** |
| **R04** | **La Falta de Seguridad Física para los Elementos de Telecomunicaciones del HGPIA-Loja** |
| **R05** | **La Falta de Seguridad Lógica para el Servidor de Internet y de Aplicaciones del HGPIA-Loja.** |

| | |
|---|---|
| **R06** | **La Falta de Seguridad Lógica de las pc´s y laptops del HGPIA-Loja.** |
| **R07** | **La Falta de Seguridad Lógica para los Elementos de Telecomunicaciones del HGPIA-Loja.** |
| **R08** | **Falta de Controles de la Temperatura y Humedad del Entorno del Hardware del HGPIA-Loja** |
| **R09** | **La Falta de Actualización de los Antivirus de los Equipos Informáticas del HGPIA-Loja** |
| **R10** | **Ausencia de Seguros contra robo para los recursos de TI (pc´s, laptops, servidores y ruteadores) del HGPIA-Loja** |
| **R11** | **Ausencia de Controles en el tratamiento del Hardware del HGPIA-Loja** |
| **R12** | **Alteración, Destrucción y/o Pérdida de Información relevante para el HGPIA-Loja.** |
| **R13** | **Falta de inventario actualizado de las partes y/o piezas de los computadores del HGPIA-Loja** |
| **R14** | **Falta de licencias para Instalación y Actualización del software del HGPIA-Loja.** |
| **R15** | **La Falta de un Inventario Detallado y Actualizado de los Equipos Informáticos del HGPIA-Loja, por parte del subproceso Gestión Informática.** |
| **R16** | **El Uso de Material Inflamable en la Construcción de la Sala de Servidores del HGPIA-Loja** |
| **R17** | **Existencia de Material Inflamable en las Instalaciones de la Sala de Servidores del HGPIA-Loja** |
| **R18** | **Incendio en el Centro de Cómputo del HGPIA-Loja.** |
| **R19** | **Inexistencia de la administración de cuentas de usuario de los computadores del HGPIA-Loja.** |

| | |
|---|---|
| R20 | No existe la respectiva administración de configuraciones del servidor de internet del HGPIA-Loja. |
| R21 | No existe la respectiva administración de configuraciones del servidor de Aplicaciones del HGPIA-Loja |
| De Procesos | |
| R22 | Inexistencia del plan informático y ejecución |
| R23 | Inexistencia del Plan de Mantenimiento Físico del Hardware. |
| R24 | Inexistencia del Plan de mejoramiento de procesos automatizados. |
| R25 | Inexistencia del Plan administración de redes de conectividad y central telefónica. |
| R26 | Inexistencia del plan informático de contingencia y ejecución |
| R27 | Inexistencia del plan de obtención y almacenamiento de los respaldos de información. |
| R28 | Inexistencia del plan de mantenimiento físico de la red del HGPIA-Loja |
| R29 | Inexistencia del plan de mantenimiento lógico de la red del HGPIA-Loja |
| R30 | Inexistencia del Plan de Adquisición de Hardware y Software para Redes |
| R31 | Inexistencia del plan de adquisición de hardware para el HGPIA-Loja |
| R32 | Inexistencia del Plan para la Contratación del Personal de Informática del HGPIA-Loja |
| R33 | Inexistencia del plan de adquisición de software para el HGPIA-Loja |

| | |
|---|---|
| **R34** | **Inexistencia del plan de adquisición de elementos de telecomunicaciones para el HGPIA-Loja** |
| **R35** | **Inexistencia del plan de continuidad del Negocio del HGPIA-Loja:**<br>• **Falta de un plan de Recuperación**<br>• **Falta de un plan de Reanudación**<br>• **Falta de un plan de Contingencia en el caso:**<br>  ○ **Robo**<br>  ○ **Incendio**<br>  ○ **Vandalismo**<br>  ○ **Perdida de Energía** |
| **De Personal** | |
| **R36** | **La falta de entrenamiento y capacitación al personal del centro de cómputo en estándares y tecnología de vanguardia.** |
| **R37** | **La falta de asignación de funciones formalizadas al personal de gestión informática.** |
| **R38** | **Desconocimiento de que hacer para salvaguardar el hardware en el caso de incendios.** |

### *4.3.2 Evaluación de riesgos de TI*

**Ponderación de riesgos de TI del HPGI-Loja**

Los riesgos de calcularán multiplicando la cuantificación del impacto (severidad) por la cuantificación de la probabilidad (ocurrencia) de aparición. Es decir:

**PONDERACIÓN DEL RIESGO= IMPACTO * PROBABILIDAD**

La cuantificación del impacto como la de probabilidad se calificara en valores de 1 a 5 como se describe en las siguientes tablas:

El **impacto** es la medida del daño o perjuicio que ocasionaría un riesgo en caso de que se haga realidad.

| Análisis de riesgos Impacto | |
|---|---|
| Muy alto | 5 |
| Alto | 4 |
| Moderado | 3 |
| Bajo | 2 |
| Muy bajo | 1 |

La **probabilidad de ocurrencia** de un riesgo es la estimación de la posibilidad de que este se haga realidad.

| Análisis de riesgos Probabilidad de ocurrencia | |
|---|---|
| Muy probable | 5 |
| Bastante probable | 4 |
| Probable | 3 |
| Poco probable | 2 |
| Improbable | 1 |

Para determinar el nivel de aceptación del riesgo, se tomará como base los valores de la siguiente tabla:

| Intervalo [4] | Nivel de Riesgo |
|---|---|
| (1-6.25) | Muy Bajo |
| (7.25-12.50) | Bajo(Aceptable) |
| (13.50-18.75) | Medio(Precauciones) |
| (19.75-25) | Alto(Inaceptable) |

**MATRIZ DE RIESGOS DEL HGPIA – LOJA**

| Cód_Riesgo | Descripción del Riesgo | Impacto | Probabilidad. | Riesgo Inherente | Nivel del Riesgo | Asignado al |
|---|---|---|---|---|---|---|
| **De Infraestructura** | | | | | | |
| R01 | Falta de Mecanismos de Seguridad para el acceso al Centro de Computo del HGPIA-Loja. | 5 | 5 | 5*5=25 | **25 (Alto Inaceptable)** | Administrador |
| R02 | La Falta de Seguridad Física de las pc´s y laptops del HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R03 | La Falta de Seguridad Física para el Servidor de Internet y de Aplicaciones del HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R04 | La Falta de Seguridad Física para los Elementos de | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Telecomunicaciones del HGPIA-Loja | | | | | |
| R05 | La Falta de Seguridad Lógica para el Servidor de Internet y de Aplicaciones del HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | |
| R06 | La Falta de Seguridad Lógica de las pc´s y laptops del HGPIA-Loja. | 4 | 5 | 4*5=20 | **20(Alto Inaceptable)** | Administrador |
| R07 | La Falta de Seguridad Lógica para los Elementos de Telecomunicaciones del HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable) )** | Administrador |
| R08 | Falta de Controles de la Temperatura y Humedad del Entorno del Hardware del HGPIA-Loja | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R09 | La Falta de Actualización de los Antivirus de los Equipos Informáticos del HGPIA-Loja | 5 | 3 | 5*3=15 | **15 (Medio Precauciones)** | Administrador |
| R10 | Ausencia de seguros contra robo para los recursos de TI del HGPIA-Loja. | 4 | 3 | 4*3=12 | **12 (Bajo Aceptable)** | Administrador |
| R11 | Ausencia de Controles en el Tratamiento o Destrucción del Hardware del HGPIA-Loja | 4 | 4 | 4*4=16 | **16 (Medio Precauciones)** | Administrador |

| | | | | | | |
|---|---|---|---|---|---|---|
| R12 | Alteración, Destrucción y/o Pérdida de información relevante para el HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R13 | Falta de inventario actualizado de las partes y/o piezas de los computadores del HGPIA-Loja | 5 | 3 | 5*3=15 | **15(Medio Precauciones)** | Administrador |
| R14 | Falta de licencias para instalación y actualización del software del HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R15 | La Falta de un Inventario Detallado y Actualizado de los Equipos Informáticos del HGPIA-Loja, por parte del subproceso Gestión Informática. | 5 | 3 | 5*3=15 | **15(Medio Precauciones)** | Administrador |
| R16 | El Uso de Material Inflamable en la Construcción de la Sala de Servidores del HGPIA-Loja | 5 | 5 | 5*5=25 | **25 (Alto Inaceptable)** | Administrador |
| R17 | Existencia de Material Inflamable en las Instalaciones de la Sala de Servidores del HGPIA-Loja | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R18 | Incendio en el Centro de Cómputo del HGPIA-Loja. | 5 | 3 | 5*3=15 | **15 (Medio Precauciones)** | Administrador |

| | | | | | | |
|---|---|---|---|---|---|---|
| R19 | Inexistencia de la administración de cuentas de usuario de los computadores del HGPIA-Loja. | 3 | 3 | 3*3=9 | **9 (Bajo Aceptable)** | Administrador |
| R20 | No existe la respectiva administración de configuraciones del servidor de internet del HGPIA-Loja. | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| R21 | No existe la respectiva administración de configuraciones del servidor de Aplicaciones del HGPIA-Loja | 5 | 4 | 5*4=20 | **20 (Alto Inaceptable)** | Administrador |
| **De Proceso** | | | | | | |
| R22 | Inexistencia del plan informático y ejecución | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R23 | Inexistencia del Plan de Mantenimiento Físico del Hardware | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R24 | Inexistencia del plan de mejoramiento de procesos automatizados. | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |

| | | | | | | |
|---|---|---|---|---|---|---|
| R25 | Inexistencia del plan administración de redes de conectividad y central telefónica. | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R26 | Inexistencia del plan informático de contingencia y ejecución | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R27 | Inexistencia del plan de obtención y almacenamiento de los respaldos de información. | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R28 | Inexistencia del plan de mantenimiento físico de la red del HGPIA-Loja | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R29 | Inexistencia del plan de mantenimiento lógico de la red del HGPIA-Loja | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R30 | Inexistencia del Plan de Adquisición de Hardware y Software para Redes | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R31 | Inexistencia del plan de adquisición de hardware para el HGPIA-Loja | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R32 | Inexistencia del Plan para la Contratación del Personal de Informática del HGPIA-Loja | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R33 | Inexistencia del plan de adquisición de software | 4 | 5 | 4*5=20 | **20 (Alto** | Administr |

| | | | | | | |
|---|---|---|---|---|---|---|
| | para el HGPIA-Loja | | | | **Inaceptable)** | ador |
| R34 | Inexistencia del plan de adquisición de elementos de telecomunicaciones para el HGPIA-Loja | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| R35 | Inexistencia del plan de continuidad del Negocio del HGPIA-Loja:<br>• Falta de un plan de Recuperación<br>• Falta de un plan de Reanudación<br>• Falta de un plan de Contingencia:<br>○ Robo<br>○ Incendio<br>○ Vandalismo<br>○ Perdida de Energía<br>○ Humedad | 4 | 5 | 4*5=20 | **20 (Alto Inaceptable)** | Administrador |
| **De Personal** | | | | | | |
| R36 | La falta de entrenamiento y capacitación al personal del centro de cómputo en estándares y tecnología de vanguardia. | 3 | 4 | 3*4=12 | **12 (Bajo Aceptable)** | Recursos Humanos |
| R37 | La falta de asignación de funciones formalizadas al personal del subproceso Gestión Informática. | 3 | 4 | 3*4=12 | **12 (Bajo Aceptable)** | Jefe de Gestión Informática |
| R38 | Desconocimiento de que hacer para salvaguardar el hardware en el caso de incendios. | 5 | 3 | 5*3=15 | **15 (Medio Precauciones)** | Personal |

Una vez que los riesgos han sido ponderados se procede a evaluar la "calidad de la gestión", con el fin de determinar cuán eficaces son los controles establecidos por la institución para mitigar los riesgos identificados. En la medida que los controles sean más eficientes y la gestión de riesgos pro-activa, el indicador de riesgo inherente neto tiende a disminuir.

Para valorar la efectividad de los controles se lo hará en base a los datos de la siguiente tabla:

| CONTROL | EFECTIVIDAD |
|---|---|
| Destacados | 5 |
| Alto | 4 |
| Medio | 3 |
| Bajo | 2 |
| Ninguno | 1 |

Finalmente, se procede a calcular el "riesgo neto o residual", que es la relación entre el nivel de Riesgo Inherente y el Promedio de Efectividad de los Controles, es decir:

**Riesgo Residual= Nivel de Riesgo Inherente/Promedio de Efectividad de Controles**

**MATRIZ DE RIESGO RESIDUAL**

| Cod_Riesgo | Nivel del Riesgo | Calidad de Gestión | | | Riesgo Residual (**) |
|---|---|---|---|---|---|
| | | Tipo de medidas de Control | Efectividad | Promedio (*) | |
| **De Infraestructura** | | | | | |
| R01 | 25 | No se aplica ningún Control | 1 | 1 | 25 |
| R02 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R03 | 20 | Aislado en un cuarto | 2 | 2 | 10 |
| R04 | 20 | No se aplica ningún Control | 2 | 2 | 20 |
| R05 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R06 | 20 | Uso de contraseñas | 2 | 2 | 10 |
| R07 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R08 | 20 | Uso de Aire Condicionado | 2 | 2 | 10 |
| R09 | 15 | No se aplica ningún Control | 1 | 1 | 15 |
| R10 | 12 | No se aplica ningún Control | 1 | 1 | 12 |

| | | | | | |
|---|---|---|---|---|---|
| R11 | 16 | No se aplica ningún Control | 1 | 1 | 16 |
| R12 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R13 | 15 | No se aplica ningún Control | 1 | 1 | 15 |
| R14 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R15 | 15 | No se aplica ningún Control | 1 | 1 | 15 |
| R16 | 25 | No se aplica ningún Control | 1 | 1 | 25 |
| R17 | 25 | No se aplica ningún Control | 1 | 1 | 25 |
| R18 | 15 | Uso de Extintor | 2 | 2 | 7.5 |
| R19 | 9 | No se aplica ningún Control | 1 | 1 | 9 |
| R20 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R21 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| **De Procesos** | | | | | |
| R22 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R23 | 20 | No se aplica ningún Control | 1 | 1 | 20 |

| | | | | | |
|---|---|---|---|---|---|
| R24 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R25 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R26 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R27 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R28 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R29 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R30 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R31 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R32 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R33 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R34 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| R35 | 20 | No se aplica ningún Control | 1 | 1 | 20 |
| **De Personal** | | | | | |
| R36 | 12 | No se aplica ningún Control | 1 | 1 | 12 |

| | | | | | |
|---|---|---|---|---|---|
| R37 | 12 | No se aplica ningún Control | 1 | 1 | 12 |
| R38 | 15 | No se aplica ningún Control | 1 | 1 | 15 |

(*) Promedio de los datos de efectividad

(**) Resultado de la división entre nivel de riesgo / Promedio de efectividad

### *4.3.3 Respuesta a los riesgos de TI*

**De Infraestructura**

**Riesgo R01: <u>Falta de Mecanismos de Seguridad para el acceso al Centro de Cómputo del HGPIA-Loja.</u>**

Como el Centro de Cómputo es el lugar donde se concentran los recursos informáticos de gran valor y necesarios para el procesamiento de información de la institución, es conveniente que se apliquen una serie de controles para proteger físicamente el equipamiento informático y de telecomunicaciones. El ingreso a las instalaciones del centro de cómputo del hospital Isidro Ayora no es controlado, cualquier persona puede entrar y salir del mismo sin registrarse. Esta situación podría ocasionar, que personas no autorizadas manipulen de mala manera los equipos, alterando el estado de los mismos, haciendo más difícil el trabajo para el administrador, ya que no se podrá determinar fácilmente que usuario estuvo ahí y que cambio realizo en los equipos.

**Recomendación:** Para controlar el acceso físico al Centro de Cómputo es necesario que se implementen mecanismos de seguridad tales como:

- ✓ Llevar un registro de entrada y salida de las personas que visitan el Centro de Cómputo, para ello se debe solicitar información de sus datos personales. Siempre es importante verificar que los datos proporcionados sean reales, esto se puede conseguir solicitando el documento de identidad de la persona que accedió al lugar.

- ✓ Establecer un listado de personas que tengan la respectiva autorización para el ingreso al centro de cómputo, se deberá validar su ingreso verificando en la lista, seguidamente se deberá hacer el registro de la persona.
- ✓ En el caso de infraestructura y tecnología se podría usar: Torniquetes, Cámaras de Seguridad, Tarjetas de Identificación, Detectores de Movimiento, Sistemas Biométricos. Pero si por falta de presupuesto no se puede implementar ninguno de los ítems propuestos anteriormente por lo menos se debería tener la política de mantener la puerta de entrada al centro de cómputo y sala de servidores con llave. También es importante colocar la respectiva señalética para zonas de acceso restringidas.

**Riesgo R02: La Falta de Seguridad Física de las pc's y laptops del HGPIA-Loja.**

En base a la observación y encuestas aplicadas al personal administrativo de la institución que trabaja con equipos informáticos, se pudo determinar que no existe un respectivo plan de trabajo para dar el adecuado mantenimiento físico a los equipos, únicamente se les da mantenimiento cuando estos tienen alguna alteración en su funcionamiento.

Como es de esperarse, es imposible evitar que el personal administrativo tenga acceso a las pc's o laptops sobre las que tiene que trabajar, convirtiéndose así en uno de los puntos más difíciles de controlar, siempre es importante asegurarse de que los computadores están siendo manipulados por la persona idónea.

Las pc's y laptops deben estar sometidas a las directrices establecidas en las Políticas de Seguridad de la institución.

**Recomendación:** Para proteger la seguridad física de las pc´s y laptops se debería:

- ✓ Hacer conocer al usuario del equipo que es el responsable de impedir que personas no autorizadas hagan uso de las pc's o laptops.
- ✓ Dar el respectivo mantenimiento físico preventivo de las pc's y laptops para evitar posibles fallas o daños.
- ✓ En las áreas donde se tenga pc's o laptops, no se permitirá fumar ya que si se deja colillas de cigarrillo mal apagadas se puede provocar un incendio, tomar

ningún tipo de bebidas o consumir alimentos porque estos pueden ser derramados accidentalmente sobre los equipos y producir daño total o parcial en su funcionamiento.

- ✓ Implantar soluciones para controlar las conexiones de dispositivos USB en las pc's y laptops. Esto se puede lograr:
  - Desahabilitando los puertos USB desde: el Administrador de Dispositivos del Windows -Controladores de bus serie universal- controlador USB Family -propiedades controlador USB Family-click pestaña controlador-click en el botón Deshabilitar (puerto seleccionado) y finalmente click en el botón en Aceptar
- ✓ Controlar que los usuarios, no cambien las configuraciones de los equipos e intenten solucionar los problemas de funcionamiento por su propia cuenta, deberán notificar en todo caso al departamento de Gestión Informática. Este punto se puede controlar asignando una cuenta de usuario invitado a cada empleado administrativo que tenga a su cargo un computador.
- ✓ Limitar el uso de disqueteras y unidades lectoras/grabadoras de CD's y DVD's, para evitar que se pudiera grabar información sensible o se pudiera introducir contenidos dañinos en el equipo(virus, troyanos, gusanos o programas espías)
- ✓ Implementar soluciones para evitar que se roben los componentes que están dentro del CPU:
  - Sellar cada caja del CPU con adhesivos para evitar que la caja del computador sea abierta fácilmente por algún intruso y los componentes del CPU sean robados, estos adhesivos serán retirados únicamente cuando el personal de mantenimiento vaya a realizar su trabajo.
  - Taladrar y poner un candado o sistema similar en la caja que impida su apertura, aunque esto es difícil, puesto que lo que suele buscar un supuesto intruso son los datos contenidos en el disco duro, y para eso con abrir parcialmente la caja le basta.
  - Adquirir cajas más seguras. Varias compañías venden cajas que tienen cerraduras y sistemas de anclaje de la tapa con el armazón que proporcionan una seguridad considerable contra intrusos.

**Riesgo R03: La Falta de Seguridad Física para el Servidor de Internet y de Aplicaciones del HGPIA-Loja.**

En el Hospital Isidro Ayora existen: 1 servidor de Internet y 2 de Aplicaciones, al observar la instalaciones donde se encuentran albergados estos equipos, nos pudimos dar cuenta que no se cumplen con la infraestructura adecuada, están en un cuarto pequeño, cuyas paredes están fabricadas en un 50% con material inflamable (madera), además dentro del cuarto existe gran cantidad de material inflamable (cartón, papel y plástico) que podrían conllevar a que se genere un incendio. Hay además sillas, cajas y alambres que se prestan para que existan un desorden total, todos estos objetos no deberían estar ahí puesto que se trata de una sala de servidores.

No existen controles de acceso a la sala de servidores cualquier persona puede entrar y salir fácilmente del lugar, además no existe un registro o bitácoras de las personas que estuvieron ahí, es más ni siquiera se mantiene la puerta cerrada y con llave.

Los servidores no están colocados en armarios adecuados, están ubicados casi en el piso, haciéndolos vulnerables al polvo, humedad del suelo y manipulación inadecuada de personas no autorizadas o incluso del mismo personal.

Con respecto al cableado de los equipos de red, que se encuentra en sala de servidores estos no están debidamente ordenados.

En vista de que los servidores son los recursos de TI más importantes para la institución en cuanto a costo e información que procesan, se debería cumplir con ciertas especificaciones físicas para su correcto funcionamiento.

**Recomendación:** Para la seguridad física de los servidores se debería:

- ✓ Controlar el acceso, aislando los servidores en un cuarto con llave o con cerradura electrónica cuya clave sólo conocerá el administrador. Llevar el respectivo registro de personas que entran y salen de la sala de servidores

- ✓ Ponerlos bajo llave en su estante. Las cintas de respaldo deben estar guardadas en armarios ignífugos con llave en un cuarto cerrado y para mayor seguridad de los respaldos se los podría poner en distintos lugares del edificio.
- ✓ Usar UPS o generadores y testearlos para garantizar que la producción no se detenga en el caso de que se produzca algún corte o baja del fluido eléctrico.
- ✓ Darles el adecuado mantenimiento preventivo para evitar posibles daños o fallas.
- ✓ Mantener la temperatura y humedad adecuada. La temperatura debería estar entre los 21 y 23 grados centígrados, y la humedad debería estar entre 40 y 50%.
- ✓ Retirar objetos ajenos de una sala de servidores en dicha sala.
- ✓ Los cables propios de estas ubicaciones, deberían estar perfectamente identificados**,** evitando que puedan interrumpir el paso u ocasionar molestias**.** De esta forma se protege a quien opera con los servidores, y al mismo tiempo se asegura que no se producirá un corte o daño en los mismos.

**Riesgo R04: La Falta de Seguridad Física para los Elementos de Telecomunicaciones del HGPIA-Loja.**

**Recomendación:** Para garantizar el buen funcionamiento de las telecomunicaciones y para lograr alcanzar el tiempo máximo de vida útil de sus componentes y periféricos es necesario tomar en cuenta lo siguiente:

**REQUISITOS ARQUITECTÓNICOS**

- ✓ La sala en donde se albergan los componentes de Telecomunicaciones deberá tener un área mínima de 16 $m^2$.
- ✓ Para protección del área se recomienda eliminar las ventanas de vidrio hacía el exterior o, en su caso, instalar protectores.

**REQUISITOS AMBIENTALES**

- ✓ La temperatura debe estar entre 15º C y 30º C grados centígrados, pero se recomienda que esté a 22º C estables. También se recomienda la instalación de un aire acondicionado tipo industrial de preferencia.

- ✓ La humedad debe estar entre 20 y 55% no condensada.
- ✓ La sala debe estar bien iluminada.
- ✓ El equipo debe estar alejado de fuentes de calor (reguladores, baterías de respaldo, etc.) campos electrostáticos o electromagnéticos (transformadores, tableros de control eléctrico, etc.) y de radio frecuencia (equipos de sonido, equipos de comunicación, etc.)

**REQUISITOS DE TELECOMUNICACIONES**

Se recomienda seguir las normas de cableado estructurado, según la norma vigente, que garantizan una mejor administración de los servidores de red, equipos de telecomunicaciones y cableado de los mismos, de acuerdo con los siguientes lineamientos:

- ✓ Instalación de un rack de piso de 19" de ancho y 7 pies de alto.
- ✓ Instalación de un kit de protección para la infraestructura metálica: barra de conexión a tierra, aisladores y alfombra de aislamiento.
- ✓ Usar cableado par trenzado categoría 5e+ o 6.
- ✓ Todas las conexiones de red deberán conectarse a un panel de parcheo según sea el medio físico: par trenzado o fibra óptica.
- ✓ Al menos las conexiones de inalámbricos y/o backbones deberán contar con protector de líneas. Se recomienda la instalación de un panel de protección de líneas, el cual deberá estar aterrizado a tierra.
- ✓ Instalar protectores de línea para las conexiones de los enlaces alternos: DS0 e ISDN.

**R05: La Falta de Seguridad Lógica para el Servidor de Internet y de Aplicaciones del HGPIA-Loja.**

Los servidores debido a su importancia y para el correcto funcionamiento de las aplicaciones y servicios de internet de la institución, tienen que estar sometidos a

rigurosas medidas de seguridad lógica, con respecto a los otros equipos ya que suelen integrar información sensible.

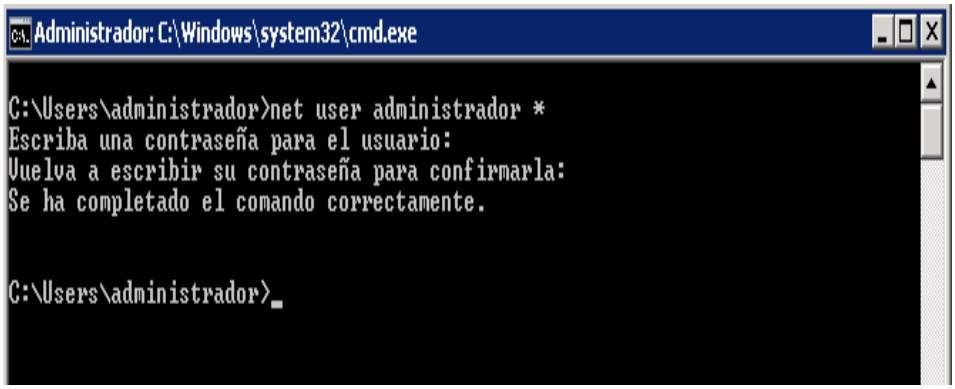
El acceso lógico a los servidores se lo hace remotamente, el administrador utiliza una cuenta de administrador para acceder a los servidores. Con la herramienta Active Directory el administrador asigna cuentas a los usuarios que necesitan acceder a alguna aplicación del servidor. Para ello el IAS (Internet Authentication Service) componente del sistema operativo Windows Server 2000 o NPS (Network Policy Server) para Windows Server 2008 comprueba el procedimiento de ingreso autentificando la contraseña, y autorizando el acceso del usuario. Ademas se encontró que en el Servidor de Aplicaciones IBM 5400 no se actualizan los parches, puesto que tienen instalado el Windows Server 2008 sin licencias, asì también en el Servidor de Aplicaciones HP Proliant DL360 G5 en el que se administra lo de central telefónica también hay inconvenientes para actualizar los parches ya que la licencia ha caducado. Para el servidor de Internet IBM no se ha realizado ninguna evaluación lógica porque el equipo se encontraba dañado.

**Recomendación:**

- ✓ Usar Contraseñas a nivel de BIOS para proteger el acceso a este elemento que registra la configuración de los servidores.
- ✓ Utilizar contraseñas de encendido de los servidores
- ✓ Utilizar herramientas que permitan reconocer las posibles vulnerabilidades a las que pueden estar expuestos los servidores; así como software de seguridad que incluya la identificación de usuario y contraseña de acceso a los recursos del servidor. A continuación se detallan algunas herramientas para evaluar vulnerabilidades y seguridades en los servidores Windows Server.
  - **Microsoft Baseline Security Analizer 2.2**
    Permite comprobar la evalución de vulnerabilidades.
  - **Herramienta de evalución de seguridad de Microsoft (MSAT)**
    Proporciona una evaluación de seguridad de alto nivel de la tecnología, procesos y usuarios que participan en la institución.

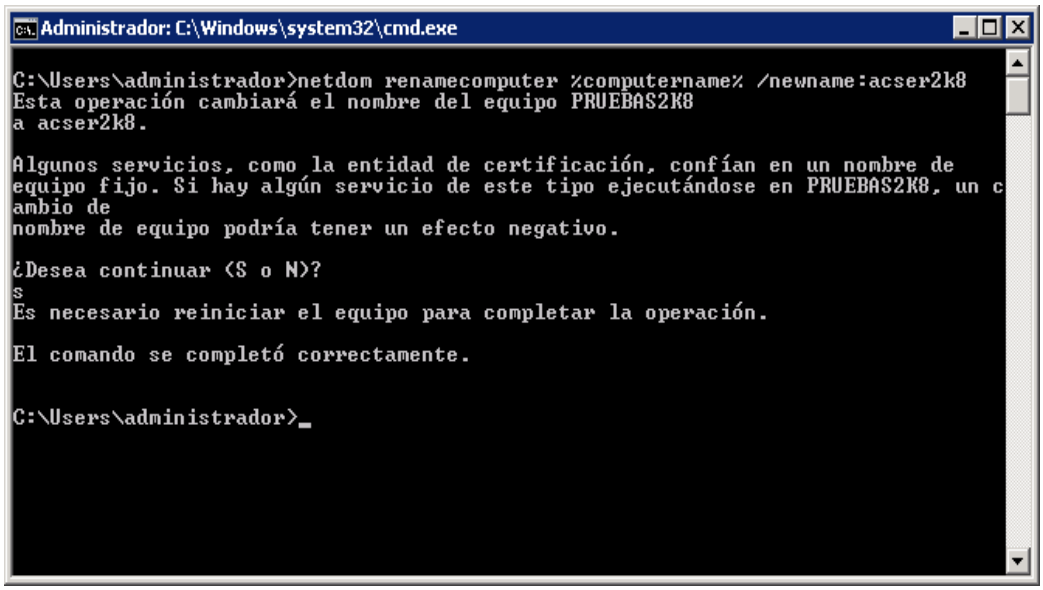
- ✓ Desactivar los servicios y las cuentas de usuario que no se vayan a utilizar. Desinstalación de las aplicaciones que no seán estrictamente necesarias.
- ✓ Documentar y mantener actualizada la relación de servicios y aplicaciones que se hayan instalado en cada servidor.
- ✓ Cambiar la configuración por defecto del fabricante seguidamente definiremos algunas de las más básicas :
    - Configurar la hora y la zona si por alguna razón no estamos de acuerdo con la configuración de la hora y la zona horaria del servidor podemos cambiarla y es importante revisarlo ya que los usuarios que se conecten tomaran estas características sobre todo la de la hora.

      Para cambiar esta opción tecleamos el comando *control timedate.cpl*
    - Cambiar el password del administrador ya que por defecto viene en blanco y esto representa un riesgo de seguridad, para ello ejecutamos el comando net user administrador *




    - Cambiar nombre de equipo que por defecto tiene un nombre del estilo WIN-L50E6NEWQSL. Algo inadmisible para cualquier dominio y esto lo hacemos con el comando:

      *netdom renamecomputer %computername% /newname:NOMBRENUEVO*




Una vez hecho el cambio tenemos que reiniciar el servidor con el comando *shutdown /r*

- ✓ Disponer de una copia de seguridad completa del Sistema Operativo de cada servidor y demás programas instalados en estos.
- ✓ Instalar software antivirus en los servidores de Internet y de Aplicaciones, y actualizarlo constantemente. Entre los antivirus que se encuentran en el mercado estan:

  - o **Kaspersky Anti-Virus para Winodws Server**

    Kaspersky Anti-Virus para Windows Server protége los datos de servidores que operan con el sistema operativo Windows contra todo tipo de programas maliciosos.

  - o **ESET NOD 32 Antivirus 4**

    ESET NOD 32 Antivirus 4 examina los canales de comunicación con codificación SSL como HTTPS y POP3S, y explora en forma inteligente los archivos comprimidos para detectar amenazas ocultas que otros productos pasan por alto.

  - o **Panda Security for Enterprise**

    Panda Security for Enterprise proteje contra antimalware, con conexión en tiempo real.

- ✓ Activar los registros de actividad de los servidores (logs) de aplicaciones Windows Server 2000 y Windows Server 2008.
- ✓ Ejecución de los servicios con los mínimos privilegios necesarios.
- ✓ Instalar las últimas actualizaciones (parches) de seguridad publicadas por el fabricante. Siempre y cuando se haya hecho pruebas de funcionamiento en máquinas de pruebas antes que en los equipos que están en producción.
    - o Microsoft define 13 parches de seguridades para servidores Windows que van desde el MS10-003 al MS10-015. Cinco de ellos están clasificados como críticos, siete como importantes y los restantes catalogados como moderados.
- ✓ Instalar una herramienta que permita comprobar la integridad de los archivos del sistema, como por ejemplo Tripwire. Es útil para monitorizar y alertar de cambios específicos de archivos en una gran variedad de sistemas.
- ✓ Modificar los mensajes de inicio de sesión para evitar que se pueda mostrar información sobre la configuración y recursos del sistema ante un posible atacante.
- ✓ Revisar el cumplimiento de otras recomendaciones de seguridad del mismo fabricante o de organismos como el SANS Institute o el NIST.

**R06: La Falta de Seguridad Lógica de las pc's y laptops del HGPIA-Loja**

En base a la información recolectada en el Hospital Isidro Ayora se pudo determinar que las pc's y laptops no cumplen con las respectivas seguridades lógicas, una gran cantidad de equipos no tienen restricciones de usuarios, no se usa claves de acceso, no existe la respectiva actualización y licencias del software instalado, no existe el respectivo control del departamento de Informática para evitar que los usuarios instalen software o programas en los equipos. La mayoría de los daños que pueden sufrir los quipos no será únicamente sobre la parte física sino contra la información almacenada y procesada. Como la información, es el activo más importante de la institución, para protegerla se debe aplicar seguridades lógicas en los equipos que la almacenan.

**Recomendación:** Para proteger las pc's y laptops de la institución a nivel lógico se debe:

- ✓ Establecer claves de acceso para el uso de las pc's o laptops
- ✓ Agregar contraseña del BIOS a todos los equipos para evitar que se manipulen las configuraciones.
- ✓ Instalar únicamente herramientas corporativas (Sistema de Control de Recursos Humanos, Sistema de Facturación, Sistema de Administración de Recursos Humanos. Sistema de Cámaras, Sistema de Control de Activos Fijos, Sistema de Administración y Control de Procesos de Estadística, quedando totalmente prohibido la instalación de otras aplicaciones de software por parte de sus usuarios en las pc's y laptops de la institución. En cualquier caso, el usuario del equipo deberá solicitar la aprobación al departamento de Gestión Informática antes de proceder a instalar algún nuevo programa o componente software. Como software corporativo se instalara el sistema operativo Windows para maquinas de escritorio y laptops; asi como también software antivirus.
- ✓ En cada pc y laptop usar un antivirus**,** actualizarlo o configurarlo para que automáticamente integre las nuevas actualizaciones del propio software de las definiciones o bases de datos de virus registrados.
- ✓ Si las pc's y laptop tienen niveles de permisos de uso de archivos y de recursos, hay que configurarlos de acuerdo a los requerimientos de la institución o usuario y no usar la configuración predeterminada que viene de fábrica, así como nombres y usuarios. Los intrusos, ladrones y hackers conocen muy bien las configuraciones predeterminadas y son las que usan al momento de realizar un ataque.
- ✓ En pc's y laptops que utilicen sistemas operativos de Microsoft, hay que realizar actualizaciones periódicamente, ya que constantemente los hacker y creadores de virus encuentran vulnerabilidades en dichos sistemas operativos.
- ✓ Utilizar programas que detecten y remuevan "spywares" (programas o aplicaciones que recopilan información sobre una persona u organización sin su conocimiento), existe diferente software que realiza esta tarea, algunos son gratuitos y trabajan muy bien. Para realizar el escaneo periódico de las pc's y portátiles se puede usar:

    - El Spyware Doctor ™ es un programa que detecta, elimina y bloquea toda clase de spyware.
    - El HiJackThis programa que ayuda a detectar y eliminar spyware en el sistema.

**R07: La Falta de Seguridad Lógica para los Elementos de Telecomunicaciones del HGPIA-Loja.**

**Recomendación:** Para proteger las telecomunicaciones a nivel lógico se debe:

- ✓ Establecer los respectivos controles de acceso entre redes y servidores.
- ✓ Uso de herramientas de protección de la información en el mismo medio en el que se genera o transmite.
- ✓ Protocolos de autenticación entre cliente y servidor.
  Los Tipos de Protocolos son:
  - TCP/IP para transmisión de datos.
  - HTTP acceder a paginas web.
  - HTTPS para la transferencia segura de datos.
  - FTP para transferencia de archivos
  - SMTP y POP para correo electrónico.
- ✓ Encriptación de datos en los diferentes enlaces que dispone el Hospital.

**R08: Falta de Controles de la Temperatura y Humedad del Entorno del Hardware del HGPIA-Loja**

En el centro de cómputo y oficinas donde existen equipos informáticos, el factor más crítico suele ser la temperatura del ambiente, la humedad es un factor secundario que lo tiene en cuenta en climas muy determinados en donde si la humedad podría afectar a los equipos.

**Recomendación:** Para prevenir una excesiva temperatura en el entorno del Hardware del Hospital Isidro Ayora lo primordial es**:**

- ✓ Tener una correcta ventilación, además se debería instalar aparatos de aire acondicionado para mantener la temperatura adecuada del ambiente donde se albergan gran cantidad de equipos informáticos. A mayor temperatura menor tiempo entre fallos para todos los dispositivos electrónicos, incluidos los

computadores, los dispositivos de red y cualquier sistema que genere por si mismo calor.

- ✓ Que los computadores tengan una ventilación interior suficiente, incluyendo ventiladores para los discos duros y una fuente de alimentación correctamente ventilada. También son convenientes las cajas que incorporan uno o varios ventiladores para refrigerar las maquinas.
- ✓ Tomar las medidas necesarias para tener la temperatura dentro de límites aceptables (21$^{o}$C a 23$^{o}$C) se disponga de un sistema de monitorización de la temperatura. Este sistema puede ser un simple termómetro electrónico en la sala de cómputo y oficinas que albergan gran cantidad de computadoras, o un sistema de adquisición de datos conectado a un termómetro que pueda enviar datos de la temperatura del ambiente a un computador a través del cual se permita realizar la monitorización.
- ✓ Configurar correctamente la BIOS de las computadoras para que monitoricen correctamente la temperatura interna y avisen si esta supera los límites marcados.

**Riesgo R09: La Falta de Actualización de los Antivirus de los Equipos Informáticos del HGPIA-Loja**

Los equipos informáticos del Hospital Isidro Ayora, no están protegidos adecuadamente ante virus informáticos (troyanos, gusanos, etcétera), en todos los equipos se ha procedido a instalar software antivirus no corporativo, simplemente se descarga una copia de Internet y se procede a instalarlo, hay que tomar en cuenta que esta acción no protege de manera eficiente la propagación de virus en los equipos.

Si algún virus se introduce en los equipos informáticos puede causar destrucción, que puede ser sencilla o hasta prácticamente imposible de reparar, esto depende de las acciones que realice el código.

**Recomendación:** Para poder combatir de manera eficaz la amenaza de los virus es importante:

- ✓ Tener instalado un programa antivirus en todas las pc's, laptops y servidores del Hospital Isidro Ayora. El antivirus deberá estar actualizado, para evitar la contaminación en los equipos. Es conveniente que el proveedor del programa antivirus sea una empresa que ofrezca un buen soporte técnico a sus clientes, con servicios de alerta y una respuesta urgente ante nuevos virus.
- ✓ Configurar los cortafuegos (firewall), para filtrar puertos que utilizan determinados troyanos y gusanos información (Ver Configuración del Firewall para equipos Windows en Anexo 6).
- ✓ Configurar robustamente cada equipo informático: desactivación de servicios innecesarios, cambios de contraseña por defecto del fabricante, etc.
- ✓ Comprobar los ficheros y correos electrónicos antes de abrirlos para ello podemos hacer uso de programas antivirus para eliminar virus de archivos infectados; asi como también el Microsoft Outlook Express para Windows XP que bloquea archivos adjuntos de correo que pueden ser no seguros.
- ✓ Bloquear los mensajes de correo que incluyan ficheros ejecutables o con determinadas extensiones sospechosas (como ".txt.vbs" o ".htm.exe"), ubicándolos en una carpeta que actué a modo de cuarentena, para que pueda ser revisada posteriormente por el responsable de la red.
- ✓ Comprobar disquetes y otros dispositivos de almacenamiento que entren y salgan de cada equipo.
- ✓ Evitar la descarga de programas de páginas web poco fiables.
- ✓ En el mercado existen soluciones de programas antivirus tales como:

  - **Norton Internet Security 2010 v17.0.0.136 + Trial Reset**

    Consta de antivirus, cortafuegos, protección web, medidor de rendimiento, control parental e incluso un escáner de red sencillo.

    **Compatibilidad:** Xp/Vista/Windows 7
    **Tamaño Archivo:** 108177 KB
    **Licencia:** 1 año

  - **Norton Antivirus 2010 v17.0.0.316 + Trial Reset**

Eficaz, rápido, ligero, la velocidad se aprecia desde la instalación, muy rápido. El consumo de memoria se ha reducido, una buena noticia para quienes usan equipos modestos. El motor heurístico SONAR detecta el malware desconocido con una eficacia sorprendente, mientras que el sistema de prevención de intrusiones evita la propagación de troyanos y spyware.

**Compatibilidad:** Xp/Vista/Windows 7

**Tamaño Archivo:** 80381 KB

**Licencia:** 1 año

- **Kaspersky Internet Security v9.0.0.459 + ResseterBox**

  Esta colección de utilidades dispone de un avanzado antivirus, un cortafuegos, un sistema de detección de software espía y malicioso, un sistema anti-spam y una herramienta de control parental; todas ellas listas para ser utilizadas con un solo clic.

  **Compatibilidad:** Xp/Vista

  **Tamaño Archivo:** 65852 KB

  **Testeado:** ACTIVACIONES +30 DIAS...

- **Kaspersky Anti-Virus 2010 v9.0.0.459**

  Es un antivirus que realiza una excelente combinación de protección reactiva y preventiva, protegiéndote eficazmente de virus, troyanos y todo tipo de programas malignos. Adicionalmente, dentro del grupo de programas malignos, Kaspersky también se encarga de proteger tu registro y todo tu sistema contra programas potencialmente peligrosos como los spyware. Kaspersky cuenta con una merecida fama de ser uno de los antivirus que posee un mejor análisis en 'busca y captura' de virus. Kaspersky realiza un análisis muy a fondo con lo que suele tardar bastante**.**

**Compatibilidad:** Xp/Vista
**Tamaño Archivo:** 59104 KB
**Testeado:** ACTIVACIONES +30 DIAS

- **Avast! Antivirus Professional Edition v4.8.1335 + Serial**

Presenta en su Edición Profesional todo un pack de soluciones destinadas a un objetivo común: darte la máxima protección contra los virus informáticos. Gracias a la gran capacidad de detección de Avast y a un elevado nivel de rendimiento, este antivirus es capaz de identificar virus y troyanos con eficacia, minimizando el número de falsas alarmas.

**Compatibilidad:** Xp/Vista
**Tamaño Archivo:** 36391 KB
**Testeado:** LICENCIA 25 ABRIL 2013

- **ESET Smart Security v4.0.437 + Seriales**

Es una herramienta para la protección integral del ordenador. Está preparada para repeler virus, spyware, spam, etc. El programa permite una defensa pasiva, es decir, el usuario no percibe la actividad del antivirus que únicamente queda visible en la barra de tareas.

**Compatibilidad:** 2000/Xp/Vista/Windows 7
**Tamaño Archivo:** 35037 KB / 38489 KB
**Testeado:** LICENCIAS WEB

- **Panda Internet Security 2009 + Serial**

Es una completa suite de seguridad que incluye protección antivirus, antiespía, protección de identidad, cortafuegos, filtro anti-spam y copias de seguridad.

**Compatibilidad:** 2000/Xp/Vista/Windows 7
**Tamaño Archivo:** 97374 KB
**Testeado:** LICENCIAS WEB

**Riegos R10: Ausencia de Seguros contra Robo para los Recursos de TI del HGPIA-Loja.**

**Recomendación:** Los Recursos de TI son la herramienta de trabajo del personal. En estos se encuentra la información de la institución, considerada hoy en día un activo más. Adquirir los recursos de TI a veces resulta hacer sacrificios muy grandes para la dirección, pero como son valiosísimas a la hora de agilizar las tareas, no importa cuánto cuesten. Como son recursos de un alto valor económico para la institución es indispensable darles su importancia. Para evitar que la pérdida de alguno de los recursos de TI, le cueste mucho más a la institución, se recomienda optar por seguros contra robo, estos ayudaran en gran parte a mitigar el costo del recurso robado.

**Riesgo R11: Ausencia de Controles en el Tratamiento o Destrucción del Hardware del HGPIA-Loja**

**Recomendación:** Para darle el tratamiento adecuado al Hardware es necesario que a nivel Directivo se establezcan los controles respectivos, a través de los cuales se podrá mantener un buen funcionamiento y mayor durabilidad de los equipos. En el caso que se produzca algún daño en los activos de la institución se deberá hacer conocer sobre la situación a quien corresponda, así como también se tendrá que determinar cuáles fueron las posibles causas. Se analizará las causas y de llegarse a determinar algún responsable, la Dirección deberá señalar alguna sanción para el(los) implicado(s).

**Riesgo R12: Alteración, Destrucción y/o Pérdida de Información relevante para el HGPIA-Loja.**

Es importante exponer que existe despreocupación por el adecuado almacenamiento de las copias de seguridad de información del Hospital Isidro Ayora. Estas se encuentran en un armario sin llave, expuestas a que fácilmente sean manipuladas por cualquier individuo

que accede al centro de cómputo. Además la mayoría de usuarios no tiene la cultura o conocimiento de guardar respaldos de los archivos que manejan.

Como la información relevante para la institución, son los archivos de los procesos que se manejan en cada departamento, estos archivos únicamente deben ser manipulados por el personal autorizado para garantizar su integridad. Se debe establecer seguridades con el fin de evitar que se produzca alteración, destrucción y/o pérdida de la información.

Con el fin de garantizar la seguridad de uno de los activos más importantes para la institución (información), se hace imprescindible salvaguardar su integridad y disponibilidad. Para garantizar estos dos aspectos fundamentales de la seguridad es necesario que existan unos procedimientos de realización de copias de seguridad y de recuperación, para que en el caso de falla del sistema informático, se pueda recuperar y reconstruir los datos y archivos dañados o eliminados.

**Recomendaciones:** Para proteger la información de alteración, destrucción y/o pérdida, se aconseja:

- ✓ Crear copias de respaldo (backup) de los archivos y de las bases de datos, en soportes informáticos (cintas, discos, cd's, dvd's, disquetes, pendrives) que permitan su recuperación.
- ✓ Establecer las políticas respectivas, para determinar cuántas copias se van a generar, dependiendo del tipo y volumen de la información (Ver Políticas en Anexo 7).
- ✓ Las copias de seguridad de los datos y archivos de los servidores, deberían ser realizadas y supervisadas por el personal debidamente autorizado.
- ✓ Establecer cómo se van a inventariar y etiquetar los soportes informáticos utilizados para las copias de seguridad de la información.
- ✓ Almacenar los soportes informáticos (cintas, discos, cd’s, dvd’s, disquetes, pendrives) que contienen el respaldo de la información, en lugares seguros, preferiblemente en cuartos diferentes de donde reside la información primaria.
- ✓ Implementar medidas de protección contra posibles robos, o daños provocados por incendios o inundaciones, siendo por ello muy aconsejable que estos soportes

informáticos se depositen, convenientemente etiquetados dentro de armarios ignífugos, acondicionados para protegerlos de altas temperaturas o radiaciones.

- ✓ Establecer cómo y cuándo se realizara la verificación del estado de los soportes informáticos.
- ✓ Establecer que sistemas o técnicas se van a utilizar (algoritmos criptográficos por ejemplo.)para garantizar la privacidad de los datos que se guardan en los soportes informáticos.
- ✓ Llevar un registro de incidencias, de la pérdida o destrucción, total o parcial de los datos de un archivo.

**Riesgo R13: Falta de inventario actualizado de las partes y/o piezas de los computadores del HGPIA-Loja**

Es algo paradójico pensar que en hospital Isidro Ayora no se lleva el control de las partes y piezas del computador, ya que actualmente el servicio que presta el centro de cómputo es el mantenimiento correctivo de los equipos, se debería pensar que el servicio en este aspecto es ineficiente, puesto que en primer lugar no existe un almacén de partes y piezas del computador, entonces como se da el mantenimiento correctivo si ni siquiera se dispone de las piezas a ser cambiadas, en segundo lugar como se determina que pieza fue cambiada o remplazada en el computador si no existe un registro o documento donde se formalice todo este proceso.

El no llevar un listado o inventario de las partes y/o piezas de los computadores puede ocasionar que estas se pierdan con facilidad, como son piezas pequeñas fácilmente pueden ser sustraídas, aunque no sea una pérdida económica significativa para la institución, no deja de ser una pérdida.

**Recomendación:** En razón de que el mantenimiento de los computadores, en el departamento de Informática de la institución se lo hace únicamente a nivel correctivo, se debería:

- ✓ Llevar un listado o inventario actualizado de las partes o piezas de los computadores, para que se pueda ofrecer un servicio eficiente. El inventario permitirá llevar un control continuo de las partes y/o piezas de los computadores.

- ✓ De las partes y/o piezas nuevas, tendrán que ser puestas en el inventario antes de que pasen a formar parte de algún computador.

**Riesgo R14: Falta de licencias para instalación y actualización del software del HGPIA-Loja.**

De los Programas de Ofimática (Word, Excel), Sistemas Operativos (Windows Server 2008, Windows XP), bases de datos (SQL Server 2005), instalados en los diferentes equipos informáticos del Hospital Isidro Ayora, se pudo determinar que no existen las respectivas licencias para su instalación y funcionamiento. Es importante que si la institución opta por instalar software pagado, este se los adquiera con sus respectivas licencias para evitar posibles demandas de parte de los propietarios del software, puesto que si esto llegará a suceder puede ocasionarles grandes pérdidas económicas a la institución y por ende al estado, ya que se trata de una institución de carácter público.

**Recomendación:** Las recomendaciones que se proponen a continuación se las hace en base a la implementación de software libre, para enmarcarse en el decreto 1014 de la República del Ecuador, en el que se establece que toda institución pública debe incorporar software libre para sus sistemas y equipamiento informático:

- ✓ Instalar software libre como el Sistema Operativos Ubuntu versión 10.4, para las pc´s y laptops de la institución. Es importante hacer conocer que este Sistema Operativo es de fácil manejo ya que su interfaz gráfica es muy parecida al Windows XP.
- ✓ Instalar el Sistema Operativo Fedora 12 o Centos para Servidores.
- ✓ Instalar para la Administración de Bases de Datos Mysq las versiones finales en el mercado para ello visitar la página oficial en **www.mysql.com/downloads/**

**Riesgo R15: La Falta de un Inventario Detallado y Actualizado de los Equipos Informáticos del HGPIA-Loja, por parte del subproceso Gestión Informática.**

A más de llevar el inventario de piezas y/o partes de los computadores, el Departamento de Gestión Informática del Hospital Isidro Ayora, está en la obligación de llevar el control

de la existencia de los computadores, basado en el Reglamento Interno para la Administración y Control de Activos Fijos del Ministerio de Salud Pública.

En base a la información solicitada al Administrador del centro de cómputo se encontró que si existe un inventario de los computadores, pero este no está levantado en su totalidad, tiene algunas fallas en su estructura como el caso de que no se registra los computadores con la serie de Activos fijos, sino que se ha procedido a listarlos con una serie distinta al que maneja el departamento de Activos Fijos, toda esta situación puede causar ambigüedad en el control y administración de los mismos.

**Recomendación:**

- ✓ Llevar un inventario detallado y actualizado de los equipos informáticos distribuidos en la sala de cómputo y oficinas de la institución. Esto como medida preventiva para reducir la probabilidad de pérdida.
- ✓ Registrar cada equipo con la serie de Activo Fijo establecido por el departamento de Activos Fijos, con el fin de corroborar con la información, que maneja el departamento.

**Riesgo R16: Uso de Material Inflamable en la construcción de la Sala de Servidores.**

En visitas periódicas realizadas al centro de cómputo se encontró que el material con el que estaba construida la sala de servidores es en un 50% de madera, hay que tener precauciones, este tipo de material no se debería utilizar de ninguna manera, ya que en el caso de que se produzca un incendio este se propagaría de forma rápida en la habitación, puesto que se trata de un elemento de fácil combustión.

**Recomendación:**

- ✓ Utilizar materiales resistentes al fuego (madera terciada resistente al fuego, vidrios anti explosión, pintura con retardo al fuego), para la construcción de la sala de servidores.

**Riesgo R17: Existencia de Material Inflamable en las Instalaciones de la Sala de Servidores del HGPIA-Loja.**

Durante nuestra revisión, hemos observado que: en la sala existe gran cantidad de cartón, plástico y papel, objetos que son proclives para generar combustión.

**Recomendación:**

- ✓ Evitar la acumulación de material inflamable dentro del lugar. En el caso de que hubiere procédase a retirarlo lo más pronto posible porque como es un material de fácil combustión se corre el riesgo de que se produzca un incendio en el lugar, suceso que por obvias razones puede conllevar a destruir o dañar los servidores, causando de esta manera una pérdida económica para la institución.

**Riesgo R18: Incendio en el Centro de Cómputo del HGPIA-Loja.**

Los incendios son riesgos que se pueden producir por cortocircuitos, o por cigarrillos mal apagados. De acuerdo a la gravedad pueden producir daños irreparables en los equipos informáticos, especialmente porque producen destrucción.

En un vistazo al centro de cómputo, en especial para determinar si existían los respectivos controles para contrarrestar un incendio, nos pudimos dar cuenta que el único control que existía era un extintor de incendios de gas PQS, el mismo que no estaba apto para su aplicación, puesto que había sobrepasado el límite de expiración (10/02/2007). Además este tipo de gas no es recomendado para salvaguardar el equipo informático albergado en el centro de cómputo, debido a que el polvo causaría obstrucciones en los equipos.

**Recomendación:** Para proteger los recursos de TI del Hospital Isidro Ayora, de este tipo de riesgo se debería:

- ✓ Implementar un Sistema de Detección de Humo e incendio distribuido por toda el área. Este sistema de detección debe activar una alarma, la que avisara al personal para efectuar el plan de contingencia ya establecido.
- ✓ Cambiar el extintor de gas PQS a un Extintor de **Gas Inergen (CO2).** Este debe estar en correcto funcionamiento y su componente químico debe estar dentro de los límites de la fecha de expiración.

**Riesgo R19: Inexistencia de la administración de cuentas de usuario de los computadores del HGPIA-Loja.**

En base a encuestas aplicadas al personal que maneja equipos informáticos, se encontró que el 66% tienen una cuenta de usuario, y el 34% no tienen una cuenta de usuario para acceder al equipo.

La incorrecta administración de las cuentas de usuario por parte del administrador no permitirá salvaguardar la seguridad de los equipos del centro de cómputo del HGPIA-Loja, esto conlleva a que la información no esté protegida de personas inescrupulosas que atenten contra la información.

La falta de políticas de creación, eliminación y manejo de las claves de usuario del personal de la institución permitirá que estas no sean seguras ya que no se encuentran encriptados y administradas correctamente por parte del administrador.

**Recomendación:**

- ✓ Definir políticas de gestión de cuentas de usuario tanto de login (nombres de usuario) como de password (contraseñas de usuario) para el acceso al equipo de cómputo de la institución. Que el login y el password sean intransferibles y sólo de uso personal (Ver Políticas en Anexo 8).

**Riesgo R20: No existe la respectiva administración de configuraciones del servidor de internet del HGPIA-Loja.**

**Recomendación:** La administración de configuraciones de internet estándar permite alcanzar un gran nivel de detalle sin necesidad de realizar un esfuerzo desmedido por lo que se han registrado las siguientes:

**Configuraciones de software**:

- ✓ Sistemas operativos.
- ✓ Direcciones IP
- ✓ Permisos de usuarios para el acceso del servicio de internet
- ✓ Restricción a páginas pornográficas
- ✓ Documentación asociada.

**Configuraciones de hardware**:

- ✓ Servidores y estaciones de trabajo.
- ✓ Subcomponentes con sus interrelaciones: relaciones padre-hijo, interdependencias,...
- ✓ Documentación y controladores asociados.

**Riesgo R21: No existe la respectiva administración de configuraciones del servidor de Aplicaciones del HGPIA-Loja.**

**Recomendación:** Se aconseja la correcta administración de los servidores de aplicaciones permitiendo así la:

- ✓ Integridad de datos y códigos: al estar centralizada en una o un pequeño número de máquinas servidoras, las actualizaciones están garantizadas para todos sus usuarios. No hay riesgos de versiones viejas.
- ✓ Configuración centralizada: los cambios en la configuración de la aplicación, como mover el servidor de base de datos o la configuración del sistema, pueden ser hechos centralmente.
- ✓ Seguridad: se consideran más seguras.
- ✓ Ejecucion: permite limitar el tráfico de la red solamente al tráfico de la capa de presentación, esto es percibido como un modelo cliente/servidor que mejora la ejecucion de grandes aplicaciones.

## De Proceso

**Riesgo R22: Inexistencia del plan informático y ejecución**

**Recomendación:** La unidad de TI debe elaborar e implementar un plan informático estratégico, el cual deberá estar alineado con el plan estratégico y el presupuesto de la organización. Para la elaboración de dicho plan se deben considerar, evaluar y priorizar los requerimientos de todas las áreas de la organización. La unidad de TI debe incluir en el plan informático, consideraciones respecto de la evolución de la infraestructura tecnológica, contemplando un esquema de actualización orientado a evaluar la conveniencia de incorporar nuevas tecnologías disponibles en el mercado y evitar la obsolescencia tecnológica. El plan informático debe ser aprobado por la dirección de la organización considerando, para cada uno de los proyectos involucrados, la razonabilidad de los plazos, beneficios a obtener y costos asociados. El plan informático debe mantenerse actualizado. La unidad de TI debe elaborar un presupuesto asociado a la ejecución del plan informático y el desarrollo de sus actividades, el cual debe ser evaluado y aprobado por la dirección, e incorporado al presupuesto anual de la organización. La dirección de la organización debe controlar en forma periódica, el grado de avance del plan informático, a efectos de detectar y evitar desvíos en los plazos, costos y metas previstas. Las adquisiciones de hardware, software u otros servicios informáticos, deben responder a los proyectos incluidos en el plan informático de la organización. Las situaciones de excepción deben ser autorizadas por la dirección de la organización y auditadas por la unidad de auditoría interna.

**Riesgo R23: Inexistencia del Plan de Mantenimiento Físico del Hardware**

No existe un plan definido para dar mantenimiento preventivo a las pc´s, laptops y servidores, únicamente se lo realiza cuando se presenta daño en los equipos.

La falta de mantenimiento físico preventivo en el hardware (pc´s, laptops y servidores), hace que estos sean más vulnerables a cualquier daño o falla, deteriorándose más rápido de lo normal. Además debido al mal estado de los equipos se puede perder información.

**Recomendación:**

- ✓ Establecer un Plan de Mantenimiento Físico Preventivo para las pc´s y laptops por lo menos 3 veces al año. Este plan debe incluir el responsable y el informe que se emita del mantenimiento.
- ✓ Establecer un Plan de Mantenimiento Físico Preventivo para los servidores, por lo menos 2 veces al año, se debe considerar también el mantenimiento correctivo. Este plan debe incluir el responsable y el informe que se emita del mantenimiento.

**Riesgo R24: Inexistencia del Plan de Mejoramiento de Procesos Automatizados**

**Recomendación:**

- ✓ Se aconseja elaborar un plan para mejorar y optimizar procesos institucionales con el apoyo de aplicaciones de software se analizará, evaluará y utilizará tecnologías informáticas innovadoras como: firma electrónica, factura electrónica, microchips, celulares, etc.

El mejoramiento de procesos también se dará mediante la:

- ✓ Adopción y uso de estándares abiertos y software libre
- ✓ Minimización de compra de licencias de software privativo
- ✓ Reutilización de software desarrollado
- ✓ Creación de sitios Web institucionales para automatización de procesos
- ✓ Reducción del uso de papel y administración “cero papeles”
- ✓ Uso de tecnología informática innovadora

**Riesgo R25: Inexistencia del Plan Administración de Redes de Conectividad y Central Telefónica.**

**Recomendación:** La administración de redes de conectividad entre redes mediante módem es de gran importancia debido al éxito y provecho que de ella se obtiene. Comprende, entre otras funciones, permitir el acceso a los recursos de la red para los usuarios y determinar cuál ha de ser el tipo de acceso de estos. Es la respuesta de cómo

elegir el funcionamiento de la red en cuanto al compartimiento ordenado de recursos. En las redes se forman cuentas para los usuarios en el acceso a los recursos. Para esto, los servidores en los nodos de la red deben mantener un nivel de seguridad. El sistema operativo de red ayuda a determinar el tipo de cuenta de cada usuario. Los usuarios pueden ser agrupados en categorías que determinan el tipo de acceso. Dentro de las cuentas existen algunas denominadas:

**Cuentas individuales**

Son para que cada persona acceda a la red y utilice los recursos compartidos o utilerías. En este tipo de cuentas se proporciona el nombre del servidor, el nombre del usuario (login) y el password o contraseña.

**Cuentas comodines**

Son para que varios usuarios pidan acceso a un servidor por medio de nombres de cuentas similares. Permiten instalar cuentas para grupos de personas o departamentos.

**Cuentas de grupo**

Son entre los diferentes sistemas operativos de red.

**Riesgo R26**: **Inexistencia del Plan Informático de Contingencia y Ejecución**

La inexistencia de un plan informático de contingencia y ejecución por parte del administrador, conlleva a que la continuidad del negocio y las operaciones del hospital no sean importantes.

**Recomendación:** Se aconseja elaborar el plan que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones del hospital. Un plan de contingencias es un caso particular de plan de continuidad de negocio aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista. No obstante, dada la importancia de las tecnologías en las organizaciones modernas, el plan de contingencias es el más relevante y se clasifica en:

**El plan de respaldo.** Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.

**El plan de emergencia**. Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es paliar los efectos adversos de la amenaza.

**El plan de recuperación**. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Por otra parte, el plan de contingencias no debe limitarse a estas medidas organizativas. También debe expresar claramente:

- ✓ Qué recursos materiales son necesarios.
- ✓ Qué personas están implicadas en el cumplimiento del plan.
- ✓ Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.
- ✓ Qué protocolos de actuación deben seguir y cómo son.

**Riesgo R27: Inexistencia del Plan de Obtención y Almacenamiento de los Respaldos de Información.**

La inexistencia de planes de obtención y almacenamiento de los respaldos de información por parte del administrador, conlleva a que no exista la seguridad apropiada de todos los mecanismos que se utilizan para almacenar y respaldar la información de todos los procesos que se realizan en la institución.

**Recomendación:** Se deberá establecer planes con los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o Aplicativos del Hospital. El almacenamiento de los Backups (respaldos) se los realizara en condiciones ambientales óptimas, dependiendo del medio magnético empleado. Para lo cual se debe contar con:

- ✓ **Backups del Sistema Operativo** (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).
- ✓ **Backups del Software Base** (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).
- ✓ **Backups del Software Aplicativo** (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.
- ✓ **Backups de los Datos** (Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).
- ✓ **Backups del sitio Web** (Aplicativo y Bases de Datos, Índices, ficheros de descarga, contraseñas).
- ✓ **Backups del Hardware**. Se puede implementar bajo dos modalidades:

**Modalidad Externa**. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

**Modalidad Interna**. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos. En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

**Riesgo R28: Inexistencia del Plan de Mantenimiento Físico de la Red del HGPIA-Loja**

La inexistencia del plan de mantenimiento físico de la red del HGPIA-Loja, conlleva a que no exista un cronograma establecido de trabajo por parte del administrador del centro de cómputo de la institución.

**Recomendación:** El personal responsable de la Administración de la Red deberá tener un Plan de Mantenimiento Físico de Red. En el que como mínimo deberá constar que se debe hacer el Mantenimiento de manera trimestral de los Switches y Ruteadores, esto se lo hará mediante el cronograma de trabajo determinado por el administrador.

**Riesgo R29: Inexistencia del Plan de Mantenimiento Lógico de la Red del HGPIA-Loja**

La inexistencia del plan de mantenimiento lógico de la red del HGPIA-Loja, conlleva a que no exista un cronograma para la asignación de direcciones, de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios de la institución, por parte del administrador del centro de cómputo.

**Recomendación:** El personal responsable de la Administración de la Red deberá tener un Plan de Mantenimiento Lógico de Red, en el que se administra las actividades de una red, que por lo general incluyen la asignación de direcciones, asignación de protocolos de ruteo y configuración de tablas de ruteo así como, configuración de autenticación y autorización de los servicios de la institución

**Riesgo R30: Inexistencia del Plan de Adquisición de Hardware y Software para Redes**

La inexistencia del plan de adquisición de hardware y software, conlleva a que no exista un documento estándar, y métricas de adquisiciones que se usarán para gestionar contratos y evaluar vendedores, por parte del administrador del centro de cómputo de la institución.

**Recomendación:** Definir políticas para la adquisición de hardware y software, definiendo responsables y niveles de autorización. El Plan de gestión de las adquisiciones, que puede incluir lo siguiente:

- ✓ Los tipos de contratos que serán usados
- ✓ Quién preparará las estimaciones independientes y si son necesarias como criterios de evaluación
- ✓ Las acciones que el equipo de dirección del proyecto puede llevar a cabo por sí mismo, si la organización ejecutante tiene un departamento de adquisiciones, contratación o compras
- ✓ Documentos de adquisición estandarizados, si fueran necesarios
- ✓ Gestión de múltiples proveedores
- ✓ Coordinación de las adquisiciones con otros aspectos del proyecto, como establecer el cronograma e informar el rendimiento
- ✓ Restricciones asunciones que podrían afectar a las compras y adquisiciones planificadas
- ✓ Manejo de los períodos de adelanto (“leads”) requeridos para comprar o adquirir artículos a los vendedores, y coordinación de los mismos con el desarrollo del cronograma del proyecto
- ✓ Manejo de las decisiones de fabricación propia o compra y vinculación de las mismas en los procesos de Estimación de Recursos de las Actividades y Desarrollo del Cronograma
- ✓ Determinación de las fechas planificadas en cada contrato para los productos entregables del contrato y coordinación con los procesos de Desarrollo y Control del Cronograma
- ✓ Identificación de garantías de cumplimiento o de contratos de seguros para mitigar algunas formas de riesgos del proyecto
- ✓ Determinación de las instrucciones que se proporcionarán a los vendedores para desarrollar y mantener una estructura de desglose de trabajo del contrato.
- ✓ Determinación de la forma y el formato que se usarán en el enunciado del trabajo del contrato
- ✓ Identificación de vendedores seleccionados precalificados, si los hubieran, que se utilizarán

- ✓ Métricas de adquisiciones que se usarán para gestionar contratos y evaluar vendedores.

Se deberá tener en cuenta:

- ✓ Enunciado del trabajo del contrato.
- ✓ Decisiones de fabricación propia o compra
- ✓ Documentos de la adquisición
- ✓ Criterios de Evaluación

Para la compra del hardware y software de la red se tomara en cuenta todos los ítems antes mencionados, también el software deberá ser licenciado para un perfecto funcionamiento de los procesos que se realizan.

**Riesgo R31: Inexistencia del Plan de Adquisición de Hardware para el HGPIA-Loja**

La inexistencia del plan de adquisición de hardware para el HGPIA-Loja, por parte del administrador conlleva a que no exista un documento estándar de características mínimas para la compra de cualquier componente o periférico para los equipos informáticos de la institución.

**Recomendación:** Definir políticas para la adquisición de hardware, estableciendo responsables y niveles de autorización. El plan deberá contener y establecer prioridades en su selección, deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad.

Para la adquisición de Hardware se observará lo siguiente:

a) El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la Institución.
b) Deberán tener un año de garantía como mínimo

c) Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.
d) La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local.
e) Tratándose de equipos microcomputadoras, a fin de mantener actualizado la arquitectura informática de la Institución, el Comité emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.
f) Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en el ciclo del proceso.
g) Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y de la Institución, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
h) Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
i) Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
j) Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.
k) En lo que se refiere a los computadores denominados servidores, equipo de comunicaciones como enrutadores y concentradores de medios, y otros que se justifiquen por ser de operación crítica y/o de alto costo; al vencer su período de garantía, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones.

En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones.

Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización del Comité.

En la adquisición del Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente.

**Riesgo R32: Inexistencia del Plan para la Contratación del Personal de Informática del HGPIA-Loja**

La inexistencia del plan para la contratación del personal de informática del HGPIA-Loja, por parte del administrador conlleva a que no exista un documento formal de todos los requerimientos, conocimientos y actitudes que debe cumplir.

**Recomendación:** El Plan para la Contratación de Personal del área Informática del HGPIA-Loja, se lo deberá desarrollar en base a lo siguiente:

- ✓ Determine el perfil que necesita, no es lo mismo un programador Junior. a un Sénior, y mucho menos uno con experiencia en Pascal y otro en C#
- ✓ No realice una entrevista personal hasta que se haya pasado por los siguientes filtros:
  - Analice con cuidado el currículo vitae del o los solicitantes
  - Realice entrevista telefónica en donde solicite detalles de los proyectos en los que el postulante haya colaborado
  - Valide las referencias laborales, preste especial atención en el tipo de compañía y actividades realizadas, contacte preferentemente al departamento de RH.
  - Realice un pequeño examen, ya sea de lectura de código, solución de problemas básicos o de lógica, cuestione en referencia a la implementación de algoritmos básicos así como metodologías de desarrollo empleadas, no solo es tirar código.
  - Antes de contratar, envié al prospecto a realizar psicométricos e incluya un estudio de personalidad, nunca se sabe que loco puede estar tocando a la puerta.

- Preste atención en el desempeño del candidato en proyecto en los que deba de trabajar en equipo e interactuar con sus compañeros, en muchas ocasiones, existen personas que solo tienen resultados exitosos cuando trabajan solas.
- En la contratación de personal con poca experiencia, busque características que pueda desarrollar dentro de su organización, La capacidad para aprender y emplear lo aprendido es fundamental en estos casos.
- Un título universitario no es garantía de capacidad o de conocimiento, simplemente, indica que se concluyó con un plan de estudios, no subestime la capacidad de las personas que no se han graduado, muchos lo los mejores Hacker no terminaron la Universidad.
- Si el puesto implica la codificación, prefiera personal relacionado a carreras tecnológicas y no administrativas, algunas carreras solo enseñan a utilizar paquetería.

**Riesgo R33: Inexistencia del Plan de Adquisición de Software para el HGPIA-Loja.**

La inexistencia del plan de adquisición de software para el HGPIA-Loja, por parte del administrador conlleva a que no exista un documento formal sobre el software adquirido a medida, y de las licencias y parches para la actualización de todo el software de la institución.

**Recomendación:** Definir Políticas para la Adquisición de Software licenciado para los Servidores y Software libre para las pc's y laptops de la institución, estableciendo responsables y niveles de autorización. Los planes deberán contener y establecer prioridades en su selección, para la adquisición de Software base y utilitarios, el comité dará a conocer periódicamente las tendencias con tecnología de punta vigente, siendo la lista de productos autorizados la siguiente:

a) Plataformas de Sistemas Operativos licenciados y libres
b) Bases de Datos
c) Manejadores de bases de datos

d) Lenguajes de programación

Los lenguajes de programación que se utilicen deben ser compatibles con las plataformas enlistadas.

e) Hojas de cálculo:
f) Procesadores de palabras:
g) Diseño Gráfico:
h) Programas antivirus.
i) Correo electrónico
j) Browser de Internet

En la generalidad de los casos, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante el Comité. Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectiva.

**Riesgo R34: Inexistencia del Plan de Adquisición de Elementos de Telecomunicaciones para el HGPIA-Loja.**

La inexistencia del plan de adquisición de elementos de telecomunicaciones para el HGPIA-Loja, conlleva a que no exista un documento estándar formal para la compra de los mismos por parte del administrador del centro de cómputo de la institución.

**Recomendación:** Definir políticas para la adquisición de elementos de telecomunicaciones, estableciendo responsables y niveles de autorización:
Los siguientes son algunos de los puntos que deberían considerarse en lo relacionado con políticas de adquisición.

- La determinación de las necesidades debe ser un proceso participativo, así como los ajustes previos y posteriores a la elaboración del Plan de Adquisición de elementos de telecomunicaciones, con el fin de propender por el buen uso de los recursos.

- Una de las tareas primordiales en la toma de decisiones de elementos a comprar, debe ser la de normalizar, estandarizar, regularizar y disminuir la variedad de referencias de un mismo elemento o elementos con usos y fines similares.
- Algunos de los principales criterios a considerar en la selección de oferentes, son los referentes a los antecedentes de seriedad y calidad de los bienes y/o servicios ofrecidos, como también el servicio post-venta (tecnología, repuestos, mantenimiento, etc.).
- En la elaboración del Plan de Adquisición de elementos de telecomunicaciones es preciso considerar los objetivos y estrategias de algunos de los proyectos de inversión, especialmente los destinados a edificios (infraestructura física), sistemas, software, hardware y elementos para las telecomunicaciones.
- El Plan de Adquisición es uno de los instrumentos esenciales para fortalecer el proceso de descentralización administrativa y financiera.

También se deberá considerar principalmente el cableado estructurado de todos los puntos de red y los puntos de voz de la institución.

**Riesgo R35: Inexistencia del Plan de Continuidad del Negocio del HGPIA-Loja:**

La inexistencia de ninguno de estos planes para la continuidad del negocio del HGPIA-Loja, conlleva a que si ocurre cualquier percance pase desapercibido, esto permitirá que la continuidad de los servicios, procesos y operaciones no se realicen.

- ✓ **Falta de un plan de Recuperación**
- ✓ **Falta de un plan de Reanudación**
- ✓ **Falta de un plan de Contingencia:**
  - ✓ **Robo**
  - ✓ **Incendio**
  - ✓ **Vandalismo**
  - ✓ **Perdida de Energía**
  - ✓ **Humedad**

**Recomendación:** Se aconseja mantener la continuidad de los servicios/procesos críticos del hospital tienen beneficios que redundan en la estabilidad de los servicios hacia los usuarios y empleados de la misma. De la misma manera permite que el percance "pase desapercibido" al exterior del hospital, y garantiza la continuidad en la operación. Para llevar a cabo la elaboración del plan de continuidad, se desarrolla una metodología cuyas etapas son:

- ✓ Identificación y prioridad de los procesos y recursos vitales. Situación Actual
- ✓ Análisis de Riesgo e Impacto, Recomendaciones de Protección
- ✓ Estrategias y alternativas de recuperación
- ✓ Equipo humano de recuperación, funciones y acciones de recuperación
- ✓ Guías y ejecución de una prueba
- ✓ Elaboración del manual de Contingencia
- ✓ Presentación Ejecutiva.

Resaltamos como parte integral del servicio, la realización de una prueba del plan, de tal manera que garantice que cuando se requiera su ejecución durante una calamidad, realmente funcione. Estos planes son una herramienta de estabilidad y continuidad que aporta prestigio a las empresas que los implantan.

## De Personal

**Riesgo R36: La falta de entrenamiento y capacitación al personal del centro de cómputo en estándares y tecnología de vanguardia.**

La falta de entrenamiento y capacitación al personal del centro de cómputo por parte de las autoridades del hospital, conlleva a que no tengan capacidad para dar respuestas a necesidades de la realidad y la posibilidad de aplicarlas a la vida cotidiana de los recursos de TI.

**Recomendación:** Para proteger del uso mal intencionado o del mal uso por falta de conocimiento es necesario instruir al personal y en general a los usuarios del centro

informático que son ellos quienes utilizan dicho centro. Es importante tener en cuenta lo siguiente:

- ✓ Implementar un reglamento interno que defina el uso adecuado del centro informático.
- ✓ No se debe permitir sin autorización el uso de equipos de fotografía, vídeo o audio u otros equipos de grabación.
- ✓ Instruir al usuario del área de servicios informáticos en particular y al resto de la organización en general, sobre medidas de seguridad física, planes de recuperación y de contingencias.
- ✓ Incentivar al personal para cumplir las normas de seguridad.
- ✓ Evaluar las políticas de entrenamiento de usuarios, para asegurar que alcanzan el nivel de conocimiento sobre seguridad para el caso de accidentes.
- ✓ Efectuar reuniones periódicas relativas a la seguridad para mantener un nivel adecuado de interés, responsabilidad y cumplimiento.
- ✓ Penalizar a los responsables por las violaciones a las normas vigentes relacionadas a la seguridad.

La capacitación del personal en el área de informática debe basarse en las siguientes condiciones:

- ✓ Las necesidades de las Personas.
- ✓ El crecimiento individual
- ✓ La capacidad para dar respuestas a necesidades de la realidad y la posibilidad de aplicarlas a la vida cotidiana.
- ✓ Los conocimientos y experiencias de los participantes, revalorizando y reforzando el aprendizaje existente e incorporando nuevos conocimientos.
- ✓ El aprendizaje en equipo que permite mayor posibilidad de interacción e intercambio.

**Riesgo R37: La falta de asignación de funciones formalizadas al personal del subproceso Gestión Informática.**

La falta de asignaciones y funciones definidas claramente al personal técnico que labora en el centro de cómputo, conlleva a que no se cumplan con las actividades y procesos eficientemente.

Se formalizaran las asignaciones y funciones mediante un documento por escrito en la que conste las actividades que tendrá a su cargo cada uno de sus integrantes.

**Recomendación:**

- ✓ Definir claramente las funciones que deberá cumplir cada uno de los integrantes del Centro de Cómputo.
- ✓ Se formalizaran las funciones mediante un documento por escrito en la que conste las actividades que tendrá a su cargo.

**Riesgo R38: Desconocimiento de que hacer para salvaguardar el hardware en el caso de incendios.**

Mediante entrevistas realizadas a los líderes o coordinadores de la institución, se pudo determinar que se desconoce lo qué se debería hacer para salvaguardar el hardware de la institución en el caso de que se produjera un incendio.

**Recomendación:**

Para salvaguardar el hardware de la institución en caso de desastres se deberá elaborar un plan de emergencia, de evacuación que debidamente tendrá que ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá. :

- ✓ Ante todo, conservar la serenidad.

- ✓ Asegurarse de que todos los miembros sean notificados.
- ✓ Informar al director de informática.
- ✓ Cuantificar el daño o pérdida del equipo.
- ✓ Notificar a los proveedores del equipo cual fue el daño.
- ✓ El personal deberá ser capacitado por el departamento local de bomberos contra desastres.
- ✓ Se deberá tener señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. normales.
- ✓ Ubicación y señalización de los elementos contra el siniestro
- ✓ Se deberá establecer la formación de equipos, cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.
- ✓ Establecer un programa de entrenamiento de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.
- ✓ Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.
- ✓ En ese momento cualquiera que sea(n) el (los) proceso(s) que se esté(n) ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador", seguidamente digitar Down en el (los) servidor(es).
- ✓ Se apagará (poner en OFF) la caja principal de corriente del departamento de sistemas
- ✓ Tomando en cuenta que se trata de un incendio de mediana o mayor magnitud, se debe tratar en lo posible de trasladar el servidor fuera del local, se abandonará el edificio en forma ordenada, lo más rápido posible, por las salidas destinadas para ello.

- ✓ Se deberá realizar simulacros con todo el personal que esté involucrado con el área informática.
- ✓ Si existen sistemas automatizados para los desastres el personal no deberá interferir con los procesos que se realicen.
- ✓ Tener siempre actualizada una relación de Pc's requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los Servicios Informáticos de la Institución).

## 4.4 Obtener resultados parciales

Consiste en emitir un pre-informe de los resultados cuyo objetivo es hacer que el administrador forme parte del trabajo realizado para que pueda estudiar las conclusiones emitidas por los auditores.

El pre-informe es una matriz que contiene la lista de todos los riesgos encontrados (VER MATRIZ DE RESULTADOS). Cada Riesgo está identificado como hallazgo y contiene las debidas recomendaciones.

## 4.5 Reunión con los administradores auditados

Es la forma de poder transmitir a los auditados nuestro trabajo, de manera que el documento del pre-informe pueda ser leído y entendido, sin que se preste a dudas con respecto al mensaje que contiene. Se debe discutir con los auditados para llegar a un acuerdo entre las partes intervinientes y luego proceder a la elaboración del informe final de auditoría.

Una vez que los auditados han llegado a la aceptación del pre-informe se procede a la elaboración del informe final de auditoría, del que se hará llegar una copia para el director del hospital, para el administrador del hospital y para el administrador del centro de cómputo. Finalmente los auditados deberán entregar un documento de su aprobación.

# FASE 5:

## COMUNICACIÓN DE RESULTADOS

## CONTENIDOS

# 5 COMUNICACIÓN DE RESULTADOS

## 5.1 Informe de Auditoría Informática

### *5.1.1 Alcance*

La presente **AUDITORÍA DE PRODUCTIVIDAD DEL HARDWARE, SOFTWARE Y TELECOMUNICACIONES TOMANDO COMO REFERENCIA EL MARCO DE TRABAJO DE COBIT 4.0",** se encargará de analizar y evaluar la gestión del hardware, software y elementos de telecomunicaciones existentes en el Hospital Isidro Ayora, para determinar si se cumple con los controles de seguridad y las características de los equipos van acorde con los procesos que se les ha asignado.

### 5.1.2 Objetivos

#### *5.1.2.1 General*

- ✓ Auditar la Productividad del Hardware, Software y Telecomunicaciones tomando como referencia el marco de trabajo de Cobit 4.0.

#### *5.1.2.2 Específicos*

- ✓ Determinar la situación actual del área Informática del Hospital Isidro Ayora.
- ✓ Definir procesos críticos a evaluar mediante la aplicación de matrices de riesgo de la seguridad y productividad.
- ✓ Ejecutar la Auditoría Informática aplicando los 3 dominios de COBIT 4.0, tomando de ellos los procesos genéricos que están enfocados a la productividad del hardware y software.
- ✓ Elaborar matrices de recomendación para incrementar la productividad del hardware, software y telecomunicaciones.

### 5.1.3 Tiempo empleado

- Viernes 11 de Septiembre del 2009 al viernes 30 de Abril del 2010, 154 días laborados.

### 5.1.4 Destinatarios

- Dr. Daniel Astudillo, **DIRECTOR DEL HOSPITAL PROVINCIAL GENERAL ISIDRO AYORA-LOJA.**
- Ing. Ángel Cárdenas, **ADMINISTRADOR DEL HOSPITAL PROVINCIAL GENERAL ISIDRO AYORA-LOJA.**
- Ing. Mario Cueva, **ADMINISTRADOR DEL CENTRO DE CÓMPUTO.**
- Dr. Hernán Ruiz, **AUDITOR DE LA CONTRALORÍA GENERAL DEL ESTADO REGIONAL- LOJA.**

### 5.1.5 Auditores

- Patricia Soledad Sigüenza Granda
- Ángel Manuel Naula Maita

### 5.1.6 Fecha de Entrega

- Lunes 16 de Agosto del 2010

### 5.1.7 Resultados

A continuación se detalla los resultados de la evaluación de cada uno de los procesos definidos para la presente auditoría informática, organizados en los 3 dominios de COBIT 4.0, (Planear y Organizar, Adquirir e Implementar, Entregar y dar Soporte), basados en el modelo de madurez que manejan una escala de medición creciente a partir de 0 (no existente) hasta el 5 (Optimizado)

**DOMINIO PLANEAR Y ORGANIZAR**

**PO1. DEFINIR UN PLAN ESTRATÉGICO (Nivel de madurez 1)**

**CONCLUSIÓN**.-Este proceso se encuentra en el nivel de madurez 1 puesto que no se cuenta con un plan estratégico definido para el HPGIA-Loja.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel (nivel 2)
- Administrar el valor de TI, significa garantizar el portafolio de inversiones de TI del HPGIA.
- Alinear las TI con el negocio, significa educar a los líderes o coordinadores departamentales sobre las capacidades tecnológicas actuales y el futuro de estas, así como las oportunidades que ofrece TI en el desempeño de actividades del HPGIA
- Evaluar el desempeño actual de los planes existentes y de los sistemas de información y su contribución con los objetivos del HPGIA.
- Crear un plan estratégico de TI para definir una cooperación de las TI con los objetivos estratégicos del HPGIA, así como los costos y riesgos relacionados.
- Crear planes tácticos de TI, que resulten del plan estratégico de TI, estos servirán para describir las iniciativas y los requerimientos de recursos requeridos por TI, estos deben ser bien detallados para lograr la definición de planes proyectados.
- Administrar el portafolio de TI, significa administrar efectivamente el portafolio de inversiones de TI requerido para lograr la consecución de objetivos estratégicos y específicos del HPGIA.

**PO2. DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que no existe definido un proceso para arquitectura de la información.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2)
- Establecer y mantener un modelo de información para facilitar el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, el modelo facilita la creación, uso y compartición óptimas de la información.
- Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos del HPGIA.
- Establecer un diseño de clasificación datos que aplique a todo el HPGIA, basado en que tan crítica y sensible es la información.

- Definir e implantar procedimientos para garantizar integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

**PO3. EVALUAR Y ADMINISTRAR RIESGOS DE TI (Nivel de madurez 0)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 0 puesto que no existe una evaluación y administración de riesgos de los procesos de TI.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 1)
- Evaluar y administrar los riesgos encontrados periódicamente.
- Identificar los dueños de los riesgos, así como los dueños de los procesos en caso de que estos sucedieran para elaborar y mantener respuestas a los riesgos, con el fin de generar controles y seguridades que ayuden a mitigarlos.

**ADQUIRIR E IMPLANTAR**

**AI1. IDENTIFICAR SOLUCIONES AUTOMATIZADAS (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que no existe un análisis formal de cómo implementar procesos automatizados.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2).
- Identificar, priorizar, especificar y acordar los requerimientos de negocios funcionales y técnicos que cubran todas las iniciativas requeridas para lograr los resultados deseados.
- Identificar, documentar y analizar los riesgos asociados con los procesos del HPGIA para el desarrollo de los requerimientos.
- Desarrollar un estudio de factibilidad que examine si es posible implantar los requerimientos.

- El patrocinador del negocio se encarga de aprobar y autorizar los requisitos del negocio tanto funcionales como técnicos y los reportes de estudio de factibilidad en las etapas clave.

**AI2. ADQUIRIR Y MANTENER EL SOFTWARE APLICATIVO (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones, pero aún no hay una definición formal para este proceso.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2)
- Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para el desarrollo de software.
- Garantizar la integridad de la información, el control de acceso, los respaldos y el diseño de pistas de auditoría
- Elaborar un diseño detallado y los requerimientos técnicos del software.
- Asegurar que el diseño del software sea de calidad.
- Desarrollar estrategias y planes de mantenimiento del software aplicativo en el HPGIA.

**AI3. ADQUIRIR Y MANTENER LA INFRAESTRUCTURA TECNOLÓGICA (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que no existe un plan para adquirir y mantener tecnología. Por tanto no se puede controlar los procesos para adquirir, implantar y actualizar infraestructura tecnológica.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2)
- Elaborar un plan para adquirir, implantar y mantener la infraestructura tecnológica.

- Proteger la infraestructura tecnológica mediante medidas de control interno, seguridad y auditabilidad durante la configuración, integración, y mantenimiento de hardware y software de la infraestructura para garantizar su integridad y disponibilidad
- Elaborar un plan de mantenimiento de la infraestructura tecnológica y garantizar el control de cambios.

**A14. FACILITAR LA OPERACIÓN Y EL USO (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que no existen los respectivos manuales y políticas definidos para que ayuden en la operación y uso de las TI.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2)
- Elaborar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación, y los niveles de servicio requeridos.
- Pasar el conocimiento a la gerencia para permitirles que tomen posesión del sistema y los datos.
- Pasar el conocimiento a los usuarios finales, para que usen con eficiencia y efectividad el sistema.
- Pasar el conocimiento al personal de soporte técnico, para que este a su vez apoye y mantenga la aplicación.

**AI5. ADQUIRIR RECURSOS DE TI (Nivel de madurez 4)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 4 puesto que la adquisición de recursos de TI se la hace en base compras públicas, este proceso se integra totalmente con el sistema general de adquisición de recursos.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 5)

- Elaborar y seguir un conjunto de procedimientos y estándares definidos en el proceso general de adquisición del HPGIA.
- Tomar medidas en la administración de contratos y adquisiciones.
- Seleccionar proveedores mediante una práctica justa y formal.
- Garantizar que el software adquirido cumpla con los acuerdos pactados de adquisición.

**ENTREGAR Y DAR SOPORTE**

**DS1 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que no se administra niveles de servicio, no hay rendición de cuentas.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2).
- Definir un marco de trabajo que brinde un proceso formal de administración.
- Mantener alineados los requerimientos y prácticas del negocio.
- Realizar acuerdo de niveles de servicios para todos los procesos críticos de TI.

**DS3 ADMINISTRAR DESEMPEÑO Y CAPACIDAD (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que la mayoría de veces son los usuarios los que tienen que ver como solucionan el problema encontrado. No hay un proceso definido.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2)
- Tener en cuenta un proceso de planeación para evaluar el desempeño y la capacidad de los recursos de TI.
- Establecer métricas de desempeño y evaluación de la capacidad.
- Realizar un monitoreo continuo del desempeño y la capacidad de los recursos de TI.

**DS11 ADMINISTRAR LOS DATOS (Nivel de madurez 1)**

**CONCLUSIÓN.-** Este proceso se encuentra en el nivel de madurez 1 puesto que no existe definido un proceso para almacenar, recuperar y respaldar los datos.

**RECOMENDACIONES COBIT**

- La recomendación principal es ascender al siguiente nivel de madurez (nivel 2)
- Acordar con los usuarios la forma de almacenar y recuperar los datos.
- Mantener un inventario de todas las copias de los datos.
- Prevenir el acceso de personas no autorizadas a los datos sensibles.
- Realizar la eliminación de datos a través de herramientas especializadas para evitar la recuperación por parte de personas inescrupulosas.
- Implementar procesos de respaldos y restauración de sistemas, datos y configuraciones.
- Establecer mecanismos de entrega, recepción, procesamiento y almacenamiento físico de la información.
- Definir responsables en la propiedad de los datos
- Establecer políticas de administración de datos.

# ESQUEMA DE METODOLOGÍA PARA EL DESARROLLO DEL SOFTWARE

Metodología XP para el desarrollo del Sistema Web para el control de los recursos de Tecnología de la Información para el Hospital Provincial General Isidro Ayora de la ciudad de Loja.

1. Antecedentes del Proyecto
2. Planificación
3. Diseño
4. Desarrollo
5. Pruebas

# ANTECEDENTES DEL PROYECTO

# ANTECEDENTES DEL PROYECTO

En los Antecedentes del Proyecto, se considera información de la institución para la cual será desarrollada la aplicación en este caso el HGPIA-Loja, se toma aspectos importantes de la institución como historia, misión, visión, entre otros; así también se detalla sobre la metodología de desarrollo de software a utilizar.

| FICHA TÉCNICA | |
|---|---|
| CONTENIDO | Introducción<br>Objetivos<br>Alcance<br>Marco Teórico<br>Descripción de HGPIA-Loja<br>Historia<br>Datos Generales<br>Direccionamiento Estratégico<br>• Misión<br>• Visión<br>Estructura Organizacional<br>Metodología de Desarrollo de Software<br>Metodología XP<br>¿Qué es Xtreme Programming (XP)?<br>Introducción a la Metodología XP |
| **GRÁFICOS** | • Gráfico1. Estructura Organizacional del HPGIA |
| **PROBLEMAS Y SOLUCIONES ENCONTRADAS** | |
| **Problemas:** Falta de profesionales que puedan ar asesoría en la instalación y configuración de herramientas de código libre. | **Soluciones:** Continua investigación por parte de los desarrolladores y a nivel universitario se debería difundir el estudio de herramientas de código libre. |

# INTRODUCCIÓN

La informática es una de las ciencias que está en nuestras vidas, las sociedades se desarrollan al amparo de las nuevas tecnologías y su éxito se debe en gran parte a esta ciencia. Gracias a la informática se puede administrar fácilmente la información que se genera de las actividades diarias que realizan las instituciones, puesto que esta ciencia es la que se encarga del tratamiento automático de la información. Este tratamiento automático es el que ha propiciado y facilitado la manipulación de grandes volúmenes de datos y la ejecución rápida de cálculos complejos.

Con la informática la mayoría de los procesos que se llevan de forma manual en la institución se pueden automatizar y de esta manera se puede dar un aporte significativo para agilizar los procesos que se llevan en la administración de los recursos de TI del Hospital Isidro Ayora.

El proceso de administración de los recursos de TI del Hospital Isidro Ayora se lleva de forma manual, no existe ningún procedimiento automatizado que permita llevar un mejor control y registro de las pc's, laptops, servidores, impresoras, ruteadores, teléfonos, etc. por parte del departamento de Gestión Informática. Es así como nace la idea por parte de los postulantes para desarrollar e implementar un Sistema Web para el Control de los Recursos de Tecnología de la Información, el mismo que servirá para llevar el registro y control del hardware, software y elementos de telecomunicaciones que tiene la institución. Además permitirá controlar el mantenimiento del hardware y elementos de telecomunicaciones. El sistema web también constara de un módulo de respaldos de base de datos a través del cual el administrador creará respaldos de las bases de datos. Otra característica importante de nuestro sistema es que permitirá generar reportes generales de información para el usuario, los mismos que facilitarán y ayudarán en la toma de decisiones a los directivos institucionales en lo referente al hardware, software y elementos de telecomunicaciones que poseen.

El apoyo que brinda la informática para el desarrollo de las instituciones que la integran es muy significativo, puesto que colabora en la consecución de los objetivos de forma óptima y eficiente.

# Objetivos

## Objetivo General

- Desarrollo de un Sistema Web para el Control de los Recursos de Tecnología de la Información, para el Hospital General Provincial Isidro Ayora de la ciudad de Loja.

## Objetivos Específicos

- Informar en la Web sobre datos generales del Hospital Provincial Isidro Ayora.
- Administrar de manera automatizada la información referente a los recursos de TI.
- Mantener el inventario de los recursos de TI actualizado.
- Determinar cuándo un recurso de TI ha sido movido de su ubicación.
- Determinar al responsable o custodio de los recursos de TI.
- Llevar un control detallado de los recursos de TI.
- Llevar el registro del mantenimiento de los recursos de TI.
- Imprimir reportes generales del Inventario, Equipos, Hoja de Trabajo, Movimiento Interno, Salida de Equipo, Custodio y Características Básicas de Compras.

## Alcance

El Sistema Web para el Control de los Recursos de Tecnología de la Información para el Hospital General Provincial Isidro Ayora, estará conformado de los módulos que se especifican a continuación:

**SYSCORTI. Portal WEB**

En este módulo se dará a conocer información general del Hospital Isidro Ayora, a través de la publicación web como: Historia, Misión y Visión, Servicio que Ofrece, Programas, Ley de Transparencia, Contactos y un link para acceder a la aplicación SYSCORTI.

**MÓDULO DE ACCESO AL SISTEMA**

Este módulo sirve para ingresar datos de acceso al software por parte del usuario. Se validará las entradas del usuario para determinar si este usuario tiene el permiso autorizado para acceder al sistema.

**MÓDULO ADMINISTRATIVO**

En este módulo se administra la información referente a proveedores, administrativos, departamentos, contacto, custodios, usuarios del sistema; el acceso a este módulo sólo le corresponde al usuario administrador, quien puede agregar y modificar datos de las tablas mencionadas.

**MÓDULO INVENTARIO**

Este módulo sirve para administrar el hardware, software y elementos de telecomunicaciones que existen en la institución. En el Inventario se podrá Agregar, Modificar y Buscar datos, también permitirá generar reportes del hardware, software y elementos de telecomunicaciones de los que dispone la institución.

- **Hardware**

Se llevara un control detallado de todo el hardware existente en la institución.

- ✓ Equipos
- ✓ Servidores
- ✓ Cases
- ✓ Monitores
- ✓ Discos duros
- ✓ Scanner
- ✓ Mainboards
- ✓ Procesadores
- ✓ Tarjetas audio y video fax modem, de red, etc.
- ✓ Memorias RAM
- ✓ Fuentes de poder
- ✓ Teclados
- ✓ Mouse
- ✓ Impresoras
- ✓ Parlantes
- ✓ Audífonos
- ✓ Micrófonos
- ✓ Unidades de cd-r, cd-rw, dvd-r, cd-rw
- ✓ Unidades lectoras de memorias
- ✓ Unidades de diskette
- ✓ UPS
- ✓ Kit (Juego) de Herramientas.

- **Software**

Se llevará un control detallado de todo el software existente en la institución.

- ✓ Sistemas Operativos (Windows, Linux, otros )

- ✓ Licencias de sistemas operativos, de paquetes de ofimática, de sistemas de transacciones, etc.
- ✓ Claves de las licencias de los sistemas operativos, paquetes de ofimática, sistemas de transacciones, etc.
- ✓ Claves de acceso en Windows u otro sistema operativo como usuario administrador o invitado
- ✓ Programas de escritorio
- ✓ Aplicaciones desarrolladas para la institución
- ✓ Antivirus para la protección de la información.

- **Telecomunicaciones**

Se llevara un control detallado de las telecomunicaciones existente en la institución.

- ✓ Switchs
- ✓ Hubs
- ✓ Conmutadores
- ✓ Enrutadores
- ✓ Cableado telefónico
- ✓ Equipos terminales(teléfono)
- ✓ Cableado para red interna.
- ✓ Ponchadoras
- ✓ Conectores
- ✓ Puntos de red
- ✓ Canaletas
- ✓ Cabinas metálicas y vidrio para locutorios
- ✓ Materiales adicionales para central telefónica y para la red

**MÓDULO MANTENIMIENTO**

En el módulo de mantenimiento el administrador o usuario invitado llevará el registro de mantenimiento de hardware y elementos de telecomunicaciones, el administrador o

usuario invitado ingresará los datos en una ficha técnica de mantenimiento (hoja de trabajo), que a futuro será utilizada en el módulo de reportes.

Para el mantenimiento correctivo de los equipos y los elementos de telecomunicaciones en el caso de que se produzca algún daño en un componente del equipo o de las telecomunicaciones, se generará una búsqueda del componente en el Almacén TI para verificar que la pieza existe; y así poder reemplazarla, si un componente es reemplazado en un equipo el administrador o usuario invitado deberá modificar la característica del equipo en el módulo Equipo por la nueva característica del componente que reemplazo, luego de esto el sistema deberá actualizar los datos.

**MÓDULO DE REPORTES**

En este módulo el administrador o usuario invitado podrá visualizar e imprimir:

- ✓ Reportes generales del mantenimiento de recursos TI
- ✓ Listado general del inventario.
- ✓ Listado general de proveedores.
- ✓ Listado general de custodio de equipo.
- ✓ Listado general de equipos con sus características de hardware y software.
- ✓ Listado general de almacén de TI
- ✓ Listado de general del software de la Institución.
- ✓ Listado general de movimiento interno de equipo.
- ✓ Listado general de salida de equipo.

**MÓDULO DE RESPALDO_BDD**

En este módulo se creará respaldos de la información de las bases de datos que se encuentran en nuestro web hosting. El administrador a través del sistema guardará diariamente respaldos de los datos en un disco duro e imprimirá una copia mensual en dispositivos cd-dvd – rw, flash memory u otros.

**MÓDULO DE ACTIVOS**

En este módulo el administrador o usuario invitado agregará nuevos equipos informáticos adquiridos por la institución con sus características de hardware y software; así también podrá modificar los datos referentes al equipo agregado.

Además se agregara las nuevas adquisiciones de Software que posee la institución; así como también se podrá modificar los datos referentes al Software agregado.

**MÒDULO MOVIMIENTO DE TI**

En este módulo el administrador o usuario invitado podrá llevar el registro de los equipos informáticos que han sido movidos internamente es decir dentro de la institución de un de departamento a otro; así también se llevará el registro de los equipos que han sido movidos externamente es decir que han salido a talleres particulares fuera de la institución para ser reparados.

# Marco Teórico

## IDE NetBeans 6.9.1[1]

El IDE NetBeans es un reconocido entorno de desarrollo integrado disponible para Windows, Mac, Linux y Solaris. El proyecto NetBeans está formado por un IDE de código abierto y una plataforma de aplicación que permite a los desarrolladores crear con rapidez aplicaciones web, empresariales, de escritorio y móviles utilizando la plataforma Java, así como JavaFX, PHP, JavaScript y Ajax, Ruby y Ruby on Rails, Groovy and Grails y C/C++.

El IDE NetBeans 6.9.1 introduce JavaFX Composer, una herramienta de diseño para la creación de aplicaciones gráficas JavaFX, parecido al constructor de aplicaciones gráficas Swing para aplicaciones Java SE. Otras notoriedades incluyen la interoperatividad OSGi para aplicaciones de plataforma NetBeans, y la compatibilidad para desarrollar paquetes OSGi con Maven; compatibilidad para el SDK de JavaFX 1.3.1, Famework Zend PHP, y RoR (Ruby on Rails) 3.0; así como mejoras en el editor Java, Depurador Java, seguimiento de incidencias, y muchas más.

1. http://netbeans.org/community/release/69. **NetBeans IDE 6.9.1 Divulgación de Información. 2010**

**JOOMLA![2]**

Joomla! es un sistema de gestión de contenidos, y entre sus principales virtudes está la de permitir editar el contenido de un sitio web de manera sencilla. Es una aplicación de código abierto programada mayoritariamente en PHP bajo una licencia GPL. Este administrador de contenidos puede trabajar en Internet o intranets y requiere de una base de datos MySQL, así como, preferiblemente, de un servidor HTTP Apache.

2. http://es.wikipedia.org/wiki/. **Joomla. 26-07- 2011**

## JAVA[3]

Java es un lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems a principios de los años 90. El lenguaje en sí mismo toma mucha de su sintaxis de C y C++, pero tiene un modelo de objetos más simple y elimina herramientas de bajo nivel, que suelen inducir a muchos errores, como la manipulación directa de punteros o memoria.
Las aplicaciones Java están típicamente compiladas en un bytecode, aunque la compilación en código máquina nativo también es posible. En el tiempo de ejecución, el bytecode es normalmente interpretado o compilado a código nativo para la ejecución, aunque la ejecución directa por hardware del bytecode por un procesador Java también es posible.

La implementación original y de referencia del compilador, la máquina virtual y las bibliotecas de clases de Java fueron desarrolladas por Sun Microsystems en 1995. Desde entonces, Sun ha controlado las especificaciones, el desarrollo y evolución del lenguaje a través del Java Community Process, si bien otros han desarrollado también implementaciones alternativas de estas tecnologías de Sun, algunas incluso bajo licencias de software libre.

Entre diciembre de 2006 y mayo de 2007, Sun Microsystems liberó la mayor parte de sus tecnologías Java bajo la licencia GNU GPL, de acuerdo con las especificaciones del Java Community Process, de tal forma que prácticamente todo el Java de Sun es ahora software libre (aunque la biblioteca de clases de Sun que se requiere para ejecutar los programas Java aún no lo es).

3. http://es.wikipedia.org/wiki/. **Java (lenguaje_de_programación). 24-09-2010**

**Servidor HTTP Apache[4]**

El servidor HTTP Apache es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que Behelendorf quería que tuviese la connotación de algo que es firme y enérgico pero no agresivo, y la tribu Apache fue la última en rendirse al que pronto se convertiría en gobierno de EEUU, y en esos momentos la preocupación de su grupo era que llegasen las empresas y "civilizasen" el paisaje que habían creado los primeros ingenieros de internet. Además Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, a patchy server (un servidor "parcheado").

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

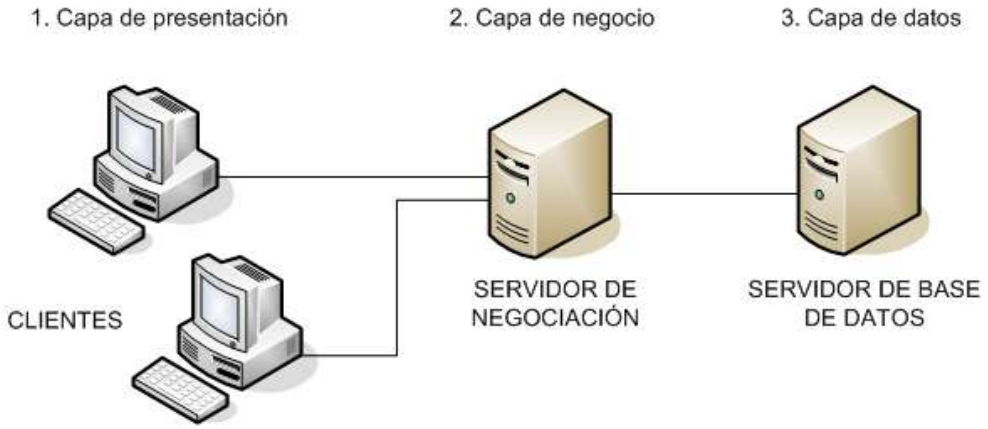
Apache presenta entre otras características altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.
Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cuota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años. (Estadísticas históricas y de uso diario proporcionadas por Netcraf).

La mayoría de las vulnerabilidades de la seguridad descubiertas y resueltas tan sólo pueden ser aprovechadas por usuarios locales y no remotamente. Sin embargo, algunas se pueden accionar remotamente en ciertas situaciones, o explotar por los usuarios locales malévolos en las disposiciones de recibimiento compartidas que utilizan PHP como módulo de Apache.

4. http://es.wikipedia.org/wiki/. **Servidor HTTP Apache. 2011**

## PROGRAMACIÓN POR CAPAS[5]

La programación por capas es un estilo de programación en el que el objetivo primordial es la separación de la lógica de negocios de la lógica de diseño; un ejemplo básico de esto consiste en separar la capa de datos de la capa de presentación al usuario.




**Ventajas**

- El desarrollo se puede llevar a cabo en varios niveles y, en caso de que sobrevenga algún cambio, sólo se ataca al nivel requerido sin tener que revisar entre código mezclado.
- Permite distribuir el trabajo de creación de una aplicación por niveles; de este modo, cada grupo de trabajo está totalmente abstraído del resto de niveles, de forma que basta con conocer la API que existe entre niveles.

En el diseño de sistemas informáticos actuales se suele usar las arquitecturas multinivel o programación por capas. En dichas arquitecturas a cada nivel se le confía una misión simple, lo que permite el diseño de arquitecturas escalables (que pueden ampliarse con facilidad en caso de que las necesidades aumenten).
El diseño más utilizado actualmente es el diseño en tres niveles (o en tres capas).

**1.- Capa de presentación:** es la que ve el usuario (también se la denomina "capa de usuario"), presenta el sistema al usuario, le comunica la información y captura la información del usuario en un mínimo de proceso (realiza un filtrado previo para

comprobar que no hay errores de formato). Esta capa se comunica únicamente con la capa de negocio. También es conocida como interfaz gráfica y debe tener la característica de ser "amigable" (entendible y fácil de usar) para el usuario.

**2.- Capa de negocio:** es donde residen los programas que se ejecutan, se reciben las peticiones del usuario y se envían las respuestas tras el proceso. Se denomina capa de negocio (e incluso de lógica del negocio) porque es aquí donde se establecen todas las reglas que deben cumplirse. Esta capa se comunica con la capa de presentación, para recibir las solicitudes y presentar los resultados, y con la capa de datos, para solicitar al gestor de base de datos para almacenar o recuperar datos de él. También se consideran aquí los programas de aplicación.

**3.- Capa de datos:** es donde residen los datos y es la encargada de acceder a los mismos. Está formada por uno o más gestores de bases de datos que realizan todo el almacenamiento de datos, reciben solicitudes de almacenamiento o recuperación de información desde la capa de negocio.
Todas estas capas pueden residir en un único ordenador, si bien lo más usual es que haya una multitud de ordenadores en donde reside la capa de presentación (son los clientes de la arquitectura cliente/servidor). Las capas de negocio y de datos pueden residir en el mismo ordenador, y si el crecimiento de las necesidades lo aconseja se pueden separar en dos o más ordenadores. Así, si el tamaño o complejidad de la base de datos aumenta, se puede separar en varios ordenadores los cuales recibirán las peticiones del ordenador en que resida la capa de negocio.

Si, por el contrario, fuese la complejidad en la capa de negocio lo que obligase a la separación, esta capa de negocio podría residir en uno o más ordenadores que realizarían solicitudes a una única base de datos. En sistemas muy complejos se llega a tener una serie de ordenadores sobre los cuales corre la capa de negocio, y otra serie de ordenadores sobre los cuales corre la base de datos.

En una arquitectura de tres niveles, los términos "capas" y "niveles" no significan lo mismo ni son similares.

El término "capa" hace referencia a la forma como una solución es segmentada desde el punto de vista lógico:
Presentación/ Lógica de Negocio/ Datos.
En cambio, el término "nivel" corresponde a la forma en que las capas lógicas se encuentran distribuidas de forma física. Por ejemplo:

- Una solución de tres capas (presentación, lógica del negocio, datos) que residen en un solo ordenador (Presentación + lógica + datos). Se dice que la arquitectura de la solución es de tres capas y un nivel.
- Una solución de tres capas (presentación, lógica del negocio, datos) que residen en dos ordenadores (presentación + lógica, lógica + datos). Se dice que la arquitectura de la solución es de tres capas y dos niveles.
- Una solución de tres capas (presentación, lógica del negocio, datos) que residen en tres ordenadores (presentación, lógica, datos). La arquitectura que la define es: solución de tres capas y tres niveles.

5.http://docs.google.com/viewer?a=v&q=cache:q85qQAEUZrAJ:oasis.ciscug.org/cisc/tutoriales/tercero/.**Programación por capas.doc. 2007**

## JAVA WEB START[6]

Es la implementación de referencia de la especificación JNLP (JSR 56, Java Networking Launching Protocol), que define como ejecutar aplicaciones Java remotamente desde un entorno de red cualquiera.

Java Web Start revoluciona el concepto tradicional que tenemos de las aplicaciones. Normalmente cuando se quiere ejecutar una aplicación que no se encuentra instalada en un equipo, se descarga del servidor, se instala en dicho equipo y por último se ejecuta. Java Web Start intenta simplificar al máximo todo este proceso de modo que el usuario lo único que tiene que hacer para lanzar una aplicación será simplemente pinchar en un enlace de su navegador, a partir de ese momento, todo el proceso relacionado con la descarga, instalación y ejecución del programa se realiza de una manera transparente.

A pesar de su parecido, una aplicación de Java Web Start no tiene nada que ver con un Applet. Java Web Start sólo utiliza el navegador como medio para que el usuario pueda ejecutar las aplicaciones. Una vez que el usuario pincha en un enlace de una aplicación, ésta se ejecuta en la máquina virtual del cliente como cualquier otra aplicación.
Java Web Start no forma parte del navegador web, es una aplicación independiente y por lo tanto no requiere del navegador para su funcionamiento. Una vez que el usuario pincha en un enlace para ejecutar una aplicación, puede continuar navegando o cerrar el navegador sin que esto interfiera en el funcionamiento de la aplicación que ha sido lanzada. Además, Java Web Start va guardando en una caché interna las aplicaciones que va ejecutando el usuario, de modo que éste pueda lanzarlas posteriormente sin la necesidad de abrir el navegador o incluso ejecutarlas localmente sin conectarse a ninguna red.

Las aplicaciones Java Web Start siguen el modelo de seguridad de la plataforma Java 2 por lo que la integridad de los datos que obtenemos a través de la red está garantizada. Como veremos, comúnmente las aplicaciones que se ejecuten han de estar debidamente firmadas y se requiere siempre que el usuario autorice su ejecución.

Java Web Start viene incluido de serie dentro en el JRE a partir de su versión 1.4. La última versión es la 1.2 (beta) que viene con el JRE 1.4.1 también beta. Como curiosidad reseñar que el sistema operativo OS X de Macintosh ya trae preinstalado soporte para aplicaciones Java Web Start. Aunque técnicamente es necesario que se encuentre instalado al menos un JRE dentro de la máquina cliente para poder ejecutar aplicaciones Java Web Start, lo cierto es que éstas se pueden configurar de manera que el JRE utilizado se descargue automáticamente si no se encuentra disponible con lo que se consigue una transparencia absoluta para el cliente.

6.http://javatipsandtricks.blogspot.com/2007/01/.**java-web-start.html. 2007**

# DESCRIPCIÓN DEL HPGIA-LOJA

## Historia

El Hospital Regional y Docente "Isidro Ayora" fue inaugurado por el Gobierno del General Guillermo Rodríguez Lara, el 2 agosto de 1.979, gracias a la gestión del Ministro de Salud de ese entonces Doctor Gil Bermeo Vallejo, siendo el Director de Salud de Loja el Doctor Hugo Guillermo Gonzales. El primer Director del Hospital fue el Doctor Humberto Franco Castillo, inicia sus actividades brindando a la comunidad lojana, la oportunidad de acceder a una atención de calidad científica y humanística. Se inicia así la etapa de la vigencia de las especialidades, contribuyendo de esta manera a la aportación de nuevos conocimientos, como en el tratamiento y la recuperación de los pacientes.

## Datos Generales

El Hospital Provincial General Isidro Ayora es una entidad de servicios de salud del Ministerio de Salud Pública, implementado para prestar atención de salud integral de tipo ambulatorio y de internamiento las 24 horas del día y los 365 días del año, en cada uno de los servicios de salud del Hospital, con un acceso de demanda de usuarias-os provenientes de los 16 cantones de la provincia de Loja, parte de las provincias de El Oro y Zamora y del norte de la República del Perú. Es además, un centro de formación profesional de personal médico y de enfermería, así como de investigación bio-social.

El hospital cuenta con 243 camas, 23 consultorios, 4 Quirófanos (uno para gíneco-obstetricia y 3 para el resto de especialidades quirúrgicas), sala de partos para 3 camillas, Centro Obstétrico, Unidad de Cuidados Intensivos, Área de Neonatología, Laboratorio Clínico e Histopatológico, Servicio de Imagenología, Unidad de Quemados, Salud Mental, Odontología, Farmacia, Hemodiálisis, Fisiatría y Rehabilitación, Central de Esterilización y de Enfermería.

Además, el hospital cuenta con las siguientes Áreas Técnicas según Ciclo Vital: Servicios de Medicina Transfusional; Club de Diabéticos e Hipertensos; Atención Integral de la Violencia de Género, Intrafamiliar y Sexual por Ciclos de Vida; Programa de Tuberculosis; Unidad de Atención Diferenciada al Adolescente; Clínica del V.I.H; y, Seguridad y Salud Ocupacional.

Por otra parte, el hospital cuenta con los servicios generales de trabajo social, hotelería, bodegas, almacenamiento, talleres de mantenimiento y otros.

## Direccionamiento Estratégico

### Misión

Presar atención de salud especializada y sub-especializada en prevención, diagnóstico, tratamiento y rehabilitación, con calidad, calidez y equidad a las-os que demanden sus servicios.

### Visión

El Hospital Provincial General Isidro Ayora de Loja, será la Institución líder en la Región 7 en prestar atención de salud integral y constituirse en un centro docente y de investigación en salud, con personal formado humanística y científicamente, equipado con tecnología de punta, con infraestructura física adecuada que satisfaga plenamente las necesidades de las-os usuarios.

## Estructura Organizacional

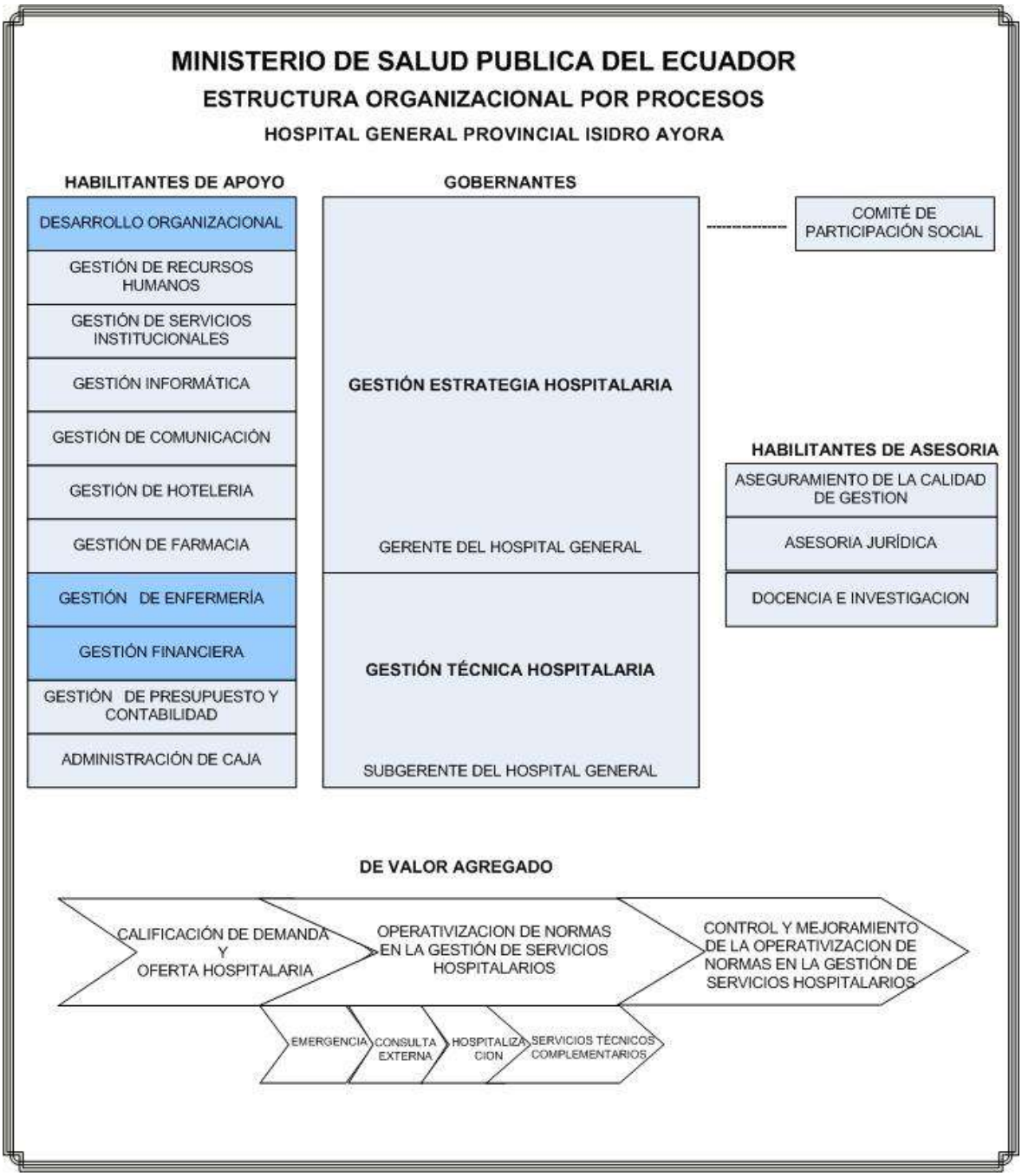



Gráfico1. Estructura Organizacional del HPGIA

# METODOLOGÍA DE DESARROLLO DE SOFTWARE

## Metodología XP

## ¿Qué es Xtreme Programming (XP)?

La Programación Extrema es una metodología de desarrollo de software ligera, que se basa en los principios de la simplicidad, la comunicación y la retroalimentación o reutilización del código desarrollado.

## Introducción a la Metodología XP

Las cuatro variables:

- Coste: Máquinas, especialistas y oficinas
- Tiempo: Total y de Entregas
- Calidad: Externa e Interna
- Alcance: Intervención del cliente

## Fases de la Metodología XP

**I. PLANIFICACIÓN:**

1. Historias de Usuarios
2. Plan de entregas
3. Velocidad del Proyecto
4. Iteraciones
5. Rotaciones
6. Reuniones

**II. DISEÑO:**

1. Diseños Simples
2. Glosario de Términos
3. Tarjetas C.R.C
4. Soluciones Puntuales
5. Funcionalidad Mínima
6. Reciclaje

## III. DESARROLLO:

1. Disponibilidad de Clientes
2. Unidad de Pruebas.
3. Programación en Pareja
4. Integración

## IV. PRUEBAS:

1. Implantación
2. Pruebas de Aceptación

# FASE I: PLANIFICACIÓN

# PLANIFICACIÓN

**Propósito.** En esta fase se considera las historias de usuario con su respectiva prioridad, además los programadores realizan las estimaciones de esfuerzo necesario para cada historia de usuario. Se toman acuerdos sobre el contenido de la primera entrega y se determina un cronograma en conjunto con el cliente.

**Introducción**

Para el desarrollo del sistema Web para el Control de los Recursos de Tecnología de la Información del HPGIA; hemos seleccionado la metodología de desarrollo de software XP (Extreme Programming), puesto que este tipo de metodología es muy buena, y se adapta a las necesidades de los desarrolladores. La propuesta que se presenta para este proyecto, corresponde al desarrollo de: un Portal Web Informativo para la Institución, y además el desarrollo de una herramienta de software para llevar el Control de los recursos de TI del Hospital. El software desarrollado tiene como objetivo llevar el registro y control del hardware, software y elementos de telecomunicaciones que tiene la institución, ayudando de esta manera al administrador del centro de cómputo a llevar de forma eficiente el proceso de administración de los recursos de TI.

La metodología XP sugiere diseños simples y sencillos. Se procurará hacerlo sencillo para conseguir un diseño entendible e implementarlo, que a la larga signifique menos tiempo y esfuerzo al desarrollar.

Definir la arquitectura del sistema, el cual será implementado por N capas, a través de la construcción de clases (librerías de clases); además la capa de presentación será multiplataforma (Windows o Linux).

| FICHA TÉCNICA | |
|---|---|
| CONTENIDO | 1. Historias de Usuarios<br>2. Plan de entregas<br>3. Velocidad del Proyecto<br>4. Iteraciones<br>5. Reuniones<br>6. Requerimientos Funcionales |
| **GRÁFICOS** | |
| **REGISTROS** | Registro 2.0 Historia Usuario HU.1 (Acceso al Sistema)<br>Registro 2.1 Historia Usuario HU.2 (Administrativo)<br>Registro 2.2 Historia Usuario HU.3 (Inventario)<br>Registro 2.3 Historia Usuario HU.4 (Ingreso Equipo)<br>Registro 2.4 Historia Usuario HU.5 (Movimiento Equipo)<br>Registro 2.5 Historia Usuario HU.6 (Mantenimiento Equipo)<br>Registro 2.6 Historia Usuario HU.7 (Respaldo BDD)<br>Registro 2.7 Historia Usuario HU.8 (Reportes)<br>Registro 2.8 Estimación de Esfuerzo EE.1 (Administrativo)<br>Registro 2.9 Estimación de Esfuerzo EE.2 (Departamento)<br>Registro 2.10 Estimación de Esfuerzo EE.3 (Proveedor)<br>Registro 2.12 Estimación de Esfuerzo EE.4 (Contacto)<br>Registro 2.13 Estimación de Esfuerzo EE.5 (Custodio)<br>Registro 2.14 Estimación de Esfuerzo EE.6 (Inventario)<br>Registro 2.15 Estimación de Esfuerzo EE.7 (Hoja-Trabajo)<br>Registro 2.16 Estimación de Esfuerzo EE.8 (Respaldo BDD)<br>Registro 2.17 Estimación de Esfuerzo EE.9 (Reporte)<br>Registro 2.18 Estimación de Esfuerzo EE.10 (Equipo)<br>Registro 2.19 Estimación de Esfuerzo EE.11 (Componente-Equipo)<br>Registro 2.20 Estimación de Esfuerzo EE.12 (Software-Equipo)<br>Registro 2.21 Estimación de Esfuerzo EE.13 (Software)<br>Registro 2.22 Estimación de Esfuerzo EE.14 (Almacén TI)<br>Registro 2.23 Estimación de Esfuerzo EE.15 (Movimiento Interno) |

| | |
|---|---|
| | Registro 2.24 Estimación de Esfuerzo EE.16 (Movimiento Externo)<br>Registro 2.25 Estimación de Esfuerzo EE.17(Estimaciones Total) |
| **PROBLEMAS Y SOLUCIONES ENCONTRADAS** | |
| **Problemas:** | **Soluciones:** |

## 1. Historias de Usuarios

Las historias de usuario tienen la misma finalidad que los casos de uso pero con algunas diferencias:

- Constan de 3 ó 4 líneas escritas por el cliente en un lenguaje sencillo, sobre las necesidades del sistema.
- Son usadas para estimar tiempos de desarrollo de la parte de la aplicación que describen.
- Se utilizan en la fase de pruebas, para verificar si la aplicación cumple con lo que especifica la historia de usuario.
- Para implementar una historia de usuario, el cliente y los desarrolladores se reúnen para concretar y detallar lo que tiene que hacer dicha historia.
- El tiempo de desarrollo ideal para una historia de usuario es entre 1 y 3 semanas.

La principal diferencia entre un caso de uso y una historia de usuario radica en el nivel de detalle. Las historias de usuarios unicamente proporcionan los detalles sobre la estimación de riesgo y cuánto tiempo conllevará su implementación.

<table>
<tr><td>UH.1</td><td colspan="3">Historia Usuario #1</td></tr>
<tr><td colspan="2">REFERENCIA A LA HISTORIA 1</td><td colspan="2"></td></tr>
<tr><td colspan="4">NOMBRE:ACCESO USUARIO SISTEMA</td></tr>
<tr><td>FECHA: 17/08/2010</td><td>ACTIVIDAD: Corregida</td><td colspan="2">PRUEBA FUNCIONAL: Concurrente</td></tr>
<tr><td colspan="4">PRIORIDAD TECNICA DEL ADMINISTRADOR: Alta<br>DESCRIPCIÓN: Al momento de ingresar un nuevo usuario se debe verificar la cuenta de usuario si existe o no en el sistema, se pide que ingrese su nombre y contraseña.<br>RIESGO: Ninguno<br>FECHA INICIO:17/08/2010<br>FECHA CULMINACIÓN:18/08/2010</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
</table>

| UH.2 | Historia Usuario #2 |
|---|---|
| REFERENCIA A LA HISTORIA 2 | |
| NOMBRE:ADMINISTRATIVO | |
| FECHA: 18/08/2010 | ACTIVIDAD: Corregida |
| PRUEBA FUNCIONAL: Concurrente | |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se registrará y modificará datos de departamento, usuario sistema, proveedor, administrativo, custodio y contacto. Proceso que sólo lo puede ejecutar el usuario Administrador.<br>**RIESGO:** Ninguno<br>**FECHA INICIO:**18/08/2010<br>**FECHA CULMINACIÓN**:19/08/2010 | |
| | |

| UH.3 | Historia Usuario #3 |
|---|---|
| REFERENCIA A LA HISTORIA 3 | |
| NOMBRE:INVENTARIO | |
| FECHA: 19/08/2010 | ACTIVIDAD: Corregida |
| PRUEBA FUNCIONAL: Concurrente | |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se registrará y modificará datos del inventario, cada bien se registrará con un único código de activo fijo determinado por el departamento de activos fijos.<br>**RIESGO:** Ninguno<br>**FECHA INICIO:**19/08/2010<br>**FECHA CULMINACIÓN**:20/08/2010 | |
| | |

| UH.4 | Historia Usuario #4 |
|---|---|
| REFERENCIA A LA HISTORIA 4 | |
| NOMBRE:INGRESO EQUIPOS | |
| FECHA: 20/08/2010 | ACTIVIDAD: Corregida |
| PRUEBA FUNCIONAL: Concurrente | |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se registrará un nuevo equipo, con sus datos de componente de hardware y software. Comprobando la existencia de los equipos.<br>**RIESGO:** Ninguno<br>**FECHA INICIO:**20/08/2010<br>**FECHA CULMINACIÓN**:21/08/2010 | |
| | |

| UH.5 | Historia Usuario #5 | |
|---|---|---|
| REFERENCIA A LA HISTORIA 5 | | |
| NOMBRE: MOVIMIENTO EQUIPOS | | |
| FECHA: 21/08/2010 | ACTIVIDAD: Corregida | PRUEBA FUNCIONAL: Concurrente |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se registrará el movimiento de un equipo, con sus datos de tipo de movimiento interno o externo. Comprobando físicamente el tipo de movimiento.<br>**RIESGO:** Alto<br>**FECHA INICIO:**21/08/2010<br>**FECHA CULMINACIÓN**:22/08/2010 | | |
| | | |

| UH.6 | Historia Usuario #6 | |
|---|---|---|
| REFERENCIA A LA HISTORIA 6 | | |
| NOMBRE: MANTENIMIENTO EQUIPOS | | |
| FECHA: 22/08/2010 | ACTIVIDAD: Corregida | PRUEBA FUNCIONAL: Concurrente |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se registrará el mantenimiento de equipo, con sus datos de tipo de mantenimiento correctivo o preventivo, etc. Comprobando la existencia de solicitud de Hoja-Trabajo.<br>**RIESGO:** Ninguno<br>**FECHA INICIO:**22/08/2010<br>**FECHA CULMINACIÓN**:23/08/2010 | | |
| | | |

| UH.7 | Historia Usuario #7 | |
|---|---|---|
| REFERENCIA A LA HISTORIA 7 | | |
| NOMBRE:RESPALDO BDD | | |
| FECHA: 23/08/2010 | ACTIVIDAD: Corregida | PRUEBA FUNCIONAL: Concurrente |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se creará una copia de respaldo de las bases de datos del servidor Centos 5.4.<br>**RIESGO:** Alto<br>**FECHA INICIO:**23/08/2010<br>**FECHA CULMINACIÓN**:24/08/2010 | | |
| | | |

| UH.8 | Historia Usuario #8 | |
|---|---|---|
| REFERENCIA A LA HISTORIA 8 | | |
| NOMBRE:REPORTES | | |
| FECHA: 24/08/2010 | ACTIVIDAD: Corregida | PRUEBA FUNCIONAL: Concurrente |
| **PRIORIDAD TECNICA DEL ADMINISTRADOR**: Alta<br>**DESCRIPCIÓN:** Se observará e imprimirá reporte generales de equipos, inventario, mantenimiento, movimiento y administrativo.<br>**RIESGO:** Ninguno<br>**FECHA INICIO:**24/08/2010<br>**FECHA CULMINACIÓN**:25/08/2010 | | |
| | | |

## 2. Plan de entregas

El plan de entrega se basa en el tiempo o el alcance del proyecto, se puede efectuar una evaluación apropiada con relación a la prioridad de cada historia de usuario, es de gran importancia puesto que ayuda a determinar el cronograma de entregas.

Se establece estimaciones de esfuerzo inscritas en la implementación de las historias de usuario, se usa un punto como medida. Donde un punto equivale a una semana ideal de programación, yendo estas generalmente de 1 a 3 puntos.

Asi también se lleva un registro de la velocidad de desarrollo, establecida en puntos de iteración, teniendo presente la suma de puntos proporcionados a las historias de usuario que son terminadas en la iteración final.

Estimaciones de Esfuerzo

**ADMINISTRACIÓN:**

| | EE.1 |
|---|---|
| **ADMINISTRATIVO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.2 |
|---|---|
| **DEPARTAMENTO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.3 |
|---|---|
| **PROVEEDOR** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.4 |
|---|---|
| **CONTACTO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.5 |
|---|---|
| **CUSTODIO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

**INVENTARIO:**

| | EE.6 |
|---|---|
| **INVENTARIO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

**MANTENIMIENTO**

| | EE.7 |
|---|---|
| **HOJA_TRABAJO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

**RESPALDOS BDD**

| | EE.8 |
|---|---|
| **RESPALDO_BDD** | |
| Crear Prueba | **2** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

**REPORTES**

| | EE.9 |
|---|---|
| **REPORTES** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los data sets | |
| 1 semana | |

**ACTIVOS**

| | EE.10 |
|---|---|
| **EQUIPO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.11 |
|---|---|
| **COMPONENTE_EQUIPO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.12 |
|---|---|
| **SOFTWARE_EQUIPO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.13 |
|---|---|
| **SOFTWARE** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.14 |
|---|---|
| **ALMACEN_TI** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

**MOVIMIENTO**

| | EE.15 |
|---|---|
| **MOVIMIENTO INTERNO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

| | EE.16 |
|---|---|
| **SALIDA EQUIPO** | |
| Crear Prueba | **1** |
| Crear Métodos | |
| Crear Acceso a los Datos | |
| 1 semana | |

**TOTAL:**

| | EE.17 |
|---|---|
| **ESTIMACIONES** | |
| Administración | **5** |
| Inventario | **1** |
| Mantenimiento | **1** |
| Respaldos BDD | **2** |
| Reportes | **1** |
| Activos | **5** |
| Movimiento | **2** |
| **Total** | **17** |

El 17 representa el número de semanas aproximadas que se necesitan para codificar todos los módulos de la aplicación.

## 3. Velocidad del Proyecto

La velocidad del proyecto es una medida que representa la rapidez con la que se desarrolla el proyecto; estimarla es muy sencillo, basta con contar el número de historias de usuario que se pueden implementar en una iteración; de esta forma, se sabrá el cupo de historias que se pueden desarrollar en las distintas iteraciones.

Usando la velocidad del proyecto controlaremos que todas las tareas se puedan desarrollar en el tiempo del que dispone la iteración. Es conveniente reevaluar esta medida cada 3 ó 4 iteraciones y si se aprecia que no es adecuada hay que negociar con el cliente.

## 4. Iteraciones

Todo proyecto que siga la metodología X.P. se ha de dividir en iteraciones de aproximadamente 3 semanas de duración. Al comienzo de cada iteración los clientes deben seleccionar las historias de usuario definidas a ser implementadas. También se seleccionan las historias de usuario que no pasaron el test de aceptación que se realizó al terminar la iteración anterior. Estas historias de usuario son divididas en tareas de entre 1 y 3 días de duración que se asignarán a los programadores.

Las iteraciones se efectúan en el orden que la institución realiza los procesos de manejo de la información.

**Primera Iteración:** se valida las entradas para usuarios, que pueden ser de tipo: administrador o invitado.

| **UH.1** | | **Historia Usuario utilizadas en la Iteración** |
|---|---|---|
| **Referencia historia 1** | **Referencia:RP.1** | |
| **NOMBRE: Acceso Usuario al Sistema** | | |
| **PRIORIDAD TECNICA Y DEL ADMINISTRADOR: Alta**<br>**RIESGO: Ninguno** | | |
| | | |

**Segunda Iteración:** se crea la base de datos, los métodos y propiedades para las tablas departamento, usuarios, proveedor, administrativo, custodio y contacto, de acuerdo a los requerimientos definidos en la etapa de recolección de datos.

| **UH.2** | | **Historia Usuario utilizadas en la Iteración** |
|---|---|---|
| **Referencia historia 2** | **Referencia:RP.2** | |
| **NOMBRE: Administrativo** | | |
| **PRIORIDAD TÉCNICA Y DEL ADMINISTRADOR: Alta**<br>**RIESGO: Ninguno** | | |
| | | |

**Tercera Iteración:** se crea la base de datos, los métodos y propiedades para la tabla inventario, de acuerdo a los requerimientos definidos en la etapa de recolección de datos.

| UH.3 | | Historia Usuario utilizadas en la Iteración |
|---|---|---|
| Referencia historia 3 | Referencia:RP.3 | |
| NOMBRE: Inventario | | |
| PRIORIDAD TÉCNICA Y DEL ADMINISTRADOR: Alta<br>RIESGO: Ninguno | | |
| | | |

**Cuarta Iteración:** se crea la base de datos, los métodos y propiedades para el ingreso de un nuevo equipo a la institución, de acuerdo a los requerimientos definidos en la etapa de recolección de datos.

| UH.4 | | Historia Usuario utilizadas en la Iteración |
|---|---|---|
| Referencia historia 4 | Referencia:RP.4 | |
| NOMBRE: Ingreso Equipo | | |
| PRIORIDAD TÉCNICA Y DEL ADMINISTRADOR: Alta<br>RIESGO: Ninguno | | |
| | | |

**Quinta Iteración:** se crea la base de datos, los métodos y propiedades para el registro de movimiento de un recurso de TI de la institución, de acuerdo a los requerimientos definidos en la etapa de recolección de datos (Ver Anexo 1 y Anexo 2).

| UH.5 | | Historia Usuario utilizadas en la Iteración |
|---|---|---|
| Referencia historia 5 | Referencia:RP.5 | |
| NOMBRE: Movimiento Equipos | | |
| PRIORIDAD TÉCNICA Y DEL ADMINISTRADOR: Alta<br>RIESGO: Ninguno | | |
| | | |

**Sexta Iteración:** se crea la base de datos, los métodos y propiedades para el registro de mantenimiento de un recurso de TI de la institución, de acuerdo a los requerimientos definidos en la etapa de recolección de datos (Ver Anexo 3).

| UH.6 | | Historia Usuario utilizadas en la Iteración |
|---|---|---|
| Referencia historia 6 | Referencia:RP.6 | |
| NOMBRE: Mantenimiento Equipos | | |
| PRIORIDAD TECNICA Y DEL ADMINISTRADOR: Alta<br>RIESGO: Ninguno | | |
| | | |

**Séptima Iteración:** se crea el respaldo de la bases de datos del servidor Centos 5.4

| UH.7 | | Historia Usuario utilizadas en la Iteración |
|---|---|---|
| Referencia historia 7 | Referencia:RP.7 | |
| NOMBRE: Respaldo de BDD | | |
| PRIORIDAD TECNICA Y DEL ADMINISTRADOR: Alta<br>RIESGO: Alto | | |
| | | |

**Octava Iteración:** se crea la base de datos y las consultas para los reportes de los procesos de administración de los recursos de TI.

| UH.8 | | Historia Usuario utilizadas en la Iteración |
|---|---|---|
| Referencia historia 8 | Referencia:RP.8 | |
| NOMBRE: Reportes | | |
| PRIORIDAD TECNICA Y DEL ADMINISTRADOR: Alta<br>RIESGO: Ninguna | | |
| | | |

## 5. Reuniones

Con este tipo de programación, los desarrolladores se reúnen diariamente y exponen sus problemas, soluciones e ideas de forma conjunta. Las reuniones tienen que ser fluidas y todos sus integrantes tienen voz y voto.

Previo a una reunión con el Director del Hospital Isidro Ayora Dr. Daniel Astudillo y el Administrador de Gestión Informática Ing. Mario Cueva se llegó al acuerdo de desarrollar una herramienta de software que permita registrar y controlar los recursos de TI de la institución denominada: “Sistema Web para el Control de los Recursos de TI del Hospital Isidro Ayora”.

En vista de que el administrador de los recursos de TI es conocedor de los procesos en la administración de las TI, se convierte en un integrante fundamental en el equipo de desarrollo del software, al administrador se le solicito de manera formal toda la información referente al manejo de los recursos de TI, la información recolectada sirvió de apoyo para el levantamiento de los requerimientos.

Luego de realizada la reunión y posteriormente haber recolectado la información se procede a desarrollar la aplicación, cuyo fin es registrar y controlar los recursos de TI que posee la institución.

## 6. Requerimientos Funcionales

**Requerimientos de SYSCORTI**

| Requerimiento | Descripción |
|---|---|
| RS.1 | Mantener ordenada y automatizada la información de los recursos de TI del HGPIA-Loja. |
| RS.2 | Registrar cada uno de los equipos con sus características de hardware y software. |
| RS.3 | Permitir el registro de activos (equipos informàticos) cada vez que se ha hecho una nueva adquisición. |
| RS.4 | Hacer conocer a nivel mundial de los servicios que presta el HGPIA-Loja, por medio de la web. |
| RS.5 | Facilitar la toma de decisiones, a traves de la generación de reportes. |
| RS.6 | Registrar y controlar el mantenimiento de los equipos informáticos. |

## Requerimientos del Sistema

### Administraciòn del Sistema

| Requerimiento | Descripción | Tipo |
|---|---|---|
| AS.1 | Acceder mediante el nombre de usuario y password. | Evidente |
| AS2 | Registrar un nombre y password para el usuario. | Evidente |
| AS.3 | Validar el nombre y password del usuario. | Oculto |
| AS.4 | Modificar datos del usuario. | Evidente |
| AS.5 | Bloquear datos del usuario(administrador del centro de cómputo) | Evidente |

### Atributos de la Aplicaciòn

| Atributo | Descripción | Tipo |
|---|---|---|
| AA.1 | Sitio web y aplicación java con iterfaz de usuario amigable y fácil de manipular; que contiene elementos como: links, botónes y gráficos. | Obligatorio |
| AA2 | Entrada de la informaciòn, a través del teclado y mouse. | Obligatorio |
| AA.3 | Salida de la informaciòn, a través del monitor y la impresora. | Obligatorio |
| AA.4 | Tiempo de respuesta al sistema, técnicamente admisible en conexiones a internet rápidas. | Anhelado |
| AA.5 | Plataformas del sistema operativo, Windows 7, Windows XP y Centos 5.4, técnicamente admisible. | Anhelado |

# FASE II: DISEÑO

# DISEÑO

**Propósito** El propósito fundamental de esta fase es definir la estructura esquematizada de las interfaces de usuario, base de datos y diagrama de clases. Además se desarrolla las tarjetas CRC y el diseño de portal Web Informativo de la Institución.

**Introducción**

Esta parte de diseño global se realiza mediante lluvia de ideas, intentando lograr entre todos un cuadro global del sistema. Mediante la lluvia de ideas, los miembros del equipo intentan detectar todas las tareas necesarias para desarrollar las historias de usuario. Por regla general, nos encontramos con que el equipo ha encontrado una solución correcta, que implica una extensión de las funcionalidades de la última versión desarrollada. Otras veces, encontramos la existencia de varias aproximaciones, por la que el equipo debe elegir la más simple, acorde con la filosofía que siempre se sigue en XP. En otras ocasiones, no se encuentra ninguna solución factible apriori. Estas son las ocasiones típicas en las que se debe iniciar una iteración experimental, que nunca debe durar más de un día o dos, intentando ver cuál es una posible solución. Aquí nunca se resolverá el problema, se debe encontrar únicamente la manera, pero sin profundizar más allá de lo necesario para saber qué hacer. Una vez se tiene una visión global del sistema a desarrollar en la iteración en cuestión, se dividen las tareas en grupos de dos personas, que iniciarán un ciclo como el visto en la figura 3 del punto anterior, estimando su tarea, de manera que ayudan al jefe de proyecto a la hora de la estimación del tiempo y consiguen cierta libertad al desarrollar en un plazo de tiempo en el que ellos creen.

| FICHA TÉCNICA | |
|---|---|
| **CONTENIDO** | 1. Metáfora del Sistema<br>2. Diseños Simples<br>3. Glosario de Términos<br>4. Tarjetas C.R.C<br>5. Soluciones Puntuales<br>6. Funcionalidad Mínima<br>6.1. Arquitectura del Sistema<br>6.1.1. Capa de Presentación<br>6.1.2. Capa de Negocio<br>6.1.3. Capa de Datos<br>7. Diseño del Portal Web<br>7.1. Metodología<br>7.2. Estructura del sitio Web<br>7.3. Diagramación de Páginas<br>7.4. Diseño Imágenes<br>7.5. Diseño de Páginas<br>7.6. Incorporación Multimedia<br>7.7. Descripción de página<br>8. Diseño de Base de Datos<br>9. Diagrama de Clases<br>10. Diseño de la Aplicación<br>10.1 Desarrollo de Interfaz de Usuario<br>11. Diseño de Registros<br>12. Reciclaje |
| **GRÁFICOS** | Gráfico 2. Arquitectura Funcional del Sistema<br>Grafico 3. Arquitectura N-Capas<br>Gráfico 4. Metodología de Diseño de Páginas Web<br>Gráfico 5. Diagramación Portal Web |

| | |
|---|---|
| **REGISTROS** | Tarjeta CRC en blanco (pág.165)<br>Tarjeta CRC Usuario (pág.166)<br>Tarjeta CRC Inventario (pág.167)<br>Tarjeta CRC Componente_Equipo(pág.167)<br>Tarjeta CRC Software_Equipo(pág.168)<br>Tarjeta CRC Custodio(pág.168)<br>Tarjeta CRC Administrativo(pág.169)<br>Tarjeta CRC Departamento(pág.169)<br>Tarjeta CRC Proveedor(pág.170)<br>Tarjeta CRC Hoja_Trabajo(pág.170)<br>Tarjeta CRC Movimiento_Interno(pág.171)<br>Tarjeta CRC Salida_Equipo(pág.171)<br>Tarjeta CRC Almacen_RecursosTI(pág.172)<br>Tarjeta CRC Contacto(pág.172)<br>Tarjeta CRC Reportes(pág.173)<br>Tarjeta CRC RespaldoBDD(pág.174)<br>Tarjeta CRC Equipo(pág.174)<br>Tarjeta CRC Software(pág.175)<br>Tarjeta CRC Operación_Log(pág.175) |

# Diseño de la Aplicación

## 1. Metáfora del Sistema

**Metáfora.** Es una historia o narración a través de la cual se puede definir la funcionalidad del sistema. Las metáforas permiten a cualquier persona entender cuál es el objeto de la aplicación.

El objetivo fundamental del proyecto es desarrollar el Sistema Web para el Control de los Recursos de Tecnología de la Información (SYSCORTI) del Hospital Isidro Ayora, el mismo que permitirá administrar adecuadamente los recursos de TI (pc's, laptops, servidores, switchs, ruteadores) de la institución.

El Sistema constara de dos partes: La parte Web, que muestra información de la institución como: Historia, Misión y Visión, Servicio que Ofrece, Programas, Ley de Transparencia, Contactos y además al lado derecho de la página Syscorti existirá un botón de descarga de SYSCORTI. La Parte de la Aplicación estará desarrollada en un lenguaje de programación multiplataforma (Java), y estará compuesta de cinco módulos: El Módulo de Acceso al Sistema, el Módulo Control de Inventario, el Módulo Mantenimiento Físico y Lógico, el Módulo de Toma de Decisiones y por último el Módulo de Respaldo de Base de Datos.

## 2. Diseños Simples

Un Diseño Simple se enfoca en proporcionar un sistema que cubra las necesidades inmediatas del cliente, ni más ni menos. Este proceso permite eliminar la redundancia y rejuvenecer los diseños obsoletos de forma sencilla.

El diseño adecuado para el software es aquel que:

1. Trabaja con todas las pruebas
2. No tiene lógica transcrita

3. Muestra cada intención importante para los programadores
4. Tiene el menor número de clases y métodos

El diseño de la aplicación maneja un modelado sencillo y fácil de entender, está basado en una arquitectura distribuida de N capas que hace fácil la administración de los recursos que intervienen en el proceso del desarrollo de la aplicación.

El lenguaje de programación java, es una tecnología a usar para el desarrollo de la aplicación, con este lenguaje podemos obtener una aplicación multiplataforma, que pueden trabajar tanto en entornos Windows, Linux y Mac. Este lenguaje permite interactuar con objetos, dando lugar a la reutilización de código fuente, por lo que es necesario tener en cuenta, cuales son los objetos que se utilizaran en el desarrollo de la aplicación.

## 3. Glosario de Términos

El glosario de términos permitirá a los lectores del presente proyecto tener una idea clara de ciertas palabras, términos básicos o compuestos que se utilizan en la documentación y en el desarrollo del proyecto. Este se encontrará màs adelante.

## 4. Tarjetas CRC

Las tarjetas CRC (Clase-Responsabilidad-Colaboración), es una técnica sencilla que permite al programador centrarse en el desarrollo orientado a objetos, creada por Ward Cunningham y Kent Beck.

- ✓ Cada tarjeta CRC representa un objeto, la clase a la que pertenece el objeto se puede escribir en la parte de arriba de la tarjeta, en la columna izquierda se puede escribir las responsabilidades que debe cumplir el objeto y a la derecha, las clases de colaboración con cada responsabilidad.

- ✓ Cada tarjeta representara una clase en el sistema. Además de registrar información de las clases (tarjetas CRC), está técnica propone un proceso llamado CRC.

**PROCESO CRC**

Mediante este proceso se investiga una solución orientada a objetos del sistema, permitiendo el pensamiento creativo a través de la interacción con las personas del grupo de trabajo.

El proceso CRC ayuda a:

- ✓ Identificar las clases que participan del diseño del sistema.
- ✓ Obtener responsabilidades que deberá cumplir cada clase
- ✓ Establecer como colabora una clase con otras clases para cumplir con sus responsabilidades.

Los pasos que se debe seguir para llenar una tarjeta CRC son:

- ✓ Encontrar clases
- ✓ Encontrar responsabilidades
- ✓ Definir colaboradores
- ✓ Definir casos de uso(situaciones potenciales)
- ✓ Disponer de las tarjetas.

| CRC <<Nro. Tarjeta>>: <<Nombre de la Clase>> | |
|---|---|
| Responsabilidades | Colaboradores |

**Tabla 3. Modelo e Tarjeta CRC en blanco**

**Tarjetas CRC para SYSCORTI (**Sistema Web para el Control de los Recursos de Tecnología de la Información de Hospital Isidro Ayora-Loja**).**

| **CRC 3.1: Clase Usuario** | |
|---|---|
| ✓ Usando el método **crearUsuario()**, se creara un único usuario con privilegios de administrador u otros de tipo usuario invitado.<br>✓ Usando el método **modificarUsuario(),** se podrá cambiar o modificar la información de los datos del usuario administrador o de usuarios invitados registrados en la base de datos.<br>✓ Usando el método **accesoSYSCORTI(),** el sistema solicitara el nombre de usuario y password, luego verifica y valida el nombre de usuario y password ingresado,<br>o Si el nombre pertenece a usuario administrador y la validación es correcta el sistema presenta la ventana que contiene el mensaje de Bienvenida a **"SYSCORTI"** que permite acceder a todos los módulos del sistema. O si el nombre pertenece a usuario invitado y la validación es correcta el sistema presenta la ventana que contiene el mensaje de Bienvenida a **"SYSCORTI"** que permite acceder a todos los módulos del sistema excepto el de administración.<br>o Caso contrario si la validación de datos es incorrecta el sistema bloquea los campos de nombre y password en la clase usuario. | |

| CRC 3.2: Clase Inventario | |
|---|---|
| ✓ Cargar el inventario de recursos TI que se encuentra en la base de datos, para ello utilizaremos el método **inventarioT().**<br>✓ Permitir el ingreso de datos generales de los recursos TI (pc's, laptops, servidores y elementos de telecomunicaciones) adquiridos por la institución, para ello utilizaremos el método **crearInventario().**<br>✓ Permitir la modificación de datos generales de los recursos TI (pc's, laptops, servidores y elementos de telecomunicaciones) adquiridos por la institución para ello utilizaremos el método **modificarInventario().** | **Custodio Departamento** |

| CRC 3.3: Clase Componente_Equipo | |
|---|---|
| ✓ Permitir el ingreso de los distintos componentes del Equipo, mediante el método **crearCompEquipo().**<br>✓ Permitir la modificación de las características de los compontes, para ello utilizaremos el método **modificarCompEquipo().** | **Equipo** |

| CRC 3.4: Clase Software_Equipo | |
|---|---|
| ✓ Cargar las características de componentes TI que se encuentra en la base de datos, para ello utilizaremos el método **softwareEquipo().**<br>✓ Permitir el ingreso de las características de los componentes TI (pc's, laptops, servidores y elementos de telecomunicaciones) adquiridos por la institución, para ello utilizaremos el método **crearSoftEqui().**<br>✓ Permitir la modificación de las características del software de los equipos (pc's, laptops, servidores y elementos de telecomunicaciones), para ello utilizaremos el método **modificarSoftEqui().** | **Equipo** |

| CRC 3.5: Clase Custodio | |
|---|---|
| ✓ Cargar las características del Custodio que se encuentra en la base de datos, para ello utilizaremos el método **custodio().**<br>✓ Permitir el ingreso de las características del Custodio, para ello utilizaremos el método **crearCustodio().**<br>✓ Permitir la modificación de las características del custodio, para ello utilizaremos el método **modificarCustodio().** | **Administrativo**<br>**Inventario** |

| CRC 3.6: Clase Administrativo | |
|---|---|
| ✓ Cargar los datos del empleado que se encuentra en la base de datos, para ello utilizaremos el método **administrativo().**<br>✓ Permitir el ingreso de los datos de los empleados administrativos de la institución, para ello utilizaremos el método **crearA().**<br>✓ Permitir la modificación de los datos de los empleados administrativos, para ello utilizaremos el método **modificarA()**. | **Departamento** |

| CRC 3.7: Clase Departamento | |
|---|---|
| ✓ Cargar las características del departamento que se encuentra en la base de datos, para ello utilizaremos el método **departamento().**<br>✓ Permitir el ingreso de las características del departamento, para ello utilizaremos el método **crearD().**<br>✓ Permitir la modificación de las características del departamento, para ello utilizaremos el método **modificarD().** | |

| CRC 3.8: Clase Proveedor | |
|---|---|
| ✓ Cargar los datos del proveedor que se encuentra en la base de datos, para ello utilizaremos el método **proveedor().**<br>✓ Permitir el ingreso de los datos de los proveedores para ello utilizaremos el método **crearP1()**.<br>✓ Permitir la modificación de los datos de los proveedores para ello utilizaremos el método **modificaP()**. | |

| CRC 3.9: Clase Hoja_Trabajo | |
|---|---|
| ✓ Cargar los datos de la tabla hoja_trabajo que se encuentra en la base de datos, para ello utilizaremos el método **hoja_trabajo1().**<br>✓ Permitir el ingreso de los datos del mantenimiento para ello utilizaremos el método **crearHoja_T()**.<br>✓ Si el Administrador, remplazo algún componente de Equipo, deberá modificar componente de equipo en el módulo Equipo.<br>✓ Permitir la modificación de los datos de Mantenimiento para ello utilizaremos el método **modificarHT()**. | **Inventario**<br>**Equipo**<br>**Recurso_TI**<br>**Componente_Equipo**<br>**Software_Equipo** |

| CRC 3.10: Clase Movimiento_Interno | |
|---|---|
| ✓ Cargar los datos de la tabla movimiento_Interno, para ello utilizaremos el método **movimiento_Interno().**<br>✓ Permitir el ingreso de los datos del movimiento interno para ello utilizaremos el método **crearMovimiento_I().**<br>✓ Si el Administrador, realiza el movimiento interno del activo fijo, deberá modificar los datos en la tabla **Inventario.**<br>✓ Permitir la modificación de los datos del movimiento interno, utilizaremos el método **modificarM_I().** | **Inventario** |

| CRC 3.11: Clase Salida_Equipo | |
|---|---|
| ✓ Cargar los datos de la tabla salida_Equipo, para ello utilizaremos el método **salidaEquipo().**<br>✓ Permitir el ingreso de los datos del movimiento externo para ello utilizaremos el método **crearSalidaE().**<br>✓ Permitir la modificación de los datos de la tabla salida_Equipo para ello utilizaremos el método **modificarSalida_E().** | **Inventario** |

| CRC 3.12: Clase Almacen_RecursosTI | |
|---|---|
| ✓ Cargar los datos del almacén de TI que se encuentran en la base de datos, para ello utilizaremos el método: **AlmacenRTI().**<br>✓ Permitir el ingreso de los datos del almacén de TI para ello utilizaremos el método: **crearAlmacen_recursosTIC().**<br>✓ Permitir la modificación de los datos del almacén de TI para ello utilizaremos el método: **modificarAlmacenR_TIC()** | **Inventario** |

| CRC 3.13: Clase Contacto | |
|---|---|
| ✓ Cargar los datos del contacto que se encuentran en la base de datos, para ello utilizaremos el método: **contacto().**<br>✓ Permitir el ingreso de los datos de contacto del administrativo para ello utilizaremos el método: **crearContacto().**<br>Permitir la modificación de los datos de contacto del administrativo para ello utilizaremos el método: **modificar Contacto()** | **Administrativo** |

| CRC 3.14: Clase Reportes | |
|---|---|
| ✓ Cargar reportes con la clase **ReportesPDFPersonalizados** y con el método **GenerarPDF().**<br>✓ Si la opción de reporte es Inventario, usamos el método: **GenerarPDFInventario().**<br>✓ Si la opción de reporte es mantenimiento Equipos usamos el método: **GenerarPDFHojatrabajo().**<br>✓ Si la opción de reporte es determinar características mínimas para comprar recursos de TI (pc´s,laptops,servidores, Switch,Ruteadores) usamos el método: **GenerarPDFCompras().**<br>✓ Si la opción de reporte es Custodio de recursos de TI usamos el método: **GenerarPDFCustodio().**<br>✓ Si la opción de reporte es Movimiento Interno de Equipo usamos el método: **movimientoI_PLANTILLA().**<br>✓ Si la opción de reporte es Movimiento Externo de Equipo usamos el método: **salidaE_PLANTILLA().** | **Inventario**<br>**Proveedor**<br>**Administrativo**<br>**Movimiento_Interno**<br>**Movimiento_Externo**<br>**Custodio**<br>**Hoja_Trabajo** |

| CRC 3.15: Clase RespaldoBDD | |
|---|---|
| ✓ Acceder al archivo de la Base de Datos usando el método: **verArchivoBaseDatos()**<br>✓ Crear el respaldo de Base de Datos usando el método: **guardarArchivoBaseDatos()** | |

| CRC 3.16: Clase Equipo | |
|---|---|
| ✓ Cargar los datos del Equipo que se encuentra en la base de datos, para ello utilizaremos el método **equipo().**<br>✓ Permitir el ingreso de los datos de los equipos para ello utilizaremos el método **crearEquipo().**<br>✓ Permitir la modificación de los datos de los equipos para ello utilizaremos el método **modificarEquipo().** | **Proveedor**<br>**Inventario**<br>**Componente_Equipo**<br>**Software_Equipo** |

| CRC 3.17: Clase Software | |
|---|---|
| ✓ Cargar los datos del Software que se encuentra en la base de datos, para ello utilizaremos el método **software().**<br>✓ Permitir el ingreso de los datos del software para ello utilizaremos el método **crearSoftware()**.<br>✓ Permitir la modificación de los datos del software para ello utilizaremos el método **modificarSoftware().** | **Proveedor**<br>**Inventario** |

| CRC 3.18: Clase Log | |
|---|---|
| ✓ El administrador será el encargado de administrar esta clase dependiendo del usuario que acceda al sistema, el tendrá que ingresar primeramente la información referente al usuario para darle los permisos de lectura o de escritura. | **Usuario** |

## 5. Soluciones Puntuales

Una vez que se ha analizado como se administran los recursos de TI en la institución y que los requerimientos del cliente han sido revisados se ha procedido a establecer las soluciones puntuales que el sistema debe cumplir:

- ✓ Permitir al administrador del centro de cómputo del HGPIA-Loja:

  - Manejar los datos de los recursos de TI.
  - Guardar respaldos de las base de datos con extensión sql del servidor Centos.
  - Manejar los datos del custodio o responsable de los recursos de TI
  - Manejar los registros del mantenimiento físico o lógico de las pc's, laptops, servidores, ruteadores y switch, etc.
  - Manejar los datos del movimiento interno y externo de los recursos de TI.
  - Actualizar los archivos.doc de características mínimas de los recursos de TI.

- ✓ Generar reportes sobre:

  - Inventario de recursos de TI
  - Mantenimiento equipos
  - Custodio de equipos
  - Proveedores
  - Equipos que han sido movidos internamente
  - Equipos que han sido sacados de la Institución.
  - Equipos con sus características de hardware y software
  - Software de la Institución

## 6. Funcionalidad Mínima

Para establecer la funcionalidad mínima del sistema, es importante analizar cuáles son las necesidades de la institución con respecto a la administración de los recursos

de TI, para lo cual se debe tratar especialmente con la persona que interviene directamente en la administración de los recursos, en este caso es el Administrador del Centro de Cómputo del Hospital Isidro Ayora.

Una vez que se ha conversado con el Administrador en base a los requerimientos del sistema, ya se puede determinar la funcionalidad mínima de nuestro sistema, cuyo objeto principal es administrar adecuadamente los datos de los recursos de TI de la Institución, y entregar los respectivos reportes para corroborar la existencia física y estado de cada uno de los equipos informáticos dentro del Hospital.

## 6.1. Arquitectura del Sistema

Para el desarrollo del software se ha definido la Arquitectura de N-Capas, por las grandes ventajas que representa, puesto que permite crear sistemas escalables y seguros, así también se consideró la Arquitectura Cliente Servidor en vista de que se trata de una aplicación Web.

En las gráficas que mostraremos a continuación, se representa el esquema de la arquitectura N-Capas y la arquitectura Funcional del Sistema.


**Gráfico 2. Arquitectura Funcional del Sistema**

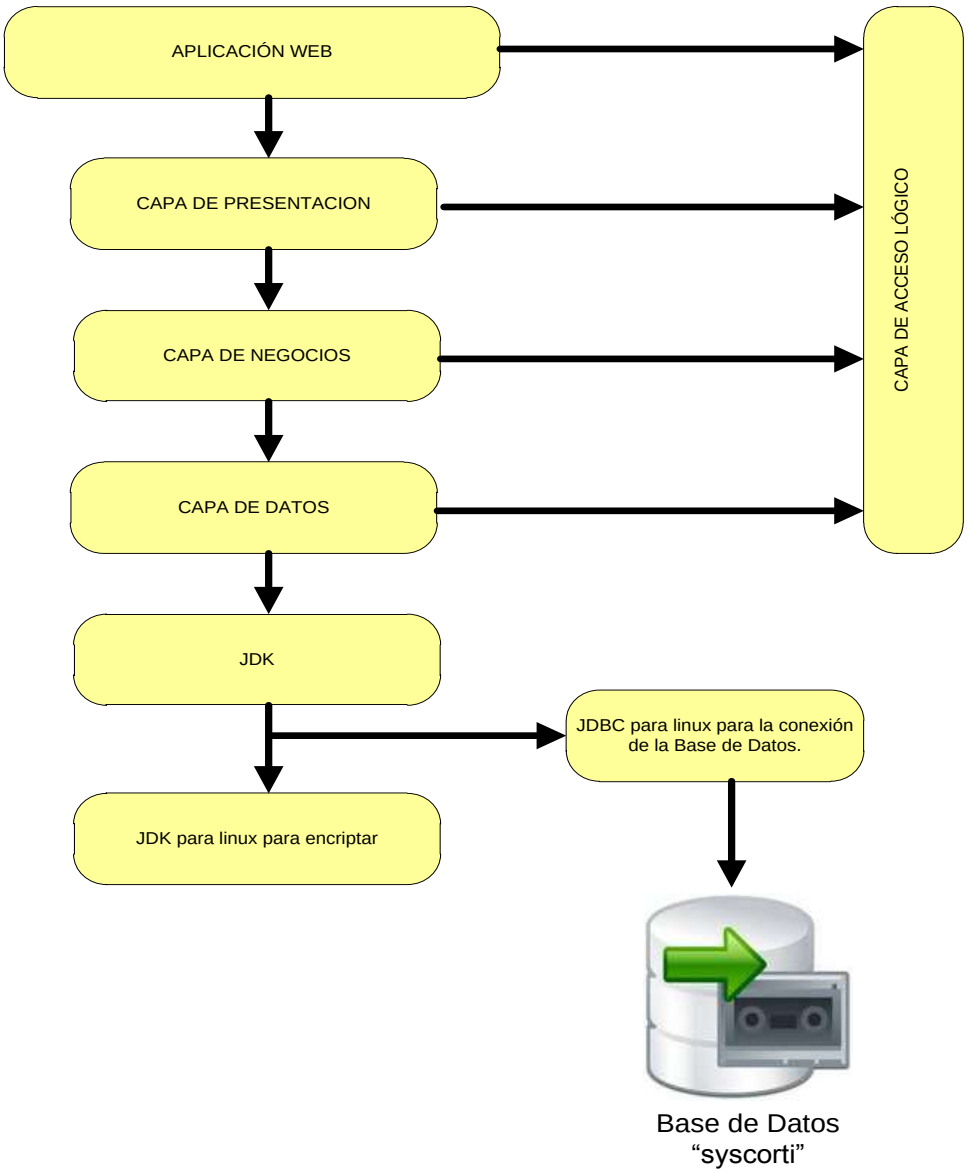



**Gráfico 3. Arquitectura N-Capas**

## 6.2. Capa de Presentación

Es la capa que ve el usuario, presenta el sistema al usuario (la interfaz de portal web y de la aplicación SYSCORTI), le comunica la información y captura la información del usuario en un mínimo de proceso (realiza un filtrado previo para comprobar que no

hay errores de formato). Esta capa se comunica únicamente con la capa de negocio. También es conocida como interfaz gráfica y debe tener la característica de ser "amigable" (entendible y fácil de usar) para el usuario.

### 6.3. Capa de Negocio

Es la capa donde reside la aplicación, se reciben las peticiones del usuario y se envían las respuestas tras el proceso. Se denomina capa de negocio (e incluso de lógica del negocio) porque es aquí donde se establecen todas las reglas que deben cumplirse. Esta capa se comunica con la capa de presentación, para recibir las solicitudes y presentar los resultados, y con la capa de datos, para solicitar al gestor de base de datos para almacenar o recuperar datos de él.

### 6.4. Capa de Datos

Es la capa donde residen los datos y es la encargada de acceder a los mismos. Está formada por uno o más gestores de bases de datos que realizan todo el almacenamiento de datos, reciben solicitudes de almacenamiento o recuperación de información desde la capa de negocio.

## 7. Diseño del Portal Web

### 7.1 Metodología[7]

Nuestra página o sitio Web, muestra la imagen de nuestro negocio hacia el mundo, por ello el proceso de creación y explotación de nuestro sitio Web requiere de una metodología contrastada y bien definida.

La figura siguiente muestra una metodología que nos permitirá alcanzar las expectativas de nuestro sitio Web:

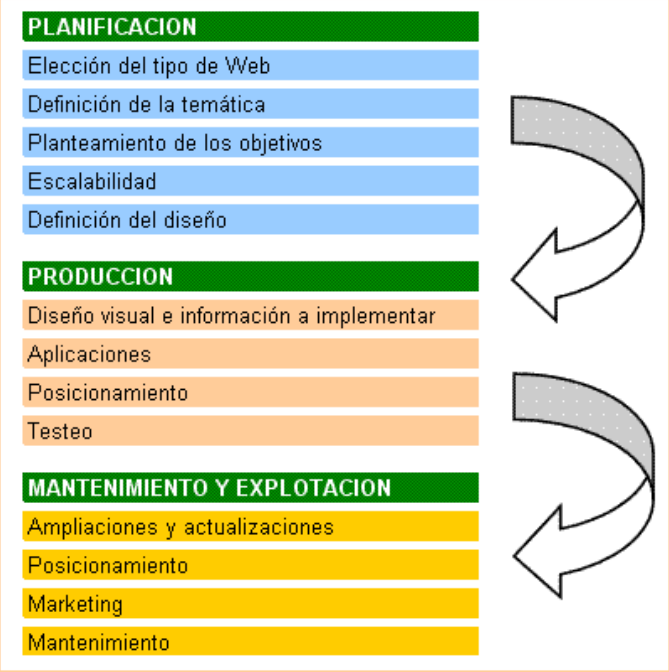



**Gráfico 4. Metodología del diseño de páginas Web.**

7. http://www.webandmacros.com/Diseno_web_metodologia.htm. **Metodología diseño páginas web. 2006-2009**

## PLANIFICACIÓN DEL SITIO O PÁGINA WEB

✓ Elección del tipo de Web

Lo primero que se ha de decidir es el tipo de Web que queremos crear, es el punto de partida que afecta a todas las etapas posteriores de creación, realizaremos un diseño, aplicaciones, navegabilidad... adecuadas al tipo de Web seleccionada.

Ejemplos:

- Sitio Web comercial.
- Sitio Web profesional.
- Sitio Web de información.
- Sitio Web de ocio.

Para nuestro caso se trata de una página Web de tipo Informativo, en la que queremos dar a conocer información con respecto al servicio que ofrece el Hospital General Isidro Ayora de la Ciudad de Loja.

✓ Definición de la Temática

En este punto se va a definir los temas que se van a exponer en el sitio Web, permitiendo definir términos claves de búsqueda para posteriormente realizar una metodología de posicionamiento:

- Sitio Web de información de los servicios que ofrece el HPGIA-Loja.

✓ Planteamiento de objetivos

Se plantean los objetivos por los cuales se crea el sitio web, para luego fijar estrategias funcionales que permitan alcanzar los objetivos propuestos.

- Dar a conocer la Historia del Hospital Isidro Ayora-Loja
- Dar a conocer la Misión y Visión de la Institución.
- Dar a conocer los Servicios de Salud que presta la Institución.
- Dar a conocer los Programas de Salud que maneja.
- Dar a conocer la Ley de Transparencia que rige a los Hospitales Públicos.

✓ Escalabilidad

Se define como las visiones a corto y largo plazo acerca de nuestro sitio Web, si a lo largo del tiempo queremos ampliar nuestro sitio Web con nuevas aplicaciones, nuevas páginas, actualizaciones constantes.

✓ Definición del diseño

Dependiendo del tipo de Web, la temática seleccionada, los objetivos planteados y la escalabilidad definida, estamos preparados para definir sobre papel el diseño de la Web, incluyendo los fondos, tipos de letras, botones, formularios, links, plantillas, aplicaciones… de tal forma que obtengamos "storyboard" de los elementos y diseño que queremos implementar en nuestro sitio Web.

**PRODUCCIÓN Y CREACIÓN DEL SITIO O PÁGINA WEB.**

- ✓ Diseño visual y creación de la información a implementar

  Creación del esqueleto de la Web, tablas, encabezados, espacio para imágenes, texto, botones...

  Creación de las imágenes que acompañara a nuestro sitio Web, logos, cabeceras, fotografías, además del proceso concepción y materialización de la información que se va a ofrecer.

- ✓ Aplicaciones Web

  Creación de enlaces entre nuestro sitio Web y la aplicación SYSCORTI.

- ✓ Posicionamiento

  Una vez que nuestro sitio Web ha sido terminado, es importante establecer una metodología que nos ayude a definir cómo nuestro sitio web puede aparecer en las primeras posiciones en los buscadores. Para esto se puede inscribir la página web en buscadores importantes como: google, yahoo, altavista, etc., los mismos que usan palabras claves de búsqueda.

- ✓ Testeo

  Consiste en realizar pruebas de nuestro sitio Web para comprobar la navegabilidad y su correcto funcionamiento. Es importante que nuestra página muestre una imagen positiva a sus visitantes.

**MANTENIMIENTO Y EXPLOTACIÓN DEL SITIO O PÁGINA WEB.**

- ✓ Ampliaciones y actualizaciones

  Es muy importante actualizar la información que nuestra página muestra, puesto que ayuda a que los usuarios en-línea se mantengan enterados de todas las novedades actuales de la institución con respecto a servicios y programas de salud que ofrece.

- ✓ Posicionamiento

  Mantener una página posicionada requiere de implementar una metodología: que permita ampliar y actualizar el sitio web, dar un adecuado mantenimiento y emplear estrategias de marketing para darlo a conocer.

- ✓ Marketing

  La estrategia de mercado que utilizaremos para dar a conocer nuestro sitio web es a través de: publicaciones en periódicos, hojas volantes, radio y mensajes de correo electrónico.

- ✓ **Mantenimiento**

  Realizar un programa de mantenimiento para que nuestro Sitio Web funcione durante su existencia.

## 7.2 Estructura del Sitio WEB

**Menú Principal**

Nuestro Sitio Web contendrá los siguientes links:

HISTORIA
MISIÓN Y VISIÓN
SERVICIO QUE OFRECE
PROGRAMAS
LEY DE TRANSPARENCIA
CONTACTOS
SYSCORTI

**Contenido por Páginas**

**HISTORIA**

Esta página mostrará información de los antecedentes Históricos de la institución y una imagen de cómo se ve actualmente.

**MISIÓN Y VISIÓN**

Esta página mostrará información de la Misión y Visión del Hospital Isidro Ayora Loja.

**SERVICIO QUE OFRECE**

Esta página mostrará información de los Servicios que ofrece la institución y la galería de imágenes. Se mostrara información de cada servicio de acuerdo al link seleccionado.

**PROGRAMAS**

Esta página mostrará información del Programa de “Plan de Mejoramiento y Desarrollo Institucional”.

**LEY DE TRANSPARENCIA**

Esta página mostrará información de la ley de transparencia que rige a las Instituciones de Salud Pública.

**CONTACTOS**

Esta página mostrará información de la ubicación y teléfonos de la institución.

**SYSCORTI**

En esta página se mostrará información de cómo funciona la aplicación Syscorti y cuáles son los requisitos previos para su uso.

### 7.3 Diagramación de Páginas

Es la manera de distribuir organizadamente sobre nuestra página web los elementos o componentes que la conforman. La estructura esquematizada de nuestro sitio web ha sido fragmentada en 3 tablas.

### Página Principal

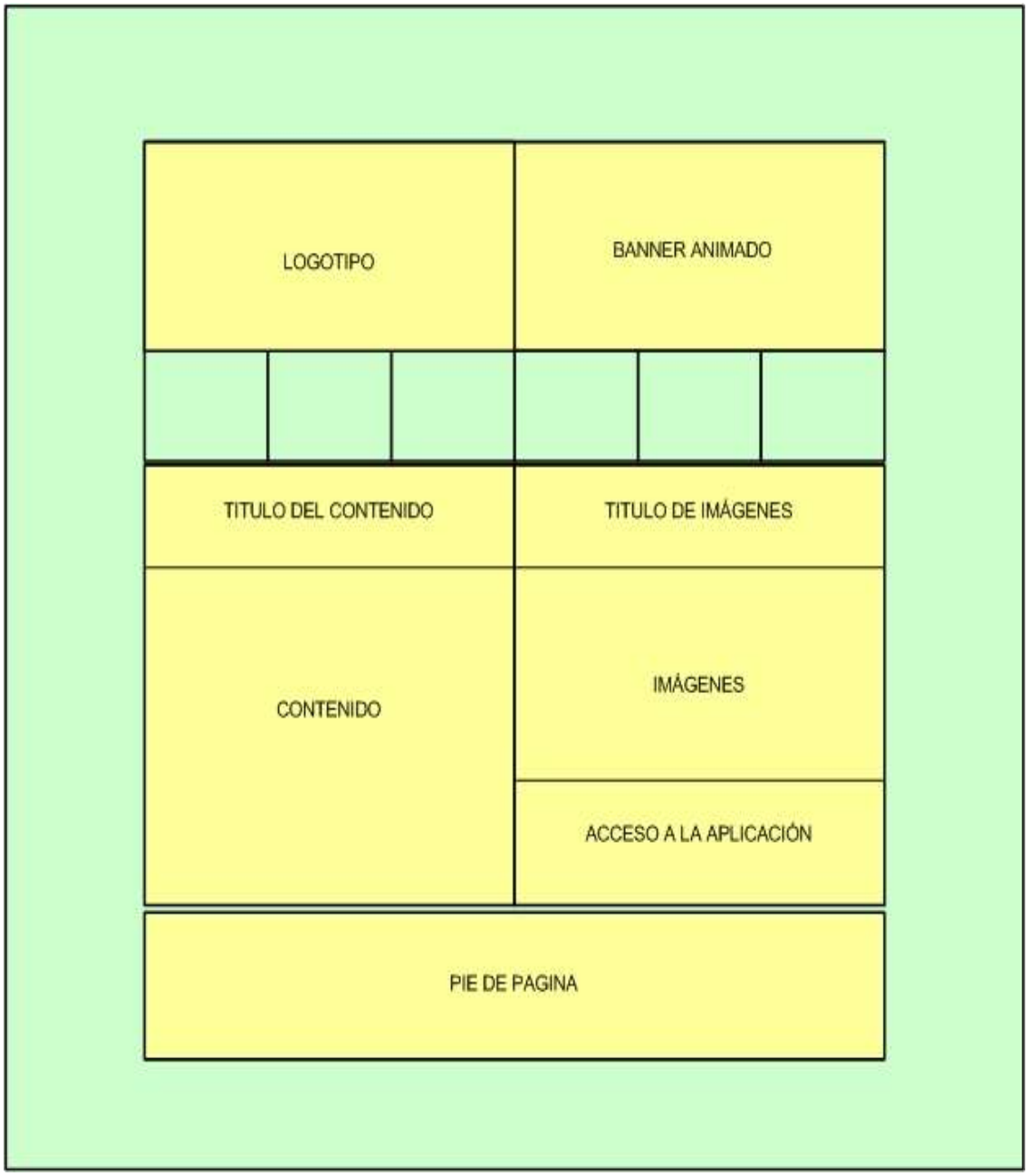



**Gráfico 5: Diagramación del Portal Web**

En el gráfico 5 se puede ver que el Portal Web está construido en base a tres tablas, de acuerdo al siguiente orden:

- ✓ **Tabla 1:** Muestra el Nombre y Logotipo de la Institución, el Menú Principal y una Animación.

- ✓ **Tabla 2:** Muestra al lado izquierdo el título y contenido que tiene relación con link seleccionado y al lado derecho muestra una galería de imágenes en un formato jpg. Además muestra el link de acceso a SYSCORTI.

- ✓ **Tabla 3:** Muestra la dirección, números de teléfonos, link del correo electrónico, nombre del portal web y horarios de atención de la institución.

**Páginas Secundarias**

La estructura esquematizada de nuestro sitio web ha sido fragmentada en 3 tablas igual que en la página principal. Ver gráfico 12.

- ✓ **Tabla 1:** Similar que la diagramación de la Página Principal.
- ✓ **Tabla 2:** Similar que la diagramación de la Página Principal.
- ✓ **Tabla 3:** Similar que la diagramación de la Página Principal.

## 7.4 Diseño Imágenes

Las imágenes que se ubican en un sitio web, deben tener una buena aceptación por parte del usuario, es por ello que es importante retocar las imágenes que se utilizaran. La herramienta que se usara para el retocado de imágenes que se colocaran en el portal Web es Adobe Phothoshop CS4, este permite editar, diseñar, retocar fotografías y la pintura base de imágenes de mapa de bits.

## 7.5 Diseño de Páginas

Para el diseño del portal Web se utilizó la herramienta Joomla, esta permite administrar toda la información publicada en las páginas desde un navegador web, dando lugar al fácil mantenimiento de sitio.

## 7.6 Incorporación Multimedia

Para incorporar imágenes animadas al portal, y darle una mejor presentación se lo hace mediante la plantilla preestablecida de Joomla 1.5.22 en español.

## 7.7 Descripción de cada Página

**INICIO**

Muestra en la parte superior el nombre de la institución, un banner con imágenes y los respectivos links del sitio web informativo.

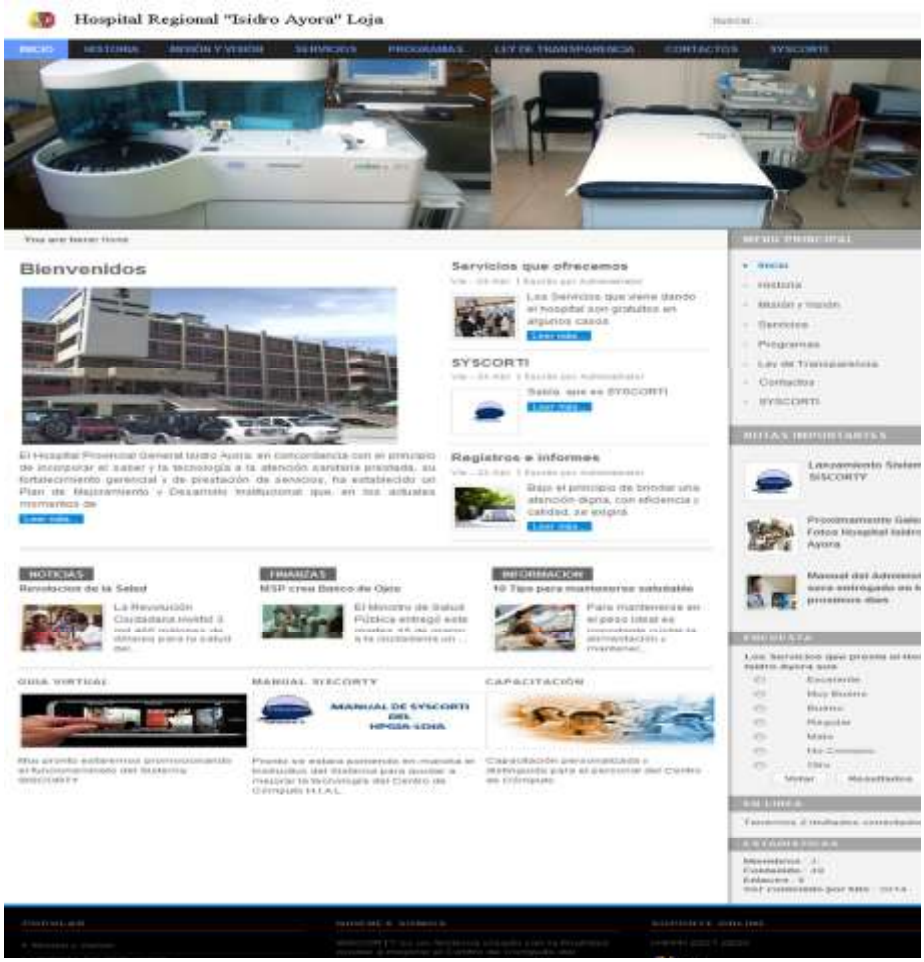



**Gráfico 6.** Página Inicio

## HISTORIA

Muestra información de la historia y datos generales del HPGIA-Loja.

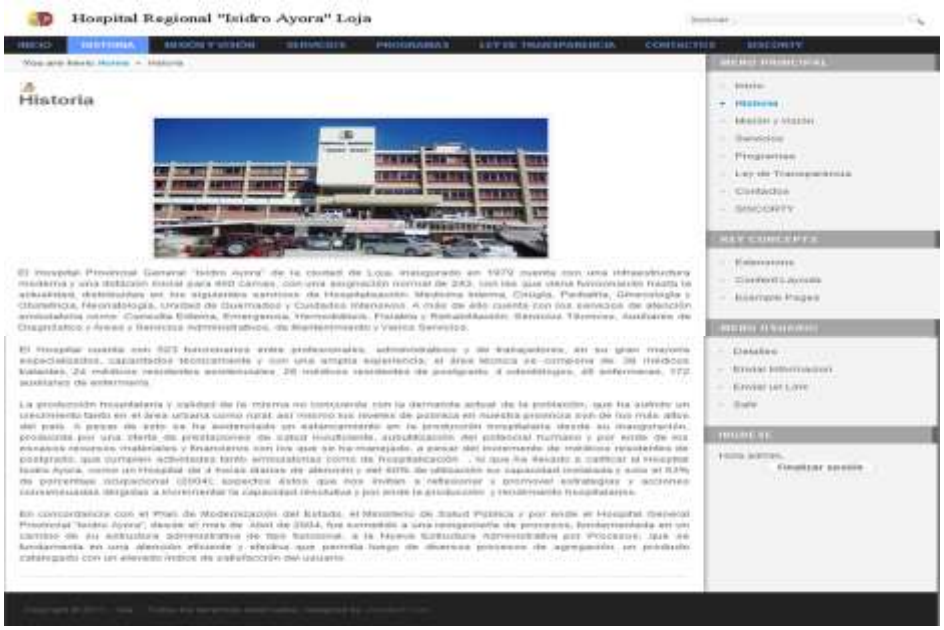



**Gráfico 7.** Página Historia

## MISIÓN Y VISIÓN

Muestra información de la misión y visión del HPGIA-Loja.

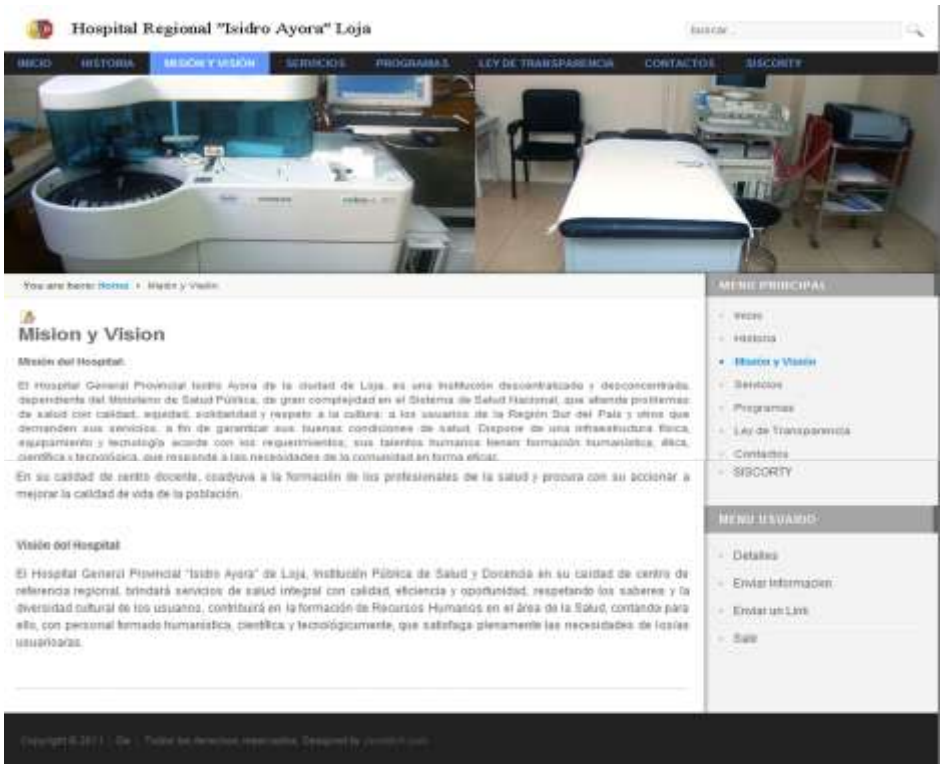



**Gráfico 8.** Página Misión y Visión

## SERVICIOS

Muestra información de los servicios que presta el HPGIA-Loja; así como también los links para acceder a la información de cada uno de los servicios que ofrece.


**Gráfico 9.** Página Servicios HPGIA-Loja

## PROGRAMAS

Muestra información del programa “Plan de Mejoramiento y Desarrollo Institucional”, del HPGIA-Loja.


**Gráfico 10.** Página Programas

## LEY DE TRANSPARENCIA

Muestra información sobre la ley de transparencia que rige a las instituciones de salud pública.


**Gráfico 11.** Página Ley de Transparencia

## CONTACTOS

Muestra información de la ubicación y teléfonos del HPGIA-Loja.


**Gráfico 12.** Página Contactos

**SYSCORTI**

Muestra información general de cómo usar “Syscorti; así como cuáles son los requerimientos mínimos para ejecutar la aplicación en una máquina remota, al lado derecho de la página esta la sección para que el usuario se registre y pueda acceder a la descarga de la aplicación “Syscorti”

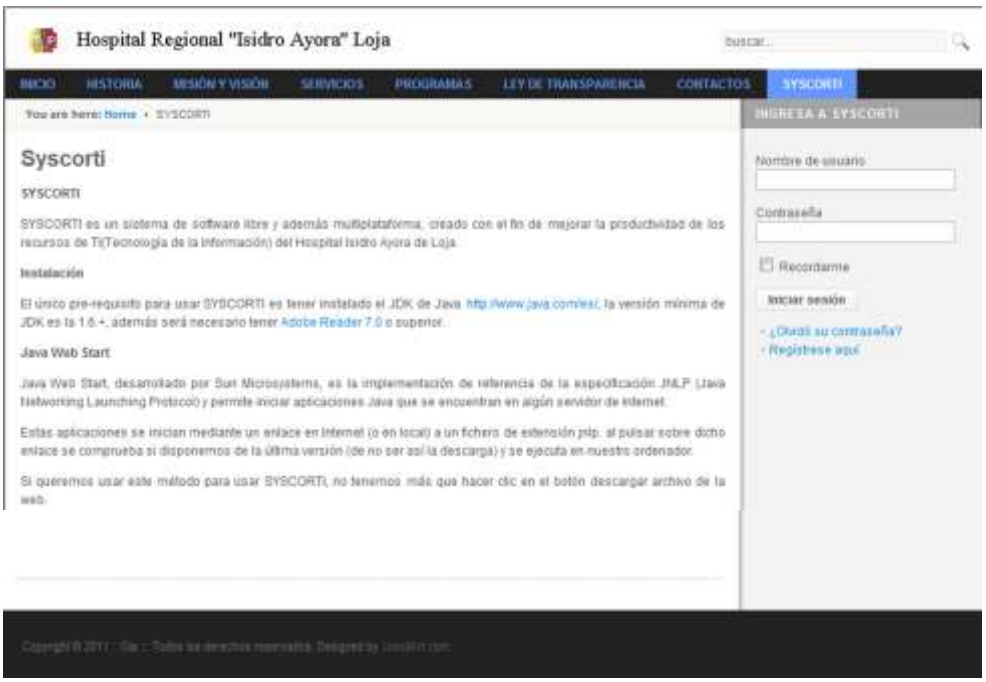



**Gráfico 13.** Página SYSCORTI (Registrar)

Luego del registro del usuario se muestra en la página un botón para hacer la descarga de la aplicación Syscorti.


**Gráfico 14.** Página SYSCORTI (Descargar Aplicación)

## 8. Diseño de la Base de Datos[8]

El proceso de diseño de una base de datos se guía por algunos principios. El primero de ellos es que se debe evitar la información duplicada o, lo que es lo mismo, los datos redundantes, porque malgastan el espacio y aumentan la probabilidad de que se produzcan errores e incoherencias. El segundo principio es que es importante que la información sea correcta y completa. Si la base de datos contiene información incorrecta, los informes que recogen información de la base de datos contendrán también información incorrecta y, por tanto, las decisiones que tome a partir de esos informes estarán mal fundamentadas.

Un buen diseño de base de datos es, por tanto, aquél que:

- Divide la información en tablas basadas en temas para reducir los datos redundantes.
- Ayuda a garantizar la exactitud e integridad de la información.
- Satisface las necesidades de procesamiento de los datos y de generación de informes.

El nombre de la base de datos para nuestra aplicación es **isidro_syscorti,** está almacenará toda la información de los recursos de TI del Hospital Isidro Ayora, contendrá todas las tablas y procedimientos almacenados que utiliza la aplicación “SYSCORTI”. Las tablas y procedimientos se detallan desde las páginas 240 a la 245.

El servidor de base de datos es MySQL SERVER 5.0, por la compatibilidad con la tecnología de desarrollo java a utilizar.

8. http://office.microsoft.com/es-ar/access-help. **Conceptos básicos del diseño de una base de datos**

## 9. Diagrama de Clases[9]

Un diagrama de clases es un tipo de diagrama estático que describe la estructura de un sistema mostrando sus clases, atributos y las relaciones entre ellos. Los diagramas de clases son utilizados durante el proceso de análisis y diseño de los sistemas, donde se crea el diseño conceptual de la información que se manejará en el sistema, y los componentes que se encargarán del funcionamiento y la relación entre uno y otro. Ver el diagrama de clases en la pág. 243

9. http://es.wikipedia.org/wiki/ Diagrama de claes. **2011**

# 10. Diseño de la Aplicación

Una vez que se ha reunido toda la información, los requerimientos del software han sido levantados, se ha realizado la planificación del proyecto y se ha establecido los objetivos a alcanzar, se procede a realizar el diseño de la aplicación, para más adelante proceder a implementarla en el entorno Java.

Para poder ingresar a la aplicación se describen las siguientes acciones de manera general:

- Desde el portal Web el usuario descarga la aplicación "SYSCORTI" y la ejecuta en su máquina cliente, para el ingreso a la aplicación se muestra la ventana de Autentificación de Usuario.
- Seguidamente se muestra, si se trata del usuario Administrador la Ventana Principal 1 que contiene todos los módulos de la Aplicación o sino para el Usuario Invitado la Ventana Principal 2 que contiene ciertos módulos de la Aplicación.
- Las acciones se realizaran según los permisos asignados a cada tipo de usuario, tomando en cuenta que el administrador es el único que puede acceder a todos los módulos del sistema.

## 10.1 Desarrollo de la Interfaz de Usuario

La aplicación comprende de las ventanas que se muestran a continuación:

**MÓDULO DE ACCESO AL SISTEMA**

**VENTANA ADMINISTRAR USUARIO**

En esta ventana se valida el ingreso del usuario al Sistema.


**Gráfico 15.** Administrar Usuario

**VENTANA PRINCIPAL 1:**

En esta ventana el administrador tiene acceso a todo los módulos del sistema SYSCORTI (Administrativo, Inventario, Mantenimiento, Respaldo BDD, Activos, Movimiento, Reportes).


**Gráfico 16.** Ventana Principal 1

**VENTANA PRINCIPAL 2:**

En esta ventana el usuario invitado tiene acceso a los módulos: Inventario, Mantenimiento, Respaldo BDD, Activos, Movimiento, Reportes, excepto al módulo Administrativo.


**Gráfico 17.** Ventana Principal 2

## MÓDULO ADMINISTRATIVO

### VENTANA MÓDULO ADMINISTRATIVO

En esta ventana el sistema muestra el menú para agregar y modificar datos de Departamento, Administrativo, Custodio, Usuario, Contacto, Rol de Usuario y Proveedor.


**Gráfico 18.** Ventana Administrativo

### VENTANA AGREGAR USUARIO

En esta ventana el administrador puede crear usuarios de tipo administrador y usuario invitado.


**Gráfico 19.** Ventana Agregando Usuario

## VENTANA MODIFICAR USUARIO

En esta ventana el adminitrador puede modificar datos de usuarios tipo administrador o usuario invitado.


**Gráfico 20.** Ventana Modificando Usuario

## VENTANA AGREGAR ADMINISTRATIVO

En esta ventana el administrador puede agregar datos de personal administrativo.


**Gráfico 21.** Ventana Agregando Administrativo

## VENTANA MODIFICAR ADMINISTRATIVO

En esta ventana el administrador puede modificar datos de personal administrativo.


**Gráfico 22.** Ventana Modificando Administrativo

## VENTANA AGREGAR PROVEEDOR

En esta ventana el administrador puede agregar datos de proveedor.


**Gráfico 23.** Ventana Agregando Proveedor

**VENTANA MODIFICAR PROVEEDOR**

En esta ventana el administrador puede modificar datos de proveedor.


**Gráfico 24.** Ventana Modificando Proveedor

**VENTANA AGREGAR CUSTODIO**

En esta ventana el administrador puede agregar datos de custodio.


**Gráfico 25.** Ventana Agregando Custodio

**VENTANA MODIFICAR CUSTODIO**

En esta ventana el administrador puede modificar datos de custodio.


**Gráfico 26.** Ventana Modificando Custodio

**VENTANA AGREGAR CONTACTO**

En esta ventana el administrador puede agregar datos de contacto.


**Gráfico 27.** Ventana Agregando Contacto

**VENTANA MODIFICAR CONTACTO**

En esta ventana el administrador puede modificar datos de contacto.


**Gráfico 28.** Ventana Modificando Contacto

**VENTANA AGREGAR DEPARTAMENTO**

En esta ventana el administrador puede agregar datos de departamento.


**Gráfico 29.** Ventana Agregando Departamento

**VENTANA MODIFICAR DEPARTAMENTO**

En esta ventana el administrador puede modificar datos de departamento.


**Gráfico 30.** Ventana Modificando Departamento

**MÓDULO INVENTARIO**

**VENTANA MÓDULO INVENTARIO**

En esta ventana el usuario puede elegir entre las opciones: Consultar Datos del Inventario, Agregar Datos Inventario o Modificar Datos del Inventario.


**Gráfico 31.** Ventana Inventario

**VENTANA CONSULTAR DATOS INVENTARIO**

En esta ventana el sistema muestra un listado de los datos del inventario, además el usuario puede hacer búsquedas específicas ingresando el código de activo fijo del bien y presionando sobre el botón buscar, el sistema presenta información de la búsqueda encontrada.


**Gráfico 32.** Ventana Consultar Inventario

## VENTANA AGREGAR DATOS INVENTARIO

En esta ventana el usuario podrá agregar datos del inventario.


**Gráfico 33.** Ventana Agregando Inventario

### VENTANA MODIFICAR DATOS INVENTARIO

En esta ventana el usuario podrá modificar datos del inventario.


**Gráfico 34.** Ventana Modificando Inventario

## MÓDULO MANTENIMIENTO

### VENTANA MÓDULO MANTENIMIENTO

En esta ventana el sistema muestra el menú para agregar y modificar datos de Mantenimiento (Hoja de Trabajo),


**Gráfico 35.** Ventana Mantenimiento

## VENTANA AGREGAR HOJA_TRABAJO

En esta venta el administrador o usuario invitado puede agregar datos de mantenimiento (hoja-trabajo).


**Gráfico 36.** Ventana Agregando Hoja_Trabajo

## VENTANA MODIFICAR HOJA_TRABAJO

En esta venta el administrador o usuario invitado puede modificar datos de mantenimiento (hoja-trabajo).


**Gráfico 37.** Ventana Modificando Hoja_Trabajo

## MÓDULO REPORTES

En esta ventana el administrador o usuario invitado puede imprimir un reporte de cada uno de los módulos sistema.


**Gráfico 38.** Ventana Reportes

## MÓDULO RESPALDO BDD

En esta ventana el administrador podrá respaldar las bases de datos (mysql) de cualquier aplicación que tenga como motor de BDD mysql.

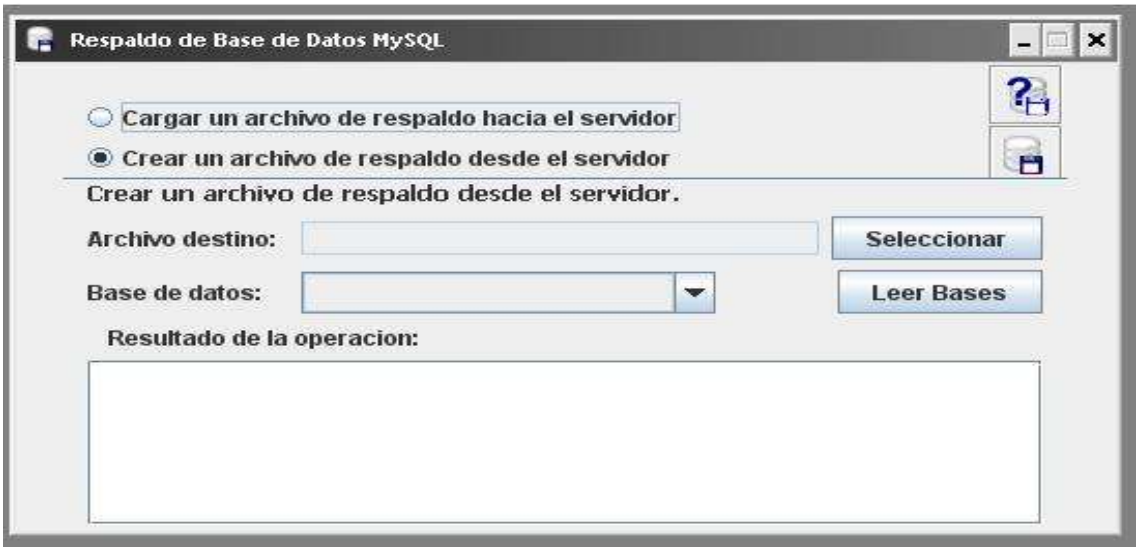



**Gráfico 39.** Ventana Respaldo de Base de Datos MySQL

## MÓDULO ACTIVOS

### VENTANA MÓDULO ACTIVOS

En esta ventana el administrador o usuario invitado, puede elegir para agregar o modificar: Componente Equipo, Software Equipo, Software, Almacén Recursos TI, Equipo.


**Gráfico 40.** Ventana Activos

### VENTANA AGREGAR EQUIPO

En esta ventana el administrador o usuario invitado puede agregar datos de equipo.


**Gráfico 41.** Ventana Agregando Equipo

## VENTANA MODIFICAR EQUIPO

En esta ventana el administrador o usuario invitado puede modificar datos de equipo.


**Gráfico 42.** Ventana Modificando Equipo

## VENTANA AGREGAR COMPONENTE_ EQUIPO

En esta ventana el administrador o usuario invitado puede agregar datos de componente_equipo.


**Gráfico 43.** Ventana Agregando Componente_Equipo

## VENTANA MODIFICAR COMPONENTE_ EQUIPO

En esta ventana el administrador o usuario invitado puede modificar datos de componente_equipo.


**Gráfico 44.** Ventana Modificando Componente_Equipo

## VENTANA AGREGAR SOFTWARE_EQUIPO

En esta ventana el administrador o usuario invitado puede agregar datos de software_equipo.


**Gráfico 45.** Ventana Agregando Software_Equipo

## VENTANA MODIFICAR SOFTWARE_EQUIPO

En esta ventana el administrador o usuario invitado puede modificar datos de software_equipo.


**Gráfico 45.** Ventana Modificando Software_Equipo

## VENTANA AGREGAR SOFTWARE

En esta ventana el administrador o usuario invitado puede agregar software que tiene la institución.


**Gráfico 46.** Ventana Agregando Software

## VENTANA MODIFICAR SOFTWARE

En esta ventana el administrador o usuario invitado puede modificar datos de software que tiene la institución.


**Gráfico 47.** Ventana Modificando Software

## VENTANA AGREGAR ALMACEN TI

En esta ventana el administrador o usuario invitado puede almacenar información de partes o piezas nuevas de recursos TI para mantenimiento.


**Gráfico 48.** Ventana Agregando Almacén TI

### VENTANA MODIFICAR ALMACEN TI

En esta ventana el administrador o usuario invitado puede modificar información de partes o piezas ingresadas al almacén de recursos TI.


**Gráfico 49.** Ventana Modificando Almacén TI

## MODULO MOVIMIENTO

### VENTANA MÓDULO MOVIMIENTO

En esta ventana el sistema muestra el menú para agregar y modificar datos de Movimiento Interno y Salida de Equipos.

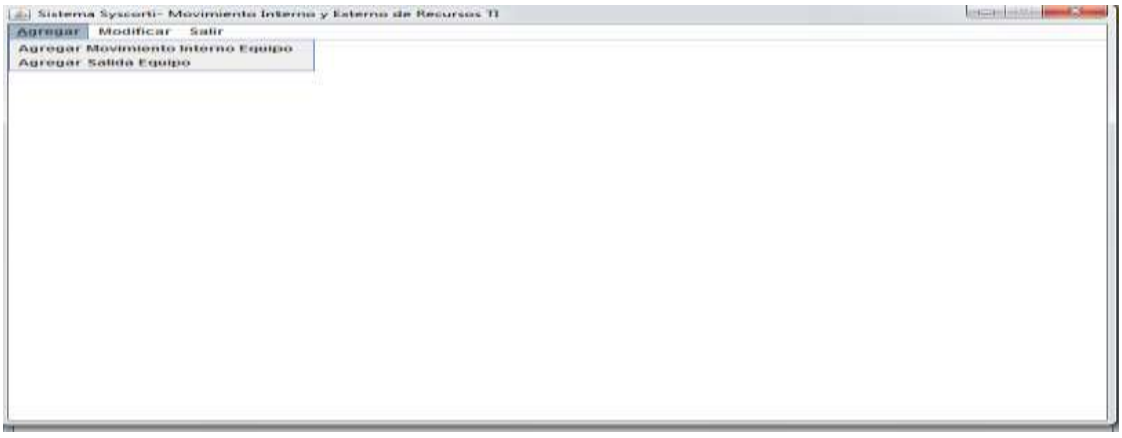



**Gráfico 50.** Ventana Movimiento

**VENTANA AGREGAR MOVIMIENTO INTERNO**

En esta ventana el administrador o usuario invitado puede agregar datos de movimiento interno de equipo.


**Gráfico 51.** Ventana Agregando Movimiento Interno

**VENTANA MODIFICAR MOVIMIENTO INTERNO**

En esta ventana el administrador o usuario invitado puede modificar datos de movimiento interno de equipo.


**Gráfico 52.** Ventana Modificando Movimiento Interno

**VENTANA AGREGAR SALIDA EQUIPO**

En esta ventana el administrador o usuario invitado puede agregar datos de salida de equipo.


**Gráfico 53.** Ventana Agregando Salida Equipo

**VENTANA MODIFICAR SALIDA EQUIPO**

En esta ventana el administrador o usuario invitado puede modificar datos de salida de equipo.


**Gráfico 54.** Ventana Modificando Salida Equipo

## 11. Diseño de Registros.

Estos son importantes permiten realizar el fiel seguimiento al manejo y administración de la información de los recursos de TI, con la emisión de los reportes el director y administrador de centro de cómputo puede constatar las actividades más relevantes a tomar en cuenta dentro la institución.

| | R.1 |
|---|---|
| HOJA TRABAJO (MANTENIMIENTO) | |
| DESCRIPCIÓN: | Permite obtener información del listado general del mantenimiento de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | **R.2** |
|---|---|
| **ADMINISTRATIVO** | |
| DESCRIPCIÓN: | Permite obtener información del listado general del personal administrativo de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | **R.3** |
|---|---|
| **PROVEEDOR** | |
| DESCRIPCIÓN: | Permite obtener información del listado general de los proveedores l de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | **R.4** |
|---|---|
| **MOVIMIENTO INTERNO TI** | |

| | |
|---|---|
| DESCRIPCIÓN: | Permite obtener información general del movimiento interno de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.5 |
|---|---|
| **SALIDA RECURSO TI** | |
| DESCRIPCIÓN: | Permite obtener información general de los recursos de TI que han salido fuera de la institución. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.6 |
|---|---|
| **SOFTWARE** | |
| DESCRIPCIÓN: | Permite obtener información general del listado software que posee la institución. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.7 |
|---|---|
| **SOFTWARE EQUIPO** | |
| DESCRIPCIÓN: | Permite obtener información general del listado software que posee cada equipo. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.8 |
|---|---|
| **ALMACEN_RECURSOS TI** | |
| DESCRIPCIÓN: | Permite obtener información del listado general |

| | |
|---|---|
| | del almacén de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.9 |
|---|---|
| **USUARIO** | |
| DESCRIPCIÓN: | Permite obtener información del listado general de los usuarios del sistema "SYSCORTI" |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.10 |
|---|---|
| **COMPRA_RECURSOS TI** | |
| DESCRIPCIÓN: | Permite obtener información de las carateristicas básicas para la compra de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.11 |
|---|---|
| **INVENTARIO** | |
| DESCRIPCIÓN: | Permite obtener información del listado general del inventario de los recursos de TI. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.12 |
|---|---|
| **EQUIPO** | |
| DESCRIPCIÓN: | Permite obtener información del listado general |

| | |
|---|---|
| | de equipos de la institución. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.13 |
|---|---|
| **COMPONENTE EQUIPO** | |
| DESCRIPCIÓN: | Permite obtener información del listado general de los componentes de cada equipo. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

| | R.14 |
|---|---|
| **CUSTODIO** | |
| DESCRIPCIÓN: | Permite obtener información del listado general de los custodios de equipos. |
| FILTRO DE REPORTE | Este reporte no acepta ningún parámetro. |
| CATEGORIZACIONES | |
| | |

## 12. Reciclaje

Consiste básicamente en eliminar el código que resulte redundante durante la programación, aunque este es un proceso que implica tiempo la metodología XP sugiere realizarlo para obtener un proyecto de calidad.

La situación más evidente de código repetido se presentó en los formularios que utilizan métodos que sirven para controlar el estado de los botones y para validar los campos de los cuadros de texto.

A continuación detallamos el método que nos sirve para salir de una ventana o de la aplicación.

```
private void jButton3ActionPerformed(java.awt.event.ActionEvent evt) {//GEN-FIRST:event_jButton3ActionPerformed
        this.dispose();
        String ac = evt.getActionCommand();
         if (ac.equals("Confirmar")){
              System.exit(0);
         }
    }
```

Validar campo de texto  numérico.

```
private void t3KeyTyped(java.awt.event.KeyEvent evt) {//GEN-FIRST:event_t3KeyTyped
        t3.setToolTipText("Solo digitos");
        String cad;
        cad=t3.getText();
        char c = evt.getKeyChar();
        if (!(Character.isDigit(c) || (c == KeyEvent.VK_BACK_SPACE)) ||
              (cad.length()==10 && (c != KeyEvent.VK_BACK_SPACE))) {
            getToolkit().beep();
            evt.consume();
        }
}
```

Validar campo de texto de cadena de caracteres.

```
private void t1KeyTyped(java.awt.event.KeyEvent evt) {//GEN-FIRST:event_t1KeyTyped
        t1.setToolTipText("Solo Letras");
        String cad;
        cad=t1.getText();
        char c = evt.getKeyChar();
```

```
        if ((Character.isDigit(c) || (c == KeyEvent.VK_DELETE)) ||
              (cad.length()==30 && (c == KeyEvent.VK_BACK_SPACE))) {
           getToolkit().beep();
           evt.consume();
        }
}
```

Además en un 100% de los formularios se utilizó el método:

```
 private void formWindowOpened(java.awt.event.WindowEvent evt) {
        mp1 mp = new mp1();
        this.add( mp , BorderLayout.CENTER);
        mp.repaint();
  }
```

# FASE III: DESARROLLO

# DESARROLLO

**Propósito** El desarrollo y codificación de la aplicación se lo realizará mediante el uso de las tarjetas CRC y la programación en parejas siguiendo estándares previamente establecidos. El objeto principal de esta fase será mantener un código consistente para facilitar su comprensión y escalabilidad.

**Introducción**

El cliente es una parte más del equipo de desarrollo; su presencia es indispensable en las distintas fases de X.P. A la hora de codificar una historia de usuario su presencia es aún más necesaria. No olvidemos que los clientes son los que crean las historias de usuario y negocian los tiempos en los que serán implementadas. Antes del desarrollo de cada historia de usuario el cliente debe especificar detalladamente lo que ésta hará y también tendrá que estar presente cuando se realicen los test que verifiquen que la historia implementada cumple la funcionalidad especificada.

Crear test que prueben el funcionamiento de los distintos códigos implementados nos ayudará a desarrollar dicho código. Crear estos test antes nos ayuda a saber qué es exactamente lo que tiene que hacer el código a implementar y sabremos que una vez implementado pasará dichos test sin problemas ya que dicho código ha sido diseñado para ese fin. Se puede dividir la funcionalidad que debe cumplir una tarea a programar en pequeñas unidades, de esta forma se crearán primero los test para cada unidad y a continuación se desarrollará dicha unidad, así poco a poco conseguiremos un desarrollo que cumpla todos los requisitos especificados.

Como ya se comentó anteriormente, X.P opta por la programación en pareja ya que permite un código más eficiente y con una gran calidad para el desarrollo de aplicaciones de escritorio y web.

| FICHA TÉCNICA | |
|---|---|
| **CONTENIDO** | 1. Valores en XP<br>2. Disponibilidad del Cliente<br>3. Unidad de Pruebas<br>3.1 Consideraciones para la Codificación<br>3.2 Programación por Parejas<br>3.3 Integración<br>3.3.1 Integración Secuencial y Frecuente<br>3.4 Controles Utilizados en el desarrollo<br>3.4.1 Controles de Formulario<br>3.5 Estandarización<br>3.5.1 Estándar de la Base de Datos<br>3.6 Diagrama Entidad-Relación<br>3.7 Diagrama de Clases<br>3.8 Presentación del Modelo “Syscorti”<br>3.9 Procedimientos Almacenados<br>3.10 Métodos Utilizados |
| **GRÁFICOS** | Diagrama de Base de Datos<br>Diagrama de Clases |
| **REGISTROS** | Registro 4.1 Prueba Unitaria #1<br>Registro 4.2 Prueba Unitaria #2<br>Registro 4.3 Prueba Unitaria #3<br>Registro 4.4 Controles del Formulario.<br>Registro 4.5 Estándar de Datos.<br>Registro 4.6 Estándar de Controles.<br>Registro 4.7 Estándar de Codificación.<br>Registro 4.8 Conformación de Capas.<br>Registro 4.9 Usuario.<br>Registro 4.10 Inventario. |

| | |
|---|---|
| | Registro 4.11 Componente_Equipo.<br>Registro 4.12 Software_Equipo<br>Registro 4.13 Custodio<br>Registro 4.14 Administrativo<br>Registro 4.15 Departamento<br>Registro 4.16 Proveedor<br>Registro 4.17 Hoja_Trabajo<br>Registro 4.18 Movimiento_Interno<br>Registro 4.19 Movimiento_Externo<br>Registro 4.20 Operación_Log<br>Registro 4.21 Reportes<br>Registro 4.22 RespaldoBDD<br>Registro 4.23 Equipo<br>Registro 4.24 Software |

**PROBLEMAS Y SOLUCIONES ENCONTRADOS**

| **Problemas:** | **Soluciones:** |
|---|---|
| • El diagrama de la Arquitectura software | • Encontrar un diseño acertado y correcto, para “El Diagrama de la Arquitectura del Software”. |
| • El lenguaje de programación Java. | • La investigación continúa durante el desarrollo de la aplicación. |
| • El gestor de base de datos. | • La configuración correcta del servidor de base de datos en un servidor Linux. |
| • Herramientas web para Linux. | • La investigación continúa de como configurar estas herramientas en un servidor Linux. |
| • Herramientas de modelado para la Base de datos. | • Mediante la investigación se logró investigar herramientas gráficas para el modelado de la base de datos. |

| | |
|---|---|
| • Fallos al ejecutar los reportes por la falta de soporte de Jasperreport 4.0 para aplicaciones Swing que trabajan con conexiones a base de datos remotas y que se descargan distribuidamente con la tecnología Java Web Start. | • Implementamos los reportes con código java, realizando primeramente la consulta a una tabla, para luego cargar el resultado a un archivo con extensión .pdf. |

# Desarrollo y Codificación de la Aplicación

## 1. Valores en XP

XP se basa en cuatro valores, que deben estar presentes en el equipo de desarrollo para que el proyecto tenga éxito.

Estos cuatro valores son:

- Comunicación
- Sencillez
- Retroalimentación
- Valentía

### Comunicación

Muchos de los problemas que existen en proyectos de software (así como en muchos otros ámbitos) se deben a problemas de comunicación entre las personas. La comunicación permanente es fundamental en XP. Dado que la documentación es escasa, el diálogo frontal, cara a cara, entre desarrolladores, directores y el cliente es el medio básico de comunicación. Una buena comunicación tiene que estar presente durante todo el proyecto.

### Sencillez

XP, como metodología ágil, apuesta a la sencillez, en su máxima expresión. Sencillez en el diseño, en el código, en los procesos, etc. La sencillez es esencial para que todos puedan entender el código, y se trata de mejorar mediante recodificaciones continuas.

### Retroalimentación

La retroalimentación debe funcionar en forma permanente. El cliente debe brindar retroalimentación de las funciones desarrolladas, de manera de poder tomar sus

comentarios para la próxima iteración, y para comprender, cada vez más, sus necesidades. Los resultados de las pruebas unitarias son también una retroalimentación permanente que tienen los desarrolladores acerca de la calidad de su trabajo.

### Valentía

Cuando se encuentran problemas serios en el diseño, o en cualquier otro aspecto, se debe tener el coraje suficiente como para encarar su solución, sin importar que tan difícil sea. Si es necesario cambiar completamente parte del código, hay que hacerlo, sin importar cuanto tiempo se ha invertido previamente en el mismo.

## 2. Disponibilidad del cliente

Uno de los requerimientos de XP es tener al cliente disponible durante todo el proyecto. No solamente como apoyo a los desarrolladores, sino formando parte del grupo. El involucramiento del cliente es fundamental para que pueda desarrollarse un proyecto con la metodología XP. Al comienzo del proyecto, el cliente debe proporcionar las historias de usuarios. Pero, dado que estas historias son expresamente cortas y de “alto nivel”, no contienen los detalles necesarios para realizar el desarrollo del código. Estos detalles deben ser proporcionados por el cliente, y discutidos con los desarrolladores, durante la etapa de desarrollo. No se requieren de largos documentos de especificaciones, sino que los detalles son proporcionados por el cliente, en el momento adecuado, “cara a cara” a los desarrolladores.

Si bien esto parece demandar del cliente recursos por un tiempo prolongado, se debe tener en cuenta que en otras metodologías este tiempo es insumido por el cliente en realizar los documentos detallados de especificación. Adicionalmente, al estar el cliente en todo el proceso, puede prevenir a tiempo de situaciones no deseables, o de funcionamientos que no eran los que en realidad se deseaban. En otras metodologías, estas situaciones son detectadas en forma muy tardía del ciclo de desarrollo, y su corrección puede llegar a ser muy complicada.

## 3. Unidad de Pruebas.

Las modernas arquitecturas de software tienen la capacidad de ser estudiadas como uno de sus elementos esenciales. Así asumimos el riesgo de tener a diferentes programadores trabajando en distintos módulos sin que esto signifique un problema. De la misma forma es posible imaginar a nuestros programadores ejecutando pruebas locales sobre sus módulos, a fin de tener una certificación del buen funcionamiento -autónomo- de lo que han estado programando.

A continuación puntualizaremos algunas pruebas que se realizó a la aplicación

**Pruebas Unitarias**

| PRUEBA UNITARIA # 1 | |
|---|---|
| DESCRIPCIÓN | Permite verificar el funcionamiento correcto del portal web. |
| REQUISITOS PREVIOS | Ejecutar el navegador. |
| ACCIONES DEL USUARIO | RESPUESTA DEL SISTEMA |
| Ingresar a www.isidroayoraloja.org en la dirección del navegador. | Mantener la página de Inicio |
| Hacer clic en el link del menú Historia | Mostrar la página Historia |
| Hacer clic en el link del menú Misión y Visión | Mostrar la página Misión y Visión |
| Hacer clic en el link del menú Servicios | Mostrar la página Servicios |
| Hacer clic en el link del menú | Mostrar la página Programas |

| | |
|---|---|
| Programas | |
| Hacer clic en el link del menú Ley de Transparencia | Mostrar la página Ley de Transparencia |
| Hacer clic en el link del menú Contactos | Mostrar la página Contactos |
| Hacer clic en el link del menú Syscorti | Mostrar la página Syscorti, que contiene los requerimientos para poder descargar y ejecutar el sistema "Syscorti" |
| REQUISITOS POSTERIORES | Ingresar el login y el password para acceder a la administración del sistema"SYSCORTI" |
| RESPUESTA: Satisfactoria. | |

| PRUEBA UNITARIA # 2 | |
|---|---|
| DESCRIPCIÓN | Permite verificar el ingreso al sistema por parte del administrador y su autentificación en forma correcta |
| REQUISITOS PREVIOS | Hacer clic en el botón descargar Archivo para descagar el sistema y ejecutarlo en la máquina cliente por parte del usuario administrador o usuario invitado. |
| ACCIONES DEL USUARIO | RESPUESTA DEL SISTEMA |
| Digitar en el TextBox el nombre del administrador. | |
| Digitar en el TextBox la clave del administrador. | |

| | |
|---|---|
| Hacer clic en el botón ingresar. | Toma los datos del TextBox y llama al método validar el ingreso al sistema. |
| | Si es satisfactorio el método para validar el ingreso al sistema se accederá a la ventana en la que nos permitirá ingresar el nombre y la clave para acceder a la aplicación de escritorio como administrador, que se encuentra instalada en el servidor. |
| | Si el método es incorrecto para validar el ingreso al sistema, se indicar en un mensaje de texto que la información debe ingresar correctamente para acceder al sistema. |
| REQUISITOS POSTERIORES | Ingreso al Sistema Administrativo. |
| RESPUESTA: Satisfactoria. | |

| PRUEBAS UNITARIA # 3 | |
|---|---|
| DESCRIPCIÓN | Permite verificar si se almacena en forma correcta los datos de personal Administrativo en el sistema. |
| REQUISITOS PREVIOS | Prueba Unitaria #2 |
| ACCIONES DEL USUARIO | RESPUESTA DEL SISTEMA |
| Al hacer clic en módulo administrativo | Nos presentará una ventana de menús con sus respectivos submenús como: Agregar Departamento, Agregar Administrativo, Modificar Departamento, Modificar Administrativo, etc; al hacer clic en cualquiera de los submenús se cargará la ventana correspondiente, luego se ingresan los datos para ser almacenados o modificados en la base de datos, |

| | |
|---|---|
| | también encontramos la opción salir para cambiarnos de módulo si asi lo deseamos. |
| Escoger en la lista desplegable el departamento al cual pertenece el personal administrativo. | |
| Al hacer clic en el botón aceptar. | Se verificará la información guardada con el cual nos presentará un mensaje diciendo que se ha guardado la información correctamente en la base de datos del sistema |
| | Si los campos están vacíos o la información ingresada es incorrecta el sistema, indicara en un mensaje de texto que la información ingresada es errónea. |
| REQUISITOS POSTERIORES | Ninguno. |
| RESPUESTA: Satisfactoria. | |

## 3.1 Consideraciones para la Codificación

Al momento de realizar la codificación de la aplicación debemos considerar varias pautas y principios, a fin de obtener un código entendible y con facilidad para su mantenimiento.

- ✓ Se colocó comentarios en los bloques de código que lo requieran.
- ✓ El código se organizó por secciones, con motivo de facilitar la detención de errores, mientras duraba su desarrollo.
- ✓ Las líneas de comentario que estaban redundantes se las elimino.

## 3.2 Programación por parejas

XP propone que se desarrolle en pares de programadores, ambos trabajando juntos en un mismo ordenador. Si bien parece que ésta práctica duplica el tiempo asignado al proyecto (y por ende, los costos en recursos humanos), al trabajar en pares se minimizan los errores y se logran mejores diseños, compensando la inversión en horas. El producto obtenido es por lo general de mejor calidad que cuando el desarrollo se realiza por programadores individuales.

El emparejamiento es dinámico, puedo estar emparejado por la mañana con una persona y por la tarde con otra, si tienes un trabajo sobre un área que no conoces muy bien puedes emparejarte con otra persona que si conozca ese área. Cualquier miembro del equipo se puede emparejar con cualquiera.

## 3.3 Integración Permanente

Todos los desarrolladores necesitan trabajar siempre con la "última versión". Realizar cambios o mejoras sobre versiones antiguas causan graves problemas y retrasan al proyecto.

Es por eso que XP promueve publicar lo antes posible las nuevas versiones, aunque no sean las últimas, siempre que estén libres de errores. Idealmente, todos los días deben existir nuevas versiones publicadas.

Para evitar errores, solo una pareja de desarrolladores puede integrar su código a la vez.

### *3.3.1 Integración Secuencial y Frecuente*

**Integración Secuencial**

- ✓ Debido a la integración completa de todos los diferentes módulos de software a menudo causar problemas de integración que son difíciles de detectar, XP recomienda secuencial (paso a paso) de integracion.

**Integración Frecuente**

- ✓ Los programadores deben integrar su código a un repositorio común cada cierto tiempo, al menos una vez por día cada pareja. Por lo regular todos deben trabajar con las últimas versiones.
- ✓ La integración continua evitando los esfuerzos divergentes o fragméntales donde no se comunica lo que se puede compartir o reutilizar, esto da lugar a que se detenten las incompatibilidades tempranamente.

## 3.4 Controles Utilizados en el Desarrollo.

Si los programadores realizan distintas partes del sistema intercambiando integrantes, haciendo refactoring, debemos establecer un estándar de codificación aceptado por todo el equipo.

En principio no podemos pedir al equipo que codifique bajo un estándar común, los programadores somos individualistas. A menos que todo XP le dé la posibilidad de sentirse dentro de un equipo ganador.

### *3.4.1 Controles del Formulario*

A continuación ponemos algunos controles utilizados en los formularios para el desarrollo de nuestra aplicación.

| **Controles del Formulario** | |
|---|---|
| **Controles del Formulario utilizados en la Aplicación** | |
| **Versión 1.0** | |
| **OBJETIVO** | **NOMBRE DEL CONTROL** |
| **Acceso al sistema** | JLabel, JTextField, JFormattedTextField, |

| | |
|---|---|
| | JButton, ventana interna de avisos. |
| **crearUsuario** | JLabel, JTextField, JFormattedTextField JTextArea, JButton, JComboBox |
| | ventana interna de avisos. |
| **modificarUsuario** | JLabel, JTextField, JFormattedTextField JButton, JComboBox, JTextArea ventana interna de avisos. |
| | JLabel, JTextField, JButton, JTable. |
| **consultarInventario** | JButton |
| **aceptar** | JButton |
| **salir** | JLabel |
| **control de imágenes** | JLabel, JTextField, JTable, ventana de avisos. |
| **reportes** | |

## 3.5 Estandarización

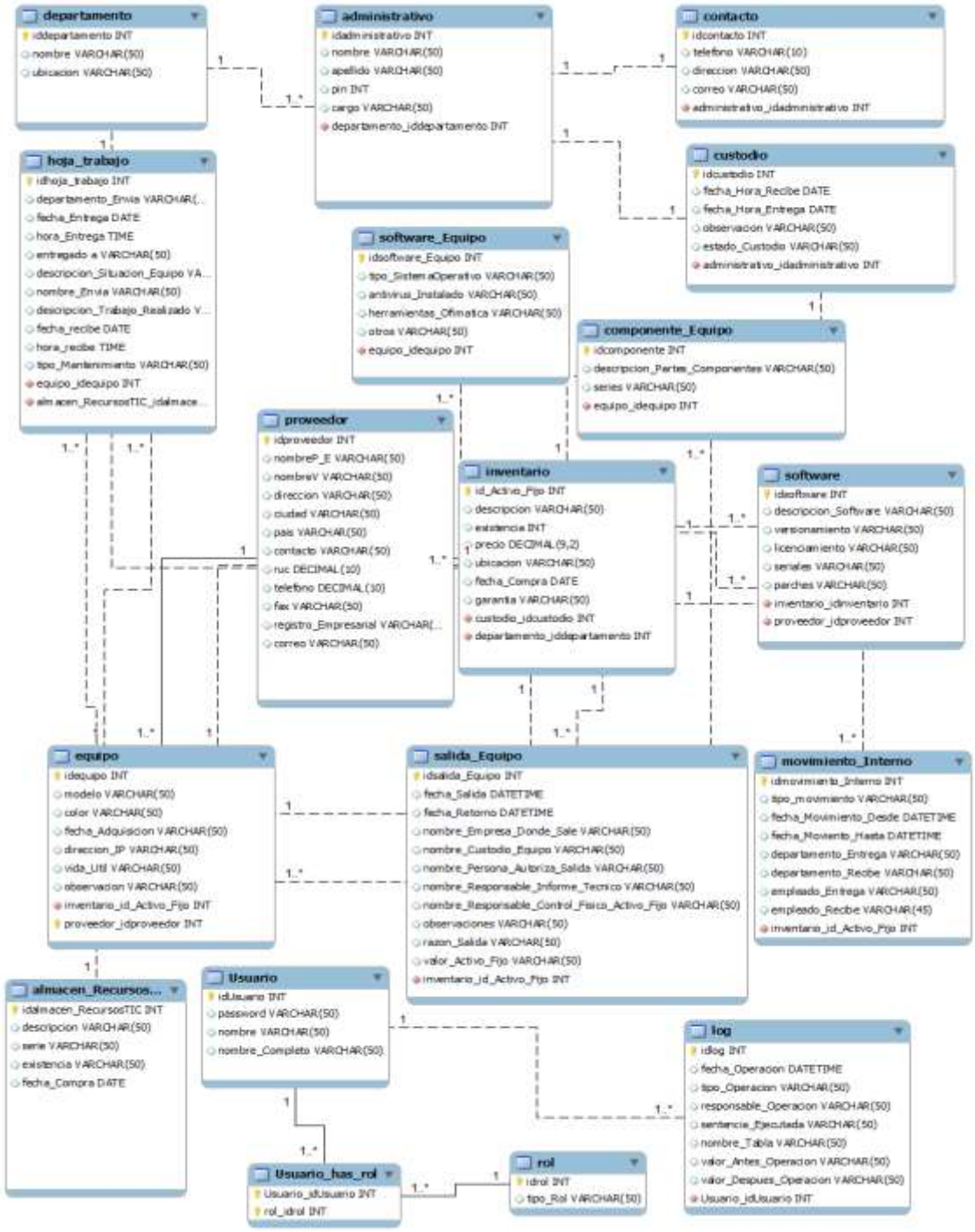
### *3.5.1 Estándar de la Base de Datos.*

A continuación detallamos algunas tablas, campos y procedimientos almacenados para el desarrollo de nuestra aplicación.

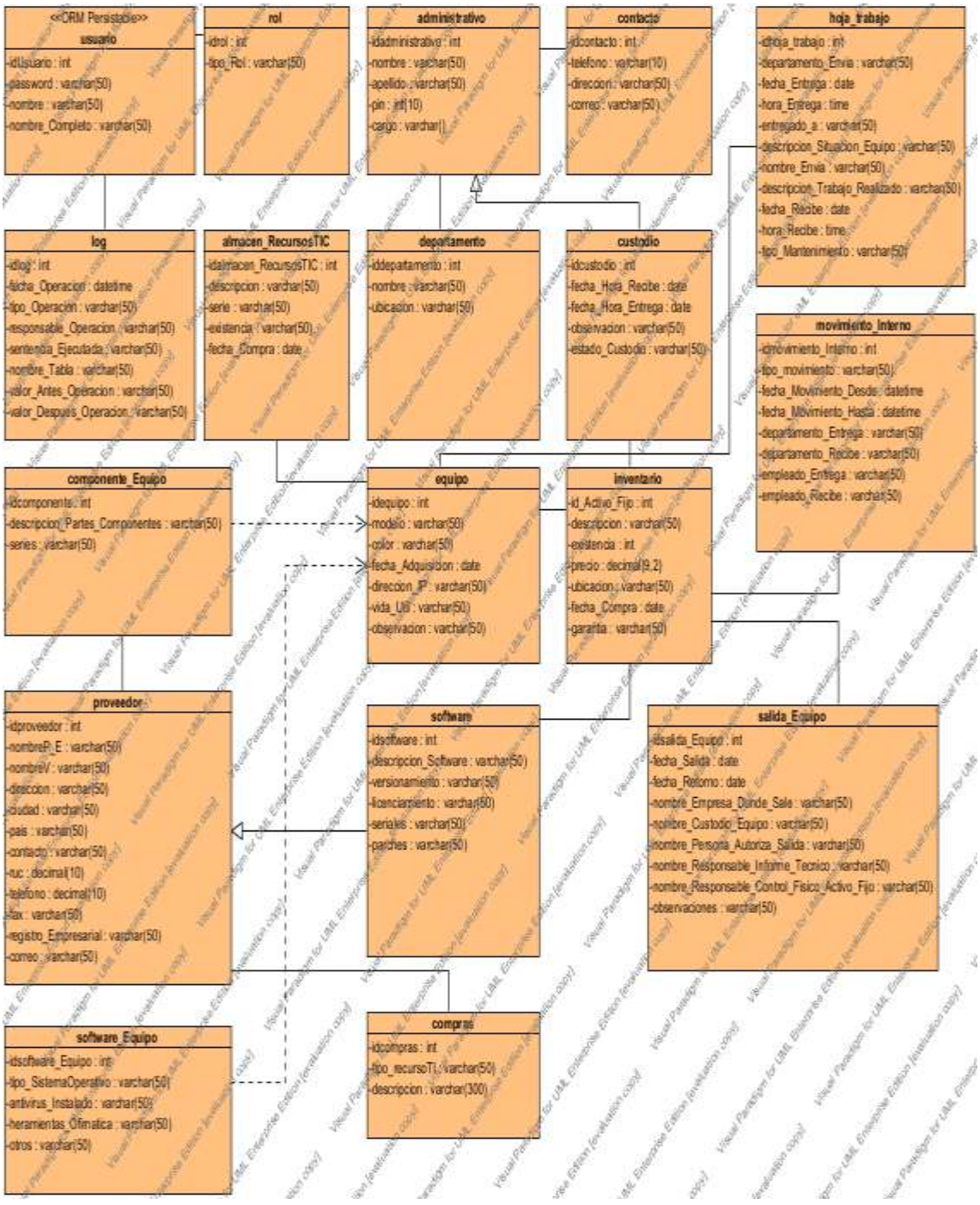
| Estándar Datos | |
|---|---|
| **ESTANDAR DE BASE DE DATOS TABLAS, CAMPOS Y PROCEDIMIENTOS ALMACENADOS** | |
| **Versión 1.0** | |
| **Descripción** | **Argumentos** |
| **BASE DE DATOS** | El nombre de la base de datos será dado de forma particular este se formará de dos o más palabras, que irán separadas por un guion bajo.<br>Formato.<br>palabra1_palabra2.<br>Ejemplo.<br>isidro_syscorti |
| **TABLAS** | El nombre de cada una de las tablas está escrita en minúsculas estas están compuestos por el mismo nombre de la entidad que indicara la actividad principal dentro del sistema.<br>**Usuario** nosotros hemos puesto los mismos nombre de la entidad.<br>El nombre puede componerse de dos o más palabras, que irán separadas por un guion bajo.<br>Formato.<br>nombre1_nombre2<br>Ejemplo.<br>hoja_trabajo |
| **CAMPOS** | Cada una de las columnas que forman las tablas de la base de datos para nuestra aplicación, contienen datos de tipo diferente a los de otros campos. A continuación detallamos algunos campos de una tabla de nuestra base de datos.<br>• **idhoja_trabajo** id de la hoja de trabajo.<br>• **Departamento_Envia** hace referencia el nombre del departamento que envía.<br>• **descripción_TR** descripción del trabajo realizado. |

| | |
|---|---|
| | • **entregado_a** persona a quien entrega el recuso TI para su mantenimiento.<br>**tipo_Mantenimiento** hace referencia al tipo de mantenimiento para el recurso TI que se realizara. |
| **PROCEDIMIENTOS ALMACENADOS** | La creación de los procedimientos almacenados involucra: la especificación del nombre del procedimiento, sus parámetros y el cuerpo que contiene los comandos SQL estos **estarán formados por tres partes.**<br>**Primero** un prefijo que hace referencia al reporte<br>**Segundo** estará dado por el nombre de la clase a la cual se obtendrá el reporte.<br>**Tercero** el nombre de la base de datos donde se realizara la consulta.<br>El nombre del procedimiento almacenado estará dado en letras minúsculas el primer nombre y el segundo nombre con letra mayúscula.<br>Formato.<br>nombre1_NOMBRE2<br>Ejemplo.<br>Usuario_REPORT |

## 3.6 Diagrama Entidad-Relaciòn



## 3.8 Diagrama de Clases



## 3.9 Tablas

**Presentación del Modelo "Syscorti"**

| Nombre | Valor |
|---|---|
| Autor | |
| Create Date Time | 30-mar-2011 15:52:30 |
| Last Modified | 23-abr-2011 9:56:11 |
| Nombre | SYSCORTI |

**LISTA DE OBJETOS A NIVEL DEL MODELADO**

**ENTIDADES**

**LISTA DE TABLAS**

| Nombre | Documentación |
|---|---|
| usuario | Tabla que registra la información de los usuarios del sistema "SYSCORTI". |
| rol | Tabla que registra el rol del usuario de los recursos de TI del HPGIA-Loja. |
| administrativo | Tabla que registra el personal administrativo que tiene a su cargo los recursos de TI del HPGIA-Loja. |
| contacto | Tabla que registra el contacto para la adquisición de los recursos de TI del HPGIA-Loja. |
| hoja_trabajo | Tabla que registra el tipo de mantenimiento de los recursos de TI del HPGIA-Loja. |
| log | Tabla que registra operación que realizo el usuario de los recursos de TI del HPGIA-Loja. |
| almacen_RecursosTIC | Tabla que registra la adquisición de los recursos de TI del HPGIA-Loja. |
| departamento | Tabla que registra el departamento en donde se encuentran ubicados los recursos de TI del HPGIA-Loja. |
| custodio | Tabla que registra la información del custodio de los recursos de TI del HPGIA-Loja. |
| movimiento_Interno | Tabla que registra la información del movimiento de los recursos de TI del HPGIA-Loja. |

| | |
|---|---|
| componente_Equipo | Tabla que registra la información de los componentes de los recursos de TI del HPGIA-Loja. |
| equipo | Tabla que registra la información de todos los recursos de TI del HPGIA-Loja. |
| inventario | Tabla que registra la información general de los recursos de TI del HPGIA-Loja. |
| proveedor | Tabla que registra la información de los proveedores de los recursos de TI del HPGIA-Loja. |
| software | Tabla que registra la información del software de los recursos de TI del HPGIA-Loja. |
| salida_Equipo | Tabla que registra la información de la salida de los recursos de TI del HPGIA-Loja. |
| compras | Tabla que registra la información de la compra de los recursos de TI del HPGIA-Loja. |
| software_Equipo | Tabla que registra la información del software de los equipos de todos los recursos de TI del HPGIA-Loja. |

**DETALLE DE LAS TABLAS**

**usuario**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idUsuario | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| Password | varchar(30) | Registra el password del usuario. |
| Nombre | varchar(30) | Registra el nombre de usuario. |
| nombre_Completo | varchar(50) | Registra el nombre completo del usuario que ingresa al sistema. |

**rol**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idrol | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| tipo_Rol | varchar(30) | Registra el tipo de rol que realiza el usuario. |

**administrativo**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idadministrativo | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| nombre | varchar(30) | Registra el nombre de administrativo. |

| | | |
|---|---|---|
| Apellido | varchar(30) | Registra el apellido de administrativo. |
| Pin | int | Registra el número de cedula de administrativo. |
| Cargo | varchar(50) | Registra el cargo de admistrativo. |
| departamento_iddepartamento | int | Registra la clave primaria de departamento al que pertenece el administrativo. |

**contacto**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idcontacto | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| Teléfono | varchar(10) | Registra el teléfono del contacto. |
| Dirección | varchar(50) | Registra la dirección del contacto. |
| Correo | Varchar(50) | Registra el correo del contacto. |
| administrativo_idadministrativo | int | Registra la clave primaria del administrativo al que pertenece el contacto. |

**hoja_trabajo**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idhoja_trabajo | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| departamento_Envia | varchar(50) | Registra el nombre del departamento que envía. |
| fecha_entrega | date | Registra la fecha de entrega de equipo. |
| hora_Entrega | time | Registra la sentencia que ejecuta el usuario. |
| entregado_A | varchar(50) | Registra el nombre usuario a quien es estregado el equipo. |
| descripción_SE | varchar(50) | Registra la descripción de la situación del equipo. |
| nombre_Envia | varchar(50) | Registra el nombre del usuario que envía el equipo. |
| descripción_TR | int | Registra la descripción del trabajo realizado en el equipo. |
| fecha_recibe | date | Registra la fecha que recibe el equipo. |

| | | |
|---|---|---|
| hora_recibe | time | Registra la fecha que recibe el equipo |
| tipo_Mantenimiento | varchar(50) | Registra el tipo de mantenimiento que realiza al equipo. |
| equipo_idequipo | int | Registra la clave primaria de equipo al que pertenece en la hoja_trabajo. |
| almacen_RecursosTIC_idalmacen_RecursosTIC | int | Registra la clave primaria del almacen_RecursosTIC al que pertenece en la hoja_trabajo. |

**log**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idlog | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| fecha_Operacion | datetime | Registra el password del usuario. |
| responsable_Operacion | varchar(50) | Registra el nombre del responsable de la operacion. |
| sentencia_Ejecutada | varchar(50) | Registra la sentencia que ejecuta el usuario. |
| nombre_Tabla | varchar(50) | Registra el nombre de la tabla |
| valor_Antes_Operacion | varchar(50) | Registra el valor antes de la operación |
| valor_Despues_Operacion | varchar(50) | Registra el valor después de la operacion |
| usuario_idUsuario | Int | Registra la clave primaria del usuario al que pertenece el log. |

**almacen_recursostic**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idalmacen_RecursosTIC | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| descripción | varchar(50) | Registra la descripción de los equipos. |
| serie | varchar(50) | Registra las series de los equipos. |
| existencia | varchar(1) | Registra la existencia de los equipos. |
| fecha_Compra | Date | Registra la fecha de compra de los equipos. |

**departamento**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| iddepartamento | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| nombre | varchar(50) | Registra el nombre del departamento. |
| ubicacion | varchar(50) | Registra la ubicación del departamento. |

**custodio**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idcustodio | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| fecha_Hora_Recibe | date | Registra la fecha que recibe el equipo. |
| fecha_Hora_Entrega | date | Registra la fecha que entrega el equipo. |
| observacion | varchar(50) | Registra la observacion del equipo. |
| estado_Custodio | varchar(50) | Registra el estado del custodio |
| administrativo_Idadministrativo | int | Registra la clave primaria de administrativo al que pertenece el custodio. |

**movimiento_interno**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idmovimiento_Interno | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| tipo_movimiento | varchar(50) | Registra el tipo de movimiento del movimiento_Interno |
| fecha_MovimientoD | datetime | Registra la fecha del movimiento desde el movimiento interno. |
| fecha _MovimientoH | datetime | Registra la fecha del movimiento hasta el movimiento interno. |
| departamento_Entrega | varchar(50) | Registra el nombre del departamento que entrega del movimiento interno. |
| departamento_Recibe | varchar(50) | Registra el nombre del departamento que recibe del movimiento interno. |
| empleado_Entrega | varchar(50) | Registra el nombre del empleado que entrega del movimiento interno |
| empleado_Recibe | varchar(50) | Registra el nombre del empleado que recibe del movimiento interno |
| inventario_id_Activo_Fijo | int | Registra la clave primaria del inventario al que pertenece el movimiento interno. |

**componente_equipo**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idcomponente | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| descripción_Partes_Componentes | varchar(50) | Registra la descripción de partes de componentes de los equipos. |
| Series | varchar(50) | Registra la serie de componente de equipo. |
| equipo_idequipo | Int | Registra la clave primaria del equipo al que pertenece el componente de equipo. |

**equipo**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idequipo | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| Modelo | varchar(50) | Registra el modelo de equipo. |
| Color | varchar(50) | Registra el color de equipo. |
| fecha_Adquisicion | Date | Registra la fecha de adquisición de equipo. |
| dirección_IP | varchar(50) | Registra la dirección ip de equipo. |
| vida_Util | varchar(50) | Registra la vida util de equipo. |
| Observación | varchar(50) | Registra la observación de equipo. |
| inventario_id_Activo_Fijo | Int | Registra la clave primaria del id_Activo_Fijo al que pertenece el equipo |
| proveedor_idproveedor | Int | Registra la clave primaria del proveedor del equipo. |

**inventario**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| id_Activo_Fijo | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| Descripción | varchar(50) | Registra la descripción en el inventario. |
| Existencia | varchar(50) | Registra la existencia en el inventario. |
| Precio | decimal(9,2) | Registra el precio en el inventario. |
| fecha_Compra | Date | Registra la fecha compra en el inventario. |
| Garantía | varchar(50) | Registra la garantía en el inventario. |
| custodio_idcustodio | Int | Registra la clave primaria del custodio al que pertenece en el inventario. |
| departamento_iddepartamento | Int | Registra la clave primaria del departamento al que pertenece en el inventario. |
| id_Activo_Fijo_Externo | Int | Registra la clave secundaria externa |

| | | |
|---|---|---|
| | | del inventario al que pertenece el equipo en el inventario |
| Estado | varchar(6) | Registra el estado en el inventario. |

**proveedor**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idproveedor | Int | Clave primaria de la tabla con autoincremento de uno en uno. |
| nombreP_E | varchar(50) | Registra el nombre de proveedor o nombre de empresa proveedora. |
| nombreV | varchar(50) | Registra el nombre del vendedor. |
| Dirección | varchar(50) | Registra la dirección del proveedor. |
| Ciudad | varchar(50) | Registra la ciudad del proveedor. |
| País | varchar(50) | Registra el país del proveedor. |
| Contacto | varchar(50) | Registra el contacto del proveedor. |
| Ruc | decimal(10) | Registra el ruc del proveedor. |
| Teléfono | decimal(10) | Registra el teléfono del proveedor. |
| Fax | varchar(50) | Registra el fax del proveedor. |
| registro_Empresarial | varchar(50) | Registra el registro_Empresarial del proveedor. |
| Correo | varchar(50) | Registra el correo del proveedor. |

**software**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idsoftware | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| descripción_Software | varchar(50) | Registra la descripción del software. |
| Versionamiento | varchar(50) | Registra el versionamiento del software. |
| Vicenciamiento | varchar(50) | Registra el licenciamiento del software. |
| Seriales | varchar(50) | Registra el serial del software |
| Parches | varchar(50) | Registra el parche del software. |
| inventario_idinventario | int | Registra la clave primaria del id_Activo_Fijo al que pertenece el software. |
| proveedor_idproveedor | int | Registra la clave primaria del proveedor del software. |

**salida_equipo**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idsalida_Equipo | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| fecha_Salida | datetime | Registra la fecha de la salida_Equipo |
| fecha_Retorno | datetime | Registra la fecha de retorno de la salida_Equipo |
| nombre_Empresa_Donde_Sale | varchar(50) | Registra el nombre donde sale en la salida_Equipo. |
| nombre_Custodio_Equipo | varchar(50) | Registra el nombre del custodio en la salida_Equipo. |
| nombre_Persona_Autoriza_Salida | varchar(50) | Registra la persona que autoriza la salida en la salida_Equipo |
| nombre_Responsable_Informe_Tecnico | varchar(50) | Registra el informe técnico en la salida_Equipo. |
| nombre_Responsable_Control_Fisico_Activo_Fijo | varchar(50) | Registra el nombre del responsable del control de activo fijo en la salida_Equipo. |
| Observaciones | | Registra la observación en la salida_Equipo. |
| razón_Salida | | Registra la razón de la salida en la salida_Equipo. |
| valor_Activo_Fijo | varchar(50) | Registra el valor del activo fijo en la salida_Equipo. |
| inventario_id_Activo_Fijo | int | Registra la clave primaria del inventario al que pertenece la salida_Equipo. |

**software_equipo**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| idsoftware_Equipo | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| tipo_SistemaOperativo | varchar(50) | Registra el sistema operativo instalado en el software_equipo |
| antivirus_Instalado | varchar(50) | Registra el antivirus instalado en el software_equipo. |
| herramientas_Ofimatica | varchar(50) | Registra la herramienta de ofimatica en el software_equipo. |
| equipo_idequipo | int | Registra la clave primaria del equipo al que pertenece el software_equipo. |

**compras**

| Campo | Tipo de Dato | Descripción |
|---|---|---|
| Idcompras | int | Clave primaria de la tabla con autoincremento de uno en uno. |
| tipo_recursoTI | varchar(50) | Registra el tipo de recurso de ti en compras |
| Descripción | varchar(50) | Registra la descripción en compras |
| Precio | varchar(50) | Registra el precio en compras |
| proveedor_idproveedor | int | Registra la clave primaria del proveedor al que pertenecen las compras. |

## Lista de Relaciones entre Tablas

| Relaciones entre Tablas | | | |
|---|---|---|---|
| **Nombre** | **Entidad 1** | **Entidad2** | **Entidad3** |
| **usuario_idUsuario** | **Usuario** | **log** | |
| **inventario_id_Actifo_Fijo**<br>**proveedor_idproveedor** | **Inventario** | **proveedor** | **Equipo** |
| **equipo_idequipo**<br>**almacen_RecursosTIC_idalmacen_RecursosTIC** | **Equipo** | **Almacen_RecursosTIC** | **hoja_trabajo** |

| | | | |
|---|---|---|---|
| **departamento_idepartamento** | **departamento** | **administrativo** | |
| **administrativo_idadministrativo** | **administrativo** | **contacto** | **Custodio** |
| **equipo_idequipo** | **Equipo** | **software_Equipo** | **componente_Equipo** |
| **custodio_idcustodio**<br><br>**departamento_iddepartamento** | **Custodio** | **departamento** | **Inventario** |
| **inventario_id_Activo_Fijo**<br><br>**proveedor_idproveedor** | **Inventario** | **proveedor** | **Software** |
| **Inventario_id_Activo_Fijo** | **salida_Equipo** | **movimiento_Interno** | |
| **Compras** | **Proveedor** | | |

## 3.10 Procedimientos Almacenados

A continuación detallaremos algunos procedimientos almacenados realizados en java:

**NOMBRE DE LA BASE DE DATOS A USARSE**

isidro_syscorti;

**Procedure: GenerarPDFUsuarios**

```
private void agregarTabla(Paragraph parrafo) throws BadElementException{
  float anchosFilas[] = { 0.2f,0.5f,0.5f,0.5f };
  PdfPTable tabla = new PdfPTable(anchosFilas);
  String rotulosColumnas[] =
  {"idUsuario","Password","Nombre","Nombre_Completo"};
  tabla.setWidthPercentage(90);
  tabla.setHorizontalAlignment(Element.ALIGN_CENTER);
  PdfPCell cell = new PdfPCell(new Paragraph("REPORTE DEL LISTADO
  GENERAL DE LOS USUARIOS DEL SISTEMA SYSCORTI"));
```

```
cell.setColspan(4);
cell.setHorizontalAlignment(Element.ALIGN_CENTER);
cell.setBackgroundColor (azulClaro);
tabla.addCell(cell);
try{
        if ( ConectarBD() ){
                for(int i=0; i<rotulosColumnas.length; i++){
                        cell = new PdfPCell(new
                        Paragraph(rotulosColumnas[i],fuenteNegra10));
                        cell.setVerticalAlignment(Element.ALIGN_MIDDLE);
                        cell.setHorizontalAlignment(Element.ALIGN_CENTER);
                        cell.setBackgroundColor (grisClaro);
                        tabla.addCell(cell);
        }
        strConsultaSQL = "SELECT * FROM usuario";
         rs = estSQL1.executeQuery(strConsultaSQL);
        while (rs.next()){
                cell = new PdfPCell(new Paragraph(String.valueOf(rs.getInt
                ("idUsuario")),fuente8 ));
                tabla.addCell(cell);
                cell = new PdfPCell(new
                Paragraph(rs.getString("password"),fuente8));
                tabla.addCell(cell);
                cell = new PdfPCell(new
                Paragraph(rs.getString("nombre"),fuente8));
                tabla.addCell(cell);
                cell = new PdfPCell(new
                Paragraph(rs.getString("nombre_Completo"),fuente8));
                tabla.addCell(cell);
        }
        CrearConexion.cerrar(rs);          //ResultSet
        CrearConexion.cerrar(estSQL1);  //Statement
        CrearConexion.cerrar(conn);     //Connection
```

```
        }
        }catch(Exception e){
                System.out.println("Excepcion al ejecutar CONSULTA!!!");
                e.printStackTrace();
        }
        parrafo.add(tabla);
  }
```

**Procedure: GenerarPDFProveedor**

```
private void agregarTabla(Paragraph parrafo) throws BadElementException{
        float anchosFilas[] = { 0.2f,0.3f,0.2f,0.4f,0.2f,0.2f,0.3f,0.2f,0.2f,0.2f,0.2f,0.4f };
        PdfPTable tabla = new PdfPTable(anchosFilas);
        String rotulosColumnas[] =
        {"IdPvdor","NombrePE","NombreV","Direccion","Ciudad","Pais","Contacto","Ruc","T
        elefono","Fax","RegistroE","Correo"};
        tabla.setWidthPercentage(106);
        tabla.setHorizontalAlignment(Element.ALIGN_CENTER);
        PdfPCell cell = new PdfPCell(new Paragraph("REPORTE DEL LISTADO
        GENERAL DE LOS PROVEEDORES DE LOS RECURSOS DE TI DEL HPGIA-
        LOJA"));
        cell.setColspan(12);
        cell.setHorizontalAlignment(Element.ALIGN_CENTER);
        cell.setBackgroundColor (azulClaro);
        tabla.addCell(cell);
        try{
                if ( ConectarBD() ){
                        for(int i=0; i<rotulosColumnas.length; i++){
                        cell = new PdfPCell(new
                        Paragraph(rotulosColumnas[i],fuenteNegra10));
                        cell.setVerticalAlignment(Element.ALIGN_MIDDLE);
                        cell.setHorizontalAlignment(Element.ALIGN_CENTER);
                        cell.setBackgroundColor (grisClaro);
```

```
            tabla.addCell(cell);
}
strConsultaSQL = "SELECT * FROM proveedor";
rs = estSQL1.executeQuery(strConsultaSQL);
while (rs.next()){ //Agregar 9 celdas
            cell = new PdfPCell(new Paragraph(String.valueOf(rs.getInt
            ("idproveedor")),fuente8 ));
            tabla.addCell(cell);
            cell = new PdfPCell(new
            Paragraph(rs.getString("nombreP_E"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new
            Paragraph(rs.getString("nombreV"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new
            Paragraph(rs.getString("direccion"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new Paragraph(rs.getString("ciudad"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new Paragraph(rs.getString("pais"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new
            Paragraph(rs.getString("contacto"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new Paragraph(rs.getString("ruc"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new
            Paragraph(rs.getString("telefono"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new Paragraph(rs.getString("fax"),fuente8));
            tabla.addCell(cell);
            cell = new PdfPCell(new
            Paragraph(rs.getString("registro_Empresarial"),fuente8));
```

```
                    tabla.addCell(cell);
                    cell = new PdfPCell(new Paragraph(rs.getString("correo"),fuente8));
                    tabla.addCell(cell);
                }
                CrearConexion.cerrar(rs);
                CrearConexion.cerrar(estSQL1);
                CrearConexion.cerrar(conn);

                }
        }catch(Exception e){
                System.out.println("Excepcion al ejecutar CONSULTA!!!");
                e.printStackTrace();
        }
        parrafo.add(tabla);
  }
```

**Tabla de los Procedimientos Almacenados**

| PROCEDIMIENTOS ALMACENADOS | | |
|---|---|---|
| **Procedimientos Almacenados de la Base de Datos** | | |
| **Versión 1.0** | | |
| **ALIAS** | **PARAMETROS** | **TABLA DE REFERENCIA** |
| GenerarPDFUsuarios | Password<br>nombre<br>nombre_Completo<br>tipo_Rol | usuario. |
| GenerarPDFProveedor | Idproveedor<br>nombreP_E<br>nombreV<br>dirección<br>ciudad | proveedor |

| | | |
|---|---|---|
| | país<br>contacto<br>ruc<br>teléfono<br>fax<br>registro_Empresarial<br>correo | |

## 3.11 Métodos Utilizados

Detallamos algunos métodos utilizados en esta aplicación.

**private void *********ActionPerformed(java.awt.event.ActionEvent evt) {**

Este método permite ingresar la información en cada control correspondiente y guardarlo en la BDD.

**private void *********ActionPerformed(java.awt.event.ActionEvent evt) {**

Este método permite obtener la información en cada control correspondiente, modificándola y guardándola en la BDD.

**private void *********ActionPerformed(java.awt.event.ActionEvent evt) {**

Este método permite consultar mediante la información ingresada al JTextField el cual nos mostrará la información en un JTable el registro correspondiente.

**private void *********ActionPerformed(java.awt.event.ActionEvent evt) {**

Este método permite cargar la información en un JComboBox y cuando seleccionemos algún ítem nos muestre la información en cada control correspondiente y si modifica algún dato este se guardará en la BDD.

**private void *********ActionPerformed(java.awt.event.ActionEvent evt) {**

Este método permite consultar mediante la información ingresada al JTextField el cual nos mostrará la información en un JTable el registro correspondiente, con lo cual obtendremos un reporte del mismo.

# FASE IV: PRUEBAS

# PRUEBAS

**Propósito** En esta fase se realiza pruebas con el usuario final que va a manejar la aplicación, quien nos ayudará a la aceptación del sistema. Para ello se realizan pruebas de cada módulo o unidad, de la integración de todos los módulos y de la validación de las especificaciones funcionales; se realizan las correcciones necesarias para su buen funcionamiento.

**Introducción**

Las pruebas son una parte muy significativa del proyecto de adecuación de las aplicaciones, no solo por su importancia en el logro de resultados correctos sino por el tiempo y recursos requeridos. Se estima que demandan del orden del 60% del total del proyecto.

Independientemente de que la conversión haya sido realizada con equipos de trabajo interno o externos, en la fase de pruebas se deberá comprometer a toda la organización, siendo el usuario final quien certifica la "aceptación" del sistema que utiliza.

Las pruebas de cambios para "adecuación al año 2011" tienen características particulares. Mientras para los cambios tradicionales se debe probar que los sistemas tienen un nuevo comportamiento, acorde con los cambios establecidos, en estas se deberá verificar que:

a) Se mantenga inalterado el comportamiento de los sistemas, con datos anteriores al año 2011.
b) Los sistemas sean capaces de procesar en forma correcta fechas de este milenio, del próximo y de la transición entre ambos.
c) No aparezcan nuevos campos de fechas, sin convertir, por no haber sido identificados en fases anteriores.

| FICHA TÉCNICA | |
|---|---|
| **CONTENIDO** | 1. Implantación<br>1.1 Alojamiento en Hosting<br>1.2 Pruebas funcionales Técnicas<br>2. Pruebas de Aceptación<br>2.1 Encuesta |
| **GRÁFICOS** | |
| **REGISTROS** | Forma del “Syscorti” v.1.0.0. |

| PROBLEMAS Y SOLUCIONES ENCONTRADOS | |
|---|---|
| **Problemas:** | **Soluciones:** |

| INFORME ADICIONAL | |
|---|---|
| **OBSERVACIONES** | |

# IMPLEMENTACIÓN Y PRUEBAS

## 1. Implementación

Una implementación o implantación es la realización de una aplicación, o la ejecución de planes, ideas, modelos científicos, diseños, especificaciones, estándares, algoritmos o políticas.

En la computación o informática, implementación es la realización de una especificación técnica o algoritmos como un programa, componente software, u otro sistema de cómputo. Muchas implementaciones son dadas según a una especificación o un estándar. Por ejemplo, un navegador web respeta (o debe respetar) en su implementación, las especificaciones recomendadas según el World Wide Web Consortium, y las herramientas de desarrollo del software contienen implementaciones de lenguajes de programación.

### 1.1 Alojamiento del Hosting.

El alojamiento del sitio web informativo esta publicado en el hosting adquirido en yamburara.com con los requerimientos de Joomla, Apache y Php; con un dominio principal de isidroayoraloja.org, para que este sea consumido desde el internet con la dirección www.isidroayoraloja.org, a continuación se detalla algunas características que posee y que son necesarias para implementar el proyecto.

| **Características** | |
|---|---|
| Espacio en disco | 50 GB |
| Centos 5.4 | Linux |
| Mysql server 5.0 | Linux |

| | |
|---|---|
| Netbeans 6.9.1 | Linux |
| Jdk 24 | Linux |
| Php 5.0 | Linux |
| Mysql workbench 2.3 | Windows 7 |
| BASpeed v 7 | Windows 7 |
| phpMyAdmin 3.4.7.1 | Linux |
| Apache 5.0 | Linux |
| Joomla 1.5.2 en español | Linux |
| Vp suite PE | Windows 7 |
| Configuración Personalizada de mysql server 5.0 | ✓ |
| Configuración Personalizada del Joomla | ✓ |
| Administración de Dominios (Cpanel) | ✓ |
| Copias de seguridad de las Bases de datos | ✓ |

## 1.2 Pruebas Funcionales Técnicas.

Las pruebas funcionales radican en la ejecución, revisión y retroalimentación de las funcionalidades que ya han sido desarrolladas con anticipación para el software. Con estas pruebas se evaluá el sitio web informativo y la aplicación de escritorio Syscorti para lograr la calidad en su funcionalidad.

Para hacer un test de velocidad de la descarga de la aplicación Syscorti y transferencias desde el servidor a una máquina cliente utilizamos la herramienta BASpeed V7 que nos dió los siguientes resultados.

- **Con la velocidad del servicio de Internet a:** 639 Kbps

| Descripción | Velocidad | Tiempo/minutos |
|---|---|---|
| Descargar la Aplicaciòn. | 79 Kbytes/s | 5 |
| Agregando datos a la tabla Departamento. | 79 Kbytes/s | 1 |
| Modificando datos de la tabla departamento. | 79 Kbytes/s | 1 |
| Obtener reporte de la tabla usuario. | 79 Kbytes | 4 |

Por supuesto que estos cálculos pueden variar debido a la pérdida de señales en la red de transmisión, insuficiente rendimiento del hardware en la pc y otros factores que siempre conspiran contra el total aprovechamiento de la red.

## 2. Pruebas de Aceptación.

Cuando se construye un software a la medida para un cliente (en especial desde el punto de vista de la Programación Extreme), con lo cual se llevará a cabo una serie de pruebas de aceptación para permitir que el cliente valide y verifique todos los requerimientos, estas pruebas las realiza el usuario final.

### 2.1 Encuesta

Las encuestas son un conjunto de preguntas normalizadas que se aplican a una muestra representativa de la población, formada a menudo por personas, empresas o instituciones con el fin de conocer una opinión del objeto a evaluar.

La encuesta para evaluar Syscorti se aplica en base a tres puntos específicos como la facilidad de uso, la tecnología y la arquitectura del sistema. Ver modelo de encuesta y tabulación de datos en el Anexo 5.

# CONCLUSIONES

## Para la Auditoría

- El desarrollo de la presente auditoría informática ha permitido determinar, que existe despreocupación por la adecuada administración de los recursos de TI de la institución auditada.

- La presente auditoría no solo se enmarca en el control y manejo de los recursos de TI del departamento de Gestión Informática, sino que además abarca a todos los equipos distribuidos en los 41 departamentos del HPGIA.

- Con este estudio se ha definido una gran cantidad de soluciones que pueden ayudar a contrarrestar los riesgos potenciales encontrados.

- Al administrar adecuadamente los recursos de TI del Hospital Isidro Ayora puede lograr una mayor productividad de los equipos informatizados.

- Mediante el marco de trabajo COBIT 4.0, se ha podido analizar y evaluar cada uno de los procesos de TI en el Hospital Provincial General Isidro Ayora de Loja.

## Para el Desarrollo del Software

- Para una excelente investigación y una correcta definición de los requerimientos, será primordial conocer totalmente el entorno de desenvolviendo del hospital.

  Para poder determinar en forma irrefutable todos los componentes de la solución a desarrollarse.

- Siguiendo la metodología XP ha sido más fácil llevar toda organización y desarrollo del Sistema Web para el Control de los Recursos de Tecnología de la Información, para el HPGIA-Loja.

- La utilización de herramientas de código libre contribuyen al desarrollo de aplicaciones flexibles, puesto que permite a otros programadores evaluar y mejorar sin ningún límite el código fuente disponible del sistema “SYSCORTI”.

- El uso de herramientas GPL (Licencia Publica General) como: Centos 5.4, Netbeans 6.9.1, iReport 4.0, Mysql Workbench 5.2, Mysql server 5.0, Php 5.1 , Apache 2.2 y Joomla 1.5.22, se ha podido desarrollar con éxito toda la aplicación, ya que estas herramientas ofrecen una interfaz gráfica fácil de manejar.

- Mediante la implementación del sistema “SYSCORTI”, el administrador del centro de cómputo del HPGIA-Loja podrá administrar eficientemente los recursos de TI de la institución.

- En el desarrollo del sitio web informativo, del Hospital Provincial General Isidro Ayora de la ciudad de Loja, utilizamos herramientas de multimedia que permiten desenvolver con interactividad, profesionalidad y eficiencia, convirtiéndose en un portal agradable y beneficioso.

- La utilización del portal web informativo del HPGIA-Loja, contribuye a que cada usuario que realice una consulta tenga información sobre los servicios que ofrece en cada uno de los departamentos y el equipo de médicos con que cuenta la institución.

- Se debe contemplar todas las opciones requeridas dentro de cada módulo del sistema para poder realizar cada acción que este tenga.

- La utilización de base de datos: tablas y procedimientos almacenados, contribuye a que la información se lleve en forma ordenada y segura.

- La utilización de métodos y constructores facilito la programación de cada uno de los módulos y de los reportes, ya que se estos se reutilizaron en el desarrollo de la aplicación.

# RECOMENDACIONES

## Para la Auditoría

- Adecuar las instalaciones del centro de cómputo ya que el espacio físico asignado es muy reducido y no cuenta con las debidas seguridades físicas.

- Capacitar al administrador del Centro de Cómputo en la *Gobernabilidad* de las Tecnologías de la Información.

- Tener presente los procesos que se encuentran con el nivel de Madurez 0 y 1, puesto que son los de factor crítico.

- Capacitar al personal de informática sobre el marco de trabajo COBIT 4.0, para tener una mejor apreciación del presente trabajo.

- Definir los procesos y actividades ejecutadas por el departamento de Gestión Informática de manera formal y que se mantenga su respectiva documentación como fuente de apoyo para futuras auditorías.

- Implementar software libre, para enmarcarse en el decreto 1014 de la República del Ecuador, en el que se establece que toda institución pública debe incorporar software libre para sus sistemas y equipamiento informático.

- Establecer un espacio físico que cumpla con las debidas condiciones de seguridad para almacenar los respaldos de información de los servidores y las pc`s que manejen información crítica.

- Se debería diseñar un manual de políticas que ayuden a regular el buen uso y trato de los recursos de TI de la institución.

**Para el Desarrollo del Software**

- Implementar arquitecturas de desarrollo N-Capas, para obtener Sistemas Informáticos flexibles y fiables a los que se les puede dar mantenimiento y soporte de manera sencilla.

- Capacitar al administrador y usuarios invitados del sistema "SYSCORTI", mediante el documento Manual del Usuario el mismo que ofrece la información concreta del uso o manejo del sistema.

- La Planificación eficaz, concisa y adaptable del sistema, para evitar inconvenientes posteriores, dentro del desarrollo del sitio web y de la aplicación de escritorio.

- Para la UIDE a través de sus Docentes y Alumnos, la investigación del uso de herramientas de GPL para desarrollar e implementar Soluciones Informáticos.

- Apoyar a los estudiantes de la carrera de Informática y Multimedia, con el mejoramiento de libros, laboratorios, tecnología, talleres, jornadas informáticas, intercambios estudiantiles con otras universidades; con el fin de potencializar el conocimiento de sus estudiantes.

- Trabajar con versiones finales estables del software desde el inicio hasta la finalización del proyecto de tesis.

- Mejorar la presente solución informática, ya que existe aún mucho campo por desarrollar.

# BIBLIOGRAFÍA

## Para la Auditoría

### Textos:


- Lic. Enrique Hernández, AUDITORÍA EN INFORMÁTICA, UN ENFOQUE METODOLÓGICO Y PRÁCTICO, PRIMERA EDICIÓN, México 1997.
- Mario G. Piattini y Emilio del Peso, AUDITORÌA INFORMÀTICA, UN ENFOQUE PRÀCTICO,SEGUNDA EDICIÓN, México 2001
- Dr. Wellington Ríos, AUDITORIA INFORMATICA, GUIA PARA SU APLICACIÓN, PRIMERA EDICION, Ecuador 1994
- Marcelo León Cornejo, EL PROCESO DE LA AUDITORIA, GUIA DIDACTICA, PRIMERA EDICIÓN, Loja 2006.
- Álvaro Gómez, ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA, PRIMERA EDICIÓN 2007
- IT Governance Institute COBIT 4.0 Objetivos de Control, Directrices Gerenciales y Modelos de Madurez., Estados Unidos 2005.
- Acuerdo Ministerial No.00000161 del 4 de Marzo del 2009, REGLAMENTO INTERNO PARA LA ADMINISTRACIÓN DE ACTIVOS FIJOS DEL MINISTERIO DE SALUD PÚBLICA. Quito 2009.
- Llumihuasi Quispe Juan, AUDITORÍA DE LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL GOBIERNO MUNICIPAL DE SAN MIGUEL DE URCUQUÍ UTILIZANDO COMO MODELO DE REFERENCIA COBIT 4.0, Quito septiembre 2010.


### Direcciones Electrónicas:


- http://www.isaca.org
- http://gestionempresarial.info/
- http://es.wikipedia.org/wiki/Proceso
- http://www.cemla.org/pdf/pub-di-aud-cg.pdf
- http://www.synotion.com/es/Producten/COBIT

- www.isaca.org/glossary
- http://www.desarrolloweb.com/faq/408.php
- http://www.iso.org/iso/en/prods-services/ISOstore/store.html
- http://www.aenor.es/desarrollo/normalizacion/normas/buscadornormas.asp
- http://opendocument4all.com/
- http://sourceforge.net/projects/ooo-word-filter
- http://www.mnlibros.com.ar/DespLibro.asp?Libro=8478290761
- http://www.movimientos.org/imagen/Ecuador Decreto 1014 software libre.pdf
- http://www.alcancelibre.org/article.php/decreto-de-uso-soft-libre-en-ecuador


**Para el Desarrollo del software.**

**Textos:**


- Coloma Andrade María de los Ángeles, DESARROLLO E IMPLEMENTACIÓN DE UN SISTEMA WEB PARA LA ASOCIACIÓN DE PRODUCTORES DE CAFÉ DE ALTURA DE ESPÍNDOLA Y QUILANGA, Loja 2010.
- Manuel ortez, Manual de Java, universidad del Salvador , diciembre del 2006
- MySQL AB ,Manual de Mysql, Diciembre 20 del 2011
- Steven Holzner, Anaya.Multimedia.La.Biblia.De.Java.2, Octubre 10 del 2009
- Lan Gilfillan, Anaya. Multimedia.La.Biblia.De.Mysql.pdf, Noviembre 25 del 2009
- Bustos Junior, Instalación Joomla 1.5, Febrero 10 del 2008
- Mario Carvajal, Manual de Joomla en español, Noviembre 28 del 2006
- ESIME-CULHUACAN, Manual básico de java, Septiembre 15 del 2008
- Foros de java online.
- Oracle, Manual de manejo de netbeans, julio 28 del 2010


**Direcciones Electrónicas.**

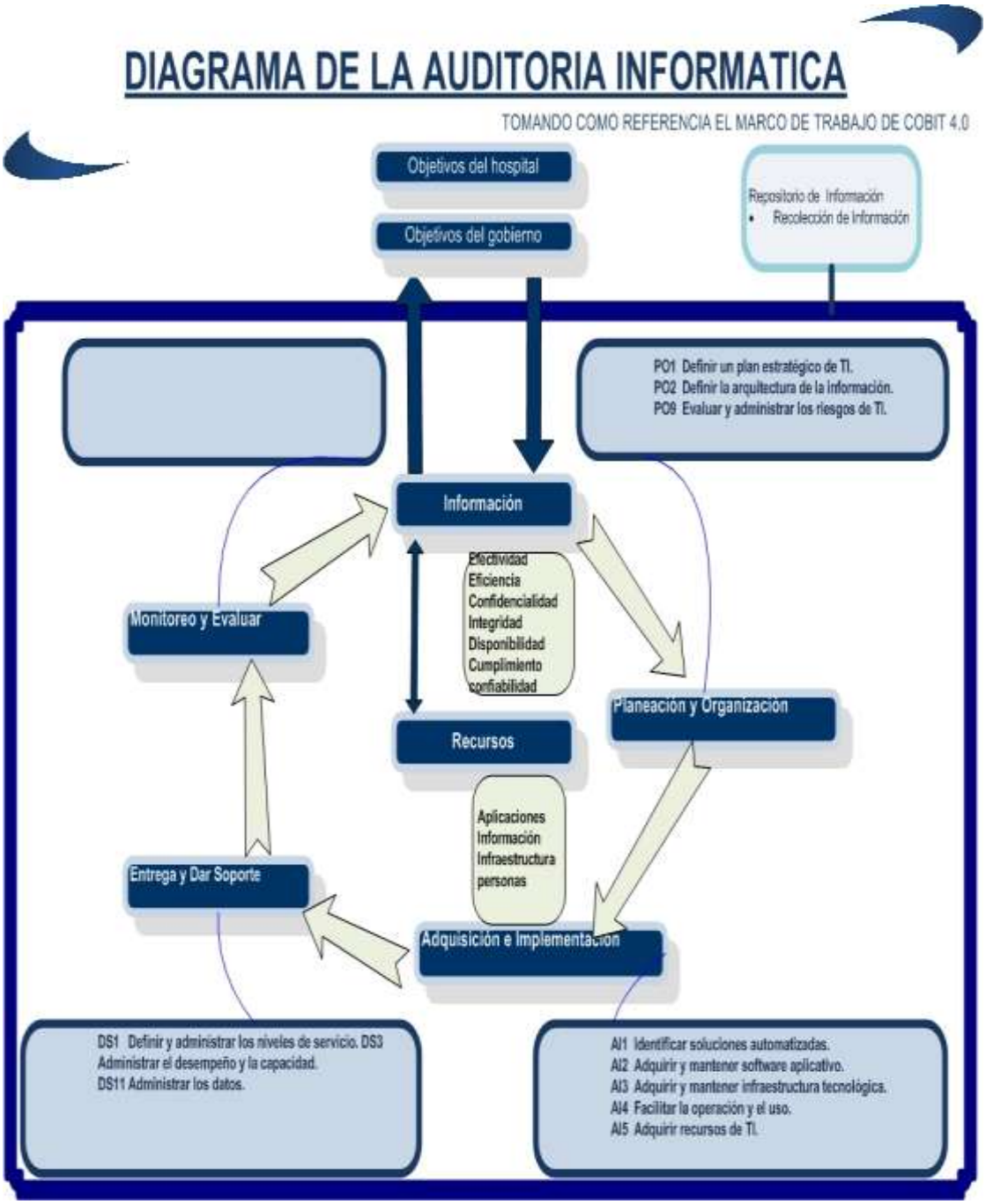

- http://www.netbeans.org
- http://jasperforge.org

- http://dev.mysql.com
- http://php.net
- http:// www.apache.org
- http://www.joomlaspanish.org
- http://www.centos.org
- http://es.wikipedia.org/wiki/Java
- http://es.wikipedia.org/wiki/Joomla
- http://es.wikipedia.org/wiki/Php
- http://es.wikipedia.org/wiki/Servidor_apache
- http://es.wikipedia.org/wiki/Netbeans
- http://es.wikipedia.org/wiki/CentOS
- http://lists.centos.org/mailman/listinfo/centos-es

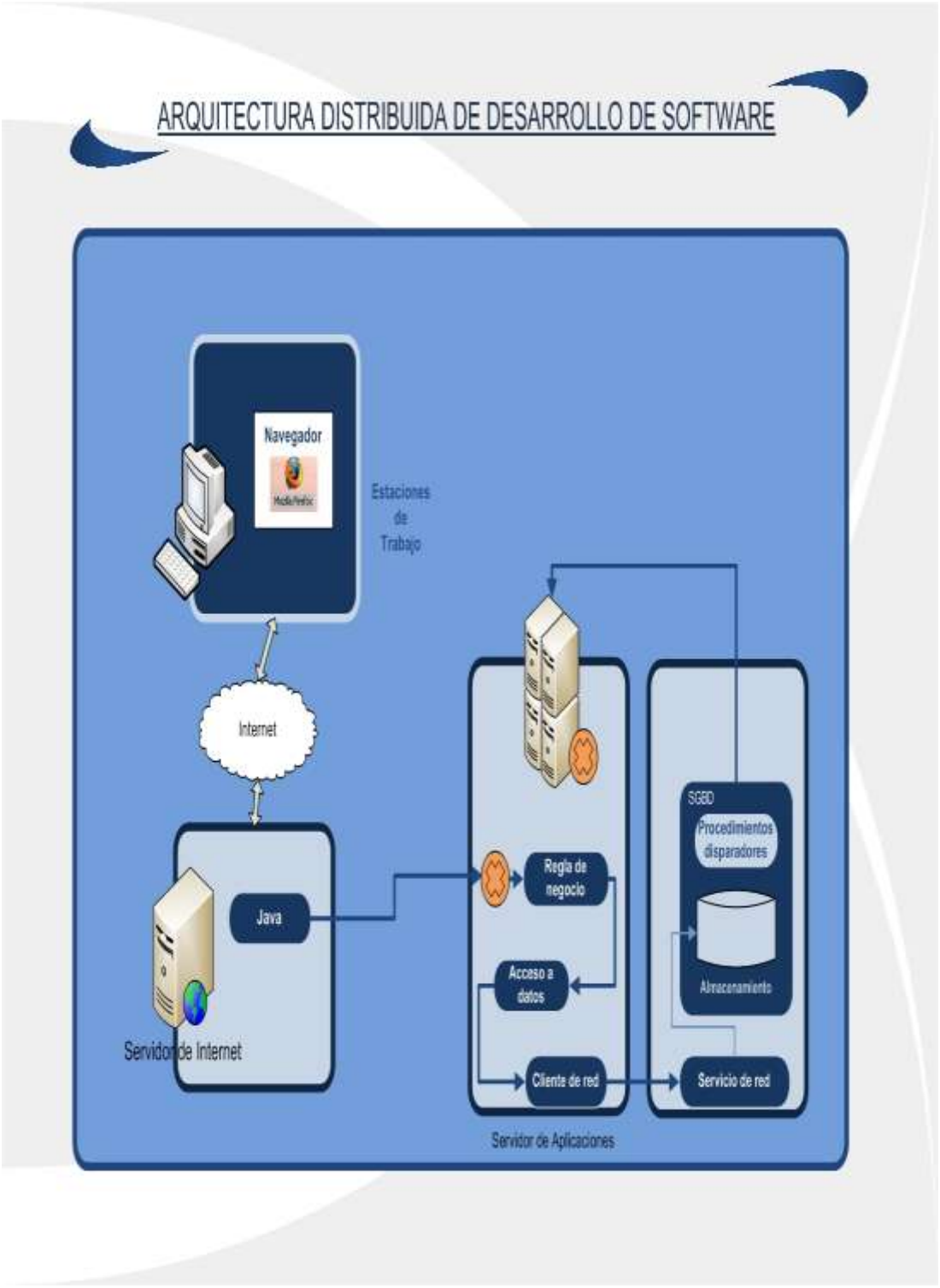
# ANEXOS

## Para la Auditoría

**ANEXO 1**



**ANEXO 2**


ARQUITECTURA DISTRIBUIDA DE DESARROLLO DE SOFTWARE
Navegador
Estaciones de Trabajo
Internet
Java
Servidor de Internet
Regla de negocio
Acceso a datos
Cliente de red
SGBD
Procedimientos disparadores
Almacenamiento
Servicio de red
Servidor de Aplicaciones

**ANEXO 3**

**FORMATO PARA ANALIZAR LA INFORMACION RECOLECTADA EN EL HOSPITAL ISIDRO AYORA LOJA**

| COD_INF | FECHA_SOL | FECHA_ENT | FUENTE_INF | RESPONSABLE | TIPO_INF | ANLISIS DE LA INFORMACIÓN |
|---|---|---|---|---|---|---|
| EOHI_01 | 11/09/2009 | 11/09/2009 | Departamento de Gestión de Servicios Institucionales | Ing. Ángel Cárdenas | Documento de la Estructura Organizacional del HGPIA-Loja | **VER ANEXO No 3.1** |
| ENCU_02 | 15/10/2009 | 15/11/2009 | Los 42 departamentos del HPGIA | 61 Personas que laboran en el área administrativa de los 42 departamentos del HPGIA | Tabulación de Datos de las encuestas aplicadas al personal administrativo que labora en los 42 departamentos del HPGIA | **VER ANEXO No 3. 2** |
| ENTR-03 | 19/11/2009 | 05/01/2009 | Los 42 departamentos del HPGIA | 42 Personas, que laboran como coordinadores o líderes, en los 42 departamentos del HPGIA | Tabulación de datos de las entrevistas aplicadas a los coordinadores y lideres, que trabajan en los 42 departamentos del HPGIA | **VER ANEXO No 3. 3** |
| LHST-05 | 26/01/2010 | 05/02/2010 | Gestión Informática | Ing. Mario Cueva (Administrador encargado del Centro de Computo del HPGIA) | Documentación del siguiente listado : **Hardware:** PC´S, Laptops y Servidores. **Software:** Ofimática, Sistemas de Información, Base de Datos, Sistemas Operativos. **Telecomunicaciones:** Enlaces, Hardware para Comunicaciones, Telefonía (marca, modelo), Tipo de Cableado, Proveedor de Internet | **VER ANEXO No 3. 4** |
| INVI-06 | | 12/02/2010 | Gestión Informática | Ing. Mario Cueva (Administrador encargado del Centro de | Inventario de computadoras del HPGIA | **VER ANEXO No 3. 5** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Computo del HPGIA) | | |
| IVAF-07 | | 12/01/2010 | Gestión Servicios Institucionales | Ing. Ángel Cárdenas (Administrador del HPGIA) | | **VER ANEXO No 3. 6** |
| RIAF-08 | | 21/04/2009 | MINISTERIO DE SALUD PUBLICA DIRECCIÓN DE GESTIÓN ADMINISTRATIVA-UNIDAD DE ACTIVOS FIJOS | Lcda. María Eugenia Aguirre (Directora de Gestión Administrativa) | Reglamento Interno para la Administración y Control de Activos Fijos | **VER ANEXO N 3. 7** |
| **PODI_09** | **14/09/2009** | **15/09/2009** | **Gestión Informática** | **Ing. Mario Cueva (Administrador del departamento informático del HGPIA-Loja)** | Documento sobre el perfil optimo de desempeño individual del servidor Ing. Mario Cueva. Encargado del departamento Informático<br>**Actividad esencial**<br>✓ **Plan informático y ejecución l**<br>✓ **Plan de mantenimiento se software y hardware.**<br>✓ **Plan de mejoramiento de procesos automatizados.**<br>✓ **Administración de redes de conectividad y central telefónica.**<br>✓ **Plan informático de contingencia y ejecución.** | **VER ANEXO No 3. 8** |
| **IMVI_10** | **23/03/2010** | **23/03/2010** | **Subproceso** | **Ing. Mario Cueva** | **Imágenes y videos obtenidos de las** | **VER ANEXO No 3. 9** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | **Gestión Informática** | **(Administrador del departamento informático del HGPIA-Loja)** | **instalaciones del centro de cómputo del HGPIA-Loja.** | |

**ANEXO No 3.1**

El Ministerio de Salud Pública del Ecuador, establece el modelo estándar para organizar los procesos que se manejan en hospitales públicos, revisando el documento de la Estructura Organizacional por Procesos del HGPIA-Loja, se llegó a determinar que no consta en el un proceso que se denomine Gestión Informática, como se puede notar la Tecnología de la Información es aún incipiente en las instituciones de Salud Pública, no se presta atención a que la TI, se ha convertido en una herramienta poderosa que puede ayudar a llevar los procesos de forma eficiente e independiente. Se debería incluir el proceso Gestión Informática dentro de la estructura organizacional, para que a través de esta pueda ejercer su propia autonomía, en donde se pueda administrar adecuadamente los recursos asignados y ejecutar sus propias actividades.

**ANEXO No 3.2**

El siguiente análisis corresponde a los resultados de las encuestas aplicadas a 61 personas que laboran en el área administrativa de los 42 departamentos del HGPIA-Loja. Para una mejor interpretación de los resultados, el análisis se lo realizara pregunta por pregunta así como se lo detalla a continuación:

**Pregunta 1: ¿Existen equipos de computación en el Departamento de (nombre del departamento)?**

61 personas que representan el 100% respondieron que si existen equipos de computación en los departamentos que laboran. De las 61 personas que se encuesto se obtuvo la información de que en el Hospital Isidro Ayora existen 138 equipos informáticos de los cuales: 131 son pc´s, 5 son laptops y 2 son servidores.

**Pregunta 2: ¿El computador que usted usa cuenta con los componentes y periféricos necesarios para realizar sus actividades diarias?**

58 personas que representan el 95% respondieron que sus computadores si cuentan con todos los componentes y periféricos para realizar sus actividades. Mientras que 3 personas que representan un 5% respondieron que sus computadores no cuentan con los componentes o periféricos necesarios, solicitando: 1 quemador de CD O DV, 1 impresora y una mesa para computador.

**Pregunta 3: ¿Existe algún Sistema Informático implantado en el Departamento de (nombre del departamento) para cumplir con las labores diarias?**

23 personas que representan el 38%, respondieron que si existen Sistemas Informáticos implantados en sus departamentos, sistemas como el de Activos Fijos, el de Estadística, el de Control de Personal, el de Control de Recursos Humanos, el de Seguridad, el Soat, el Esiget, entre otros. Mientras que 38 personas que representan el 62% respondieron que no tienen ningún Sistema Informático implantado en su departamento, teniendo de cierta forma algunos departamentos la necesidad de implementar algún Sistema, como es el caso de Gestión Farmacia que requiere de un Sistema para llevar el Control de Ingresos y Egresos de medicamentos, Oferta y Demanda Hospitalaria requiere de un Sistemas que ayude a llevar el control de la Producción Hospitalaria, el área de Laboratorio Patológico requiere de un Sistema para llevar el Control de Registro de Exámenes que se realizan.

**Pregunta 4: ¿La/s computadora(s) del departamento (nombre del departamento) cuentan con servicio de Internet?**

24 personas que representan el 39%, respondieron que los computadores de sus respectivos departamentos si cuentan con servicio de internet, del 39% que dijeron si se obtuvo la información de que 33 computadores están conectados al internet. Mientras que 37 personas que representan el 61% dijeron que no tienen servicio de internet.

**Pregunta 5: ¿Existen claves de acceso para el uso del computador?**

40 personas que representan, el 66% respondieron que si existen claves de acceso para el uso del computador. Mientras que 21 personas que representan el 34%, dijeron que no hay claves de acceso para ingresar al computador.

**Pregunta 6: ¿Conoce usted de la existencia de algún antivirus instalado en el computador que usa?**

51 personas que representan, el 84% respondieron que **Si** había un antivirus instalado en los computadores. De estas 51 personas se obtuvo la siguiente información:

**NOMBRE ANTIVIRUS**

- 39 personas dijeron que el antivirus instalado es el Nod 32
- 2 personas dijeron que el antivirus instalado es el Eset Esmart Security

- 1 persona dijo que el antivirus instalado es el Avg.
- 9 personas dijeron desconocer el nombre del antivirus.

**PERIOCIDAD DE ACTUALIZACIÓN**

- 8 personas dijeron que se actualizaba cada mes
- 15 personas dijeron que se actualizaba cada 3 meses
- 6 personas dijeron que se actualizaba cada 6 meses
- 2 personas dijeron que se actualizaba cada año
- 6 personas dijeron que se actualizaba cada que se solicita
- 14 personas dijeron que se actualizaba automáticamente.

Mientras que 10 personas que representan, el 16 % dijeron **No** saber de la existencia de algún antivirus instalado en sus computadores, aduciendo que de eso se encarga el Centro de Cómputo.

**Pregunta 7: ¿Cree usted que el espacio físico es el adecuado para la ubicación del computador?**

32 personas que representan, el 52% respondieron que el espacio físico **Si** es el adecuado para la ubicación del computador que no existía inconveniente alguno, que estaban totalmente bien ubicados. Mientras que 29 personas que representan el 48% dijeron que **No** es adecuado el espacio físico, argumentado que: es muy reducido, existe poca ventilación en las habitaciones y los muebles para la ubicación del computador no son los adecuados.

**Pregunta 8: ¿Qué tipo de información usted maneja en el computador? Explique.**

Del 100% de la información que se procesa en el Hospital Isidro Ayora, el:

- 16,67% corresponde a Oficios
- 16,67% corresponde a Memorandos
- 16,67% corresponde a Informes
- 13,10% corresponde a Pedidos
- 4,37% corresponde a Ingresos (de pacientes, de insumos médicos, de equipos)

- 4,73% corresponde a Egresos (de pacientes, de insumos médicos, de equipos)
- 1,59% corresponde a Presupuesto
- 0,79% corresponde a Activos Fijos
- 0,79% corresponde a Compras Públicas
- 3,97% corresponde a Certificados
- 1,59% corresponde a Planillas de Facturación
- 5,16% corresponde a Control de Personal (Asignación de turnos de personal, Conteo de horas de trabajo)
- 2,38% corresponde a Elaboración de Contratos del Personal
- 1,19% corresponde a Elaboración de Proyectos
- 2,78% corresponde a Planes
- 0,79% corresponde a Producción Hospitalaria
- 7,14% corresponde a Registro de Pacientes

Si sumamos todos los porcentajes detallados anteriormente, vamos a obtener el 100%, que representa el total de la información que se maneja en el hospital.

**Pregunta 9: ¿Guarda usted la información que maneja en el computador?**

55 personas que representan el 90,16%, respondieron que **Si** guardan la información que manejan en el computador. De las 55 personas respondieron se obtuvo además la información de cuál es la periodicidad con que se obtiene los respaldos y en que medio lo hacen. A continuación se hace el detalle:

**PERIODICIDAD CON QUE SE OBTIENEN LOS RESPALDOS DE INFORMACIÓN**

- **47** personas dijeron que obtienen respaldo de la información a **DIARIO**
- **6** personas dijeron que obtienen respaldo de la información **SEMANAL**
- **2** personas dijeron que obtienen respaldo de la información **MENSUAL**

**MEDIO FISICO EN QUE ALMACENAN LOS RESPALDOS DE INFORMACIÓN**

- **55** personas dijeron que guardaban los respaldos en el **Disco Duro**

- **10** personas dijeron que guardaban los respaldos en la **Flash Memory**
- Mientras que 6 personas que representan el 9,84%, dijeron que **No** guardan la información que manejan en el computador.

**Pregunta 10: ¿Con qué frecuencia el personal técnico de la institución le da mantenimiento a los equipos?**

Del 100% de personas que se entrevistó en el Hospital Isidro Ayora, respondieron de la siguiente manera:

- **1** persona que representa el 1,64% respondió que se lo hacía **SEMANAL**
- **4** personas que representa el 6,56% respondieron que se lo hacía **MENSUAL**
- **52** personas que representa el 85,25% respondieron que se lo hacía **CUANDO SE SOLICITA**
- **4** personas que representa el 6,56% respondió que **NUNCA**

**Pregunta 11: ¿En su lugar de trabajo existe algún otro elemento electrónico para cumplir con sus labores?**

6 personas que representan el 9,84 % respondieron, que **Si** existen elementos electrónicos**,** entre los que se encuentran: 2 copiadoras, 2 duplicadoras, 1 cámara de digital, 4 fax modem. Mientras que 55 personas que representan el 91,16% respondieron que **No** existían.

**Pregunta 12: Describa el procedimiento que el departamento sigue para solicitar el cambio, actualización, reparación o adquisición de un equipo de cómputo u otro relacionado.**

El 100% de encuestados definieron el siguiente procedimiento:

**PARA ACTUALIZACIÓN Y REPARACIÓN**

- Emitir hoja de trabajo al Centro de Computo (Administrador)

**PARA CAMBIO O ADQUISICIÓN**

- Emitir una Solicitud de Cambio o de Adquisición al departamento de Gestión Estratégica (Director).

**Pregunta 13: En relación al suministro eléctrico en el departamento, éste es**

29 personas que representan el 48%, respondieron que el suministro eléctrico es ininterrumpido, 32 personas que representan el 52% respondieron que es variable (con picos).

**CON RELACIÓN AL PERFIL DEL PERSONAL ADMINISTRATIVO**

**Pregunta 14: ¿Usted tiene conocimientos de computación?**

El 100% de las personas encuestadas respondieron que si tienen conocimientos de computación, a estas personas además se les pidió indicar. **¿Cuál es su nivel de conocimiento?,** las mismas que respondieron a la interrogante de la siguiente manera:

- 31 personas dijeron que su nivel de conocimiento es **BAJO**
- 25 personas dijeron que su nivel de conocimiento es **MEDIO**
- 5 personas dijeron que su nivel de conocimiento es **ALTO**

**Pregunta 15: Indique que programas del computador usted maneja.**

- El 100% de las personas encuestadas maneja Word, pero cabe aclarar que hay algunas que si manejan otro tipo de programas tal como se detalla a continuación:
- El 95% de las personas encuestadas maneja Word y Excel.
- El 49% maneja Power Point

**Pregunta 16: ¿Posee usted una guía de normas y reglas, que le indiquen como usar adecuadamente los recursos tecnológicos de la institución, en particular de los de su área de trabajo?**

El 100% de las personas encuestadas en el hospital, respondieron que **No** tenían una guía de normas y reglas que les indique como usar adecuadamente los recursos tecnológicos de la institución.

**ANEXO No 3.3**

El siguiente análisis corresponde a los resultados de las entrevistas aplicadas a los coordinadores y líderes de los 42 departamentos del HGPIA-Loja.

Con respecto a los resultados de las entrevistas se encontró lo siguiente:

**Pregunta1:**

Los resultados de las entrevistas dicen que, existen 138 equipos informáticos en la institución (131pc's, 5 laptops y 2 servidores), se entrevistó a 42 personas de las que 31 que representan el 74% respondieron que **Si** son suficientes los equipos asignados a sus departamentos, mientras que 11 personas que representan el 26% respondieron, que **No** son suficientes los computadores asignados. De los 138 computadores del Hospital 125 que representa el 91% están en buen estado mientras que 13 computadoras que representa el 9% están en mal estado. Además 109 computadores que representan el 79% están acorde a la tecnología actual, mientras que 29 que representan el 21% son computadores que no corresponden a la tecnología actual.

**Pregunta 2:** 11 personas que representan el 26% dijeron que si existen herramientas software (Soat, Esiget, Esipren, Activos Fijos, Control de Personal, Estadística, Seguridad) implantadas en sus departamentos, mientras que 31 personas que representan el 74% respondieron a que no tienen software instalado en sus computadores.

**Pregunta 4:** De 42 personas encuestadas, 38 personas que representan el 90% respondieron que la institución si se debería capacitarlos en el uso de herramientas de ofimática, mientras que 4 personas que representa el 10% respondieron que no es responsabilidad de la institución capacitarlos, creen que la capacitación es personal.

**Pregunta 5:** 11 personas que representa el 26%, grupo en el que se incluye a las máximas autoridades del hospital, respondieron que si existen recursos suficientes para adquirir equipos de computación, mientras que 8 personas que representa el 19% respondieron que no existen los recursos y por último 23 personas que representan el 55% adujeron que simplemente lo desconocen.

**Pregunta 6:** 40 personas que representan el 95% respondieron a que se debería crear un manual de políticas a través del cual se puede dar el uso y manejo adecuado de los equipos de computación, mientras que 2 personas que representa el 5% dijeron que no porque si existía dicho manual.

**Pregunta 7:** 36 personas que representa el 86% supieron responder que la información que manejan en su departamento si es crítica, mientras que 6 personas que representan el 14% respondieron que la información que manejan no es crítica.

**Pregunta 8:** 42 personas que representan al 100% de los entrevistados, supieron responder que no existen planes de contingencia para salvaguardar la integridad de los equipos computacionales en el caso de robo, incendio, inundación y perdida de energía eléctrica.

**Pregunta 9:** 19 personas que representan el 45% respondieron que si tienen la información digitalizada, mientras que 23 personas que representan el 55% respondieron que la información no está digitalizada.

**Pregunta 10:** 15 personas que representan el 36% respondieron que si estaban de acuerdo con el servicio que ofrece el centro de computo, que les parecía eficiente, mientras que 27 personas que representan el 64% respondieron que no que el servicio les parecía ineficiente, e insuficiente principalmente por la falta de personal, falta de tecnología y falta de una planificación.

**Pregunta 11:** 16 personas que representan el 38% respondieron que 36 computadores si cuentan con servicio de internet, mientras que 26 personas que representan el 62% respondieron que los computadores de su departamento no cuentan con este servicio.

**Pregunta 12:** 42 personas que representan el 100%, supieron manifestar que existe falta de planificación y falta de recurso humano para que el Centro de Computo del HGPIA-Loja pueda cumplir con los servicios que presta de manera eficiente.

**ANEXO No 3.4**

De acuerdo a la información obtenida del listado de hardware, software y telecomunicaciones del HGPIA-Loja, encontramos que a nivel de:

**Hardware,** existen 171 computadoras, 8 portátiles y 3 servidores en la institución

**Software,** existen 6 Sistemas de información para la institución:

1. Sistema de Control de Recursos Humanos (Programas empleados)
2. Sistema de Facturación (Administración de Caja)
3. Sistema de Administración de Recursos Humanos (Recursos Humanos).
4. Sistema de Cámaras (Servicios Generales).
5. Sistema de Control de Activos Fijos (Contabilidad)
6. Administración y Control de Procesos de Estadística (Implementándose).

**Ofimática:** tiene programas Microsoft Office no licenciados

**Base de Datos:** Mysql Server versión 3.23.49-nt, SQL Server 2005 (no licenciado).

**Sistema Operativo:** Windows XP, Fedora 11, Ubuntu, Windows 2000 Profesional, Windows server 2000, Windows server 2008 (no licenciado).

**Elementos de Telecomunicaciones en el Centro de Cómputo:**

Existen 3 switch Cisco Catalyst 2900 Series XL, 24 puertos
1 Ruteador Relay Cisco 3600
Cableado estructurado puntos de voz 95 y puntos de datos de 103, categoría 5.
Edificio nuevo 18 puntos de voz y 30 puntos de datos, categoría 6.
Proveedor Internet CNT
Central Telefónica Alcatel 4400.
UPS-3000 Powerware Prestige.

**Analizando la información obtenida:**

1. Existe inconsistencia de la información, el hardware listado en el documento entregado por el Ing. Mario Cueva describe que existen 182 equipos incluyendo, las pc´s, laptop y servidores, mientras que de acuerdo a los resultados de las entrevistas y encuestas, se encontró que existen 138 equipos informáticos en los que se incluye las pc´s, laptops y servidores.
2. No existen las respectivas licencias del software instalado, en los equipos de la institución.
3. Los Sistemas de Información de la institución han sido desarrollados para trabajar en entornos Windows, según el decreto 1014 de la República del Ecuador, establece que toda institución pública debe incorporar software libre para sus sistemas y equipamiento informático.

**ANEXO No 3.5**

De acuerdo al reglamento Interno para la Administración y control de Activos Fijos del Ministerio de Salud Pública, en su artículo 47.2, le corresponde al **Departamento de Informática** llevar un inventario actualizado de los equipos informáticos de la institución. Pero de acuerdo al listado entregado por gestión informática, este no cumple, apenas 87 equipos están levantados en el inventario, valor que representa el 48%, faltando aun un

62% de equipos por levantar. Es decir no hay un inventario actualizado no se está cumpliendo con el reglamento.

1. Falta de una política en la que se estipule que cada computador debe tener una clave personal, de usuario o de administrador. Esta no debe ser escrita en ningún medio impreso o digital. Dicha clave debe ser conocida únicamente por el operador o responsable del mantenimiento físico y lógico del equipo.
2. Para realizar un mantenimiento correctivo, se requiere saber las series de las piezas que son remplazadas, para de esa forma llevar un control más detallado de que componentes se arreglaron o reemplazaron en el equipo, esta información ayudara a mantener actualizado el inventario. Cabe aclarar que en el inventario entregado por Gestión Informática, no se encuentran series de ningún componente que integra el computador.
3. En el Inventario de Gestión Informática se debería listar a los equipos de acuerdo al código de activos fijo, para poder llevar un mejor control de los equipos existentes. Revisando el inventario estos no están listados por el código de activo fijo.

**ANEXO No 3.6**

De acuerdo al reglamento Interno para la Administración y control de Activos Fijos del Ministerio de Salud Pública, el departamento de **Gestión Servicios Institucionales** tiene a cargo la administración y control del listado de activos fijos clasificados por fecha y compra de equipos de cómputo, sistemas, paquetes informáticos y equipos para comunicación del HGPIA-Loja, encontramos que a nivel de:

- ✓ **Equipos**
- ✓ **Sistemas**
- ✓ **Paquetes informáticos**
- ✓ **Equipos de comunicación**

En el documento entregado por la unidad de activos fijos sobre los ítems antes mencionados no se encuentra la información correcta de cómo llevar los activos fijos de la institución, solo existe información escueta de la misma

.

A continuación detallaremos la información entregada:

**Equipos de cómputo**

En el documento de activos sobre los equipos de cómputo se tiene lo siguiente:

- ✓ Descripción de activo
- ✓ Fecha de adquisición
- ✓ Costo
- ✓ Cantidad
- ✓ Subtotal
- ✓ Ubicación
- ✓ Responsable

En el documento descrito no se encuentra detallado todos los componentes o periféricos, sus números de series de cada equipo de cómputo de la institución

**Sistemas**

Los sistemas adquiridos por el hospital algunos no tienen manuales para su manejo. Además no cumplen con la función para la cual fueron adquiridos, a continuación detallaremos los siguientes:

1. Sistema de Control de Recursos Humanos (Programas empleados)
2. Sistema de Facturación (Administración de Caja)
3. Sistema de Administración de Recursos Humanos (Recursos Humanos).
4. Sistema de Cámaras (Servicios Generales).
5. Sistema de Control de Activos Fijos (Contabilidad)
6. Administración y Control de Procesos de Estadística (Implementándose).

**Paquetes informáticos**

En el inventario entregado de los activos fijos no se encuentra detallado los paquetes informáticos por cada equipo de cómputo ni su licenciamiento.

**Equipos de comunicación**

En los equipos para la comunicación no se encuentra detallada en forma correcta la cantidad exacta de los teléfonos que existen en la institución ya que en el documento existe información escueta de la misma.

Los equipos deberán están registrados con el mismo código de activo fijo tanto la para Unidad de Activos Fijos como para el departamento de Gestión Informática; clasificados

por fecha y compra de equipos de cómputo, sistemas, paquetes informáticos y equipos para comunicación del HGPIA-Loja.

**ANEXO No 3.7**

De acuerdo al **Reglamento Interno para la Administración y Control de Activos Fijos del Ministerio de Salud Pública**, en el **CAPÍTULO IX (MANTENIMIENTO Y CONTROL DE EQUIPOS INFORMATICOS)**, establece que el departamento de Gestión Informática o a quien más corresponda, debe cumplir obligatoriamente con las especificaciones que se enuncian en los **artículos 47, 48, 49, 50 y 51** del reglamento.

Para hacer un poco de énfasis en lo que enuncian los artículos mencionados anteriormente, se va a analizar a cada uno, y a la vez se determinara, si estos se están aplicando en la Administración y Control de los recursos de TI, que en definitiva de acuerdo a la administración de los bienes públicos estos vendrían a ser activos fijos del hospital Isidro Ayora.

**Art.47.- Del Control**

47.1 Manifiesta que el jefe de activos fijos conjuntamente con el jefe de la unidad informática o quien haga sus veces, deberán remitir obligatoriamente a la Dirección de Gestión Administrativa, un informe trimestral con documento de respaldo de la situación de los equipos.

En caso de cambio, adición o disminución de accesorios a los equipos informáticos, el jefe de Informática informara en el plazo de 48 horas, dichos cambios al proceso de Gestión Administrativa, con copia de la unidad de Activos Fijos o quien haga sus veces con el fin de actualizar la hoja de vida y registro cantable del bien.

47.2 Corresponde al subproceso informática, independientemente del inventario que mantenga la Unidad de Activos Fijos, mantener una lista actualizada de los equipos informáticos de la institución.

47.3 El subproceso informática, deberá mantener un historial de los trabajos efectuados en los equipos

47.4 El subproceso informática, deberá mantener un registro actualizado del licenciamiento del software adquirido, el mismo que comprenderá el código de activo fijo, identificación del producto, descripción del contenido, número de versión, número de serie, nombre del proveedor, fecha de adquisición y otros datos que sean necesarios.

47.5 Los equipos informáticos tendrán un movimiento interno de acuerdo al formulario "Movimiento Interno de Activos Fijos /equipos informáticos", establecido para el efecto, previo el conocimiento del Director de Gestión Administrativa y el Jefe de la Unidad de Activos Fijos.

47.6 El subproceso de informática, deberá mantener actualizados los programas antivirus, así como los respaldos de los informes de todos los procesos y subprocesos.

**Art.48.- Del Mantenimiento**

El mantenimiento de los equipos informáticos está a cargo del subproceso informática o quien haga sus veces.

**Art.49.- Del Plan de Mantenimiento**

El Hospital Isidro Ayora deberá tener un Plan Anual de Mantenimiento de equipos Informáticos, el mismo que se ejecutara en base al cronograma trimestral con financiamiento y aprobación por las máximas autoridades. Este plan lo deberá realizar el subproceso Informática

**Art.50.- Reparación en talleres particulares**

Cuando los equipos, deban ser reparados en talleres fuera de la institución, previamente a su salida, se debe contar con un informe técnico del subproceso informática, y autorización del Director de Gestión Administrativa a la Unidad de Activos Fijos, mediante la subscripción del formulario establecido para el efecto, "Autorización de Salida de Activos Fijos" y con los documentos personales de respaldo del custodio personal del equipo.

**Art.51.-Clase de Mantenimiento**

51.1 Mantenimiento Correctivo, procedimiento utilizado para arreglar un equipo deteriorado o dañado

51.2 Mantenimiento Preventivo, inspección periódica de equipos, para evaluar su funcionamiento y encontrar fallas, prevenir y poner en condiciones de funcionamiento óptimo el equipo.

51.3 Mantenimiento Predictivo, monitoreo continuo de los equipos con el fin de detectar y evaluar cualquier pequeña variación en su funcionamiento, antes de que se produzca una falla.

**ANEXO No 3.8**

De acuerdo al **Ministerio de salud Pública del Ecuador** el perfil óptimo del desempeño individual del servidor público encargado de la Administración del Centro de Computo del **HGPIA-Loja**, tendrá que realizar las actividades para lo cual ha sido contratado.

A continuación mediante el análisis realizado detallaremos los procesos que no se cumplen a cabalidad por parte del administrador del centro de cómputo del HGPIA-Loja.

- ✓ No existe un plan informático y ejecución / reportes de análisis y requerimientos de los recursos tecnológicos, control de consumo de central telefonía, elaborar reportar actividades del plan operativo.
- ✓ No existe un plan de mantenimiento de software y hardware / Operador, supervisor, mantenimiento preventivo y correctivo de hardware, software y central telefónica (teléfonos), cámaras digitales, instalación de componentes de computadoras.
- ✓ No existe un plan de mejoramiento de procesos automatizados/ Asesor a autoridades y empleados de la institución en los campos informático y tecnológico, así como su automatización. Participar en el comité institucional como asesor para la adquisición de recursos tecnológicos
- ✓ No existe un plan de Administración de redes de conectividad y central telefónica/ Supervisor, mantenimiento preventivo y seguridad de la red, administrar la red y central telefónica.
- ✓ No existe un plan informático de contingencia y ejecución/ Controlar, respaldar y asesorar el desarrollo, mantenimiento y funcionamiento de sistemas informáticos y tecnológicos (base de datos, sistemas operativos, central telefónica, etc.).

1. Se ha solicitado la información formalmente e informalmente sobre el documento de los planes elaborados para cumplir con los productos /actividades esenciales para la administración del centro de cómputo del subproceso de gestión informática y estos no existen.

2. Se realizan las actividades esenciales, semanalmente pero no se tiene documentado los procesos que se realizan.

No se cumplen con los indicadores y metas de todos los productos/ actividades esenciales del subproceso de gestión informática por parte de la persona que es responsable de la administración del centro de cómputo debido a esto, no se pude dar una mejor productividad a los equipos de cómputo, de comunicación y sistemas informáticos que tiene la institución.

**ANEXO No 3.9**

De acuerdo a las imágenes obtenidas de la sala de servidores que se encuentra dentro del centro de cómputo del **HGPIA-Loja,** nos encontramos que no existe la seguridad respectiva para el acceso a las instalaciones de ninguna índole ya que cualquier persona puede acceder al mismo.

Además el acceso a la sala de servidores no tiene las seguridades respectivas; así lo demuestran las fotos obtenidas, también existe materiales que pueden servir como combustible al momento de provocarse un incendio.

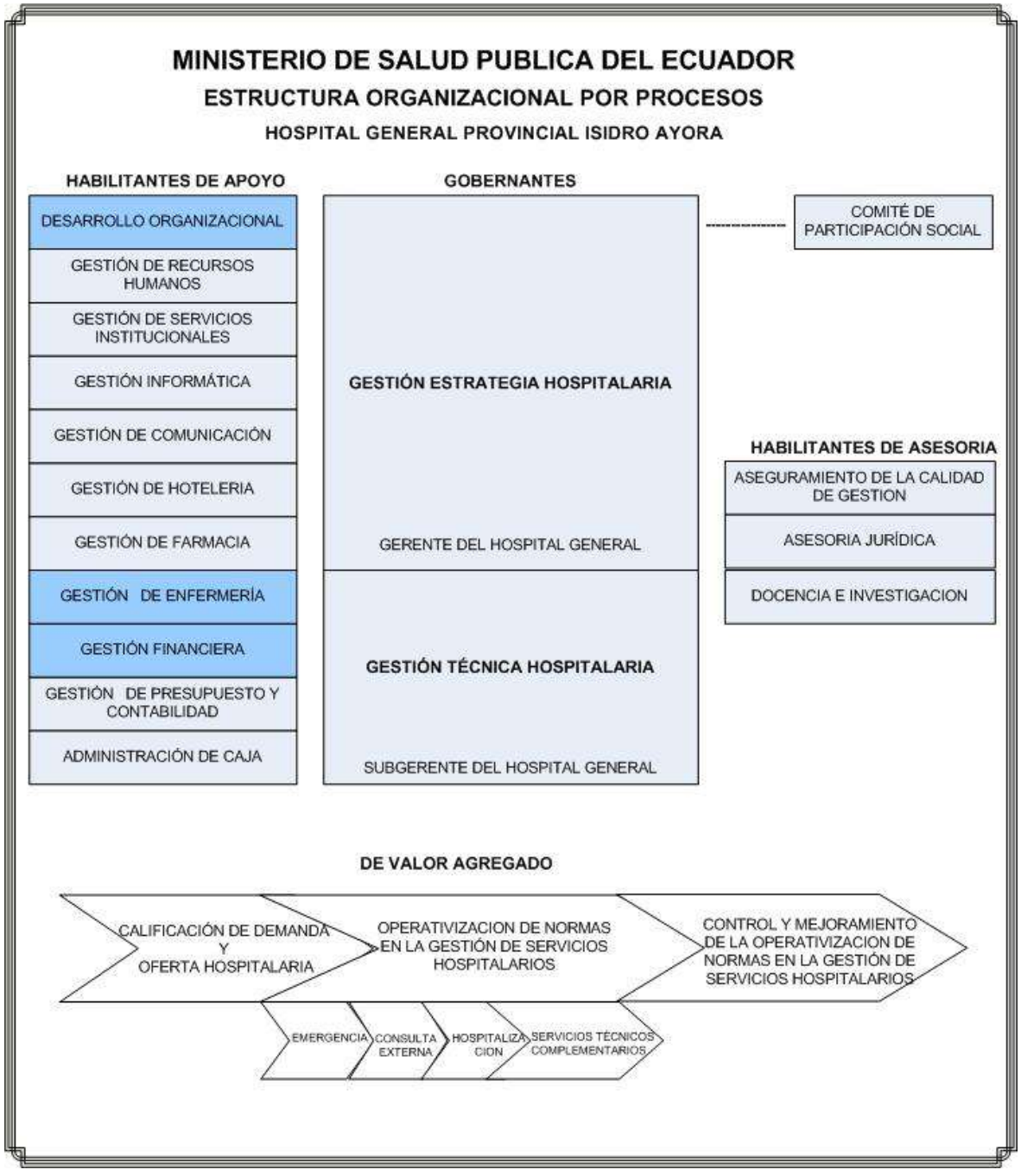
El cableado de red no se encuentra debidamente ordenado, ya que no existen los pack panel para ordenarlos de manera correcta.

La temperatura ambiental de la sala de servidores no es la correcta ya que deberá estar entre los 17 a 19 grados centígrados, además no existe detectores de humo, cámaras de vigilancia tampoco existen extintores especiales para salvaguardar los servidores y equipos informáticos del centro de cómputo del hospital, sólo se encuentran 1 extintor de tipo ABC que esta caducado y que no sirve para apagar el fuego de equipos informáticos.

El material que está construido la sala de servidores no es el adecuado en caso de un incendio este servirá como un combustible para que se propague el fuego rápidamente en el centro de cómputo del hospital.

Las fotografías obtenidas nos demuestran cómo se lleva la seguridad en el centro de cómputo y por ende en la sala de servidores de la institución.

**ANEXO 4**


MINISTERIO DE SALUD PUBLICA DEL ECUADOR
ESTRUCTURA ORGANIZACIONAL POR PROCESOS
HOSPITAL GENERAL PROVINCIAL ISIDRO AYORA
HABILITANTES DE APOYO
DESARROLLO ORGANIZACIONAL
GESTIÓN DE RECURSOS HUMANOS
GESTIÓN DE SERVICIOS INSTITUCIONALES
GESTIÓN INFORMÁTICA
GESTIÓN DE COMUNICACIÓN
GESTIÓN DE HOTELERIA
GESTIÓN DE FARMACIA
GESTIÓN DE ENFERMERÍA
GESTIÓN FINANCIERA
GESTIÓN DE PRESUPUESTO Y CONTABILIDAD
ADMINISTRACIÓN DE CAJA
GOBERNANTES
GESTIÓN ESTRATEGIA HOSPITALARIA
GERENTE DEL HOSPITAL GENERAL
GESTIÓN TÉCNICA HOSPITALARIA
SUBGERENTE DEL HOSPITAL GENERAL
COMITÉ DE PARTICIPACIÓN SOCIAL
HABILITANTES DE ASESORIA
ASEGURAMIENTO DE LA CALIDAD DE GESTION
ASESORIA JURÍDICA
DOCENCIA E INVESTIGACION
DE VALOR AGREGADO
CALIFICACIÓN DE DEMANDA Y OFERTA HOSPITALARIA
OPERATIVIZACION DE NORMAS EN LA GESTIÓN DE SERVICIOS HOSPITALARIOS
CONTROL Y MEJORAMIENTO DE LA OPERATIVIZACION DE NORMAS EN LA GESTIÓN DE SERVICIOS HOSPITALARIOS
EMERGENCIA
CONSULTA EXTERNA
HOSPITALIZACION
SERVICIOS TÉCNICOS COMPLEMENTARIOS

**ANEXO 5**

**MODELO DE ENCUESTA APLICADA PARA EVALUAR SYSCORTI**

# UNIVERSIDAD INTERNACIONAL DEL ECUADOR SEDE LOJA.

## ENCUESTA APLICADA A LOS PROFESIONALES DE LA UIDE LOJA Y OTROS PROFESIONALES INFORMÁTICOS

Datos Informativos.

Nombres:……..

Cargos:……..

Fechas:……..

| **Instrucciones** |
|---|
| Estimado encuestado, por favor sírvase contestar las siguientes preguntas con el afán de evaluar la aplicación “SYSCORTI”, en algunas preguntas hay una opción elegible denominada “NO APLICA”, en estos casos si el usuario carece de conocimientos acerca de dicho tema puede marcar una opción y no responder el porqué. |

Facilidad de uso

1. ¿Qué valoración considera Ud. con respecto a la facilidad del uso de la aplicación "SYSCORTI"?

| | |
|---|---|
| Excelente | ( ) |
| Muy bueno | ( ) |
| Bueno | ( ) |
| Regular | ( ) |
| Medio | ( ) |

2. ¿Qué valoración Ud. consideraría en la aplicación y distribución de colores para aplicación "SYSCORTI" y para el portal web?

| | |
|---|---|
| Excelente | ( ) |
| Muy bueno | ( ) |
| Bueno | ( ) |
| Regular | ( ) |
| Medio | ( ) |

3. ¿Considera Ud. que la aportación de la información en cada una de las pantallas de la aplicación es completa?

| | |
|---|---|
| Si | ( ) |
| No | ( ) |

¿Por qué?.....
……..

4. Considera Ud. que los componentes de la aplicación reflejan la mayoría de los procesos utilizados en la productividad de los recursos de TI.

| | |
|---|---|
| Reflejan todos los procesos | ( ) |
| La mayoría de los procesos | ( ) |
| Algunos procesos | ( ) |
| Pocos procesos | ( ) |
| Ningún proceso | ( ) |
| No aplica | ( ) |

¿Por qué?.....
……

5. En una valoración de 1 al 10, establezca la aportación de información y de los procesos de los siguientes componentes.

| | |
|---|---|
| Bitácoras | ( ) |
| Planes administración de recursos TI. | ( ) |
| Recursos de TI | ( ) |
| Personal | ( ) |
| Procesos | ( ) |
| Infraestructura | ( ) |

¿Por qué?.....
……

## Tecnología

6. La tecnología java, php y Joomla, es apropiada para realizar y desarrollar soluciones informáticas de escritorio y portales web cliente servidor multiplataforma.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | ( ) |

¿Por qué?.....
……

7. Considera importante seleccionar una base de datos como mysql server 5.0 para trabajar con aplicaciones de escritorio y web.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | ( ) |

¿Por qué?.....
……

**Arquitectura.**

8. Utilizaría esta arquitectura mostrada en este sistema para construir una aplicación de escritorio y web.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | ( ) |

¿Por qué?.....
……

9. Considera de gran aporte ingenieril la construcción de aplicaciones de escritorio y web con herramientas multiplataforma gratuitas.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |

| | |
|---|---|
| No Aplica | ( ) |

¿Por qué?.....
……

10. ¿Considera una buena decisión a nivel de ingeniería de sistemas, que la solución desarrollada incluya dos aplicaciones de escritorio y web?

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | ( ) |

¿Por qué?.....
……

11. Considera Ud. la existencia de puntos negativos en la solución desarrollada que deberían solventarse para asegurar que la aplicación cumpla con mínimos elementos de ingeniería.

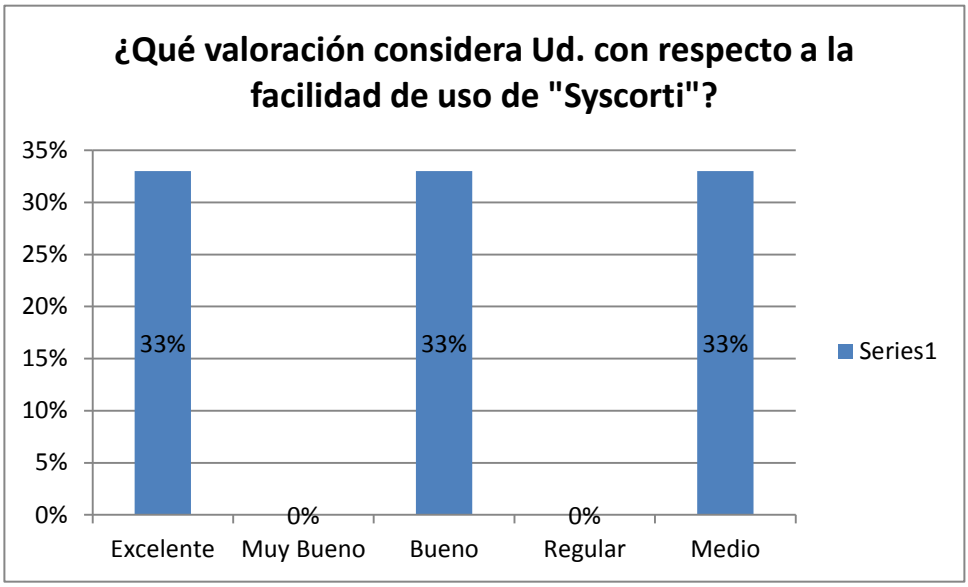
| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué o Cuales?.....
……
……
……
……

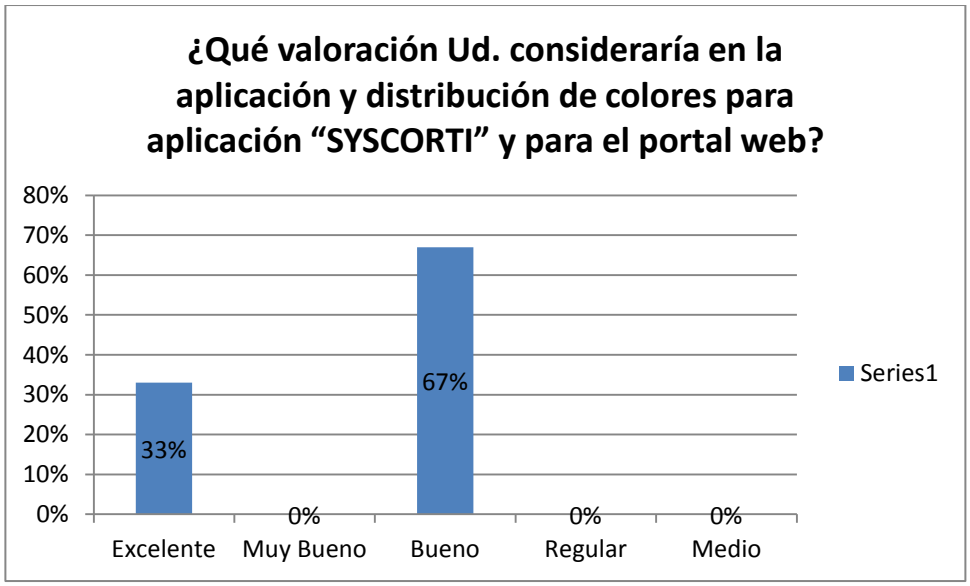
## Tabulación de datos

### Facilidad de Uso

### Pregunta 1.

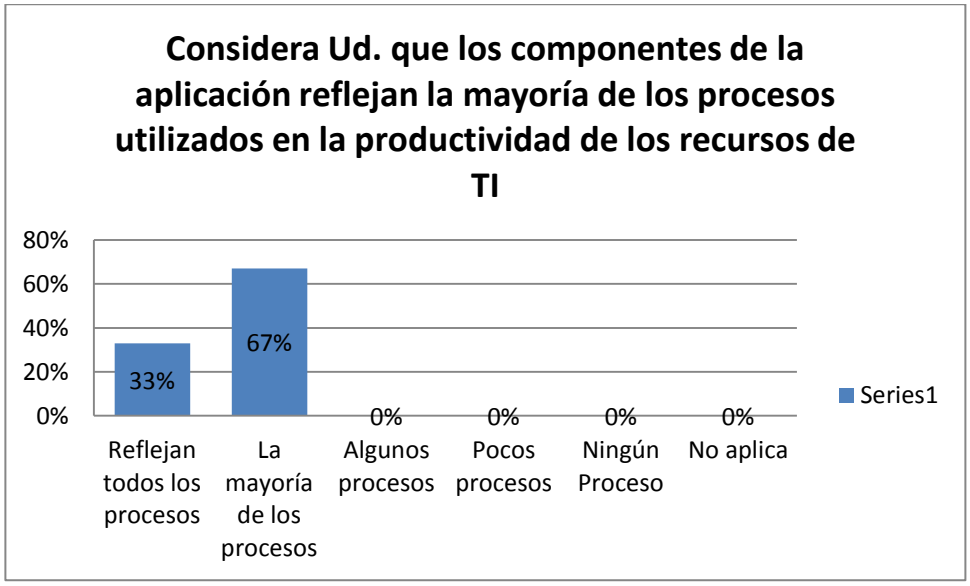



### Pregunta 2.



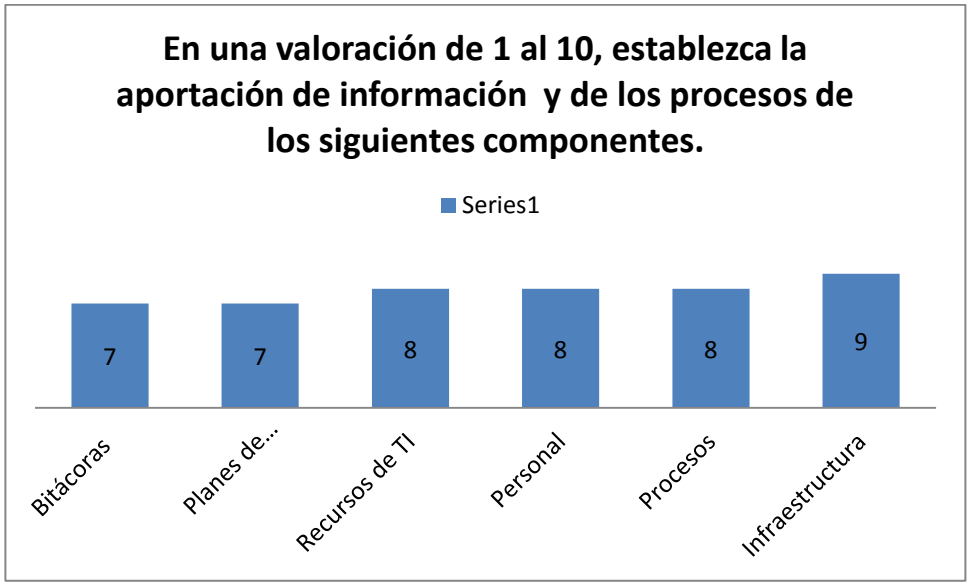
**Pregunta 3.**


**Pregunta 4.**

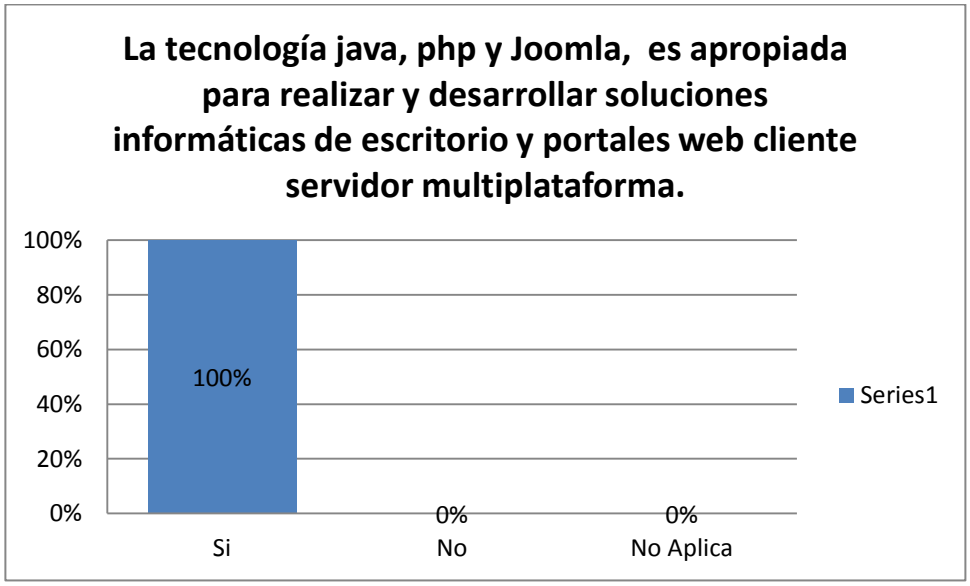


## Tecnología

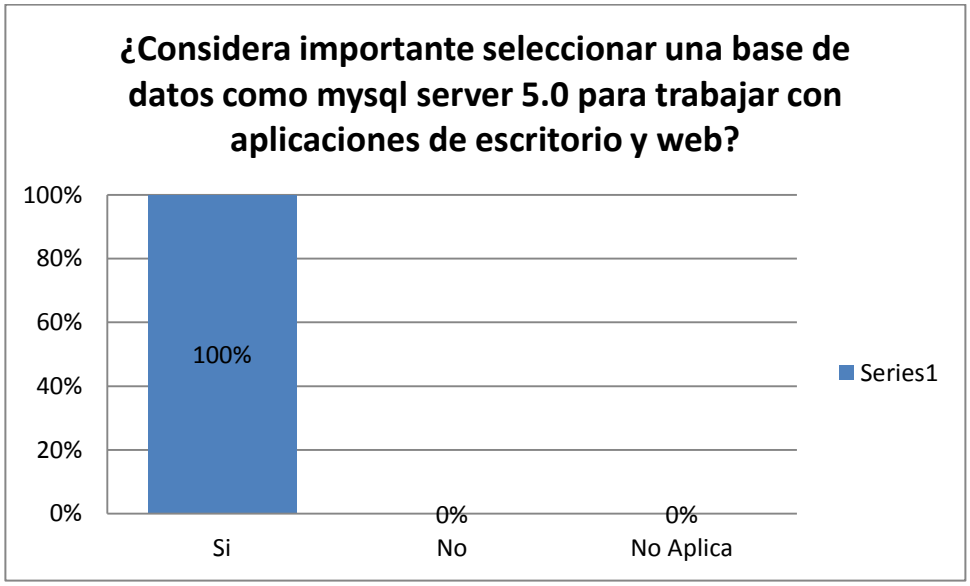
### Pregunta 5.




### Pregunta 6.

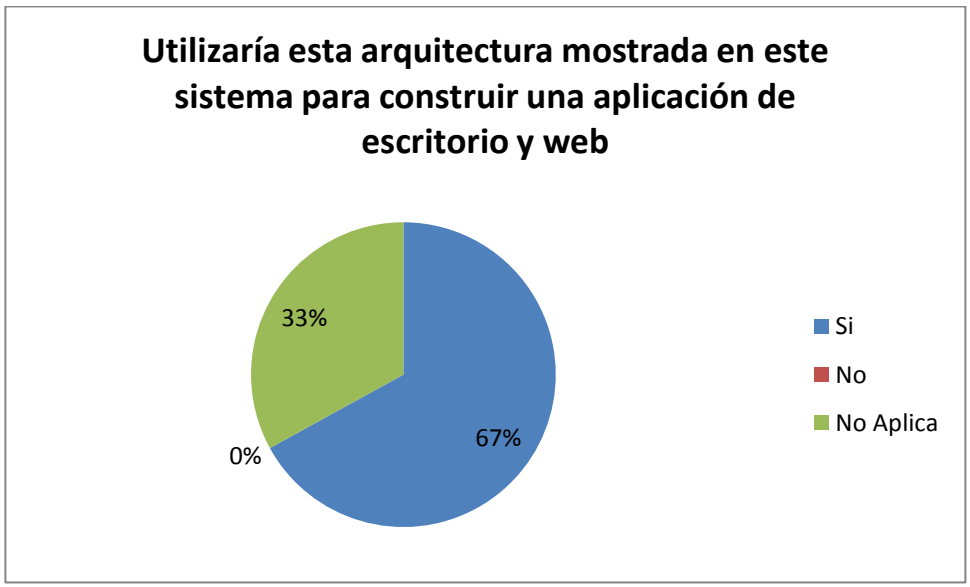


**Pregunta 7.**

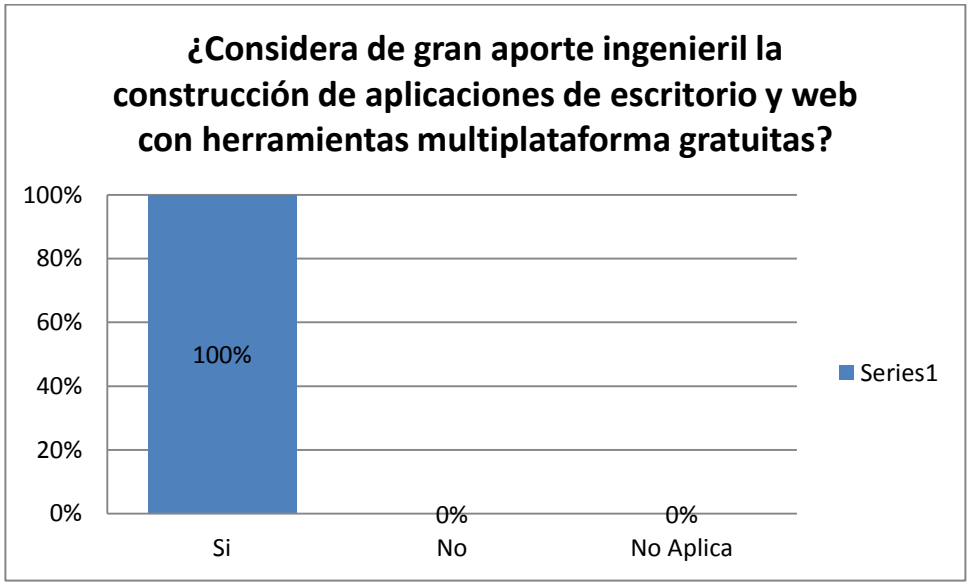



**Arquitectura**

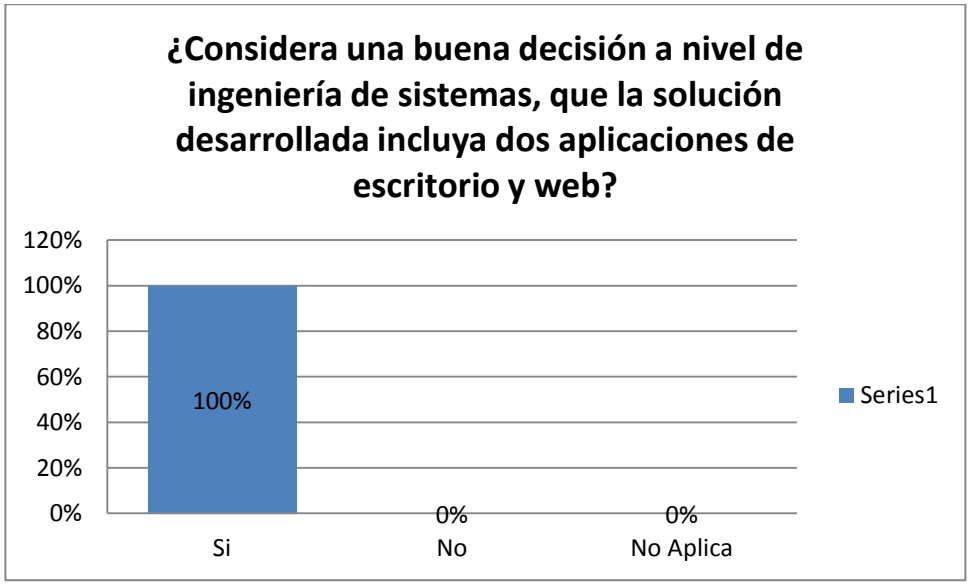
**Pregunta 8.**



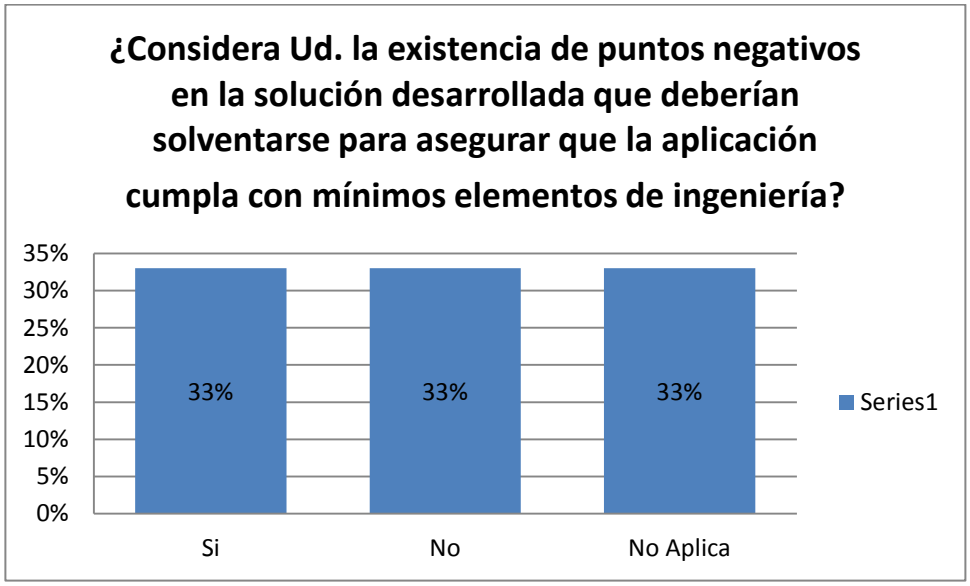
**Pregunta 9.**




**Pregunta 10.**



**Pregunta 11.**


¿Considera Ud. la existencia de puntos negativos en la solución desarrollada que deberían solventarse para asegurar que la aplicación cumpla con mínimos elementos de ingeniería?
35%
30%
25%
20%
15%
10%
5%
0%
33%
33%
33%
Si
No
No Aplica
Series1

## ANEXO 6

## CONFIGURACIÓN DEL FIREWALL PARA EQUIPOS WINDOWS XP[10]

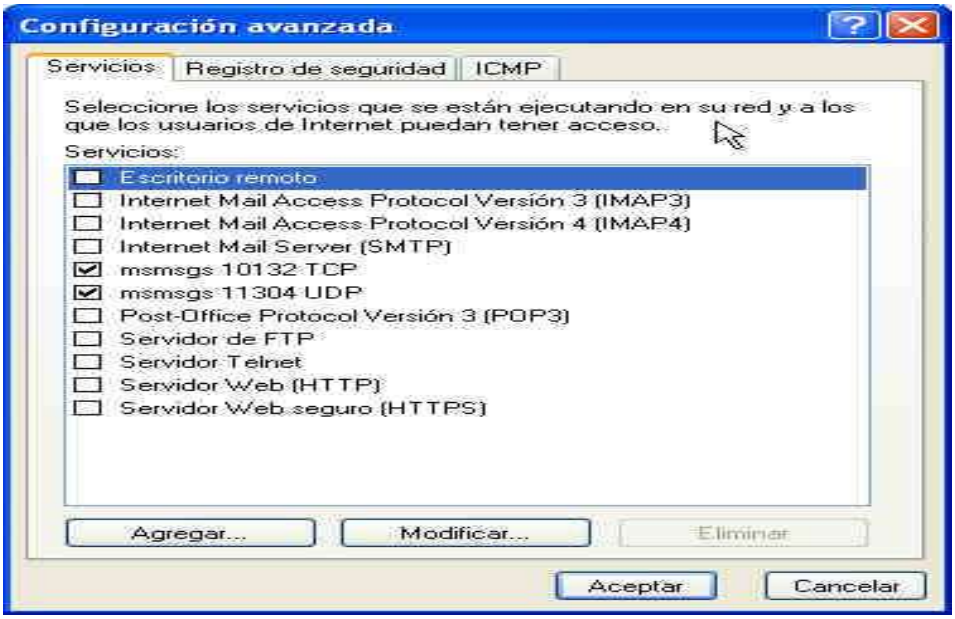
Vamos a INICIO, luego a Configuración, Panel de control y ahí hacemos click con el botón derecho del ratón sobre el icono "Configuración de red" y pinchamos en "Abrir".


En nuestro caso la conexión a internet es la que pone "Conexión de área local". En la imagen anterior siempre veremos las distintas conexiones que tendremos tanto de área local, como módems, etc.

Hacemos click con el botón derecho sobre la conexión deseada y pinchamos en propiedades, luego seleccionamos la pestaña "Avanzadas"


Pinchamos en "Proteger mi equipo y mi red limitando o impidiendo el acceso a el desde internet" con esto activaremos el firewall. Luego veremos que el icono de nuestra conexión aparece con un "candado" en la esquina superior derecha indicando que esta activado el firewall.

Ahora veremos como hacer para que otros programas o servicios pasen a través del firewall. Pichamos en el botón de "Configuración" que se muestra en la imagen anterior.




Aquí podernos activar servicios como Servidor FTP, Servidor HTTP, etc. También podemos agregar otros programas o servicios mediante el botón de agregar. La mayoría

de los programas de comunicaciones siempre especifican los puertos a través de los cuales se conecta (debemos buscar en manuales, sitios web del programa, etc.). Para agregar un programa haremos click en el botón de "Agregar" y veremos la siguiente ventana:


Descripción del servicio: aquí colocaremos un nombre para ayudarnos a identificar el servicio.

Nombre o dirección IP: pondremos el nombre del equipo que nos da el servicio o su dirección IP

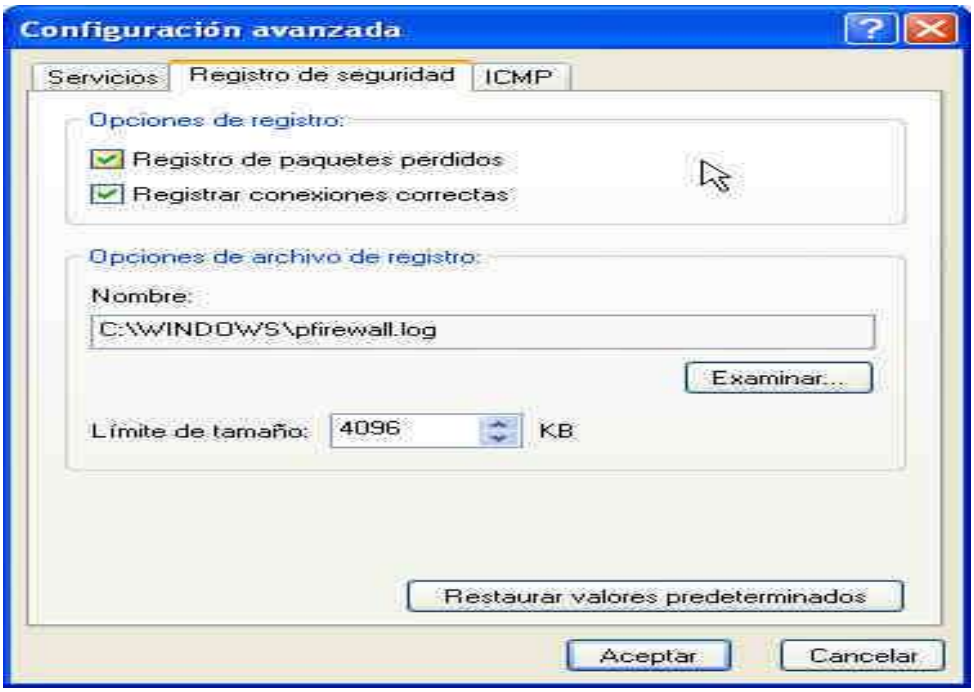
Numero de puerto externo: el número de puerto que los ordenadores usaran para entrar

Numero de puerto interno: el número de puerto que nuestro ordenador usara para este servicio o programa.

También debemos especificar si el servicio o programa usara TCP o UDP (este tipo de información la deberemos de saber mediante un manual, etc.).

Ahora también podemos crear reportes de lo que nuestro firewall esta haciendo. Para esto vamos al botón de "Configuración" de la imagen 2.

Seleccionamos la pestaña "Registro de Seguridad":




Aquí dependiendo de lo que queramos ver en el reporte podemos hacer que nos muestre:

Paquetes perdidos: serán los paquetes de información que el firewall ha detenido (normalmente serán intentos de alguien por acceder sin permiso en nuestro ordenador)

Conexiones correctas: nos dirá todas las conexiones que ha dejado pasar (puede que no tenga mucho sentido, mas que nada por que el reporte será de gran tamaño ya que incluirá todas las conexiones permitidas ).

Opciones de archivo de registro: aquí especificaremos donde se guardara y como se llamara el archivo de reporte (podremos verlo con cualquier procesador de texto, ej.: bloc de notas).

Limite de tamaño: el tamaño máximo que tendrá nuestro archivo de reporte.

Para poder entender la información que nos dará el archivo de reporte usaremos la siguiente tabla que nos explica que es cada columna y la información que nos da:

| | |
|---|---|
| Fecha | fecha en que ocurrió el evento |
| Hora | hora a la que ocurrió el evento |
| Acción | la acción que tomo el cortafuegos: abrir, cerrar, desechar |
| Protocolo | protocolo que se uso: TCP, UDP, ICMP |
| IP de origen | la dirección IP del ordenador que inicio la comunicación |
| IP de destino | la dirección IP de nuestro ordenador |
| Puerto de origen | el puerto del ordenador que ha enviado la información |
| Puerto de destino | el puerto al que el ordenador que ha enviado la información quiso entrar |

**10.** http://www.compuayuda.net/ **guia18.htm**

**ANEXO 7**

## POLÍTICAS PARA LA OBTENCIÓN Y ALMACENAMIENTO DE LOS RESPALDOS DE INFORMACIÓN (BACKUPS) [11]

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

1) Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

2) Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

3) Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

4) Backups de los Datos (Bases de Datos, Indices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

5) Backups del Hardware. Se puede implementar bajo dos modalidades:

**Modalidad Externa**. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

**Modalidad Interna**. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

**11. http://www.ongei.gob.pe/publica/metodologias/Lib5007/ 121.HTM**

**ANEXO 8**

## POLÍTICAS PARA LA ADMINISTRACIÓN DE CUENTAS DE USUARIO[12]

1. El uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada. La cuenta es para uso personal e intransferible.
2. La cuenta de usuario se protegerá mediante una contraseña. La contraseña asociada a la cuenta de usuario, deberá seguir los Criterios para la Construcción de Contraseñas Seguras descrito más abajo.
3. Las cuentas de usuario (usuario y contraseña) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como están.
4. No compartir la cuenta de usuario con otras personas: compañeros de trabajo, amigos, familiares, etc.
5. Si otra persona demanda hacer uso de la cuenta de usuario hacer referencia a estas políticas. De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, deberá solicitarlo por escrito y dirigido al administrador del centro de cómputo.
6. Tipos de Cuentas de Usuario

   Para efectos de las presentes políticas, se definen dos tipos de cuentas de usuario:

   **1. Cuenta de Usuario de Sistema de Información:** todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario del Sistema.

   **2. Cuenta de Administración de Sistema de Información:** corresponde a la cuenta de usuario que permite al administrador del Sistema realizar tareas específicas de usuario a nivel directivo, como por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema.

7. Todas las contraseñas para acceso a los Sistemas Web con carácter administrativo deberán ser cambiadas al menos cada 6 meses.
8. Todas las contraseñas para acceso a los Sistema Web de nivel usuario deberán ser cambiadas al menos cada 12 meses.
9. Todas las contraseñas deberán ser tratadas con carácter confidencial.
10. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
11. Si es necesario el uso de mensajes de correo electrónico para la divulgación de contraseñas, estas deberán transmitirse de forma cifrada.
12. Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de otros.
13. Se evitará el revelar contraseñas en cuestionarios, reportes o informes.
14. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
15. Se evitará el activar o hacer uso de la utilidad de ?Recordar Contraseña? o ?Recordar Password? de las aplicaciones.
16. No se almacenarán las contraseñas en libretas, agendas, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo.
17. No se almacenarán las contraseñas sin encriptación, en sistemas electrónicos personales (asistentes electrónicos personales, memorias USB, teléfonos celulares, agendas electrónicas, etc).
18. Si alguna contraseña es detectada y catalogada como no segura, deberá darse aviso al(los) usuario(s) para efectuar un cambio inmediato en dicha contraseña.

**Criterios en la construcción de contraseñas seguras**

Una contraseña segura deberá cumplir con las siguientes características:

- La longitud debe ser como mínimo de 8 caracteres.
- Contener caracteres tanto en mayúsculas como en minúsculas.
- Puede tener dígitos y caracteres especiales como _, -, /, *, $, ¡, ¿, =, +, etc.
- No debe ser una palabra por sí sola, en ningún lenguaje, dialecto, etc.

- No debe ser un palíndromo (ejemplo: agasaga)
- No debe ser basada en información personal, nombres de familia, etc.
- Procurar construir contraseñas que sean fáciles de recordar o deducir.
- Algunos ejemplos de contraseñas NO seguras por si solas:
    - Nombres de familiares, mascotas, amigos, compañeros de trabajo, personajes, etc
    - Cualquier palabra de cualquier diccionario, términos, sitios, compañías, hardware, software, etc.
    - Cumpleaños, aniversarios, información personal, teléfonos, códigos postales, etc.
    - Patrones como 1234?, aaabbb, qwerty, zyxwvuts, etc.
    - Composiciones simples como: MINOMBRE1, 2minombre, etc.

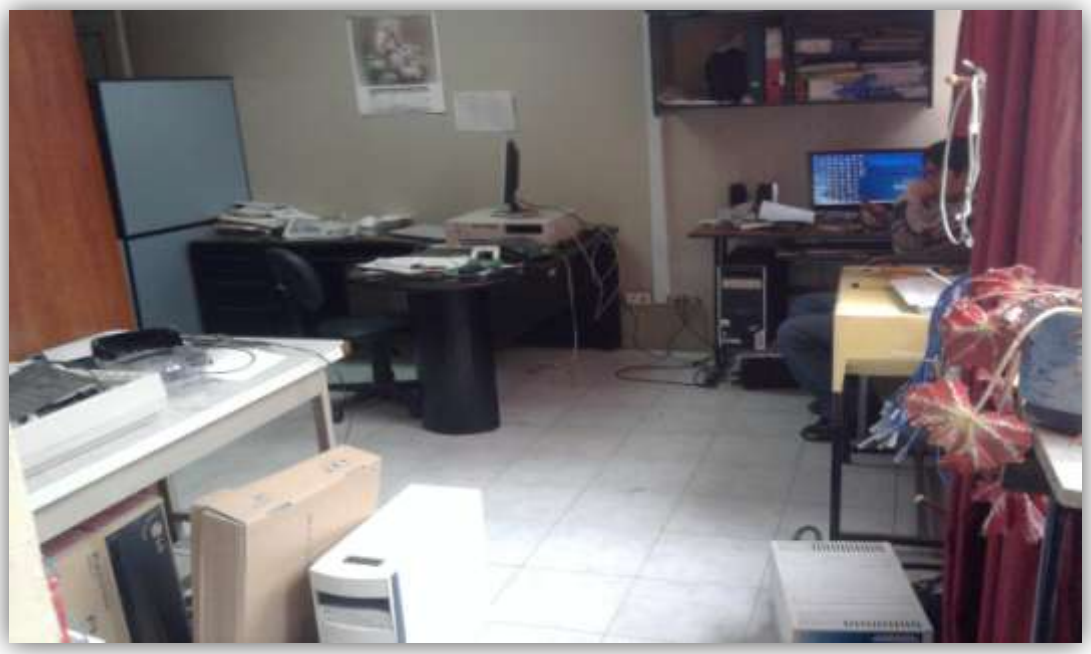
12. http://sistemas.cenac.ipn.mx/ServicioSocila/politicas/**UsoDeCuentas.do**

**ANEXO 9**

# FOTOS E IMÁGENES DEL CENTRO DE CÓMPUTO DEL HOSPITAL GENERAL PROVINCIAL ISIDRO AYORA DE LOJA.

ENTRADA AL CENTRO DE CÓMPUTO

INSTALACIONES DEL CENTRO DE CÓMPUTO



SALA DE SERVIDORES

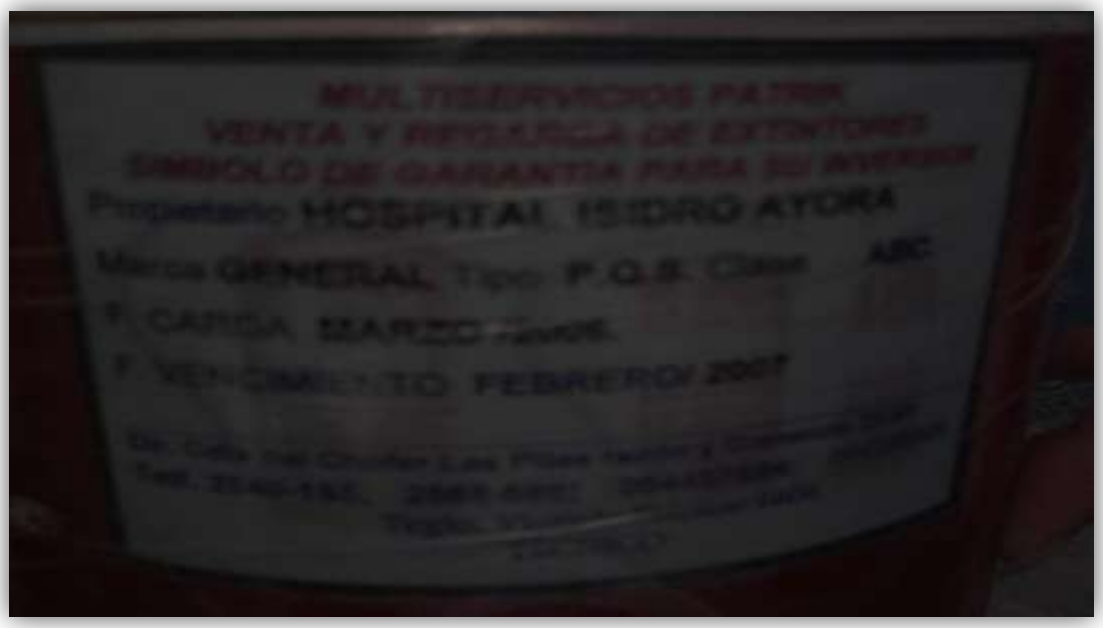
MATERIALES QUE SE ENCUENTRAN DENTRO DE LA SALA DE SERVIDORES


SERVIDOR COLOCADO EN EL ARMARIO DE RACK

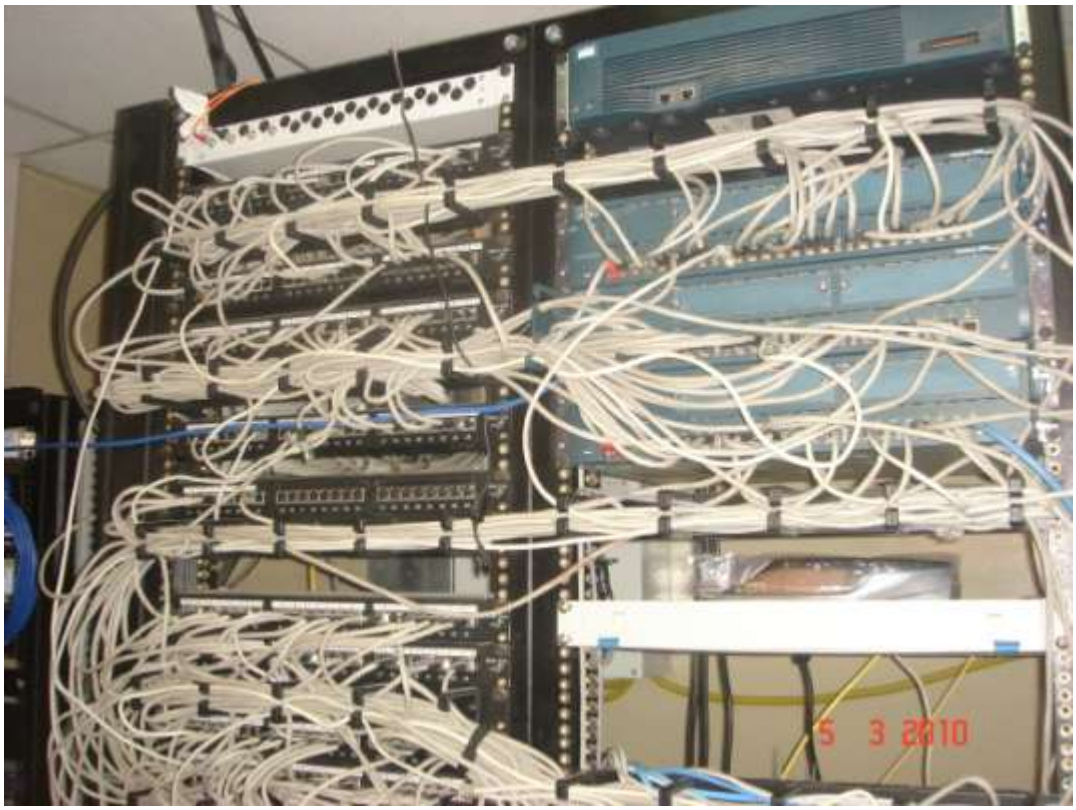
TEMPERATURA EN LA SALA DE SERVIDORES


ESPACIO FÍSICO DONDE SE DA MANTENIMIENTO AL EQUIPO INFORMÁTICO

EXTINGUIDOR PARA EL CENTRO DE CÓMPUTO

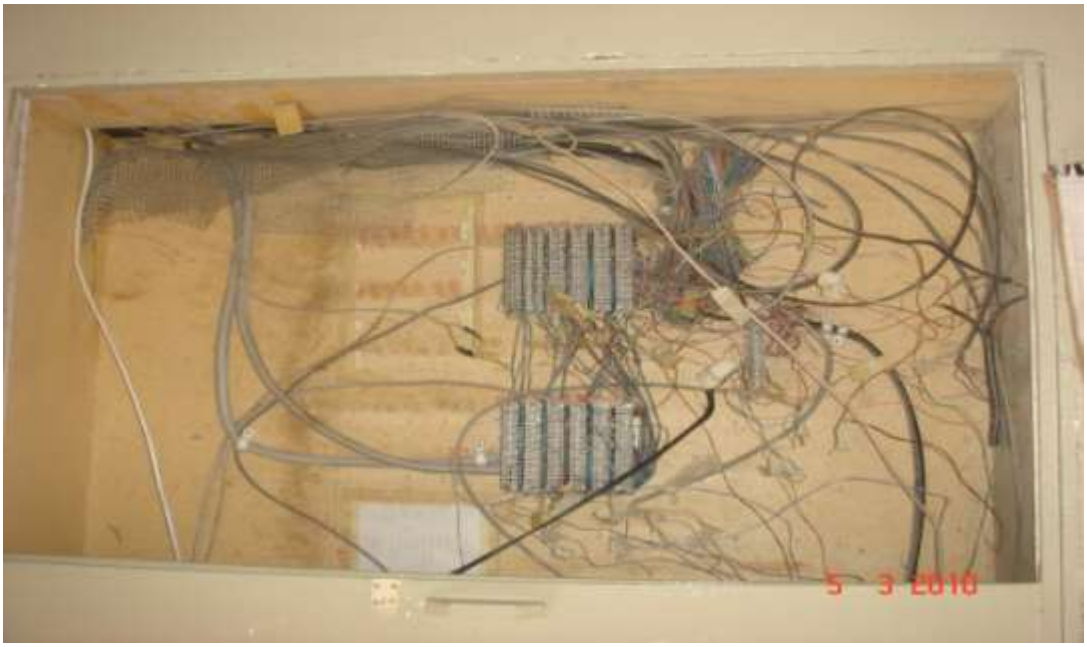



CABLEADO DE RED EN LA SALA DE SERVIDORES



ARMARIO DONDE SE GUARDAN LOS BACKUPS

CABLEADO DE LOS PUNTOS DE VOZ



# GLOSARIO DE TÉRMINOS

## Para la Auditoría

**Auditoría Informática.-** Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado protege los activos tangibles e intangibles de la empresa.

**Backup.-** Copia de respaldo o de seguridad de la información.

**BGP (Border Gateway Protocol).-** Es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

**COBIT.-** (Los Objetivos de Control para la Información y la Tecnología Relacionada), marco de referencia utilizado en el control de las tecnologías de la información.

**Control.-** Se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar seguridad.

**HGPIA.-** Hospital General Provincial Isidro Ayora.

**Log.-** Registro de actividad de un Sistema, que generalmente se guarda en un fichero de texto, al que se le va añadiendo líneas a medida que se realizan acciones sobre el sistema.

**Laptops.-** Computadores portátiles.

**PC's.-** Computadores personales o de escritorio.

**OSPF (Open Shortest Path First).-** Es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible.

**Proceso.-**Conjunto de actividades o eventos que se realizan o suceden bajo ciertas circunstancias con un fin determinado.

**Pendrive (Flash memory).-** Dispositivo de almacenamiento.

**Plan Estratégico.-** Es un plan a largo plazo aprobado por una empresa.

**Programas de Ofimática.-** Son programas utilizados en la oficina y sirven para diferentes funciones como crear, modificar, organizar, escanear, imprimir, etc. archivos y documentos.

**Riesgo.-** Significa "contingencia o proximidad de un daño".

**SANS (SysAdmin Audit, Networking and Security Institute).-** Es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios , agencias gubernamentales, etc.)

**TI.-** Tecnología de la Información.

**Tripwire.-**Es un programa de computador Open Source consiste en una herramienta de seguridad e integridad de los datos.

**Firewall.-** Un cortafuego (Firewall) es un programa que se encarga de monitorear el tráfico de información desde y hacia nuestro ordenador. Es especialmente útil cuando usamos una conexión a internet ya que sin él es como si tuviéramos las puertas abiertas de nuestro ordenador y no todas la personas que puedan entrar en nuestro ordenador poseen buenas intenciones.

**Para el Desarrollo del Software**

**Sistema de Escritorio.-**Es la aplicación creada para ejecutarse en un ordenador de escritorio, sobre un sistema operativo de interfaz visual como Windows o Linux.

**Sitio Web Informativo.-**Con un sitio web informativo dedicado exclusivamente para el evento, usted garantizará una mejor divulgación y dará un mejor servicio a los interesados. Información general del evento, agenda, perfiles de expositores, información hospitalaria, archivos descargables, contacto con la institución, boletines de noticias son algunos ejemplos de la información que puede estar en esta página.

**JDK (Java Development Kit).-** Es un software que provee herramientas de desarrollo para la creación de programas en java.

**GNU (General Public License).-** O simplemente sus siglas del inglés **GNU GPL**, es una licencia creada por la Free Software Foundation en 1989 (la primera versión), y está orientada principalmente a proteger la libre distribución, modificación y uso de software.

**Banner.-**Es un formato publicitario en Internet. Esta forma de publicidad online consiste en incluir una pieza publicitaria dentro de una página web.

**Base de Datos.-**Es un conjunto exhaustivo no redundante de datos estructurados organizados independientemente de su utilización y su implementación en máquina accesibles en tiempo real y compatibles con usuarios concurrentes con necesidad de información diferente y no predicable en tiempo.

**Browser.-**Es un navegador o navegador web (del inglés, web browser) es un programa que permite ver la información que contiene una página web, (ya se encuentre ésta alojada en un servidor dentro de la World Wide Web o en un servidor local), como ejemplo tenemos: Firefox, Internet Explorer.

**Código Fuente.-**Es un programa informático (o software) formado de un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa.

**Contraseña.-**Una contraseña o clave (en inglés password) es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso

**Dominio.-**Un dominio de Internet es una red de identificación asociada a un grupo de dispositivos o equipos conectados a la red Internet.

**Hipertexto.-**En informática, es el nombre que recibe el texto que en la pantalla de un dispositivo electrónico conduce a otro texto relacionado.

**Hipervínculo.-**Un hipervínculo (también llamado enlace, vínculo, o hiperenlace) es un elemento de un documento electrónico que hace referencia a otro recurso, por ejemplo, otro documento o un punto específico del mismo o de otro documento.

**Icono.-**Un icono es un pequeño gráfico en pantalla que identifica y representa a algún objeto (programa, comando, documento o archivo), usualmente con algún simbolismo gráfico para establecer una asociación.

**Interfaz Gráfica de Usuario.-**Conocida también como GUI es un programa informático que actúa de interfaz de usuario, utilizando un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

**JPEG, JPG.-**Uno de los formatos más populares para guardar imágenes digitales, este formato fue creado por Joint Phorographic Experts Group, las siglas de este grupo son las que dan el nombre del formato JPEG o también denominado JPG.

**Modelo Cliente-Servidor.-**Consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta. Aunque esta idea se puede aplicar a

programas que se ejecutan sobre una sola computadora es más ventajosa en un sistema operativo multiusuario distribuido a través de una red de computadoras.

**Página Web.-**Es un documento o información electrónica adaptada para la World Wide Web que generalmente forma parte de un sitio web. Su principal característica son los hipervínculos de una página, siendo esto el fundamento de la WWW.

**PNG**(**Portable Network Graphics).-**Es un formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps no sujeto a patentes.

**Servidor.-**Un servidor es una computadora que formando parte de una red, provee servicios a otras computadoras denominadas clientes.

**Servidor de Aplicaciones.-**Se denomina servidor de aplicaciones a un servidor en una red de computadores que ejecuta ciertas aplicaciones.

**Reporte.-**Es un documento que se utilizará cuando se quiera informar o dar noticia acerca de una determinada situación**.**

**Hosting o alojamiento web** (en inglés web hosting) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

**Servidor Web.-** Es un programa que se ejecuta continuamente en un computador, manteniéndose a la espera de peticiones de ejecución que le hará un cliente o un usuario de Internet.

## UNIVERSIDAD INTERNACIONAL DEL ECUADOR
## SEDE LOJA.

### ENCUESTA APLICADA A LOS PROFESIONALES DE LA UIDE LOJA Y OTROS PROFESIONALES INFORMÁTICOS

Datos Informativos.

Nombres: Dario Jimenez

Cargos: Tecnico de Infraestructura Tecnologica.

Fechas: 2011-11-24.

| **Instrucciones** |
|---|
| Estimado encuestado, por favor sírvase contestar las siguientes preguntas con el afán de evaluar la aplicación "SYSCORTI", en algunas preguntas hay una opción elegible denominada "NO APLICA", en estos casos si el usuario carece de conocimientos acerca de dicho tema puede marcar una opción y no responder el porqué. |

Facilidad de uso

1. Que valoración considera Ud. con respecto a la facilidad del uso de la aplicación "SYSCORTI".

| | |
|---|---|
| Excelente | ( ) |
| Muy bueno | ( ) |
| Bueno | ( ) |
| Regular | (X) |
| Medio | ( ) |

2. ¿Qué valoración Ud. consideraría en la aplicación y distribución de colores para aplicación "SYSCORTI" y para el portal web?

| | |
|---|---|
| Excelente | ( ) |
| Muy bueno | ( ) |
| Bueno | (X) |
| Regular | ( ) |
| Medio | ( ) |

3. ¿Considera Ud. que la aportación de la información en cada una de las pantallas de la aplicación es completa?

| | |
|---|---|
| Si | (X) |
| No | ( ) |

¿Por qué?.....
.....

4. Considera Ud. que los componentes de la aplicación reflejan la mayoría de los procesos utilizados en la productividad de los recursos de TI.

| | |
|---|---|
| Reflejan todos los procesos | ( ) |
| La mayoría de los procesos | (X) |
| Algunos procesos | ( ) |
| Pocos procesos | ( ) |
| Ningún proceso | ( ) |
| No aplica | ( ) |

¿Por qué?.....
.....

5. En una valoración de 1 al 10, establezca la aportación de información y de los procesos de los siguientes componentes.

| | |
|---|---|
| Bitácoras | (6) |
| Planes administración de recursos TI. | (6) |
| Recursos de TI | (6) |
| Personal | (6) |
| Procesos | (6) |
| Infraestructura | (6) |

¿Porqué?.....
.....

**Tecnología**

6. La tecnología java, php y Joomla, es apropiada para realizar y desarrollar soluciones informáticas de escritorio y portales web cliente servidor multiplataforma.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....
.....

7. Considera importante seleccionar una base de datos como mysql server 5.0 para trabajar con aplicaciones de escritorio y web.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

**Arquitectura.**

8. Utilizaría esta arquitectura mostrada en este sistema para construir una aplicación de escritorio y web.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | (✓) |

¿Porqué?.....

.....

9. Considera de gran aporte ingenieril la construcción de aplicaciones de escritorio y web con herramientas multiplataforma gratuitas.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

10. ¿Considera una buena decisión a nivel de ingeniería de sistemas, que la solución desarrollada incluya dos aplicaciones de escritorio y web?

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

11. Considera Ud. la existencia de puntos negativos en la solución desarrollada que deberían solventarse para asegurar que la aplicación cumpla con mínimos elementos de ingeniería.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | (✓) |

¿Porqué o Cuales?.....

.....

.....

.....

.....

## UNIVERSIDAD INTERNACIONAL DEL ECUADOR
## SEDE LOJA.

### ENCUESTA APLICADA A LOS PROFESIONALES DE LA UIDE LOJA Y OTROS PROFESIONALES INFORMÁTICOS

Datos Informativos.

Nombres: Roberto Valdiviezo

Cargos: Supervisor Service desk

Fechas:

| **Instrucciones** |
|---|
| Estimado encuestado, por favor sírvase contestar las siguientes preguntas con el afán de evaluar la aplicación "SYSCORTI", en algunas preguntas hay una opción elegible denominada "NO APLICA", en estos casos si el usuario carece de conocimientos acerca de dicho tema puede marcar una opción y no responder el porqué. |

Facilidad de uso

1. Que valoración considera Ud. con respecto a la facilidad del uso de la aplicación "SYSCORTI".

| | |
|---|---|
| Excelente | ( ) |
| Muy bueno | ( ) |
| Bueno | (/) |
| Regular | ( ) |
| Medio | ( ) |

2. ¿Qué valoración Ud. consideraría en la aplicación y distribución de colores para aplicación "SYSCORTI" y para el portal web?

| | |
|---|---|
| Excelente | ( ) |
| Muy bueno | ( ) |
| Bueno | (✓) |
| Regular | ( ) |
| Medio | ( ) |

3. ¿Considera Ud. que la aportación de la información en cada una de las pantallas de la aplicación es completa?

| | |
|---|---|
| Si | (✓) |
| No | ( ) |

¿Porqué?.....
.....

4. Considera Ud. que los componentes de la aplicación reflejan la mayoría de los procesos utilizados en la productividad de los recursos de TI.

| | |
|---|---|
| Reflejan todos los procesos | ( ) |
| La mayoría de los procesos | (✓) |
| Algunos procesos | ( ) |
| Pocos procesos | ( ) |
| Ningún proceso | ( ) |
| No aplica | ( ) |

¿Porqué?.....
.....

5. En una valoración de 1 al 10, establezca la aportación de información y de los procesos de los siguientes componentes.

| | |
|---|---|
| Bitácoras | (10) |
| Planes administración de recursos TI | (10) |
| Recursos de TI | (10) |
| Personal | (10) |
| Procesos | (10) |
| Infraestructura | (10) |

¿Porqué?.....

.....

**Tecnología**

6. La tecnología java, php y Joomla, es apropiada para realizar y desarrollar soluciones informáticas de escritorio y portales web cliente servidor multiplataforma.

| | |
|---|---|
| Si | ( ) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

7. Considera importante seleccionar una base de datos como mysql server 5.0 para trabajar con aplicaciones de escritorio y web.

| | |
|---|---|
| Si | (/) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

**Arquitectura.**

8. Utilizaría esta arquitectura mostrada en este sistema para construir una aplicación de escritorio y web.

| | |
|---|---|
| Si | ( ✓ ) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

9. Considera de gran aporte ingenieril la construcción de aplicaciones de escritorio y web con herramientas multiplataforma gratuitas.

| | |
|---|---|
| Si | ( ✓ ) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

10. ¿Considera una buena decisión a nivel de ingeniería de sistemas, que la solución desarrollada incluya dos aplicaciones de escritorio y web?

| | |
|---|---|
| Si | ( ✓ ) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué?.....

.....

11. Considera Ud. la existencia de puntos negativos en la solución desarrollada que deberían solventarse para asegurar que la aplicación cumpla con mínimos elementos de ingeniería.

| | |
|---|---|
| Si | ( X ) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué o Cuales?.....

.....

.....

.....

.....

## UNIVERSIDAD INTERNACIONAL DEL ECUADOR
## SEDE LOJA.

### ENCUESTA APLICADA A LOS PROFESIONALES DE LA UIDE LOJA Y OTROS PROFESIONALES INFORMÁTICOS

Datos Informativos.

Nombres: BORIS DIAZ

Cargos: Jefe de Centro de Cómputo - Bco Loja

Fechas: 2011/11/29

| **Instrucciones** |
|---|
| Estimado encuestado, por favor sírvase contestar las siguientes preguntas con el afán de evaluar la aplicación "SYSCORTI", en algunas preguntas hay una opción elegible denominada "NO APLICA", en estos casos si el usuario carece de conocimientos acerca de dicho tema puede marcar una opción y no responder el porqué. |

Facilidad de uso

1. Que valoración considera Ud. con respecto a la facilidad del uso de la aplicación "SYSCORTI".

| | |
|---|---|
| Excelente | (✓) |
| Muy bueno | ( ) |
| Bueno | ( ) |
| Regular | ( ) |
| Medio | ( ) |

2. ¿Qué valoración Ud. consideraría en la aplicación y distribución de colores para aplicación "SYSCORTI" y para el portal web?

| | |
|---|---|
| Excelente | (✓) |
| Muy bueno | ( ) |
| Bueno | ( ) |
| Regular | ( ) |
| Medio | ( ) |

3. ¿Considera Ud. que la aportación de la información en cada una de las pantallas de la aplicación es completa?

| | |
|---|---|
| Si | (✓) |
| No | ( ) |

¿Porqué? En cada link se muestra información referente al HIA muy concisa y certera

4. Considera Ud. que los componentes de la aplicación reflejan la mayoría de los procesos utilizados en la productividad de los recursos de TI.

| | |
|---|---|
| Reflejan todos los procesos | (✓) |
| La mayoría de los procesos | ( ) |
| Algunos procesos | ( ) |
| Pocos procesos | ( ) |
| Ningún proceso | ( ) |
| No aplica | ( ) |

¿Porqué? Se considera el registro de todo el proceso, compra, mantenimiento interno y externo

5. En una valoración de 1 al 10, establezca la aportación de información y de los procesos de los siguientes componentes.

| | |
|---|---|
| Bitácoras | (5) |
| Planes administración de recursos TI. | (6) |
| Recursos de TI | (9) |
| Personal | (7) |
| Procesos | (8) |
| Infraestructura | (10) |

¿Porqué? Considero que es el orden de prioridad de todos los recursos de TI.

**Tecnología**

6. La tecnología java, php y Joomla, es apropiada para realizar y desarrollar soluciones informáticas de escritorio y portales web cliente servidor multiplataforma.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué? Por facilidad de utilización, comparten con otros componentes y sistemas operativos, además de librerías.

7. Considera importante seleccionar una base de datos como mysql server 5.0 para trabajar con aplicaciones de escritorio y web.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué? Por la garantía de brinda esta BD para este tipo de aplicaciones. Además esto.

**Arquitectura.**

8. Utilizaría esta arquitectura mostrada en este sistema para construir una aplicación de escritorio y web.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué? Por esto y por convivencia en dos aplicaciones.

9. Considera de gran aporte ingenieril la construcción de aplicaciones de escritorio y web con herramientas multiplataforma gratuitas.

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué? Por esto y convivencia en dos aplicaciones.

10. ¿Considera una buena decisión a nivel de ingeniería de sistemas, que la solución desarrollada incluya dos aplicaciones de escritorio y web?

| | |
|---|---|
| Si | (✓) |
| No | ( ) |
| No Aplica | ( ) |

¿Porqué? Todo va en función del requerimiento del usuario y de la solución que se plantee. Debe plantearse el negocio.

11. Considera Ud. la existencia de puntos negativos en la solución desarrollada que deberían solventarse para asegurar que la aplicación cumpla con mínimos elementos de ingeniería.

| | |
|---|---|
| Si | ( ) |
| No | (✓) |
| No Aplica | ( ) |

¿Porqué o Cuales? NINGUNA