CAPITULO 4

ANALISIS Y DISEÑO DEL SISTEMA

“Si una imagen vale por mil palabras, un diagrama puede valer aún más; un diagrama puede presentar la lógica de una situación”. Jerry FitzGerald Fundamentos de Análisis de Sistemas

1 ANALISIS Y DISEÑO DEL SISTEMA

1.1 METODOLOGÍA DE DESARROLLO DEL SISTEMA

La metodología utilizada para el diseño e implementación del Sistema automatizado para la ejecución de una auditoria informática aplicando una norma internacional, caso de estudio norma ISO/IEC 17799:2000 en la sede central de la Universidad Francisco Gavidia es el "Ciclo de vida de desarrollo de los Sistemas" (SDCL por sus siglas en ingles).

1.1.1 SDCL (Modelo De Cascada) Como una Metodología

El SDLC es una metodología para el diseño e implementación de un sistema de información en una organización (Figura 4.1). Una metodología es un acercamiento formal para resolver problemas basados en una secuencia estructurada de procedimientos. Usando una metodología se asegura un proceso riguroso y evita fallos en las etapas o pasos que puedan comprometer la meta o el resultado final. También incrementa la probabilidad de éxito.

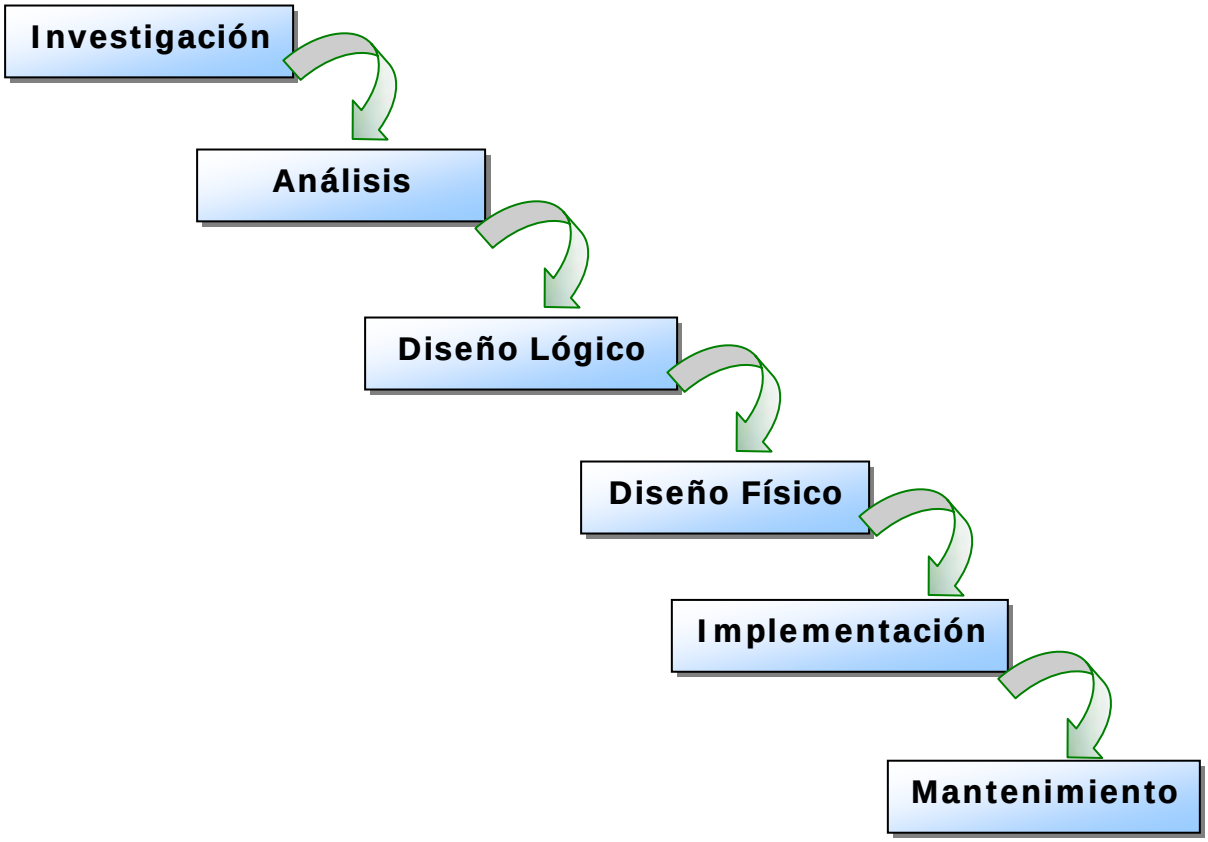

Fig.4.1 Ciclo de vida del desarrollo de Software (SDLC)

1.1.2 Las Fases del SDCL (Modelo de Cascada)

El Tradicional SDLC consiste en seis fases generales. Estas fases provienen del ***Modelo de Cascada*** donde cada fase empieza con los resultados de información recolectada de la fase anterior.

Todo el proceso puede ser iniciado en respuesta a condiciones específicas ó a una combinación de condiciones.

El proceso inicia con una ***investigación*** de los problemas que afronta la organización, luego continúa con un ***Análisis*** de las prácticas organizacionales actuales, considerados en el contexto de la investigación, y entonces procede dentro de las fases del ***diseño lógico y físico***. Durante las fases de diseño, se identifican soluciones potenciales y son asociadas con criterio de evaluación. Mientras tanto en la fase de **implementación**, las soluciones son evaluadas, seleccionadas y puesta en producción.

Los usuarios del sistema son entrenados o capacitados, se desarrolla la documentación del sistema. Finalmente el sistema es terminado y luego se le da **mantenimiento** y se va modificando en su vida operacional.

El presente proyecto contempla únicamente las fases de: Investigación, Análisis, Diseño lógico y Diseño físico.

A continuación se presenta el desarrollo de la fase: diseño lógico del sistema.

1.2 ESTUDIO DE FACTIBILIDAD

Un estudio de factibilidad se desarrolla con el objeto de determinar la posibilidad o probabilidad de que el nuevo sistema sea viable desde el punto de vista económico, técnico y operacional de la organización y que se cuente con la capacidad de implementarlo con los recursos que el sistema requiere.

1.2.1 Factibilidad Técnica

Este tipo de factibilidad busca determinar que los recursos tecnológicos y humanos con que cuenta la organización son óptimos para el funcionamiento del nuevo sistema o si será necesario adquirir nuevo equipo tecnológico o personal calificado.

De acuerdo a la información obtenida durante la investigación de campo realizada en las instalaciones del centro de cómputo de la UFG, se presenta a continuación la infraestructura tecnológica y humana actual relacionada con el proyecto.

Recursos tecnológicos de la Universidad Francisco Gavidia

Características de WebServer

Hadware	**Especificación**
Procesador	Intel Xeon 2.8ghz
Memoria Primaria	2GB DDR ECC REG
Memoria Secundaria	Discos duros de 73GB ultra 320 SCSI 10.000 rpm
Tarjeta de red	100 Mbps
Software	**Especificación**
Servidor Web	Apache
Sistema Operativo	Linux Suse 9.0
Base de datos	Mysql, Postgress
Módulos	Php, Perl, C++

Especificaciones técnicas mínimas requeridas para el sistema.

Tabla de especificaciones técnicas

Hardware	**Especificación**
Cliente	
Procesador	Pentium III, equivalente o superior
Memoria	128 MB o superior
Tarjeta de red	100 Mbps
Servidor	
Procesador	Pentium IV, equivalente o superior
Memoria	512 MB o superior
Tarjeta de Red	100 Mbps o superior
Software	**Especificación**
Cliente	
Sistema Operativo	Windows, Linux, etc
Navegador	Internet Explorer, Mozilla FireFox,etc
Servidor	
Sistema Operativo	Windows, Linux, Solaris

WebServer	Apache, IIS Microsoft
Base de datos	Mysql, Sql Server, Oracle,etc
Otro	Modulo PHP(para plataforma seleccionada)
Recurso Humano(Cargo)	**Experiencia**
Un Administrador de Servidores Web	• Conocimientos en administración, configuración de Servidores Web Apache y IIS. • Conocimientos de publicación de sitios web

Luego de presentar los recursos con que cuenta la Universidad actualmente y los requeridos por el sistema, se comprueba que la UFG cuenta con la infraestructura tecnológica y humana necesaria para llevar a cabo la implementación del presento proyecto.

1.2.2 Factibilidad Económica

Este estudio esta enfocado a determinar que la inversión económica realizada para implementar el proyecto es superada por los ingresos o beneficios que éste genere en un futuro. Para realizar este proceso se realizara un análisis de costos y beneficios.

a) Costos:

El presupuesto del proyecto se presenta en la siguiente tabla 4.1

PRESUPUESTO DEL PROYECTO

Todas los montos son expresados en Dólares

COSTOS DIRECTOS.

Rubro	Cantidad	Honorarios por Mes	No. Meses	Subtotal
Investigadores	2	900.00	4	7,200.00
Coordinador del proyecto	1	1,000.00	6	6,000.00
Analista de Sistemas	1	600.00	5	3,000.00
Programador	1	450.00	3	1,350.00
Asistente/Digitador	1	300.00	4	1,200.00
Asesor	1	675.00	1	690.00

Subtotal 19,440.00

COSTOS INDIRECTOS

Rubro	descripción	Subtotal
Suministros	Papelería, Tinta, Tener, etc.	971.00
Software	Dreamweaver, Zend Php, SqlYog	777.00

Otros	Libros, impuestos		500.00
Subtotal			2,248.00
TOTAL DE COSTOS DIRECTOS E INDIRECTOS			21,688.00
IMPREVISTOS (5%)			1,085.00
			$
COSTO TOTAL			**22,773.00**

Tabla 4.1 de presupuesto del proyecto

b) Beneficios directos:

- La UFG ahorraría el cien por ciento de los costos del proyecto, ya que el software se desarrollara en plataformas de código abierto (open source), evitando gastos de licencias o compra de equipos, y el análisis y diseño del sistema esta libre de gastos por ser un trabajo de graduación elaborado por estudiantes egresados de la facultad de ingeniería y arquitectura de la Institución.

Inversión	**Costo($)**
Inversión licencias (BD, WebServer, Lenguaje de desarrollo):	0.00
Compra de equipo	0.00
Investigación, Análisis y Diseño:	0.00
Total:	**0.00**

- El sistema permitirá una serie de beneficios relacionados de forma directa o indirecta con este nuevo sistema, a continuación se presentan una tabla con los beneficios y las áreas donde van dirigidos:

Dirigido a	**Beneficios**
Universidad	• Reconocimiento como la primera Institución educativa en El Salvador en aplicar el estándar internacional de seguridad informática ISO 17799. • Permitir la comprobación sobre la efectividad en transacciones electrónicas seguras, creando confianza con otras Instituciones nacionales e internacionales.
Dirección, Rectoría y Accionistas	• Elaboración de Informes electrónicos e impresos sobre la ejecución de la Auditoría de Seguridad Informática actual o histórica. • Información precisa para la toma de decisiones en áreas de seguridad informática, como: compras de equipo, presupuesto destinado a apoyar los sistemas de seguridad informática. • Información para ser utilizada como parte de

	documentos estadísticos y gerenciales. • Fácil medición de los niveles de efectividad alrededor de la seguridad informática en la Universidad.
Auditores	• Apoyo a la gestión de evaluación y control de los sistemas de información • Elaboración rápida y sencilla de informes automatizados de los controles al cumplimiento de la norma ISO 17799.
Decanatos, Profesores y Alumnos	• Mayor confianza sobre los procesos electrónicos que se realizan actualmente en la Universidad.
Personal Administrativo y Técnico	• Acceso a consultas de la norma ISO 17799. • Participación y conciencia de los esfuerzos dirigidos a mejorar los niveles de seguridad informática.

Tabla 4.2 Beneficios esperados

Como se puede observar el análisis de costos y beneficios ha comprobado la viabilidad del proyecto a nivel financiero, siendo rentable para la Universidad la implementación del mismo, por la gran variedad de beneficios que este generaría a corto, mediano y largo plazo.

1.2.3 Factibilidad Operacional

Este análisis determina si el sistema es coherente operacionalmente con los procesos de la organización, y si el usuario podrá adaptarse fácilmente al sistema.

Durante la investigación preliminar realizada en la Dirección de tecnología y comunicaciones, se logro determinar los siguientes puntos relacionados con este análisis.

- El Director de la Unidad de tecnología y comunicaciones mostró gran interés en el proyecto, manifestando la necesidad que la Institución tiene por contar con herramientas que ayuden a la gestión de la seguridad informática.

- El sistema esta enfocado a ser parte de los esfuerzos en los procesos de certificaciones que la Universidad viene desarrollando desde el año 2003, el sistema utiliza la norma de seguridad informática ISO 17799.

- El personal técnico no presentaron resistencia al uso del sistema y lo consideraron beneficioso para la Institución.

- El departamento de Auditoría interna también mostró interés en el sistema, esperando que este sirva para mejorar los controles de seguridad de la Unidad de tecnología y comunicaciones de la UFG.

Por lo anterior mencionado, se comprueba que el proyecto es viable desde el punto de vista operacional, sin encontrar resistencia por parte del personal de Administración Académica y Unidad de tecnología y comunicaciones.

Resultado Final del Estudio de Factibilidad

Luego de finalizar los estudios de factibilidad, se ha logrado comprobar que **el proyecto es viable y coherente con los recursos técnicos, financieros y humanos**, por lo que es posible llevar a cabo el desarrollo del sistema.

1.3 ANALISIS Y DETERMINACION DE REQUERIMIENTOS

La conversión de ideas a realidades requiere del uso de métodos y recursos reales. Así el analista debe definir los métodos y recursos reales que se requieran para pasar del sistema de la mesa de trabajo a la operación en vivo. Para lograr esto se deben establecer los objetivos generales de funcionamiento.

La información presentada en este apartado fue recolectada a través de los cuestionarios y entrevistas durante la etapa de investigación preliminar realizada en las Unidades de Administración Académica y Dirección de Tecnología y Comunicaciones.

A continuación se presentan los requerimientos del sistema, en términos de:

- Salidas que debe proporcionar
- Entradas que necesita para producir las salidas
- Operaciones que debe efectuar para producir las salidas
- Recursos que debe usar para producir las salidas

- Controles operacionales

1.3.1 Salidas que debe proporcionar

- Lista de dominios de la norma ISO 17799 para realizar consultas
- Lista de secciones de la norma ISO 17799 para consultar
- Información sobre cada control, incluyendo su objetivo, justificación y guía de uso.
- Reporte en pantallas e impresor de cuestionarios para elaborar exámenes de conformidad con la norma ISO 17799 (papel de trabajo).
- Informe de Auditoría, Será presentado en formato Web , y las secciones a incluir en el informe podrán ser seleccionadas por el usuario, de la lista presentada a continuación:
  - Introducción
  - Objetivo
  - Alcance
  - Título
  - Resolución
  - Mensaje de confidencialidad del informe
  - Preguntas y respuestas a cuestionarios del examen
  - Nivel de conformidad de la norma ISO 17799 por dominio
  - Nivel de conformidad de la norma ISO 17799 global
  - Estatus comparativo de examen actual y anterior (Cuando el examen es de seguimiento).
  - Observaciones
  - Recomendaciones
  - Conclusiones
  - Dirigido a
  - Gráfica de resultados

1.3.2 Entradas que necesita para producir las salidas

- Ingreso de solicitud para consulta de la norma ISO 17799: El sistema permitirá seleccionar el dominio, sección y control a consultar, posteriormente podrá navegar por cada control, y revisar la documentación sobre la ISO 17799.

- Petición de papel de trabajo: Se seleccionan los dominios a incluir para la elaboración del papel de trabajo (Checklist).
- Ingreso de Exámenes: Se ingresa datos del examen ha desarrollar (Objetivos y Alcances) y finalmente las respuestas obtenidas en el examen desarrollado con la ayuda del papel de trabajo (Cheklist).
- Seguimiento a exámenes creados, completando los módulos de la norma
- Petición de Informe de Auditoría: Se ingresa el número de referencia del examen a evaluar del nivel de conformidad.
- Parametrización del informe de Auditoría: Se seleccionan las secciones que incluirá el reporte (listadas en los requerimientos de salida)

1.3.3 Operaciones que debe efectuar para producir las salidas

- Buscar datos de documentación de la norma según el dominio y sección solicitados
- Formatear los resultados de documentación sobre la norma para su presentación en pantalla o impresor.
- Buscar y asociar cada una de las preguntas de los controles de la norma, para elaborar cuestionarios o papel de trabajo, agrupadas y ordenadas por dominio y sección.
- Calcular el puntaje obtenido para cada respuesta del cuestionario de cumplimiento.
- Almacenar resultado del examen
- Calcular el puntaje total por dominio. El sistema debe calcular el nivel de conformidad de dos formas diferentes, el primero conocido como **calculo por pesos**, donde cada control tiene asociado un valor de importancia para la organización y es a través de este que se calcula el nivel de conformidad, el segundo llamada **calculo general**; donde cada control tienen un mismo nivel de importancia, y busca determinar la aplicación absoluta de la norma ISO 17799.
- Elaborar exámenes a partir de otro ya creado. Elaborar un nuevo examen como continuidad a otro ya evaluado, replicando cada uno de los resultados obtenidos, y que posteriormente podrán ser actualizados en el nuevo examen.
- Desarrollar un análisis del nivel de cumplimiento a la norma a nivel de dominio y de forma global.

- Preparar información de la norma, respuestas de examen, resultados de la evaluación y lista de parámetros para construir el informe final de Auditoría.
- Almacenar información de evidencia de los estudios de Auditoría, subiendo al sistema cualquier tipo de archivo para dar garantía a los resultados obtenidos.

1.3.4 Recursos que debe usar para producir las salidas

- Servidor para publicación y procesamiento de paginas Web
- Computador personal con un navegador de paginas Web
- Conexión de red para Internet o Intranet
- Impresor
- Personal capacitado en el sistema

1.3.5 Controles Operacionales

- Controlar que el usuario esté autorizado para ingresar al sistema
- Controlar la identificación del usuario durante esté conectado, a través de una sesión
- Verificar el estado actual del usuario
- Controlar las operaciones que realiza cada usuario en el sistema.
- Manejar y controlar cuatro tipos de usuario:
    - Usuario de Consulta: Podrá realizar únicamente consultas a la norma y documentos de referencia sobre seguridad y auditoría.
    - Usuario Ejecutivo: Podrá realizar consultas a la norma y documentos de seguridad, y además preparar informes de Auditoría de exámenes almacenados.
    - Usuario Evaluador: Podrá realizar lo mismo que el usuario ejecutivo, además podrá elaborar papeles de trabajo para realizar exámenes de cumplimiento y almacenar resultados de exámenes.
    - Usuario Administrador: Es el usuario con todos los privilegios al sistema, es el único con capacidad de administrar los catálogos del sistema y cada una de las funciones principales.

- Validar la información enviada al sistema a través de los formularios; no debe permitir el envío de solicitudes incompletas o inconsistentes.
- Revisar que todos los parámetros solicitados son recibidos en cada transacción con el servidor.
- Verificar que se lleven a cabo correctamente los procesos de almacenamiento con la base de datos del sistema.
- Notificar del éxito de las transacciones
- Comparar los resultados obtenidos contra la base de conocimientos al cumplimento de la norma y revisar recomendaciones y conclusiones.
- Controlar el estatus de las evaluaciones en el sistema
- Informar al usuario de situaciones anómalas, como fallas de conexión con la base de datos, error en transacciones, procesos incompletos.

1.4 ESTRUCTURA

En esta sección se hace uso del Análisis Estructurado, para describir la estructura del Sistema de Control de Auditoría para conformidad a la ISO 17799. Se presentan los diagramas de flujos de datos, diagrama entidad-relación, diagrama de jerarquía del sistema, diagrama conceptual del sitio web y por último se describen los diccionarios de datos.

1.4.1 Diagrama de Flujo de Datos

El **Diagrama de Flujo de Datos** (**DFD**) es una herramienta para modelar que permite describir de un sistema, la transformación de entradas en salidas; el DFD también es conocido con el nombre de Modelo de Procesos de Negocios (**BPM**, **B**usiness **P**rocess **M**odel).

El objetivo del DFD es:

1. Describir el contexto del sistema, determinando lo que ocurrirá en cada una de las áreas de la empresa, denominadas Entidades externas, que participen de este sistema;
2. Detallar los procesos a ser realizados;
3. Enumerar los archivos de datos necesarios, en cada proceso;
4. Definir los flujos de datos, que participen en el procedimiento.

Una de las principales características de este modelo es su simplicidad, y se debe al hecho que son solamente cuatro los símbolos utilizados que representan a los elementos (entidades externas, archivos, procesos y flujos de información); con los cuales se puede producir un esquema, que alcance el nivel de detalle requerido por el proyectista (Figura 4.2).

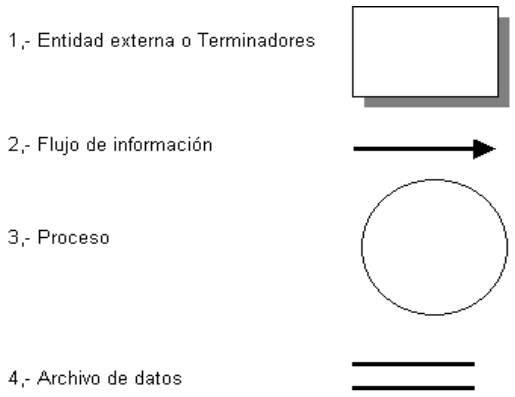

Figura 3.2. Simbología del DFD

Se presenta a continuación el diagrama de flujo de datos de nivel de contexto y de niveles 1 y 2.

VER DIAGRAMAS EN TESIS IMPRESA

1.4.2 Diagrama Entidad Relación (ER)

La pareja objeto-relación, es la piedra angular del modelo de datos. Esta pareja se puede representar gráficamente mediante el Diagrama Entidad Relación (DER). En este
Se identifican un conjunto de componentes primarios: objetos de datos, atributos, relaciones y varios indicadores tipo.

El diagrama ER posee dos importantes componentes, que son las Entidades y las Relaciones:

1. Entidades o Tipos de objetos: Son representadas por un cuadrado en el RDM. Una Entidad representa a una colección o conjunto de objetos (cosas) del mundo real, cuyos miembros diseñan un papel en el sistema que se está desarrollando. Las Entidades pueden ser identificadas de forma única y, ser descritas a través de uno ó más hechos (Atributos). Como regla general, tomamos que, en cada archivo de datos definido por el DFD, se almacenan los datos que describen a las Entidades del sistema de información, o sea, a cada archivo de datos del DFD le corresponde una Entidad al ER.

2. Relaciones: Una relación representa un conjunto de conexiones o asociaciones entre las Entidades, conectadas por vectores al relacionamiento. Normalmente, cada entidad que compone la base de datos de un sistema podrá estar relacionada con otras; por ejemplo, un cliente podrá estar relacionado con varias ventas, una venta con varios productos, un vendedor con varias ventas, y así sucesivamente en cada uno de los procedimientos.

A continuación se presenta el diagrama ER para el sistema de control de Auditoría para conformidad de la ISO 17799 (ver figura 4.3).

DIAGRAMA ENTIDAD RELACION

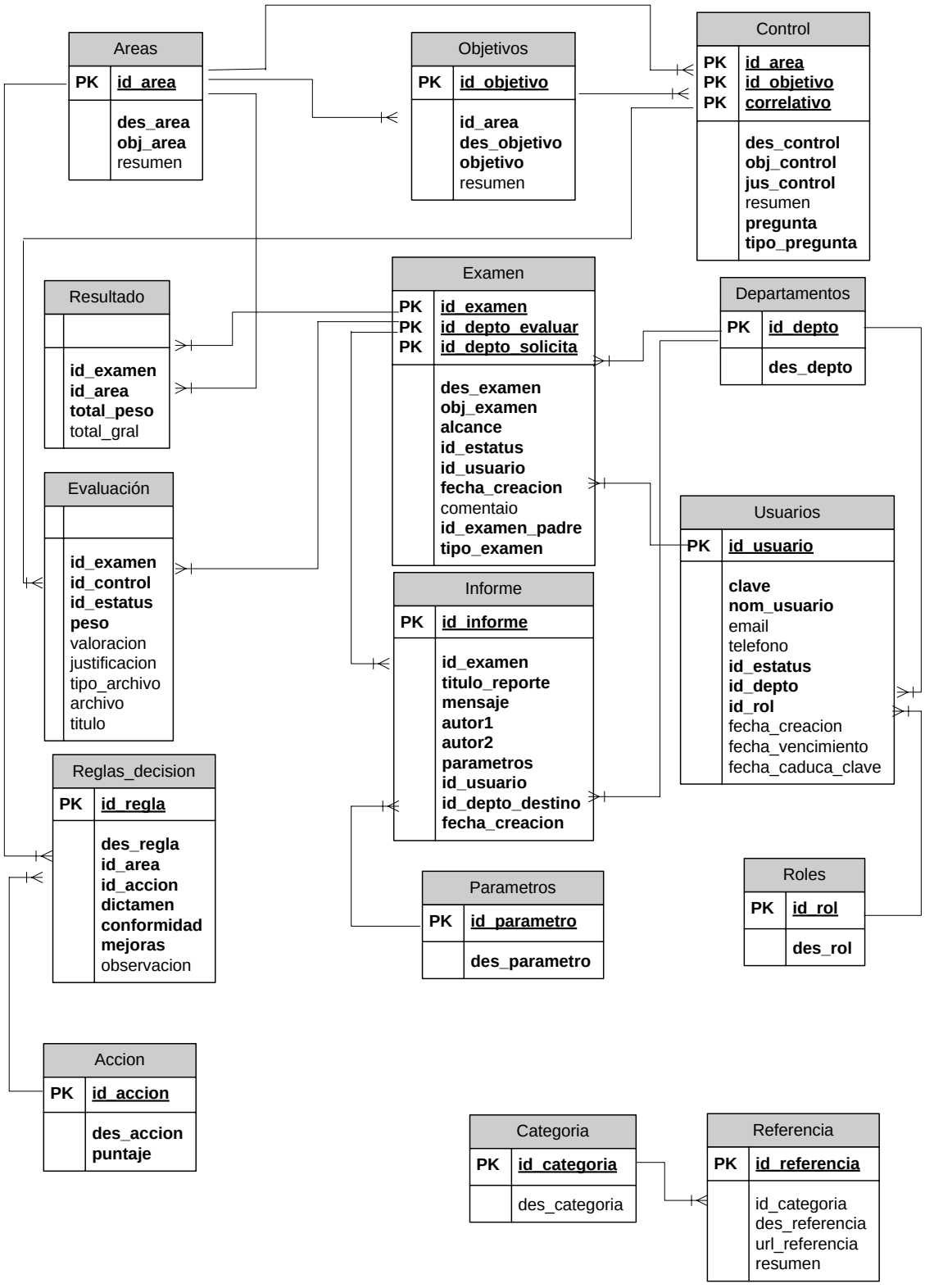

Fig.4.3 Diagrama Entidad Relación