Versión

1

"SISTEMA AUTOMATIZADO PARA LA EJECUCION DE UNA AUDITORIA INFORMATICA APLICANDO UNA NORMA INTERNACIONAL, CASO DE ESTUDIO NORMA ISO/IEC 17799:2000 EN LA SEDE CENTRAL DE LA UNIVERSIDAD FRANCISCO GAVIDIA"

Manual Técnico

SOFTWARE DE APLICACION ISO 17799

Manual Técnico

Tabla de contenido

CAPITULO 1

Introducción.....1

Objetivo.....2

CAPITULO 2

Diccionario de Datos.....3

Diagrama ER.....12

Tabla de códigos del sistema.....13

Diccionario de procesos.....15

Flujos de Procesos.....19

Capítulo

1

Introducción

Software de aplicación para apoyo a la gestión de seguridad informática, tomando como líneas de acción las recomendaciones que formas parte de la norma ISO/IEC 17799:2000. Este sistema ayuda a identificar áreas débiles en la organización y aporta recomendaciones de acuerdo al criterio de expertos en el área de seguridad informática.

El manual técnico esta orientada para el personal de desarrollo y análisis de la Institución, especificando estructura de la base de datos, flujos de procesos y otros elementos del área propiamente técnica.

Objetivo

Apoyar la continuidad del sistema, ofreciendo una guía de referencia para programadores y analistas, los cuales pueden enriquecer de nuevas funcionalidades al software; sin ser necesario la participación de los creadores de la herramienta.

Objetivos específicos

- Mostrar diccionario de datos del sistema y diagrama de entidad relación
- Presentar diagramas jerárquicos del sistema.
- Mostrar flujos de procesos.
- Presentar Tabla de códigos del sistema
- Mostrar Script de creación de la BD del software

.

Capítulo

2

Diccionario de Datos

Permite detallar la descripción lógica de la información almacenada en el sistema, su estructura y relación. A continuación se presentar el diccionario de datos del sistema

Descripción de Entidades

Nombre Entidad	**AREA**
Descripción	Entidad que almacena el nivel más alto de la estructura de la norma ISO 17799 que define las diferentes áreas.
Entrada:	Descripción, objetivo y datos informativos sobre el área.
Salida:	Ninguna
Observación	Es parte de la llave principal del sistema, se representa con números enteros del 1 al 10

Nombre Entidad	**SECCION**
Descripción	Entidad que contiene el segundo nivel de la norma, que define los objetivos asociados a cada área.
Entrada:	descripción, objetivo y datos informativos sobre el objetivo
Salida:	Ninguno
Observación	Es parte de la llave principal del sistema, se representa con números enteros(1.1)

Nombre Entidad	**CONTROL**
Descripción	Entidad que administra el tercer y último nivel de la norma
Entrada:	Información de cada control de la norma, asociando área, objetivo y correlativo del control, además su objetivo general, justificación y pregunta relacionada al control
Salida:	Pregunta para papel de trabajo(Checklist)
Observación	Es parte de la llave principal del sistema, se representa con números enteros (1.1.1)

Nombre Entidad	EXAMEN
Descripción	Entidad que almacena información general de los exámenes de cumplimiento.
Entrada:	Información de identificación de exámenes, fecha, usuario, y otros datos particulares del examen
Salida:	Información general del examen realizado para presentar el informe de Auditoría.
Observación	Esta entidad trabaja junto con las entidades de evaluación y resultado, administrando los datos de exámenes de cumplimiento.

Nombre Entidad	EVALUACION
Descripción	Entidad que administra los resultados obtenidos durante la evaluación de campo a través de los cuestionarios de cumplimiento.
Entrada:	Información a detalle de los resultados obtenidos durante el desarrollo del examen de cumplimiento, respuestas de cada control de la norma ISO17799, justificación de los resultados y documentos de evidencia, que respalden la investigación.
Salida:	Información de resultados obtenidos por cada control durante el examen de cumplimiento.
Observación	Esta entidad alimenta a la entidad resultado para el proceso de consolidación de resultados por áreas y globales.

Nombre Entidad	RESULTADO
Descripción	Entidad que almacena la información consolidada de la evaluación realizada a un examen de cumplimiento.
Entrada:	Información de puntajes por área, valores consolidados por pesos.
Salida:	Valores de puntajes por áreas.
Observación	A través de esta entidad se puede calcular los resultados globales al nivel de cumplimiento de la norma.

Nombre Entidad	INFORME
Descripción	Entidad que administra la información para la elaboración de los informes de Auditoría.
Entrada:	Resultados del examen, reglas de cumplimiento, puntajes consolidados, base de conocimiento de la norma ISO 17799 y parámetros del informe.
Salida:	Informe de Auditoría.
Observación	Esta entidad permitirá que se generen informes sobre exámenes de cumplimiento a la norma ISO 17799.

Nombre Entidad	REGLAS DE CUMPLIMIENTO
Descripción	Entidad que almacena las reglas o tratamiento a realizar por cada uno de los posibles resultados obtenidos durante el proceso de evaluación del examen de cumplimiento.
Entrada:	Información del dominio, posible resultado, recomendación, conclusión y cualquier otra observación
Salida:	Resultados analizados área y puntaje. Análisis del nivel de cumplimiento obtenido, sus observaciones, recomendaciones y conclusiones.
Observación	Se debe crear una regla por cada área y acción.

Nombre Entidad	USUARIO
Descripción	Almacena información de los usuarios autorizados para ingresar al sistema
Entrada:	Datos personales del usuario, nivel de permiso, departamento al que pertenece y el estatus actual.
Salida:	Código, nombre del usuario conectado al sistema, nombre, permisos.
Observación	

Nombre Entidad	DEPARTAMENTO
Descripción	Contiene información del departamento o unidad donde labora el usuario
Entrada:	Datos del departamento
Salida:	Código del departamento
Observación	

Nombre Entidad	ACCION
Descripción	Entidad que almacena los posibles resultados de conformidad
Entrada:	Datos de resultados del examen, Resultado del nivel de cumplimiento a la norma ISO17799.
Salida:	Valor del puntaje
Observación	Esta entidad asocia la acción o resultado final del calculo de conformidad

Nombre Entidad	PARAMETRO INFORME
Descripción	Almacena información general del sistema
Entrada:	Datos del parámetro
Salida:	Código del parámetro
Observación	Esta entidad es usada para el proceso de creación del informe, donde el usuario puede determinar que secciones del reporte desea incorporar como: título, usuario, introducción, alcance, objetivo.

Nombre Entidad	ROL
Descripción	Entidad que controla los roles de cada usuario
Entrada:	Datos del rol o permiso
Salida:	Código del rol o permiso
Observación	

Nombre Entidad	CATEGORIA
Descripción	Entidad que administra las diferentes categorías de material de referencia sobre seguridad informática.
Entrada:	Datos de cada categoría
Salida:	Código de categoría.
Observación	

Nombre Entidad	REFERENCIA
Descripción	Entidad que administra la información de sitios con material de interés sobre seguridad informática.
Entrada:	Datos de cada categoría y referencia
Salida:	Sitio de referencia
Observación	Las referencias pueden ser hacia sitios en Internet o dentro de la Institución

Almacenes de Datos

PK = Llave primaria (Primary Key), FK:= Llave foranea (Foreign Key)

Tabla	**Area**				
Descripción	Tabla con información con de cada área de la norma				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_area	Numérico	2	Si	PK	Campo identificador único para áreas
des_area	Texto	50	Si		Nombre o descripción del área
obj_area	Texto	150	Si		Objetivo que persigue el área
resumen	Text	500	No		Información adicional del área, para ser parte de la guía del usuario.
Tabla	**Seccion**				
Descripción	Tabla con información de los objetivos asociados a cada área de la norma ISO 17799				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_seccion	Numérico	2	Si	PK	Campo identificador único de sección
id_area	Numérico	2	Si	FK	Campo identificador para área
des_seccion	Texto	50	Si		Nombre o descripción de la sección
obj_seccion	Texto	150	Si		Objetivo general que persigue esta sección
resumen	Texto	500	No		Información adicional del objetivo, para ser parte de guía del usuario.

Tabla	**Control**				
Descripción	Tabla con información de los controles asociados a cada objetivo y área de la norma ISO 17799				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_area	Numérico	2	Si	FK	Campo identificador para Secciones
id_seccion	Numérico	2	Si	FK	Campo identificador del dominio
id_control	Numérico	2	Si	PK	Correlativo del control que pertenece a un objetivo y área específica de la norma
des_control	Texto	100	Si		Descripción del control
obj_control	Texto	150	Si		Objetivo que persigue el control
guia	Texto	500	No		Información adicional del control, para ser parte de guía del usuario.
pregunta	Texto	200	Si		Pregunta que se incluirá en el papel de trabajo del examen.
peso	Numérico	3	Si		Determina la importancia de este control en la Institución.
Tabla	**Examen**				
Descripción	Tabla que almacena la información general de cada examen de cumplimiento a la norma				
Tipo	Detalle				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
Id_examen	Numérico	4	Si	PK	Campo identificador para exámenes
des_examen	Texto	2	Si		Descripción del examen
obj_examen	Texto	150	Si		Objetivo que persigue el examen
alcance	Texto	100	Si		Alcance del examen
Id_estatus	Texto	2	Si		Identificador del estatus actual del examen (1=Completo, 0=incompleto).
Id_usuario	Numérico	2	Si	FK	Identificador del usuario que crea el examen.
fecha_creacion	Fecha	8	Si		Fecha de creación del examen
comentario	Texto	100	No		Comentario adicional sobre el examen realizado
Id_depto_evaluar	Numérico	2	Si	FK	Identificador del departamento a evaluar en el examen
Id_depto_solicita	Numérico	2	Si	FK	Identificador del departamento que solicita la evaluación
id_examen_padre	Numérico	4	No		id de examen del cual hereda el actual para llevar acabo la actividad de seguimiento.
tipo_examen	Numérico	1	No		Campo que determina si el examen es privado o publico(0 = público, 1= privado)

Tabla	**Evaluación**				
Descripción	Tabla que almacena la información que detallada de cada examen, y el resultado a cada control, asignando un puntaje a ese resultado				
Tipo	Detalle				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_examen	Numérico	2	Si	FK	Campo identificador del examen
id_control	Numérico	2	Si	FK	Campo identificador para el control
id_estatus	Numérico	2	Si	FK	Código del puntaje asociado a la calificación(0,=Sin realizar,1=Si,2=No,3=Parcialmente)
justificacion	Texto	250	No		Justificación de la respuesta
tipo_archivo	Texto	40	No		Identifica el tipo de archivo a guardar como evidencia
Archivo	Blob	16 MB	No		Contenido del archivo a manejar como evidencia
Titulo	Texto	150	No		Nombre del archivo a presentar en pantalla para ser consultado por el usuario.

Tabla	**Reglas_Cumplimiento**				
Descripción	Tabla que almacena la información del tratamiento que se dará a los resultados obtenidos al nivel de cumplimiento de la norma ISO17799				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_regla	Numérico	3	Si	PK	Campo identificador para cada regla
des_regla	Texto	150	Si		Descripción de la regla
id_area	Numérico	2	Si	FK	Campo identificador para área
id_accion	Numérico	2	Si	FK	Campo identificador de posibles acciones (1=Excelente, 2=Bueno, 3=Básico, 4=Deficiente, 5=Falla Gravemente)
dictamen	Texto	150	Si		Descripción de la resolución a la acción y área especifica.
resultado	Texto	250	Si		Información sobre el resultado global obtenido para esa acción y área en particular.
conclusión	Texto	250	Si		Conclusión del resultado
recomendación	Texto	250	Si		Recomendación del resultado
observación	Texto	250	No		Observaciones

Tabla	**Acción**				
Descripción	Tabla que almacena acción o resultado final del calculo de conformidad de la norma ISO 17799 a cada informe de auditoría.				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_accion	Numérico	2	Si	PK	Identificador de acción (1=Excelente, 2=Muy bueno, 3=Básico, 4=Deficiente, 5=Falla Gravemente)
des_accion	Texto	40	Si		Descripción del puntaje. Valor asociado (100=Excelente, 80=Muy bueno, 60=Básico, 40=Deficiente, 20=Falla Gravemente)

Tabla	**Informe**				
Descripción	Tabla con información de los informes de Auditoría generados				
Tipo	Detalle				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
Id_informe	Numérico	2	Si	PK	Campo identificador único para cada informe
Id_examen	Numérico	2	Si	FK	Campo identificador del examen asociado al informe
titulo	Texto	50	No		Titulo para ser impreso al inicio del reporte, identificando el reporte
mensaje	Texto	50	No		Mensaje personalizado para imprimir en cada página, por ejemplo: Derechos reservados, fecha, banner en especial, etc.
autor1	Texto	40	No		Nombre de persona adicional que participó del estudio, es opcional
autor2	Texto	40	No		Nombre de persona adicional que participó del estudio, es opcional
depto_destino	Texto	2	Si	FK	Departamento al que va dirigido el informe
parámetros	Texto	40	No		Parámetros o secciones que se pueden agregar al reporte como: título del reporte, objetivos, alcance del informe, introducción a la ISO 1779 y al informe, respuestas a las preguntas del examen realizado.
id_usuario	Texto	10	Si	FK	Identificador del usuario que genera el reporte
fecha_creacion	Date		Si		Fecha del día que se creo el informe.

Tabla	**Parámetro_Informe**				
Descripción	Tabla que almacena información de parámetros o secciones que pueden ser agregados en los informes				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
Id_paramentro	Numérico	2	Si	PK	Campo identificador para cada parámetro o sección del informe
des_parametro	Texto	40	Si		Descripción o nombre del parámetro
Tabla	**Usuario**				
Descripción	Tabla con información de usuarios autorizados para trabajar con el sistema				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_usuario	Texto	2	Si	PK	Código identificador para usuarios
login	Texto	20	Si		Nombre con que se valida
clave	Texto	8	Si		Palabra clave para ingresar al sistema
nom_usuario	Texto	50	Si		Nombre del usuario
email	Texto	35	No		Correo electrónico del usuario
teléfono	Texto	8	No		Teléfono de contacto del usuario
id_depto	Numérico	2	Si	FK	Identificador del departamento al que pertenece el usuario
id_rol	Numérico	2	Si	FK	Identificador del nivel de permisos asociado al usuario.
fecha_creacion	Date		Si		Fecha en la que se crea el usuario
fecha_vencimiento	Date				Fecha cuando el usuario será de baja
Tabla	**Departamento**				
Descripción	Tabla que almacena información de cada departamento con usuarios relacionados directa o indirectamente con el sistema				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
id_depto	Numérico	2	Si	PK	Campo identificador para cada departamento o unidad
des_depto	Texto	40	Si		Descripción o nombre del departamento

Tabla	**Rol**				
Descripción	Tabla que almacena información de los diferentes niveles de permiso para ser asociados a cada usuario				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
Id_rol	Numérico	2	Si	PK	Identificador del nivel de permisos asociado al usuario(1=Auditor, 2=Ejecutivo,3=Consulta.)
des_rol	Texto	20	Si		Descripción del nivel
Tabla	**Categoría**				
Descripción	Tabla que almacena la información de las categorías asociadas a las referencias sobre seguridad informática y temas relacionados.				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
Id_categoria	Numérico	2	Si	PK	Identificador de la categoría
des_categoria	Texto	150	Si		Descripción de la categoría
Tabla	**Referencia**				
Descripción	Tabla que almacena la información de las referencias sobre seguridad informática y temas relacionados.				
Tipo	Maestra				
Campo	**Tipo**	**Longitud**	**Obligatorio**	**Llave**	**Descripción**
Id_categoria	Numérico	2	Si	FK	Identificador de la categoría
Id_rerefencia	Numérico	4	Si	PK	Identificador único de la referencia
des_referencia	Texto	150	Si		Titulo de la referencia
url_referencia	Texto	150	Si		Dirección del documento(Internet o Intranet)
Resumen	Texto	250	Si		Breve descripción del material que se encuentra en la referencia.

Diagrama ER

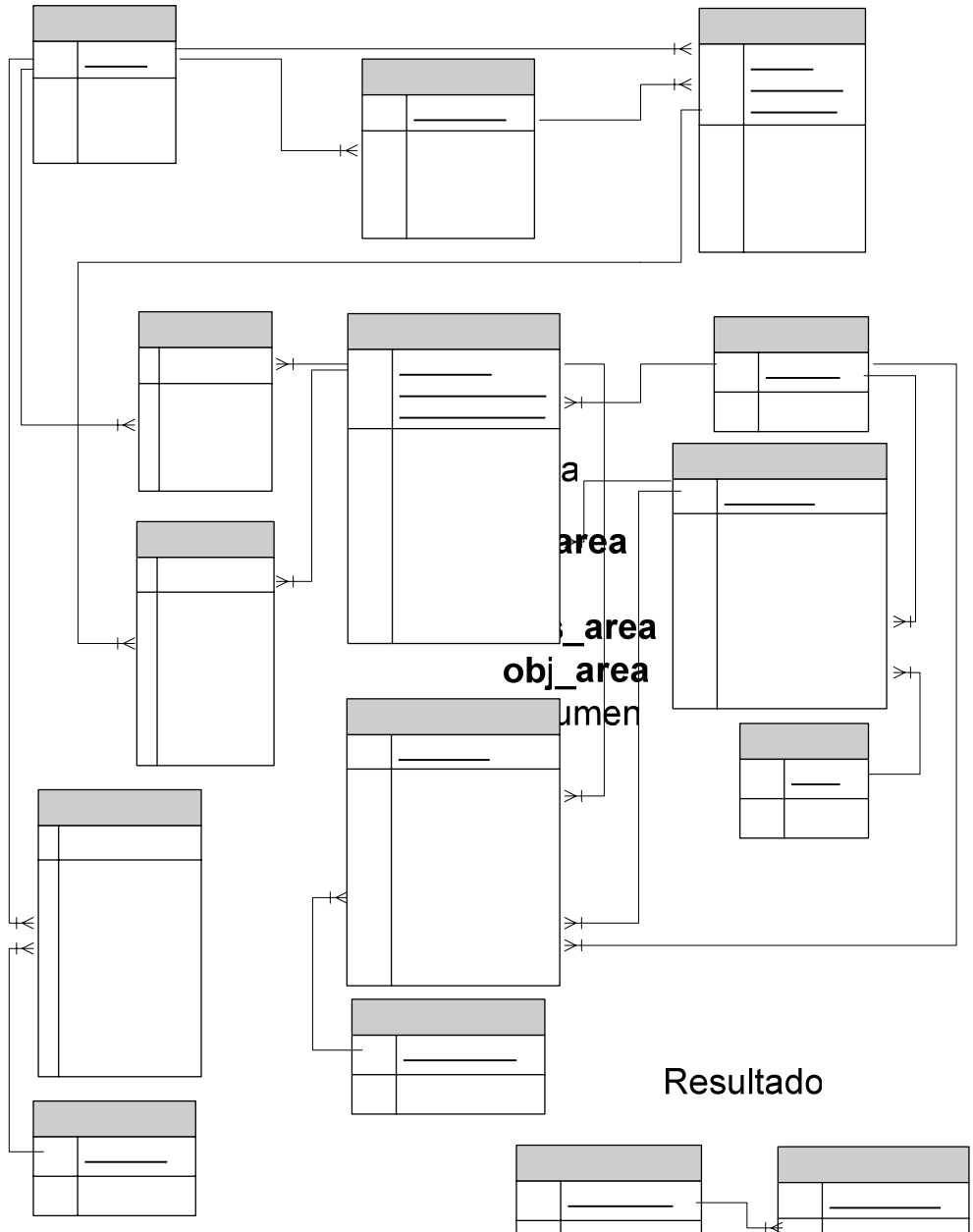

a
area
_area
obj_area
umen
Resultado
_exa
id_area
total_peso
total_gral
Seccio
PK id_sec
id_area
des_se
obj_se
resume
Exam
PK id_exam
PK id_depto
PK id_depto
des_exa
obj_exa
alcance
id_estat
id_usua
fecha_c
comenta
id_exam
Evaluación

Tabla de códigos del sistema

El sistema hace uso de códigos internos, con los cuales lleva a cabo una serie de procesos, a continuación se detalla cada uno de ellos.

Entidad	**EXAMEN**	
Campo	**Estatus de examen “id_estatus”**	
Valor	**Descripción**	**Comentario**
0	Incompleto	Permite identificar que el examen esta en estatus de pendiente, aun no se ha completado el examen.
1	Completo	Identifica la finalización del examen, todas las preguntas han sido evaluadas
Campo	**Tipo de examen “tipo_examen”**	
Valor	**Descripción**	**Comentario**
0	Publico	Identificado que el examen puede ser visto por todos los usuarios evaluadores.
1	Privado	Código que asegura el examen, restringiendo el uso solamente al usuario que lo creo.
Entidad	**ACCION**	
Campo	**Tipo de acción “id_accion”**	
Valor	**Descripción**	**Comentario**
1	Excelente	Código que determina el dictamen de evaluación excelente, este se asigna a los puntajes consolidados por área de 81 a 100 %
2	Muy Bueno	Código que determina el dictamen de evaluación Muy Bueno, este se asigna a los puntajes consolidados por área de 61 a 80 %
3	Básico	Código que determina el dictamen de evaluación Básico, este se asigna a los puntajes consolidados por área de 41 a 60 %
4	Deficiente	Código que determina el dictamen de evaluación Deficiente, este

		se asigna a los puntajes consolidados por área de 21 a 40 %
5	Falla gravemente	Código que determina el dictamen de evaluación Falla gravemente, este se asigna a los puntajes consolidados por área de 0 a 20 %
Entidad	**EVALUACION**	
Campo	**Resultado a pregunta de controles “id_estatus”**	
Valor	**Descripción**	**Comentario**
0	No evaluado	Identificador que el control no ha sido evaluado.
1	Si cumple	Identificador que el resultado de la evaluación al control fue positivo totalmente (Calculo por peso toma el 100% del peso asignado al control evaluado).
2	No Cumple	Identificador que el resultado de la evaluación al control fue negativo (Calculo por peso toma el 0% del peso asignado al control evaluado).
3	Parcialmente Cumple	Identificador que el resultado de la evaluación al control fue parcialmente positivo (Calculo por peso toma el 50% del peso asignado al control evaluado).

Diccionario de procesos

SISTEMA	*Control automatizado para la ejecución de una auditoría informática aplicando la norma iso1779***.**
MODULO	**Usuarios** Administra la gestión de los usuarios autorizados para utilizar el sistema, manejando identificador, clave, nivel de permiso de cada usuario.
Procesos	**Descripción**
Consulta usuario	Presenta lista de usuarios creados en el sistema, tomando en cuenta solo aquellos que se encuentran en estado de alta (activos).
Crea usuario	Adición de usuario al sistema
Modifica usuario	Actualización de datos del usuario; no se puede modificar el código o identificador.
Elimina usuario	Borra el registro seleccionado de forma definitiva.
MODULO	**Roles** Controla los permisos que se otorgarán a cada usuario creado para utilizar el sistema.
Procesos	**Descripción**
Consulta roles	Presenta las diferentes opciones de roles que controla el software, por definición el sistema permite únicamente tres tipos de roles: Auditor, Ejecutivo y Consulta, la explicación de cada rol se puede revisar en la sección de requerimientos (controles) del documento de análisis y diseño del proyecto.
Crea rol	Adiciona un nuevo rol al sistema. La versión 1 tiene deshabilitada esta función
Modifica rol	Actualiza datos de roles ya creados, sin poder cambiar el código o identificador del rol. La versión 1 tiene deshabilitada esta función
Elimina rol	Borra el registro seleccionado de forma definitiva. La versión 1 tiene deshabilitada esta función
MODULO	**Base de conocimiento** Administra el contenido de la norma ISO17799, sus áreas, secciones y controles.
	Procesos para: Áreas, Secciones y Controles
Procesos	**Descripción**
Crea Base de conocimiento	Proceso a cargo de crear las diferentes áreas, secciones y controles relacionados entre si y que forman parte del contenido de la norma ISO17799.
Modifica Base de conocimiento	Actualiza información de la base de conocimiento; sin poder modificar códigos o identificadores de registro.
Elimina Base de conocimiento	Borra el registro seleccionado de forma definitiva, este proceso verifica que se lleve a cabo de forma jerárquica de hijos a padres; es decir, es necesario eliminar primero los controles asociados a una sección, luego las secciones asociadas a una área.

MODULO	**Reglas y políticas de cumplimiento** Administra la definición de resultados, tratamiento a los diferentes niveles de cumplimiento, reglas de recomendaciones y observaciones.
Procesos	**Descripción**
Consulta Reglas	Proceso que presenta la lista de reglas asociadas por áreas y niveles de cumplimiento.
Crea Regla	Adiciona una nueva regla asociada a un área y puntaje específico, definiendo las características de esta regla.
Modifica Regla	Actualiza información de reglas; sin poder modificar códigos o identificadores de registro.
Elimina Regla	Borra el registro seleccionado de forma definitiva.
MODULO	**Departamentos** Controla las unidades donde laboran los usuarios creados en el sistema
Procesos	**Descripción**
Consulta Departamentos	Proceso que presenta la lista de reglas asociadas por áreas y niveles de cumplimiento.
Crea Departamentos	Adiciona un nuevo registro al catálogo de departamentos.
Modifica Departamentos	Actualiza información de departamentos; sin poder modificar códigos o identificadores de registro.
Elimina Departamentos	Borra el registro seleccionado de forma definitiva.
MODULO	**Acciones** Administra la asignación de resultados finales a las evaluaciones de exámenes de cumplimiento.
Procesos	**Descripción**
Consulta Acciones	Presenta la lista de acciones almacenadas en éste catálogo.
Crea Acciones	Adiciona una nueva acción al catalogo. Para la versión 1 no se permite crear.
Modifica Puntajes	Actualiza información de acciones ya almacenadas; sin poder modificar códigos o identificadores de registro. La versión 1 no esta habilitada este función
Elimina Puntajes	Borra el registro seleccionado de forma definitiva. La versión 1 no permite eliminar registros de este catalogo.
MODULO	**Parámetros de Informe** Administra los diferentes parámetros o elementos que se pueden adicionar durante la presentación de los informes de Auditoría.
Procesos	**Descripción**
Consulta Parámetros	Proceso que presenta la lista de parámetros creados, con su detalle respectivo
Crea Parámetros	Adiciona un nuevo parámetro al sistema
Modifica Parámetros	Actualiza información de parámetros; sin poder modificar códigos o identificadores de registro.
Elimina Parámetros	Borra el registro seleccionado de forma definitiva.

MODULO	**Centro de Documentación** Administra la consulta a la documentación sobre la norma de seguridad informática ISO17799
Procesos	**Descripción**
Consulta Áreas	Proceso que lista las áreas de la norma, y cada uno de los objetivos o secciones asociadas.
Consulta Secciones-Controles	Proceso que lista todos los controles asociados a la sección y área seleccionada.
Consulta Controles-Detalle	Proceso que presenta a nivel de detalle la información del control de la norma y permite navegar por el resto de controles asociados a la sección y área seleccionada. En esta parte se puede navegar por cada control asociado al área y sección.
MODULO	**Papel de trabajo** Modulo perteneciente a la gestión principal del sistema, herramienta de trabajo para llevar a cabo la medición del nivel de conformidad con la norma ISO17799.
Procesos	**Descripción**
Identificación del examen y listado de áreas	Proceso que permite ingresar la identificación del examen a realizar a través del cuestionario, además presenta las diferentes áreas de la norma para poder incorporar en el cuestionario de cumplimiento
Selecciona áreas	Selección de algunas o todas las áreas de la norma para la creación del examen de cumplimiento
Crear cuestionario	Proceso que construye la herramienta de trabajo para el proceso de evaluación con el nivel de conformidad.
MODULO	**Exámenes de cumplimiento** Módulo que administra los resultados obtenidos al examen de conformidad con la norma.
Procesos	**Descripción**
Solicitud de cuestionarios	Proceso que presenta la lista de los diferentes cuestionarios creados en el sistema y sobre el cual se llevara a cabo el proceso de evaluación.
Resultado de cuestionario	Almacenamiento de cada respuesta al cuestionario de cumplimiento, asignando un estatus de resultado a cada control de la norma, este proceso alimenta el almacén de datos evaluación. Además este proceso permite almacenar documentos de cualquier tipo como evidencia a la investigación realizada, los cuales pueden ser consultados luego de ser almacenados.
Calcular puntajes de resultados	Este proceso realiza el cálculo de conformidad por control de dos formas diferentes simultáneamente. El primero por pesos, tomando el valor de importancia asociado a cada control por la Institución. El segundo considera a cada control de igual importancia y se van consolidando los resultados positivos los resultados. Posteriormente se consolidan los resultados de la evaluación por cada área de la norma, este proceso alimenta el almacén de los datos “Resultados”.

MODULO	**Informes de cumplimiento** Módulo que elabora los informes (reportes) de auditoría para mostrar el nivel de conformidad de la norma a cada uno de los exámenes desarrollados.
Procesos	**Descripción**
Lista de exámenes	Proceso que presenta la lista de exámenes ya realizados en el sistema y sobre el cual se desea crear un informe de cumplimiento.
Calcular puntajes consolidados	Proceso que consolidada los resultados totales para elaborar un nivel de conformidad global de la norma.
Análisis de resultados	Proceso que verifica el puntaje obtenido a cada área de la norma y extrae las reglas asociadas con estos resultados, con lo cual elabora el análisis correspondiente para hacer impreso en el informe.
Consolidar información	Este proceso recopila toda la información que será parte del informe de cumplimiento, elementos como: Base de conocimiento ISO17799, respuestas al examen, puntajes, resultado, introducción sobre la norma, título del reporte, recomendaciones, conclusiones.
Crea Informe	Proceso que genera el reporte hacer presentado a los usuarios involucrados en la gestión de la seguridad de los sistemas de información de la UFG.
MODULO	**Referencias** Administra información sobre sitios de interés relacionados al tema de seguridad informática, siendo un apoyo directo al esfuerzo de documentar al personal técnico de la Intitución.
Procesos	**Descripción**
Consulta Referencias	Lista de sitios de interés incorporados en el catálogo de referencias.
Crea Referencias	Adiciona un nuevo registro a la tabla de referencias, describiendo su URL, un breve resumen del contenido y una calificación de la calidad de la información del sitio. Este proceso consta de dos subprocesos. El primero crea las categorías posibles de referencias y el segundo adiciona referencias asociadas a estas categorías definidas.
Modifica Referencias	Actualiza información de referencias; sin poder modificar códigos o identificadores de registro.
Elimina Referencias	Borra el registro seleccionado de forma definitiva.
MODULO	**Ayuda** Proporciona la documentación de apoyo para el uso del sistema.
Procesos	**Descripción**
Consulta Ayuda	Proceso que presenta la ayuda en línea para el usuario, además permite que se pueda descargar en varios formatos: doc, pdf. Además existe otra ayuda de preguntas más frecuentes (FAQ), que proporciona de formas más precisa algunas dudas acerca del uso del sistema.

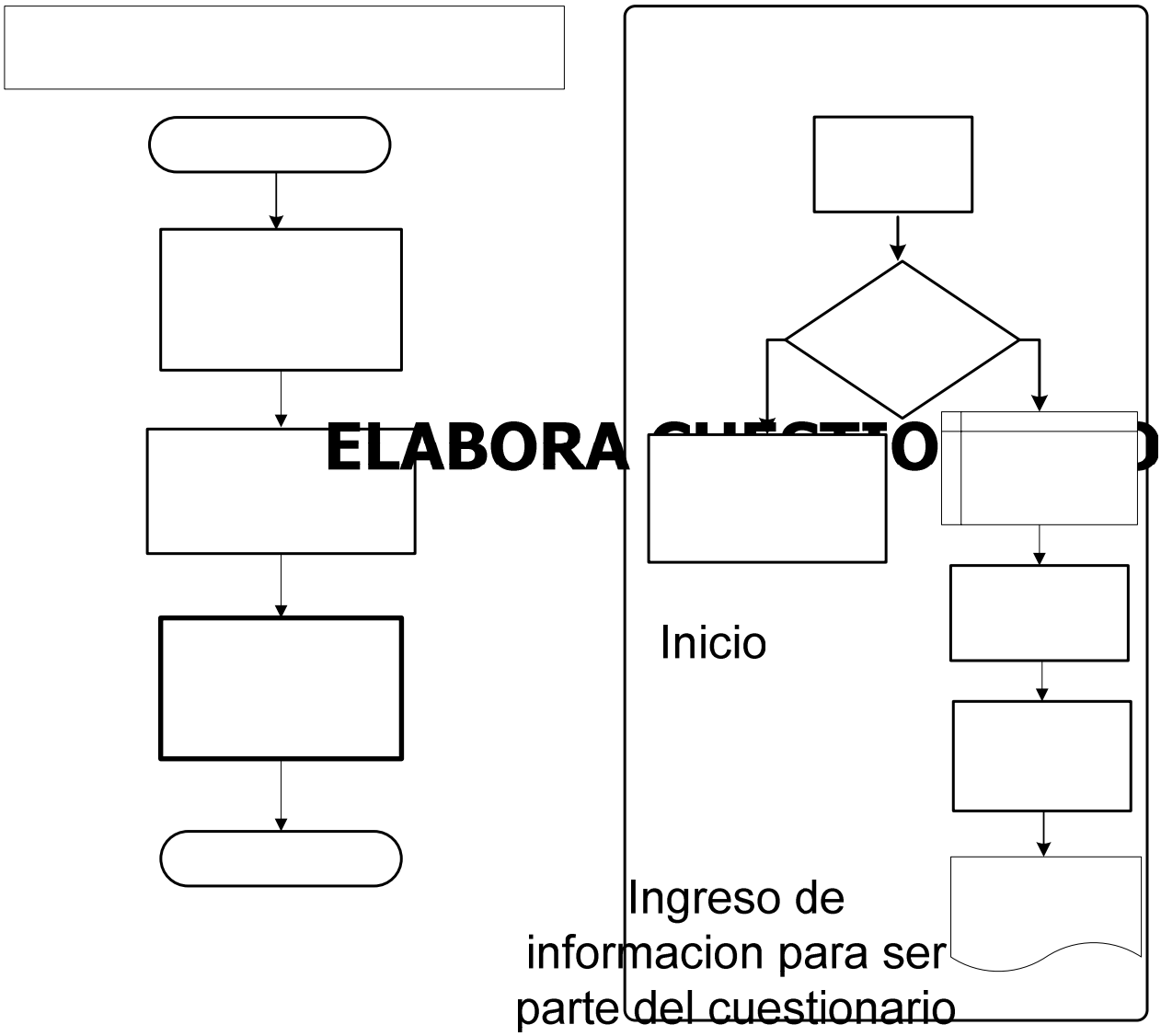
Flujos de Procesos

Esquema gráfico sobre los procesos, subproceso del modulo de cumplimiento 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”.

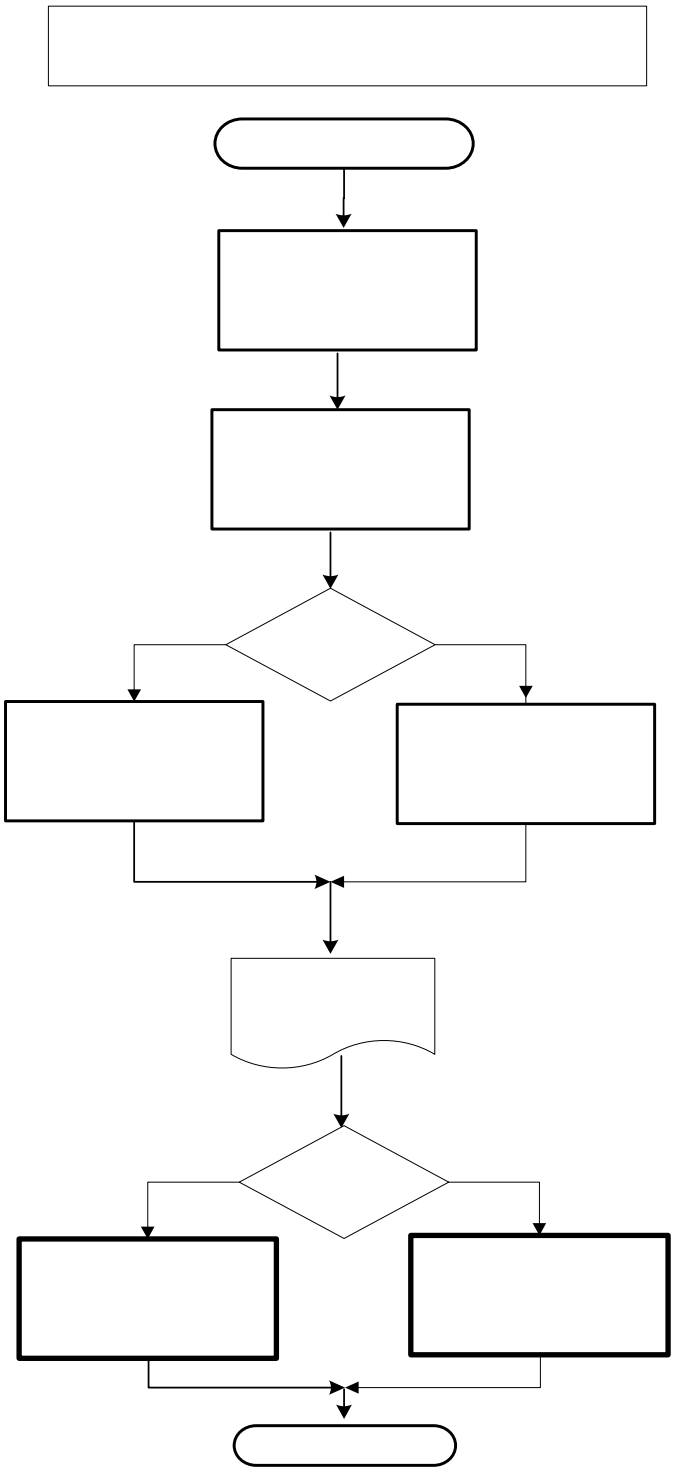
A continuación se presentan los procesos de las secciones:

- Cuestionarios ISO 17799
- Exámenes de cumplimiento
- Calculo de Conformidad
- Motor de Reglas de decisión
- Informe de Auditoria

Cuestionario ISO 17799



Exámenes de cumplimiento



LISTA EX

Ini

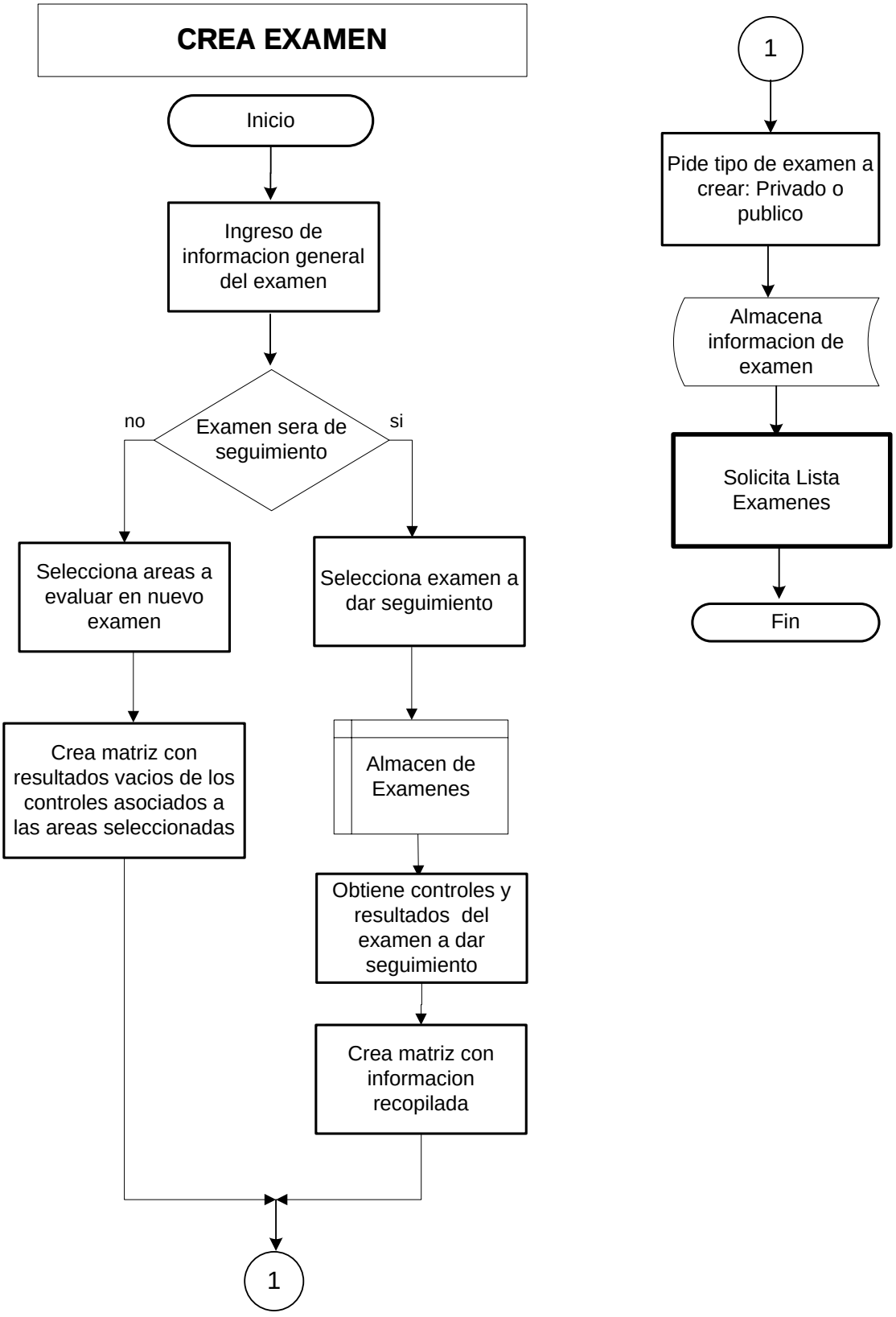
Seleccion
en estatus
usuario ac
los pu

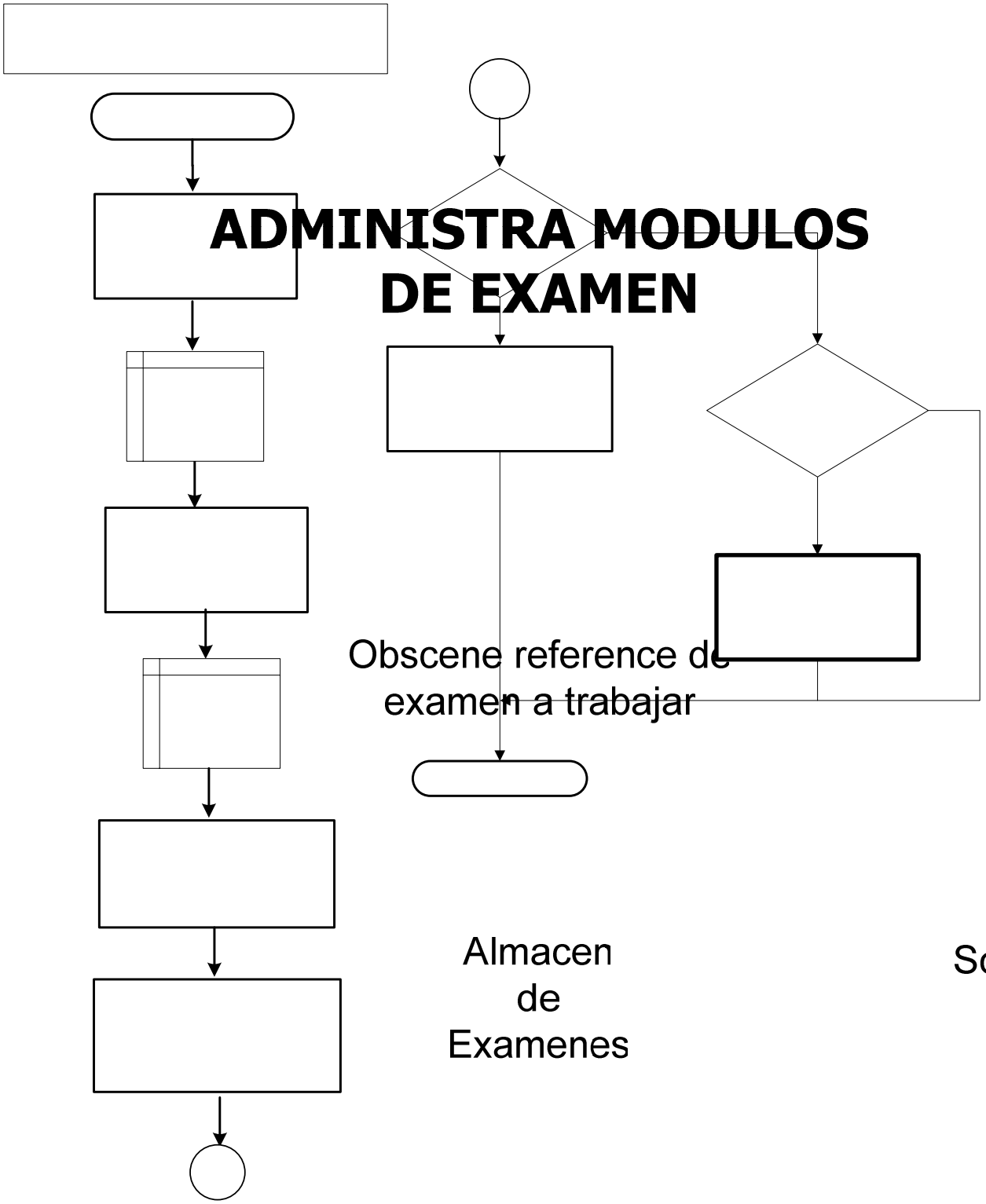
Ordena exa
fecha ma

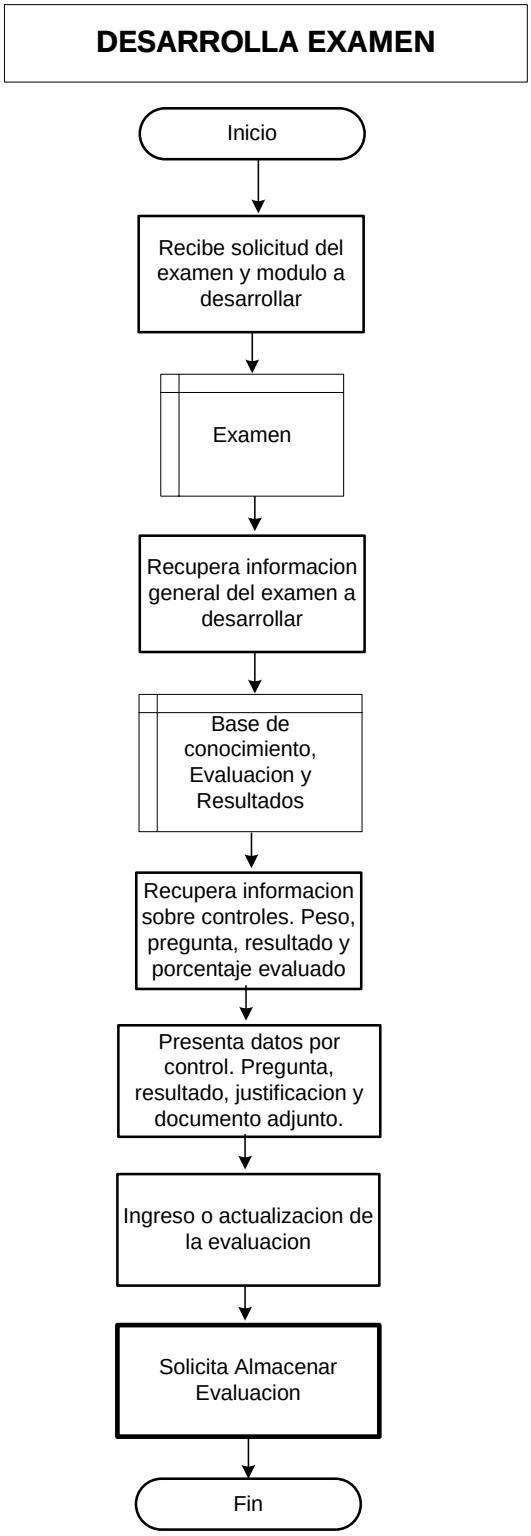
no

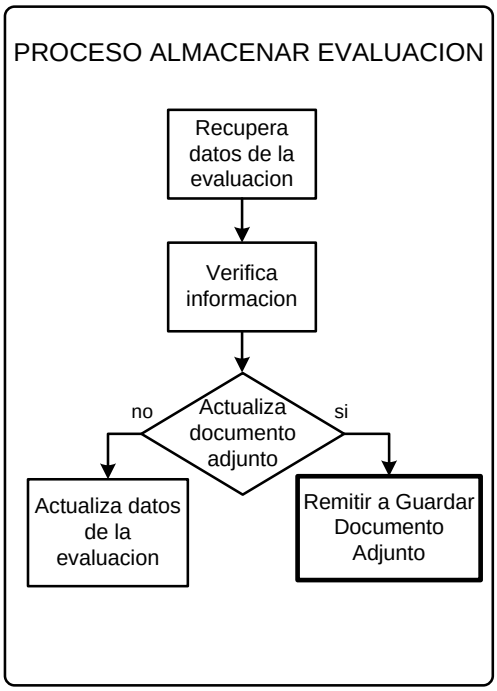
Exame
publ

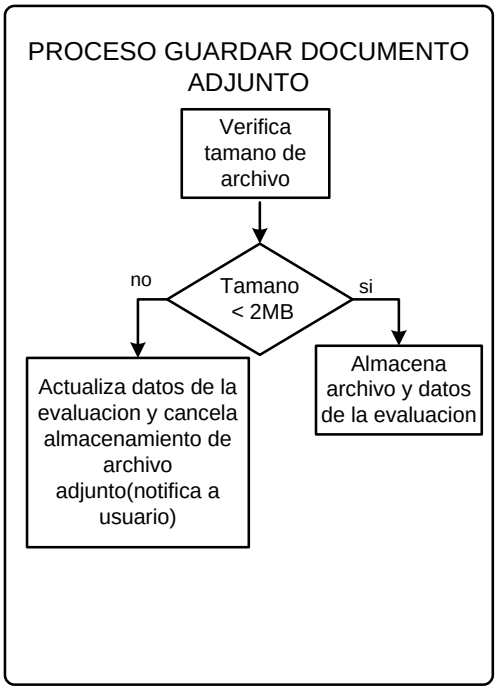
Activa unicamente

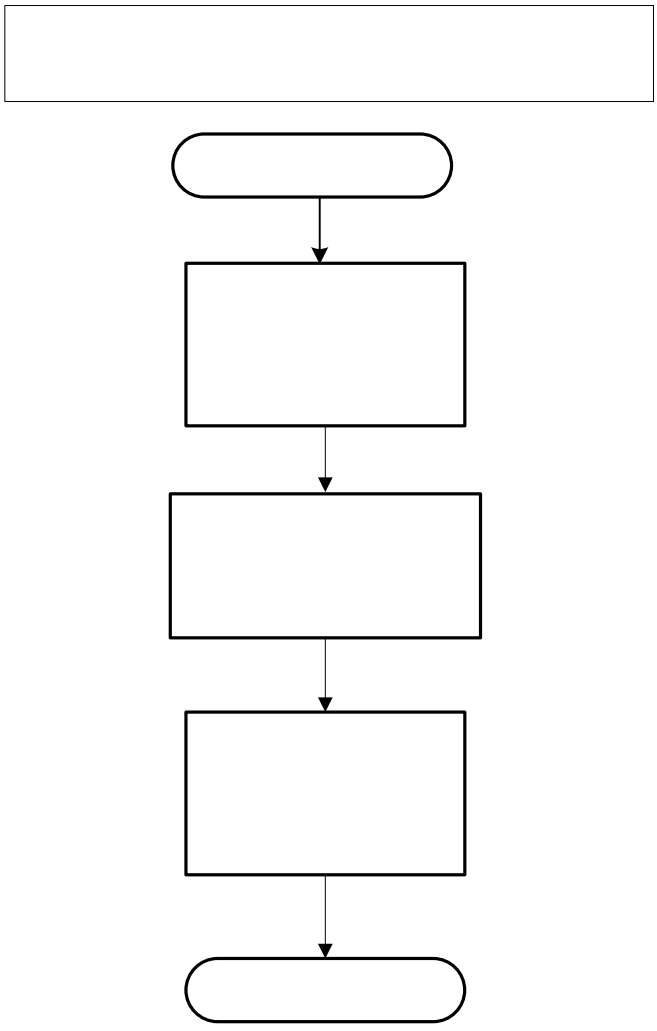

CREA EXAMEN
Inicio
Ingreso de informacion general del examen
Examen sera de seguimiento
no
si
Selecciona areas a evaluar en nuevo examen
Selecciona examen a dar seguimiento
Crea matriz con resultados vacios de los controles asociados a las areas seleccionadas
Almacen de Examenes
Obtiene controles y resultados del examen a dar seguimiento
Crea matriz con informacion recopilada
1
1
Pide tipo de examen a crear: Privado o publico
Almacena informacion de examen
Solicita Lista Examenes
Fin


ADMINISTRA MODULOS DE EXAMEN
Obscene reference de examen a trabajar
Selec
accio
ava
si
Almacen de Examenes
Solicita Ve
Eex
Crea matriz detallada por control y consolidada por seccion y area


DESARROLLA EXAMEN
Inicio
Recibe solicitud del examen y modulo a desarrollar
Examen
Recupera informacion general del examen a desarrollar
Base de conocimiento, Evaluacion y Resultados
Recupera informacion sobre controles. Peso, pregunta, resultado y porcentaje evaluado
Presenta datos por control. Pregunta, resultado, justificacion y documento adjunto.
Ingreso o actualizacion de la evaluacion
Solicita Almacenar Evaluacion
Fin


PROCESO ALMACENAR EVALUACION
Recupera datos de la evaluacion
Verifica informacion
Actualiza documento adjunto
no
si
Actualiza datos de la evaluacion
Remitir a Guardar Documento Adjunto


PROCESO GUARDAR DOCUMENTO ADJUNTO
Verifica tamano de archivo
Tamano < 2MB
no
si
Actualiza datos de la evaluacion y cancela almacenamiento de archivo adjunto(notifica a usuario)
Almacena archivo y datos de la evaluacion



VER AVANCE

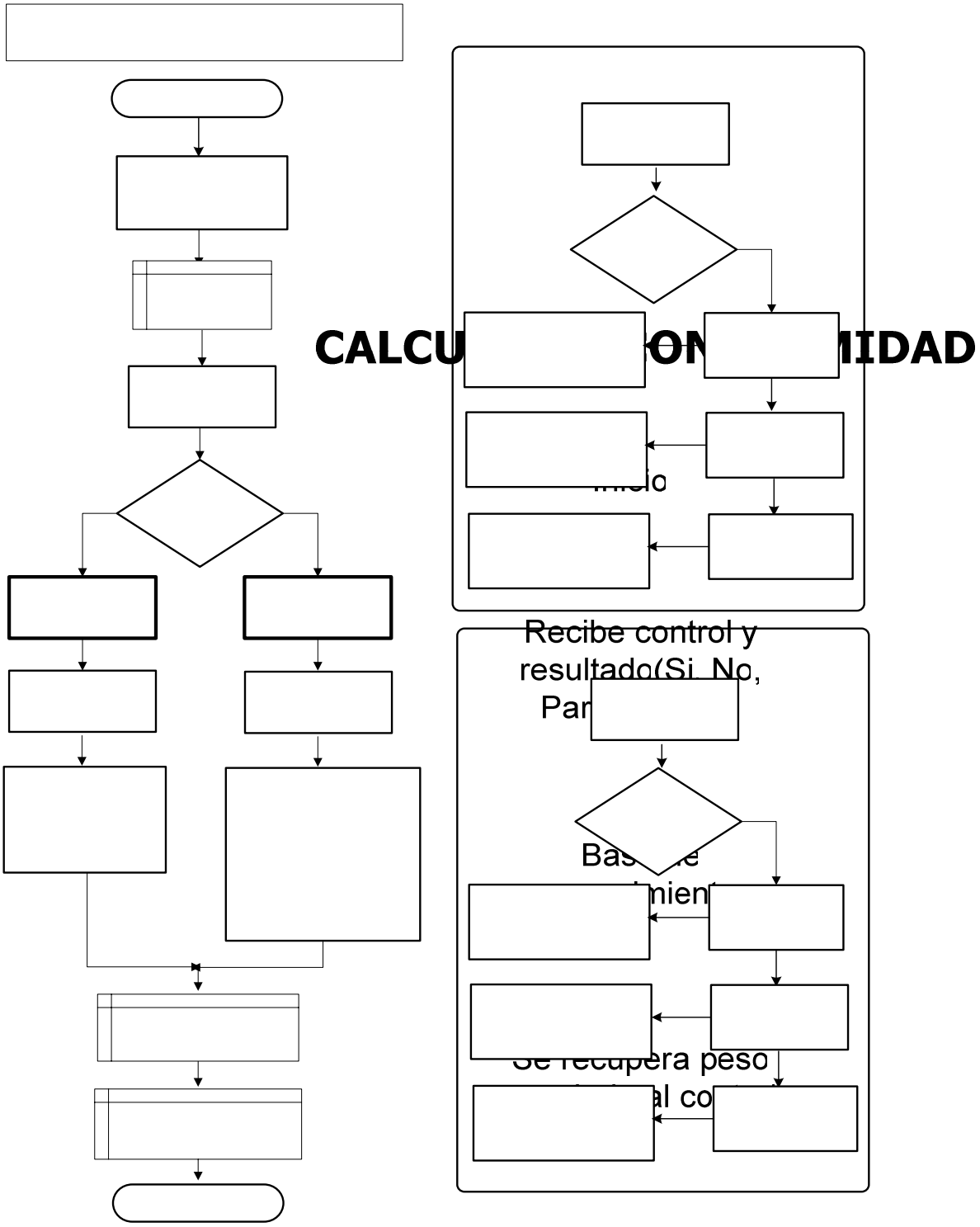
Inici

Recibe d
examen y
revi

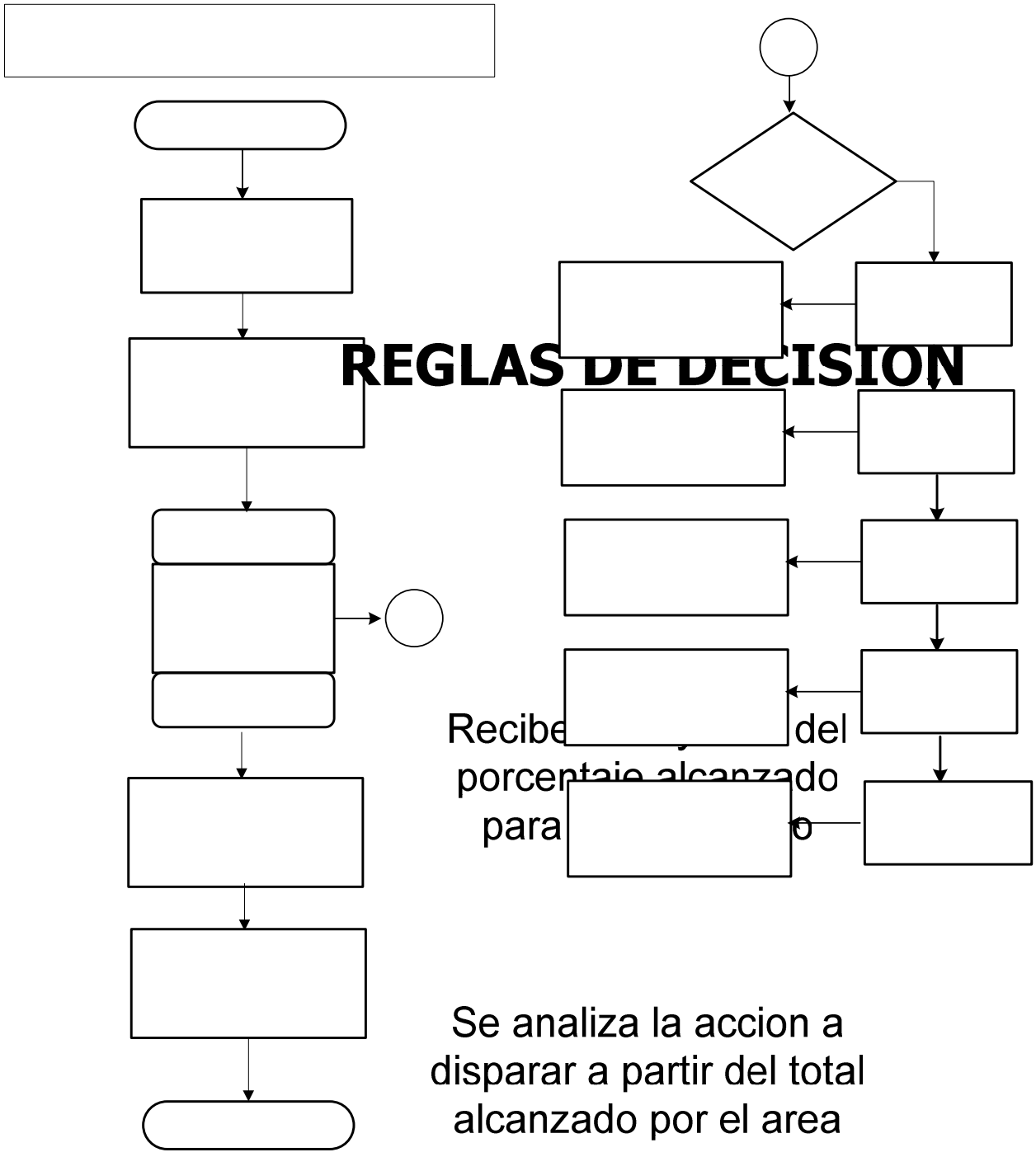
Elabora
resultados d
control, % p
% por d

Crea pag
presentar

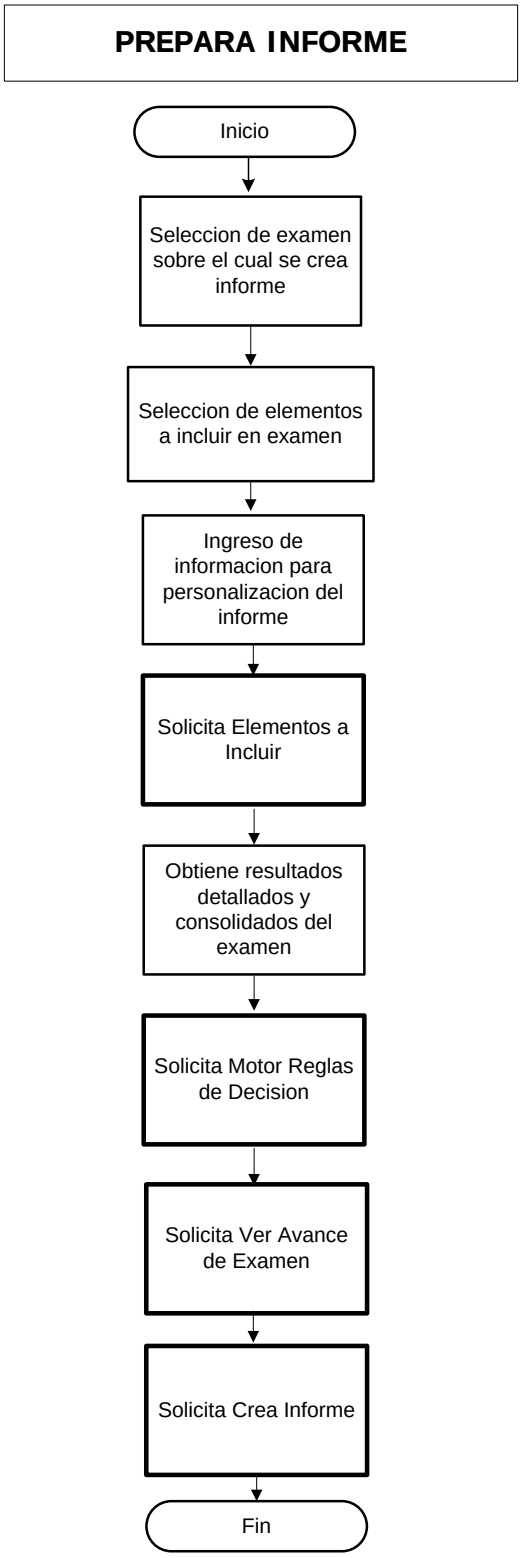
Calculo de conformidad

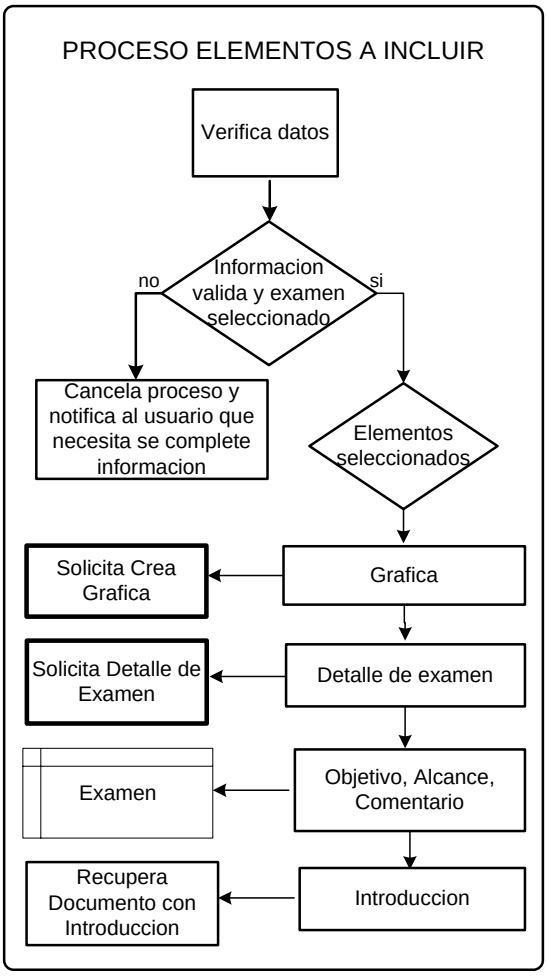


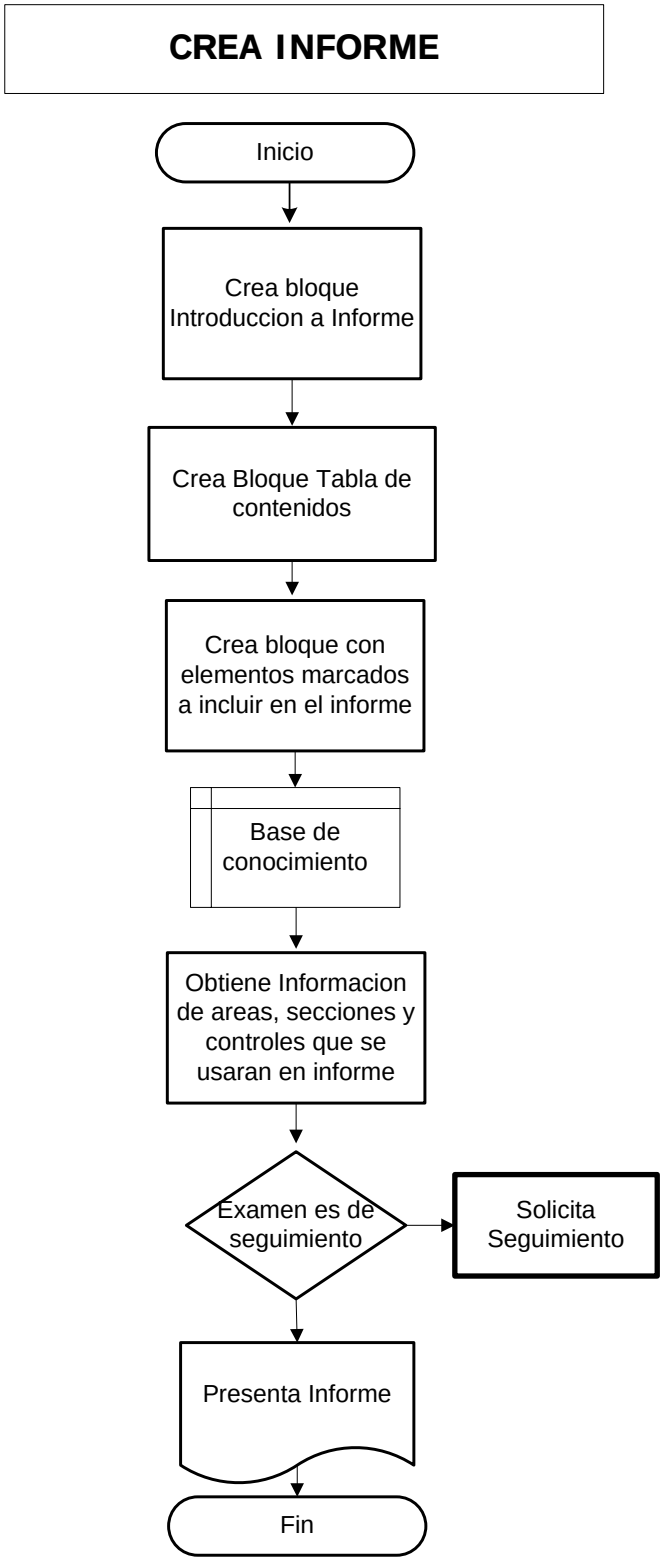
Motor de reglas de decisión

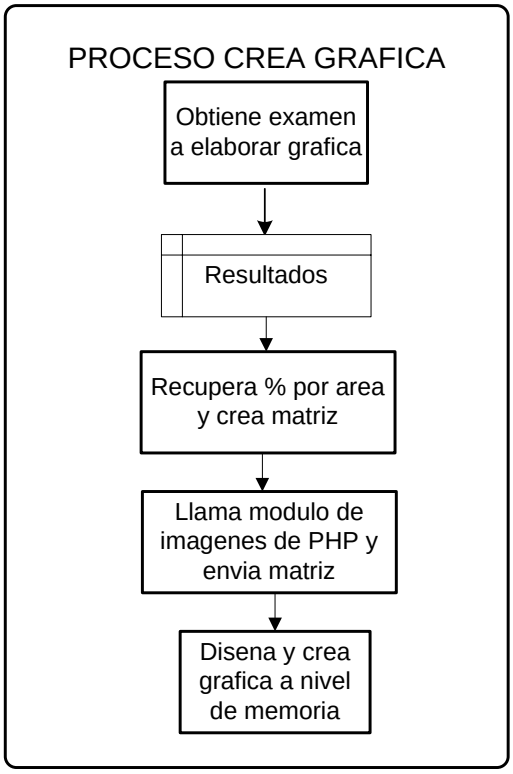


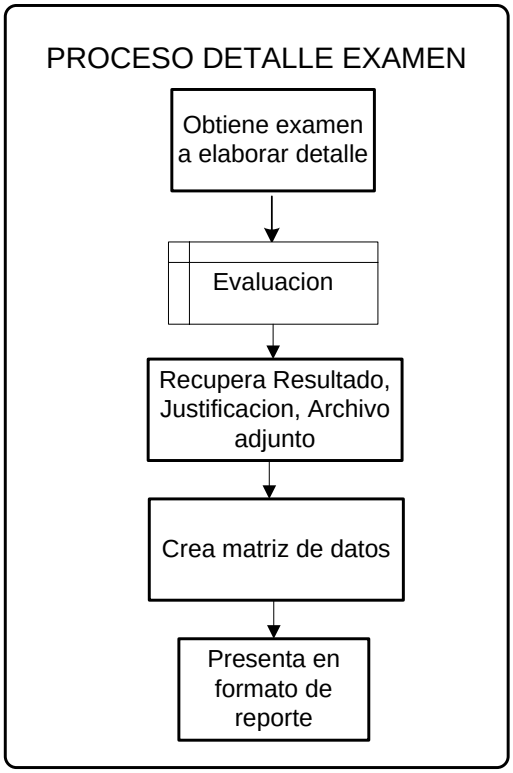
Informe de auditoria

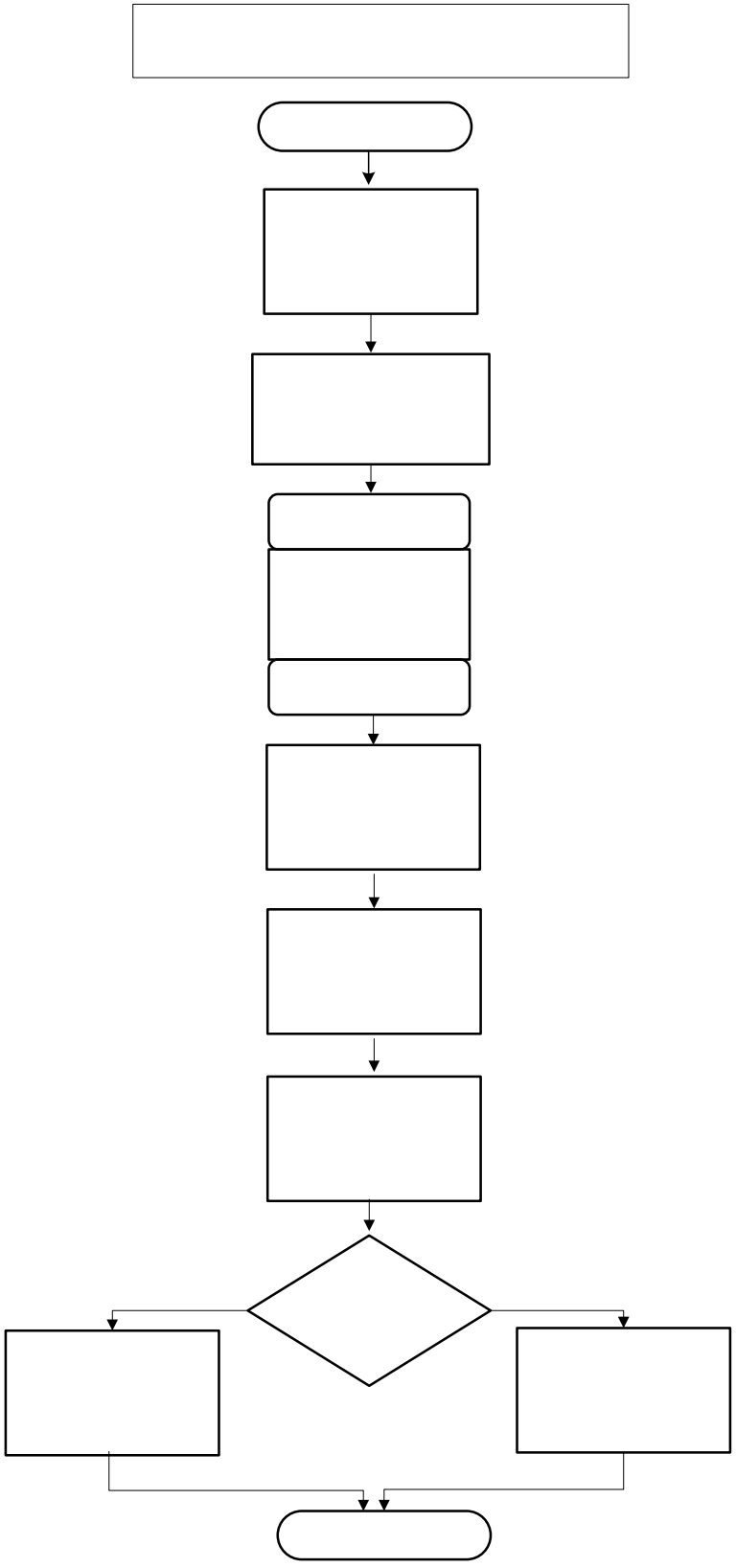





CREA INFORME
Inicio
Crea bloque Introduccion a Informe
Crea Bloque Tabla de contenidos
Crea bloque con elementos marcados a incluir en el informe
Base de conocimiento
Obtiene Informacion de areas, secciones y controles que se usaran en informe
Examen es de seguimiento
Solicita Seguimiento
Presenta Informe
Fin


PROCESO CREA GRAFICA
Obtiene examen a elaborar grafica
Resultados
Recupera % por area y crea matriz
Llama modulo de imagenes de PHP y envia matriz
Disena y crea grafica a nivel de memoria


PROCESO DETALLE EXAMEN
Obtiene examen a elaborar detalle
Evaluacion
Recupera Resultado, Justificacion, Archivo adjunto
Crea matriz de datos
Presenta en formato de reporte



SEGUI

Inic

Recibe e
eva

Verifica
exame

Exa

Obtiene in
de exa
resulta
evalu

Evalu

Crea matri

Script de creación BD

Definición de estructura de base de datos, en formato de SQL (Lenguaje de consulta estructurada) para instalarse en motor de base de datos.

```
/*
Script de creación
Database - iso17799 , Version 1.0
**********************************************************************
El Salvador, Julio/05
*/

create database if not exists `iso17799`;

USE `iso17799`;

/*Table structure for table `accion` */

drop table if exists `accion`;

CREATE TABLE `accion` (
  `id_accion` decimal(2,0) NOT NULL default '0',
  `des_accion` varchar(100) NOT NULL default '',
  PRIMARY KEY  (`id_accion`)
);

/*Table structure for table `area` */

drop table if exists `area`;
`
CREATE TABLE `area` (
  `id_area` decimal(2,0) NOT NULL default '0',
  `des_area` varchar(100) NOT NULL default '',
  `obj_area` mediumtext NOT NULL,
  `resumen` mediumtext,
  PRIMARY KEY  (`id_area`)
);


/*Table structure for table `categoria` */

drop table if exists `categoria`;

CREATE TABLE `categoria` (
  `id_categoria` decimal(2,0) NOT NULL default '0',
  `des_categoria` varchar(100) NOT NULL default '',
  PRIMARY KEY  (`id_categoria`)
);
```

```
/*Table structure for table `control` */

drop table if exists `control`;

CREATE TABLE `control` (
  `id_area` decimal(2,0) NOT NULL default '0',
  `id_seccion` decimal(2,0) NOT NULL default '0',
  `id_control` decimal(2,0) NOT NULL default '0',
  `des_control` varchar(100) NOT NULL default '',
  `obj_control` mediumtext NOT NULL,
  `guia` mediumtext,
  `pregunta` mediumtext NOT NULL,
  `peso` decimal(3,0) NOT NULL default '0',
  PRIMARY KEY  (`id_area`,`id_seccion`,`id_control`),
  FOREIGN KEY (id_area) REFERENCES area (id_area),
  FOREIGN KEY (id_seccion) REFERENCES seccion (id_seccion)

);


/*Table structure for table `departamento` */

drop table if exists `departamento`;

CREATE TABLE `departamento` (
  `id_depto` decimal(2,0) NOT NULL default '0',
  `des_depto` varchar(100) NOT NULL default '',
  PRIMARY KEY  (`id_depto`)
);

/*Table structure for table `evaluacion` */

drop table if exists `evaluacion`;

CREATE TABLE `evaluacion` (
  `id_examen` decimal(5,0) NOT NULL default '0',
  `id_control` decimal(6,0) NOT NULL default '0',
  `id_estatus` decimal(2,0) NOT NULL default '0',
  `justificacion` mediumtext,
  `tipo_archivo` varchar(40) default NULL,
  `archivo` mediumblob,
  `titulo` varchar(250) default NULL
  FOREIGN KEY (id_examen) REFERENCES examen (id_examen),
  FOREIGN KEY (id_control) REFERENCES control (id_control)

);
```

```
/*Table structure for table `examen` */

drop table if exists `examen`;

CREATE TABLE `examen` (
  `id_examen` decimal(5,0) NOT NULL default '0',
  `des_examen` varchar(100) NOT NULL default '',
  `obj_examen` mediumtext NOT NULL,
  `alcance` mediumtext NOT NULL,
  `id_estatus` decimal(2,0) NOT NULL default '0',
  `id_usuario` decimal(2,0) NOT NULL default '0',
  `fecha_creacion` varchar(8) NOT NULL default '',
  `comentario` mediumtext,
  `id_depto_evaluar` decimal(2,0) NOT NULL default '0',
  `id_depto_solicita` decimal(2,0) NOT NULL default '0',
  `id_examen_padre` decimal(5,0) default '0',
  `tipo_examen` decimal(1,0) NOT NULL default '0',
  PRIMARY KEY  (`id_examen`),
  FOREIGN KEY (id_examen)       REFERENCES examen (id_examen),
  FOREIGN KEY (id_usuario)      REFERENCES usuario (id_usuario),
  FOREIGN KEY (id_depto_evaluar) REFERENCES depto (id_depto),
  FOREIGN KEY (id_examen_padre)  REFERENCES depto (id_depto),
  FOREIGN KEY (id_examen_padre)  REFERENCES examen (id_examen),
);


/*Table structure for table `informe` */

drop table if exists `informe`;

CREATE TABLE `informe` (
  `id_informe` decimal(5,0) NOT NULL default '0',
  `id_examen` decimal(5,0) NOT NULL default '0',
  `titulo_reporte` varchar(100) default NULL,
  `mensaje` varchar(100) default NULL,
  `autor1` varchar(40) default NULL,
  `autor2` varchar(40) default NULL,
  `id_depto_destino` decimal(2,0) NOT NULL default '0',
  `parametros` varchar(40) default NULL,
  `id_usuario` decimal(2,0) NOT NULL default '0',
  `fecha_creacion` varchar(8) NOT NULL default '',
  PRIMARY KEY  (`id_informe`),
  FOREIGN KEY (id_examen)       REFERENCES examen (id_examen),
  FOREIGN KEY (id_usuario)      REFERENCES usuario (id_usuario),
  FOREIGN KEY (id_depto_destino) REFERENCES depto (id_depto),
);
```

```
/*Table structure for table `parametro_informe` */

drop table if exists `parametro_informe`;

CREATE TABLE `parametro_informe` (
  `id_parametro` decimal(2,0) NOT NULL default '0',
  `des_parametro` varchar(100) NOT NULL default '',
  `resumen` varchar(150) NOT NULL default '',
  PRIMARY KEY  (`id_parametro`)
);

/*Table structure for table `referencia` */

drop table if exists `referencia`;

CREATE TABLE `referencia` (
  `id_referencia` decimal(5,0) NOT NULL default '0',
  `id_categoria` decimal(2,0) NOT NULL default '0',
  `des_referencia` varchar(150) NOT NULL default '',
  `url_referencia` varchar(100) NOT NULL default '',
  `resumen_referencia` mediumtext NOT NULL,
  PRIMARY KEY  (`id_referencia`,`des_referencia`),
  FOREIGN KEY (id_categoria) REFERENCES categoria (id_categoria)
);


/*Table structure for table `regla_decision` */

drop table if exists `regla_decision`;

CREATE TABLE `regla_decision` (
  `id_regla` decimal(5,0) NOT NULL default '0',
  `des_regla` varchar(150) NOT NULL default '',
  `id_area` decimal(2,0) NOT NULL default '0',
  `id_accion` decimal(2,0) NOT NULL default '0',
  `dictamen` varchar(150) NOT NULL default '',
  `resultado` mediumtext NOT NULL,
  `recomendacion` mediumtext,
  `observacion` mediumtext,
  `conclusion` mediumtext,
  PRIMARY KEY  (`id_regla`),
  FOREIGN KEY (id_area)       REFERENCES area (id_area),
  FOREIGN KEY (id_accion)     REFERENCES accion (id_accion)
);
```

```
/*Table structure for table `resultado` */

drop table if exists `resultado`;

CREATE TABLE `resultado` (
  `id_examen` decimal(5,0) NOT NULL default '0',
  `id_area` decimal(2,0) NOT NULL default '0',
  `total_peso` double(4,2) NOT NULL default '0.00',
  `total_gral` double(4,2) NOT NULL default '0.00',
  PRIMARY KEY  (`id_examen`,`id_area`),
  FOREIGN KEY (id_examen)    REFERENCES examen (id_examen),
  FOREIGN KEY (id_area)      REFERENCES area (id_area)
);


/*Table structure for table `rol` */

drop table if exists `rol`;

CREATE TABLE `rol` (
  `id_rol` decimal(2,0) NOT NULL default '0',
  `des_rol` varchar(100) NOT NULL default '',
  PRIMARY KEY  (`id_rol`)
);


/*Table structure for table `seccion` */

drop table if exists `seccion`;

CREATE TABLE `seccion` (
  `id_seccion` decimal(2,0) NOT NULL default '0',
  `id_area` decimal(2,0) NOT NULL default '0',
  `des_seccion` varchar(100) NOT NULL default '',
  `obj_seccion` mediumtext NOT NULL,
  `resumen` mediumtext,
  PRIMARY KEY  (`id_seccion`,`id_area`),
  FOREIGN KEY (id_area)      REFERENCES area (id_area)
);
```

```
/*Table structure for table `usuario` */

drop table if exists `usuario`;

CREATE TABLE `usuario` (
  `id_usuario` decimal(2,0) NOT NULL default '0',
  `login` varchar(20) NOT NULL default '',
  `clave` varchar(8) NOT NULL default '',
  `nom_usuario` varchar(50) NOT NULL default '',
  `email` varchar(35) default NULL,
  `telefono` decimal(8,0) default NULL,
  `id_depto` decimal(2,0) NOT NULL default '0',
  `id_rol` decimal(2,0) NOT NULL default '0',
  `fecha_creacion` varchar(8) NOT NULL default '',
  `fecha_vencimiento` varchar(8) NOT NULL default '',
  PRIMARY KEY  (`id_usuario`),
  FOREIGN KEY (id_depto)    REFERENCES depto (id_depto),
  FOREIGN KEY (id_rol)      REFERENCES rol (id_rol),
);
```