4.6 DISEÑO DE SEGUIMIENTO Y AUDITORIA

La auditoria en informática es la revisión y la evolución de controles, sistemas, procedimientos de informática; de los equipos de computo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logra una utilización mas eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no solo la evaluación de los equipos de cómputo, de un sistema o procedimiento especifico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoria en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

4.6.1 Auditoria del SIMID: El siguiente diseño de auditoria proporciona una herramienta para la verificación futura del funcionamiento del SIMID, y el satisfactorio cumplimiento de todas las funcionalidades tanto técnicas como procedimentales, también permite evaluar el correcto cumplimiento de las políticas, estándares y normatividad de la Delegación Departamental de la Registraduría Nacional Regional Quindío.

El diseño de la presente auditoria proporciona la base para evaluar el sistema de control interno de la organización, en lo que respecta al área de sistemas en el manejo del SIMID.

El diseño de la auditoria se basa en listas de chequeo y cuestionarios de control interno, que permiten obtener información concreta respecto al tema de interés.

A continuación se especifican las fases que podrían hacer parte de una futura auditoría al SIMID.

4.6.1.1. Levantamiento de Información.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo del mismo.

En esta etapa se recolecta información básica acerca de la organización y especialmente en el área de sistemas; los temas específicos que deben tenerse en cuenta en la etapa son:

Cabe destacar que las personas vinculadas al proyecto, han prestado toda su colaboración y tiempo para colaborarnos en lo que este a su alcance.

4.6.1.2 Identificación De La Empresa Auditada.

En esta parte se maneja la información general de la Delegación Departamental de la Registraduría Nacional del Estado Civil Regional Quindío, sobre la caracterización de la empresa, los cuales poseen los siguientes ítems:

- Misión
- Visión
- Antecedentes
- Organigrama

4.6.1.3 Conocimientos del Departamento de Sistemas

La Delegación Departamental de la Registraduría Nacional del Estado Civil Regional Quindío, posee en la Registraduría Municipal de Armenia, el departamento de sistemas, el cual se encuentra apoyado por el centro de acopio que maneja la parte de identificación, que poseen a nivel general los siguientes ítems:

- Marco operativo y funcional
- Plan estratégico de sistemas de operación.
- Estándares de trabajo
- Manual de funciones.
- Plan de contingencias
- Planes objetivos y políticas
- Infraestructura tecnológica existente
- Sistemas operativos
- Aplicativos de propósito general (Desde de la Registraduría Nacional en Bogotá).
- Dependencias encargadas del manejo del SIMID.
- Información que maneja el SIMID.

- Personal que maneja el SIMID.
- Modificaciones después de la instalación del SIMID.

4.6.1.4 Planeación de Auditoria.

Para hacer una adecuada planeación de la auditoria en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoria en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos.

- Evaluación de los sistemas y procedimientos
- Evaluación de los equipos de cómputo

En esta etapa se evalúan los problemas encontrados en el levantamiento de información, esto es importante, ya que permite identificar aquellas áreas que requieren un estudio más a fondo.

4.6.1.5 Personal Participante.

Una de las partes más importantes dentro de la planeación de la auditoria en informática es el personal que deberá participar y sus características.

Para tener un adecuado control en el desarrollo de la auditoria se debe tener en cuenta que el personal que intervenga este debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o recompense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoria, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

También se debe contar con personas asignadas por los usuarios, para que en el momento que se solicite información o bien se efectué alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando y contemplen el grupo multidisciplinario, ya que se debe analizar no solo el punto de vista de la dirección de informática, sino también el del usuario del sistema (SIMID).

Para completar el grupo, como colaboradores directos en la realización de la auditoria se debe tener personas con las siguientes características.

- Técnico en informática

- Experiencia en el área de informática
- Conocimientos de los procesos que realizan con el SIMID.

4.6.1.6 Desarrollo de la auditoria.

Durante esta etapa se recolectara información referente al SIMID, y al sistema de control interno implantado alrededor de este. Dicha información se recolectara por medio de cuestionarios de control internos y listas de chequeo. Se deben tener en cuenta las opiniones de los usuarios.

4.6.1.7 Diagnóstico de la Auditoría.

Después de realizar el levantamiento de información se procede al análisis de los mismos, para así poder detectar las fortalezas y debilidades del sistema. El diagnóstico debe estar basado en datos objetivos y expresados en cifras, datos estadísticos, es decir, datos precisos de manera que coincidan con la situación real de la entidad. Basados en estos datos se elabora un informe de los problemas encontrados y las posibles soluciones para mejorar y optimizar el buen funcionamiento del sistema.

4.6.1.8 Presentación de Conclusiones.

Las conclusiones se presentaran por medio de un informe a los usuarios del sistema los cuales podrán dar opinión de los resultados obtenidos, para unificar criterios y presentarlos en un informe final de manera que ambas partes funcionarios y auditores coincidan con las conclusiones.

El administrador estará en el deber de preparar un plan de acciones correctivas que presentará al auditor en un plazo no superior a 15 días después de haber presentado el informe final. Este plan será puesto en marcha para aplicar dichas correcciones.

Se fijará un plazo para verificar la ejecución de dichas acciones con el objeto de saber si se cumplieron y si se logro el objetivo de mejorar el sistema que se ha manejado por el SIMID, o si por el contrario es mejor seguirlo manejando de forma manual a nivel de la DDRNEC Regional Quindío.

4.6.1.9 Cuestionario de control interno para el procesamiento electrónico de datos.

OBJETIVOS:
Evaluar la funcionalidad del área de sistemas, el tipo de relación con las demás áreas y aporte que brinda la organización en general.

Tabla 287. Lista de chequeo verificar el sistema implantado cumpla con todas las normas legales internas y externas

Área: Dependencias donde este funcionando el SIMID **Actividad:** verificar que el sistema implantado cumpla con todas las normas legales internas y externas	
LISTA DE CHEQUEO	**Si/No/N.A**
Se ha adquirido legalmente todo el Software instalado en los equipos de la Entidad ?	N
Se sigue alguna metodología de adquisición del Software ?	N
Se sigue alguna metodología de adquisición de equipos ?	S
Se ejerce control sobre los programas instalados, además de no permitirse la duplicidad de instalaciones o de archivos ?	N
Se encuentra debidamente licenciada la totalidad del software que usa la Entidad ?	N
Se tienen en cuenta las políticas de la Entidad para controles administrativos que aseguren la confiabilidad en la captura de los datos ?	N
¿El sistema atenta contra alguna de las normas establecidas en la entidad?	N

Tabla 288. Lista de chequeo comprobar los niveles de seguridad del sistema.

Área: Dependencias donde este funcionando el SIMID. **Actividad:** Comprobar los niveles de seguridad del sistema.

LISTA DE CHEQUEO	Si/No/N.A
Se cuenta con un documento oficial que relacione los usuarios de los diferentes sistemas de la Entidad así como el respectivo nivel de atribución dentro de los mismos?	N
Las claves de acceso (*passwords*) al sistema son únicas para cada usuario?	S
Se inhabilitan oportunamente las claves de acceso del personal que se ausenta temporal o definitivamente de sus labores en la Empresa?	S
Son confidenciales y restrictivas las claves de acceso de los usuarios ?	S
Permite el sistema individualizar las operaciones de adición, modificación, consulta, borrado y reporte de información dentro de las opciones del sistema y asignar estas operaciones a usuarios específicos?	S
Permite el sistema restringir el acceso de procesos o acciones específicas del sistema a usuarios no autorizados?	S
Se encuentra implementado el cambio periódico y forzoso de las claves de acceso a todos los usuarios del sistema?	N
Controla el sistema un número determinado de intentos de acceso al sistema?	S
El administrador de seguridad del sistema lleva un control periódico de los usuarios que se ausentan temporal o definitivamente de la Entidad a fin de inhabilitarlos?	N
Se cuenta con procedimientos claros para los casos en que los usuarios olviden su clave de acceso?	N
Cuenta el sistema con un archivo de pistas de auditoría que registre las acciones efectuadas por los usuarios dentro del sistema?	S
Existe sólo un único empleado con privilegios especiales de administración del sistema?	S

Tabla 289. Lista de chequeo revisar los procedimientos que se llevan a cabo dentro de la entidad con el SIMID

Área: Dependencias donde este funcionando el SIMID **Actividad:** revisar los procedimientos que se llevan acabo dentro de la entidad	
LISTA DE CHEQUEO	**Si/No/N.A**
Existe un funcionario autorizado que examine los listados de la consola para detectar problemas del operador o intervenciones no autorizadas en el SIMID?	N
Para el inicio de un proceso en el SIMID, es indispensable una orden de proceso autorizada?	S
Hay restricciones de manejo de computador por cuenta de los operadores para corrida de programas externos?	S
Los operadores envían los listados al área del inventario de la DDRNEC Regional Quindío?	N
Se dispone de controles efectivos para impedir que personal del Centro de Cómputo pueda instalar *software* pirata?	N
Puede el personal que trabaja en el Centro de Cómputo acceder a programas, opciones o información no permitida?	S

Tabla 290. Lista de chequeo revisar seguridad en los archivos electrónicos y base de datos

Área: Dependencias donde este funcionando el SIMID

Actividad: revisar seguridad en los archivos electrónicos y base de datos	
LISTA DE CHEQUEO	**Si/No/N.A**
Existe un manual que describa el contenido y la estructura de los archivos de datos?	N
Se cuenta con un manual que describa los procedimientos para el mantenimiento (depuración, fusión, corte, copia de respaldo) de los archivos de datos que posee el sistema?	S
Dejan los procesos ejecutados evidencias de: ▪ Fecha de ejecución ▪ Nombre y/o número de trabajo ▪ Hora de iniciación y terminación del mismo ▪ Actividades realizadas	S
Permite el sistema a los operadores y/o usuarios en general, manipular los archivos tipo reporte?	S
Es restringido el acceso a este tipo de archivos?	N
Se cuenta con una única persona responsable de llevar a cabo las copias de respaldo?	S
Se cuenta con una política de copias de respaldo dentro de la Empresa?	S

Tabla 291. Lista de chequeo revisar los procesos que se llevan a cabo en la trascripción de datos

Área: Dependencias donde este funcionando el SIMID **Actividad:** revisar los procesos que se llevan a cabo en la

trascripción de datos	
LISTA DE CHEQUEO	**Si/No/N.A**
Cuenta la Entidad con políticas administrativas para asegurar una adecuada atención de los usuarios?	S
Existen manuales que registren el procedimiento para la trascripción de datos?	S
Facilita el sistema la detección de errores durante la captura (p. ej. inclusión de dígito de chequeo en campos claves) ?	S
Se lleva un control que asegure que el trámite pagado corresponde al trámite solicitado?	S
Fue probado el diseño del aplicativo por parte del personal de la Entidad (área de tecnología y usuarios)?	S
Participó el personal de la Entidad en el diseño de los requerimientos funcionales de los programas de captura?	S
Se ajusta dicho diseño a las necesidades de la Entidad?	S
Las adiciones y cambios al diseño del sistema se realizan con la participación o aprobación de personal de la Entidad?	S