ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

Auditoría y Control de Gestión

Diseño e Implementación de un Sistema de Control para realizar Peritajes Informáticos a un Sistema de Información Caso: Una Cooperativa de Ahorro y Crédito

TESIS DE GRADO

Previo a la obtención del título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentado por:

Roxana Elizabeth Díaz Rodríguez

Guayaquil – Ecuador

2008

DEDICATORIA

Dedico este trabajo a mi mamá Eva Rodríguez y hermana Eva Díaz, las personas más importantes en mi vida, quienes vigilan mis pasos y me empujan a seguir adelante; a mi tío Marcos Rodríguez por ser un gran ejemplo a lo largo del camino académico.

A Dios por ser mi apoyo en cualquier situación, por estar incondicionalmente en cada día de mi vida, darme fuerza y cuidarme siempre. Gracias.

AGRADECIMIENTO

A mis amigos y compañeros que siempre estuvieron ahí para apoyarme y tenderme la mano cuando era necesario, a mis profesores de quienes siempre aprendí mucho, a mi Directora de Tesis por su valiosa colaboración y comprensión, a mi familia, y a la Institución por acogerme y formarme. Gracias.

TRIBUNAL DE GRADUACIÓN

Ing. Pablo Álvarez	MAS. Alice Naranjo
PRESIDENTE	DIRECTORA DE TESIS
Econ. Julio Aguirre	Ing. Dalton Noboa
VOCAL	VOCAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

_____

Roxana E. Díaz Rodríguez

RESUMEN

El tema “DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL PARA REALIZAR PERITAJES INFORMÁTICOS A UN SISTEMA DE INFORMACIÓN - CASO: UNA COOPERATIVA DE AHORRO Y CRÉDITO”, consistió en hacer un análisis de los factores claves que intervienen en la realización del peritaje informático a un sistema de software a la medida contratado por una cooperativa, con el fin de establecer controles que garanticen la veracidad, consistencia y completitud en el resultado de la pericia, es decir en el dictamen pericial, de forma que éste sea útil a la empresa que lo solicita.

Se realizó el peritaje informático por el incumplimiento de un contrato de software, el mismo que constituyó la base para identificar las temáticas que se deben considerar, que de no aplicarse los criterios correctos por parte del perito, darían como resultado opiniones sesgadas, sin valor para el cliente.

Se creó un tablero de controles y se estableció los medios para su implementación por parte del cliente, generando en su mayoría la documentación de procedimientos para los procesos relacionados, de tal forma que se mantenga evidencia para futuros peritajes.

ÍNDICE GENERAL

Resumen……VI

Índice general……VII

Índice de figuras e ilustraciones……..XV

Índice de tablas……XVI

Abreviaturas…….....XVII

Introducción…….....1

1. ANTECEDENTES

1.1 Delito informático……..……...….....3

1.2 Peritaje informático……..…….…….....4

2. MARCO TEÓRICO

2.1.Peritaje……...……..……..……7

2.2. Informática……..……..……...7

2.3. Peritaje informático……..……...8

2.3.1. Definiciones……..……...…….....8

2.3.2. Importancia y ámbito de aplicación ……..……10

2.3.3. Áreas de peritación en la empresa……...……....11

2.3.4. Características generales de la peritación 11

2.4. El perito informático……..…….....12

2.4.1. Definiciones……..…….....12

2.4.2. Requisitos……..…….....13

2.4.3. Ámbitos de actuación…….....14

2.4.4. Capacitación……..……..…….....16

2.4.5. Código deontológico – ética……..…….....17

2.4.6. Obligaciones……..……..…….....20

2.4.7. Prohibiciones……..……..…….....23

2.4.8. Responsabilidades……..……..24

2.4.8.1. Responsabilidad civil…….....25

2.4.8.2. Responsabilidad penal……..26

2.4.9. Sanciones ……..……..…….....27

2.4.10. Honorarios……..……..……....27

2.5. Fases de peritación ……..…..……...28

2.5.1. Planificación……..……..…….....28

2.5.2. Recopilación de información……30

2.5.2.1. Prueba pericial informática……..……31

2.5.3. Análisis de datos……..……..……..33

2.5.4. Confección del dictamen pericial ……..……..…36

2.5.5. Discusión del informe……..……..37

2.5.5.1. Ampliación del dictamen……..….39

2.6. Sistema de Control……..…….39

2.6.1. Antecedentes ……..…….....39

2.6.2. Definición……..……..…….....39

2.6.3. Tipos……..……..…….....40

2.6.3.1. Hechos por el hombre……...40

2.6.3.2. Naturales……..…….....40

2.6.3.3. Cuyos componentes están unos hechos por el hombre y los otros son naturales…….....…….……..……....41

2.6.4. Ingeniería en los sistemas de control……..……..41

3. MARCO NORMATIVO Y/O ESTÁNDARES INTERNACIONALES

3.1 COSO…….....42

3.1.1. Antecedentes……..……...……....42

3.1.2. Definición……..……..……...…....42

3.1.3. Componentes……..……..……...…....43

3.1.3.1. Ambiente de control…..……..……..……..……..…44

3.1.3.2. Evaluación de riesgos……....…….....45

3.1.3.3. Actividades de control……..……...45

3.1.3.4. Información y comunicación……..……..46

3.1.3.5. Supervisión……....…….....47

3.1.3.5.1. Modalidades de supervisión…..……..……..……...48

3.1.3.5.1.1. Actividades continuas……....…48

3.1.3.5.1.2. Evaluaciones puntuales …..……..……..……..……...…48

3.2 COBIT…..……..……..……..……..……..……..……..……49

3.2.1. Generalidades……..……..49

3.2.2. Dominios de COBIT……....50

3.2.3. Procesos y Objetivos de Control aplicables……..……..50

3.3 IEEE 730…..……..……..……..……..……..……..……....55

3.3.1. Antecedentes……..……..……55

3.3.2. Definición…….…….…….....….56

3.3.3. Recomendaciones más aplicables……..…56

3.4. ISO 9000-3…..……..……..……..……..……..…….....57

3.4.1. Generalidades……..……..…….....57

3.4.2. Cláusulas……..……..……..……....58

3.4.3. Descripción de cláusulas aplicables ……60

3.5. ISO 17799…..……..……..……..……..……..……..…….....70

3.5.1. Generalidades……..……...……70

3.5.2. Estructura……..……..……..……71

3.5.3. Descripción de los objetivos de control que guardan mayor relación.....72

3.5.3.1. Aspectos organizativos para la seguridad……..…72

3.5.3.1.1. Identificación de riesgos del acceso de terceras partes……..…73

3.5.3.1.1.1. Tipos de acceso……..……..……..…73

3.5.3.1.1.2. Razones para el acceso……...……..…….73

3.5.3.1.1.3. Contratistas in situ……..……74

3.5.3.1.2. Requerimiento de seguridad en contratos con terceros……..…75

3.5.3.2. Seguridad del personal….....…….……78

3.5.3.2.1. Comunicación de anomalías del software.....78

3.5.3.3. Seguridad física y ambiental……..……79

3.5.3.3.1. Controles de acceso físico……..……...…79

3.5.3.4. Gestión de comunicaciones y operaciones……..…80

3.5.3.4.1. Aprobación del sistema……...……80

3.5.3.5. Desarrollo y mantenimiento de sistemas…….……..81

3.5.3.5.1. Desarrollo externo de software…….82

3.6. NEA No. 11…..……..……..……..……..……..……..……82

3.6.1. Habilidad y competencia…….……..……83

3.6.2. Planificación……..…….....……....83

3.6.3. Evaluación del riesgo……..…….....……84

3.6.4. Procedimientos de auditoría ……...……85

4. DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL PARA REALIZAR PERITAJES INFORMÁTICOS A UN SISTEMA DE INFORMACIÓN ADQUIRIDO POR UNA COOPERATIVA DE AHORRO Y CRÉDITO: ASPECTOS PREVIOS

4.1. Información preliminar…….……86

4.1.1. Introducción…….....86

4.1.2. Objetivo General…….....87

4.1.3. Objetivos Específicos…….....88

4.1.4. Alcance…….....…..….....89

4.1.4.1. Realizar el peritaje informático…….....89

4.1.4.2. Diseñar el sistema de control…….....89

4.1.4.3. Aplicar el sistema de control al peritaje realizado…..……..……89

4.2. Estrategias - Metodología…….....90

4.2.1. Metodología para realizar el peritaje informático ……..……....90

4.2.1.1. Planificación…….....…….…….....90

4.2.1.2. Ejecución……...…..…….….....91

4.2.1.3. Dictamen……..……..……..……..……..……..……..…..91

4.2.2. Metodología para diseñar e implementar el sistema de control ……..91

4.2.2.1. Identificar las diferentes temáticas que consideran a lo largo del peritaje…….....92

4.2.2.2. Identificar los puntos de evaluación bajo cada temática…….92

4.2.2.3. Asignar a cada punto, el o los documentos que sirvan para verificar su cumplimiento…….....93

4.2.2.4. Proponer los controles a implementar por cada punto …….....93

4.2.2.5. Establecer metodología de evaluación por temáticas. …….. 94

4.2.2.5.1. Aplicación de lista de chequeo de cumplimiento.....94

4.2.2.5.2. Identificación de porcentaje de eficiencia……..…….94

4.2.2.5.3. Interpretación de resultados…….....95

4.2.2.6. Verificar implementación de controles.....96

5. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CONTROL PARA REALIZAR PERITAJES INFORMÁTICOS A UN SISTEMA DE INFORMACIÓN ADQUIRIDO POR UNA COOPERATIVA DE AHORRO Y CRÉDITO: DESARROLLO

5.1. Peritaje Informático…..……..……..……..……..……..……97

5.1.1. Planeación…….…….....…..…….….....97

5.1.1.1. Identificar el motivo del peritaje……..…….....97

5.1.1.2. Realizar una visita preliminar al área…….…….....97
5.1.1.3. Establecer los objetivos…….…….....98
5.1.1.4. Determinar los puntos que serán evaluados.....99
5.1.1.5. Elaborar programas de trabajo …….…….....99
5.1.1.6. Identificar y seleccionar las herramientas, instrumentos y procedimientos necesarios…….…….....99
5.1.1.7. Asignar el valor de los honorarios a percibir…..…….…….....100
5.1.2. Ejecución…….…….....…..…….……..100
5.1.2.1. Realizar las acciones programadas…….…….....100
5.1.2.2. Aplicar las técnicas y herramientas…….…….....100
5.1.2.3. Identificar y elaborar los documentos de las desviaciones encontradas…….…….....101
5.1.2.4. Integrar el legajo de los papeles de trabajo…..…….……..…102
5.1.3. Dictamen…….…….....102
5.1.3.1. Establecer situaciones detectadas…….....102
5.1.3.1.1. Sobre el cumplimiento de plazos y su razonabilidad 102
5.1.3.1.2. Razonabilidad del precio y pagos…….…….....103
5.1.3.1.3. Sobre las condiciones técnicas estipuladas y calidades…..……104
5.1.3.2. Elaborar el dictamen final……..…….....105
5.2. Diseño e implementación del sistema de control…..…….……108
5.2.1. Identificar las diferentes temáticas que se consideran a lo largo del peritaje…..……..……..……..……..……..……..…….108
5.2.1.1. Temáticas según el caso de pericia…..……..……..……....108

5.2.1.2. Temáticas inherentes a cualquier peritaje.....108

5.2.2. Identificar los puntos de evaluación bajo cada temática.....109

5.2.2.1. Capacidad del Proveedor …….…….....109

5.2.2.2. Contratante……..……...…..…….....109

5.2.2.3. Consistencia del contrato…….....109

5.2.2.4. Idoneidad del perito…….….....110

5.2.2.5. Oportunidad en los tiempos de respuesta…….....110

5.2.2.6. Evidencia suficiente y consistente …….….....110

5.2.3. Asignar a cada punto, el o los documentos que sirvan para verificar su cumplimiento……..…….....110

5.2.4. Proponer los controles a implementar por cada punto……. …...110

5.2.5. Establecer metodología de evaluación por temáticas..……111

5.2.5.1. Aplicación de lista de chequeo de cumplimiento……...111

5.2.5.2. Identificación de porcentaje de eficiencia…..…….….....111

5.2.5.3. Interpretación de resultados……..……..…….....112

5.2.6. Verificar implementación de controles. ……..…….....112

CONCLUSIONES

RECOMENDACIONES

GLOSARIO

BIBLIOGRAFÍA

ANEXOS

ÍNDICE DE FIGURAS E ILUSTRACIONES

Pág.

3.1. Pirámide de componentes COSO……..…44

3.2. Logo de IEEE……...55

3.3. Logo de la ISO.....57

3.4. Dominios de control ISO 17799……..……72

5.1. Porcentaje de eficiencia de peritaje…….....111

ÍNDICE DE TABLAS

Pág.

3.1. Índice de cláusulas de la ISO 9000- 3……58

4.1. Nivel de rendimiento de puntos de evaluación……..…….....95

ABREVIATURAS

COBIT.- The Control Objectives for Information and related Technology

Corp.- Corporation

ID.- Identificación

ISO.- Organización de Estándares Internacionales

Ej.- Ejemplo

NEA.- Norma(s) Ecuatoriana(s) de Auditoría

PIN.- Número de identificación personal

TI.- Tecnología de Información

SIC.- Sistemas de Información Computarizada

SQA.- Software Quality Assurance

INTRODUCCIÓN

Todos los inventos producidos por el ingenio a lo largo de la historia de la humanidad, han producido importantes beneficios a la ciencia, a la cultura, a la calidad de vida de la civilización. En este caso, debido a que los sistemas de información adquieren un papel cada vez más relevante en nuestra actividad diaria, los conflictos y diferencias que por su causa se originan, son más comunes.

Los robos de información, fraude, manipulación y abusos de los correos electrónicos, ataques a web, accesos no autorizados, incumplimientos de contratos, etc…, son algunas de las muestras de los peligros que acechan a las organizaciones; por tanto, la opinión de un perito independiente, que aclare la realidad de los hechos, es en muchos casos necesaria.

Debido a la importancia de la suficiencia y transparencia del dictamen pericial, este trabajo muestra un sistema de control que permite garantizar resultados veraces del peritaje realizado sobre un sistema de información.

En el primer capítulo se describen los antecedentes, es decir producto de qué nace el peritaje informático; se enfocan el delito y el peritaje informático, uno como consecuencia del otro.

En la segunda parte se presenta el marco teórico detallado sobre todos los aspectos inherentes al peritaje principalmente, y se trata también sobre el significado de los sistemas de control.

En el tercer capítulo se cita toda la normativa nacional e internacional que guarda estrecha relación con el desarrollo de sistemas, la relación con terceras partes y el incumplimiento de contratos de software.

En la cuarta parte se inicia el caso práctico dando las generalidades de lo que se va a realizar, así como las metodologías a aplicar.

En la quinta sección se lleva a cabo el diseño e implantación del sistema de control, determinando la matriz de aspectos con sus respectivos controles.

Finalmente se presentan las conclusiones y recomendaciones.

CAPÍTULO 1

1. ANTECEDENTES

1.1. Delito informático

Para definir el delito informático, comenzaré haciendo referencia a la definición etimológica de la palabra delito.

Delito deriva del verbo latino “delinquere”, que significa abandonar, apartarse del buen camino, alejarse del sendero señalado por la ley.

La definición precedente nos lleva a pensar que desde su origen, la palabra delito era utilizada para referirse a un comportamiento no deseado por la sociedad, alejado de las pautas de conductas idóneas. La historia registra que desde la antigua Roma se distinguía entre delitos públicos (crimina) y delitos privados (delicta). Los primeros ponían en peligro a toda la comunidad y eran perseguidos por las autoridades por oficio o a petición de cualquier ciudadano, estos delitos eran sancionados con penas públicas como decapitación o ahorcamiento; los segundos, causaban daño a un particular y solo indirectamente provocaban una perturbación social, se perseguían a iniciativa de la víctima y daban lugar a una multa privada a favor de ella.

En la ciencia del Derecho, la palabra delito ha sido definida por varios autores; la acción antijurídica, típica, culpable y sancionada con una pena, es una de las definiciones más completas. Así también, la acción u omisión que castigan las leyes penales, es concebida como delito.

Con este preámbulo, definimos al Delito Informático como cualquier acto ilegal intencional llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software; en los cuales la víctima ha o habría podido sufrir una pérdida, y cuyo autor ha o habría podido obtener un beneficio, siendo esencial el conocimiento de la tecnología informática para su comisión, investigación y persecución.

1.2. Peritaje informático

El cambio de generaciones está principalmente señalado por los cambios de tecnología electrónica, aún cuando las modificaciones en las técnicas de almacenamiento y recuperación de la información también marcan un hito en las divisiones generacionales, pero tomadas desde el punto de vista de los bienes tangibles.

Con la existencia de delitos automáticamente nace una actividad de investigación, descubrimiento, análisis y establecimiento de responsables, búsqueda de correcciones, cuyo nombre se condensa en peritaje informático.

Por los años noventa cuando comenzaron a surgir los primeros casos delictivos dentro de la informática, la necesidad de buscar responsables, crear medios para que no se vuelvan repetir, hizo que los conocedores de la materia se concentraran en contrarrestar los ataques que sufrían, y a la vez crear planes de contingencia en caso de situaciones que podrían ocurrir.

Como resultado nació la auditoría informática, una ciencia que se encarga de la detección, reporte y seguimiento de circunstancias de carácter dudoso, delictivo, que pudieran ocasionar daños futuros en caso de no ser controladas oportunamente. Así mismo, con el ánimo de llevar a la ley los hallazgos y castigar a los responsables directos o indirectos de los hechos delictivos, aparece el peritaje informático, como apoyo para un juez en su labor de dirimir las causas referentes a la informática.

El peritaje informático se encuentra bien desarrollado en los países de tecnología avanzada, donde las amenazas diarias representan altos riesgos en cualquiera de las áreas donde se produzcan, y por consecuencia grandes pérdidas materiales.

En ciertos países tercermundistas el peritaje informático llega a partir del año 1998, mientras que en otros como el Ecuador, lo que se practica es la auditoría informática con orientaciones al peritaje informático por el tipo de

investigaciones que se realizan, mas no porque el resultado de la investigación pueda ser usado en los juzgados de nuestro país, debido a la inexistencia de una legislación completa aplicable, pese a que se encuentra en vigencia la Ley de Comercio Electrónico, Firmas, Mensajes de Datos que podría emplearse, aunque su principal objetivo es proteger a los usuarios de Internet de los delitos comunes en la web.

CAPÍTULO 2

2. MARCO TEÓRICO

2.1. Peritaje

Peritaje proviene de la palabra pericia, la misma que nace del latín “peritia” y significa sabiduría, práctica, experiencia y habilidad en una ciencia o arte.

El peritaje es el conjunto de exámenes y estudios que realiza el perito sobre el problema encomendado, para luego entregar su informe o dictamen pericial con sujeción a lo dispuesto por la ley. También es llamado peritación.

Un peritaje puede ser ejecutado en cualquier área de estudio; es decir la palabra peritaje no sólo está destinada al uso informático, sino que puede aplicarse a cualquier otra materia específica; por ejemplo en la valoración de activos dentro del área financiera, en la valoración legal de víctimas para la medicina forense, en la reconstrucción de accidentes de tráfico, en la ingeniería en minas, entre otras.

2.2. Informática

La palabra informática proviene del francés “informatique”, que a su vez es la contracción de “information” y “automatique”; es el conjunto de conocimientos

científicos y técnicos que hacen posible el tratamiento automatizado de la información a través de dispositivos de proceso electrónico.

La misión de la informática es el procesamiento de la información con el fin de sintetizarla, combinarla y ordenarla según las necesidades del usuario.

En la sociedad actual, la Informática es una de las herramientas más importantes e imprescindibles, por lo que es necesario mantener un control sobre sus diferentes aplicaciones a fin de garantizar la integridad en el manejo de la información.

2.3. Peritaje informático

2.3.1. Definiciones

La pericia informática es el estudio de las dos facetas del equipamiento informático, lo material o tangible (hardware) y lo inmaterial (software); consiste en la aplicación de técnicas de investigación y análisis profundo a fin de determinar la existencia de evidencia legal almacenada en sistemas de computación, medios informáticos o responder consultas específicas en materia informática.

Entre los tipos de incidentes que podemos citar para la pericia tenemos: los relacionados con soportes informáticos, el uso fraudulento de equipos, la piratería informática, las pérdidas provocadas por empleados

desconsiderados, los daños fortuitos, la ocultación de documentos, el incumplimiento de contratos de software, entre otros.

Por ejemplo, en un caso específico el peritaje tiene por objeto certificar y dar fe del contenido o de la ausencia de contenido de un disco, y precisar la naturaleza y motivo de la pérdida de información.

Para iniciar la pericia es necesario determinar las necesidades del cliente; finalizado el proceso para recuperar los datos, se reconstruye el historial del soporte magnético dañado, estableciendo el carácter doloso o fortuito de la pérdida de datos, y registrando las alteraciones que haya sufrido el contenido originalmente gravado y las modificaciones de datos previos al fallo del sistema.

El proceso finaliza con el dictamen del perito, que responde a los puntos de pericia solicitados por el juez en un determinado caso.

En la dimensión del Derecho, el peritaje informático tiene el fin de presentar bajo juramento al juzgador, pruebas y puntos litigiosos en cuanto se relacionan con su especial saber o experiencia.

Como conclusión podemos decir que el peritaje informático es el trabajo sobre una materia concreta de la informática que realiza un experto o perito en dicha materia con el fin de emitir un informe.

2.3.2. Importancia y ámbito de aplicación

La importancia radica en que el peritaje informático constituye un verdadero medio de prueba, tanto para las partes interesadas en asuntos judiciales como en los extrajudiciales.

Así vemos que en la vía legal para resolver un determinado asunto, el juez necesita que le aporten conocimientos de tipo científico y técnico que faciliten el discernimiento de los sucesos, y que creen convicción de determinados hechos. La pericia tiene una función integradora para que el juez tenga el conocimiento completo; procede entonces esta clase de diligencia para verificar hechos que interesen al proceso y requieran especiales conocimientos.

En las pericias informáticas, hay que tener en cuenta, que no siempre se relacionan con delitos informáticos exclusivamente, es decir, no siempre que la informática forma parte de un asunto judicial es con motivo de un delito.

La informática puede verse implicada, por ejemplo:

- Cuando es utilizada como medio de un delito.

- Cuando la informática es el objeto propio del delito (ej. compra de software ilegal).
- Cuando tiene lugar en el conflicto de forma colateral, pero en ocasiones, determinante.
- Los **incumplimientos de contratos** de programación y desarrollo.

2.3.3. Áreas de peritación en la empresa

Son muchas las áreas y puntos a considerar en una peritación informática, pueden ser agrupadas en los siguientes dominios:

- Peritación de área física y entorno
- Peritación de desarrollo y explotación
- Peritación de Bases de datos
- Peritación de comunicaciones
- Peritación Técnica de Sistemas
- Informática laboral
- Peritación de e-mails

2.3.4. Características generales de la peritación

- La pericia es el resultado de una actividad humana, ya que son los peritos quines constatan, observan, verifican para luego emitir un dictamen.
- El dictamen debe versar sobre hechos. No puede versar sobre cuestiones jurídicas.

- Debe tenerse un encargo judicial, cuando se despliega la actividad indicada, para que se pueda hablar de perito. Se requiere nombramiento y posesión para que surja la predisposición en emplear los conocimientos que se tienen.
- La naturaleza del hecho crea la necesidad, es decir la pericia.
- Es una declaración de ciencias, es un concepto, el perito expone lo que sabe para que el juez se informe y a su vez tenga un medio probatorio a su disposición para su valoración.

2.4. El perito informático

2.4.1. Definiciones

La palabra perito posee varias definiciones según su ámbito de aplicación:

Definido en la Real Academia de la Lengua como la persona que poseyendo especiales conocimientos teóricos o prácticos informa, bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relaciona con su espacial saber o experiencia.

Definido en el diccionario jurídico como la persona que posee un título; especialista en algo determinado que informa en un procedimiento, bajo juramento sobre cuestiones litigiosas relacionadas con su especialidad o experiencia.

2.4.2. Requisitos

Un perito informático debe ser un profesional del peritaje informático, no un experto en una sola área de la informática. Esto significa, un informático preparado, idóneo en varias disciplinas, y sobre todo eficaz "perito en la materia".

Se requiere ser conocedor de la materia en cuestión y saber demostrarlo. El saber demostrarlo es fundamental en un peritaje informático, porque aunque de entrada se le supone la valía profesional al perito, éste debe tener la preparación para fundamentar convenientemente las conclusiones de su estudio, y para observar lo que interese en la producción del dictamen. Para ello es necesario usar en lo posible métodos científicos contrastados y no dejarse arrastrar por la subjetividad.

Además debe poseer las siguientes características:

- Persona idónea: que tiene buena disposición o suficiencia para una cosa.
- Conducta intachable.
- Excelente reputación.
- Incuestionable imparcialidad.
- Versación: Hacerse práctico o perito por el ejercicio de una cosa, en su manejo o inteligencia.

- Título profesional legal en la ciencia o actividad técnica especializada a que pertenezcan las cuestiones acerca de las cuales deba tratar. Cuando no hubiera un perito con título habilitante se podrá nombrar a cualquier persona con conocimientos en la materia para que haga sus veces.

2.4.3. Ámbitos de actuación

Los ámbitos en que se desarrolla la actividad de un perito informático están en función del dominio en que se mueve la informática; lo que debido a las nuevas tecnologías, incluye prácticamente todo el manejo mercantil, comercial y financiero.

A continuación se exponen casos que en principio la actuación de un perito informático parece no propicia, pero más adelante resulta necesaria:

- Verificar si hay vicios ocultos y es necesario sanearlos, lo que puede estar ligado a un contrato de software a la medida.
- Las aportaciones no dinerarias a una sociedad pueden consistir en programas de ordenador u ordenadores, y ser necesaria su tasación por un perito informático.
- Se considera difícil que una persona que no sea auditor informático pueda realizar un examen de contabilidad de una empresa, cuando en la mayoría de los casos esta forma parte de un sistema de información.

Un perito informático puede actuar básicamente por dos vías: Judicial y Extrajudicial.

- Vía Judicial.- Funciona como elemento auxiliar del Juez, aclarando puntos y conceptos necesarios para que éste pueda dictar las resoluciones judiciales. Produciendo así un dictamen pericial o asesoría; suministra al juez “argumentos o razones para la formación del convencimiento”.
- Vía Extrajudicial.- Funciona como medio de prueba para acreditar o perfeccionar las pretensiones formuladas por las partes a través de su peritaje informático, no es manejada por la vía legal.

En cualquiera de los campos, un perito tiene como objetivo el estudio de las alternativas utilizadas para llegar a un determinado resultado; no sólo se limita a solucionar problemas operativos, sino que persigue explicar la causa y el porqué de esos problemas, luego de un profundo estudio de los recursos humanos y tecnológicos utilizados por esa consecuencia.

En varios países, en los que la actividad de peritaje informático se encuentra legislada, las constantes solicitudes de pericias dirigidas hacia la Función Judicial, han originado la integración de grupos de apoyo técnico informático. Debido a que en los últimos años la cantidad de litigios ha aumentado progresivamente, apareció la necesidad de incorporar pericias informáticas,

siendo razonable contar con funcionarios dotados de la capacidad técnica para resolver los requerimientos en esta materia. Cabe recalcar la opinión favorable de los diferentes Juzgados hacia la integración de nuevos profesionales, implicación que se puede reflejar en la creación de un Cuerpo de Peritos Oficiales en Sistemas Informáticos a futuro.

Esperemos que el peritaje informático en el país se desarrolle rápidamente para poder dar solución a muchos problemas para los que todavía existen vacíos legales, y al mismo tiempo establecer un nuevo enfoque laboral para los profesionales en la ciencia informática, imitando las acciones de países más avanzados en esta área.

2.4.4. Capacitación

Existen ciertas capacidades que debe adquirir un perito informático para realizar un análisis de datos sobre medios informáticos. Para ello se requiere una capacitación específica en el uso de técnicas y herramientas informáticas utilizadas para pericias informáticas.

En el país no se ha desarrollado todavía el peritaje informático, por lo tanto no existen cursos en esta materia; sin embargo citamos algunas de las organizaciones o centros de capacitación en el exterior que brindan programas de entrenamiento o cursos de especialización en este campo.

a)Organizaciones que proveen certificaciones de especialización en pericias informáticas:

- The International Association of Computer Investigative Specialists (IACIS)
- High-Tech Crime Network (HTCN)

b)Empresas que proveen entrenamiento para pericias informáticas con alguna herramienta informática específica:

- Key Computes Services Inc.
- New Technologies Inc.
- CyberEvidence Inc.
- Guidance Software Inc.
- AccessData Corp.

A partir de la capacitación específica, y de acuerdo a las características de las herramientas que se utilicen, se puede aplicar el estándar definido para los puntos de pericias informáticas y establecer otros más específicos.

2.4.5. Código deontológico – ética

El código deontológico define básicamente los deberes éticos que un profesional ha de cumplir durante el desarrollo de sus funciones en el peritaje informático. Esto es de suma importancia porque está en juego el honor profesional del perito.

Ética del perito

El perito siempre supeditará el saber y el poder a la ética y a la moral. Se considerarán violaciones a la ética particular del perito las siguientes acciones:

- Abandonar o descuidar inexcusablemente las diligencias periciales.
- Ejercer abusivamente las facultades conferidas para la labor pericial, durante procedimientos o tareas periciales. No favorecer la solución amigable del litigio, cuando sea posible evitar daños para las partes.
- Demorar injustificadamente la entrega de documentación que le hubiera sido confiada al sólo efecto de la tarea pericial.
- Expresarse con términos ofensivos a la dignidad de las personas que participen en el procedimiento o en la causa.
- Procurarse consultorías técnicas por medios incompatibles con la dignidad profesional.
- Informar falsa o maliciosamente sobre el estado de avance de la labor pericial encomendada.
- Aceptar la consultoría técnica de una parte, luego de haber dado consejos a la otra.
- Incluir en sus dictámenes citas tendenciosamente incompletas o falsas.
- Ofrecer soluciones a través de la consultoría técnica contrarias a las leyes o que violen las mismas.

- Comisionar a personas para la búsqueda de clientes a cambio de dinero.
- Aceptar tareas que contraríen las leyes o disposiciones vigentes o que puedan significar malicia o dolo.
- Asociar el propio nombre a personas o entidades que aparezcan indebidamente como profesionales.
- Hacer uso de medios de propaganda en los que la jactancia constituya la característica predominante. Tales medios deberán siempre ajustarse a las reglas de la prudencia y el decoro profesional.
- Utilizar ideas, documentos técnicos u otros elementos propios de la profesión, sin el consentimiento de sus autores o licenciatarios legítimos, para su aplicación en trabajos profesionales propios.
- Señalar, sin utilizar la vía técnica o científica, presuntos errores profesionales de otros peritos, sin darles antes oportunidad de reconocerlos o rectificarse.
- Menospreciar a colegas que ocupen cargos subalternos al propio.
- Revelar datos reservados de carácter técnico, financiero o personal sobre los intereses confiados a su estudio o custodia.
- No dedicar su mejor actitud para entender con diligencia y probidad los asuntos de su cliente, como consultor técnico. Toda otra acción o actuación pública o privada que, no encuadrada en las apuntadas anteriormente, comprometa el honor y la dignidad de la profesión.

2.4.6. Obligaciones

Todo perito informático está obligado a cumplir con los siguientes lineamientos:

- Respetar y hacer respetar las disposiciones legales que incidan en actos de la profesión, como también velar por su prestigio.
- Realizar personalmente las diligencias que en su caso sean necesarias para la emisión del dictamen correspondiente, acudiendo al lugar donde se encuentren los objetos a periciar.
- Presentar el dictamen por escrito, acompañado en su caso de los documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de la pericia. Si no fuese posible o conveniente aportar estos materiales e instrumentos, el escrito del dictamen contendrá sobre ellos las indicaciones suficientes. Podrán, asimismo, acompañarse al dictamen los documentos que se estimen adecuados para su más acertada valoración.
- Emitir dictámenes apegados estrictamente al conocimiento de la profesión y con rigor científico, sin limitar a la experiencia individual su valoración si observa necesaria una ampliación de conceptos, solicitando en estos casos el aporte de colegas u organizaciones.
- Guardar reserva de todos sus actos relacionados con las labores periciales practicadas sin excepciones.

- Ser discreto evitando relatos u otras manifestaciones que signifiquen adelantar las conclusiones antes de presentar su trabajo.
- Ser absolutamente imparcial en su función de perito de oficio o como parte de un tribunal arbitral.
- En todas las actuaciones, el perito empleará el idioma castellano. Cuando se produzcan declaraciones o se aporten documentos en otros idiomas, se recogerán en el expediente y se hará la correspondiente interpretación o traducción al castellano, que constará en el acta que se levante con motivo de la diligencia.
- Si entre los entrevistados en el relevamiento de información durante la labor pericial, hay quienes no conozcan suficientemente el idioma castellano, común entre especialistas extranjeros en la profesión, así como a quien se encuentre afectado de alguno de los sentidos y no pueda, por esta causa, escuchar o entender lo que se dice y manifestar de viva voz su declaración, se les designará intérprete o traductor que le asista a fin de lograr una pericia clara y sin fallidos por malas interpretaciones, el perito velará porque así sea.
- Se debe destacar que la falta de intérprete o traductor puede ocasionar la nulidad del acto pericial, independientemente de que los participantes hubiesen otorgado su conformidad para actuar sin la asistencia de aquellos.
- Actualizar permanentemente sus conocimientos a fin de ofrecer un servicio profesional de calidad, a la altura del avance de los recursos

informáticos y a la constante incorporación de nuevos medios que pueden aparejar cuestiones dirimibles judicialmente.

- Determinar éticamente su idoneidad para el desempeño de la labor pericial encomendada, por lo que se apartará de la causa si lo estima prudente, al no sentirse predispuesto para encarar la labor pericial con el nivel ideal.
- Justificar su negativa a efectuar un dictamen encomendado.
- Emitir el dictamen en el plazo que sea fijado por el juez y en caso de considerar que el plazo es insuficiente para elaborar la pericia solicitada, podrán pedir al juez de la causa, una prorroga, quien de acuerdo a su prudente arbitrio tomando en cuenta la facultad del peritaje y conforme a lo recomendado por los Códigos concederá el plazo que considere pertinente, el que respetará el perito sin excepciones.
- Cuando no se fije plazo ni término para las diligencias, se entenderá que ha de practicarlas sin dilación.
- Emitir el dictamen agotando los puntos propuestos y efectuar las observaciones que estimen pertinentes para el conocimiento de la verdad.
- Prestar su asistencia profesional como auxiliar del juez y en servicio de la justicia.
- Ejercer la asistencia pericial a personas carentes de recursos, en los casos en que la ley o disposiciones actuales o futuras lo determinaren.

- Aceptar los nombramientos que le hicieran los jueces y Tribunales con arreglo a la Ley, pudiendo excusarse solamente con justa causa.
- Dar estricto cumplimiento a las normas de ética generales y particulares del perito, deberes de la profesión y a las disposiciones legales vigentes.
- Denunciar las ofensas, restricciones o trabas de que fuere objeto por parte de los magistrados, funcionarios y empleados judiciales o de cualquier autoridad, en el ejercicio de sus funciones.
- Comunicar al perito consultor anterior su designación como tal, si fuese designado luego de una participación previa de algún colega.
- Acudir al juzgado cuantas veces sea requerido por el juez.
- Conservar y exhibir recibo de honorarios con los requisitos fiscales correspondientes una vez que le sean cubiertos.
- Obrar en un legajo personal, en poder del perito, antecedentes básicos de toda intervención pericial de los últimos cinco años, aún en las que actuare como perito consultor, para cualquier ulterior tratamiento que emanare, producto de la actuación pericial en el proceso.

2.4.7. Prohibiciones

Existen casos en que el perito no puede actuar como tal, debido a que la exposición de sus apreciaciones se puede ver afectada por el vínculo con determinado grupo de personas, por lo que para un perito es prohibido:

- Intervenir como profesional en asuntos propios, del cónyuge, parientes consanguíneos o en línea directa sin límite de grado, de alguna de las partes, sus apoderados, abogados u autorizados.
- Intervenir al ser dependiente, socio, arrendatario o tener negocios de cualquier clase, con las personas que se indican en el punto anterior.
- Actuar como perito al tener interés directo o indirecto en el pleito, juicio o participación en la sociedad o empresa con alguna de las personas que se indican en el primer punto.
- Actuar como tal al tener amistad íntima o enemistad manifiesta con alguna de las partes, sus representantes, abogados o con cualquier persona de relación familiar cercana a aquellos.
- Además de las anteriores, es prohibido intervenir como perito informático, en los asuntos que no sean propios según su especialidad dentro de la informática en la que ha desarrollado su experiencia, salvo que posea título referente a la rama aludida.
- Finalmente, en base a sus competencias, y al exclusivo cumplimiento de su encargo, los peritos tienen prohibición absoluta de emitir en el dictamen cualquier juicio de responsabilidad penal.

Todas estas prohibiciones garantizarán la independencia del perito en la revisión o juicio que estuviere atendiendo, lo que reflejará la veracidad y consistencia en todos sus pronunciamientos.

2.4.8. Responsabilidades

Los peritos en el desempeño de su labor como auxiliares de la justicia, están sujetos a responsabilidades de tipo civil y penal, que pueden resultar de su modo de actuar durante las diligencias.

2.4.8.1. Responsabilidad civil

Los peritos responderán civilmente por los daños y perjuicios que infrinjan a las partes litigantes. La demora injustificada en la presentación de un dictamen, o cualquier otro tipo de conducta en contra del derecho, es causa de culpa. Esto se ve respaldado en principios contractuales (cuando el perito es designado por una de las partes) o extracontractuales (cuando el perito es designado por el juez o respecto a la parte distinta de quien lo designó) y por lo tanto no hace falta norma legal que la consagre para hacerla efectiva judicialmente.

Cuando se trate de una pericia a cargo de varios peritos en forma conjunta, se protege al resto de la negligencia de uno, sin hacerlos solidarios con la misma; ya que cada uno debe terminar en tiempo y forma su cometido, determinándose claramente el origen de la negligencia en cuestión.

En países como Argentina, cuando un perito es reemplazado por presentar su renuncia después de haber aceptado el cargo, o por mora injustificada en cumplirlo, la ley le impone la obligación de pagar los gastos y los perjuicios.

Cabe tener en cuenta, que el perito está obligado a dar las explicaciones que le requieran las partes, siempre a instancias del juez y respetando los procedimientos judiciales; la negativa a hacerlo, conlleva una violación de sus deberes profesionales, haciéndose responsable de los daños que su conducta pueda ocasionar.

2.4.8.2. Responsabilidad penal

Dentro de las responsabilidades penales sobresale el dolo, el que se origina intencionalmente en el momento que el perito:

- Asevera o refuta falsamente hechos o circunstancias.
- Encubre hechos o circunstancias que harían modificar su dictamen.
- Afirma haber constatado ciertos experimentos sin que sea verdad.
- Sustenta una conclusión sin poseer la certeza de ella.
- Brinda un concepto contrario a la realidad, por interés económico o particular, o estimulado por la amistad o enemistad.

En algunos países, ya se sanciona al perito penalmente cuando recurre a excusas fraudulentas para no asumir el cargo o se niega ilegítimamente a ejercer sus funciones, ya sea por invocar falsa incapacidad o incompatibilidad; además son sancionados en casos más graves como la violación del secreto cuando perjudica la investigación.

2.4.9. Sanciones

Dentro de las organizaciones, comisiones, tribunales y demás entidades que delinean y regulan el comportamiento de los peritos en los diferentes países, generalmente se administran las siguientes sanciones:

- Llamado de atención por escrito.
- Multas que oscilan entre veinte y doscientas horas según el arancel máximo por hora fijado.
- Suspensión temporal del registro, la cual que podrá ser de uno a seis meses.
- Cancelación del registro.

La cancelación del registro, sólo podrá darse por las siguientes causas:

- Haber emitido con dolo o mala fe dictámenes que contengan datos o apreciaciones falsas.
- Haber obtenido la inscripción proporcionando datos o documentos falsos.
- Revelar dolosamente o sin causa justificada datos del peritaje.
- Actuar con parcialidad en la elaboración del dictamen.
- Negarse a prestar servicios reiteradamente sin causa justificada.
- Elaborar dictámenes estando inhabilitado por decisión judicial.
- Cuando se comprobase que no diligenció personalmente la prueba pericial.

2.4.10. Honorarios

El peritaje informático implica la percepción de honorarios por parte del perito, los que están en función de varias variables:

- El tipo de actividad a realizar, consulta específica o análisis de datos.
- La magnitud y profundidad del trabajo en cuestión.
- Los recursos humanos y materiales que puedan requerirse.

2.5. Fases de peritación

2.5.1. Planificación

La primera tarea es definir con el cliente qué es lo quiere averiguar y el ámbito que abarcará. Ya en esta primera fase está presente la ética profesional del perito, pues no ha de proseguir si estima que no va a ser capaz de resolver lo que le piden por no ser experto en esa materia concreta.

Se denomina puntos de pericia a cada una de las interrogantes que el interesado quiere resolver. Los puntos de pericia pueden ser de tipo análisis de datos como consultas específicas.

Dentro de los puntos de pericia sobre análisis de datos se pueden suscitar:

- Localización de archivos mediante palabras claves especificadas por el juez.
- Localización de archivos mediante palabras claves extraídas de documentos.
- Localización de imágenes especificadas por el juez.

- Localización de imágenes extraídas de documentos.
- Identificación de fechas de creación, acceso o modificación de archivos y documentos.
- Identificación de fechas de creación, recepción o envío de e-mails.
- Identificación de entradas y salidas de usuario sobre un sistema informático.
- Identificación de accesos a páginas o sitios web.

Como consultas específicas nos pueden requerir:

- Especificar el tipo de equipamiento que se necesita para ejecutar un sistema y su respectiva copia, el costo de la operación.
- Especificar la capacidad de un dispositivo de almacenamiento.
- Especificar los tipos de dispositivos de almacenamiento utilizados por un sistema informático.
- Si es característica exclusiva de un sistema permitir la consulta alfabética de datos.
- Distinciones entre sistemas en cuanto al diseño de pantalla.
- Determinar similitudes o diferencias entre listados de los programas fuentes de dos sistemas informáticos.
- Especificar que módulos comprenden un sistema.
- Si ambos sistemas están destinados al mismo nivel de mercado.
- Determinar si un sistema trabaja en batch o en forma interactiva.

- Si ambos sistemas operan con los mismos criterios para organizar la emisión de listados.
- Determinar cuando dos sistemas son similares en cuanto a la estructura de datos utilizada para el almacenamiento de la información.
- Especificar los archivos que presentan uno y otro sistema.
- Si ambos sistemas utilizan las teclas de función y/o mandato para realizar cualquier tipo de operación.
- Que tiempo se necesita para cargar en un disco rígido.
- Que cantidad de formulario continuo se requiere para imprimir la totalidad de los programas fuentes de un sistema.
- Valor de mercado del alquiler horario de un equipo de computación.
- Que tiempo demandaría traducir los programas fuentes de un sistema a otro.
- Cantidad de programas de cada sistema.
- Preguntas generales sobre la ejecución de un sistema informático.

2.5.2. Recopilación de información

En la segunda fase, se recopila toda la documentación existente sobre el caso necesaria para dar respuesta a lo que nos están pidiendo averiguar. Si es suficiente, se pasa a la siguiente fase; de lo contrario, será necesario realizar un reconocimiento pericial, es decir, someter a la revisión técnica los

elementos informáticos para obtener determinados datos de comportamiento o detalles técnicos imprescindibles.

La revisión técnica puede convertirse en la tarea más delicada de todo el peritaje; es necesario tener en cuenta detalles como son una adecuada metodología de trabajo o tener experiencia en informática forense (por ejemplo, para no destruir pruebas, o realizar simulaciones en un entorno lo más real posible, etc.) En todo caso, es muy importante que el cliente sea informado cuanto antes del coste que puede suponer lo que nos pide, o incluso de la imposibilidad de averiguar algo.

Durante el desarrollo de la recopilación pueden existir dificultades para el resguardo de datos, se mencionan:

- Lentitud de los dispositivos.
- Importancia no siempre marcada de realizar esta operación.
- Imposibilidad de realizar la operación por cuestiones de recursos, tiempo o lugar.
- Requerimiento de amplios conocimientos técnicos en el manejo de herramientas.
- No siempre se puede realizar sobre un único medio de almacenamiento.

2.5.2.1. Prueba pericial informática

Es el medio de prueba, de suma importancia para cualquier actuación judicial y/o arbitraje que precisen conocimientos científicos o técnicos especializados, que ayudarán al juez o al interesado a valorar la naturaleza de los hechos.

El objeto de la prueba pericial es establecer la causa de los hechos y los efectos del comportamiento o fenómeno de estudio, la forma y circunstancia como se cometió el hecho delictivo.

La prueba pericial procede cuando la apreciación de los hechos requiere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica.

La parte interesada en este medio de pruebas propondrá con claridad y precisión el objeto sobre el cual deba recaer el reconocimiento pericial, y en casos de pericias judiciales, el juez se encargará de resolver sobre la necesidad, o no, de esta prueba; así mismo nombrará a los peritos para conocimiento de las partes, a fin de que puedan ser recusados o tachados por causas anteriores o posteriores al nombramiento.

Tanto en pericias judiciales y extrajudiciales, las partes pueden concurrir al reconocimiento pericial y dirigir a los peritos las observaciones que estimen oportunas, en ambos casos se informará verbalmente los resultados y se

dejará constancia en un acta; los peritos judiciales deberán elaborar un informe que posteriormente será ratificado bajo juramento ante un juez.

Cuando la revisión se va a realizar fuera del área de trabajo, se debe seleccionar exclusivamente el material útil para la investigación; además se debe tener en cuenta medidas de seguridad para el traslado de los elementos, ya que debido a su fragilidad corren peligro si no son transportados correctamente. Por ejemplo un disco duro en una bolsa de plástico puede ser golpeado e inutilizado; igualmente una computadora personal deberá tener precintadas las tomas eléctricas, las entradas de disquetes y CD ó unidades de cinta, de lo contrario podrían destruirse pruebas mediante la aplicación de descargas eléctricas.

2.5.3. Análisis de datos

En la tercera fase se buscan las relaciones entre los datos adquiridos para llegar a conclusiones intermedias que permitan construir los fundamentos del estudio.

Existen varias limitaciones a tener en cuenta para el análisis dentro de un peritaje:

- Disponibilidad de equipos: Debido a la variedad de marcas y modelos de hardware, a veces se dificulta la investigación; dado que es imposible contar con todas las versiones. De la misma forma, no siempre es posible clonar (hacer una copia imagen) el sistema a

periciar para un posterior análisis de datos por cuestiones de recursos, tiempo y lugar.

- Equipos compatibles: En muchos casos, no se puede prescindir del equipo sobre el cual se ejecuta el software. Si el sistema no puede ser clonado y ejecutado en otra plataforma, deberá evaluarse la posibilidad realizar la pericia sobre el sistema original, reduciéndose el alcance de la misma.
- Equipos antiguos: En la mayoría de los casos el tiempo que transcurre entre la intervención de los equipos y el desarrollo pericial es extremadamente extenso. En estos casos, si no se logra reconstruir un equipo de similares características, no se puede realizar ningún tipo de investigación.
- Desconocimiento de las claves de seguridad: En ciertos casos hay que hacer uso de los servicios de algún hacker. El acceso y descifrado de archivos encriptados es virtualmente imposible con las herramientas que se utilizan en la actualidad.
- Registro de la Propiedad Intelectual: Versiones desactualizadas y/o distintas al material conseguido, es recomendable encarar el tema de la Propiedad Intelectual, para exigir las actualizaciones de las modificaciones y cambios que sufren los sistemas.
- Desconocimiento de aspectos técnicos específicos de hardware, software o comunicaciones. Según el tipo de pericia y el área de competencia del perito, pueden existir limitaciones en las habilidades

prácticas sobre algunos elementos o herramientas específicas. En estos casos, se requerirá de personal técnico auxiliar para llevar a cabo la investigación.

Aparte de las limitaciones, también se debe considerar las dificultades que pueden aparecer en el análisis de los datos:

- Se requieren herramientas específicas para la extracción de evidencia de archivos borrados, o espacios de disco reutilizables o áreas de memoria virtual, así como también para la visualización de la información a peritar.
- La búsqueda de datos es muy rudimentaria y consume mucho tiempo. No existen clasificaciones de palabras estándares, formatos u organizaciones de datos que puedan ser aplicadas a la investigación de delitos específicos.
- No hay una forma automática de identificar a la información relevante, sin necesidad de leer los archivos. Las herramientas informáticas, sólo permiten definir el espacio de búsqueda, sin embargo, dada la gran cantidad de información que puede almacenarse en un sistema informático, no es posible realizar una investigación exhaustiva sobre todos los archivos localizados. En algunos casos, se debe realizar un análisis de datos sobre un subconjunto de ellos.

- No existe una técnica informática para identificar a los posibles autores de la información localizada, en base a su vocabulario, gramática o estilo de escritura.
- Existen algunas herramientas informáticas que permiten desencriptar datos, pero se basan en prueba y error, lo que implica tiempos de procesamiento no eficaces.
- No hay disponibles herramientas informáticas que correlacionen la información almacenada en los sistemas informáticos analizados. En algunos casos, se deben desarrollar bases de datos específicas para el procesamiento de la información.

2.5.4. Confección del dictamen pericial

El dictamen pericial es el estudio riguroso del problema encomendado para en base a los resultados obtenidos, producir una explicación consistente, la misma que se es condensada en un documento que refleja las secuencias fundamentales del estudio efectuado mediante una exposición razonada y coherente; excluyendo términos demasiado técnicos, considerando que el cliente puede ser lego en la materia.

Todo dictamen pericial debe contener:

- Datos y perfil del perito

- Objeto, antecedentes: Descripción de la persona, objeto o cosa materia de examen o estudio, así como, el estado y forma en que se encontraba.
- Período temporal: accesos / cambios
- Fuentes de información
- Medios científicos o técnicos que han servido para emitir el dictamen
- Relación detallada de todas las operaciones practicadas en la pericia y su resultado
- Criterios y estándares de base
- Limitaciones del dictamen: Personas, visitas, logs, lenguajes, idioma, entorno
- Anexos: Descripción de productos, listados de programas, gráficos
- Conclusiones a las que llegan los peritos
- Fecha
- Firma

2.5.5. Discusión del informe

Esta fase de discusión o defensa del informe tiene por objeto ratificar y afianzar el trabajo realizado.

El perito comparece y de forma oral aclara las conclusiones obtenidas y los métodos empleados para conseguirlas. El juez debe apreciar y valorar con un criterio de conciencia y sana crítica las pruebas periciales efectuadas,

analizando la coordinación lógica y científica de las conclusiones, la suficiencia e importancia de sus motivos y sus razones, que en caso de falta podrán ocasionar el rechazo de la pericia u ordenarse su aclaración.

Los jueces y tribunales no están obligados a sujetarse al dictamen de los peritos, es por ésto que se dice "El juez es perito de peritos". Si el juez no está convencido de la consistencia de la pericia, puede refutarla, pero tendrá que exponer las razones de su desacuerdo, sin dar cabida a su arbitrariedad o capricho. La corrección o incorrección de sus argumentos serán a su vez valoradas, así como los de pericia, por el superior jurisdiccional.

Es bastante común que durante la defensa surjan nuevas preguntas, a las que por desconocimiento del solicitante, espere respuestas “en vivo y en directo”. En esos casos, es preferible negarse a responder y aclarar que no es posible contestar la pregunta sin estudiar el fondo de la cuestión. De lo contrario, dependiendo del asunto podríamos incurrir en una falta y todo un deshonor profesional.

Como se expone, en el caso de un peritaje judicial, la última fase es muy relevante pues un buen trabajo mal defendido es lo peor que puede pasar y lo mejor para aquellos a los que las conclusiones les perjudicaban. La preparación de la defensa es en muchos casos algo que no se debe descuidar. Lo ideal es reunirse con la parte que ha solicitado el peritaje con el fin de aclarar determinadas cuestiones.

2.5.5.1. Ampliación del dictamen

Cuando el dictamen pericial requiriese operaciones o conocimientos de alta especialización, el juez podrá solicitar la opinión de colegios de profesionales, universidades, academias, entidades públicas o privadas de carácter científico o técnico. De igual forma, cuando el juez no está convencido del examen realizado por los peritos, puede solicitar pronunciamientos de estos grupos para que informen por escrito sobre el tema, obteniéndose otro objeto de valoración, ya que no es usual que se repita el examen o estudio de lo ya peritado.

2.6. Sistemas de Control

2.6.1. Antecedentes

Los sistemas de control según la Teoría Cibernética se aplican en esencia para los organismos vivos, las máquinas y las organizaciones. Estos sistemas fueron relacionados por primera vez en 1948 por Norbert Wiener en su obra titulada ‘Cibernética y sociedad’ con aplicación en la teoría de los mecanismos de control.

2.6.2. Definición

Un sistema de control está definido como un conjunto de componentes que pueden regular su propia conducta o la de otro sistema con el fin de lograr un

funcionamiento predeterminado. Se podría especificar que el sistema de control es la estructura de organización, de responsabilidades, de actividades, de recursos y de procedimientos que se establecen para llevar a cabo la gestión de control.

El sistema de control debe ser concordante con los objetivos de control contenidos en las normas relacionas al caso.

2.6.3. Tipos

Los sistemas de control son agrupados en tres tipos básicos:

2.6.3.1. Hechos por el hombre.- Como los sistemas eléctricos o electrónicos que están permanentemente capturando señales de estado del sistema bajo su control y que al detectar una desviación de los parámetros pre-establecidos del funcionamiento normal del sistema, actúan mediante sensores y actuadores, para llevar al sistema de vuelta a sus condiciones operacionales normales de funcionamiento.

2.6.3.2. Naturales, incluyendo sistemas biológicos.- Por ejemplo, los movimientos corporales humanos como el acto de indicar un objeto, éste incluye como componentes del sistema de control biológico los ojos, el brazo, la mano, el dedo y el cerebro del hombre. En la entrada se procesa el movimiento o no, y la salida es la dirección hacia la cual se hace referencia.

2.6.3.3. Cuyos componentes están unos hechos por el hombre y los otros son naturales.- Por ejemplo, el sistema de control de un hombre que conduce su vehículo; este sistema está compuesto por los ojos, las manos, el cerebro y el vehículo. La entrada se manifiesta en el rumbo que el conductor debe seguir sobre la vía y la salida es la dirección actual del automóvil.

Un sistema de control puede ser neumático, eléctrico, mecánico o de cualquier tipo, y su función es recibir entradas, y coordinar una o varias respuestas según su lazo de control (para lo que esta programado-creado).

2.6.4. Ingeniería en los sistemas de control

Los problemas considerados en la ingeniería de los sistemas de control básicamente se tratan mediante dos pasos fundamentales:

- El análisis.- En el análisis se investiga las características de un sistema existente.
- El diseño.- En el diseño se escogen los componentes para crear un sistema de control que posteriormente ejecute una tarea particular.

Existen dos métodos de diseño:

- Diseño por análisis.- Modifica las características de un sistema existente o de un modelo estándar del sistema.
- Diseño por síntesis.- Define la forma del sistema a partir de sus especificaciones.

CAPÍTULO 3

3. MARCO NORMATIVO Y/O ESTÁNDARES INTERNACIONALES

En este capítulo se mencionará a manera de síntesis las partes relativas al caso de estudio. Se incluirán antecedentes, generalidades, definiciones o estructuras de la normativa aplicable, profundizando los temas de mayor relevancia.

3.1. COSO

3.1.1. Antecedentes

Grupos de interés de Canadá, Estados Unidos, Reino Unido, Francia, Nueva Zelanda y otros países (Comisión Treadway) realizaron muchos esfuerzos para definir formalmente el Modelo de Control Interno COSO, que contiene objetivos y elementos del control interno, así mismo establecieron los roles de todos los interesados incluyendo la Junta Directiva, los directivos, los jefes de mandos medios, los supervisores y empleados.

3.1.2. Definición

La Comisión Treadway estableció la siguiente definición de control interno la cual ha sido adoptada ampliamente a nivel internacional.

“El control interno es un proceso llevado a cabo por la junta directiva de la entidad, los directivos y otro personal designado para proveer garantía razonable en cuanto al logro de objetivos en las tres siguientes categorías:

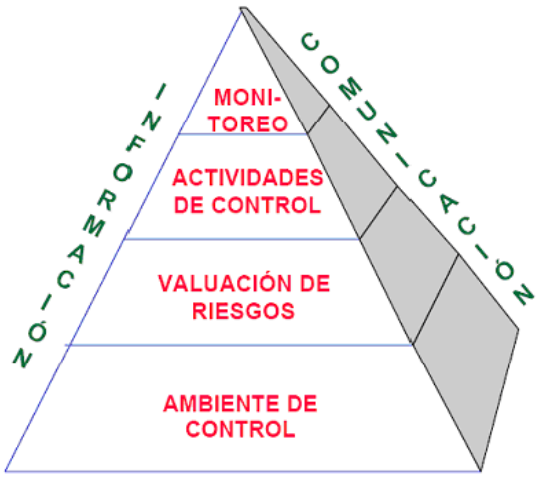
- Eficiencia y eficacia de las operaciones
- Razonabilidad de los estados financieros
- Cumplimiento con las políticas y procedimientos internos y con las leyes y regulaciones aplicables”. [16]

3.1.3. Componentes

El marco integrado de control consta de cinco componentes interrelacionados:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión

Figura 3.1. Pirámide de componentes COSO



Fuente: Referencia bibliográfica [16]

3.1.3.1. Ambiente de control

El ambiente de control refleja el espíritu ético vigente en una entidad respecto del comportamiento de los agentes, la responsabilidad con que encaran sus actividades, y la importancia que le asignan al control interno.

Los principales factores del ambiente de control son:

- La filosofía y estilo de la dirección y la gerencia.
- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades y de administración y desarrollo del personal.

- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

3.1.3.2. Evaluación de riesgos

Se define como riesgo la probabilidad de que un suceso ocurra y provoque pérdidas. El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones.

Cada entidad enfrenta una variedad de riesgos de fuentes internas y externas que deben ser evaluadas. La evaluación de riesgos comprende su identificación y análisis, conformando una base para determinar como los riesgos deben ser manejados. Es necesario entonces, que la organización posea mecanismos para identificar y manejar riesgos nuevos debido a las condiciones cambiantes de la economía, industria, condiciones reglamentarias y operacionales.

3.1.3.3. Actividades de control

Están constituidas por los procedimientos específicos establecidos como un reaseguro para el cumplimiento de los objetivos, orientados primordialmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos según lo expresado en el punto anterior: conociendo los riesgos, se disponen los controles destinados a evitarlos o minimizarlos.

A continuación se lista una gama de actividades de control, sin ser la totalidad de las mismas:

- Análisis efectuados por la dirección.
- Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades.
- Comprobación de las transacciones en cuanto a su exactitud, totalidad, y autorización pertinente: aprobaciones, revisiones, cotejos, recálculos, análisis de consistencia, prenumeraciones.
- Controles físicos patrimoniales: arqueos, conciliaciones, recuentos.
- Dispositivos de seguridad para restringir el acceso a los activos y registros.
- Segregación de funciones.
- Aplicación de indicadores de rendimiento.

3.1.3.4. Información y comunicación

En este elemento del sistema de control interno se diferencian la información de la comunicación; la primera son los datos necesarios para cumplir con las funciones, y la comunicación es la manera como la información fluye.

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales.

La comunicación es inherente a los sistemas de información. Las personas deben conocer a tiempo las cuestiones relativas a sus responsabilidades de gestión y control. Cada función ha de especificarse con claridad, entendiendo en ello los aspectos relativos a la responsabilidad de los individuos dentro del sistema de control interno.

La existencia de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos resultan vitales.

3.1.3.5. Supervisión

Los sistemas de control interno necesitan ser monitoreados. El monitoreo es un proceso que evalúa la calidad del comportamiento de los sistemas a través del tiempo.

Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado.

3.1.3.5.1. Modalidades de supervisión

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

3.1.3.5.1.1. Actividades continuas

Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias que pueden surgir.

3.1.3.5.1.2. Evaluaciones puntuales

En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

a) Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.

b) Son ejecutados por los propios responsables de las áreas de gestión, la auditoria interna y los auditores externos.

c) Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios ineludibles.

d) Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.

e) El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.

f) Debe confeccionarse un plan de acción que contemple:

- El alcance de la evaluación
- Las actividades de supervisión continuadas existentes.
- La tarea de los auditores internos y externos.
- Áreas o asuntos de mayor riesgo.
- Programa de evaluaciones.
- Evaluadores, metodología y herramientas de control.
- Presentación de conclusiones y documentación de soporte
- Seguimiento para que se adopten las correcciones pertinentes.

Mediante un esquema de controles incorporados como el descrito:

- Se fomentan la calidad, las iniciativas y la delegación de poderes.
- Se evitan gastos innecesarios.
- Se generan respuestas ágiles ante circunstancias cambiantes.

3.2. COBIT

3.2.1. Generalidades

COBIT es una herramienta para la administración y operación a un nivel superior a los estándares de tecnología para la administración de sistemas de información.

El objetivo principal de COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

El concepto fundamental del Marco Referencial de COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

3.2.2. Dominios de COBIT

Dentro de los niveles de actividades de TI de COBIT (2002) distinguimos los siguientes dominios: planeación y organización, adquisición e implementación, entrega y soporte y monitoreo.

3.2.3. Procesos y Objetivos de Control aplicables

A continuación se detallan los procesos y actividades que aplican para este estudio.

PLANEACIÓN Y ORGANIZACIÓN

En el caso de estudio, se aplica para lograr un balance entre las oportunidades de tecnología de información y los requerimientos del negocio, aprovechar la tecnología disponible para posibilitar la estrategia del negocio, mantener tareas y responsabilidades definidas bajo una dirección efectiva, asegurar el financiamiento y el control de los recursos, aplicar técnicas de administración de proyectos y planificar e implementar estándares de calidad en los sistemas.

1.0 Definición de un Plan Estratégico de Tecnología de Información

- 1.1 Tecnología de información como parte del Plan de la Organización a corto y a largo plazo
- 1.2 Plan a largo plazo de Tecnología de Información
- 1.8 Evaluación de los sistemas existentes

3.0 Determinación de la Dirección Tecnológica

- 3.4 Planes de Adquisición de Hardware y Software

4.0 Definición de la Organización y de las Relaciones de TI

- 4.5 Responsabilidad del aseguramiento de la calidad

4.6 Responsabilidad por la seguridad lógica y física

4.8 Propiedad de datos y sistemas

4.13 Personal clave de TI

4.14 Procedimientos y políticas para el personal contratado.

5.0 Manejo / Administración de la Inversión en Tecnología de Información

5.1 Presupuesto Operativo anual para la función de Servicios de Información

5.2 Monitoreo de Costo – Beneficios

5.3 Justificación de Costo - Beneficios

10.0 Administración de Proyectos

10.8 Plan de Aseguramiento de Calidad de Sistemas

11.0 Administración de Calidad

11.9 Marco Referencial para la adquisición y mantenimiento de la Infraestructura de Tecnología

11.10 Relaciones con terceras partes en su rol de implementadores

11.11 Estándares para la documentación de programas

11.13 Estándares para Pruebas de Sistemas

11.15 Documentación de las Pruebas del Sistema

ADQUISICIÓN E IMPLEMENTACIÓN

Nos asegura un efectivo y eficiente enfoque para satisfacer los requerimientos del usuario, proporciona plataformas apropiadas para soportar las aplicaciones, verifica y confirma que la solución (nuevo sistema) sea adecuada para el propósito deseado.

1.0 Identificación de soluciones

- 1.4 Requerimientos de servicios de terceros
- 1.14 Adquisición de Productos de Software
- 1.16 Contratos para la Programación de Aplicaciones

3.0 Adquisición y mantenimiento de la Arquitectura Tecnológica

- 3.1 Evaluación de nuevo hardware y software

5.0 Instalación y Acreditación de Sistemas

ENTREGA DE SERVICIOS Y SOPORTE

Provee controles para asegurar que los roles de terceras partes (proveedores de software) estén claramente definidos y que satisfagan los requerimientos, además sirve para garantizar la seguridad de los sistemas contra uso no autorizado, daño o pérdida.

2.0 Administrar servicios de terceros

- 2.3 Contratos con terceros

2.4 Calificaciones de terceros

2.5 Contratos de outsourcing

2.8 Monitoreo

5.0 Garantizar la seguridad de sistemas

5.11 Manejo de incidentes

MONITOREO

Aplicable para asegurar el logro de los objetivos establecidos, incrementar los niveles de confianza entre la organización, clientes y proveedores externos a través de evaluaciones de cumplimiento de compromisos contractuales o revisiones de auditoría.

1.0 Monitoreo del Proceso

3.0 Obtención de aseguramiento independiente

3.4 Evaluación independiente de la efectividad de los proveedores externos de servicios

3.6 Aseguramiento independiente del cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales con proveedores externos de servicios

4.0 Proveer Auditoría Independiente

3.3. IEEE 730

3.3.1. Antecedentes

“IEEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática e ingenieros en telecomunicación.” [46]

Figura 3.2. Logo de IEEE

Fuente: Referencia bibliográfica [31]

Su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales. Uno, entre los más de 900 estándares publicados es el IEEE 730.

3.3.2. Definición

El estándar IEEE 730 - Plan de aseguramiento de la calidad del software, establece el puente entre la gestión de la calidad y la ingeniería del software; comprende requerimientos para llevar a cabo un Plan de Garantía de Calidad asociado a un proyecto de software. Cabe señalar, que mientras que la aplicación del ISO 9000-3 está dirigida a toda la organización, el IEEE 730 es para aplicación en un único proyecto dentro de esa organización.

El IEEE 730 describe el conjunto de actividades sistemáticas necesarias para aportar la confianza en que el software satisfará los requisitos dados de calidad. Esta norma aplica para el desarrollo y mantenimiento de software crítico; la norma nos ayuda a evaluar el proceso mediante el cual se desarrolla el software.

A su vez el IEEE 730 tiene relación con otros estándares como el IEEE 828 y el 1219, que son de utilidad para aplicar las necesidades expuestas en el 730.

3.3.3. Recomendaciones más aplicables

Siguiendo el estándar IEEE, al iniciar un proyecto software hay que:

- Seleccionar uno o varios modelos del ciclo de vida, y concretarlo luego en uno determinado para dicho proyecto.
- Definir los aspectos relacionados con la financiación y viabilidad del proyecto.
- Definir las metodologías, técnicas y herramientas a utilizar.
- Planificar la gestión del proyecto software. Esta planificación debe incluir y describir:
    1. El día a día del proyecto, con los correspondientes controles de auditorias y revisiones
    2. La planificación del aseguramiento de la calidad del software (SQA)
    3. La planificación de la documentación del proyecto

3.4. ISO 9000-3

3.4.1. Generalidades

Esta parte de la ISO 9001:2000 tiene vinculación con situaciones donde se desarrolla software específico como parte de un contrato, siguiendo las especificaciones del comprador; sin embargo, puede ser de valor en otras situaciones.

Figura 3.3. Logo de la ISO

Fuente: Referencia bibliográfica [28]

La ISO 9000-3 intenta proporcionar directrices aplicables cuando un contrato entre dos partes requiere la demostración de la capacidad de un proveedor para desarrollar, suministrar y mantener productos de software, en otras palabras proporciona una guía para asegurar la calidad del software.

En la naturaleza del desarrollo del software algunas actividades están relacionadas a fases particulares del proceso de desarrollo, mientras que otras pueden aplicarse a través de todo el proceso.

3.4.2. Cláusulas

Se presenta en tabla adjunta el índice de cláusulas que comprenden la norma. Cada cláusula esta identificada con un número.

Tabla III.I. Indice de cláusulas de la ISO 9000-3

NÚMERO	CLÁUSULA
4	Sistema de calidad-modelo
4.1	Administración de la Responsabilidad
4.2	Sistema de Calidad
4.3	Auditorias Internas del Sistema de Calidad
4.4	Acción Correctora
5	Sistema de calidad -actividades de ciclo de vida

5.1	General
5.2	Revisión del Contrato
5.3	Especificación de los requerimientos de la Organización
5.4	Planificación del desarrollo
5.5	Planificación de la Calidad
5.6	Diseño e Implementación
5.7	Testeo y Validación
5.8	Aceptación
5.9	Generación, Entrega e Instalación
5.10	Mantenimiento
6	Sistema de calidad - actividades de apoyo
6.1	Administración de la Configuración
6.2	Documentos de Control
6.3	Calidad de los Archivos
6.4	Medidas
6.5	Reglas y Convenciones
6.6	Herramientas y Técnicas
6.7	Compra
6.8	Productos de software incluidos
6.9	Formación

Fuente: Referencia bibliográfica [32]

3.4.3. Descripción de cláusulas aplicables

Se hará una descripción breve de las cláusulas más relacionadas con el tema, siguiendo la numeración que se mostró en la tabla anterior.

4.1 Administración de la Responsabilidad

4.1.1 Responsabilidad gerencial del proveedor

4.1.1.2 Organización

4.1.1.2.1 Autoridad y responsabilidad

Debe definirse la responsabilidad, la autoridad y las relaciones entre todo el personal que dirige, realiza y verifica cualquier trabajo relacionado con la calidad, particularmente aquel personal que precisa independencia y autoridad para:

1. Iniciar, acciones para prevenir la ocurrencia de productos no conformes.

2. Identificar y registrar cualquier problema relacionado con la calidad del producto.

3. Iniciar, recomendar o aportar soluciones a través de los canales establecidos.

4. Comprobar que se ponen en práctica las soluciones adoptadas.

5. Controlar el procesamiento posterior, el envío y la entrega o la instalación del producto no conforme, hasta que la deficiencia o la condición insatisfactoria haya sido corregida.

4.1.2 Responsabilidad gerencial del comprador

“El comprador deberá colaborar con el proveedor para proporcionar a tiempo toda la información necesaria y resolver las situaciones pendientes de arreglo.

El comprador designará un representante con la responsabilidad de tratar con el proveedor sobre asuntos contractuales. Este representante tendrá la autoridad necesaria que le permita tratar cualquier asunto contractual que incluya, pero no esté limitado, a los siguientes aspectos:

1. Definir los requerimientos del comprador hacia el proveedor;

2. Responder a preguntas del proveedor;

3. Aprobar las propuestas del proveedor;

4. Finalizar acuerdos con el proveedor;

5. Asegurar que la organización del comprador cumpla con los acuerdos hechos con el proveedor;

6. Definir los criterios y los procedimientos de aceptación;

7. Resolver acerca de los componentes de software que se considere son inadecuados para ser usados, siguiendo los criterios comprador – proveedor". [12]

4.1.3 Revisiones conjuntas

Se debe establecer revisiones conjuntas periódicas que involucran al proveedor y al comprador, de modo de cubrir los siguientes aspectos, si ello es apropiado:

1. La conformidad del software con los requisitos de la especificación del comprador acordada;

2. Los resultados de la verificación;

3. Los resultados de los ensayos de aceptación.

Los resultados de tales revisiones deben ser acordados y estar documentados.

4.4 Acciones Correctivas

El proveedor debe establecer, documentar y mantener procedimientos para:

1. Investigar las causas de los productos no conformes y la acción correctivo que debe aplicarse para evitar su repetición;

2. Analizar todos los procesos, operaciones, autorizaciones, registros de calidad, informes de servicio y quejas de clientes para detectar y eliminar las causas potenciales que generan productos no conformes;

3. Iniciar acciones preventivas para tratar los problemas a un nivel que corresponda a los riesgos encontrados;

4. Realizar controles para asegurar que se tomen las acciones correctivas y que éstas sean efectivas,

5. Aplicar y registrar las modificaciones a los procedimientos que resulten de las acciones correctivas.

5.2 Revisión de Contratos

5.2.1 Generalidades

“El proveedor establecerá y mantendrá procedimientos para la revisión de contratos y para la coordinación de estas actividades.

Cada contrato será revisado por el proveedor para asegurar que:

1. El objeto y los requisitos del contrato están definidos y documentados;

2. Se ha identificado posibles riesgos o contingencias;

3. La propiedad de la información está adecuadamente protegida;

4. Se ha resuelto cualesquiera requisitos que difieren de aquellos que están en la propuesta;

5. El proveedor tiene la capacidad para cumplir los requisitos contractuales;

6. Se ha definido la responsabilidad del proveedor con respecto al trabajo subcontratado;

7. La terminología está acordada por ambas partes;

8. El comprador tiene la capacidad para cumplir las obligaciones contractuales.

Se debe mantener registros de tales revisiones de contrato.” [12]

5.2.2 Detalles del contrato sobre calidad

Se encuentra, frecuentemente, que es pertinente que los siguientes detalles, entre otros, figuren en el contrato:

1. Criterios de aceptación;

2. Manejo de los cambios en los requisitos del proveedor durante el desarrollo;

3. Manejo de los problemas detectados después de la aceptación, incluyendo las reclamaciones y las quejas del comprador relacionadas con calidad;

4. Actividades llevadas a cabo por el comprador, especialmente la función del comprador en la especificación de los requisitos, en la instalación y en la aceptación;

5. Instalaciones, herramientas y componentes de software a ser suministrados por el comprador;

6. Normas y procedimientos a ser usados;

7. Requisitos de reproducción.

5.3 Especificación de los Requisitos del Comprador

5.3.1 Generalidades

Con la finalidad de llevar a cabo el desarrollo de software el proveedor dispondrá de un conjunto completo y no ambiguo de requisitos funcionales. Además, estos requisitos incluirán todos los aspectos necesarios para satisfacer las necesidades del comprador. Éstos pueden incluir, pero no están limitados, a los siguientes: comportamiento, seguridad, confiabilidad, protección y privacidad. Estos requisitos serán establecidos en forma suficientemente precisa, de modo de permitir la validación durante la aceptación del producto.

La especificación de los deseos y las necesidades del comprador es el documento que registra estos requisitos. En algunos casos, este documento es proporcionado por el comprador. En caso contrario, el proveedor deberá desarrollar estos requisitos en estrecha colaboración con el comprador, para lo cual el proveedor deberá obtener la aprobación del comprador antes de iniciar la etapa de desarrollo. Como parte de la documentación de desarrollo, la especificación de los requisitos del comprador estará sometida a control de documentación y a gestión de configuración.

En la especificación de los requisitos del comprador, deberán establecerse totalmente todas las interfases entre el producto de software y otros

productos de software y de hardware, ya sea directamente o mediante referencia.

5.3.2 Colaboración mutua

Se recomienda que durante el desarrollo de la especificación de los requisitos del comprador, se preste atención a los siguientes puntos:

1. La designación de personas (de ambas partes) que tengan responsabilidad para establecer la especificación de los requisitos del comprador;

2. Los métodos para acordar los requisitos y aprobar los cambios;

3. Las acciones para prevenir malas interpretaciones, tales como definiciones de términos, explicación de fundamentos de los requisitos;

4. Los resultados de la discusión deben ser registrados y revisados por ambas partes.

5.4 Planificación del Desarrollo

5.4.1 Generalidades

El plan de desarrollo deberá cubrir lo siguiente:

1. La definición del proyecto, incluyendo una declaración de sus objetivos y la referencia a los proyectos conjuntos entre comprador y proveedor;

2. La organización de los recursos del proyecto, incluyendo la estructura del grupo humano, las responsabilidades, el uso de subcontratistas y los recursos materiales a ser usados;

3. Las fases de desarrollo (como se definen en inciso 5.4.2.1);

4. El calendario del proyecto, identificando las tareas que se deben realizar, los recursos y el tiempo necesario para cada una de ellas y cualesquiera interrelaciones entre las tareas;

5. La identificación de los planes relacionados, tales como:

- plan de calidad,
- plan de gestión de configuración,
- plan de integración,
- plan de ensayo.

El plan de desarrollo debe irse adecuando a medida que el desarrollo progresa y cada fase debe ser definida como en el inciso 5.4.2.1, antes de comenzar las actividades en esa fase. Dicho plan debe ser revisado y aprobado antes de su ejecución.

5.4.2 Plan de desarrollo

5.4.2.1 Fases

El plan de desarrollo definirá un proceso o una metodología para transformar la especificación de los requisitos del comprador en un producto de software.

Esto puede involucrar la segmentación del trabajo en fases y la identificación de:

1. Las fases de desarrollo a llevar a cabo;

2. Los elementos de entrada requeridos a cada fase;

3. Los elementos de salida requeridos de cada fase;

4. Los procedimientos de verificación a llevar a cabo en cada fase;

5. El análisis de los problemas potenciales asociados con las fases de desarrollo y con el logro de los requisitos especificados.

5.4.2.2 Gestión

El plan de desarrollo definirá la forma en que se gestionará el proyecto, incluyendo la identificación de:

1. Calendario de desarrollo, de aplicación y de distribuciones asociadas;

2. Control del progreso del trabajo;

3. Responsabilidades organizativas, recursos y asignación de trabajo;

4. Interfases organizativas y técnicas entre los diferentes grupos de trabajo.

5.4.3 Control de progreso

Las revisiones de progreso deben ser planificadas, mantenidas y documentadas para asegurar que los temas vinculados con recursos

pendientes, son resueltos y para asegurar la ejecución efectiva de los planes de desarrollo.

5.8 Aceptación

5.8.1 Generalidades

Cuando el proveedor está en condiciones de despachar el producto validado, el comprador debe juzgar si el mismo es o no aceptable, según los criterios previamente acordados y de la manera especificada en el contrato.

El método de manejo de los problemas detectados durante el procedimiento de aceptación y su destino, deberán ser acordados entre el comprador y el proveedor, debiendo ser esto documentado.

5.9 Reproducción, Despacho e Instalación

5.9.3 Instalación

Las funciones, las responsabilidades y las obligaciones del proveedor y del comprador deberán ser establecidas claramente, tomando en cuenta lo siguiente:

1. El calendario, incluyendo horarios de trabajo extra y fines de semana;

2. El acceso a los locales del comprador (distintivos de seguridad, claves, escoltas);

3. La disponibilidad de personal calificado;

4. La disponibilidad y el acceso a los sistemas y al equipamiento del comprador;

5. La necesidad de realizar validación formal, como parte de cada instalación, deberá ser determinada en forma contractual;

6. Un procedimiento formal para la aprobación final de cada instalación.

3.5. ISO 17799

3.5.1. Generalidades

La ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de seguridad de la información; está dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

La seguridad de la información se define como la preservación de:

- Confidencialidad.- Asegura que la información sea accesible sólo para aquellos autorizados a tener acceso.
- Integridad.- Garantiza la exactitud y completitud de la información y de los métodos de su procesamiento.
- Disponibilidad.- Asegura que los usuarios autorizados tengan acceso cuando lo requieran a la información y sus activos asociados.

El objetivo principal de la ISO 17799 es proporcionar un conjunto de normas comunes de seguridad de información reconocidas globalmente, y ser una práctica eficaz de la gestión de la seguridad capaz de someterse a auditorías independientes.

3.5.2. Estructura

La norma ISO 17799:2002 establece diez dominios de control que cubren todos los aspectos fundamentales aplicables a la seguridad en el manejo de la información:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Administración de la continuidad del negocio
- Conformidad con la legislación

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

Figura 3.4. Dominios de control ISO 17799

Fuente: Referencia Bibliográfica [44]

3.5.3. Descripción de los objetivos de control que guardan mayor relación

3.5.3.1. Aspectos organizativos para la seguridad

Dentro de los aspectos organizativos podemos encontrar aspectos referentes a la infraestructura de seguridad de la información, seguridad frente al acceso de terceros y la tercerización. Se profundizará en el segundo punto, cuyo objetivo es mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

3.5.3.1.1. Identificación de riesgos del acceso de terceras partes

3.5.3.1.1.1. Tipos de acceso

El tipo de acceso otorgado a terceras partes es de especial importancia. Por ejemplo, los riesgos de acceso a través de una conexión de red son diferentes de los riesgos relativos al acceso físico. Los tipos de acceso que deben tenerse en cuenta son:

a) acceso físico, por ejemplo, a oficinas, salas de cómputos, armarios ;
b) acceso lógico, por ejemplo, a las bases de datos y sistemas de información de la organización.

3.5.3.1.1.2. Razones para el acceso

Puede otorgarse acceso a terceros por diversas razones. Por ejemplo, existen terceros que proveen servicios a una organización y no están ubicados dentro de la misma pero se les puede otorgar acceso físico y lógico, tales como:

a) personal de soporte de hardware y software, quienes necesitan acceso a nivel de sistema o a funciones de las aplicaciones;
b) socios comerciales o socios con riesgos compartidos, quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos.

La información puede ponerse en riesgo si el acceso de terceros se produce en el marco de una inadecuada administración de la seguridad. Cuando existe una necesidad de negocios que involucran una conexión con un sitio externo, debe llevarse a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos. Ésta debe tener en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y la incidencia de este acceso en la seguridad de la información de la organización.

3.5.3.1.1.3. Contratistas in situ

Las terceras partes que sean ubicadas in situ por un período de tiempo determinado según contrato, también pueden originar debilidades en materia de seguridad. Entre los ejemplos de terceras partes in situ se enumeran los siguientes:

a) personal de mantenimiento y soporte de hardware y software;
b) limpieza, catering, guardia de seguridad y otros servicios de soporte tercerizados;
c) pasantías de estudiantes y otras designaciones contingentes de corto plazo;
d) consultores.

Es esencial determinar qué controles son necesarios para administrar el acceso de terceras partes a las instalaciones de procesamiento de

información. En general, todos los requerimientos de seguridad que resultan de los controles internos o del acceso de terceros, deben estar reflejados en los contratos celebrados con los mismos. Por ejemplo, si existe una necesidad específica de confidencialidad de la información, podrían implementarse acuerdos de no-divulgación.

No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o el acceso.

3.5.3.1.2. Requerimientos de seguridad en contratos con terceros

Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización. El contrato debe garantizar que no surjan malentendidos entre la organización y el proveedor. Las organizaciones deben estar satisfechas con las garantías de su proveedor. Se deben considerar las siguientes cláusulas para su inclusión en el contrato:

a) la política general de seguridad de la información;
b) la protección de activos, con inclusión de:

1) procedimientos de protección de los activos de la organización, incluyendo información y software;
2) procedimientos para determinar si se han comprometido los activos, por ej., debido a pérdida o modificación de datos;
3) controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato, o en un momento convenido durante la vigencia del mismo;
4) integridad y disponibilidad;
5) restricciones a la copia y divulgación de información;

c) una descripción de cada servicio del que podrá disponerse;
d) el nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables;
e) disposición que contemple la transferencia de personal cuando corresponda;
f) las respectivas obligaciones de las partes con relación al acuerdo;
g) responsabilidades con respecto a asuntos legales, por ej., legislación referida a protección de datos, especialmente teniendo en cuenta diferentes sistemas legales nacionales si el contrato contempla la cooperación con organizaciones de otros países;
h) derechos de propiedad intelectual y asignación de derecho de propiedad intelectual, y protección de trabajos realizados en colaboración;
i) acuerdos de control de accesos que contemplen:

1) los métodos de acceso permitidos, y el control y uso de identificadores únicos como IDs y contraseñas de usuarios;
2) un proceso de autorización de acceso y privilegios de usuarios;
3) un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso;

j) la definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos;

k) el derecho a monitorear, y revocar (impedir), la actividad del usuario;

l) el derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditorías;

m) el establecimiento de un proceso gradual para la resolución de problemas; también deben considerarse, si corresponde, disposiciones con relación a situaciones de contingencia;

n) responsabilidades relativas a la instalación y el mantenimiento de hardware y software;

o) una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos;

p) un proceso claro y detallado de administración de cambios;

q) los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos;
r) los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad;
s) los controles que garanticen la protección contra software malicioso;
t) las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad; la relación entre proveedores y subcontratistas.

3.5.3.2. Seguridad del personal

La norma considera dentro de la seguridad del personal, la respuesta a incidentes y anomalías, en este caso se ampliará el tema sobre la comunicación de anomalías del software.

3.5.3.2.1. Comunicación de anomalías del software

Se deben considerar las siguientes acciones:

a) Deben advertirse y registrarse los síntomas del problema y los mensajes que aparecen en pantalla.
b) La computadora debe ser aislada, si es posible, y debe detenerse el uso de la misma. Se debe alertar de inmediato a la persona pertinente (contacto). Si se ha de examinar el equipo, éste debe ser desconectado de las redes de la organización antes de ser activado

nuevamente. Los disquetes no deben transferirse a otras computadoras.

c) El asunto debe ser comunicado inmediatamente al gerente de seguridad de la información.

Los usuarios no deben quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados a hacerlo. La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

3.5.3.3. Seguridad física y ambiental

Se tratará únicamente sobre los controles de acceso físico.

3.5.3.3.1. Controles de acceso físico

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

a) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado

exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ej. Tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.

c) Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.
d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

3.5.3.4. Gestión de comunicaciones y operaciones

Tiene como objetivo garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Para el caso de estudio, se explicará sobre la planificación y aprobación del sistema.

3.5.3.4.1. Aprobación del sistema

Se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, y se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación. Los gerentes deben garantizar que los requerimientos y criterios de aprobación de nuevos sistemas sean claramente definidos, acordados, documentados y probados. Se deben considerar los siguientes puntos:

a) desempeño y requerimientos de capacidad de las computadoras;
b) recuperación ante errores y procedimientos de reinicio, y planes de contingencia;
c) preparación y prueba de procedimientos operativos de rutina según estándares definidos
d) conjunto acordado de controles de seguridad implementados
e) procedimientos manuales eficaces;
f) disposiciones relativas a la continuidad de los negocios,
g) evidencia que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento, como durante los últimos días del mes
h) evidencia de que se ha tomado en cuenta el efecto que tiene el nuevo sistema en la seguridad global de la organización
i) entrenamiento en la operación o uso de nuevos sistemas.

Para los principales nuevos desarrollos, las funciones y usuarios de operaciones deben ser consultados en todas las etapas del proceso de desarrollo para garantizar la eficiencia operativa del diseño propuesto del sistema. Deben llevarse a cabo pruebas apropiadas para constatar el cumplimiento cabal de todos los criterios de aprobación.

3.5.3.5. Desarrollo y mantenimiento de sistemas

Se indica consideraciones para el desarrollo de software por parte de terceros.

3.5.3.5.1. Desarrollo externo de software

Cuando se terceriza el desarrollo de software, se deben considerar los siguientes puntos:

a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual;
b) certificación de la calidad y precisión del trabajo llevado a cabo;
c) acuerdos de custodia en caso de quiebra de la tercera parte;
d) derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado;
e) requerimientos contractuales con respecto a la calidad del código; realización de pruebas previas a la instalación para detectar códigos troyanos.

3.6 NEA No. 11

En la NEA No. 11 - Auditoría en un ambiente de información por computadora, se enfocan principios básicos y procedimientos esenciales para desempeñar el trabajo del auditor en un ambiente de sistemas de información; estos guardan similitud con los lineamientos que el perito debe seguir durante su ejercicio. Esta NEA abarca contenidos sobre la habilidad y competencia del auditor, la planificación, la evaluación del riesgo y los

procedimientos de auditoría; de los cuales citaremos las partes más importantes con el fin de dar una idea de lo que la norma ecuatoriana indica, y que está relacionado con el tema en análisis.

3.6.1. Habilidad y competencia

"El auditor debería tener suficiente conocimiento del SIC para planificar, dirigir, supervisar y revisar el trabajo desarrollado. El auditor debería considerar si se necesitan habilidades especializadas en SIC en una auditoría". [4]

3.6.2. Planificación

"De acuerdo con la NEA "Evaluaciones del Riesgo y Control Interno" el auditor debería obtener una suficiente comprensión de los sistemas de contabilidad y de control interno, para planificar la auditoría y desarrollar un enfoque de auditoría efectivo". [4]

"Al planificar las porciones de la auditoría que pueden verse afectadas por el ambiente SIC del cliente, el auditor debería obtener una comprensión de la importancia y complejidad de las actividades del SIC y la disponibilidad de datos para el uso en la auditoría. Esta comprensión incluiría asuntos como:" [4]

- La importancia y complejidad del procesamiento por computadora en cada operación importante de contabilidad.

- La estructura organizacional de las actividades SIC del cliente y el grado de concentración o distribución del procesamiento por computadora en toda la entidad, particularmente en cuanto puedan afectar la segregación de deberes.
- La disponibilidad de datos. Los documentos fuente, ciertos archivos de computadora, y otro material de evidencia que puede ser requerido por el auditor, pueden existir por un corto periodo de tiempo o solo en forma legible por computadora. El SIC del cliente puede generar reportes internos que pueden ser útiles para llevar a cabo ciertas pruebas sustantivas (particularmente procedimientos analíticos).

3.6.3. Evaluación del riesgo

"De acuerdo con la NEA "Evaluación del riesgo y control interno", el auditor debería hacer una evaluación de los riesgos inherente y de control para las aseveraciones importantes de los estados financieros." [4]

Los riesgos inherentes y de control en un ambiente de SIC pueden tener tanto efectos generales como específicos:

- Los riesgos pueden resultar de deficiencias en actividades generales de SIC como desarrollo y mantenimiento de programas, respaldo de software de sistemas, operaciones, seguridad física de SIC y control sobre el acceso a programas de privilegio especial.

- Los riesgos pueden incrementar el potencial de errores y actividades fraudulentas en aplicaciones, bases de datos o archivos maestros. Los sistemas que controlan desembolsos de efectivo u activos líquidos son susceptibles a acciones fraudulentas por los usuarios o por el personal del SIC.

3.6.4. Procedimientos de auditoría

De acuerdo con la NEA “Evaluaciones del riesgo y control interno” el auditor debería considerar el ambiente SIC al diseñar los procedimientos de auditoría para reducir el riesgo a un nivel aceptablemente bajo.

CAPÍTULO 4

4. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CONTROL PARA REALIZAR PERITAJES INFORMÁTICOS A UN SISTEMA DE INFORMACIÓN ADQUIRIDO POR UNA COOPERATIVA DE AHORRO Y CRÉDITO: ASPECTOS PREVIOS

4.1. Información Preliminar

4.1.1. Introducción.- El presente trabajo ha sido desarrollado en una cooperativa de ahorro y crédito cuyo nombre se mantendrá en reserva, y para efectos de esta revisión se la denominará “La Cooperativa”.

La Cooperativa, ubicada en el centro de la Ciudad de Guayaquil, fue creada hace quince años con el objetivo de captar los ahorros de los empleados de una reconocida institución de servicios, y, asimismo extender créditos de acuerdo a la necesidad de sus clientes.

Con el objetivo de mantener un control adecuado sobre sus procesos, y debido a la necesidad de actualizar el software utilizado para el registro y

manipulación de datos, contrató un servicio de outsourcing para la creación de un software a la medida.

La Cooperativa desea esclarecer la realidad de los hechos en cuanto al cumplimiento del contrato, la utilidad del software de ser posible, y los motivos que causaren el fracaso de dicho proyecto; para lo cual contrata los servicios de un perito informático, encargado de elaborar el informe pericial con base a las revisiones efectuadas.

El diseño de un sistema de control para garantizar resultados veraces del peritaje informático aplicado al sistema de software a la medida contratado por la Cooperativa, será el resultado de este caso de estudio.

4.1.2. Objetivo General.- El objetivo general del diseño de un sistema de control es enfocar los principales puntos de revisión que el perito debe evaluar como mínimo, para alcanzar opiniones reales y bien fundamentadas, que coadyuven a la minimización de impactos informáticos producto de debilidades sobre los sistemas de información o procedimientos relacionados, que pudieran generar pérdidas económicas o de reputación para La Cooperativa.

4.1.3. Objetivos Específicos del Diseño e Implementación del Sistema de Control para realizar Peritajes Informáticos a un Sistema de Información.- Entre los principales objetivos que motivan la implementación de un Sistema de Control tenemos:

- Mostrar paso a paso la metodología adecuada para el peritaje por incumplimiento del contrato de software, así como la estructura del informe pericial.
- Redefinir políticas y procedimientos sobre contratación de servicios de terceros referentes a la adquisición, desarrollo y mantenimiento de software, el pago de honorarios y la supervisión, con el fin de evitar pérdidas por futuros incumplimientos de contratos.
- Brindar una mayor integridad, confidencialidad y confiabilidad de la información de clientes de la Cooperativa, mediante la implantación de controles en los procesos.
- Proporcionar a cualquier usuario una herramienta de medición y control de la cobertura del peritaje, que garantice resultados eficientes en la evaluación a la contratación de un sistema de información.
- Establecer controles administrativos, financieros y tecnológicos necesarios con el fin de asegurar la correcta administración de cualquier empresa en cuanto al manejo de procesos relativos a los contratos de sistemas de software.

4.1.4. Alcance.- El sistema de control a implementarse, está dirigido específicamente a la realización de peritajes informáticos sobre contratos de diseño, desarrollo e implementación de software.

De acuerdo a los objetivos definidos anteriormente el alcance del trabajo radica básicamente en:

4.1.4.1. Realizar el peritaje informático.

- Aplicar los procedimientos de peritación.
- Presentar el dictamen pericial sobre la contratación del sistema de software a la medida.

4.1.4.2. Diseñar el sistema de control para la realización de peritajes informáticos.

- Establecer la metodología de diseño de un sistema de control.
- Incluir los aspectos normativos en la matriz de aspectos y controles.

4.1.4.3. Aplicar el sistema de control al peritaje realizado.

- Establecer metodología de calificación en función de las temáticas abordadas.
- Mostrar resultados.

4.2. Estrategias - Metodologías

Se aplicarán dos metodologías, la primera para realizar el peritaje informático al contrato de software a la medida suscrito por la Cooperativa y el Proveedor; y la segunda para el diseño e implementación del sistema que controle la realización del peritaje informático relacionado. Ambas serán desarrolladas en el siguiente capítulo.

4.2.1. Metodología para realizar el peritaje informático

La metodología a proponer puede ser aplicable a cualquier tipo de peritaje. Se presentará en tres fases la guía utilizada para realizar la evaluación, comprendiendo desde la planificación hasta la presentación del dictamen pericial.

4.2.1.1. Planeación

- Identificar el motivo del peritaje
- Realizar una visita preliminar al área
- Establecer los objetivos
- Determinar los puntos que serán evaluados
- Elaborar programas de trabajo
- Identificar y seleccionar las herramientas, instrumentos y procedimientos necesarios
- Asignar el valor de los honorarios a percibir

4.2.1.2. Ejecución

- Realizar las acciones programadas
- Aplicar los instrumentos y herramientas
- Identificar y elaborar los documentos de las desviaciones encontradas
- Integrar el legajo de los papeles de trabajo

4.2.1.3. Dictamen

- Analizar la información y elaborar un informe de situaciones detectadas
- Elaborar el dictamen final

4.2.2. Metodología para el diseñar e implementar el sistema de control

En casi todos los casos, la implantación de un sistema de control va de la mano de la evaluación de riesgos, es decir la identificación y medición de riesgos, de forma que se propongan controles en función del nivel de riesgo identificado.

Para nuestro caso de estudio, el riesgo identificado se reflejaría en la emisión de una opinión sesgada por parte del perito, que es producto de omisiones en su revisión, falta de profundidad en las pruebas, conflicto de intereses, vinculaciones, etc..

Para garantizar que los resultados del peritaje vayan de acuerdo a la realidad de los hechos, se va a identificar puntos de revisión obligatorios dentro de cada una de las temáticas que son materia de análisis del perito al evaluar el cumplimiento del contrato de software, así como también puntos de revisión relacionados a la práctica del peritaje.

Del porcentaje de cumplimiento de los puntos de revisión tomados en cuenta en el peritaje, se determinará su nivel de rendimiento.

4.2.2.1. Identificar las diferentes temáticas que se debieron tener en cuenta a lo largo del peritaje.

Para la identificación de las temáticas, se toman en cuenta todas las actividades que intervinieron para la toma de decisión de la contratación del diseño del sistema informático, es decir el proceso de contratación; así también, se consideran las temáticas inherentes a cualquier peritaje, es decir, el perito, tiempos de respuesta y la evidencia.

4.2.2.2. Identificar los puntos de evaluación bajo cada temática.

Los puntos para cada temática se descubren haciendo preguntas sobre la misma, como las siguientes:

- ¿Qué necesita cumplir el _____ para ser ideal?
- ¿Qué características debe tener el _____ para estar completo?
- ¿De qué dependen _____ para ser óptimos?

Todas las preguntas están orientadas a buscar los puntos de evaluación a tener en cuenta para que la temática alcance su estado óptimo, sean estas personas, aspectos, etc..

4.2.2.3. Asignar a cada punto, el o los documentos que sirvan para verificar su cumplimiento.

Una vez definidos los puntos de análisis por temática, se busca como evidenciar su realización, es decir los documentos que deberían existir como soporte para cualquier usuario, de que se ha realizado o se ha cumplido la actividad que propone el punto de evaluación.

4.2.2.4. Proponer los controles a implementar por cada punto.

Los controles a implementar garantizan que la organización siga las buenas prácticas definidas dentro de cada proceso relacionado a la temática.

Resultado del seguimiento de los controles, la organización, dentro de su operación normal, generará documentación soporte de las actividades realizadas. Esta documentación es la que sirve como medio de prueba durante la búsqueda de evidencia en el peritaje. Mientras más documentación válida exista, el resultado del peritaje será más completo; ya que la no existencia de documentación, sea física o lógica, limita la opinión del perito.

Para los puntos de evaluación de temáticas inherentes a todo peritaje, como son la idoneidad del perito, la oportunidad en los tiempos de respuesta y la suficiencia de evidencia sobre lo dictaminado, los controles a proponer no afectan directamente a los procesos de la organización que solicita el peritaje, ya que dependen mayormente del desenvolvimiento del perito.

4.2.2.5. Establecer metodología de evaluación por temáticas

4.2.2.5.1. Aplicación de lista de chequeo de cumplimiento

La lista de chequeo está compuesta por la totalidad de puntos de evaluación y contiene tres alternativas de respuesta: SI, NO, NO SE PUDO EVALUAR. Será de utilidad para las empresas, jueces, colegios de profesionales y para el mismo perito en caso de auto-evaluación, para controlar que la pericia realizada haya contemplado todos los aspectos necesarios para la emisión de una opinión consistente sobre el caso, y además se haya cumplido con los requisitos del perito y fases de la peritación.

4.2.2.5.2. Identificación de porcentaje de eficiencia

El porcentaje de eficiencia, se obtiene segregando la temática o puntos de temática que no se han podido evaluar, es decir se reflejará en cifras lo que el perito indica como abstención de opinión; asimismo, de existir, se separará los puntos que no apliquen en la revisión. Finalmente, el porcentaje de eficiencia será el resultado de los puntos considerados en el peritaje más los

puntos que no se pudieron evaluar, siempre que la limitación del examen no guarde relación con imposibilidad del perito; este total será dividido entre el total de puntos de evaluación propuestos.

4.2.2.5.3. Interpretación de resultados

En base al porcentaje de eficiencia, se establecerán tres niveles de rendimiento: alto, medio – regular y bajo.

Tabla IV.I. Nivel de rendimiento de puntos de evaluación

	ESCALA (%)	NIVEL	DESCRIPCIÓN
NIVEL DE RENDIMIENTO	**100 – 65**	ALTO	Indica que el peritaje ha considerado la mayor parte de los puntos de revisión y la opinión del perito está acorde a la realidad de los hechos, a su vez los puntos no evaluados no influyen significativamente en los motivos de pericia solicitados por el cliente y/o juez.
	64 – 40	MEDIO - REGULAR	Indica que en la revisión no se han considerado aspectos relevantes que de haber sido evaluados modificarían parcialmente los resultados del peritaje; o en su defecto ha existido limitaciones provocando asimismo opiniones puntuales sobre la totalidad de los puntos de pericia.
	39 – 1	BAJO	Indica que los puntos de revisión evaluados han sido insuficientes o no ha existido disponibilidad de documentos de prueba para poder emitir opinión confiable por parte del perito.

En general, el peritaje deja de ser eficiente cuando en cuatro o más de los aspectos (son 6), existe al menos la mitad de puntos de revisión no evaluados, es decir; el nivel de aceptabilidad del peritaje, basado en el sistema de control propuesto, admite máximo la omisión de evaluación de hasta nueve puntos.

4.2.2.6. Verificar implementación de controles.

Se verificará la implementación de los controles resultantes, a través de las cédulas resumen de observaciones generadas durante el peritaje; además se incluirán los formularios de control de los procedimientos propuestos que hayan sido adoptados por La Cooperativa.

CAPÍTULO 5

5. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA DE CONTROL PARA REALIZAR PERITAJES INFORMÁTICOS A UN SISTEMA DE INFORMACIÓN ADQUIRIDO POR UNA COOPERATIVA DE AHORRO Y CRÉDITO: DESARROLLO

5.1. Peritaje Informático

5.1.1. Planeación

5.1.1.1. Identificar el motivo del peritaje

El motivo del peritaje corresponde a la petición expresa de una de las partes; la Cooperativa necesitó establecer el grado de cumplimiento del contrato de adquisición de software a la medida suscrito con el Proveedor.

5.1.1.2. Realizar una visita preliminar al área

Se realizó la visita preliminar, para lo cual se aplicó el cuestionario de visita previa **(Anexo 1),** el mismo que contiene aspectos generales de la contratación, responsabilidad de los empleados de la Cooperativa y cuestionamientos sobre el desarrollo del sistema.

Como resultado se obtuvo una visión general de lo ocurrido, causas atribuibles y posibles debilidades de control. Cabe indicar que el cuestionario fue aplicado al administrador del contrato; particular que limita el relevamiento, pero sin embargo constituyó una buena fuente para formarse una idea básica de lo sucedido.

5.1.1.3. Establecer los objetivos

En este caso, los objetivos de la pericia van de la mano con las necesidades del cliente, que es quien ha solicitado la prueba. Las interrogantes del cliente se traducen en los siguientes objetivos:

- Establecer el grado de cumplimiento por parte del proveedor de los plazos de ejecución comprometidos en el contrato; asimismo, estimar su razonabilidad.
- Determinar la razonabilidad y competitividad en el mercado del precio pactado en el contrato, y del valor por el que se podría demandar al proveedor por valores cobrados en exceso.
- Establecer el grado de cumplimiento por parte del proveedor de las condiciones técnicas estipuladas en el contrato; asimismo, dictaminar si el resultado entregado cumple las medidas de calidad técnica exigibles en contratos similares.

5.1.1.4. Determinar los puntos que serán evaluados

Para la consecución de objetivos, será necesario evaluar los puntos citados a continuación:

- Proceso de contratación.
- Existencia de contrato de diseño, desarrollo e implementación de software a la medida.
- Consistencia de las cláusulas, que sean suficientes y concernientes para el tipo de servicio a contratar.
- Existencia de soportes razonables sobre todos pagos realizados al proveedor a partir de la suscripción del contrato.
- Registros de comunicaciones enviadas y recibidas entre la Cooperativa y el Proveedor.
- Existencia de sistema instalado en las computadoras de la Cooperativa.
- Grado de implementación de los módulos del sistema.

5.1.1.5. Elaborar programas de trabajo

Para la realización del programa de trabajo se consideraron aspectos legales, aspectos procedimentales establecidos y mejores prácticas de operación de acuerdo a lo tratado en el capítulo 3.

5.1.1.6. Identificar y seleccionar las herramientas, instrumentos y procedimientos necesarios

De acuerdo al avance en el desarrollo del programa se concertará citas con los empleados responsables o relacionados con la documentación o el procedimiento a evaluar, sea este administrativo o técnico.

Se utilizarán cuestionarios, listas de verificación, cédulas de resumen, tablas de resultados, cuadros de registro de las debilidades o inconsistencias encontradas.

5.1.1.7. Asignar el valor de los honorarios a percibir

Este punto de la planificación fue considerado únicamente por motivos ilustrativos de la completitud de pasos a seguir en el peritaje; pero no fue asignado valor alguno para la realización del trabajo.

5.1.2. Ejecución

5.1.2.1. Realizar las acciones programadas

Consistió en seguir paso a paso el programa de trabajo elaborado **(Ver Anexo 2)**.

Como procedimientos generales se solicitó documentación sobre la intervención de los empleados en el contrato **(Ver Anexo 3),** y sobre los manuales de funciones, políticas y procedimientos existentes para la contratación de terceros, sin obtenerse documentación alguna de este último.

5.1.2.2. Aplicar las técnicas y herramientas

Durante el desarrollo del programa se aplicaron las siguientes técnicas:

- Inspección de registros físicos de la Cooperativa, documentación lógica y actividades y responsabilidades del personal y proveedores.
- Confirmación de datos obtenidos: licencias de software, pagos realizados.
- Cotización comparativa del precio de un proyecto similar a cargo de otras empresas.
- Comparación de opiniones: cuestionarios vs. situación real detectada.
- Revisión documental: actas de reunión, contrato, facturas, seguimiento e informes de fiscalización.
- Observación física.

Todas las técnicas de evaluación se apoyaron en el uso de cuestionarios y listas de chequeo **(Ver Anexos 4 al 10).**

5.1.2.3. Identificar y elaborar los documentos de las desviaciones encontradas

Se analizó la información recabada y se elaboraron los respectivos registros de las observaciones encontradas. Según la relación con la actividad afectada, se generó:

- Contratación de proveedores: **Anexos 11 y 12**
- Instrumentación del contrato: **Anexos 13 al 17**
- Cumplimiento del contrato: **Anexos 18 y 19**
- Monitoreo del desempeño del outsourcing: **Anexos 20 al 23**

5.1.2.4. Integrar el legajo de los papeles de trabajo

Consistió básicamente en ordenar los papeles secuencialmente e incluir referencias; por ejemplo, coordinar la relación entre el programa de trabajo, los incumplimientos detectados en cuestionarios, la cédula resumen (relevamiento) y el correspondiente registro de la observación en caso de existir.

La integración de los papeles en forma correcta y cautelosa aporta al momento de dar el enfoque completo de las observaciones, su análisis y redacción en el dictamen final.

5.1.3. Dictamen

5.1.3.1. Establecer situaciones detectadas

Por cada uno de los objetivos de la pericia, se presentarán las situaciones de desviación u omisión detectadas.

5.1.3.1.1. Sobre el cumplimiento de plazos y su razonabilidad

Se identificó:

- El proveedor no fue conciente de aspectos claves:
    1. La envergadura del proyecto, punto que conllevó a una valoración errónea en el tiempo y en el coste del proyecto.

2. La indefinición del proyecto: la Cooperativa ha tenido que dedicar muchas horas y esfuerzo para poder llegar a concretar varios aspectos críticos de la aplicación.

- La ausencia de documentación fiable que describa qué se ha hecho y cómo se ha planteado la implementación de las necesidades y objetivos implica:
    1. Dificultad para verificar la valía de los elementos contratados.
    2. Dependencia completa hacia el proveedor del sistema, ya que se desconoce lo que se ha hecho y cómo se ha hecho.

- Inexistencia de información sobre la administración del tiempo, su organización y control por parte del proveedor; razón suficiente para considerar muy poco, y muy mal planificado el proyecto.

- No existe evidencia del cobro a la compañía proveedora de la multa de 1 por mil del valor del programa por incumplimiento del plazo.

5.1.3.1.2. Razonabilidad del precio y pagos

Se identificó:

- De la documentación revisada, resulta evidente que el proyecto no fue correctamente presupuestado por el proveedor, independientemente

de que su importe fuera mayor o menor, no hay desglose de costes, ni previsiones que no fueran las de la entrega final y la de los pagos.

- No existió relación entre el desglose de pagos y las etapas del sistema que debían estar terminadas previo a cada desembolso.

- No se pudo evidenciar informes de fiscalización por parte de la Cooperativa, que sustenten los pagos realizados.

- Debido a que es práctica habitual en el sector informático el adquirir los equipos al mismo suministrador de los programas o viceversa; el hardware suministrado para la implementación del software fue sobrevalorado en relación al precio de mercado.

5.1.3.1.3. Sobre las condiciones técnicas y calidades

Se identificó:

- El contrato no hace referencia a la calidad del software, los métodos, normas o recomendaciones en el desarrollo de aplicaciones, mismas que deberían haberse estipulado de forma alguna; además no establece quién y cómo se debería evaluar la calidad.

- No se documentaron correctamente el análisis y el diseño de las aplicaciones, responsabilidad del proveedor es establecer la descripción de requerimientos y objetivos del proyecto.

- A pesar de haberse nombrado un administrador de contrato para tratar con el proveedor materias contractuales, se omitieron procedimientos generales previos a cualquier contratación, requisitos de documentación mínima que nos permita conocer el proveedor del servicio contratado, su experiencia, seriedad, etc..

5.1.3.2. Elaborar el dictamen final

En base a las preguntas de La Cooperativa, se redactará el cuerpo del informe pericial; citaremos las consideraciones, limitaciones en el alcance y conclusiones.

Grado de cumplimiento por parte del Proveedor de los plazos de ejecución comprometidos en el contrato suscrito el 28 de octubre de 2002; asimismo, estimación de su razonabilidad y si una compañía del nivel del proveedor puede, razonablemente, cumplirlos.

Conclusiones:

- El grado de cumplimiento de los plazos expresamente comprometidos por el proveedor es inaceptable desde cualquier perspectiva profesional.

- La estimación de lo razonables que pudieran haber sido los plazos dados resulta difícil en términos periciales, ya que exigiría un análisis funcional, prácticamente como si el perito fuera a hacer él mismo la aplicación. Pero se puede considerar que en unos cuatro meses, o no más de seis, un equipo de profesionales capaces puede concluir la informatización básica.

Aclaraciones sobre el alcance:

La lectura de los documentos disponibles lleva a estas conclusiones, pero no puede afirmarse nada sobre un software al que no se ha tenido acceso.

Determinación de la razonabilidad y competitividad en el mercado del precio pactado en el contrato, y del valor que se podría cargar al proveedor en caso de demanda.

Para determinar los precios de los desarrollos informáticos hay que tener en cuenta muchos factores en función de la naturaleza, complejidad y especialidad de la aplicación.

En general, los precios se reducen significativamente en las aplicaciones ‘paquetizadas’; mientras que, aumentan considerablemente cuando se trata de aplicaciones ‘a la medida’ de un solo cliente, aun cuando tengan aparentemente la misma complejidad.

- El precio pactado en el contrato parece razonablemente competitivo, y prueba de ello sería que por ese valor habría varias empresas informáticas que estarían dispuestas a realizar este mismo trabajo.

- El precio pagado por las compras de hardware por parte de la Cooperativa, para poder cumplir con el suministro de equipos para el desarrollo del software, es motivo de reclamación; de las cotizaciones realizadas, se detectó un exceso en el valor cobrado de aproximadamente $703; esto se debe particularmente a que es práctica habitual en el sector informático el adquirir los programas al mismo suministrador del hardware por evitar problemas, o viceversa.

Grado de cumplimiento por parte del proveedor de las condiciones técnicas y calidades estipuladas en el contrato; asimismo, deberá dictaminarse acerca de si el resultado entregado cumple las medidas de calidad técnica exigibles en contratos similares.

Conclusiones:

- No se documentó desde el principio correctamente el análisis y el diseño de las aplicaciones, causa principal del incumplimiento del contrato.

- Es imposible evaluar concluyentemente el grado de cumplimiento de condiciones técnicas y calidades estipuladas en el contrato sin haber sido expresamente pactadas, y menos aun sin haber podido tener acceso por vía normal al software cuya calidad y técnica se cuestiona.

- Las recomendaciones internacionales (ISO 9000-3) son tanto para comprador y vendedor de software, siendo el último quien tiene mayores responsabilidades y obligaciones.

5.2. Diseño e implementación del sistema de control

A continuación se desarrollan los pasos formulados en capítulo 4.

5.2.1. Identificar las diferentes temáticas que se debieron tener en cuenta a lo largo del peritaje.

5.2.1.1. Temáticas según el caso de pericia:

- Capacidad del Proveedor
- Contratante
- Consistencia del contrato

5.2.1.2. Temáticas inherentes a cualquier peritaje:

- Idoneidad del perito
- Oportunidad en los tiempos de respuesta
- Evidencia suficiente y consistente

5.2.2. Identificar los puntos de evaluación bajo cada temática.

Se identificaron como mínimo tres características – puntos medibles para cada temática.

5.2.2.1. Capacidad del Proveedor

- Experiencia
- Calidad comprobada
- Compromiso de servicio
- Formación académica suficiente

5.2.2.2. Contratante

- Identificación clara de necesidad
- Estabilidad financiera
- Constitución Legal
- Supervisión de contratistas

5.2.2.3. Consistencia del contrato

- Definición clara de objeto del contrato
- Veracidad de registro de firmas
- Honorarios pactados
- Tiempo estipulado
- Detalle de aspectos técnicos

5.2.2.4. Idoneidad del perito

- Independencia frente a las partes
- Nivel académico suficiente
- Experiencia
- Trayectoria

5.2.2.5. Oportunidad en el tiempo de respuesta

- Conocimiento del caso específico a peritar
- Estimación del periodo de revisión
- Planificación de actividades a realizar

5.2.2.6. Evidencia suficiente

- Técnica de relevamiento al personal
- Técnica de inspección
- Identificación de hallazgos detectados
- Técnica de confirmación

5.2.3. Asignar a cada punto, el o los documentos que sirvan para verificar su cumplimiento.

Se estableció en la cuarta columna del **Anexo 24** como mecanismo de comprobación, documentación avaladora de los puntos considerados.

5.2.4. Proponer los controles a implementar por cada punto.

Se definieron controles específicos para garantizar la existencia de documentación de respaldo de los procesos. **Ver Anexos 25 a 37.**

5.2.5. Establecer metodología de calificación por temáticas.

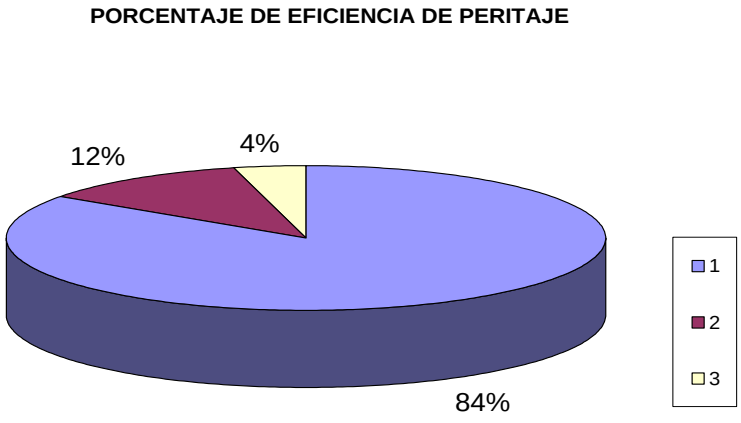
5.2.5.1. Aplicación de lista de chequeo de cumplimiento

En **Anexo 38** se presenta la lista de chequeo aplicada al peritaje.

5.2.5.2. Identificación de porcentaje de eficiencia

Como resultado del numeral anterior, en Anexo 38, el porcentaje de eficiencia fue del 88,47%. Del mismo 3,85% responden a abstención de opinión del perito por imposibilidad de evaluación por aspectos externos, y 84,62% al cumplimiento de los puntos de evaluación de la totalidad de las temáticas consideradas.

Figura 5.1. Diagrama pastel de porcentaje de eficiencia



Fuente: Resultados de lista de comprobación – Anexo 38

5.2.5.3. Interpretación de resultados

El porcentaje de eficiencia, se ubica en nivel de alto, es decir indica que el peritaje ha considerado la mayor parte de los puntos de revisión y la opinión del perito está acorde a la realidad de los hechos, a su vez los puntos no evaluados no influyen significativamente en los motivos de pericia solicitados por el cliente y/o juez.

5.2.6. Verificar implementación de controles.

En **Anexos 25, 26, 32, 35, 36 y 37** se indica la acción de seguimiento realizada y su fecha de culminación. Se omiten algunos anexos dentro de esta verificación de implementación, debido a que guardan relación con no conformidades por omisión de cláusulas específicas de los contratos, acción correctiva que se deja definida, pero que no es posible evaluar hasta una futura contratación de servicios de diseño y desarrollo de software. Además en **Anexos 35.1, 36.1 y 37.1** se proponen formatos de registros para complementar la definición de procedimientos.

CONCLUSIONES

1. Dentro del proceso de contratación de proveedores, no existió un concurso de ofertas consistente; la contratación se efectuó debido a sugerencias de un delegado. De la documentación existente sólo se pudo verificar una cotización, la misma que no correspondía a la empresa contratada.

2. Inexistencia de documentación del proveedor; no se encontró documentación mínima que permita conocer el proveedor del servicio contratado, su constitución real como compañía, todos los servicios que ofrece, su antigüedad en el medio, su responsabilidad, competencia y calidad en contratos anteriores, entre otras.

3. El contrato suscrito con el proveedor no establece relación entre los pagos a realizar y las etapas de entrega de cada módulo del sistema. Los pagos se realizarían cada mes y los módulos no tenían fecha de entrega pactada.

4. El contrato suscrito con el proveedor del software, omite algunas cláusulas de respaldo en caso de reclamaciones de terceras partes por derechos de autor, patentes, marcas registradas, entre otras; de

la misma forma no establece garantías por parte del proveedor sobre el derecho para conceder licencias del uso del sistema, sus limitaciones o prohibiciones.

5. La Cooperativa realizó una compra no documentada de equipos de computación al proveedor; en dicha compra se omitieron procedimientos de valoración de los activos a reemplazar y cotizaciones; las autorizaciones para desembolsos se realizaron de forma verbal. El monto invertido fue de US$ 3,743.04, y el valor aproximado cobrado en exceso US$ 703.

6. La multa de 1 por mil del valor del programa por incumplimiento del plazo, no fue cobrada; tampoco la garantía del 5% por fiel cumplimiento del contrato.

7. El contrato por diseño y desarrollo de software a la medida se canceló en un 80% de acuerdo a los pagos contemplados; los informes de fiscalización que debieron realizarse previo a cada desembolso, no se pudieron evidenciar.

8. Para que el diseño e implementación de un software resulten exitosos, se deben cumplir estrictamente con metodologías de análisis y diseño sobre los procesos, datos y estructuras; su omisión

conlleva retrasos, pérdidas de recursos, finalización de contratos e inclusive problemas legales.

9. El seguimiento y control oportuno de los proveedores, asesores y desarrolladores de sistemas garantiza las adquisiciones más adecuadas, al menor costo, y con la más alta calidad y servicio para las necesidades de cualquier tipo de empresa.

10. El peritaje informático como tal provee claridad ante los hechos o motivos de problemática acaecidos en el ámbito de informático, dictaminando, con una óptica neutral sobre lo que pudiera ser una reclamación infundada desde la perspectiva profesional.

11. El dictamen emitido ayuda también a los responsables de las áreas a tomar mejores decisiones respecto a los inconvenientes en el desempeño de actividades futuras de sistemas.

12. La disponibilidad de la información constituye el recurso más importante al momento de emitir una opinión completa sobre los puntos de pericia encargados.

13. La idoneidad del perito para analizar el caso propuesto es el segundo aspecto en importancia dentro de un peritaje, ya que se necesita

agudeza para definir la profundidad de las investigaciones en tal o cual punto de pericia.

14. El sistema de control basado en el uso de indicadores o temáticas sirvió para medir el grado de cumplimiento – efectividad del perito en el peritaje realizado.

15. El sistema de control implantado permitirá la verificación del cumplimiento de políticas, límites, procesos y procedimientos establecidos para la contratación y seguimiento de las actividades a cargo de terceros, así como para los procesos relacionados intervinientes en este caso de estudio.

RECOMENDACIONES

Se recomienda a La Cooperativa lo siguiente:

1. Cumplir con el procedimiento de contratación de terceros establecido, evitando así conflictos de intereses, vinculaciones y demás factores que puedan afectar a la contratación transparente de equipos de trabajo capaces para cumplir con el objetivo pactado.

2. Evaluar el nivel del proveedor, experiencia, formación, disponibilidad de la plantilla de trabajo, así como los recursos técnicos y las referencias de clientes y proyectos anteriores.

3. Aplicar normas de calidad ISO-ANSI para valorar el nivel (calidad) de las empresas a contratar, y no sólo al producto resultante, aunque no es frecuente certificar empresas desarrolladoras de software.

4. Contratar el anteproyecto y el presupuesto detallado de lo que se desea, a un buen profesional independiente, incluso cuando el proyecto va a ser realizado por una entidad diferente a la que éste proponga.

5. Someter los contratos de servicios de outsourcing de tecnología de información, previa la suscripción, a revisión de profesionales en materia

informática, así como de los futuros usuarios; de forma que se contemplen las cláusulas específicas necesarias para asegurar el buen cumplimiento del servicio, y se especifiquen todos los pormenores que son de conocimiento del personal operativo.

6. Asimismo, verificar la existencia de cláusulas de respaldo para La Cooperativa, en caso de incumplimientos parciales o totales del objeto del contrato; aclaraciones relativas a la inexistencia de responsabilidad laboral sobre los derechos y deberes previstos en el Código de Trabajo por parte de la contratante hacia los empleados de la contratista; abstenciones sobre emplear u ofrecer empleo a los empleados entre las partes; indemnizaciones por reclamos judiciales o extrajudiciales por infracciones a derechos de autor, patentes, marcas registradas o propiedad intelectual; o las que hubiere lugar de acuerdo al tipo de contrato que se suscriba.

7. Hacer efectivo el cobro de cualquier multa o garantía estipulada en los contratos de forma oportuna; en caso de detección de incumplimientos, asignar a personal con conocimientos legales para efectuar la actividad.

8. Asignar fiscalizadores para el servicio contratado, procurando que cuenten con la instrucción suficiente en la materia de su revisión, y las

capacidades comprobadas para dar seguimiento eficiente al servicio contratado.

9. Realizar informes preliminares de avances parciales, análisis y seguimiento sistemático del proyecto / servicio, incluyendo firmas de responsabilidad del fiscalizador(es), para asegurar que los temas vinculados con recursos pendientes, son resueltos, y para asegurar la ejecución efectiva de los planes de desarrollo.

10. Hacer cumplir el procedimiento de adquisiciones propuesto, desde la creación de la solicitud de compra hasta el archivo de documentación soporte, con el fin de mantener un registro cronológico de los desembolsos realizados, que sirva como respaldo ante cualquier reclamación interna o de terceros.

11. Acordar criterios internos para juzgar el producto o servicio contratado, es decir validar si es o no aceptable en función de lo especificado en el contrato.

12. Asignar a un responsable del levantamiento y actualización de los procedimientos, con el fin de que todos los empleados cuenten con una guía de consulta para realizar sus actividades diarias; o en su defecto

contratar asesoría para el mantenimiento de los manuales de procedimientos.

13. Definir los métodos y procedimientos de entrenamiento de usuarios para capacitar al personal en el seguimiento de la normativa creada por proceso durante esta revisión, de tal forma que se minimicen los eventos de riesgo a nivel operativo, ya que éstos se ven reflejados en incumplimientos en la planificación de cualquier tipo de proyectos.

14. La dirección de La Cooperativa debe encargarse de la existencia de una estructura de control interno idónea y eficiente, así como de su revisión y actualización periódica para mantenerla en un nivel adecuado acorde a los procesos vigentes.

15. La dirección de la Cooperativa debe manejar la inversión en Tecnología de Información, realizando un presupuesto anual que incluya la función de servicios de información; monitoreando los costos y justificándolos frente al beneficio que éstos generarán en el futuro.

GLOSARIO

Amnistía.- Mediante esta figura, el Poder Legislativo borra, por así decirlo, una infracción penal, anulando el proceso iniciado o las sentencias pronunciadas. Mientras el indulto solo conmuta o reduce la pena, la amnistía hace desaparecer el delito como si nunca se hubiere cometido. Se trata, más bien, de una medida de índole conciliatoria y de naturaleza política, y como tal, suele aplicarse más generalmente a los delitos denominados de orden político.

Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones.

Arbitraje.- Juicio arbitral. Procedimiento para resolver conflictos.

Cibernética.- Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología. La cibernética también se aplica al estudio de la psicología, la inteligencia artificial, los servomecanismos, la economía, la neurofisiología, la ingeniería de sistemas y al de los sistemas sociales. La palabra cibernética ha dejado de identificar un área independiente de estudio y la mayor parte de la

actividad investigadora se centra ahora en el estudio y diseño de redes neurales artificiales.

Confidencialidad (confidentiality).- Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.

Control.- Políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

Crimen.- Delito grave; un crimen es de mayor entidad que un delito.

Delito.- Acción u omisión voluntaria, castigada por la ley con pena grave. Quebrantamiento de la ley.

Deontológico.- Relativo a la deontología. Ciencia de los deberes.

Dilación.- Retardación o detención de una cosa por algún tiempo.

Diligencia.- Trámite de un asunto administrativo, y constancia escrita de haberlo efectuado. Cuidado en ejecutar una cosa. Prontitud, agilidad, prisa.

Disponibilidad (availability).- Propiedad de ser accesible y usable bajo demanda por una entidad autorizada.

Dolo.- Voluntad deliberada de cometer un delito a sabiendas de su ilicitud. En los actos jurídicos, voluntad maliciosa de engañar a alguien o de incumplir una obligación contraída.

Falta.- Infracción de naturaleza penal o administrativa que, por su escasa trascendencia, se sanciona con penas muy leves o una simple multa.

Gobierno de TI.- Estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el retorno sobre TI y sus procesos.

Ilícito.- Todo acto que se verifica contraviniendo la ley y que, por lo mismo, es motivo de castigo.

Incidente de seguridad.- Uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan la seguridad de la información.

Indulto.- Acto de gracia que la autoridad concede a un condenado por sentencia judicial y en virtud del cual se le exime de cumplir con la sentencia impuesta, o se le conmuta ésta por otra menos severa.

Infracción.- Acto cometido en contra de lo dispuesto legalmente, o faltando al cumplimiento de un compromiso libremente contraído.

Instalaciones.- Infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información.

Integridad.- Propiedad de salvaguardar la precisión y completitud de los recursos.

Legajo.- Conjunto de papeles reunidos pertenecientes a una misma materia.

Lego.- Falto de instrucción en determinado tema.

Licenciatarios.- El que concede a otra persona o entidad el derecho de usar aquella con fines industriales o comerciales.

Litigio.- Pleito. Disputa en un juicio.

Multa.- Consiste en una sanción en dinero o en especie, casi siempre pecuniaria y en beneficio del Estado o de cualquier entidad oficial o estatal facultada para imponerla. Cuando se multa a una persona se le condena a pagar cierta cantidad de dinero.

Objetivo de Control en TI.- Sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en un actividad de TI particular.

Partes litigantes.- Personas naturales o jurídicas que disputan en juicio sobre algo.

Pena.- Contenido de las sentencias o el castigo impuesto por un tribunal competente o juez, a un responsable por un delito o infracción penal; en consecuencia, esta pena puede afectar su libertad o su patrimonio, o ambas, o el ejercicio de algún o algunos derechos.

Principios contractuales.- Principios procedentes o derivados del contrato.

Probidad.- Integridad y honradez en el obrar.

Recusar.- Poner tacha legítima al juez, al oficial, o al perito que interviene en un procedimiento o juicio.

Rehabilitación.- Acto legal mediante el cual, una persona recobra la capacidad de volver a gozar de ciertos derechos de los cuales estaba privado por disposición de un juez o tribunal. Así, un preso al recuperar su libertad corporal adquiere a su vez su rehabilitación a sus derechos políticos.

Sanción.- En términos jurídicos, se entiende por sanción, la pena o represión impuesta al que en alguna forma ha faltado a la ley penal.

Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Tacha.- Falta o defecto. Culpa o censura.

Telemático.- Relacionado con las técnicas utilizadas para conectar las redes de comunicación y los materiales informáticos.

Tecnología de Información.- Conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información.

Ulterior.- Que se dice, sucede o se ejecuta después de otra cosa. Posterior, futuro, venidero.

Vicio.- Defecto moral en las acciones. Falsedad o engaño.

BIBLIOGRAFÍA

1. Alain Ambrosi, Valérie Peugeot y Daniel Pimienta; Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información (C & F Éditions, 2005)

2. Asociación de Ingenieros en Informática de Aragón
   http://www.aiia.es/modules.php?name=News&file=article&sid=15 - 16k

3. Caffaro Miguel Angel; Informática Profesional, publicación del Consejo Profesional en Ciencias Informáticas Año 17, Nº 87, (Mayo de 2003). Recuperado en agosto 29 de 2006.
   http://www.cpci.org.ar/newsletters/87/Pericia.ht- 22k

4. Caffaro Miguel Angel; Pericias Informáticas, REDI Revista Electrónica de Derecho Informático, ISSN: 1576-7124, (2001). Recuperado en noviembre 6 de 2006.
   http://publicaciones.derecho.org/redi/No._32_-_Marzo_del_2001/6

5. Centro de Estudios Monetarios Latinoamericanos; Banco de la República de Colombia; Metodología de Trabajo de Auditoría.
   http://www.cemla.org/pdf/aud-meto1.PDF

6. Centro de Ingeniería de Software e Ingeniería del Conocimiento, Instituto Tecnológico de Buenos Aires; Taller Pericias Informáticas; http://www.itba.edu.ar/capis/webcapis/talleres/pericias-informaticas.htm

7. Colegio Oficial de Ingenieros en Informática del País Vasco; Curso de Dictámenes y Peritajes Informáticos. http://www.coiie.org/formacion/cursos2006/Curso_Peritajes_2006.pdf

8. Comité Directivo de COBIT y El IT Governance Institute, (2002). COBIT – Objetivos de Control, Tercera Edición (ISBN: 1-893209-17-2) Páginas 25-30.

9. Concepto de peritaje. La prueba pericial. Los peritos en el proceso penal. Los peritos y los testigos. Objeto de la prueba pericial. Recuperado en noviembre 5 de 2006. http://www.monografias.com/New/2006-07-25.shtml - 53k - 28 Jul 2006

10. Corletti Estrada Alejandro; Análisis de ISO-27001:2005 breve resumen del estándar. www.shellsec.net/documentacion.php?id=21

11. Cuervo José; Delitos informáticos: Protección Penal de la Intimidad. Recuperado en septiembre 30 de 2006. http://www.informatica-juridica.com/trabajos/delitos.asp

12. Curso de peritajes informáticos organizado desde el CIIRM y auspiciado por la Escuela Práctica Tecnológica de Murcia. http://www.um.es/estructura/escuelas/ept/2004-2005-cursos.php#PERITAJES

13. De la Cadena Valenzuela Gilberto Douglas; Aspectos de controversia respecto al delito de peligro de contagio. Recuperado en agosto 5 de 2006. http://www.universidadabierta.edu.mx/Biblio/C/Cadena%20Gilberto-Controversia%20delito%20contagio.htm - 297k

14. Del Peso Navarro Emilio, Peritajes Informáticos (ISBN: 84-7978-497-0, Ed. Díaz de Santos, 2001)

15. Departamento de Sistemas Informáticos y Computación, Universidad Politécnica de Valencia; ISO 9000-3; recuperado en marzo 22 de 2008. http://www.dsic.upv.es/asignaturas/facultad/lsi/trabajos/102000.doc

16. Estándares IEEE para Ingeniería del Software perdidos por la web. Recuperado en marzo de 2008. http://www.navegapolis.net/content/view/583

17. Federación Nacional de Contadores del Ecuador; Normas Ecuatorianas de Auditoría (ISBN: 9978-966-48-X, Pudeleco Editores S.A., 2000) Páginas 161 -168.

18. Fleitman Jack, Evaluación Integral, (ISBN: 970-10-0445-0, McGraw-Hill, México, 2000). Páginas 92-97, 177-181.

19. García Sánchez Sergio Antonio; El peritaje informático, Revista de Ingeniería Informática del CIIRM. Recuperado en septiembre 30 de 2006. http://www.cii-murcia.es/informas/ene05/articulos/El_peritaje_informatico.html

20. Gómez Leopoldo Sebastián M.; Argentina: Marco normativo para el desarrollo de pericias informáticas, REDI Revista Electrónica de Derecho Informático Nº 42, Enero de 2002. Recuperado en noviembre 6 de 206. http://www.premium.vlex.com/doctrina/REDIRevista-Electrónica-Derecho-Informático/Argentina-Marco-normativo-desarrollo-pericias-informaticas/2100-122758,01.html

21. Gómez, L.S.M.; ”Actuaciones en Delitos Informáticos", Reporte Técnico, Tribunal Superior de Justicia, Poder Judicial del Neuquén, (1999).

22. Hachette Castell, Diccionario Enciclopédico (ISBN 84-7489-273-2, 1989)

23. IEEE Standars: acceso al texto completo de las normas IEEE. Recuperado en marzo de 2008. http://www.udc.es/biblioteca/castellano/internor.htm normas

24. Internacional Organization for Standarization. Recuperado en mayo de 2008. http://www.iso.org/iso/home.htm

25. Internacional Organization for Standarization, ISO/IEC 90003:2004. Recuperado en marzo de 2008. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35867

26. IEEE Std. Recuperado en marzo de 2008. http://members.fortunecity.es/jorgechip/IEEE1016.doc

27. Logotex, Enciclopedia Autodidáctica Océano, Volumen II (ISBN 84-7764-011-4, Grupo Editorial Océano, 1988)

28. López Óscar, Haver Amaya, Ricardo León; Informática forense: generalidades, aspectos técnicos y herramientas. http://www.urru.org/papers/RRfraude/InformaticaForense_OL_HA_RL.pdf

29. Martos Juan; El perito informático, ese gran desconocido. http://www.recoverylabs.com/prensa/original/2006/10_06_peritaje_informatico.pdf

30. Microsoft Corporation, Biblioteca Premium Microsoft Encarta 2006.

31. Multimedia University Cyberjaya; Faculty of Information Technology http://pesona.mmu.edu.my/~wruslan/SE2/Readings/

32. Muñoz Razo Carlos, Auditoría en Sistemas Computacionales (ISBN: 970-17-0405-3, Pearson Education, México, 2002). Páginas 185, 435, 529 - 537, 726.

33. Peritaje ppt. Recuperado en febrero 7 de 2008. http://www.it.uniovi.es/material/ telematica/proyectos/3-Peritajes.pdf

34. Peritaje Informático. Recuperado en julio 8 de 2006. http://www.audea.com

35. SRDI Servicio de Recuperación de Datos Informáticos; Peritaje Informático;
http://www.recuperadatos.net/peritaje_informatico.htm

36. Asesoría Informática, Fiscal y Contable TAI XXI; Perito informático - Peritaje informático. Recuperado en octubre 12 de 2006.
http://www.taixxi.com/contenidos/servicio/perito_informatico.htm

37. Prueba pericial informática. Recuperado en octubre 12 de 2006. http://www2.compendium.com.ar/juridico/peri2.html

38. Reglamento interno de peritos informáticos. Recuperado en octubre 29 de 2006.
http://www.cpcipc.org/reglamento.asp

39. Rol del contador/auditor en la aplicación de la justicia. (segunda parte)
http://www.interamericanusa.com/articulos/Auditoria/Rol-Cont-2.htm - 172k

40. Villalón Huerta Antonio; Códigos de Buenas Prácticas de Seguridad UNE-ISO/IEC 17799; Septiembre de 2004.
http://www.shutdown.es/ISO17799.pdf -

41. Vox, Diccionario Enciclopédico, Tomo IV (ISBN 84-7153-005-8, Bibliograf S.A., 1973.

42. Wikimedia Foundation, Inc., Sistema de control, Enero de 2008. http://es.wikipedia.org/wiki/Sistema_de_control

43. Wikimedia Foundation, Inc., IEEE, modificada por última vez el 9 abril de 2008. http://es.wikipedia.org/wiki/Computer_Society

ANEXOS