AUDITORÍA DE SISTEMAS
una visión práctica

UNIVERSIDAD NACIONAL DE COLOMBIA
SEDE MANIZALES
I.S.B.N 958-9322-66-2

© 2001 UNIVERSIDAD NACIONAL DE COLOMBIA SEDE MANIZALES

AUTOR:
ALONSO TAMAYO ALZATE
Administrador de Empresas
Esp. en Sistemas con énfasis en Diseño de Sistemas de Auditoría
Esp. en Computación para la Docencia
Profesor Asociado
Universidad Nacional de Colombia
Sede Manizales

REVISADO:
ALFONSO PIO AGUDELO SALAZAR
Ingeniero Electricista
Economista
Esp. en Sistemas con énfasis en Administración de Sistemas Informáticos
Esp. en Sistemas con énfasis en Diseño de Sistemas de Auditoría
Profesor Asociado
Universidad Nacional de Colombia
Sede Manizales

NESTOR DARIO DUQUE MÉNDEZ
Ingeniero Mecánico
Esp. en Sistemas con énfasis en Diseño de Sistemas de Auditoría
Profesor Asistente
Universidad Nacional de Colombia
Sede Manizales

IMPRESO:
Centro de Publicaciones
Universidad Nacional de Colombia
Sede Manizales

Julio de 2001
Octubre de 2002
Febrero de 2003
Primera Edición
CONTENIDO

PRÓLOGO ................................................................................................................................. 7

UNIDAD I. LA FUNCIÓN DE AUDITORÍA DE SISTEMAS

CAPÍTULO 1
CONCEPTUALIZACIÓN ............................................................................................................... 9

1.1 INTRODUCCIÓN .................................................................................................................... 9
1.2 AUDITORÍA DE SISTEMAS .................................................................................................... 9
1.3 OBJETIVOS DE LA AUDITORÍA DE SISTEMAS ............................................................... 10
  1.3.1 Objetivos Generales ........................................................................................................ 11
  1.3.2 Objetivos Específicos ...................................................................................................... 12
1.4 JUSTIFICACIÓN DE LA AUDITORÍA DE SISTEMAS ....................................................... 12
1.5 PERFIL DEL AUDITOR DE SISTEMAS ............................................................................. 14
1.6 CONTROL DE LOS SISTEMAS DE INFORMACIÓN .......................................................... 14
  1.6.1 El Control. Definición ..................................................................................................... 14
  1.6.2 Características del Sistema de Control ......................................................................... 14
  1.6.3 Clasificación de los Controles ...................................................................................... 15
  1.6.4 El Control en los Sistemas de Información ................................................................. 17
1.7 BIBLIOGRAFÍA ..................................................................................................................... 19

CAPÍTULO 2
PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS ................................................................ 21

2.1 INTRODUCCIÓN .................................................................................................................. 21
2.2 DEFINICIÓN ........................................................................................................................ 21
2.3 OBJETIVOS DE LA PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS ......................... 21
2.4 METODOLOGÍA DE PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS ...................... 22
2.5 PLAN DE AUDITORÍA DE SISTEMAS .............................................................................. 25
2.6 BIBLIOGRAFÍA ..................................................................................................................... 29
UNIDAD II. AUDITORÍA PARA APLICACIONES EN FUNCIONAMIENTO Y EN PROCESO DE DESARROLLO

CAPÍTULO 3
CUESTIONARIOS DE CONTROL INTERNO 31

3.1 INTRODUCCIÓN 31
3.2 CUESTIONARIO DE CONTROL INTERNO. DEFINICIÓN 31
  3.2.1 Cuestionario de control interno para las entradas a la aplicación 31
  3.2.2 Cuestionario de control interno para las salidas de la aplicación 33
  3.2.3 Cuestionario de control interno para el software del sistema 34
  3.2.4 Cuestionario de control interno para la seguridad en aspectos físicos de la aplicación 36
  3.2.5 Cuestionario de control interno para la seguridad en aspectos técnicos de la aplicación 36
  3.2.6 Cuestionario de control interno para controles organizacionales de la aplicación 38
  3.2.7 Cuestionario de control interno para el talento humano que interviene en la aplicación 39

3.3 BIBLIOGRAFÍA 42

CAPÍTULO 4
PROCEDIMIENTOS DE AUDITORÍA 43

4.1 INTRODUCCIÓN 43
4.2 PROCEDIMIENTOS DE CUMPLIMIENTO. DEFINICIÓN 43
  4.2.1 Entradas a la aplicación 43
  4.2.2 Salidas de la aplicación 44
  4.2.3 Software del sistema 44
  4.2.4 Seguridad en aspectos físicos de la aplicación 45
  4.2.5 Seguridad en aspectos técnicos de la aplicación 45
  4.2.6 Controles organizacionales de la aplicación 45
  4.2.7 Talento humano que interviene en la aplicación 46

4.3 BIBLIOGRAFÍA 47

CAPÍTULO 5
DISEÑO DE LOS PAPELES DE TRABAJO 49

5.1 INTRODUCCIÓN 49
5.2 PAPELES DE TRABAJO. DEFINICIÓN 49
5.3 OBJETIVOS DE LOS PAPELES DE TRABAJO 50
5.4 TIPOS DE PAPELES DE TRABAJO 50
  5.4.1 Archivo permanente 51
5.4.2 Archivo corriente.....................................................................................................................51
5.5 PROPIEDAD DE LOS PAPELES DE TRABAJO ........................................................................51
5.6 DISEÑO Y CONTENIDO DE LOS PAPELES DE TRABAJO ....................................................52
  5.6.1 En cuanto a su diseño...............................................................................................................52
  5.6.2 En cuanto a su contenido.........................................................................................................52
  5.6.3 Diseño sugerido de los papeles de trabajo...............................................................................53
5.7 BIBLIOGRAFÍA...............................................................................................................................57

CAPÍTULO 6
INFORMES DE AUDITORÍA DE SISTEMAS.....................................................................................59

  6.1 INTRODUCCIÓN ........................................................................................................................59
  6.2 INFORMES DE AUDITORÍA DE SISTEMAS. DEFINICIÓN ...................................................59
  6.3 OBJETIVOS DE LOS INFORMES DE LA AUDITORÍA DE SISTEMAS .................................60
  6.4 RECOMENDACIONES APLICABLES A LOS INFORMES DE AUDITORÍA DE SISTEMAS ............60
  6.5 TIPOS DE INFORMES DE AUDITORÍA DE SISTEMAS .........................................................61
    6.5.1 Informes abreviados .............................................................................................................61
    6.5.2 Informes extensos .................................................................................................................61
  6.6 ESTRUCTURA DE LOS INFORMES DE AUDITORÍA DE SISTEMAS ...................................62
    6.6.1 Informe de auditoría .............................................................................................................62
    6.6.2 Informe ejecutivo de auditoría ...............................................................................................63
    6.6.3 Manual del auditor ................................................................................................................63
    6.6.4 Manual técnico .....................................................................................................................64
    6.6.5 Manual de operación de la aplicación (Manual de usuario) ....................................................66
    6.6.6 Manual de procedimientos de la aplicación .........................................................................66
    6.6.7 Manual de funciones de la aplicación ................................................................................70
  6.7 BIBLIOGRAFÍA...........................................................................................................................67

UNIDAD III. AUDITORÍA AL CENTRO DE INFORMÁTICA

CAPÍTULO 7
ELEMENTOS TEÓRICOS Y PRÁCTICOS .....................................................................................69

  7.1 INTRODUCCIÓN .....................................................................................................................69
  7.2 OBJETIVOS DE LA AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA .....................69
    7.2.1 Objetivos Generales .............................................................................................................70
    7.2.2 Objetivos específicos ..........................................................................................................71
7.3 JUSTIFICACIÓN DE LA AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA ................................................................. 71
7.4 PLANEACIÓN DE LA AUDITORÍA PARA EL CENTRO DE INFORMÁTICA .................. 72
7.5 PROGRAMA DE AUDITORÍA DE SISTEMAS PARA EL CENTRO DE INFORMÁTICA .... 73
  7.5.1 Metodología a seguir ............................................................................................................... 74
  7.5.2 Alcance ................................................................................................................................... 74
7.6 CUESTIONARIO DE CONTROL INTERNO PARA SER APLICADO AL CENTRO DE INFORMÁTICA .................................................. 75
  7.6.1 Cuestionario de Control Interno para aspectos administrativos ........................................ 75
  7.6.2 Cuestionario de Control Interno para aspectos técnicos ...................................................... 81
  7.6.3 Cuestionario de Control Interno para aspectos de seguridad ............................................. 90
7.7 PROCEDIMIENTOS DE AUDITORÍA PARA SER APLICADOS AL CENTRO DE INFORMÁTICA ................................................................. 95
  7.7.1 Procedimientos de auditoría para aspectos administrativos ................................................ 95
  7.7.2 Procedimientos de auditoría para aspectos técnicos ........................................................... 97
  7.7.3 Procedimientos de auditoría para aspectos de seguridad ..................................................... 100
7.8 DISEÑO DE PAPELES DE TRABAJO ................................................................. 102
  7.8.1 Descripción detallada de los papeles de trabajo que componen el archivo permanente ..... 102
  7.8.2 Descripción detallada de los papeles de trabajo que componen el archivo corriente ..... 104
7.9 INFORMES DE AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA .......... 104
  7.9.1 Estructura del informe ejecutivo de auditoría al centro de informática .............................. 105
  7.9.2 Estructura del informe detallado de auditoría al centro de informática .............................. 106
7.10 BIBLIOGRAFÍA ......................................................................................................................... 106

ANEXOS .................................................................................................................................................. 109
Hasta hace pocos años, los datos en las empresas estaban orientados principalmente a alimentar sus sistemas contables, financieros, de inventarios, de producción, de talento humano y de ventas, pero en la medida que los negocios y las transacciones comerciales en el ámbito mundial se hicieron más competitivas y complejas, la información depurada, confiable y segura cobró más importancia, llegando a convertirse en un pilar clave para la toma de decisiones.

En nuestro medio la introducción de los sistemas de información se dio de manera paulatina, limitándose en un principio a la adquisición de hardware y software, y fueron contadas las empresas económicamente pudientes que empezaron a desarrollar sus programas con recursos propios y apoyadas en asesores externos, pero de poca o ninguna experiencia en el diseño de controles que las condujera a concebir aplicaciones integrales considerando a la Auditoría de Sistemas como parte inherente de los sistemas de información, criterio atribuible muy posiblemente a la incipiente formación del talento humano que inicialmente le correspondió laborar en el área, lo que ha traído como consecuencia que los controles aplicados se limiten en un alto porcentaje sólo a aquellos que brindan el software y el hardware proporcionado por las casas matrices.

Generalmente los primeros programas carecían de controles dentro de su estructura, puesto que no existía conciencia sobre la importancia de la seguridad, lo cual condujo a que los esfuerzos iniciales en esta materia se enfocaran básicamente hacia la implementación de controles físicos de acceso al sistema, protección de las instalaciones y equipos, y a garantizar la privacidad en el manejo de la información. Sólo en el presente, las empresas están empezando a reconocer la importancia y la necesidad de implementar mecanismos de control y es así como comienzan a surgir las primeras dependencias especializadas en esta área, aunque aún se carece en gran proporción de las debidas metodologías y herramientas que garanticen su operatividad y eficacia.

Actualmente la aplicación de las medidas de seguridad se ha difundido más ampliamente, así como su cobertura, siendo cada vez mayor el número de empresas que las ponen en práctica; el radio de acción de la seguridad es mucho más amplio y lo constituye el establecimiento de seguridades de todo tipo, definidas de la siguiente manera: actualización de equipos, desarrollo y actualización del software, mayor eficiencia en la inversión, la optimización de programas, la implementación de aplicaciones, el establecimiento de redes y comunicaciones, la confrontación y verificación, la simulación, la consulta periódica de bitácoras y el cambio de passwords, entre otros, se destacan como los procedimientos para evaluar mecanismos de seguridad de más corriente uso. La confiabilidad y la integridad se establecen como los beneficios más importantes derivados de la seguridad, considerándose en general, que éstos superan ampliamente las inversiones realizadas y centrándolas pautas en la capacitación y provisión de cargos de auditoría tanto en el sector público como en el privado.

Este libro tiene como propósito suministrar al lector una guía, sustentada sobre una base conceptual sólida, para llevar a cabo la función de Auditoría de Sistemas; para el efecto se ha agrupado la temática en tres unidades de la siguiente forma:
Unidad I. La Función de Auditoría de Sistemas. Tiene como fin ampliar el concepto de Auditoría de Sistemas exponiendo sus objetivos y justificación, estableciendo una terminología de referencia.

Unidad II. Auditoría para aplicaciones en funcionamiento y en proceso de desarrollo. El propósito que persigue esta unidad es mostrar paso a paso el desarrollo de la auditoría partiendo desde el diseño cuidadoso de los cuestionarios de control interno, que permiten obtener y analizar aquella información deseada y culminando con la presentación de las conclusiones y recomendaciones del proceso ejercido.

Unidad III. Auditoría al Centro de Informática. Se presentan aquellos aspectos tanto teóricos como prácticos: planeación, programas de auditoría, cuestionarios de control interno, procedimientos, diseño de papeles de trabajo y presentación de los informes de la auditoría de sistemas aplicables al centro de informática; temática que se ha desarrollado con especial empeño, dado lo neurálgico y trascendente que es el manejo de la información para la totalidad de las empresas o instituciones.

Lo más importante en este momento es crear conciencia sobre el rol fundamental de la auditoría y seguridad de sistemas dentro de la organización tanto a nivel de la función del talento humano, como de la participación de la misma en las diversas etapas de la adquisición de bienes informáticos y del desarrollo de proyectos de software.

Alonso Tamayo Alzate
UNIDAD I. LA FUNCIÓN DE AUDITORÍA DE SISTEMAS

CAPÍTULO 1

CONCEPTUALIZACIÓN

1.1 INTRODUCCIÓN

La dificultad en el manejo de grandes volúmenes de información, la necesidad de disponer de información íntegra, oportuna, segura y confiable, dio origen a la revolución informática, la cual ha generado una creciente dependencia para las empresas y usuarios en general, que se benefician diariamente de ella con el registro y procesamiento de operaciones; por consiguiente surge la imperiosa necesidad de ejercer control en éste campo y es a través de la Auditoría de Sistemas la encargada de estudiar, analizar y asesorar todo lo atinente al control del área de sistemas y los recursos involucrados en su desarrollo.

El propósito de este capítulo es ampliar el concepto de auditoría de sistemas, sus objetivos y justificación, estableciendo una terminología de referencia y familiarizando al lector con la temática a desarrollar en las próximas unidades.

1.2 AUDITORÍA DE SISTEMAS

Definición

Según la definición de Euripides Rojas¹, "La auditoría de sistemas es la parte de la auditoría interna que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de computadores; es decir, en estas evaluaciones se está involucrando tanto los elementos técnicos como humanos que intervienen en el proceso de la información".

También es conveniente conocer el concepto de José A. Echenique², que al respecto expone lo siguiente: "La auditoría en informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

² Echenique, José Antonio. Auditoria en informática. Pág. 16
La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo o de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información. Ello debe incluir los equipos de cómputo como la herramienta que permite obtener la información adecuada y la organización específica (departamento de cómputo, departamento de informática, gerencia de procesos electrónicos, etc.) que hará posible el uso de los equipos de cómputo".

Con base en las definiciones anteriores, se puede concluir que la auditoría de sistemas se encarga de la evaluación de todos aquellos aspectos relacionados con los recursos informáticos de la organización como son software, hardware, talento humano, funciones y procedimientos, enfocados todos ellos desde el punto de vista administrativo, técnico y de seguridad; y propende por prevenir a la empresa de aquellos riesgos originados por omisiones, errores, violaciones, actos mal intencionados, desastres naturales, etc., asesorando y proporcionando recomendaciones y sugerencias a nivel directivo para lograr un adecuado control interno en la empresa.

1.3 OBJETIVOS DE LA AUDITORÍA DE SISTEMAS

A continuación se exponen los objetivos que persigue la auditoría de sistemas, los cuales se presentan agrupados en objetivos generales y objetivos específicos, de la siguiente forma:

**FIGURA N° 1.1 DEFINICIÓN DE AUDITORÍA DE SISTEMAS**
1.3.1 Objetivos Generales

- Evaluar las políticas generales sobre planeación, ambiente laboral, entrenamiento y capacitación, desempeño, supervisión, motivación y remuneración del talento humano.

- Evaluar las políticas generales de orden técnico con respecto al software, hardware, desarrollo, implantación, operación y mantenimiento de sistemas de información.

- Evaluar las políticas generales sobre seguridad física con respecto a instalaciones, personal, equipos, documentación, back-ups, pólizas y planes de contingencias.

- Evaluar los recursos informáticos de la empresa con énfasis en su nivel tecnológico, producción de software y aplicaciones más comúnmente utilizadas.

- Asesorar a la gerencia y altos directivos de la empresa en lo relacionado con los sistemas de información, de tal forma que el proceso de toma de decisiones se efectúe lo más acertadamente posible.

- Conocer las políticas generales y actitudes de los directivos frente a la auditoría y seguridad de los sistemas de información y proceder a hacer las recomendaciones pertinentes.

- Efectuar un análisis sobre la concepción, implementación y funcionalidad de la seguridad aplicada a los sistemas de información.

- Analizar los componentes del costo involucrado en la sistematización de los diferentes procesos, así como evaluar los beneficios derivados de la misma.
1.3.2 Objetivos Específicos

- Evaluar el grado de intervención de la auditoría de sistemas en las etapas de desarrollo, implementación y mantenimiento de las aplicaciones.
- Evaluar las políticas y criterios para la adquisición y/o desarrollo del software.
- Evaluar los riesgos y fraudes de mayor incidencia al interior de la empresa.
- Examinar la documentación existente con respecto a los manuales de sistemas, usuario, operación, auditoría, funciones y procedimientos, para determinar su actualización y efectividad.
- Revisar los procedimientos existentes sobre planeación, ambiente laboral, entrenamiento y capacitación, desempeño, supervisión, motivación y remuneración del talento humano.
- Examinar los procedimientos existentes con respecto al software, hardware, desarrollo, implementación, operación y mantenimiento de los sistemas de información.
- Revisar los procedimientos existentes sobre seguridades físicas con respecto a instalaciones, personal, equipos, documentación, back-ups, pólizas y planes de contingencias.
- Constatar si el personal se encuentra capacitado para aplicar controles y procedimientos de seguridad.
- Comprobar si los planes de seguridad son evaluados periódicamente.
- Comprobar la participación de los usuarios durante las etapas de análisis, diseño y puesta en marcha de las diferentes aplicaciones.
- Comprobar si existe una adecuada segregación de funciones y su cabal aplicación.
- Evaluar la funcionalidad de la estructura orgánica del centro de informática.
- Revisar las políticas de ascensos, promociones y vacaciones del personal.
- Evaluar los procedimientos para captura, verificación y almacenamiento de los datos.
- Evaluar los procedimientos para asignación de claves de acceso, modificaciones, cancelaciones, etc.
- Revisar los estándares de producción y comprobar la calidad de la información producida.
- Verificar la programación de los mantenimientos a las aplicaciones

1.4 JUSTIFICACIÓN DE LA AUDITORÍA DE SISTEMAS

A continuación se destacan los aspectos más relevantes que ameritan la función de la Auditoría de Sistemas.

- A la par que la tecnología avanza, las empresas deben evolucionar y es allí donde los controles aplicados deben ser evaluados, para que sean consonantes con todos los cambios efectuados.
- Los sistemas de información apoyados en computadoras son susceptibles de irregularidades como fraudes, manejos indebidos, errores, omisiones, etc, lo que obliga a ejercer un control estricto en sus operaciones.
• La normatividad, regulaciones y legislación, tanto interna como externa a la empresa, obligan a efectuar las modificaciones necesarias a los sistemas de información, lo que de hecho desactualiza los controles aplicados, por eso es necesario revisar los controles existentes y ajustarlos de acuerdo a los nuevos procedimientos implantados.

• La reducida participación que tiene la auditoría de sistemas en la adquisición y/o actualización de bienes informáticos, recayendo la responsabilidad en auditores no experimentados con ésta tecnología, es la causa del bajo porcentaje de fiscalización especializada que se ejerce al respecto.

• El incipiente desarrollo de la auditoría de sistemas y los limitados recursos de todo orden destinados a la misma, han sido el factor predominante en nuestro medio y ha traído como consecuencia que los controles ejercidos se reduzcan en un alto porcentaje solo a aquellos que brindan el software y el hardware adquirido.

• La limitada concepción que se tiene sobre el alcance de la seguridad de los sistemas de información computarizados, que recae más que todo en las seguridades físicas, hace indispensable aumentar su radio de acción y control.

• El crecimiento de las empresas y la fuerte competencia a la que están sometidas, conduce a un incremento de sus actividades cotidianas, lo que obliga a planear y controlar sus desarrollos para que sean más competitivas.

• La poca o escasa documentación existente, en la mayoría de los casos desactualizada, es el factor predominante en gran parte de las empresas de nuestro medio.

• Los planes de contingencias son muy limitados en cuanto a su alcance, y preferencialmente se ocupan de aspectos relacionados con el empleo de respaldos y la toma de pólizas de seguros, desatendiendo otros elementos atinentes al software, hardware y talento humano, que tienen profunda incidencia dentro de la auditoría.

FIGURA 1.3 JUSTIFICACIÓN DE LA AUDITORÍA DE SISTEMAS.
1.5 PERFIL DEL AUDITOR DE SISTEMAS

Para poder desempeñar adecuadamente la función de auditoría de sistemas, el auditor debe ser un profesional integro, poseedor de excelentes capacidades académicas, éticas y morales, tener conocimiento suficiente y experiencia en aspectos informáticos a nivel de hardware, software, comunicaciones, en análisis, diseño, puesta en marcha y mantenimiento de sistemas de información.

Esta formación es necesaria y así lo contempla la Guía Internacional de Auditoría N° 15. Auditoría en un ambiente PED. párrafos 4 y 5 que dice:

Párrafo 4. "Cuando se audita en un ambiente PED, el auditor debe tener conocimiento suficiente sobre hardware, software y sistemas de procesamiento en computador, para planear el trabajo y entender como afecta al PED, el estudio y evaluación del control interno y la aplicación de los procedimientos de auditoría, incluyendo técnicas de auditoría con ayuda del computador".

Párrafo 5. "El auditor debe también tener conocimiento suficiente de PED para implementar los procedimientos de auditoría en función del enfoque de auditoría que en particular se adopte".

1.6 CONTROL DE LOS SISTEMAS DE INFORMACIÓN. Introducción

Una de las razones fundamentales que justifican la aplicación del control en el área de informática se debe a la creciente dependencia de las industrias y empresas de producción, servicios y educación, tanto del sector público como privado, en los equipos de computación, en el software y en el procesamiento de la información, debido a que el uso de las computadoras acarrea riesgos de errores, omisiones, fraudes y otros sucesos adversos, que ameritan su permanente control y supervisión en mayor grado a los procesos que se llevan manualmente, para garantizar la confiabilidad, confidencialidad y seguridad de los sistemas de información.

1.6.1 El Control. Definición

Es el conjunto de normas, técnicas, acciones y procedimientos que interrelacionados e interactuando entre sí con los sistemas y subsistemas organizacionales y administrativos, permite evaluar, comparar y corregir aquellas actividades que se desarrollan en las organizaciones, garantizando la ejecución de los objetivos y el logro de las metas institucionales.

El Control actúa sobre las personas, cosas, situaciones específicas, fuentes de información y organizaciones, las cuales requieren con urgencia el diseño de estrategias que le permitan controlar y corregir los resultados de sus actividades.

1.6.2 Características del Sistema de Control

- El Control debe ser ejecutado frecuentemente para que permita identificar las desviaciones a tiempo y poder tomar las acciones correctivas oportunamente.
Debe ser económico, es decir, los beneficios que arroje deben ser superiores a los costos de implantación y mantenimiento del sistema. Entre más detallada sea la información recopilada, más oneroso resultará el Control.

El Control se debe fundamentar en datos verídicos para evitar apreciaciones subjetivas.

El proceso de Control debe corresponder a una planeación tal, que permita conocer la magnitud de la acción correctiva necesaria.

El control debe ser en lo posible, sencillo, comprensible y adaptativo, y no debe entorpecer el desarrollo normal de la empresa.

1.6.3 Clasificación de los Controles

Los Controles se pueden clasificar en Controles Internos y Controles Externos.

**Control Interno**

Es aquel proceso que se ejerce internamente en las organizaciones y es impulsado por las directivas, administradores y demás personal que está vinculado a ella, el cual posee la suficiente ética y moral, así como formación académica, que le amerite credibilidad a sus hallazgos y conclusiones y tiene como propósito lograr el cumplimiento de los objetivos institucionales.

**Control Externo**

Es aquel ejercido por personal ajeno a la organización y su propósito es establecer en que medida, los resultados alcanzados por las entidades o personas sujetas al control, satisfacen las metas y objetivos trazados en las políticas, planes, programas y propósitos fijados por la administración.

Considerando la importancia y actualidad del tema, se presenta parcialmente y a continuación la normatividad impartida por el estado, reseñando al respecto:

La Ley 87 de 1993 en su artículo 1, define el Control Interno como: "Se entiende por Control Interno el sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

El ejercicio del Control Interno debe consultar los principios de igualdad, moralidad, eficiencia, economía, celeridad, imparcialidad, publicidad y valoración de costos ambientales. En consecuencia, deberá concebirse y organizarse de tal manera que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos existentes en la entidad, y en particular de las asignadas a aquellos que tengan responsabilidad del mando.

PARAGRAFO. El control Interno se expresará a través de las políticas aprobadas por los niveles de dirección y administración de las respectivas entidades y se cumplirá en toda la escala de la estructura
administrativa, mediante la elaboración y aplicación de técnicas de dirección, verificación y evaluación de regulaciones administrativas, de manuales de funciones y procedimientos, de sistemas de conformación y de programas de selección, inducción y capacitación de personal."

NORMAS CONSTITUCIONALES Y LEGALES

OBJETIVOS
- PLANES
- MÉTODOS
- PRINCIPIOS
- NORMAS
- PROCEDIMIENTOS
- MECANISMOS DE VERIFICACIÓN
- EVALUACIÓN

ENTIDAD

ACTIVIDADES
- OPERACIONES
- ACTUACIONES
- ADMON. DE LA INFORMACIÓN
- RECURSOS

ORGANIZACIÓN

FIGURA 1.4 SISTEMA DE CONTROL INTERNO

Los Controles Internos se asimilan por lo general a aquellos que están orientados fundamentalmente a procurar los medios para que las operaciones se ejecuten en las empresas o instituciones de acuerdo con las normas, políticas y procedimientos establecidos por la alta dirección.

El Sistema de Control Interno comprende un conjunto integrado por todos los planes, métodos, normas y procedimientos que adopta la administración para coadyuvar al logro de los objetivos institucionales, asegurar la conducción ordenada y eficiente de la entidad, prevenir fraudes y errores, salvaguardar los activos y bienes, garantizar la correcta aplicación de los registros financieros, administrativos y técnicos y preparar oportunamente los informes necesarios para asegurar la marcha normal de la organización.

Ley 87 de 1993. Artículo 4. Elementos para el Sistema de Control Interno. "Toda entidad bajo la responsabilidad de sus directivos debe por lo menos implementar los siguientes aspectos que deben orientar la aplicación del Control Interno:

a) Establecimiento de objetivos y metas tanto generales como específicas, así como la formulación de los planes operativos que sean necesarios.
b) Definición de políticas como guías de acción y procedimientos para la ejecución de los procesos.
c) Adopción de un sistema de organización adecuado para ejecutar los planes.
d) Delimitación precisa de la autoridad y los niveles de responsabilidad.
e) Adopción de normas para la protección y utilización racional de los recursos.
f) Dirección y administración del personal conforme a un sistema de méritos y sanciones.
g) Aplicación de las recomendaciones resultantes de las evaluaciones del control interno.
h) Establecimiento de mecanismos que faciliten el control ciudadano a la gestión de las entidades.
i) Establecimiento de sistemas modernos de información que faciliten la gestión y el control.
j) Organización de métodos confiables para la evaluación de la gestión.
k) Establecimiento de programas de inducción, capacitación y actualización de directivos y demás personal de la entidad.
l) Simplificación y actualización de normas y procedimientos."

El titular de una entidad tiene la responsabilidad de establecer y mantener un adecuado sistema de control interno, le compete además, velar para que el sistema funcione correctamente. Cada funcionario es responsable ante su superior inmediato del control interno en su área de competencia, recayendo la responsabilidad del control interno en el nivel jerárquico más alto de la organización.


1.6.4 El Control en los Sistemas de Información

El Control en los sistemas computarizados propende porque los datos sean un fiel reflejo de la realidad, que sean exactos, oportunos, suficientes; que durante su procesamiento no se vean afectados por pérdida, omisión o redundancia, que proporcione la información necesaria y que sea de utilidad para futuros procesos y consultas.

Los Controles en los Sistemas de Información se pueden clasificar en Controles Generales, Controles Operativos y Controles Técnicos.

Controles Generales

Son aquellos controles ejercidos sobre las actividades y recursos comprendidos en el desarrollo de los Sistemas de Información e implica procesos de planeación, definición clara y precisa de metas y
objetivos institucionales, definición de valores de la organización, políticas, procedimientos, estándares, gerencia participativa, apertura a la comunicación, desarrollo de equipos de mejoramiento continuo, programas de capacitación y entrenamiento, etc.

**Controles Operativos**

Son controles diseñados, desarrollados e implementados para sistemas específicos, buscando garantizar con ellos que todas las operaciones sean autorizadas, registradas y procesadas de una manera completa, exacta y oportuna y tiene que ver con control y organización de proyectos, control de flujos de información, revisiones del diseño del sistema, administración de bases de datos, controles de cambios a programas, bitácoras de cambios, mantenimiento y documentación, control de programas, reportes varios, diseño y control de formatos, comunicaciones, etc.

**Controles Técnicos**

Tiene que ver con la tecnología de la información como son los controles de operación del hardware, seguridad sobre los sistemas de información, integración de los sistemas de información, reporte de fallas, control de usuarios, restricción de accesos a datos, archivos y programas; utilización de hardware, controles lógicos del sistema, sistemas operativos, sistemas de seguridad, respaldo y confidencialidad, control de acceso al sistema, sistema de mantenimiento, planes de contingencia, etc.

Estos controles a su vez pueden ser **Preventivos, Detectivos o Correctivos**.

**Controles Preventivos**

Son aquellos controles que están involucrados dentro de los procesos y tienen como propósito evitar la ocurrencia y frecuencia de desviaciones. Sus costos son muy económicos.
Controles Detectivos

Independientemente de que tan buenos y efectivos sean los controles preventivos, siempre ocurren errores y se necesitan mecanismos de detección. Los controles detectivos son aquellos que se activan una vez que se registra la ocurrencia de la desviación y tienen como propósito avisar a las personas involucradas en el proceso, para que estén vigilantes debido a la existencia de un problema.

Controles Correctivos

Tienen como propósito ayudar en la corrección de aquellos errores o desviaciones detectadas.

Es muy difícil que la aplicación de los Controles Preventivos sea suficiente por sí mismos, por lo general se hace necesario tomar acciones correctivas, las cuales resultan muy costosas puesto que implica mucha dificultad y tiempo hacerle adaptaciones a una aplicación en funcionamiento para corregir sus inconsistencias; caso contrario sucede cuando se hace un minucioso análisis de los Controles Preventivos que demanda la aplicación o el sistema a ser diseñado e implementado.

1.7 BIBLIOGRAFÍA

I Simposio Internacional y VI Colombiano de controles, seguridad y auditoría de sistemas. ACDAS. 1991.
www.dorado.une.edu.ve/biblio/auditoria
www.isaca.org
CAPÍTULO 2

PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS

2.1 INTRODUCCIÓN

Las fallas en los Sistemas de Información han causado grandes trastornos en la organización y provocado conflictos entre individuos, secciones y/o departamentos. Cuando un sistema de información computarizado presenta inconsistencias o no tiene buena acogida por parte de los usuarios, provoca que se vuelva difícil desarrollar nuevos sistemas en el futuro, ocasionando para la empresa u organización, la pérdida de los beneficios que un sistema de información bien estructurado, diseñado y operado, trae consigo.

Por eso se hace necesario auditar todos estos procesos apropiadamente y para lograrlo se requiere de una adecuada planeación de la auditoría a realizar, lo que implica eficiencia y rigurosidad en su desarrollo, de tal manera que no se omita algún aspecto fundamental durante la realización del trabajo y que éste sea efectuado con eficiencia y eficacia, además debe optimizar recursos de todo orden como técnicos, humanos, económicos y logísticos, entre otros.

2.2 DEFINICIÓN

La planeación de la Auditoría de Sistemas debe entenderse como la proyección del trabajo de auditoría, definiendo su norte e indicando las pautas a seguir para lograr su desarrollo, por lo tanto debe responder a los siguientes interrogantes: Qué se debe hacer?, Qué aspectos se van a auditar?, Cuándo se debe hacer?, Cómo se va a realizar?, Qué recursos demandará?, De qué recursos se dispone?, cuestionamientos que de ser respondidos adecuada y oportunamente, conducen a la optimización de recursos, evitando la improvisación y desfases en la estimación.

2.3 OBJETIVOS DE LA PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS

A continuación se presentan los objetivos más relevantes de la planeación de la Auditoría de Sistemas:

- Brindar un plan que oriente el desarrollo de la auditoría de sistemas mediante la identificación de requerimientos, de tal forma que contribuya eficiente y eficazmente en la realización de todas las actividades, minimizando costos y evitando duplicidad de esfuerzos.
• Comparar las actividades o tareas ejecutadas con las actividades proyectadas, retroalimentando el sistema mediante el análisis de las desviaciones encontradas y determinando sus posibles causas, para posteriormente realizar los ajustes necesarios.

• Comprometer a los directivos de la empresa con su desarrollo, asignación de recursos y puesta en marcha de la función de auditoría.

• Suministrar información consistente, actualizada, permanente y necesaria, propiciando el desarrollo armónico de la auditoría de sistemas.

• Propender por la optimización de recursos técnicos, humanos, económicos, logísticos y tiempo.

• Evitar la improvisación.

![Diagrama de objetivos de planeación de la auditoría de sistemas](image)

**FIGURA 2.1 OBJETIVOS DE LA PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS**

### 2.4 METODOLOGÍA DE PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS

No existen parámetros precisos que nos guíen en el desarrollo de un proyecto de auditoría de sistemas; en realidad cada proyecto debe administrarse con una estrategia diferente según sea su dimensión, alcance y nivel de riesgo, y es la falta de planeación la causa principal de los fracasos, retrasos, incumplimientos, incremento de costos y la poca calidad en las auditorías desarrolladas; para evitar estos problemas se requiere de una planeación cuidadosa y para lograrlo es fundamental que el auditor conozca la empresa del cliente que va a auditar, y entre más familiarizado esté con ella mejor.
aún. Es así como el SAS N° 22 Au 311 indica "La planeación adecuada incluye que el auditor adquiera la comprensión de la naturaleza operativa del negocio, su organización, la ubicación de sus instalaciones, los productos vendidos o servicios prestados, su estructura financiera, las operaciones relacionadas con otros, los métodos de remuneración y muchos otros asuntos".

Aunque la realidad nos lleva a concluir que por mucho que el auditor conozca la empresa del cliente, no poseerá la profundidad suficiente que pudieran tener los funcionarios y directivos que llevan vinculados a ella durante largos períodos; pero lo importante en este caso es tener el conocimiento necesario que permita identificar aquellos elementos o factores que incidirán en la planeación, desarrollo y ejecución de la auditoría y queda ratificado en la Guía Internacional de Auditoría N° 4. Planeación, párrafo 7 que dice: "El auditor necesita poseer cierto nivel de conocimiento de la industria y el negocio del cliente, que le permita identificar los eventos, transacciones y prácticas que, a su juicio, puedan tener un efecto significativo sobre la información financiera".

El objetivo de esta etapa consiste en recopilar la mayor cantidad de información relevante sobre la empresa, la cual servirá para formular el plan y posteriormente como instrumento para el desarrollo y ejecución de la auditoría. Esta información debe estar relacionada con: (ver anexo N° 1).

- Características generales de la empresa.
- Descripción de recursos informáticos relacionados por áreas, tanto a nivel de software como a nivel de hardware.
- Conceptos atinentes a la auditoría.

Para una efectiva planeación, es necesario obtener la información correspondiente en forma selectiva a través de entrevista personal, observación, encuesta y muestreo, entre otras. La entrevista personal es un método muy efectivo que permite la exitosa obtención de los datos, dependiendo de la habilidad que tenga el entrevistador para ganarse la confianza del entrevistado, logrando de esta manera familiarizarse con el entorno que rodea el tema en estudio.

Una forma de recolectar la información requerida consiste en solicitar que se responda a un cuestionario previamente elaborado, que puede obedecer al siguiente esquema:

- Solicitar y analizar la estructura orgánica de la empresa.
- Descripción del hardware (configuración) y su distribución dentro de la empresa
- Breve descripción de las distintas aplicaciones en funcionamiento.
- Breve descripción de las aplicaciones pendientes de ser computarizadas.
- Se ha involucrado al personal del área en alguna de las etapas del desarrollo del software? Si es así, explicar su participación.
- Las aplicaciones en funcionamiento incluyen conceptos de auditoría de sistemas? Si es así, explique cuales?
• El área en estudio ha sido objeto de auditoría de sistemas (interna o externa)? Si es así, con qué periodicidad se ha efectuado?
• Tiene algunas sugerencias para el mejoramiento del flujo de información actual?
• Piensa que algunos de los informes actuales son redundantes?
• La información actual le permite tomar decisiones?
• Requiere de un acceso más rápido a su archivo de información o base de datos?
• Se le presenta entramiento en algunos procesos?
• Está de acuerdo con los reportes producidos por el computador?

Es importante hacer observaciones de la ejecución de las tareas realizadas por los empleados, con el propósito de complementar la información recibida a través de la entrevista personal, además sirve como punto de control para verificar si la información proporcionada por el trabajador coincide con los hechos observados.

Resulta muy conveniente tener en cuenta que al momento de realizar las observaciones, se debe hacer con especial discreción e informalidad, de manera que no altere el desenvolvimiento normal de la actividad observada.

La encuesta es un método de uso frecuente, y puede llegar a un volumen amplio de personas; pero requiere de una buena planeación, diseño y crítica antes de ser aplicada, para que los resultados sean los esperados. La encuesta se puede realizar a través de correo, entrevistas personales, encuestas telefónicas, etc.

Cuando se dispone de poco tiempo para obtener la información o hay limitación de recursos económicos, entonces no se pueden entrevistar o encuestar a todas las personas que se desean, por lo tanto se deben aplicar técnicas estadísticas de muestreo, que permitan realizar observaciones al azar y seleccionar aleatoriamente aquellos datos que puedan proporcionar información tan valiosa como si se hubiera efectuado un censo.
Luego de culminar la etapa de recolección de información, el auditor habrá adquirido un amplio conocimiento sobre la empresa a auditar, facilitando la comunicación e intercambio de ideas y opiniones con sus funcionarios y a su vez, creando un ambiente propicio para desarrollar todas las actividades de auditoría requeridas.

2.5 PLAN DE AUDITORÍA DE SISTEMAS

Para poder realizar una auditoría efectiva, el auditor debe determinar los requisitos tanto legales como técnicos, para definir adecuadamente en el plan que aspectos o actividades serán evaluados. Según la Guía Internacional de Auditoría N° 15 Auditoría en un ambiente PED, contempla varios puntos que deben ser tenidos en cuenta, así:

Párrafo 7 "El auditor debe reunir información sobre el ambiente PED que sea relevante para el plan de auditoría, incluyendo información sobre:

• Como está organizada la función PED y el grado de concentración o distribución del procesamiento por computadora a través de la entidad.
• El hardware y software de computación usados por la entidad.
• Cada aplicación significativa procesada por el computador, la naturaleza del procesamiento (por ejemplo, lotes, en línea) y las políticas de conservación de datos.
• Implementación en proyecto de nuevas aplicaciones o modificaciones a las aplicaciones existentes."

Párrafo 8 "En la consideración de su plan general el auditor debe tomar en cuenta asuntos tales como:

• Determinación del grado de confianza, si es el caso, que espera depositar en los controles PED en su evaluación global del control interno.
• Planeación del cómo, dónde y cuándo serán revisadas las funciones PED, incluyendo la programación de expertos PED en donde sea aplicable.
• Planeación de procedimientos de auditoría usando técnicas de auditoría con ayuda del computador"

Para la consolidación de estos factores, es útil y práctico preparar un programa que básicamente debe contener los siguientes pasos:
A continuación se presenta una breve descripción de cada uno de los pasos:

1. *Objeto de la auditoría:* Se debe determinar con suma claridad que tipo de auditoría se va a realizar, por ejemplo, auditoría para aplicaciones en funcionamiento, auditoría para aplicaciones en desarrollo, auditoría al centro de informática, etc.

2. *Soporte legal:* Es necesario conocer la normatividad tanto interna como externa, así como los procedimientos y reglamentos que afectan a la empresa, para lograr un conocimiento más amplio de ella y de esta forma poder proyectar el plan más eficientemente.

3. *Alcance:* El auditor es quien determina el alcance de la auditoría que va a realizar, de acuerdo a las condiciones que se presentan en el momento y a las normas, regulaciones, extensión y complejidad que la cobija. Por ejemplo, a continuación se propone un esquema que se debe cubrir cuando se va a

*Objeto de la auditoría.
* Soporte legal.
* Alcance.
* Metodología a aplicar.
* Tiempo estimado de realización.
* Conformación del equipo auditor.
* Lugar donde se desarrollará la auditoría.
* Recursos logísticos y técnicos necesarios.
* Cronograma de actividades.
auditar aplicaciones en funcionamiento y aplicaciones en desarrollo, el cual se espera que sirva como punto de referencia, más no como una camisa de fuerza.

Con respecto a las Aplicaciones en Funcionamiento se debe realizar:

* Análisis técnico - administrativo, que incluya: Análisis de riesgos, análisis de controles existentes, análisis de controles requeridos a programas, análisis de controles de acceso al sistema, evaluación del manual técnico, evaluación del manual del usuario, sugerencias sobre tareas y funciones de la aplicación, sugerencias sobre accesos y procedimientos de la aplicación.

* Desarrollo del software de auditoría, que incluya: Desarrollo e implementación de programas monitor, elaboración del manual técnico, elaboración del manual del auditor, entrega del sistema monitor y capacitación.

Como se puede apreciar, parte del alcance lo constituye el desarrollo de software de auditoría, dado que en la mayoría de los casos no existe o no cumple con las expectativas de control requeridas por la empresa; y es así como lo estipula la Guía Internacional de Auditoría N° 16. Técnicas de Auditoría con ayuda del computador, que en su numeral 5 dice: "Los programas escritos para propósito específico son programas de computación diseñados para ejecutar tareas de auditoría en circunstancias específicas. Estos programas pueden ser preparados por el auditor, por la entidad o por un programador externo contratado por el auditor. En algunos casos, los programas existentes en la entidad pueden ser usados por el auditor en su estado original o modificado, porque puede ser más eficiente que desarrollar programas independientes".

Cook J., W. expresa al respecto: "En algunas firmas de auditoría se utilizan equipos de especialistas en auditoría del PED para evaluar el control interno y dirigir algunos procedimientos para la revisión de clientes que usan sistemas computarizados. Otras firmas se esfuerzan en familiarizar a todos los integrantes del equipo de auditoría con los sistemas de PED con el fin de que un solo equipo de auditoría lleve a cabo la totalidad de la revisión. Ambos enfoques tienen sus méritos y, si se ponen en práctica, con propiedad satisfacen los requisitos de las normas de auditoría generalmente aceptadas".

Con respecto a las Aplicaciones en Desarrollo, se debe realizar:

* Análisis del sistema, que incluya: Descripción global del sistema, marco de referencia legal y funcional, análisis de riesgos, análisis de controles existentes, análisis de controles requeridos, análisis de controles de acceso al sistema.

* Diseño del sistema, que incluya: Diagrama del sistema, descripción de las estructuras de datos, forma de procesamiento, planteamiento de soluciones alternas, definición del plan de pruebas.

* Documentación del Sistema, que incluya: sugerencias al manual técnico, sugerencias al manual del usuario, sugerencias sobre tareas y funciones, sugerencias sobre accesos y procedimientos.

3 Cook, J. W. Auditoría. Pag. 373
4. **Metodología a aplicar:** Conforme se trate de aplicaciones en funcionamiento o aplicaciones en desarrollo, se deben definir los pasos a seguir para llevar a cabo la auditoría, como son: diseño de cuestionarios de control, diseño de papeles de trabajo, definición de procedimientos de auditoría y preparación de informes.

5. **Tiempo estimado:** Se debe hacer un estimativo del tiempo requerido para auditar cada aplicación considerando la complejidad, tamaño de la aplicación, experiencia del equipo auditor y recursos disponibles; por lo tanto, es conveniente que se asigne el tiempo en horas que demandará cada actividad para su ejecución.

Para el efecto se sugiere utilizar una matriz para llevar a cabo esta actividad en donde se ubicarían las actividades a desarrollar como las filas de la matriz y el nombre de cada aplicación se colocaría en las columnas de la matriz. Se ha incluido una fila que se ha denominado "Conocimiento - ambientación", cuyo propósito específico es asignar un tiempo prudente para que el equipo auditor se familiarice con la normatividad, códigos, reglamentaciones, controles, auditorías previas, etc, de la empresa y particularmente de cada aplicación; al final se dispone de una fila adicional para totalizar los tiempos demandados para auditar cada una de las aplicaciones. Este procedimiento es aconsejable llevarlo a cabo tanto para las aplicaciones en funcionamiento, como para las aplicaciones en desarrollo (ver anexo N° 2).

6. **Conformación del equipo asesor:** El director del proyecto de auditoría conformará un equipo de trabajo de acuerdo a su criterio y necesidades, de tal manera que cubra tanto los aspectos administrativos como técnicos de la auditoría a realizar. El equipo debe ser capaz de aplicar el enfoque sistémico y debe estar integrado por profesionales de diferentes áreas del conocimiento como administradores de empresas, contadores, economistas, ingenieros industriales, administradores de sistemas informáticos, ingenieros de sistemas, analistas, diseñadores y programadores, entre otros, capaces de reunir habilidades y destrezas, y crear un sentido unificador de sus relaciones.

7. **Lugar donde se desarrollará la auditoría:** Se debe definir el sitio donde se efectuará la auditoría, como el domicilio contractual para todos los efectos y acciones a realizar; así mismo, es indispensable definir la fecha tentativa de inicio de labores.

8. **Recursos logísticos y técnicos necesarios para su desarrollo.** Se deben definir los horarios de trabajo, equipos de trabajo, equipos y elementos de oficina necesarios, recursos informáticos tanto de software como de hardware, definición de accesos, perfiles de usuario, asignación de cuentas, archivos y bibliotecas de producción, etc.

9. **Cronograma de actividades:** El cronograma de actividades es una herramienta de planeación y control de gestión muy efectiva, por lo tanto se recomienda su utilización. En el cronograma se señala el tiempo estimado para desarrollar cada una de las actividades contempladas en el alcance de la auditoría y la fecha de inicio; para su elaboración se aconseja que se tome como referencia el anexo N°2, atinente a la estimación de tiempos.

Una vez concluida la fase de planeación de la auditoría de sistemas, se envía un informe escrito al gerente y directivos de la empresa vinculados con el tema; así mismo, se deben programar reuniones para analizar los términos de la planeación, su alcance y posterior ejecución.
Cabe recordar que el proceso de planeación es continuo y se debe realizar durante el desarrollo de la auditoría, queriendo decir con ello que requiere de una permanente revisión y evaluación, para luego proceder a hacer los ajustes necesarios, manteniéndola dentro del curso esperado.

2.6 BIBLIOGRAFÍA


Guía Internacional de Auditoría N° 15. Auditoría en un ambiente PED. párrafos N°s. 7,8.


www. dorado.une.edu.ve/biblio/auditoria
3.1 INTRODUCCIÓN

Los cuestionarios de control interno deben ser cuidadosamente elaborados, de tal manera que permitan descubrir o analizar aquellos aspectos que se desean investigar, por lo tanto, se requiere de una buena planeación, diseño y crítica para que los resultados sean los esperados.

3.2 CUESTIONARIO DE CONTROL INTERNO. DEFINICIÓN.

Consiste en un conjunto amplio de preguntas que están orientadas a comprobar el cumplimiento de políticas, planes, programas, normas, procedimientos y funciones, tanto generales como específicas, relacionadas con algún negocio o aspecto en particular; por lo tanto, los cuestionarios deben ser diseñados o elaborados con sentido común, las preguntas deben ser sencillas, directas, concisas y orientadas hacia los distintos niveles jerárquicos de la empresa objeto de la auditoría.

A continuación se presentan algunos cuestionarios de Control Interno a manera de ejemplo, que cubren los siguientes tópicos con relación a la aplicación auditada: entradas, salidas, software del sistema, programas, seguridad en aspectos físicos, seguridad en aspectos técnicos, controles organizacionales, talento humano, el cual analiza los siguientes aspectos: administración y organización, ambiente laboral, entrenamiento y capacitación, desempeño, supervisión, motivación y remuneración.

3.2.1 Cuestionario de control interno para las entradas a la aplicación

• Se emplean técnicas para validar, probar y verificar los datos de entrada, que permitan garantizar la ocurrencia de un mínimo de errores? Los datos de entrada se deben validar, probar y verificar, para prevenir errores o fraudes, evitando inconsistencias en el flujo de información y buscando siempre mantener la integridad de los datos.

• Son detectados los registros o transacciones que no fueron aceptados por el sistema? Se deben producir mensajes de error y reportes de excepción que listan aquellos registros o transacciones que presentaron alguna inconsistencia durante el proceso de entrada o captura de datos.

• Existen controles razonables relacionados con la generación de los datos? Durante la preparación de los datos se debe incluir la fecha de elaboración y firma de la persona responsable, así mismo, se debe llevar un registro de autorizaciones de acceso a los documentos fuente. En lo posible se debe
procurar que la entrada al sistema se lleve a cabo a través de menús obligatorios y adicionalmente solicitar contraclaves en aquellos programas interactivos de grabación que sean críticos.

- Son los formatos utilizados para la captura los más indicados y solicitan solo los datos necesarios? Se debe utilizar, en la medida de lo posible, formatos estándar o preimpresos que sean claros, sencillos y fáciles de diligenciar.

- Están los documentos fuente debidamente protegidos y almacenados? Se deben archivar los documentos fuente en un lugar seguro, para prevenir modificaciones no autorizadas o la utilización indebida antes de su procesamiento.

- Se registra el tránsito que hacen los documentos por las distintas dependencias u oficinas? Existen controles suficientes para evitar la pérdida de documentos fuente o que sean doblemente procesados? Se deben asignar estas tareas a una persona que se encargue de registrar cada grupo de documentos y velar por su adecuado procesamiento, permitiendo efectuar el seguimiento a la aplicación cuando sea necesario.

- Existen mecanismos que restrinjan el acceso lógico a los dispositivos de entrada? Se debe exigir la identificación del usuario y clave de entrada para permitir el acceso personal al sistema, así como la debida autorización para utilizar recursos específicos tales como archivos, programas, librerías, lenguajes, etc.

- Están los discos y cintas debidamente identificados? Los discos y cintas deben estar etiquetados tanto interna como externamente para evitar confusiones y facilitar su localización.

- Existe la debida documentación que indique lo que se debe hacer con relación a la preparación, corrección, grabación y almacenamiento de datos? Deben existir procedimientos escritos relacionados con la entrada de datos, con el fin de proporcionar al usuario instrucciones comprensivas que le señalen los pasos a seguir de una manera directa y concisa.

- Existe segregación de funciones entre la generación, registro y almacenamiento de entrada de datos? Debe existir una adecuada segregación de funciones durante las fases de preparación, alimentación y almacenamiento de datos, con el propósito de evitar errores en su manipulación y proporcionar mejor seguridad.

- Brinda el sistema de computación utilizado, algún nivel de seguridad para la entrada de datos? Adicionalmente a los controles que se puedan diseñar para controlar las entradas a la aplicación, se deben aprovechar los niveles de seguridad que proporciona el sistema de computación, siempre procurando mantener la integridad de los datos.

- Existen estadísticas sobre el tipo de errores cometidos en la captura de datos? Es conveniente llevar un registro sobre el tipo de errores cometidos, como proceso de retroalimentación, para poder diseñar controles cada vez más eficaces.

- Está definido el tiempo que se deben conservar los documentos fuente? Se debe establecer el período y mecanismo para la conservación de los documentos fuente, procurando hacer uso de los procesos de microfilmación o similares.
3.2.2 Cuestionario de control interno para las salidas de la aplicación

- Se lleva a cabo un análisis general de los reportes producidos? Se debe realizar un análisis global de los reportes generados, con el objeto de determinar si existen algunos de ellos que puedan ser eliminados, reemplazados, reagrupados o simplificados, o si hay que diseñar reportes adicionales debido a la dinámica permanente de los sistemas de información.

- Es controlada la distribución de los reportes? Se debe controlar la distribución de los reportes para que se envíen únicamente al personal indicado y se debe realizar mediante oficio remisorio.

- Existen procedimientos para revisar la exactitud de las salidas? Se deben comparar los resultados esperados contra los resultados producidos por el sistema, para verificar que todo ha sido procesado correctamente o en su defecto para establecer oportunamente los correctivos que sean necesarios para procurar la integridad de la información.

- Se producen los reportes absolutamente necesarios? No se deben producir más de los reportes necesarios, para evitar fugas de información o que ésta caiga en manos inescrupulosas.

- Se supervisa la destrucción de aquellos reportes no necesarios o que son producto de procesos abortados? Los reportes y en general toda aquella información dispuesta en documentos, incluyendo el papel carbón que ya cumplieron con su propósito, debe ser destruida bajo la supervisión de una persona responsable, previa elaboración del acta respectiva.

- Se comunica al centro de informática sobre aquellos reportes que presentan inconsistencias? Se deben relacionar aquellos reportes o transacciones que presenten discrepancias y dirigirlos al centro de informática señalando la ocurrencia del error, para que se analicen las posibles causas y se tomen los correctivos del caso.

- Existen procedimientos de manejo y retención de salidas? Se deben desarrollar e implementar seguridades para los reportes que son o están en espera de ser distribuidos.

- Existen estadísticas de los errores que se presentan durante la salida de información? Se debe hacer un análisis de los errores que se presentan con mayor frecuencia durante la producción de reportes, para hacer de ellos un proceso de retroalimentación que conduzca a la elaboración de mejores controles.

- Son almacenados en un lugar seguro aquellos reportes que tienen carácter confidencial? Se debe establecer un procedimiento que señale los mecanismos necesarios a seguir para que garanticen la integridad de aquella información considerada confidencial y evitar su indebida utilización.
3.2.3 Cuestionario de control interno para el software del sistema

- Es tenido en cuenta el criterio de los usuarios de la aplicación durante las diferentes etapas del ciclo de vida del sistema? La comunicación entre los usuarios y analista de sistemas debe ser amplia y cordial, y la opinión y experiencia del usuario debe ser tenida en cuenta tanto durante el análisis, como en el diseño, puesta en marcha y mantenimiento de la aplicación.

- Los cambios y mejoras al software del sistema están debidamente justificadas? Antes de proceder con cualquier cambio, por mínimo que sea, debe ser justificado y evaluado tanto técnica como económicamente, para determinar su viabilidad.

- Son de total confianza las personas que hacen mantenimiento al sistema de información? Se debe controlar que las personas encargadas de efectuar el mantenimiento al software sean totalmente confiables; no obstante, se debe ejercer control sobre el acceso de ellos al sistema.

- Está totalmente legalizado el software utilizado por la empresa? Se debe tener especial cuidado para que el software empleado en la empresa, posea las debidas autorizaciones o patentes, evitando así posibles demandas.

- Existe un registro de aquellos problemas que se presentan con el software? Se debe registrar en una bitácora todas aquellas anomalías que presenta el sistema de información, señalando el día y hora de la ocurrencia y sus posibles causas.

- Existen controles adecuados cuando se están probando nuevas versiones del software o cuando se están aplicando programas de diagnóstico? Se deben implementar controles especiales cada que se realice un ajuste o cambio al sistema, evitando caídas del mismo o posibles intentos de fraude o fuga de información.

- Tiene el software adquirido contrato de mantenimiento? Como política general de la empresa, todo el software adquirido debe tener contrato de mantenimiento que incluya actualización de versiones.

- Es auditado el software en funcionamiento? Se debe establecer como política de la empresa la aplicación de software genérico de auditoría a los sistemas que se encuentren en funcionamiento.

- Existe documentación del software del sistema? Se debe velar por la elaboración y actualización de los manuales del software y que éstos reúnan información relativa a la operación, recuperación de errores, fallas en los equipos, reinicios, etc.

- Se llevan estadísticas o reseña de fraudes cometidos con respecto al software del sistema? Se debe llevar un registro periódico de aquellos accesos no autorizados al sistema de información, al sistema operativo, a las bases de datos y a las comunicaciones.
Programas de la aplicación

- Son autorizadas y probadas las correcciones a programas antes de su puesta en marcha? Se deben establecer procedimientos que garanticen que los programas se encuentran funcionando correctamente, y cuando se le han hecho adecuaciones o ajustes, éstos deben corresponder a lo programado y autorizado. Se debe ejercer estricto control sobre los programas para que no sean alterados sin la debida autorización.

- Se lleva un registro de los cambios efectuados a los programas? Se debe llevar un registro formal relacionado con los cambios hechos a los programas que incluya información como: fecha de solicitud, persona solicitante, justificación, viabilidad técnica, tiempo estimado para la puesta en marcha, recursos demandados, costos, fecha de inicio, autorizaciones, persona responsable, etc.

- Están adecuadamente documentados y probados los nuevos programas? Una vez que los programas están listos para entrar en funcionamiento, deben ser revisados por el auditor de la aplicación para que constate si funcionan perfectamente y si la documentación se encuentra completa y actualizada.

- Existe planeación de las pruebas que deben ser realizadas a los programas? Deben existir procedimientos debidamente establecidos en donde se señale la forma como se deben realizar las pruebas a los programas, las condiciones para llevarlas a cabo, el tiempo estimado para su ejecución y registro de los resultados producidos, entre otros.

- Existen librerías específicas para realizar las pruebas a los programas? Se debe solicitar al centro de informática la asignación de librerías especiales para realizar las pruebas a los programas, de tal manera que no se vayan a causar trastornos en el desenvolvimiento normal de los sistemas de información.

- Existe amplia difusión acerca de las pruebas a realizarse? Es muy conveniente que tanto los administradores, auditores y usuarios de la aplicación conozcan sobre la planeación de las pruebas que se llevarán a cabo a los programas, con el propósito de capitalizar la atención, sugerencias y recomendaciones de todos ellos.

- Existe un mecanismo especial para reportar dificultades o inconsistencias? Se debe establecer un procedimiento que indique que pasos se deben seguir para reportar aquellas inconsistencias o dificultades que se puedan presentar durante la corrida de un programa y proporcionar algunas alternativas de solución.

- Existen circunstancias específicas que limitan la ejecución de la aplicación? Con el propósito de brindar mayor seguridad a la aplicación y cuando se presenten aquellas situaciones que así lo ameriten, previo estudio de las mismas, se debe limitar la ejecución de la aplicación a ciertas terminales o estaciones de trabajo durante determinados días y horas, evitando así las corridas no autorizadas de programas.

- Existen controles permanentes que permitan detectar inconsistencias ocurridas durante el procesamiento de datos? Se deben definir controles suficientes, confiables, económicos y fáciles de implementar, que permitan prevenir y detectar aquellas inconsistencias presentadas durante el
procesamiento de datos, haciéndoles un seguimiento hasta encontrar el origen de su causa y tomar los correctivos necesarios.

■ Realizan los programadores actividades relacionadas con la captura de datos? Se deben establecer parámetros muy definidos que demarquen claramente las funciones de operadores, programadores y analistas de sistemas, de tal manera que no se presente un cruce de funciones y a su vez permita ejercer un mejor control sobre el trabajo realizado.

■ Que posibilidad de reproceso tiene la aplicación? Se deben diseñar mecanismos que permitan restaurar cualquier proceso a partir del punto donde se encuentre la falla, mediante la aplicación de los debidos controles, no permitiendo su vulnerabilidad.

3.2.4 Cuestionario de control interno para la seguridad en aspectos físicos de la aplicación

• Existe control sobre el ingreso de funcionarios a la dependencia? Se debe llevar registro de ingresos y egresos del personal a la dependencia y cuando un funcionario es retirado de la misma, se deben cambiar las claves de las cerraduras o chapas.

• Existen programas de prevención contra desastres? Se deben diseñar programas dirigidos a los usuarios de la aplicación que estén orientados a la prevención de desastres relacionados con fuego, temblor y/o inundación.

• Existe señalización de rutas de evacuación? Debe existir una adecuada señalización de las rutas de evacuación y todo el personal debe estar debidamente entrenado en su utilización.

• Existen extinguidores dentro de la instalación? Los extinguidores deben estar ubicados al alcance de los funcionarios y se les debe capacitar en cuanto a su manejo se refiere. Los extinguidores deben ser recargados en las fechas previstas.

• Existe un plan de contingencias? Se debe diseñar un plan de contingencias y ponerlo en marcha lo más pronto posible, de tal manera que incluya convenios con otras entidades o instituciones que posean equipos con características similares, para que sirvan de respaldo en caso de presentarse una eventualidad.

3.2.5 Cuestionario de control interno para la seguridad en aspectos técnicos de la aplicación

• Existe control sobre claves de acceso al sistema? Se debe inhabilitar la clave de acceso de aquellos usuarios que entran a disfrutar de vacaciones o son retirados de la empresa.

• Tiene la aplicación manuales técnico, de operación y del usuario? Toda aplicación debe tener los manuales técnico, de operación y del usuario actualizados y preferiblemente disponibles en línea, con el propósito de consultarlos cuando se requiera.
• Con qué periodicidad se le saca back-up (copia de seguridad) a la aplicación? Se debe diseñar un procedimiento que consigne todo lo relativo a las copias de seguridad, como son los instructivos para llevarlas a cabo, periodicidad, persona responsable de su ejecución, número de copias a realizar, lugar de almacenamiento de las copias, etc.

• Pueden los operadores o usuarios modificar los programas fuente de la aplicación? Se deben diseñar las salvaguardas necesarias para que los programas de la aplicación no sean modificados, sustituidos o ejecutados por personas no autorizadas.

• Se permite el uso de la computadora a personas extrañas a la dependencia? Se debe prohibir el acceso a personas ajenas al sistema de computación y como medida precautelativa se debe exigir que el ingreso a la aplicación siempre se haga a través de menús obligatorios y con solicitud de clave de acceso.

• Existe más de un funcionario que esté en capacidad de operar la aplicación? Se debe establecer como política que la capacitación debe ser impartida a más de un funcionario por aplicación, con el fin de prever tropiezos en caso de presentarse enfermedad o abandono del cargo por parte del funcionario que está al frente de la operación de la aplicación.

• Hay información de carácter confidencial o privada relacionada con la aplicación? En caso de tenerse que ver con información de carácter confidencial, se debe poner especial cuidado en su manejo y almacenamiento, procurando garantizar la integridad de la información.

• Existen procedimientos formales que contemplan la seguridad física y lógica de los datos transmitidos entre redes, de tal manera que garanticen la oportunidad totalidad y exactitud de los mismos? Se deben implementar los controles necesarios que garanticen la protección de los datos que son transmitidos por la red, impidiendo el monitoreo no autorizado, controlando y resguardando los accesos físicos y lógicos a la red, resguardando el software de comunicaciones, así como su respectiva documentación.

• Existe pérdida de mensajes en el sistema de conmutación de datos? Con qué frecuencia se presenta? Se debe controlar la pérdida o modificación de los mensajes durante la transmisión mediante su almacenamiento y posterior reenvío. (sistema de retardo).

• Brinda el sistema de administración de la base de datos una adecuada protección a la información y datos almacenados? Los sistemas de gestión de bases de datos (DBMS) ofrecen a desarrolladores, administradores y usuarios, una gama muy amplia de herramientas que permiten garantizar la integridad, consistencia, confidencialidad, confiabilidad y en general la seguridad de la información almacenada y con un elemento muy importante a favor: las líneas de código que se requieren por parte del implementador son mínimas, en ocasiones solo basta con una sencilla sentencia para obligar al DBMS a controlar y mantener las restricciones necesarias.

• Se revisa la bitácora de la base de datos? Se debe revisar regularmente la bitácora de reinicios y reprocesos causados por el mal funcionamiento del sistema y analizar las causas que hayan podido generar tal dificultad para que se puedan corregir apropiadamente.
• Existen estándares relacionados con los programas de la aplicación? Deben haber estándares escritos que orienten al diseño de los programas de la aplicación en donde se especifiquen las llamadas de datos que puedan ser usadas para acceder a la base de datos. La documentación debe contener las entidades, atributos e interrelaciones y debe ser revisada por el administrador de la base de datos antes de que el programa sea puesto en producción.

• Existe documentación escrita relacionada con el respaldo y recuperación de la base de datos en caso de presentarse destrucción parcial o total de ésta? Se debe verificar que haya una documentación específica para el respaldo y recuperación de la base de datos; que considere el copiado de la base de datos a intervalos regulares permitiendo su recuperación automática. La documentación debe incluir procedimientos y estándares para el reinicio y/o recuperación de los datos. El administrador de la base de datos es el responsable de garantizar la integridad, confidencialidad y confiabilidad de la base de datos e igualmente debe velar para se diseñen, prueben y apliquen planes de contingencias relacionados con la misma.

• Es empleada la criptografía para proteger el almacenamiento y transmisión de información? La criptografía está exenta de regulados sistemas de almacenamiento centralizado de claves, adicionalmente es la protección indicada para aquellas personas que desean mantener la privacidad de la información que se almacena o se transmite a través de la red, porque es segura y confiable.

• Que elementos adicionales son considerados en la seguridad de los datos? Otros elementos que contribuyen a la seguridad de los datos son: identificación del usuario o contraseña, privilegios y autorizaciones para la realización de determinadas tareas o utilización de recursos del sistema, limitaciones para la ejecución de ciertas tareas, seguridad de la estación de trabajo o terminales del sistema, menús obligatorios como acceso al sistema, etc.

3.2.6 Cuestionario de control interno para controles organizacionales de la aplicación

• Los niveles jerárquicos del departamento o unidad permiten un desenvolvimiento normal de sus actividades? Se debe revisar la estructura jerárquica del departamento o unidad, con el propósito de verificar su funcionalidad.

• Se cumplen las políticas particulares impartidas por la gerencia y relacionadas con la aplicación? Se debe supervisar el cumplimiento de políticas con respecto a la aplicación y dar aviso a las instancias pertinentes, tanto sobre su cumplimiento como sobre sus desviaciones, para que se tome el curso de acción a seguir.

• Las políticas particulares relacionadas con la aplicación encajan dentro de las políticas generales de la empresa? Debe existir una estrecha relación entre las políticas particulares de la aplicación en estudio con las políticas generales de la organización y su supervisión es indispensable.

• Existen políticas de control fiscal con respecto a la aplicación? Las políticas de orden fiscal deben estar claramente consignadas por escrito y ampliamente difundidas entre el personal que tiene la aplicación a cargo.
● Conoce la normatividad que cobija a la aplicación? Toda aplicación está sujeta a ciertas normas o regulaciones, las cuales deben estar plenamente identificadas en forma escrita.

● Existe manual de procedimientos escrito relacionado con la aplicación? Debe existir el manual de procedimientos escrito, que describa claramente todas aquellas actividades relacionadas con la aplicación y se debe velar por su permanente actualización, así como por su amplia difusión.

● Existen discrepancias entre las funciones asignadas a su cargo y las funciones desempeñadas? Ocurre con cierta frecuencia que los empleados reciben algunas ordenes de sus superiores relacionadas con actividades ajenas al cargo desempeñado.

● Existe una adecuada segregación de funciones? Debe existir una adecuada separación de funciones que permita definir claramente el grado de responsabilidad que tiene cada funcionario, a su vez, se debe buscar una mayor eficiencia en el desempeño de sus actividades.

● La responsabilidad sobre la administración de la aplicación corresponde a la unidad usuaria o al centro de informática? La administración de la aplicación en lo atinente a entrada de datos, salida de datos, distribución de reportes, etc, debe corresponder a la unidad usuaria de la aplicación y lo relacionado con el análisis, programación, pruebas a programas, mantenimiento y documentación técnica, debe corresponder al centro de informática.

3.2.7 Cuestionario de control interno para el talento humano que interviene en la aplicación

Administración y Organización

● Existen políticas sobre planeación del talento humano? Deben existir políticas plenamente establecidas sobre planeación del talento humano, que determine el número y tipo de personal requerido y deben estar enmarcadas dentro de la Planeación Estratégica de la empresa u organización.

● Existe dentro de la empresa la función de auditoría aplicada al talento humano? Dentro de toda empresa u organización se debe ejercer la función de auditoría al talento humano, puesto que es la responsable de controlar y evaluar los procesos de selección, vinculación, promoción, entrenamiento, capacitación y desarrollo, evaluación del desempeño, ambiente laboral, etc.

● Existe dentro de la empresa un sistema de información del talento humano? Debe existir un sistema de información que permita realizar un diagnóstico del talento humano y del funcionamiento social como apoyo a la toma de decisiones.
- Conoce el reglamento interno de trabajo? El departamento de personal es el responsable de su redacción, difusión y permanente aplicación.

- Existen políticas de salud ocupacional? Toda empresa debe elaborar y poner en funcionamiento programas sobre salud, higiene, seguridad y bienestar social para sus trabajadores y empleados.

- Existe un programa de trabajo y se cumple a cabalidad? Se debe establecer un programa de trabajo que incluya la periodicidad de las actividades a realizar, señalando si se deben ejecutar a diario, semanal o mensualmente, evitando así improvisación y desorden por la ausencia de éste.

Ambiente laboral del área auditada

- Como es el ambiente laboral del área auditada? Es necesario conocer cómo es el ambiente laboral que rodea al empleado o trabajador en cuanto a aspectos físicos, técnicos, sociales y psicológicos se refiere, dado que de allí depende su desempeño.

- Existen políticas de bienestar laboral por parte de la empresa? La empresa debe orientar políticas que busquen la satisfacción del empleado y de su familia, mejorando la calidad de vida y promoviendo su desarrollo integral.

- Hay estabilidad laboral en la empresa? La estabilidad laboral le aporta a la empresa mayor eficiencia y productividad y se convierte en factor determinante de motivación y bienestar para el trabajador, por lo tanto se debe procurar.

- Es alta la rotación de personal? Es necesario llevar un reporte de la rotación que se da en la empresa y conocer sus causas, las cuales pueden ser producidas por ascensos, promociones, despidos, etc. Una alta rotación del personal implica mayores costos de selección y adiestramiento, ocasiona poca eficiencia, mala calidad de los servicios prestados, etc.

- Existen programas de inducción? Se deben diseñar y poner en práctica programas de inducción, con el propósito de ambientar al empleado y familiarizarlo con la empresa y sus integrantes.

- Son periódicas y consecutivas las vacaciones del personal? Se debe establecer como política de la empresa, la obligatoriedad de tomar las vacaciones durante el período y tiempo correspondiente, esto permite que durante la ausencia del titular del cargo se detecten fallas procedimentales.

Entrenamiento y capacitación del personal del área auditada

- Existen planes de entrenamiento y capacitación programados por la empresa? Toda empresa debe planear las actividades relacionadas con el entrenamiento y capacitación que permitan desarrollar en sus trabajadores habilidades, conocimientos y actitudes que le permitan un desempeño más eficiente en su cargo.
Son evaluados los programas de entrenamiento y capacitación? Todo programa de entrenamiento y capacitación impartido por la empresa debe ser evaluado, para determinar si cumplió con los objetivos y metas fijadas.

Son evaluadas las personas que recibieron entrenamiento y capacitación? Deben ser evaluados los participantes a los cursos de entrenamiento y capacitación, con el propósito de determinar si como consecuencia de éstos, se redujo la rotación de personal, disminuyó el ausentismo, aumentó la eficiencia y habilidad de la persona para desempeñar el cargo, aumentó la calidad de los productos y servicios y se incrementó la productividad.

Desempeño del personal del área auditada

Son conocidos los estándares de desempeño y las normas que se deben seguir? Los procedimientos de desempeño deben ser conocidos por todos los empleados o trabajadores de la compañía, en donde se señale claramente las normas que se deben seguir para lograrlo.

Se realizan evaluaciones periódicas del desempeño? Se deben realizar evaluaciones periódicas del desempeño de los trabajadores y empleados, con el propósito de conocer como ha sido el desempeño en el cargo y para que sirva como herramienta para la toma de decisiones con respecto a ascensos, incrementos salariales, comunicación organizacional, etc.

Supervisión del personal del área auditada

Cómo es la disciplina laboral de los empleados? Se debe propender para que el comportamiento de los empleados se ajuste a la normatividad de la empresa o compañía.

Son frecuentes los conflictos laborales? Se deben atender los reclamos y quejas, limitando así los conflictos laborales que causan desmotivación y apatía.

Son debidamente atendidas las quejas y reclamos? Del oportuno y buen tratamiento que se le den a las quejas y reclamos efectuados por los trabajadores, manteniendo los conflictos dentro de un margen funcional aceptable, depende en gran parte el clima laboral de la empresa.

Es alto el índice de ausentismos y retardos? Es importante conocer las causas que ocasionan los ausentismos y/o retardos, encontrándose entre las más frecuentes la desmotivación, enfermedad, indisciplina, etc.

Motivación del personal del área auditada

Hay motivación al interior de la empresa u organización? Deben existir factores motivacionales que conduzcan a las personas a trabajar con responsabilidad, calidad y mística; actitudes que favorecen la consecución de los objetivos institucionales.

Existen mecanismos de ascensos y promociones? Deben existir procedimientos de ascensos y promociones como resultado de la calificación de méritos, los cuales deben ser difundidos entre los empleados y trabajadores.
Remuneración del personal del área auditada

- Existe en la empresa una política salarial definida? Toda empresa debe diseñar un programa de remuneración adecuado y acorde a las exigencias de cada cargo, que sea atractivo, que satisfaga las expectativas de los trabajadores y de la empresa y que sea ampliamente conocido.

- Existen incentivos salariales? Un programa de remuneración adecuado debe considerar aspectos como los incentivos salariales y reclasificación de cargos, factores que mantienen la fuerza laboral satisfecha y motivada.

3.3 BIBLIOGRAFÍA

ALVAREZ, C. Augusto. La Administración de Personal. Editorial Padres e Hijos. 1995.


www.dorado.une.edu.ve/biblio/auditoría
CAPÍTULO 4
PROCEDIMIENTOS DE AUDITORÍA

4.1 INTRODUCCIÓN

El trabajo del auditor debe estructurarse de tal manera que cubra apropiadamente todos los aspectos de la entidad que sean importantes a auditar, mediante la emisión de juicios al decidir el alcance de los procedimientos de auditoría y al evaluar la confiabilidad, suficiencia e integridad de la información obtenida a través de las diversas fuentes de información.

4.2 PROCEDIMIENTOS DE CUMPLIMIENTO. DEFINICIÓN.

Para llevar a cabo la revisión del control interno, el auditor debe realizar procedimientos de cumplimiento para obtener evidencia de que los controles internos por él diseñados han sido puestos en práctica y funcionan correcta y eficazmente; de no ser así, debe entrar a evaluar cuales fueron los factores de desviación, diseñar nuevos controles y definir su forma de aplicación. La Guía Internacional de Auditoría N° 6. Estudio y evaluación del sistema de contabilidad y los controles internos relativos, con respecto a una auditoría, define en el párrafo N° 12, los procedimientos de cumplimiento como: "Los procedimientos de cumplimiento son pruebas diseñadas para obtener seguridad razonable, pero no absoluta, de que están en vigor aquellos controles internos en los que se va a depositar la confianza de la Auditoría. Estos procedimientos incluyen pruebas que requieren la inspección de documentos que apoyan operaciones para obtener evidencia de que los controles han operado con propiedad (por ejemplo, verificando que el documento ha sido autorizado) e investigaciones acerca de los controles que no dejan rastro de auditoría, así como la observación de los mismos (por ejemplo, determinar quien efectúa realmente cada función, y no sólo quien supuestamente debería efectuarla)."

A continuación se relacionan los procedimientos de auditoría que son tenidos en cuenta en el presente estudio:

4.2.1 Entradas a la Aplicación

- Revisar si los datos de entrada son validados, probados y verificados.
- Determinar si se aplican controles para detectar registros o transacciones no procesadas.
- Verificar la existencia de controles razonables relacionados con la generación de los datos.
- Evaluar la funcionalidad de los formatos utilizados para la captura de datos.
- Verificar la protección y almacenamiento de los documentos fuente.
- Comprobar la existencia de controles de acceso a los dispositivos de entrada.
- Comprobar la identificación de discos y cintas.
• Observar los controles aplicados durante la preparación de los datos.
• Verificar la existencia de documentación actualizada sobre la preparación, corrección, grabación y almacenamiento de los datos.
• Comprobar la segregación de funciones entre la generación, registro y almacenamiento de los datos.
• Evaluar las estadísticas existentes de los tipos de errores cometidos durante la captura de datos.

4.2.2 Salidas de la Aplicación

• Comprobar la fecha y paginación de los informes generados.
• Comprobar la realización de un análisis global de los reportes producidos.
• Observar la distribución de los reportes.
• Evaluar los procedimientos para manejo, reporte de inconstancias y retención de salidas.
• Evaluar los procedimientos que revisan la exactitud de las salidas.
• Comprobar si los reportes producidos son absolutamente necesarios.
• Supervisar la destrucción de reportes no necesarios o defectuosos.
• Evaluar la seguridad de los reportes confidenciales.
• Evaluar las estadísticas de errores que se presentan durante la salida de información.

4.2.3 Software del Sistema

• Comprobar la participación del usuario durante las distintas etapas del ciclo de vida del sistema.
• Comprobar la justificación de los cambios y mejoras al software del sistema.
• Evaluar los controles ejercidos al personal de mantenimiento del sistema de información.
• Verificar la legalidad del software utilizado.
• Comprobar el registro de problemas presentados con el software.
• Evaluar los controles aplicados cuando se realizan cambios o ajustes al sistema.
• Comprobar la aplicación del software genérico de auditoría a los sistemas en funcionamiento.
• Verificar la existencia y actualización de la documentación del software del sistema.
• Evaluar la reseña de fraudes cometidos contra el software del sistema.
• Analizar el contrato de mantenimiento del software adquirido.

4.2.3.1 Programas de la Aplicación

• Comprobar la autorización para efectuar correcciones o cambios a los programas.
• Comprobar el registro de los cambios efectuados a los programas.
• Verificar la existencia y actualización de los manuales de la aplicación.
• Revisar si las pruebas aplicadas a los programas han sido planeadas.
• Comprobar la asignación de librerías específicas para realizar las pruebas a los programas.
• Evaluar los procedimientos para manejo de inconsistencias presentadas durante la corrida de programas.
• Evaluar las circunstancias que limitan la ejecución de la aplicación.
• Observar los controles aplicados durante el procesamiento de datos.
• Comprobar que los programadores no realicen actividades de captura de datos.
• Revisar si las aplicaciones tienen puntos de reinicio debidamente controlados.
• Verificar los estándares relacionados con los programas de la aplicación
• Revisar los procedimientos de encriptación y respaldo de los programas de la aplicación

4.2.4 Seguridad en Aspectos Físicos de la Aplicación

• Comprobar los controles físicos de ingreso a la dependencia.
• Solicitar los programas de prevención contra desastres y evaluarlos.
• Comprobar la existencia de rutas de evacuación.
• Revisar los extinguidores y su fecha de vencimiento.
• Solicitar el plan de contingencias y evaluarlo.

4.2.5 Seguridad en Aspectos Técnicos de la Aplicación

• Verificar la existencia de controles de acceso al sistema.
• Solicitar los manuales técnico, de operación, del usuario y comprobar su actualización.
• Evaluar los procedimientos de back-up a la aplicación.
• Comprobar que los operadores o usuarios no puedan modificar los programas fuente de la aplicación.
• Comprobar que el uso de la computadora solo se lleve a cabo por el personal autorizado.
• Constatar si hay varios funcionarios que estén en capacidad de operar la aplicación.
• Revisar el manejo de aquella información que tiene carácter confidencial.
• Evaluar los controles aplicados en la transmisión de datos.
• Revisar los procedimientos relacionados con la seguridad física y lógica de los datos transmitidos.
• Verificar si el almacenamiento y trasmisión de datos son protegidos criptográficamente.
• Verificar los controles que limitan el acceso a la base de datos.
• Revisar la documentación escrita relacionada con el respaldo y recuperación de la base de datos.
• Revisar las políticas de seguridad relacionadas con el sistema operativo.

4.2.6 Controles Organizacionales de la Aplicación

• Solicitar la estructura jerárquica de la unidad y analizar su funcionalidad.
• Solicitar las políticas existentes con respecto a la aplicación y verificar su cumplimiento.
• Analizar si existe coherencia entre las políticas propias de la aplicación con las políticas generales de la empresa.
• Comprobar si existen políticas de control fiscal respecto a la aplicación.
• Solicitar la normatividad relacionada con la aplicación y analizarla.
• Solicitar los manuales de funciones y de procedimientos, y revisar su contenido.
• Comprobar si las funciones asignadas corresponden con las funciones desempeñadas en cada cargo.
• Comprobar si existe una adecuada segregación de funciones.
• Comprobar la responsabilidad sobre la administración de la aplicación.
4.2.7 Talento Humano que Interviene en la Aplicación

- Solicitar las políticas existentes sobre la planeación del talento humano y analizarlas.
- Verificar si es aplicada la función de auditoría al talento humano.
- Verificar si está debidamente funcionando el sistema de información del talento humano.
- Solicitar el reglamento interno de trabajo y comprobar si es de amplio conocimiento entre el personal.
- Verificar la existencia y puesta en marcha de programas de salud ocupacional.
- Verificar si los programas de trabajo son cumplidos cabalmente.

4.2.7.1 Ambiente laboral del Área Auditada

- Conocer el ambiente laboral desde el punto de vista físico, técnico, social y psicológico.
- Evaluar las políticas de bienestar laboral.
- Comprobar si existe estabilidad laboral.
- Evaluar el índice de rotación del personal.
- Constatar si existen programas de inducción y su aplicación.
- Comprobar si las vacaciones son tomadas obligatoriamente.

4.2.7.2 Entrenamiento y Capacitación del Personal del Área Auditada

- Solicitar y evaluar los programas de entrenamiento y capacitación.
- Verificar que los programas de entrenamiento y capacitación impartidos por la empresa sean evaluados en su totalidad.
- Verificar si los funcionarios participantes en el entrenamiento y capacitación son evaluados permanentemente.

4.2.7.3 Desempeño del Personal del Área Auditada

- Verificar la existencia de estándares de desempeño y su difusión.
- Revisar la aplicación de evaluaciones periódicas del desempeño.

4.2.7.4 Supervisión del Personal del Área Auditada

- Analizar la disciplina laboral de los empleados.
- Comprobar si son frecuentes los conflictos laborales.
- Verificar si las quejas y reclamos son debidamente atendidas.
- Verificar el índice de ausentismos y retardos, y las causas que los ocasionan.

4.2.7.5 Motivación del Personal del Área Auditada

- Determinar el grado de motivación de los funcionarios del área.
- Evaluar los procedimientos de ascensos y promociones.
4.2.7.6 Remuneración del Personal del Área Auditada

- Comprobar si existe una política salarial definida.
- Determinar si se está aplicando una adecuada remuneración de acuerdo al cargo desempeñado.

4.3 BIBLIOGRAFÍA

ALVAREZ, C. Augusto. La Administración de Personal. Editorial Padres e Hijos. 1995.


www.dorado.une.edu.ve/biblio/auditoria
www.isaca.org
CAPÍTULO 5
DISEÑO DE LOS PAPELES DE TRABAJO

5.1. INTRODUCCIÓN

Los papeles de trabajo se deben diseñar y formular cuidadosamente para que sirvan de herramienta y soporte en la planeación, organización y coordinación del examen de auditoría, y a su vez para que brinden respaldo a la opinión del auditor. Aunque éstos pueden obedecer a un sinnúmero de formas, dependiendo del tamaño, complejidad y circunstancias de cada compromiso de auditoría, se preparan de acuerdo al criterio, experiencia y preferencia del auditor y se organizan teniendo en cuenta su uso y contenido.

5.2 PAPELES DE TRABAJO. DEFINICIÓN.

Es toda aquella información que se reúne y almacena durante la realización de la auditoría para facilitar su examen, constituyéndose en evidencias válidas y suficientes del trabajo realizado por el auditor.

Según el SAS (Statements on Auditing Standards) Num. 41 (AU 339.03), define los papeles de trabajo como:

"Los papeles de trabajo son registros que mantiene el auditor de los procedimientos aplicados, pruebas desarrolladas, información obtenida y conclusiones pertinentes a que se llegó en el trabajo. Algunos ejemplos de papeles de trabajo son los programas de auditoría, los análisis, los memorandos, las cartas de confirmación y declaración, resúmenes de documentos de la compañía y cédulas o comentarios preparados u obtenidos por el auditor. Los papeles de trabajo también pueden obtener la forma de información almacenada en cintas, películas u otros medios".

José Dagoberto Pinilla define los papeles de trabajo de la siguiente forma: "Comprende el conjunto de cédulas preparadas por el auditor y/o personal colaborador, con motivo del desarrollo del programa de auditoría para obtener evidencia comprobatoria suficiente y competente, que sirva como base objetiva para emitir una opinión independiente sobre el objeto auditado"

Los papeles de trabajo revisten gran importancia porque son un fiel reflejo del criterio, objetividad y profundidad de los procedimientos de auditoría aplicados, permitiendo señalar si fueron o no alcanzados los objetivos de la auditoría propuesta; así mismo, permite el fácil seguimiento, revisión y supervisión por parte del ente auditado, debido al gran soporte documental que presenta y se constituye en el registro permanente del trabajo del auditor.

5.3 OBJETIVOS DE LOS PAPELES DE TRABAJO

Entre los principales objetivos de los papeles de trabajo se destacan los siguientes:

- Proporcionar la información básica y fundamental necesaria para facilitar la planeación, organización y desarrollo de todas las etapas del proceso de auditoría.
- Respaldar la opinión del auditor permitiendo realizar un examen de supervisión y proporcionando los informes suficientes y necesarios que serán incluidos en el informe de auditoría, además, sirve como evidencia en caso de presentarse alguna demanda.
- Permiten demostrar si el trabajo del auditor fue debidamente planeado, determinando su eficiencia y eficacia.
- Permiten establecer un registro histórico disponible permanentemente en caso que se presente algún requerimiento.
- Servir como punto de referencia para posteriores auditorías.
- Servir de puente entre el informe de auditoría y las áreas auditadas.

5.4 TIPOS DE PAPELES DE TRABAJO

Aunque los papeles de trabajo varían de acuerdo a las circunstancias y criterio del auditor, se presenta a continuación una clasificación que permite su fácil empleo y comprensión:
5.4.1 Archivo Permanente

Contiene información que cubre varios períodos de la auditoría y son de utilidad en exámenes posteriores, representando sumo interés para el administrador de la aplicación y fuente de amplia consulta relacionada con cada sistema o aplicación en particular. Como ejemplo se puede mencionar aquella información relacionada con: naturaleza y justificación de la aplicación, reseña de la aplicación, estructura organizacional respecto al manejo de la aplicación, interacción con otras aplicaciones, documentación de entradas y salidas, diccionario de datos, programas, menús, diagramas del sistema, naturaleza y definición de cada proceso, etc.

5.4.2 Archivo Corriente

Se elabora para examinar cada período de auditoría a realizar, constituyéndose en evidencia del trabajo desarrollado por el auditor, mostrando todas sus fases y sirviendo como respaldo para presentar los informes respectivos. Como ejemplo se tiene: el programa de trabajo, utilización de datos de prueba, verificación al contenido de archivos, utilización de programas de auditoría, revisión lógica a los programas de la aplicación auditada, control de procesos, análisis de entradas al sistema, análisis de salidas producidas por el sistema, análisis de controles administrativos, análisis de controles organizacionales, informes de auditoría, etc.

5.5 PROPIEDAD DE LOS PAPELES DE TRABAJO

Los papeles de trabajo son de propiedad del auditor y deben ser conservados por un período no inferior a cinco años; la información que allí se consigna es considerada de carácter confidencial, por lo tanto se debe garantizar su integridad y no se debe dar a conocer a terceros, salvo por disposición legal.

La Guía Internacional de Auditoría N° 9 Documentación. Señala en los párrafos 12 y 13, lo siguiente:

Párrafo 12. "Los papeles de trabajo son de propiedad del auditor. Este puede, a su criterio, poner a disposición de su cliente parte o extractos de los papeles de trabajo. No obstante, éstos no remplazarán los registros contables del cliente".

Párrafo 13. "El auditor adoptará procedimientos razonables para asegurar la custodia y confidencialidad de sus papeles de trabajo y los retendrá durante un periodo suficiente que satisfaga las necesidades de su práctica y cubra cualquier registro legal o profesional pertinente."
5.6 DISEÑO Y CONTENIDO DE LOS PAPELES DE TRABAJO

5.6.1 En cuanto a su diseño

Debe ser claros, sencillos, completos, legibles, ordenados, fáciles de aplicar, no se deben prestar para ambigüedades y deben contener:

- Nombre de la empresa auditada.
- Nombre de la empresa auditora o auditor responsable.
- Nombre de la aplicación auditada.
- Nombre de la persona entrevistada o fuente consultada.
- Tiempo de ejecución (fecha de inicio y fecha de terminación).
- Persona que diligenció el papel de trabajo.
- Fecha de diligenciamiento del papel de trabajo.

5.6.2 En cuanto a su contenido

La Guía Internacional de Auditoría Nº 16. Auditoría en un Ambiente de Procesamiento Electrónico de Datos (PED), dice lo siguiente en su párrafo Nº23: "Los papeles de trabajo deben contener documentación suficiente para describir la aplicación de la Técnica de Auditoría con ayuda del computador (TAAC), tal como:

- **PLANEACIÓN**
  - Objetivos del TAAC.
  - TAAC específica a ser empleada.
  - Controles a ser ejercidos.
  - Personal, tiempo y costo.

- **EJECUCIÓN**
  - Procedimiento y controles de preparación y prueba de la TAAC.
  - Detalles de las pruebas efectuadas por la TAAC.
  - Detalles de entrada, procesamiento y salida.
  - Información técnica relevante sobre el sistema contable de la entidad, tal como diseños de registros de los archivos de computación.

- **EVIDENCIA DE AUDITORÍA**
  - Información de salida obtenida.
  - Descripción del trabajo de auditoría efectuado sobre la información de salida.
  - Conclusiones de la auditoría.

- **OTROS**
  - Recomendaciones para la gerencia de la entidad.

En adición, puede ser útil documentar las sugerencias para el uso de TAACs; en años futuros."
5.6.3 Diseño sugerido de los papeles de trabajo

Los papeles de trabajo son muy variados debido al tipo de auditoría que se desea desarrollar, por lo tanto, su diseño depende de la iniciativa y orientación que se le quiera dar por parte del auditor.

"La cantidad y calidad de los papeles de trabajo dependen del alcance de los objetivos y de las pruebas de auditoría. Aquí juega papel importante el criterio, la creatividad y experiencia del auditor para definir el diseño de los papeles de trabajo requeridos para asegurar un auditaje de éxito."  

A continuación se presenta un diseño de los Papeles de Trabajo para su respectivo análisis, con el propósito único de orientar sobre todo a aquellas personas que recién incursionan en este complejo y difícil campo del conocimiento; más no es la intención de encasillar o limitar la iniciativa de persona alguna en el diseño de tan fundamental herramienta.

5.6.3.1 Esquema General de los Papeles de Trabajo

<table>
<thead>
<tr>
<th>ARCHIVO PERMANENTE</th>
<th></th>
<th>ARCHIVO CORRIENTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAPELES DE TRABAJO PROPUESTOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO A: Aplicaciones en funcionamiento. Orientado al administrador de la aplicación (anexo No 3).</td>
<td>• FORMULARIO G: Hojas de trabajo para aplicaciones en funcionamiento (anexo No 9).</td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO B: Aplicaciones en funcionamiento. Orientado a los usuarios de la aplicación (anexo No 4).</td>
<td>• FORMULARIO H: Hojas de trabajo para aplicaciones en desarrollo (anexo No 10).</td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO C: Aplicaciones en funcionamiento. Orientado a los auditores de la aplicación (anexo No 5).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO D: Aplicación en desarrollo. Orientado al administrador de la aplicación (anexo No 6).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO E: Aplicaciones en desarrollo. Orientado a los usuarios de la aplicación (anexo No 7).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO F: Aplicaciones en desarrollo. Orientado a los auditores de la aplicación (anexo No 8).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• FORMULARIO I: Descripción y evaluación de procedimientos (anexo No 11).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.6.3.2 Descripción Detallada de los Papeles de Trabajo

El Archivo Permanente para Aplicaciones en Funcionamiento está compuesto por:

Formulario A. Orientado al Administrador de la aplicación y cubre los siguientes aspectos: (Ver anexo N° 3)

1. Reseña de la aplicación.
2. Naturaleza y justificación de la aplicación.
3. Estructura Organizacional y Funcional respecto al manejo de la aplicación.
4. Interacción con otras aplicaciones.
5. Documentación de entradas y salidas.
6. Diccionario de datos, programas y menús.
7. Normalización y fuentes de consulta.
8. Naturaleza y definición de cada proceso.
10. Seguimiento o Rastreo.
11. Funcionalidad.
13. Autonomía
15. Reseña de errores.
17. Observaciones.

Formulario B. Orientado a los usuarios de la aplicación y cubre los siguientes aspectos: (Ver anexo N° 4)

1. Estructura organizacional y funcional respecto al manejo de la aplicación.
2. Normalización y fuentes de consulta.
3. Riesgos detectados en la aplicación.
4. Controles requeridos.
5. Autonomía de la aplicación.
6. Evaluación de la funcionalidad.
7. Sistema de archivo de documentos.
8. Reseña de fraudes.
9. Reseña de errores.
10. Inventario de controles existentes.
11. Limitantes de la aplicación.
12. Observaciones.

Formulario C. Dirigido a los auditores de la aplicación y considera los siguientes aspectos: (Ver anexo N° 5)

1. Personal relacionado con la aplicación.
2. Controles actuales.
3. Controles requeridos.
4. Limitaciones del funcionario frente al auditaje de la aplicación.
5. Observaciones.

El Archivo Permanente para Aplicaciones en Desarrollo está compuesto por:

Formulario D. Orientado al administrador de la aplicación y cubre los siguientes aspectos: (ver anexo N° 6)

1. Reseña de la aplicación.
2. Naturaleza y justificación de la aplicación.
3. Estructura organizacional y funcional respecto a la aplicación.
4. Interacción con otras aplicaciones.
5. Normalización y fuentes de consulta.
6. Observaciones.

Formulario E. Orientado a los usuarios de la aplicación y cubre los siguientes aspectos: (Ver anexo N° 7)

1. Estructura organizacional y funcional respecto a la aplicación.
2. Normalización y fuentes de consulta.
3. Posibles riesgos de la aplicación.
4. Controles requeridos.
5. Observaciones.

Formulario F. Orientado a los auditores de la aplicación y cubre los siguientes aspectos: (Ver anexo N° 8)

1. Personal relacionado con la aplicación.
2. Participación de la auditoría en el desarrollo de la aplicación.
3. Controles sugeridos a la aplicación.
4. Limitaciones del auditor frente al auditaje de la aplicación.
5. Observaciones.

Formulario I. Tiene como propósito efectuar la descripción y evaluación de procedimientos y comprende los siguientes aspectos: (Ver anexo N° 11)

1. Generalidades.
2. Análisis de actividades.
   • Actividades principales.
   • Actividades secundarias.
   • Actividades esporádicas u ocasionales.
   • Análisis de documentos
3. Recomendaciones o sugerencias frente a los documentos manejados.
4. Análisis respecto a información confidencial.
5. Análisis de procedimientos.
6. Conocimiento de las funciones propias del cargo.
7. Inconvenientes o dificultades frente al cumplimiento de actividades.
8. Sugerencias frente a los inconvenientes analizados.

El Archivo Comente para Aplicaciones en Funcionamiento está compuesto por: (ver anexo N° 9)

2. Hoja de trabajo N° 2. Sesiones de trabajo.
   - Entradas al sistema.
   - Utilización de datos de prueba.
   - Pruebas realizadas.
   - Utilización de programas de auditoría.
   - Salidas del sistema.
   - Controles de seguridad en aspectos físicos y técnicos.
   - Controles organizacionales.
   - Talento humano.
   - Control de procesos.
5. Hoja de trabajo N° 5. Puntos de atención para futuras revisiones.

El Archivo Corriente para Aplicaciones en Desarrollo está compuesto por: (ver anexo N° 10)

2. Hoja de trabajo N° 2. Sesiones de trabajo.
5. Hoja de trabajo N° 5. Software del sistema.
5.7 BIBLIOGRAFÍA


Guía Internacional de Auditoría N° 16. Auditoría en un ambiente de procesamiento electrónico de datos (PED), párrafo N° 23.


SAS (Statements on Auditing Standards) Num. 41 (Au 339.03)


www.dorado.une.edu.ve/biblio/auditoria
CAPÍTULO 6
INFORMES DE AUDITORÍA DE SISTEMAS

6.1 INTRODUCCIÓN

La resultante del proceso de auditoría se ve reflejada en los informes de auditoría, por eso es indispensable que su confección se lleve a cabo de manera objetiva, pulcra y oportuna, para que brinde toda la credibilidad y sea ampliamente acogida por el ente auditado.

6.2 INFORMES DE AUDITORÍA DE SISTEMAS. DEFINICIÓN.

Es el resultado final debidamente documentado que se obtiene al concluir el ejercicio de auditoría, donde los responsables deben exponer claramente el tipo de examen practicado, su alcance, así como el grado de compromiso y responsabilidad asumido.

El informe de auditoría debe contener las conclusiones y recomendaciones de los hallazgos más relevantes encontrados durante el ejercicio de la auditoría y debe especificar si el trabajo se realizó de acuerdo con las normas de auditoría generalmente aceptadas, declarando independencia, integridad y objetividad en su opinión.

El informe de auditoría debe ser cuidadosa y profesionalmente confeccionado de tal manera que exprese con claridad lo necesario para que sea bien acogido, logrando mantener lo bueno y mejorando de manera oportuna lo que se requiera, para que tanto el ente auditado como el auditor queden plenamente satisfechos con la calidad del trabajo realizado y mantengan un ambiente de acercamiento, cordialidad, participación y amplia comunicación.

Es importante considerar que la información obtenida durante el desarrollo del trabajo de auditoría es confidencial, por lo tanto no debe ser dada a conocer a extraños; es así como lo contempla la Guía Internacional de Auditoría N° 3. Principios básicos que rigen una auditoría, párrafo N° 6, que dice: "El auditor debe respetar la confidencialidad de la información que obtenga en el curso de su trabajo y no debe revelar tal información a terceros sin que cuente con autorización específica, a menos que haya una obligación legal o profesional para ello".
6.3 OBJETIVOS DE LOS INFORMES DE LA AUDITORÍA DE SISTEMAS

Como objetivos de los informes de auditoría, se pueden destacar los siguientes:

1. Comunicar los resultados del examen de auditoría a los entes auditados, para que se implementen los cambios que impliquen mayor trascendencia.
2. Apoyar la toma de decisiones, sirviendo como documento de respaldo.
3. Apoyar el análisis de las causas y efectos de los hallazgos de la auditoría.
4. Retroalimentar la información recopilada, para optimizar las labores productivas.
5. Servir de referencia para futuras auditorías

![Diagrama de objetivos](image)

FIGURA 6.1 OBJETIVOS DE LOS INFORMES DE AUDITORÍA DE SISTEMAS

6.4 RECOMENDACIONES APLICABLES A LOS INFORMES DE AUDITORÍA DE SISTEMAS

Los informes de auditoría de sistemas deben estar bien presentados, utilizar párrafos cortos y relacionados con el tema de fondo, los comentarios deben estar estructurados, sin tachaduras o enmendaduras, de excelente redacción, los verbos allí conjugados deben estar en tiempo presente, la terminología empleada debe ser sencilla, directa, concisa y lo más importante, que sea comprensible y convincente al lector de la importancia de los hallazgos y de la razonabilidad y conveniencia de acatar las recomendaciones; por último, debe estar firmado y fechado por la persona responsable del informe.

Antes de emitir el informe final a los directivos de la empresa o institución, es aconsejable darlo a conocer al responsable directo de la aplicación, para efectos de éste estudio sería al administrador de la aplicación, con el propósito de analizar los resultados de los exámenes y brindar todas las explicaciones y pruebas pertinentes, garantizando así la aceptabilidad del informe.
6.5 TIPOS DE INFORMES DE AUDITORÍA DE SISTEMAS

Básicamente existen dos tipos de informes a saber: Los informes Abreviados y los informes Extensos.

6.5.1 Informes Abreviados

Van dirigidos a la gerencia y altos directivos de la empresa para que les sirva de soporte en la toma de decisiones y tiene como propósito informar de manera ágil, directa y concisa sobre aquellos aspectos más relevantes de la auditoría, pero si se requiere profundizar en algún detalle, es necesario consultar los informes extensos.

6.5.2 Informes Extensos

Van dirigidos a aquellas personas directamente involucradas con la aplicación y tanto los informes técnicos, administrativos, así como los informes del auditor, deben ser amplios, detallados y en algunos casos incluir una completa descripción del examen de auditoría efectuado.

José Antonio Echenique expone que las conclusiones de la Auditoría de Sistemas se pueden realizar de la siguiente forma: 

---

6 Echenique, José Antonio. Auditoría en Infométrico. Pág. 144
1. Una breve descripción de la situación actual en la cual se reflejen los puntos más importantes. (esta presentación es para el nivel más alto de la organización).

2. Una descripción detallada que comprende:
   a) Los problemas detectados.
   b) Posibles causas, problemas y fallas que originaron la situación presentada.
   c) Repercusiones que puedan tener los problemas detectados.
   d) Alternativas de solución.
   e) Comentarios y observaciones de la dirección de informática y de los usuarios sobre las soluciones propuestas.
   f) Si se opta por alguna alternativa de solución, cuáles son sus repercusiones, ventajas y desventajas, y tiempo estimado para efectuar el cambio.

3. Se debe hacer hincapié en cómo se corregirá el problema o se mejorará una determinada situación, cómo se obtendrán los beneficios, en cuánto tiempo y cuáles son los puntos débiles.

4. Se debe romper la resistencia a la lectura que tienen algunos ejecutivos por medio de conclusiones concretas que sean sencillas (se procurará que se entiendan los términos técnicos y, si es posible, usar técnicas audiovisuales)

6.6 ESTRUCTURA DE LOS INFORMES DE AUDITORÍA DE SISTEMAS

A continuación se presenta a nivel estructural varias modalidades de informes que pueden ser utilizados como soporte en la Auditoría de Sistemas, bien para que sirva como guía en su elaboración o como punto de referencia para la realización de los diferentes exámenes.

6.6.1 Informe de Auditoría

Presenta los resultados de la evaluación y las pruebas relacionadas sobre cada aplicación, en términos de hallazgos y recomendaciones.

**Estructura del Informe de Auditoría:**

- Nombre de la empresa auditada.
- Nombre de la aplicación auditada.
- Nombre de la firma auditora.
- Identificación del informe.
- Fecha del informe.
- Objetivos de la aplicación.
- Descripción de la aplicación.
- Alcance de la auditoría.
- Pruebas realizadas.
- Reseña de aspectos positivos.
- Hallazgos de orden administrativo.
- Hallazgos de orden técnico.
- Recomendaciones de orden administrativo.
- Recomendaciones de orden técnico.
- Firma del auditor responsable.

6.6.2 Informe ejecutivo de auditoría

Este documento sintetiza los resultados expuestos en el Informe de Auditoría, resaltando los aspectos más relevantes.

**Estructura del Informe Ejecutivo:**
- Nombre de la empresa auditada.
- Nombre de la aplicación auditada.
- Nombre de la firma auditora.
- Identificación del informe.
- Fecha del informe.
- Reseña de aspectos positivos.
- Hallazgos relevantes.
- Recomendaciones relevantes.
- Firma del auditor responsable.

6.6.3 Manual del Auditor

Contiene en un lenguaje de fácil acceso y comprensión, la descripción de cada una de las aplicaciones en función de su reseña, normatividad, entradas, procesos, archivos, almacenamiento, salidas y señalando los puntos débiles o de especial atención, permitiendo a los encargados de realizar la labor de auditaje, conocer el objeto sobre el cual se desarrolla su labor.

**Estructura del Manual del Auditor**
- Nombre de la empresa auditada.
- Nombre de la aplicación auditada.
- Nombre de la firma auditora.
- Identificación del manual.
- Fecha de elaboración.
- Fecha de la última actualización.
- Reseña de la aplicación.
  - Fecha de inicio del análisis y diseño.
  - Fecha de la puesta en marcha.
  - Tiempo de duración del análisis y diseño.
  - Personas que participaron en el análisis, diseño y programación.
  - Personas que participaron en el desarrollo de la aplicación.
• Personas usuarias de la aplicación en captura, verificación, procesos críticos y procesos de consulta.
• Mantenimiento a la aplicación.
• Naturaleza y justificación.
• Estructura organizacional y funcional respecto al manejo de la aplicación.
• Entidades o dependencias que interactúan con la aplicación interna y externamente.
• Interacción con otras aplicaciones.
• Documentos de entradas y salidas.
• Diccionario de datos, programas y menús.
• Normalización y fuentes de consulta internas y externas.
• Naturaleza y definición de procesos.
  • Captura y actualización.
  • Consultas.
  • Generación de informes.
  • Proceso de convenciones.
  • Proceso de verificación.
• Autonomía
• Motivos de consulta al centro de informática
• Calificación de autonomía.
• Motivos de dependencia.
• Funcionalidad.
  • Oportunidad.
  • Confiabilidad.
  • Amigabilidad.
• Seguimiento o rastreo.
• Posibilidad de reproceso.
• Reseña de fraudes.
• Reseña de errores.
• Auditoría sobre la aplicación.
  • Procesos de control.
  • Documentación existente.
• Anexos.

6.6.4  Manual Técnico

Contiene una reseña de la aplicación y una descripción técnica detallada del diccionario de datos, programas, menús, bibliotecas, procedimientos de actualización de archivos, generación de listados, diagramas lógicos de la aplicación y descripción del ambiente computacional requerido, entre otros.
Estructura del Manual Técnico de la Aplicación:

I Identificación.
- Nombre de la empresa.
- Nombre de la aplicación.
- Identificación del manual.
- Fecha de elaboración.
- Fecha de la última actualización.

II Descripción de la aplicación.
- Reseña de la aplicación
- Ambiente computacional requerido.
- Diccionario de datos.
  - Carga inicial de archivos.
  - Actualización del archivo maestro.
  - Actualización del archivo de movimiento.
  - Corrección de movimientos de auditoría.
  - Consulta de un rubro o ítem.
  - Listado de verificación de saldos.
  - Cierres mensuales y anuales.
  - Copia de archivos.

III Descripción de Programas:
- Inventario de menús.
- Descripción de comandos.
  - Nombre del comando.
  - Biblioteca.
  - Tipo.
  - Lenguaje.
  - Periodicidad.
  - Procedimiento que invoca.
  - Descripción funcional.
- Descripción de procedimientos.
  - Nombre del procedimiento.
  - Función general.
  - Subsistema.
  - Programa.
  - Biblioteca.
  - Usuarios.
  - Entorno.
  - Parámetros.
  - Archivos.
- Diagramas lógicos de la aplicación.

IV ANEXOS.
6.6.5 Manual de Operación de la Aplicación. (Manual de usuario)

Es una descripción amplia y completa, que indica la forma como opera la aplicación y debe contener los procedimientos que señalan lo que se debe hacer en caso de presentarse problemas tanto en la administración del sistema, así como en los reinicios y producción de reportes.

Estructura del Manual de Operación de la Aplicación:

• Nombre de la empresa.
• Nombre de la aplicación.
• Identificación del manual.
• Fecha de elaboración.
• Fecha de la última actualización.
• Objetivos de la aplicación.
• Requerimientos de operación.
• Descripción del menú de opciones.
• Descripción de los mensajes de error.
• Instrucciones a seguir en caso de presentarse novedades.
• Flujograma de operación.

6.6.6 Manual de Procedimientos de la Aplicación

Describe los procedimientos llevados a cabo con respecto a la preparación, procesamiento y utilización del producto de las aplicaciones.

Estructura del Manual de Procedimientos de la Aplicación:

• Nombre de la empresa.
• Nombre de la aplicación.
• Identificación del manual.
• Fecha de elaboración.
• Fecha de la última actualización.
• Generalidades
  - Objetivos de la aplicación.
  - Descripción de la aplicación.
• Descripción del procedimiento.
  - Interacción con otras dependencias y aplicaciones.
  - Diagramas de flujo.

6.6.7 Manual de Funciones de la Aplicación

En estos documentos se describen a nivel de tareas, las actividades realizadas por los empleados que están relacionadas con cada una de las aplicaciones auditadas. Este manual, al igual que el de
procedimientos, facilita la identificación de responsabilidades frente a cualquier eventualidad con respecto a la aplicación.

**Estructura del Manual de Funciones de la Aplicación:**

- Nombre de la empresa.
- Nombre de la aplicación.
- Identificación del manual.
- Fecha de elaboración.
- Fecha de la última actualización.
- Lista de cargos relacionados con la aplicación.
  - Nombre del cargo.
  - Dependencia.
  - Jefe inmediato.
  - Descripción del cargo.
  - Requisitos mínimos (estudios, experiencia).
  - Descripción de funciones a realizar.

### 6.7 BIBLIOGRAFÍA


www.dorado.une.edu.ve/biblio/auditoría
UNIDAD III. AUDITORÍA AL CENTRO DE INFORMÁTICA

CAPÍTULO 7

ELEMENTOS TEÓRICOS Y PRÁCTICOS

7.1 INTRODUCCIÓN

Actualmente la información se considera un activo muy valioso para cualquier empresa moderna y eso se ve reflejado a diario en la creciente dependencia en los procesos computarizados para procesar su información y tomar decisiones estratégicas y tácticas.

Las empresas han tomado conciencia de las ventajas de la informática, pero no sucede lo mismo en cuanto a la necesidad de asumir ciertas seguridades que le permitan recuperarse rápidamente de las eventualidades que se puedan presentar en esta área por la vulnerabilidad que acarrean los sistemas computarizados, debido en parte al vertiginoso avance de la tecnología que ha llevado a incrementar la complejidad de los centros de informática, teniendo poco control sobre la utilización de los equipos y de otra parte a que no existe una formalización de la seguridad informática tanto física como lógica al interior de la empresa; obedeciendo ésta más bien a la iniciativa de unos pocos empleados o funcionarios.

En los últimos años hemos visto asombrados como se han incrementado los crímenes a los centros de informática con transferencias indebidas de fondos, colocación de bombas y particularmente cabe mencionar algunos fraudes cometidos a través de computadoras en nuestro país, como el de las Empresas Públicas de Barranquilla, en donde se vieron abocados a implementar una auditoría de sistemas debido a que en la facturación sistematizada de teléfonos aparecían llamadas de larga distancia internacionales cargadas a suscriptores que nunca las habían hecho; también es conocido el fraude de Cajanal, en donde se activaron pensionados fallecidos hace muchos años, a los cuales se les estaba liquidando normalmente sus mesadas; por último el fraude a los Seguros Sociales, en el cual varias empresas que nunca hacían sus aportes fueron retiradas del listado de morosos, por lo cual la entidad perdió grandes cantidades de dinero, así mismo existen muchos otros casos que tal vez no se han detectado o no han salido a la luz pública.

Con la presente unidad se pretende aportar una herramienta analítica y comprensiva desde el punto de vista administrativo y técnico que facilite el dimensionamiento de los problemas y permita un adecuado desarrollo del centro de informática, mediante una mejor organización y administración, según lo demandan las empresas actuales.

7.2 OBJETIVOS DE LA AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

A continuación se presentan los objetivos más importantes que persigue la auditoría de sistemas al centro de informática, los cuales se encuentran agrupados en objetivos generales y objetivos específicos, de la siguiente forma:
**7.2.1 Objetivos Generales**

- Revisar que exista planeación estratégica de sistemas de información y que los planes a largo plazo del centro de informática sean coherentes con los planes a corto plazo y a su vez, que todos ellos estén enmarcados dentro de la planeación estratégica de la empresa.

- Revisar la definición e implantación de políticas del centro de informática.

- Evaluar la funcionalidad de la estructura orgánica del centro de informática.

- Velar porque los recursos económicos, técnicos y humanos asignados al centro de informática sean suficientes.

- Velar por el suministro de información consistente, actualizada, permanente y necesaria a toda la organización, propiciando el desarrollo armónico de los sistemas de información.

- Buscar la integración de los sistemas de información de la empresa, con el anhelo de minimizar costos y evitar duplicidad de esfuerzos.

- Revisar que los estándares estén debidamente documentados con base en el análisis de riesgos.
7.2.2 Objetivos Específicos

- Velar por la integridad y confiabilidad de la información
- Evaluar la protección y conservación de los bienes informáticos de la empresa.

- Recomendar la existencia de pautas sobre la renovación y/o adquisición tanto de software como de hardware, para que no obedezcan estas decisiones a circunstancias temporales.
- Velar por la existencia de un plan maestro que guíe la implementación de todos los sistemas de información, que incluya la prueba integral del sistema, adecuación, aceptación por parte del usuario, entrenamiento, entrega formal del sistema a los usuarios, documentación, back-ups, etc.
- Velar para que se prueben periódicamente los planes de seguridad, localizando los problemas y presentando alternativas de solución.
- Revisar que el plan de contingencias contemple aspectos relacionados con hardware, software, documentación, talento humano y soporte logístico.
- Evaluar el sistema de costeo aplicable a cada uno de los proyectos de sistemas de información, motivando a los directivos, técnicos y usuarios a actuar razonablemente.
- Evaluar las políticas para segregación y rotación de funciones, así como de capacitación del talento humano.

7.3 JUSTIFICACIÓN DE LA AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

La seguridad de las computadoras, por lo general, no es un tema que se considere en forma apropiada por los directivos de las empresas, la importancia y apoyo que se le da es relativamente poca, ello se debe a que no están al tanto de la atención que requieren los centros de informática, ya que éstos son muy vulnerables y se encuentran expuestos a robos, fraudes, sabotaje, vandalismo, interrupción de actividades, pérdida de información, sobrecargas eléctricas, tempestades y demás desastres naturales; aunque es bueno tener presente que muchos de los riesgos no provienen del exterior de la empresa, sino que se originan al interior del centro de informática o áreas usuarias, como son la presencia de errores, omisiones, concentración de funciones administrativas y operativas, empleados desmotivados, descuidados, mal remunerados, deshonestos, etc.
Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano, motor de desarrollo y vida de los sistemas de información; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por lo tanto, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la empresa.

De acuerdo a esta perspectiva, se puede apreciar que la complejidad es amplia y de gran trascendencia para las empresas, por lo tanto, la auditoría de sistemas al centro de informática es fundamental y tiene como propósito brindar apoyo a través de la orientación y asesoría irrestricta a todos sus funcionarios para que logren el cabal desempeño de sus funciones.

7.4 PLANEACIÓN DE LA AUDITORÍA PARA EL CENTRO DE INFORMÁTICA

Con el propósito de allegar el mayor flujo de información, se ha diseñado un formulario para que sea diligenciado por el jefe y directivos del centro de informática y el cual recoge los siguientes aspectos: (ver anexo N° 12).

I. Identificación.
II. Características generales.
   - Estructura orgánica de la empresa.
   - Políticas y objetivos de la empresa.
   - Políticas del centro de informática.
Objetivos generales y específicos del centro de informática.
Personal del centro de informática.

III. Recursos informáticos.
- Inventario y distribución de hardware.
- Inventario de software operativo.
- Inventario de software de utilidad.
- Breve descripción de las aplicaciones en funcionamiento.
- Breve descripción de las aplicaciones en desarrollo.
- Breve descripción de las aplicaciones por desarrollar.

IV. Aspectos de Auditoría.
- Personal de auditoría involucrado en las etapas de desarrollo de software.
- Usuarios involucrados en las etapas de desarrollo de software y participación.
- Conceptos de auditoría que incluye el software desarrollado.

- Documentación del centro de informática: plan estratégico de sistemas, metodologías y estándares de desarrollo de software, procedimientos de respaldo, plan de contingencias, plan de mantenimiento, pólizas/seguros, manual de funciones, manual de procedimientos, manual técnico, manual del operador, manual del digitador.
- Descripción de auditorías previas internas o externas.

V. Observaciones

Recopilada toda la información a través de distintas fuentes como son el jefe y funcionarios del centro de informática, así como por observación directa, se procede a concertar reuniones con las partes interesadas para analizar los resultados obtenidos y se elabora un informe escrito de los hallazgos inicialmente encontrados, que serán la fuente para delinear el alcance que tendrá la auditoría.

7.5 PROGRAMA DE AUDITORÍA DE SISTEMAS PARA EL CENTRO DE INFORMÁTICA

Los pasos que involucra el programa de auditoría de sistemas para el centro de informática son:

1. Objeto de la auditoría.
2. Soporte legal.
3. Alcance.
4. Metodología a aplicar.
5. Tiempo estimado de realización.
6. Lugar donde se desarrollará la auditoría.
7. Conformación del equipo auditor.
8. Recursos logísticos y técnicos necesarios.
Estos pasos están ampliamente descritos en el capítulo II, numeral 2.5, por lo tanto, en este aparte se hará referencia concretamente a la metodología y alcance que son muy propios para efectuar la auditoría al centro de informática.

7.5.1 Metodología a seguir

Con base en la información recopilada en el anexo N° 12. Planeación de la auditoría al centro de informática, así como en las visitas, entrevistas y observaciones efectuadas, se procede a diseñar los cuestionarios de control interno, los procedimientos, los papeles de trabajo e informes de auditoría, aspectos todos que se analizan detalladamente en los numerales 7.6, 7.7, 7.8, y 7.9, respectivamente de ésta unidad.

7.5.2 Alcance

A continuación se expone un esquema general del alcance que puede tener la auditoría de sistemas al centro de informática, con el propósito único que sirva de punto de referencia para futuros trabajos de auditorías.

Alcance propuesto:

I. Aspectos administrativos:
   • Evaluación de la planeación estratégica de sistemas de información (PESI).
   • Evaluación de políticas administrativas.
   • Análisis organizacional.
   • Análisis de estándares.
   • Análisis del talento humano.

II. Aspectos técnicos.
   • Evaluación de políticas técnicas.
   • Evaluación del desarrollo de sistemas.
   • Evaluación de la implementación de sistemas.
   • Evaluación de controles de entrada de datos, salida de datos, mantenimiento, operación y software del sistema.

III. Aspectos de seguridad.
   • Evaluación de políticas de seguridad.
   • Ubicación e Instalaciones.
   • Personal.
   • Equipos.
   • Documentación.
   • Back - ups.
   • Pólizas/seguros.
   • Plan de contingencias.
Una vez definido el alcance de la auditoría, se prepara un formato para estimar los tiempos que demandará la realización de cada una de las actividades allí descritas, (ver anexo N° 13. Auditoría al centro de informática - estimación de tiempos), adicionalmente ésta información sirve de base para confeccionar el cronograma de actividades, pasos que han sido debidamente explicados en el capítulo 2.

7.6 CUESTIONARIO DE CONTROL INTERNO PARA SER APLICADO AL CENTRO DE INFORMÁTICA

Se presenta a continuación el diseño del cuestionario de control interno para ser aplicado al centro de informática, el cual se encuentra dividido en tres módulos para facilitar su análisis, de la siguiente forma:

- Aspectos Administrativos. Agrupa los siguientes elementos: planeación estratégica de sistemas, políticas administrativas, análisis organizacional, estándares, talento humano que considera: administración y organización, ambiente laboral, entrenamiento y capacitación, desempeño, supervisión, motivación, remuneración, elementos financieros.

- Aspectos Técnicos. Agrupa los siguiente elementos: desarrollo e implementación de sistemas, entrada de datos, salida de datos, mantenimiento, operación, software del sistema.

- Aspectos de Seguridad. Agrupa los siguientes conceptos: seguridad física, instalaciones, personal, equipos, documentación, back-ups, pólizas/seguros, plan de contingencias.

7.6.1 Cuestionario de Control Interno para Aspectos Administrativos

Planeación Estratégica de Sistemas de Información (P.E.S.I)

- Son los objetivos del centro de informática coherentes con los objetivos de la organización? En el desarrollo de la planeación para la organización, las actividades del centro de informática deben plantearse de manera que los objetivos, ya sean a corto o a largo plazo, estén de acuerdo con los objetivos de la organización.

- Son los planes a corto plazo del centro de Informática, coherentes con los planes a largo plazo? El centro de informática debe velar porque los planes a corto plazo sean coherentes con los planes a largo plazo y que le sean asignados los recursos adecuados y suficientes, que garanticen su normal funcionamiento.

- Existe compromiso a nivel de dirección con aquellos aspectos informáticos? Se debe comprometer a un grupo de funcionarios a nivel de dirección, para que coordinen con el comité de informática, los objetivos y metas de la organización en lo atinente a aspectos informáticos.

- Quien determina las metas a largo plazo del centro de informática? En el desarrollo de los planes a largo plazo, es el jefe del centro de informática quien debe identificar las metas a largo plazo del centro a su cargo y verificar que éstas sean coherentes con las metas de la organización, considerando los cambios, los avances tecnológicos y la normatividad vigente.
• Es considerado el cronograma como herramienta de planeación? El cronograma debe ser considerado como herramienta de planeación y control de gestión en el desarrollo de sistemas.

• Hay amplia participación en la elaboración de la PESI? El proceso de planeación debe ser participativo, de tal manera que permita involucrar las ideas y aportes de gran parte de los funcionarios.

• A cuánto tiempo está proyectada la PESI? Un plan estratégico de sistemas no debe proyectarse a más de tres años y su gestación debe durar aproximadamente ocho semanas; ésto implica ser muy creativo y tener el respaldo de la gerencia para su formulación y puesta en marcha. La planeación estratégica de sistemas de información debe ser un proceso cíclico, periódico, que cubra espacios no muy extensos de tiempo, debido a la incertidumbre que conlleva el rápido cambio tecnológico.

• Es evaluada periódicamente la PESI? Se debe adoptar una política rigurosa con respecto a las evaluaciones o revisiones del plan. De un lado la dinámica de los proyectos permitirá hacer un seguimiento estricto a cada una de las acciones formuladas, por lo menos cada mes; de otro lado, el plan estratégico debe ser evaluado por lo menos cada seis meses en forma integral, incorporando los nuevos factores y experiencias en las ejecuciones del último período evaluado.

• Considera la PESI pautas para renovación y/o adquisición de software y hardware? Dentro de la PESI se deben señalar pautas sobre renovación y/o adquisición tanto de hardware como de software, para que no obedezcan estas decisiones a circunstancias del momento.

• Considera la PESI aspectos atinentes a la seguridad? Como parte integral de la planeación computacional a largo plazo, se deben incorporar objetivos y estándares de seguridad.

• Considera la PESI un análisis de costo/beneficio? Se debe elaborar técnicamente el plan, donde se determine los costos y se compare contra los posibles beneficios, transmiéndole al usuario de sistemas las bondades que esos cambios traerán a la organización.

Políticas Administrativas

• Existe una clara definición de políticas al interior del centro de informática? Se debe velar por una definición e implantación de políticas dentro del centro de informática con respecto a:

  • Elaboración y evaluación del plan estratégico de sistemas de información.
  • Integración de los sistemas de información.
  • Legalización de todo el software utilizado.
  • Implementar un sistema de costos por aplicación.
  • Buena y oportuna capacitación a todos los niveles funcionales del centro de informática.
  • Evaluación periódica del desempeño del personal.
  • Segregación de funciones para garantizar eficiencia y eficacia en el control interno.
  • Rotación de funciones.
  • Establecer vacaciones anuales obligatorias.
Los altos mandos deben monitorear el grado de cumplimiento de los planes y políticas establecidas en el desarrollo, operación, mantenimiento y control de los sistemas de información de la organización.

**Análisis Organizacional**

- Es evaluada periódicamente la estructura orgánica del centro de informática? Es conveniente realizar evaluaciones periódicas en términos de funcionalidad de la estructura orgánica del centro de informática. Dicha evaluación deberá contemplar la calidad y efectividad de las relaciones y resultados del servicio del centro hacia las demás unidades de la organización. El diagnóstico periódico permitirá aplicar correctivos frente a reales o potenciales deficiencias e inclusive facilita el planteamiento sustentado del rediseño organizacional en el centro de informática.

- Hay separación de funciones entre la captura de datos y la programación? Las operaciones que involucran el proceso de datos, deben estar totalmente separadas de las funciones de sistemas y de programación.

- Existen procedimientos escritos que indiquen como realizar cambios o modificaciones a programas? Se debe elaborar un procedimiento claro que indique como hacer las modificaciones a los programas, debe estar debidamente documentado y ponerse en práctica.

- Existen mecanismos que permitan la suspensión inmediata de empleados deshonestos? Se debe definir un mecanismo que permita la suspensión inmediata de aquellos empleados que representen algún riesgo para el centro de informática, originados por malos manejos o actitudes indebidas.

- Existen procedimientos escritos que señalen la forma de reportar las dificultades presentadas durante las diferentes etapas del procesamiento de información? Se debe establecer un procedimiento para reportar dificultades en los menús, en las corridas de la aplicación, en los reportes producidos, en la documentación existente; de tal manera que garantice el adecuado mantenimiento de la misma.

**Estándares**

- Existen estándares escritos claramente definidos? El centro de informática debe definir, coordinar y comunicar al personal involucrado, los estándares que regulan la adquisición de los recursos informáticos, el diseño, desarrollo, implementación y mantenimiento del software, así como la operación de los sistemas de información.

- Se realiza un análisis de necesidades previo a la adquisición de software y hardware? Se debe realizar un estudio de necesidades profundo y previo a la adquisición de hardware y software, tanto de los requerimientos inmediatos como futuros a corto y mediano plazo.

- Se actualiza con periodicidad el software y el hardware utilizado? Se debe actualizar hasta donde sea posible el hardware y el software de acuerdo con los avances de la tecnología, sin embargo, no se deben efectuar cambios profundos en el equipo de computación en menos de dos años, ya que sería imposible obtener una tasa de rendimiento aceptable sobre la inversión realizada.
Son autorizadas por los usuarios las modificaciones a las aplicaciones? La puesta en funcionamiento de las nuevas aplicaciones y de los cambios en las ya existentes, deben ser aprobados por los usuarios.

Existe integración en los sistemas de información? La integración de las aplicaciones debe ser uno de los objetivos en el desarrollo de los sistemas y se debe adoptar como estándar del centro de informática.

TALENTO HUMANO

Administración y Organización.

- Existen políticas sobre planeación del talento humano del centro de informática? Deben existir políticas muy bien definidas con respecto a la planeación del personal requerido y su vinculación al centro de informática, así mismo, deben estar contempladas dentro de la PESI.

- Conoce el reglamento interno de trabajo a nivel organizacional y a nivel del centro de informática? El reglamento de trabajo y los procedimientos propios del centro de informática deben ser conocidos ampliamente por su correspondiente personal.

- Existen políticas de salud ocupacional al interior del centro de informática? Todo centro de informática debe tener políticas definidas de salud ocupacional orientadas a sus funcionarios y ponerlas en práctica, para obtener así un mayor rendimiento dado los altos índices de fatiga y estrés que allí se manejan.

- Existe un programa de trabajo al interior del centro de informática? Debe existir un programa de trabajo que se lleve rigurosamente, por lo tanto, se aconseja la utilización de cronogramas como herramientas de control.

Entrenamiento y Capacitación

- Existen programas permanentes de capacitación? Se debe optar como política interna al centro de informática, el permanente entrenamiento y capacitación dirigida a los distintos niveles funcionales en aquellos aspectos más relevantes tecnológicamente y que proporcionen un beneficio directo a la organización, con el propósito de cubrir aquellas plazas que son dejadas por personal con alta formación y experiencia o cuando se requiera de personal adicional para ejecutar ciertas actividades a realizar en períodos críticos, evitando así que el centro de informática se vea abocado a traumas por el insuficiente talento humano capacitado, sobre todo en tecnologías de punta.

- Son evaluados los cursos impartidos? Los cursos tanto internos como externos, una vez hayan sido impartidos, deben ser evaluados por los participantes como también por los docentes, con el propósito de analizar si cumplieron con los objetivos propuestos y así mantener una constante retroalimentación.
Existe material bibliográfico actualizado y disponible? Complementario a los manuales suministrados por los proveedores, se debe adquirir con frecuencia material bibliográfico especializado, con el propósito de facilitar la autocapacitación a nivel interno.

Ambiente laboral del centro de informática

• Cómo es el ambiente laboral del centro de informática? El buen desempeño laboral del empleado depende de los aspectos físicos, técnicos, sociales y psicológicos que lo rodean.

• Es alta la rotación del personal del centro de informática? Es conveniente conocer el índice de rotación de los empleados del centro de informática y sus posibles causas, para así tomar las acciones pertinentes, corrigiendo este flagelo que entorpece el buen desarrollo de los sistemas de información.

• Existen políticas sobre reemplazamiento de personal? Se deben definir políticas que prevean el reemplazamiento de personal, sobre todo a nivel de programadores y analistas, de tal forma que no se altere la marcha normal del centro de informática.

• Se exigen exámenes médicos y psicológicos especiales como requisito de vinculación al centro de informática? Las políticas hacia el personal son un elemento esencial dentro de la seguridad en computación, por lo tanto, en la selección de personal no solo se deben realizar las pruebas tradicionales, sino que también es importante determinar a través de los exámenes médicos, la capacidad que tiene la persona para trabajar en situaciones de estrés; así mismo, se deben realizar pruebas psicológicas que permitan evaluar aptitudes, actitudes y estabilidad general del aspirante.

• Existen políticas con respecto a las vacaciones del personal? Las vacaciones anuales deben ser tomadas obligatoriamente por todo el personal del centro de informática de forma ininterrumpida y por ningún motivo se debe permitir su acumulación; ausencia del titular del cargo que puede ser aprovechada para la aplicación de determinados controles y evaluación del cargo.

• Se realiza un análisis de referencias y antecedentes previo a la vinculación de personal? El análisis de las referencias y antecedentes son primordiales, ya que la seguridad e integridad de los recursos informáticos dependerá siempre de la lealtad del personal.

• Existen programas de inducción? El procedimiento de inducción del personal de sistemas se debe establecer formalmente y llevarse a cabo bajo la coordinación del jefe del centro de informática.

Desempeño

• Posee el centro de informática estándares de desempeño? El centro de informática debe definir concretamente los estándares de desempeño, especificando las normas e instrucciones que se deben seguir para obtenerlo.

• Periódicamente se realizan evaluaciones del desempeño? Al interior del centro de informática se debe llevar un registro de las evaluaciones del desempeño del personal, con el propósito de
conocer las habilidades y destrezas para ejercer el cargo, así mismo sirve con fines de ascensos, promociones, renovación de contratos, etc.

**Supervisión**

- Es alto el índice de ausentismos y retardos? Se debe establecer un horario de trabajo para todos los digitadores, programadores y analistas, de tal manera que permita llevar un control de ausentismos y retardos del personal.

- Como es la disciplina laboral de los funcionarios del centro de informática? Todos los funcionarios deben mantener una excelente disciplina laboral, sin importar la jerarquía del cargo que se esté ejerciendo.

- Existen conflictos laborales al interior del centro de informática? Las buenas relaciones y entendimiento entre analistas, diseñadores, programadores y digitadores, hacen parte de un ambiente propicio de trabajo, además coadyuva a elevar la eficiencia y rendimiento del personal.

- Cuando se presentan quejas y/o reclamos, son atendidas oportunamente? El excelente clima laboral que debe reinar dentro del centro de informática se debe en parte al oportuno y buen tratamiento que se le brinde a las quejas y reclamos, no permitiendo el crecimiento de los conflictos laborales.

**Motivación**

- Existe motivación al interior del centro de informática? Son varios los factores que ayudan a elevar la motivación de los funcionarios, propiciando por ende el logro de los objetivos del centro; por lo tanto, es responsabilidad del jefe inmediato y de las directivas de la organización, facilitar las condiciones y brindar los estímulos necesarios para obtenerlo.

- Existen políticas de ascensos y promociones? Se deben establecer procedimientos para que basado en el desempeño y capacidades de los funcionarios, se les brinde la oportunidad de obtener ascensos y promociones.

**Remuneración**

- Están adecuadamente remunerados los cargos del centro de informática? Los cargos deben ser remunerados conforme a las funciones desempeñadas, por lo tanto, es necesario establecer una escala salarial adecuada y competitiva con cargos similares desempeñados en otras empresas o instituciones, para evitar así la rotación de personal altamente calificado.

- Existe una metodología para estimar tiempos y costos de cada proyecto informático? Se debe establecer una metodología que permita estimar los costos y tiempos de duración de cada proyecto y que no obedezca solo a la experiencia de los miembros del comité del centro de informática.
Elementos financieros

- Existe un sistema de costeo por aplicación? Se debe establecer un sistema de costeo que cuantifique la operación de cada una de las aplicaciones, aprovechando los registros que proporcionan el equipo de computación a través de los reportes generados de su propia contabilidad. Una vez determinados los costos de operación por aplicación, se deben dar a conocer a los usuarios respectivos y motivarlos a actuar razonablemente.

- Existe una metodología para estimar tiempos y costos de cada proyecto informático? Se debe establecer una metodología que permita estimar los costos y tiempos de duración de cada proyecto y que no obedezca solo a la experiencia de los miembros del centro de informática.

7.6.2 Cuestionario de Control Interno para Aspectos Técnicos

Desarrollo e Implementación de Sistemas

- Son frecuentemente interrumpidos los proyectos de sistemas? Los proyectos de sistemas no deben ser interrumpidos durante su desarrollo, salvo en casos excepcionales como son los cambios de legislación. Cuando se presentan solicitudes urgentes por parte de los usuarios, éstas deben ser canalizadas y estudiada su viabilidad y desarrollo por parte de un equipo diferente al de producción. Se debe evitar al máximo convertir el centro de informática en una oficina apaga incendios, lo que arrojaría resultados negativos a la planeación de sistemas.

- Existen estándares de producción definidos? Se deben definir estándares de producción por parte de la dirección del centro de informática que permita monitorear el desarrollo e implementación de todo proyecto a través de la ejecución de cada una de sus etapas, lo que facilitará tomar los correctivos adecuados garantizando un proceso de desarrollo ordenado, además, mantiene a todas las partes concentradas hacia los aspectos propios de cada sistema dentro de las fechas programadas, proporcionando un permanente monitoreo sobre el trabajo del personal de sistemas.

- Existe integración entre subsistemas? La integración de los diferentes subsistemas debe ser uno de los objetivos primordiales en el desarrollo de los sistemas de información.

- Existen políticas para aplicaciones soportadas por teleproceso? Se deben establecer políticas para aplicaciones que requieran soportarse por teleproceso y que incluyan aspectos tales como red de comunicaciones a utilizar, tipo de mensajes requeridos, tráfico esperado de las líneas de comunicación, etc.

- Como se evalúan los sistemas de información? La evaluación de los sistemas de información se debe llevar a cabo cuando el sistema se haya implementado y se encuentre trabajando normalmente, con el fin de que el usuario tenga la suficiente información para su manejo, operación y aceptación.

- Como se administran los proyectos informáticos? Para tener una buena administración de proyectos, se requiere de la elaboración de un plan en el que se especifiquen las actividades, metas, personal participante, recursos, tiempo y costos. Este plan debe ser revisado periódicamente para
evaluar el avance respecto a lo programado. Estas normas deben estar enmarcadas dentro de los lineamientos generales de la organización y del contexto particular de la dirección de informática.

- Se revisan periódicamente los sistemas en funcionamiento? Se deben llevar a cabo revisiones periódicas de los sistemas en funcionamiento mediante la realización de pruebas del sistema, que permitan garantizar que se cumplan los requisitos de las especificaciones funcionales, verificando transacciones, estadísticas, archivos, reportes producidos, registrando las fallas ocurridas y realizando los ajustes necesarios, con el propósito de comprobar que las aplicaciones cumplan con los requerimientos del usuario, que tengan los controles necesarios y que cumplan con los objetivos para los cuales fueron diseñados.

- Existe una adecuada segregación de funciones? Los analistas de sistemas no deben ejercer funciones de diseñadores y programadores, porque no es aconsejable desde el punto de vista de la auditoría de sistemas. Debe existir una adecuada segregación de funciones que brinde seguridad y confiabilidad a la aplicación.

- Es tenido en cuenta al usuario durante las etapas de análisis y diseño de la aplicación? Debe existir una mayor participación del usuario en las etapas de análisis y diseño de sistemas, y esto se logra mediante una completa comunicación entre usuarios y analistas de sistemas, definiendo en ella los elementos con que cuenta el usuario, las necesidades de procesamiento de información, requerimientos de información de salida, calidad de la información, riesgos y forma de minimizarlos a través de controles.

- Son programados los mantenimientos a las aplicaciones? Se debe establecer un procedimiento para realizar el mantenimiento de las aplicaciones, de tal forma que no obedezca a iniciativa de los analistas de sistemas. Se debe tener un proceso de prueba exhaustivo y llevado a cabo por personal diferente al que realizó las modificaciones. Cuando se haga mantenimiento a un programa, debe ser entregado al oficial de la instalación o jefe de producción, quien lo colocará en la biblioteca de producción.

- Tienen los analistas acceso directo a los archivos de la aplicación? El analista de la aplicación no debe tener acceso directo a los archivos de la aplicación ni a la biblioteca. Se debe disponer de una biblioteca de producción, en donde solo el oficial de la instalación o su delegado pueda modificar los programas y de una biblioteca de prueba, donde el analista responsable de la aplicación pueda realizar las modificaciones a los programas existentes o agregar nuevos módulos a la aplicación.

- El operador del equipo es responsable de la cintoteca? Se debe responsabilizar la custodia de la cintoteca a un funcionario de centro de informática, que no tenga que ver con la operación del equipo.

**Entrada de Datos**

- Se utilizan técnicas de verificación durante la grabación de datos? Se deben usar técnicas de verificación cuando se está grabando en cinta o en disco, para que se garantice el mínimo de errores. Se debe solicitar contrasincronía en aquellos programas interactivos de grabación considerados críticos.

- Son verificados los datos de entrada? Los datos de entrada deben estar debidamente probados y verificados con el propósito de evitar inconsistencias en el flujo de información a ser procesado.
- Hay libre acceso al cuarto de la computadora? Se debe restringir el acceso al cuarto de la computadora solo a personal autorizado.

- Los analistas de sistemas tienen acceso a los datos y programas de la aplicación? Se debe restringir el acceso del o los analistas encargados de la aplicación a solo consulta.

- Existen procedimientos escritos para el tratamiento de errores? Se deben elaborar procedimientos escritos para el manejo de errores, con el fin de proporcionar al usuario de la aplicación instrucciones comprensivas para la detección de errores en documentos fuente, en corrida de programas, en la captura de datos, etc.

- Pueden los funcionarios del centro de informática acceder al equipo y a las instalaciones por fuera del horario oficialmente establecido? Se debe exigir autorización escrita para laborar por fuera de la jornada ordinaria y ésta debe ser otorgada solo para casos excepcionales y plenamente justificados.

- Son fechados todos los movimientos o transacciones que ingresan al sistema? Todas las transacciones o movimientos deben ser fechados, sellados y registrados desde la entrada al sistema, cuadrando número de cupones, cantidad de dinero, bancos, etc., según lo demande cada aplicación.

- Están totalmente etiquetadas las cintas y discos? Se deben etiquetar tanto interna como externamente la totalidad de las cintas y discos magnéticos removibles.

- Están adecuadamente almacenados los documentos fuente? Se deben archivar los documentos fuente en un lugar seguro para prevenir modificaciones no autorizadas o el uso no autorizado antes de su procesamiento; así mismo, se deben definir políticas con respecto al tiempo que se deben almacenar los documentos fuente y el procedimiento para disponer de ellos. Preferiblemente este proceso se debe realizar a través de microfilmación.

- Se lleva un registro de documentos en tránsito? Se debe llevar un registro de documentos en tránsito que incluya origen y hora de recepción. Se debe garantizar que todas las transacciones sean transmitidas desde el punto de origen hasta el punto de procesamiento.

- Se registran los datos en formatos preimpresos? Se debe chequear que los datos se registren en formatos preimpresos, permitiendo uniformidad y minimizando errores y omisiones.

- Existe segregación de funciones entre la preparación y alimentación de los datos? Debe existir una adecuada segregación de funciones durante las fases de preparación y alimentación de datos, para garantizar la integridad de los mismos.

### Salida de Datos

- Están plenamente identificados los reportes generados? Todos los reportes generados por el centro de informática deben llevar encabezamiento donde se indique la descripción del reporte, fecha de elaboración y vigencia entre otros aspectos; así mismo, deben ser entregados con oficio remisorio.
• Están totalmente fechados y paginados los informes producidos? Todos los informes generados por el sistema de computación deben estar fechados, paginados y deben llevar el indicativo de final de reporte cuando éste haya culminado.

• Se controla la calidad de la información producida? El control de calidad de la información producida por el centro de informática debe ser una función formalmente asignada a un funcionario del centro y no dejar que ésta responsabilidad obedezca a la iniciativa de los operadores del sistema.

• Está bien protegida la información confidencial? Se debe velar porque no se obtengan fotocopias o copias de la información confidencial sin la debida autorización. Sólo el personal autorizado debe tener acceso a la información confidencial.

• Es destruida la información confidencial escrita no utilizable? La información confidencial escrita no utilizable, así como las corridas abortadas y el papel carbón, se deben picar o destruir antes de proceder a botarla, previa elaboración de la correspondiente acta.

• Existe un procedimiento para la corrida de trabajos especiales o delicados? Cuando se corra un trabajo especial o delicado, se deben emplear dos operadores y solicitar la presencia de una persona del área usuaria durante la impresión de los resultados de aquellas aplicaciones que no son formalmente entregadas al usuario.

• Se lleva un control de las transacciones generadas por el sistema? Se debe llevar un control de transacciones generadas por el sistema, obteniendo un reporte diario de aquellas transacciones extremas, cantidad promedio de transacciones, promedio recaudado en dinero; revisando si los cálculos fueron ejecutados correctamente, etc.

• Cómo se controla la ejecución de las aplicaciones? Se debe condicionar la ejecución de las aplicaciones a terminales específicas, indicando día y hora de utilización dependiendo de la seguridad que demande cada aplicación.

• Cómo se controlan las actividades del operador del equipo de computación? Se debe limitar al operador del sistema de computación para que no ejecute ciertas funciones que pueden vulnerar la integridad del mismo, como son cierres del sistema, rastreo de errores, captura de información, acceso a diagramas y listados fuentes de programas, modificación de datos, etc.

• Se rotan periódicamente a los operadores? Se deben rotar periódicamente a todos los operadores del equipo de computación en la medida que sea posible y los recursos así lo permitan.

• Se controla la corrida de los programas? Se debe llevar un registro de control de corridas de cada aplicación o programa, cubriendo conceptos como inicio de sesión, condiciones para reinicio, instrucciones de consola, de verificación, preparación de datos, fecha de proceso, firma de responsables, etc.
Mantenimiento

- Se programa la utilización del equipo de computación? Se debe programar la utilización del equipo para evitar la caída del sistema, como ocurre generalmente en las horas pico, en donde su utilización puede ser del 100%.

- Existe un plan de mantenimiento a las aplicaciones? Se debe elaborar un plan de mantenimiento para las aplicaciones, el cual debe ser administrado por el jefe del área de producción en cuanto a su ejecución se refiere.

- Se le avisa oportunamente a los usuarios cuando se va a apagar el equipo central? Antes de apagar el equipo central se les debe avisar a todos los usuarios que en ese momento estén activos, con el propósito de no estropear algún proceso.

- Cómo se controla el mantenimiento al equipo de computación? Se debe controlar el acceso y salida al área de sistemas, de los proveedores del servicio de mantenimiento.

- Se lleva un registro del mantenimiento de las UPS? Se debe llevar un registro de mantenimiento de las UPS cada dos meses y el cambio de baterías de estas unidades debe efectuarse rigurosamente cada año.

- Son atendidas oportunamente las quejas, reclamos y sugerencias formuladas por los usuarios? Se debe implementar un procedimiento que permita registrar las quejas, reclamos y sugerencias que tienen los usuarios, con el fin de efectuar la evaluación periódica de las mismas y hacer los ajustes correspondientes cuando se considere pertinente.

Operación

- Existe una adecuada segregación de funciones al interior del centro de informática? Se debe mantener una adecuada segregación de funciones dentro del centro de informática, de acuerdo con las normas de responsabilidad y de control interno.

- Se encuentran varias personas capacitadas en el funcionamiento de cada aplicación? Todas las aplicaciones deben tener asignadas dos personas, como mínimo, que conozcan su funcionamiento.

- Pueden los analistas y diseñadores de sistemas operar el equipo de computación? Únicamente los operadores del sistema de computación deben operar el equipo, debido a razones obvias de seguridad.

- Con qué frecuencia son reprocesadas las aplicaciones? Se deben llevar estadísticas de los reprocesos e identificar claramente las razones que los ocasiona, para reducirlos a un porcentaje tolerable.

- Se rotan periódicamente a los operadores? Se debe rotar periódicamente a todos los operadores del equipo de computación en la medida que sea posible y los recursos así lo permitan.
Cómo se controlan las actividades del operador del equipo de computación? Se debe limitar al operador del sistema de computación para que no ejecute ciertas funciones que pueden vulnerar la integridad del mismo, como son cierres del sistema, rastreo de errores, captura de información, acceso a diagramas y listados fuentes de programas, modificación de datos, etc.

Puede el operador de la computadora ejercer funciones de control de salidas? Los operadores no deben ejercer funciones de control de salidas como conteo de registros, totales de control, control de rechazos, logs de la consola, entre otros, dado que se presta para potenciales fraudes.

Software del Sistema

Existen estándares de calidad del software producido? El control de la calidad del software producido no debe correr por cuenta de la persona que realizó el análisis/diseño de la aplicación; éste debe obedecer a estándares o metodologías previamente definidas.

Se revisan con frecuencia las bitácoras del sistema de computación? Se debe revisar semanalmente las bitácoras del sistema, haciendo un análisis de las interrupciones efectuadas, intento de violaciones, número y frecuencia de accesos indebidos, etc. Se debe establecer ésta revisión como una de las políticas del centro de informática.

Existe un procedimiento para la corrida de trabajos especiales o delicados? Cuando se corra un trabajo especial o delicado, se deben emplear dos operadores y solicitar la presencia de una persona del área usuaria durante la impresión de los resultados de aquellas aplicaciones que no son formalmente entregadas al usuario.

Se lleva control de las transacciones generadas por el sistema? Se debe llevar un control de transacciones generadas por el sistema, obteniendo un reporte diario de aquellas transacciones extremas, cantidad promedio de transacciones, promedio recaudado en dinero; revisando si los cálculos fueron ejecutados correctamente, etc.

Cómo se determinan los controles aplicables a los programas? Se debe determinar el tipo de controles aplicables a todos los programas desde la fase de análisis y diseño, y para aquellos programas que requieran de controles específicos se les debe desarrollar de acuerdo a cada caso, evitando fraudes tipo caballo de Troya, salami, etc.

Cómo se controla la ejecución de las aplicaciones? Se debe condicionar la ejecución de las aplicaciones a terminales específicas, indicando día y hora de utilización dependiendo de la seguridad que demande cada aplicación.

Se controla la corrida de los programas? Se debe llevar un registro de control de corridas de cada aplicación o programa, cubriendo conceptos como inicio de sesión, condiciones para reinicio, instrucciones de consola, de verificación, preparación de datos, fecha de proceso, firma de responsables, etc.
- Los aspectos atinentes a la red como estudio de necesidades, evaluación del software y hardware requerido, análisis costo/beneficio, instalación, reemplazo, etc, están enmarcados dentro de la P.E.S.I.? Todo lo relacionado con la red de comunicaciones de datos debe estar contemplado dentro de la P.E.S.I. para que de esta forma no solo se garantice el cumplimiento de los objetivos y metas trazadas sino también para que exista un compromiso de la alta dirección con su desarrollo y asignación de recursos.

- Existen procedimientos formales que contemplan la seguridad física y lógica de los datos transmitidos entre redes, de tal manera que garanticen la oportunidad, totalidad y exactitud de los mismos? Se deben implementar los controles necesarios que garanticen la protección de los datos que son transmitidos por la red, impidiendo el monitoreo no autorizado, controlando y resguardando los accesos físicos y lógicos a la red, resguardando el software de comunicaciones, así como su respectiva documentación.

- Existe pérdida de mensajes en el sistema de conmutación de datos? Con qué frecuencia se presenta? Se debe controlar la pérdida o modificación de los mensajes durante la transmisión mediante su almacenamiento y posterior reenvío. (sistemas de retardo).

- Con qué frecuencia es revisada la capacidad de transmisión de mensajes? Se deben establecer políticas que contemplan la revisión periódica de la capacidad de transmisión de mensajes, la velocidad de transmisión, la identificación y sincronización de mensajes, etc., con el propósito de reducir su pérdida.

- Se considera la utilización de módems de respaldo? Se deben proveer de módems en áreas críticas con el propósito de salvar dificultades que se puedan presentar entre el centro de informática y aquellos puntos remotos.

- Existe contrato de mantenimiento de los equipos de comunicación de datos? Debe existir un contrato de mantenimiento de los equipos de comunicación, el cual debe ser evaluado permanentemente con el fin de determinar si está cumpliendo adecuadamente con los propósitos para los cuales fue celebrado.

- Es controlada la velocidad y eficacia en la transmisión de datos? A mayor velocidad se encuentre sincronizado el módem, menos tiempo se invertirá en la retransmisión y por ende mayor será el volumen de entrada de datos al sistema. Todo esto se traduce en una menor exposición a la pérdida accidental o intencionada de información a través de la red.

- Existen procedimientos formales que garanticen la seguridad física de terminales, concentradores, multiflexores, módems, tarjetas, terminales y demás equipos de comunicación? Todos los equipos de comunicación deben estar amparados para evitar la pérdida, sustracción y/o deterioro y se deben establecer procedimientos que señalen su forma de operación y funcionamiento responsable de los mismos.

- Son tenidos en cuenta aspectos como crecimiento de la red, la incorporación de nuevos usuarios, respaldos, seguridad, evaluación periódica, etc, que contribuyan al permanente mejoramiento de la red? Se debe realizar periódicamente la evaluación del software, hardware, índice de utilización, crecimiento, seguridad, administración y operación de la red, con el propósito de mantener una constante retroalimentación que redunde en beneficio de una mejor calidad y prestación de servicio.

- Que aspectos considera el software de comunicaciones utilizado en la administración de la red? El software de comunicaciones empleado debe contemplar funciones tales como monitoreo de
actividades, procedimientos de control y seguridad, capacitación y soporte a usuarios, análisis de interrupciones, control de accesos, periféricos conectados, tiempo de conexión, etc.

- Existen estándares formales de administración y operación de la red? Son evaluados periódicamente esos estándares? Los estándares de administración y operación de la red deben considerar aspectos tales como tráfico de la red, tiempo de respuesta, motivo y frecuencia, tiempo de interrupciones, tiempo de reinicio, usuarios, niveles de acceso, periféricos conectados, etc.

- Existe documentación escrita relacionada con la administración y operación de la red? Deben existir manuales escritos dirigidos a los usuarios, operadores y administradores de la red, que le indique la forma como está estructurada, su operación, administración y mantenimiento, señalando con suficiente claridad en los mismos, la manera como se debe actuar en caso de presentarse algún problema con la red.

- Existen procedimientos relacionados con la base de datos? Se deben establecer procedimientos escritos acerca de la estructura, organización, integridad, privacidad, seguridad, respaldo y recuperación de la base de datos.

- Que mecanismos de seguridad son considerados para brindar protección a la base de datos? Para proteger las bases de datos hay que adoptar medidas de seguridad a nivel físico como protección de los equipos que contienen la información, a nivel humano como el grado de confianza en el personal, a nivel del sistema operativo, a nivel de la red de comunicaciones y a nivel propiamente del sistema de gestión de bases de datos (DBMS). En este último nivel se hace referencia a las autorizaciones necesarias para la realización de tareas, perfiles de usuario, concesión de privilegios, el cifrado de datos, la inspección y análisis de los logs o bitácoras de operaciones.

- Brinda el sistema de administración de la base de datos una adecuada protección a la información y datos almacenados? Los sistemas de gestión de bases de datos (DBMS) ofrecen a desarrolladores, administradores y usuarios una gama muy amplia de herramientas que permiten garantizar la integridad, consistencia, confidencialidad, confiabilidad y en general la seguridad de la información almacenada y con un elemento muy importante a favor: las líneas de código que se requieren por parte del implementador son mínimas, en ocasiones solo basta con una sencilla sentencia para obligar al DBMS a controlar y mantener las restricciones necesarias.

- Quién es el responsable del control de la base de datos? El administrador de las bases de datos debe tener control sobre la administración de la base de datos en cuanto al almacenamiento físico, operación, supervisión, recuperación, mantenimiento y documentación; pero el administrador de la base de datos no debe tener acceso a los equipos de computación.

- Existen controles específicos que limitan el acceso a la base de datos? Se deben registrar las solicitudes de acceso, identificando terminal, hora y operador. Definir los perfiles de usuarios para que restrinjan su utilización y limitar el número de usuarios. Registrar las transacciones, controlar los cambios y actualizaciones; pruebas de datos u otro tipo de listados deben ser supervisados y controlados continuamente.

- Se revisa la bitácora de la base de datos? Se debe revisar regularmente la bitácora de reinicios y reprocesos causados por el mal funcionamiento del sistema y analizar las causas que hayan podido generar tal dificultad para que se puedan corregir apropiadamente.
- Es revisado frecuentemente el diccionario de datos? Los cambios permanentes a la base de datos son registrados en el diccionario de datos y aprobados por el administrador de la base de datos? Todos los cambios solicitados deben ser analizados y aprobados por el administrador de la base de datos y deben quedar registrados en el diccionario de datos, porque de esta forma permite realizar un control efectivo en el rastreo de datos.

- Existen estándares relacionados con los programas de la aplicación? Deben haber estándares escritos que orienten el diseño de los programas de la aplicación en donde se especifiquen las llamadas de datos que puedan ser usadas para accesar a la base de datos. La documentación debe contener las entidades, atributos e interrelaciones y debe ser revisada por el administrador de la base de datos antes de que el programa sea puesto en producción.

- Existe documentación escrita relacionada con el respaldo y recuperación de la base de datos en caso de presentarse destrucción parcial o total de ésta? Se debe verificar que haya una documentación específica para el respaldo y recuperación de la base de datos; que considere el copiado de la base de datos a intervalos regulares permitiendo su recuperación automática. La documentación debe incluir procedimientos y estándares para el reinicio y/o recuperación de los datos. El administrador de la base de datos es el responsable de garantizar la integridad, confidencialidad y confiabilidad de la base de datos y igualmente debe velar por que se diseñen, prueben y apliquen planes de contingencias relacionados con la misma.

- Son verificados los accesos y restricciones a las tablas que autorizan las contraseñas de usuarios? Se deben verificar los accesos a las tablas de autorización, revisando: control de terminales, controles del circuito, clase de transacción, programas, archivos, registros, grupo de partidas, control de contraseñas.

- Existen políticas de seguridad relacionadas con el sistema operativo debidamente establecidas al interior de la organización? Cualquier política de seguridad que se establezca debe diseñarse sobre el sistema de protección que posea el sistema operativo, deben estar consignadas por escrito y difundidas ampliamente en el personal técnico.

- Es empleada la criptografía para proteger el almacenamiento y transmisión de información? La criptografía está exenta de regulados sistemas de almacenamiento centralizado de claves, adicionalmente es la protección indicada para aquellas personas que desean mantener la privacidad de la información que se almacena o se transmite a través de la red, porque es segura y confiable. Se debe tener una bitácora de auditoría que permita la reconstrucción de archivos y movimientos, rastreo de datos entre el usuario y la terminal, recuperación de mensajes, etc.

- Se aplica el control de verificación de paridad? Se debe aplicar la verificación de paridad para asegurar que la máquina no está agregando o saltando bits en la transmisión de datos e información.

- Son controlados los accesos no autorizados al sistema? La seguridad de un sistema puede ser más efectiva cuando se restringe el ingreso no autorizado por medio de la identificación del usuario a través de claves de seguridad, tarjetas de acceso, identificación del iris del ojo, identificación de huellas dactilares, etc, y adicionalmente exigiendo autorización para la utilización de los recursos del sistema como controladores, terminales, cintas, discos e impresoras, entre otros y limitando el acceso a los programas, archivos y datos del sistema.
• Quienes están autorizados para sacar copias del sistema? Solo se debe permitir a los usuarios autorizados obtener copias de seguridad del sistema operativo, de los programas y datos almacenados en el sistema.

• Que elementos adicionales son considerados en la seguridad de los datos? Otros elementos que contribuyen a la seguridad de los datos son: identificación del usuario o contraseña, privilegios y autorizaciones para la realización de determinadas tareas o utilización de recursos del sistema, limitaciones para la ejecución de ciertas tareas, seguridad de la estación de trabajo o terminales del sistema, menús obligatorios como acceso al sistema, etc.

• Cómo se administran las claves de acceso? Se debe velar por una adecuada administración de claves (passwords), asignando fechas de vencimiento y recursos a utilizar por usuario; adicionalmente se deben modificar periódicamente las claves de acceso al sistema efectuadas a través de marcación telefónica.

• Se cambian periódicamente las palabras clave (passwords)? Las palabras clave deben ser cambiadas periódicamente dependiendo de cada caso en particular, con el fin de prevenir posibles fraudes o acciones indebidas, por eso es conveniente activar la fecha de cambio obligatorio y la fecha de caducidad de las claves de acceso.

• Se controla el número de intentos fallidos al utilizar la clave de acceso? Se debe limitar el número de intentos fallidos al ingresar la clave, procediendo simultáneamente a inhabilitar la clave y a enviar un mensaje al operador del sistema comunicándole sobre la situación presentada.

• Cómo se controlan las violaciones a la seguridad del sistema? Se deben revisar periódicamente las bitácoras del sistema para observar si se han presentado violaciones a la seguridad del sistema.

• Cómo se controla el acceso a los recursos del sistema? Los accesos a los recursos del sistema deben ser controlados por medio de listas de autorización.

• Existe algún procedimiento para la asignación de cuentas a usuarios? Los nombres de las cuentas de los usuarios deben ser asignados de acuerdo al cargo y no con base en el nombre del usuario, de tal manera que cuando haya cambio de funcionario, solo se tenga que reemplazar la clave, facilitando así su proceso.

7.6.3 Cuestionario de Control Interno para Aspectos de Seguridad

Ubicación e Instalaciones

• Cómo es la ubicación física del centro de informática? La ubicación del centro de informática debe brindar integridad y seguridad a la información y al personal que allí labora, a su vez, debe ser un sitio propicio para laborar.
• Cómo son las instalaciones del centro de informática? El centro de informática debe contar con instalaciones acordes a las necesidades de hoy en día, como son áreas suficientes y diseñadas con adecuadas instalaciones eléctricas, detectores de humo, supresores de fuego, divisiones modulares espaciosas e iluminadas y procurando al máximo la no utilización de materiales inflamables.

• Existe señalización de rutas de evacuación al interior del centro de informática? Se deben señalar las rutas de evacuación en toda la edificación manteniendo libre de obstáculos los pasillos y áreas vecinas al centro de informática. Se debe orientar al personal sobre las acciones a seguir en caso de emergencia, consignando éstas y otras recomendaciones en el manual de seguridad.

• Hay extinguidores dentro del centro de informática? Se debe controlar el tipo de extinguidores y el vencimiento de su carga para cada caso específico según sea la necesidad, así mismo, deben estar ubicados en sitios visibles de fácil alcance y los funcionarios deben recibir instrucción sobre su manejo.

• Dónde se encuentra ubicado el panel de control eléctrico? El panel de control eléctrico y el generador de emergencia deben estar protegidos y fuera de alcance de personas no autorizadas o inescrupulosas.

• Existen cables e instalaciones eléctricas sobre el piso? Todo el cableado debe estar debidamente canalizado para evitar accidentes personales y a las instalaciones.

• Cómo es la vigilancia del centro de informática? Las puertas de ingreso al centro de informática deben ser consistentes para que brinden la suficiente seguridad y debe estar dotado de vigilancia especializada que lleve un control exhaustivo del personal, tanto de visitantes como de empleados, incluyendo control de pertenencias o materiales que entren o salgan del citado centro. En aquellos casos cuando el visitante requiere ingresar a las instalaciones, debe ser escoltado hasta su destino.

• Cómo se realiza el almacenamiento de papelería? El almacenamiento de papelería y demás suministros combustibles debe hacerse en un lugar distante al centro de informática y debe contar con las suficientes precauciones de almacenamiento o bodegaje. Se debe mantener internamente solo el material necesario que va a ser utilizado prontamente.

• Cómo se realiza el aseo al equipo de computación? El aseo a las instalaciones del cuarto de equipos y cintotéca debe efectuarse mediante la utilización de aspiradora y no bajo condiciones normales de aseo, con el propósito de evitar al máximo las partículas de polvo.

• Cómo son las condiciones físico - ambientales del centro de informática? El centro de informática debe contar con condiciones físicas apropiadas que le permitan a sus funcionarios un mejor desempeño laboral y elevar el nivel de productividad; esas condiciones consisten en una adecuada y segura ventilación e iluminación, evitar al máximo la alta contaminación por ruido y polvo (polución); dotarla de suficientes equipos de oficina como líneas telefónicas, archivadores, máquinas grapadoras, etc; las sillas que se utilizan deben ser ergonómicas para evitar problemas de salud y aliviar el cansancio producido por el elevado número de horas continuas de utilización.
Personal

- Quién es el responsable de la seguridad del centro de informática? Se debe asignar esta responsabilidad a una persona del centro de informática, que recibe generalmente el nombre de oficial de seguridad o administrador de seguridad; así mismo se debe nombrar una segunda persona para que cubra los reemplazos o ausencias del titular del cargo.

- Pueden los analistas de sistemas ingresar al cuarto de la computadora? Los analistas de sistemas no deben ingresar al cuarto de la computadora y debe existir un control estricto sobre el préstamo de cintas y/o discos.

- Se inhabilita la clave de acceso al sistema de computación de aquellos funcionarios retirados temporal o definitivamente? Se debe inhabilitar inmediatamente la clave de aquellos funcionarios de sistemas que entran a disfrutar de vacaciones o son retirados de la empresa.

- Existen programas de prevención contra desastres? Se deben elaborar y poner en funcionamiento programas de prevención contra desastres causados por fuego, temblor y/o inundación.

Equipos

- Qué controles se aplican a las UPS? Se debe monitorear y controlar constantemente la frecuencia de voltaje, bien puede ser mediante procedimientos manuales o automáticos, con el propósito de minimizar el tiempo requerido en caso de realizar un IPL, proporcionando el procesamiento y transmisión normal de las operaciones computacionales.

- Se dispone de UPS de respaldo? Es necesario contar con una unidad UPS de respaldo, sobre todo para períodos de racionamiento eléctrico.

- Existen convenios con otras empresas para respaldo de equipos? Se debe formalizar la constitución de convenios con otras empresas para respaldo de equipos, cuando las circunstancias así lo demanden.

- Se cuenta con planos eléctricos actualizados? Se hace necesario disponer de planos eléctricos actualizados de toda la edificación, así como contar con protección para todos los circuitos eléctricos, en especial los del centro de informática.

- Poseen forros o cubiertas que protejan el equipo de computación? Es necesario proteger de contaminación a todas las terminales cuando no están en uso, por medio de forros o cubiertas; igualmente es conveniente la consecución de un plástico que cubra el equipo central, evitando aquellas filtraciones de agua que por alguna eventualidad puedan caer encima de él. Se debe prohibir totalmente el comer, beber o fumar dentro del cuarto de la computadora.

Documentación

"El desastre tiende a suceder cuando la aplicación está casi terminada, pero la documentación no está completa" Ley de Murphy.
• Están todas las aplicaciones sistematizadas completamente documentadas? Las aplicaciones sistematizadas deben estar totalmente documentadas por escrito y se debe optar como norma la permanente revisión de la documentación.

• Se actualiza permanentemente la documentación de la aplicación? Debe existir una permanente actualización de la documentación de cada aplicación; ésta debe hacerse tanto al manual técnico como al manual del auditor. Se debe involucrar en la elaboración de la documentación, no solo al centro de informática, sino también a los usuarios, de tal manera que todos apoyen esta actividad y no permitan que un sistema se ponga en marcha antes que la documentación esté terminada. Esta política también debe hacerse extensiva a los mantenimientos de las aplicaciones; no se debe permitir por ningún motivo, que debido a la urgencia de los mantenimientos, se obvie la documentación respectiva, no dejando huella auditables y desactualizando la documentación de la aplicación.

• Se restringe el acceso a la documentación? El acceso a la documentación se debe restringir al personal directamente vinculado con la aplicación y su consulta física se debe efectuar dentro de las instalaciones del centro de informática; en lo posible debe procurarse que la documentación permanezca en línea, con el propósito de disponer de ella de manera inmediata cuando sea requerida.

• Se dispone de duplicado de la documentación? Se debe tener duplicado de la documentación de tal manera que copia de ella permanezca almacenada en un lugar seguro y distante al centro de informática.

Back - ups

• Existen políticas definidas con respecto a los back-ups? Se debe guardar copia de todos los back-ups en lugares distantes al centro de informática y en instalaciones de alta seguridad.

• Cómo se controla el transporte de discos y cintas? Se debe tener un estricto control sobre el transporte de discos y cintas de la sala de cómputo al lugar de almacenamiento distante.

• Es revisado el log de los objetos salvados? Se debe imprimir el log de los objetos salvados, con el propósito de verificar que se almacenó lo que se deseaba.

• Con qué frecuencia se saca back-up del sistema operativo? Se debe sacar back-up del sistema operativo mínimo cada dos meses o en su defecto cada que se presente un cambio de release o actualización al mismo.

Pólizas - Seguros

• Están el software y el hardware amparados por pólizas de seguros? El seguro debe tener un cubrimiento total del hardware y su instalación. Tanto el software como el hardware deben estar asegurados por su valor comercial y se debe velar por su permanente actualización.

• Se verifican las fechas de vencimiento de las pólizas de seguros? Se deben revisar las fechas de vencimiento de las pólizas de seguros para evitar desamparos en un determinado momento.
• Se exige fianza para aquellos cargos que implican riesgo al centro de informática? Se debe exigir fianza a aquel personal que implique riesgos para el centro de informática; dicha fianza debe cubrir entre otros los siguientes tópicos: robo, negligencia, sabotaje, etc.

Otros elementos de seguridad

• Se evalúan periódicamente los planes de seguridad? Los planes de seguridad se deben detallar con profundidad y analizar los resultados de dichas pruebas para determinar los problemas que se presentaron en la ejecución y hacer los ajustes necesarios.

• Está capacitado el personal para la aplicación de controles y procedimientos de seguridad? Se debe capacitar al personal del centro de informática para la aplicación de controles y procedimientos de seguridad y verificar que los procedimientos para incendio, inundación y sistemas de alarmas estén al alcance de todo el personal.

• Está capacitado el personal de sistemas para operar los equipos de emergencia? Debe asegurarse que el personal esté capacitado adecuadamente para utilizar los equipos contra incendio e inundación y activar los sistemas de alarma; adicionalmente se debe velar para que el personal conozca la ubicación de las alarmas contra incendio, de los extinguidores, interruptores de energía auxiliar y de cualquier otro equipo de emergencia disponible en el centro de informática.

Plan de Contingencias

• Existe un plan de contingencias informático de amplia cobertura? Se debe definir un plan de contingencias que cubra los siguientes items: hardware, software, documentación, talento humano y soporte logístico; debe ser lo más detallado posible y fácil de comprender.

• Existe alguna persona responsable del plan de contingencias? Se debe asignar al personal responsable de dar a conocer el plan de contingencias a todos los funcionarios del centro de informática y adiestrarlos en su funcionamiento; también tiene como función realizar revisiones periódicas del plan y velar por su fácil y permanente actualización, así como de coordinar las operaciones en caso de presentarse alguna contingencia.

• Se realizan simulacros con periodicidad? Se deben realizar simulacros periódicamente; estos deben ser efectuados sorpresivamente y bajo condiciones críticas, evaluando los resultados con el fin de determinar su efectividad y si es del caso, hacer los ajustes que sean pertinentes.

• Existe un procedimiento que indique cómo realizar el simulacro y qué aspectos deben ser considerados? Se debe establecer un procedimiento que señale como efectuar el simulacro y que cubra aspectos tales como:

  • Frecuencia o periodicidad.
  • Alcance.
  • Análisis de resultados, incluyendo:
- Estado del software, hardware, bases de datos, sistemas operativos, comunicaciones, redes.
- Estado de los documentos fuente.
- Estado de los archivos, discos y cintas.
- Inventario del estado de las aplicaciones en funcionamiento.
- Aplicaciones en desarrollo al momento de efectuar el simulacro.
- Resultado de los procedimientos aplicados en cuanto a recuperación y respaldo.
- Documentación.
- Reacción del personal ante el evento.

• Existe un comité de seguridad al interior del centro de informática? Debe existir un comité formalmente constituido que se encargue de diseñar, elaborar, aplicar, evaluar los planes de contingencias y simulacros de desastres, velar por la seguridad e integridad de la información, de los recursos informáticos y del personal del centro.

7.7 PROCEDIMIENTOS DE AUDITORÍA PARA SER APLICADOS AL CENTRO DE INFORMÁTICA

Para el efecto se definen los procedimientos de auditoría con base en los aspectos administrativos y de seguridad, de la siguiente manera:

7.7.1 Procedimientos de Auditoría para Aspectos Administrativos:

- Planeación Estratégica de Sistemas de Información (P.E.S.I.)

Solicitar la Planeación Estratégica de Sistemas de Información y evaluar:

- Coherencia entre objetivos organizacionales y objetivos de la PESI.
- Objetivos a corto y mediano plazo.
- Compromiso institucional.
- Participación.
- Tiempo proyectado.
- Análisis costo / beneficio.
- Herramientas de la PESI.
- Componentes de la PESI.

- Políticas Administrativas

Evaluar las políticas administrativas internas del centro de informática con respecto a:
- Elaborar y evaluar la PESI.
- Integración de los Sistemas de Información.
- Legalización del software utilizado.
- Costos por aplicación.
- Capacitación.
- Desempeño.
- Segregación de funciones.
- Rotación de funciones.
- Vacaciones anuales.

**Controles organizativos generales**

- Comprobar la separación de funciones entre captura de datos y programación.
- Evaluar los procedimientos escritos para cambios o modificaciones a programas.
- Revisar los mecanismos que permitan la suspensión inmediata de empleados.
- Revisar los procedimientos para reporte de dificultades.

**Análisis organizacional**

- Solicitar la estructura orgánica del centro de informática y evaluar su funcionalidad.

**Estándares**

- Solicitar los estándares escritos para las diferentes actividades que se desarrollan en el centro de informática y evaluarlos.
- Solicitar el estudio de necesidades que justificó la adquisición de software y hardware, y evaluarlo.
- Verificar la actualidad del software y hardware.
- Verificar si las actualizaciones a las aplicaciones son autorizadas por los usuarios.
- Analizar la integración de los sistemas de información.

**Talento humano**

**Administración y Organización**

- Evaluar el ambiente laboral del centro de informática.
- Analizar el índice de rotación.
- Comprobar las políticas sobre reemplazamiento de personal.
- Comprobar la exigencia de exámenes médicos y psicológicos como requisito de vinculación.
- Evaluar la políticas respecto a las vacaciones del personal.
- Constatar si se efectúa un análisis de referencias y antecedentes previo a la vinculación de personal.
- Observar la existencia de programas de inducción.
Ambiente Laboral

• Evaluar el ambiente laboral del centro de informática.
• Analizar el índice de rotación.
• Comprobar las políticas sobre reemplazamiento del personal.

Entrenamiento y capacitación

• Solicitar los programas de capacitación y evaluarlos.
• Comprobar si los cursos impartidos son evaluados.
• Comprobar la existencia y disponibilidad de material bibliográfico actualizado.

Desempeño

• Solicitar los estándares de desempeño y analizarlos.
• Comprobar las evaluaciones periódicas del desempeño.

Supervisión

• Evaluar el índice de ausentismo y retardos.
• Observar la disciplina laboral de los funcionarios.
• Comprobar si existen conflictos laborales al interior del centro de informática.
• Observar si las quejas y reclamos son atendidas oportunamente.

Motivación

• Comprobar si existe motivación en el personal.
• Revisar si existen políticas de ascensos y promociones.

Remuneración

• Revisar si existe una adecuada remuneración de cargos.

Elementos financieros

• Revisar si existe un sistema de costeo por aplicación.
• Comprobar si existe una metodología para estimar tiempos y costos del proyecto.

7.7.2 Procedimientos de Auditoría para Aspectos Técnicos

Evaluar las políticas internas de orden técnico del centro de informática.
SOLICITAR INVENTARIO DE HARDWARE:
- Configuración del equipo central.
- Configuración del equipo de desarrollo.
- Número de terminales, características y distribución.
- Número de impresoras, características y distribución.
- Equipos para soporte de comunicación.
- Número de microcomputadores, configuración y distribución.

SOLICITAR INVENTARIO DE SOFTWARE:
- Software adquirido.
- Software desarrollado.
- Software que ofrece el equipo de computación.
- Compiladores.

DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS.
- Comprobar si los proyectos de sistemas se interrumpen con frecuencia.
- Solicitar los estándares de producción y revisarlos.
- Observar si existe integración entre los sistemas de información.
- Solicitar las políticas para aplicaciones soportadas por teleproceso y evaluarlas.
- Comprobar si los sistemas de información son evaluados.
- Conocer cómo se administran los proyectos informáticos.
- Observar cómo se efectúan las revisiones de los sistemas en funcionamiento.
- Comprobar si existe una adecuada segregación de funciones.
- Comprobar la participación del usuario durante las etapas de análisis y diseño.
- Verificar la programación de los mantenimientos a las aplicaciones.
- Investigar si los analistas tienen acceso directo a los archivos de la aplicación.
- Observar si el operador del equipo es responsable de la cintoteca.

ENTRADA DE DATOS.
- Constatar las técnicas de verificación utilizadas durante la grabación de los datos.
- Comprobar la verificación de los datos de entrada.
- Observar el acceso al cuarto de la computadora.
- Observar el acceso a los datos y programas de la aplicación.
- Solicitar los procedimientos para el tratamiento de errores y analizarlos.
- Comprobar el horario de acceso a los equipos e instalaciones del centro de informática.
- Observar el registro de las transacciones o movimientos que ingresan al sistema.
- Revisar las etiquetas de cintas y discos.
- Evaluar el almacenamiento de los documentos fuente.
- Revisar el registro de documentos en tránsito.
- Comprobar la utilización de formatos preimpresos.
- Verificar la segregación de funciones entre la preparación y alimentación de los datos.

SALIDA DE DATOS.
- Revisar la identificación de los reportes generales.
- Revisar la fecha y paginación de los reportes producidos.
- Comprobar la calidad de la información producida.
- Evaluar la protección de la información confidencial.
- Comprobar la destrucción de información escrita no utilizable.

**Programas.**
- Solicitar los criterios de asignación de controles a los programas y analizarlos.
- Solicitar el procedimiento para la corrida de trabajos especiales y evaluarlo.
- Solicitar los estándares de calidad del software producido y examinarlos.
- Averiguar los controles aplicados a las transacciones generadas por el sistema y examinarlos.
- Revisar los controles aplicados a la ejecución de las aplicaciones.
- Revisar los controles aplicados al operador del equipo.
- Verificar la rotación periódica de los operadores.
- Constatar la revisión frecuente de las bitácoras del sistema de computación.
- Evaluar los controles aplicados a la corrida de programas.

**Mantenimiento.**
- Solicitar la programación del equipo de computación y evaluarla.
- Solicitar el plan de mantenimiento de las aplicaciones y analizarlo.
- Solicitar el plan de mantenimiento del equipo de computación y de los equipos periféricos y analizarlos.
- Revisar el registro de mantenimiento de las UPS.
- Revisar si son atendidas oportunamente las quejas, reclamos y sugerencias formuladas por los usuarios.

**Operación**
- Comprobar la segregación de funciones al interior del centro de informática.
- Constatar la capacitación del personal en el funcionamiento de las aplicaciones.
- Comprobar si los analistas y diseñadores del sistema operan el equipo de computación.
- Comprobar el registro y causas del reproceso de las aplicaciones.
- Comprobar si el operador de la computadora ejerce funciones de control de las salidas producidas.

**Software del Sistema.**
- Verificar la capacidad de transmisión, velocidad, identificación y sincronización de mensajes.
- Evaluar los controles aplicados en la transmisión de datos.
- Comprobar si existe pérdida de mensajes en el sistema de conmutación.
- Revisar los procedimientos relacionados con la seguridad física y lógica de los datos transmitidos.
- Evaluar el software, hardware, utilización, crecimiento y operación de la red.
- Comprobar que los mensajes tengan válida la dirección de destino.
- Comprobar la capacidad de control y detección de errores.
- Verificar la existencia de una bitácora de auditoría que permita el rastreo y recuperación de transacciones y datos transmitidos.
- Verificar que los controles aplicados consideren la adecuada protección de los componentes de la red y garanticen el debido proceso e integridad de los datos.
- Evaluar la documentación escrita relacionada con la administración y operación de la red.
- Revisar el contrato de mantenimiento de los equipos de comunicación de datos.
- Verificar los accesos y restricciones a las tablas de autorización de contraseñas.
- Revisar las bitácoras de reinicio del sistema, tiempo de reprocesos, registro de problemas de software.
- Verificar los mecanismos de seguridad que brindan protección a la base de datos.
- Solicitar los procedimientos relacionados con la base de datos y evaluarlos.
- Revisar la efectividad de los controles aplicados a las bases de datos.
- Revisar los estándares de administración y operación de la red.
- Evaluar los controles aplicados a la base de datos.
- Verificar los controles que limitan el acceso a la base de datos.
- Revisar la bitácora de la base de datos.
- Revisar el diccionario de la base de datos.
- Verificar los estándares relacionados con los programas de la aplicación.
- Revisar los procedimientos de encriptación y respaldo de los programas de la aplicación.
- Revisar la documentación escrita relacionada con el respaldo y recuperación de la base de datos.
- Evaluar los controles que son aplicados al sistema operativo.
- Revisar las políticas de seguridad relacionadas con el sistema operativo.
- Verificar si el almacenamiento y transmisión de datos son protegidos criptográficamente.
- Evaluar el rendimiento tanto del software como del hardware.
- Analizar la administración de las claves de acceso.
- Comprobar la periodicidad del cambio de claves.
- Comprobar el número de intentos fallidos al utilizar la clave de acceso.
- Evaluar la efectividad de los controles con respecto a la seguridad del sistema.
- Comprobar que la información considerada confidencial sea criptografiada.
- Comprobar la existencia de una bitácora de auditoría.
- Examinar la periodicidad de las revisiones al log del sistema.
- Observar cómo se controla el acceso a los recursos del sistema.
- Solicitar el procedimiento para asignación de cuentas a usuarios y evaluarlo.

7.7.3 Procedimientos de Auditoría para Aspectos de Seguridad

Evaluar las políticas internas de seguridad del centro de informática.

- **Seguridad física.**
  - Conocer la ubicación física del centro de informática y conceptuar.

- **Instalaciones.**
  - Visitar las instalaciones del centro de informática y evaluarlas.
  - Verificar la señalización de las rutas de evacuación.
  - Verificar la existencia y vigencia de los extinguidores.
  - Inspeccionar la ubicación del panel de control eléctrico.
  - Inspeccionar si el cableado se encuentra totalmente canalizado.
  - Chequear la consistencia física de las puertas de acceso.
  - Comprobar como es el almacenamiento de la papelería y demás suministros.
  - Observar como se realiza el aseo del equipo de computación.
  - Analizar como son las conexiones físico - ambientales del centro de informática.
- **PERSONAL.**
  - Averiguar quién es el responsable de la seguridad del centro de informática.
  - Observar si los analistas de sistema ingresan al cuarto de computación.
  - Comprobar si las claves de acceso de los funcionarios retirados son inhabilitadas.
  - Solicitar los programas de prevención contra desastres y evaluarlos.

- **EQUIPOS.**
  - Evaluar los controles aplicados a las UPS.
  - Verificar si existen UPS de respaldo.
  - Solicitar los convenios de respaldo de equipos con otras empresas y evaluarlos.
  - Solicitar los planos eléctricos y constatar su actualización.
  - Observar si el equipo es protegido con forros o cubiertas cuando no está en uso, así mismo, observar si se fuma, come o bebe dentro de la sala de computación.

- **DOCUMENTACIÓN.**
  - Verificar si las aplicaciones están completamente documentadas.
  - Revisar si la documentación es actualizada permanentemente.
  - Comprobar si existe duplicado de la documentación.
  - Observar si se utilizan técnicas de microfilmación.

- **BACK - UPS.**
  - Solicitar las políticas con respecto a los back - ups y analizarlas.
  - Observar como se controla el transporte de discos y cintas.
  - Comprobar si el log de los objetos salvados es revisado constantemente.
  - Observar con que frecuencia se sacan back - ups del sistema operativo.

- **PÓLIZAS.**
  - Solicitar las pólizas de seguros y comprobar si el software y el hardware están amparados, así mismo, verificar la fecha de vencimiento.
  - Comprobar si exigen fianza para aquellos cargos que implican riesgo para el centro de informática.

- **OTROS ELEMENTOS DE SEGURIDAD.**
  - Comprobar si los planes de seguridad son evaluados frecuentemente.
  - Constatar si el personal se encuentra capacitado para aplicar controles y procedimientos de seguridad.
  - Observar si el personal de sistemas está capacitado para manejar los equipos de emergencia.

- **PLAN DE CONTINGENCIAS.**
  - Solicitar el plan de contingencias y analizar su cobertura.
  - Verificar la periodicidad de los simulacros.
  - Averiguar quién es el directo responsable del plan de contingencias.
  - Solicitar los procedimientos para realizar simulacros y analizar los aspectos considerados.
  - Averiguar si existe un comité de seguridad internamente en el centro de informática y cómo es su conformación.
7.8 DISEÑO DE PAPELES DE TRABAJO

El diseño de papeles de trabajo para auditar el centro de informática obedece a la siguiente estructura general:

ARCHIVO PERMANENTE:
- Formulario L: Aspectos administrativos (anexo N°14)
- Formulario M: Aspectos técnicos (anexo N°15)
- Formulario N: Aspectos de seguridad (anexo N°16)

ARCHIVO CORRIENTE:
- Formulario O: Aspectos administrativos (anexo N°17)
- Formulario P: Aspectos técnicos (anexo N°18)
- Formulario Q: Aspectos de seguridad (anexo N°19)

7.8.1 Descripción detallada de los papeles de trabajo que componen el archivo permanente

**Formulario L. Aspectos Administrativos**

1. Reseña del centro de informática.
2. Objetivos a corto y largo plazo.
3. Estructura Orgánica.
   - De la empresa.
   - Del centro de informática.
4. Políticas Administrativas.
5. Planeación Estratégica de Sistemas de Información.(PESI)
   - Coherencia entre objetivos organizacionales y de la PESI.
   - Objetivos a corto plazo y largo plazo.
   - Compromiso institucional.
   - Participación.
- Tiempo proyectado.
- Análisis costo/beneficio.
- Herramientas de la PESI.
- Componentes de la PESI.


7. Talento Humano.
- Inventario.
- Políticas.
- Estándares de desempeño.
- Reglamento interno.
- Programa de trabajo.
- Programa de entrenamiento y capacitación.
- Manual de funciones.
- Manual de procedimientos.

8. Elementos financieros.
- Costos por aplicación.
- Metodología.

**Formulario M. Aspectos Técnicos**

1. Políticas de orden técnico.
2. Inventario de software.
3. Inventario de hardware.
4. Desarrollo e implementación de sistemas.
   - Estándares de producción.
   - Estándares de calidad.
   - Estándares para aplicaciones soportadas por teleproceso.
5. Entrada de datos.
   - Procedimientos para captura de datos.
   - Procedimientos para registro de transacciones.
   - Procedimiento para registro de documentos en tránsito.
   - Procedimiento para tratamiento de errores.
6. Salida de datos.
   - Procedimiento para salida de datos.
   - Procedimiento para reporte de inconsistencias.
7. Software del sistema.
   - Procedimientos para asignación de cuentas.
   - Procedimientos relacionados con la base de datos.
   - Procedimientos relacionados con el sistema operativo.
   - Procedimiento para corrida de programas.
   - Procedimiento para corrida de trabajos especiales.
   - Criterios para asignación de controles.
Formulario N. Aspectos de Seguridad

1. Políticas de seguridad.
2. Instalaciones.
   - Ubicación.
   - Planos físicos.
   - Planos eléctricos.
   - Planos hidráulicos.
   - Planos de ductos de aire.
   - Condiciones físico - ambientales.
3. Equipos.
   - Convenios de respaldo de equipos.
4. Documentación.
   - Manual del sistema.
   - Manual del auditor.
   - Procedimientos de back - ups.
6. Pólizas.
   - Seguros de hardware.
   - Seguros de software.
   - Seguros de las instalaciones.
7. Procedimientos de seguridad.
8. Plan de contingencias.

7.8.2 Descripción detallada de los papeles de trabajo que componen el archivo corriente

Formulario O. Aspectos Administrativos
- Hoja de trabajo 1: Planeación Estratégica de Sistemas de Información.
- Hoja de trabajo 2: Políticas Administrativas.
- Hoja de trabajo 3: Análisis Organizacional.
- Hoja de trabajo 4: Estándares.
- Hoja de trabajo 5: Talento Humano.
- Hoja de trabajo 6: Aspectos Financieros.
- Hoja de trabajo 7: Puntos de atención para futuras revisiones.

Formulario P. Aspectos Técnicos
- Hoja de trabajo 1: Desarrollo e implementación de Sistemas.
- Hoja de trabajo 2: Entrada de Datos.
7.9 INFORMES DE AUDITORIA DE SISTEMAS AL CENTRO DE INFORMÁTICA

Los informes de auditoría son los únicos papeles de trabajo que se deben entregar a la persona responsable de la contratación de la auditoría por parte de la empresa auditada y contiene los resultados de los hallazgos, detallando los problemas encontrados luego de haber efectuado la auditoría, y se espera que sean bien recibidos y acogidas sus recomendaciones, por lo tanto, es muy importante que sean claros, concisos y gozén de buena presentación.

Al igual, como se explicó en el capítulo VI, se deben diseñar informes ejecutivos que van dirigidos a la gerencia de la empresa destacando los hallazgos y recomendaciones más relevantes; y para un amplio conocimiento y utilización, se debe elaborar un informe de auditoría más detallado que va dirigido al jefe del centro de informática, mostrando los hallazgos y recomendaciones tanto para los aspectos administrativos y técnicos, como para los aspectos de seguridad analizados.

7.9.1 Estructura del informe ejecutivo de auditoría al centro de informática.

- Nombre de la empresa.
- Nombre de la firma auditora.
- Identificación del informe.
- Fecha del informe.
7.9.2 Estructura del informe detallado de auditoría al centro de informática

- Nombre de la empresa.
- Nombre de la firma auditora.
- Identificación del informe.
- Fecha del informe.
- Breve reseña del centro de informática.
- Objetivos del centro de informática.
- Alcance de la auditoría efectuada.
- Hallazgos detallados de orden administrativo, técnico y de seguridad.
- Recomendaciones detalladas de orden administrativo, técnico y de seguridad.
- Firma del auditor responsable.

7.10 BIBLIOGRAFÍA

ALVAREZ, C. Augusto. La Administración de personal. Editorial Padres e Hijos. 1995.
www. dorado.une.edu.ve/biblio/auditoria
www. isaca.org
ANEXO N°1
PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS PARA
APLICACIONES EN FUNCIONAMIENTO Y EN PROCESO DE
DESARROLLO

EMPRESA A AUDITAR:
EMPRESA AUDITORA:
FECHA:

1. CARACTERÍSTICAS GENERALES DE LA EMPRESA

1.1 ESTRUCTURA ORGÁNICA DE LA EMPRESA (ANEXAR)

1.2 POLÍTICAS GENERALES

1.3 OBJETIVOS INSTITUCIONALES

1.3.1 OBJETIVOS ESPECÍFICOS

1.4 NORMATIVIDAD

1.4.1 REGLAMENTACIÓN INTERNA

1.5 DOCUMENTACIÓN

<table>
<thead>
<tr>
<th>Manual de funciones</th>
<th>SI</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual de procedimientos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual del usuario</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. DESCRIPCIÓN DE RECURSOS INFORMÁTICOS

2.1 CONFIGURACIÓN DEL HARDWARE Y SU DISTRIBUCIÓN DENTRO DE LA EMPRESA

CONFIGURACIÓN
UBICACIÓN

2.2 DESCRIPCIÓN DE LAS APLICACIONES EN FUNCIONAMIENTO

APLICACIÓN
AMBIENTE
NÚMERO DE REGISTROS

2.3 DESCRIPCIÓN DE LAS APLICACIONES EN DESARROLLO

APLICACIÓN
ESTADO

2.4 DESCRIPCIÓN DE LAS APLICACIONES POR DESARROLLAR

APLICACIÓN
FECHA DE INICIAZIÓN
3. ASPECTOS ATINENTES A LA AUDITORÍA

3.1 ¿SE HAN REALIZADO AUDITORÍAS DE SISTEMAS INTERNA O EXTERNAMENTE Y CON QUÉ PERIODICIDAD SE HAN EFECTUADO?

<table>
<thead>
<tr>
<th>ENTIDAD AUDITORA</th>
<th>PERIODICIDAD</th>
</tr>
</thead>
</table>

3.2 ¿EXISTE AL INTERIOR DE LA EMPRESA MANUAL DE AUDITORÍA DEBIDAMENTE DOCUMENTADO Y ACTUALIZADO?

3.3 DESCRIBA LOS PROCEDIMIENTOS DE AUDITORÍA UTILIZADOS AL INTERIOR DE LA EMPRESA

3.4 DESCRIBA LOS CONTROLES MÁS FRECUENTEMENTE APLICADOS EN LA EMPRESA
ANEXO N° 2
PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS

ESTIMACIÓN DE TIEMPO EN HORAS PARA APLICACIONES EN FUNCIONAMIENTO

<table>
<thead>
<tr>
<th>ACTIVIDAD/RESPECTO A</th>
<th>NOMBRE DE LA APLICACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>I. CONOCIMIENTO-AMBIENTACIÓN</td>
<td></td>
</tr>
<tr>
<td>II. ANÁLISIS TÉCNICO-ADMINISTRATIVO</td>
<td></td>
</tr>
<tr>
<td>• Análisis de riesgos</td>
<td></td>
</tr>
<tr>
<td>• Análisis de controles existentes</td>
<td></td>
</tr>
<tr>
<td>• Análisis de controles requeridos a programas</td>
<td></td>
</tr>
<tr>
<td>• Análisis de controles de acceso al sistema</td>
<td></td>
</tr>
<tr>
<td>• Evaluación del manual técnico</td>
<td></td>
</tr>
<tr>
<td>• Evaluación del manual del usuario</td>
<td></td>
</tr>
<tr>
<td>• Sugerencias sobre tareas y funciones de la aplicación</td>
<td></td>
</tr>
<tr>
<td>• Sugerencias sobre tareas y procedimientos de la aplicación</td>
<td></td>
</tr>
<tr>
<td>III. DESARROLLO DE SOFTWARE DE AUDITORÍA</td>
<td></td>
</tr>
<tr>
<td>• Desarrollo e implementación de programas monitor</td>
<td></td>
</tr>
<tr>
<td>• Elaboración del manual técnico</td>
<td></td>
</tr>
<tr>
<td>• Elaboración del manual del auditor</td>
<td></td>
</tr>
<tr>
<td>• Entrega del sistema y capacitación</td>
<td></td>
</tr>
<tr>
<td><strong>Total tiempo estimado en horas profesional</strong></td>
<td></td>
</tr>
</tbody>
</table>

NOMBRE DE LA APLICACIÓN

1.
2.
3.

OBSERVACIONES:
<table>
<thead>
<tr>
<th>ACTIVIDAD/RESPECTO A</th>
<th>NOMBRE DE LA APLICACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>I. CONOCIMIENTO-AMBIENTACIÓN</td>
<td></td>
</tr>
<tr>
<td>II. ANÁLISIS TÉCNICO-ADMINISTRATIVO</td>
<td></td>
</tr>
<tr>
<td>• Descripción global del sistema</td>
<td></td>
</tr>
<tr>
<td>• Marco de referencia legal y funcional</td>
<td></td>
</tr>
<tr>
<td>• Análisis de riesgos</td>
<td></td>
</tr>
<tr>
<td>• Análisis de controles existentes</td>
<td></td>
</tr>
<tr>
<td>• Análisis de controles requeridos</td>
<td></td>
</tr>
<tr>
<td>• Análisis de controles de acceso al sistema</td>
<td></td>
</tr>
<tr>
<td>III. DISEÑO DEL SISTEMA</td>
<td></td>
</tr>
<tr>
<td>• Diagrama del Sistema</td>
<td></td>
</tr>
<tr>
<td>• Descripción de las estructuras de datos</td>
<td></td>
</tr>
<tr>
<td>• Forma de procesamiento</td>
<td></td>
</tr>
<tr>
<td>• Planteamiento de soluciones alternas</td>
<td></td>
</tr>
<tr>
<td>• Definición del plan de pruebas</td>
<td></td>
</tr>
<tr>
<td>IV. DOCUMENTACIÓN DEL SISTEMA</td>
<td></td>
</tr>
<tr>
<td>• Sugerencias al manual técnico</td>
<td></td>
</tr>
<tr>
<td>• Sugerencias al manual del usuario</td>
<td></td>
</tr>
<tr>
<td>• Sugerencias sobre tareas y funciones</td>
<td></td>
</tr>
<tr>
<td>• Sugerencias sobre tareas y procedimientos</td>
<td></td>
</tr>
<tr>
<td>Total tiempo estimado en horas profesional</td>
<td></td>
</tr>
</tbody>
</table>

NOMBRE DE LA APLICACIÓN

1.
2.
3.

OBSERVACIONES:
CUADRO RESUMEN ESTIMACIÓN DE TIEMPO

<table>
<thead>
<tr>
<th>CONCEPTOS</th>
<th>NÚMERO HORAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>APLICACIONES EN FUNCIONAMIENTO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>APLICACIONES EN DESARROLLO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
</tr>
</tbody>
</table>
ANEXO N° 3
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES SISTEMATIZADAS EN FUNCIONAMIENTO

ARCHIVO PERMANENTE. ADMINISTRADOR DE LA APLICACIÓN. FORMULARIO A

EMPRESA A AUDITAR:
EMPRESA AUDITORA:

NOMBRE O DENOMINACIÓN GLOBAL DE LA APLICACIÓN

ENTREVISTADO

1. RESEÑA DE LA APLICACIÓN

1.1 FECHA EN QUE EMPEZÓ A FUNCIONAR LA APLICACIÓN

1.2 ANALISTAS RESPONSABLES

1.3 DISEÑADORES RESPONSABLES

1.4 OPERADORES RESPONSABLES

1.5 MANTENIMIENTOS REGISTRADOS Y/O CONOCIDOS: Desde la puesta en marcha de la aplicación se han realizado modificaciones en:

PANTALLAZOS (Explicar razones)

PROCEDIMIENTOS (Explicar razones)
1.6 DESCRIBA EL PROCEDIMIENTO UTILIZADO PARA HACER MANTENIMIENTO A LA APLICACIÓN

1.7 SON USUARIOS DE LA APLICACIÓN

A. EN CAPTURA

B. EN PROCESOS CRÍTICOS

C. EN VERIFICACIÓN DE CAPTURA

D. EN PROCESO DE CONSULTA

2. NATURALEZA Y JUSTIFICACIÓN DE LA APLICACIÓN
3. ESTRUCTURA ORGANIZACIONAL Y FUNCIONAL RESPECTO AL MANEJO DE LA APLICACIÓN

3.1 ENTIDADES O DEPENDENCIAS QUE INTERACTÚAN CON LA APLICACIÓN

<table>
<thead>
<tr>
<th>ENTIDAD O DEPENDENCIA</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTERNAS</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EXTERNAS</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. INTERACCIÓN CON OTRAS APLICACIONES

<table>
<thead>
<tr>
<th>APLICACIÓN</th>
<th>MOTIVO</th>
<th>PERÍODO</th>
<th>DURACIÓN</th>
<th>SENTIDO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTERNAS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EXTERNAS</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. DOCUMENTACIÓN DE ENTRADAS Y SALIDAS

5.1 GENERALIDADES DE LAS ENTRADAS

<table>
<thead>
<tr>
<th>NOMBRE</th>
<th>PERÍODO</th>
<th>ORIGEN</th>
<th>CALIDAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2 GENERALIDADES DE LAS SALIDAS

<table>
<thead>
<tr>
<th>NOMBRE</th>
<th>PERÍODO</th>
<th>ORIGEN</th>
<th>CALIDAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. DICCIONARIO DE DATOS - PROGRAMAS Y MENUS

6.1 ARCHIVOS DE DATOS (nombre, descripción y tipo. Solicitar un listado a su informante)

6.1.1 VERIFICAR QUE EL CONTENIDO DEL LISTADO CORRESPONDA CON LO SOLICITADO; REALIZAR ANÁLISIS COMPARATIVO Y ANEXARLO A ESTE FORMULARIO.

6.1.2 AMPLIACIÓN DEL DICCIONARIO DE DATOS

<table>
<thead>
<tr>
<th>NOMBRE</th>
<th>DESCRIPCIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6.2 ARCHIVOS-PROGRAMAS (Nombre, generalidad, lenguaje). Solicitar un listado a su informante.

6.2.1 VERIFICAR QUE EL CONTENIDO DEL LISTADO CORRESPONDA CON LO SOLICITADO, REALIZAR ANÁLISIS COMPARATIVO Y ANEXARLO A ESTE FORMULARIO.

6.3 MENÚS DEL USUARIO

<table>
<thead>
<tr>
<th>LIBRERÍA</th>
<th>NOMBRE</th>
<th>DESCRIPCIÓN</th>
<th>USUARIOS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6.4 DIAGRAMA DE PASADAS
7. NORMALIZACIÓN Y FUENTES DE CONSULTA

7.1 INTERNAS

7.1.1 NORMAS EXISTENTES QUE TIENEN QUE VER CON LA APLICACIÓN

7.1.2 FUENTES DE CONSULTA QUE TIENE LA APLICACIÓN

7.2 EXTERNAS

7.2.1 NORMAS EXISTENTES QUE TIENEN QUE VER CON LA APLICACIÓN

7.2.2 FUENTES DE CONSULTA QUE TIENE LA APLICACIÓN
8. NATURALEZA Y DEFINICIÓN DE CADA PROCESO

8.1 IDENTIFICACIÓN Y NOMBRE DEL PROCESO

8.2 NATURALEZA Y DEFINICIÓN

DEPENDENCIA
PERÍODO
DURACIÓN
CONFIABILIDAD

8.3 DIAGRAMA GENERAL DEL PROCESO (Utilizar hojas anexas para una mayor descripción)

9. POSIBILIDAD DE REPROCESO

9.1 QUE POSIBILIDAD DE REPROCESO TIENE LA APLICACIÓN?

10. SEGUIMIENTO O RASTREO

10.1 QUE POSIBILIDAD DE SEGUIMIENTO O RASTREO TIENE LA APLICACIÓN?
11. FUNCIONALIDAD

11.1 OPORTUNIDAD DE LA APLICACIÓN
MUY BUENA  BUENA  REGULAR  MALA
OBSERVACIONES

11.2 CONFIABILIDAD DE LA APLICACIÓN
MUY BUENA  BUENA  REGULAR  MALA
OBSERVACIONES

12. AMIGABILIDAD

12.1 QUE TAN AMIGABLE ES LA APLICACIÓN PARA EL USUARIO?
MUY BUENA  BUENA  REGULAR  MALA
OBSERVACIONES

13. AUTONOMÍA

13.1 FRECUENCIA Y MOTIVOS DE CONSULTA AL CENTRO DE INFORMÁTICA

<table>
<thead>
<tr>
<th>MOTIVO</th>
<th>FRECUENCIA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
13.2 CALIFICACIÓN DE AUTONOMÍA

MUY BUENA  →  BUENA  →  REGULAR  →  MALA

OBSERVACIONES

13.3 MOTIVOS DE LA DEPENDENCIA

14. RESEÑA DE FRAUDES

15. RESEÑA DE ERRORES
16. DOCUMENTACIÓN EXISTENTE

<table>
<thead>
<tr>
<th>DEL SISTEMA</th>
<th>DE PROGRAMAS</th>
<th>DE OPERACIÓN</th>
<th>DEL USUARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17. OBSERVACIONES
ANEXO N° 4
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES SISTEMATIZADAS EN FUNCIONAMIENTO

ARCHIVO PERMANENTE. USUARIOS DE LA APLICACIÓN. FORMULARIO B

EMPRESA A AUDITAR:

EMPRESA AUDITORA:

NOMBRE O DENOMINACIÓN GLOBAL DE LA APLICACIÓN

ENTREVISTADO FECHA

| 1. ESTRUCTURA ORGANIZACIONAL - FUNCIONAL RESPECTO AL MANEJO DE LA APLICACIÓN |

1.1 ENTIDADES - CARGO:

<table>
<thead>
<tr>
<th>INTERNAS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CARGOS</td>
<td>OBSERVACIÓN</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EXTERNAS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CARGOS</td>
<td>OBSERVACIÓN</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

127
2. NORMALIZACIÓN Y FUENTES DE CONSULTA

2.1 INTERNAS

2.1.1 NORMAS QUE TIENEN QUE VER CON LA APLICACIÓN

2.1.2 FUENTES DE CONSULTA QUE TIENE LA APLICACIÓN

2.2 EXTERNAS

2.2.1 NORMAS QUE TIENEN QUE VER CON LA APLICACIÓN

2.2.2 FUENTES DE CONSULTA QUE TIENE LA APLICACIÓN

3. RIESGOS DETECTADOS EN LA APLICACIÓN
4. CONTROLES REQUERIDOS

5. AUTONOMÍA DE LA APLICACIÓN

5.1 FRECUENCIA Y MOTIVOS DE CONSULTA AL CENTRO DE INFORMÁTICA

<table>
<thead>
<tr>
<th>MOTIVOS</th>
<th>FRECUENCIA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2 MOTIVOS DE DEPENDENCIA
### 6. EVALUACIÓN DE LA FUNCIONALIDAD

#### 6.1 OPORTUNIDAD DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>MUY BUENA</th>
<th>BUENA</th>
<th>REGULAR</th>
<th>MALA</th>
</tr>
</thead>
</table>

OBSERVACIONES

#### 6.2 CONFIABILIDAD DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>MUY BUENA</th>
<th>BUENA</th>
<th>REGULAR</th>
<th>MALA</th>
</tr>
</thead>
</table>

OBSERVACIONES

#### 6.3 AMIGABILIDAD DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>MUY BUENA</th>
<th>BUENA</th>
<th>REGULAR</th>
<th>MALA</th>
</tr>
</thead>
</table>

OBSERVACIONES

### 7. SISTEMA DE ARCHIVO DE DOCUMENTOS
8. RESEÑA DE FRAUDES

9. RESEÑA DE ERRORES

10. INVENTARIO DE CONTROLES EXISTENTES
11. LIMITANTES DE LA APLICACIÓN

12. OBSERVACIONES
ANEXO N° 5
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES SISTEMATIZADAS EN FUNCIONAMIENTO

ARCHIVO PERMANENTE. AUDITORES DE LA APLICACIÓN. FORMULARIO C

EMPRESA A AUDITAR:

EMPRESA AUDITORA:

NOMBRE O DENOMINACIÓN GLOBAL DE LA APLICACIÓN

ENTREVISTADO FECHA

1. PERSONAL RELACIONADO CON LA APLICACIÓN

2. CONTROLES ACTUALES (Descripción individual)

<table>
<thead>
<tr>
<th>NOMBRE</th>
<th>OBJETIVO</th>
<th>MOMENTO</th>
<th>FORMA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 3. CONTROLES REQUERIDOS (Descripción individual)

<table>
<thead>
<tr>
<th>NOMBRE</th>
<th>OBJETIVO</th>
<th>MOMENTO</th>
<th>FORMA</th>
<th>RIESGO QUE CUBRIRÁ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4. LIMITACIONES DEL FUNCIONARIO FRENTE AL AUDITAJE DE LA APLICACIÓN
5. OBSERVACIONES
ANEXO N° 6
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES
EN DESARROLLO

ARCHIVO PERMANENTE. ADMINISTRADOR DE LA APLICACIÓN. FORMULARIO D

EMPRESA A AUDITAR:

EMPRESA AUDITORA:

NOMBRE O DENOMINACIÓN GLOBAL DE APLICACIÓN

ENTREVISTADO FECHA

1. RESEÑA DE LA APLICACIÓN

1.1 FECHA DE INICIO DEL DESARROLLO DE LA APLICACIÓN

1.2 ANALISTAS RESPONSABLES

1.3 DISEÑADORES RESPONSABLES

1.4 SERÁN USUARIOS DE LA APLICACIÓN

A. EN CAPTURA B. EN PROCESOS CRÍTICOS

C. EN VERIFICACIÓN DE CAPTURA D. EN PROCESO DE CONSULTA
2. NATURALEZA Y JUSTIFICACIÓN DE LA APLICACIÓN

3. ESTRUCTURA ORGANIZACIONAL Y FUNCIONAL RESPECTO AL MANEJO DE LA APLICACIÓN

3.1 ENTIDADES O DEPENDENCIAS QUE INTERACTÚAN CON LA APLICACIÓN

<table>
<thead>
<tr>
<th>ENTIDAD O DEPENDENCIA</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INTERNAS</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EXTERNAS</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. INTERACCIÓN CON OTRAS APLICACIONES

<table>
<thead>
<tr>
<th>APLICACIÓN</th>
<th>MOTIVO</th>
<th>PERÍODO</th>
<th>DURACIÓN</th>
<th>SENTIDO</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNAS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXTERNAS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. INTERACCIÓN CON OTRAS APLICACIONES

5.1 INTERNAS

5.1.1 NORMAS EXISTENTES QUE TIENEN QUE VER CON LA APLICACIÓN

5.1.2 FUENTES DE CONSULTA QUE TIENE LA APLICACIÓN
5.2 EXTERNAS

5.2.1 NORMAS EXISTENTES QUE TIENEN QUE VER CON LA APLICACIÓN

5.2.2 FUENTES DE CONSULTA QUE TIENE LA APLICACIÓN

6. OBSERVACIONES
**1. ESTRUCTURA ORGANIZACIONAL - FUNCIONAL RESPECTO AL MANEJO DE LA APLICACIÓN**

### 1.1 ENTIDADES - CARGO:

<table>
<thead>
<tr>
<th>CARGOS</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CARGOS</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CARGOS</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CARGOS</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CARGOS</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CARGOS</th>
<th>OBSERVACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. NORMALIZACIÓN Y FUENTES DE CONSULTA

2.1 NORMAS

2.1.1 NORMAS INTERNAS QUE TIENEN QUE VER CON LA APLICACIÓN

2.1.2 NORMAS EXTERNAS QUE TIENEN QUE VER CON LA APLICACIÓN

2.2 FUENTES

2.2.1 FUENTES INTERNAS QUE TIENE LA APLICACIÓN

2.2.2 FUENTES EXTERNAS QUE TIENE LA APLICACIÓN

3. RIESGOS DETECTADOS EN LA APLICACIÓN
4. CONTROLES REQUERIDOS

5. OBSERVACIONES
ANEXO N° 8
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES EN DESARROLLO

ARCHIVO PERMANENTE. AUDITORES DE LA APLICACIÓN. FORMULARIO F

EMPRESA A AUDITAR:

EMPRESA AUDITORA:

NOMBRE O DENOMINACIÓN GLOBAL DE APLICACIÓN

ENTREVISTADO FECHA

1. PERSONAL RELACIONADO CON LA APLICACIÓN

2. PARTICIPACIÓN DE LA AUDITORÍA EN EL DESARROLLO DE LA APLICACIÓN
### 3. CONTROLES SUGERIDOS A LA APLICACIÓN

<table>
<thead>
<tr>
<th>NOMBRE</th>
<th>OBJETIVO</th>
<th>MOMENTO</th>
<th>FORMA</th>
<th>RIESGO QUE CUBRIRÁ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4. LIMITACIONES DEL AUDITOR FRENTE AL AUDITAJE DE LA APLICACIÓN
5. OBSERVACIONES
ANEXO N° 9
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES SISTEMATIZADAS EN FUNCIONAMIENTO

ARCHIVO CORRIENTE. FORMULARIO G

EMPRESA AUDITADA:

EMPRESA AUDITORA:

NOMBRE DE APLICACIÓN:

HOJA DE TRABAJO 1: GENERALIDADES

1.1 OBJETIVOS DEL DISEÑO E IMPLEMENTACIÓN DE LA AUDITORÍA DE SISTEMAS PARA APLICACIONES EN FUNCIONAMIENTO

1.2 TIEMPO DE EJECUCIÓN

FECHA DE INICIO FECHA DE TERMINACIÓN

OBSERVACIONES

1.3 DILIGENCIÓ:

1.4 FECHA DE DILIGENCIAMIENTO:
<table>
<thead>
<tr>
<th>FECHA</th>
<th>LUGAR</th>
<th>FUNCIONARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**2.2 SESIONES DE TRABAJO CON USUARIOS DE LA APLICACIÓN**

<table>
<thead>
<tr>
<th>FECHA</th>
<th>LUGAR</th>
<th>FUNCIONARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**2.3 SESIONES DE TRABAJO CON AUDITORES DE LA APLICACIÓN**

<table>
<thead>
<tr>
<th>FECHA</th>
<th>LUGAR</th>
<th>FUNCIONARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**2.4 DILIGENCIÓ**

**2.5 FECHA DE DILIGENCIAMIENTO**
3.1 ENTRADAS A LA APLICACIÓN

3.1.1 ANÁLISIS FÍSICO DE ENTRADAS A LA APLICACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANALIZAR LAS FORMAS PREIMPRESAS UTILIZADAS</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ANALIZAR LA FUNCIONALIDAD DE LOS FORMATOS UTILIZADOS</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ESTÁN DEBIDAMENTE PROTEGIDOS Y ALMACENADOS LOS DOCUMENTOS FUENTE?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿ESTÁN LOS DISCOS Y CINTAS DEBIDAMENTE IDENTIFICADOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ESTÁ DEFINIDO EL TIEMPO QUE SE DEBEN CONSERVAR LOS DOCUMENTOS FUENTE?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SE REGISTRA EL TRÁNSITO QUE HACEN LOS DOCUMENTOS POR LAS DISTINTAS DEPENDENCIAS?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 3.1.2 CONTROLES A ENTRADAS

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE EMPLEAN TÉCNICAS PARA VALIDAR, PROBAR Y VERIFICAR LOS DATOS DE ENTRADA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SON DETECTADOS LOS REGISTROS O TRANSACCIONES NO ACEPTADAS POR EL SISTEMA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN CONTROLES RAZONABLES DURANTE LA GENERACIÓN DE LOS DATOS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTE SEGREGACIÓN DE FUNCIONES ENTRE LA GENERACIÓN, REGISTRO Y ALMACENAMIENTO DE LA ENTRADA DE DATOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN MECANISMOS QUE RESTRINGAN EL ACCESO A LOS DISPOSITIVOS DE ENTRADA?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTEN PROCEDIMIENTOS PARA LA PREPARACIÓN, CORRECCIÓN, GRABACIÓN Y ALMACENAMIENTO DE DATOS?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
3.2 UTILIZACIÓN DE DATOS DE PRUEBA

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CONTEO DE REGISTRO</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>TOTALES DE CONTROL</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>CONSISTENCIA DE CAMPOS</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>DÍGITO DE AUTOVERIFICACIÓN</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>VERIFICACIÓN DE DESBORDAMIENTO</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>VERIFICACIÓN DE SECUENCIA</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 3.3 PRUEBAS REALIZADAS

#### 3.3.1 CONTROLES AL SOFTWARE DEL SISTEMA

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE CONSIDERA EL CRITERIO DE LOS USUARIOS DURANTE LAS DIFERENTES ETAPAS DEL CICLO DE VIDA DEL SISTEMA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿LOS CAMBIOS Y MEJORAS AL SOFTWARE DEL SISTEMA ESTÁN DEBIDAMENTE JUSTIFICADAS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SON DE CONFIANZA LAS PERSONAS QUE HACEN MANTENIMIENTO AL SISTEMA DE INFORMACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿ESTÁ TOTALMENTE LEGALIZADO EL SOFTWARE UTILIZADO POR LA EMPRESA?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTE UN REGISTRO DE AQUELLOS PROBLEMAS QUE SE PRESENTAN CON EL SOFTWARE?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTEN CONTROLES ADECUADOS CUANDO SE ESTÁN PROBANDO LAS NUEVAS VERSIONES DEL SOFTWARE?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
<table>
<thead>
<tr>
<th>Nº</th>
<th>NOMBRE DEL PROGRAMA</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
### CONTROLES A PROGRAMAS

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SON AUTORIZADAS Y PROBADAS LAS CORRECCIONES A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE LLEVA REGISTRO DE LOS CAMBIOS EFECTUADOS A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ESTÁN ADECUADAMENTE DOCUMENTADOS Y PROBADOS LOS NUEVOS SISTEMAS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTE PLANEACIÓN DE LAS PRUEBAS QUE DEBEN SER REALIZADAS A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN LIBRERÍAS ESPECÍFICAS PARA REALIZAR LAS PRUEBAS A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTE UNA AMPLIA DIFUSIÓN ACERCA DE LAS PRUEBAS A REALIZAR?</td>
<td></td>
</tr>
</tbody>
</table>

### DILIGENCIÓ

### FECHA DE DILIGENCIAMIENTO
### 3.4 UTILIZACIÓN DE PROGRAMAS DE AUDITORÍA (SOFTWARE DE AUDITORÍA)

<table>
<thead>
<tr>
<th>№</th>
<th>NOMBRE DEL PROGRAMA</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
### 3.5 SALIDAS DEL SISTEMA

#### 3.5.1 ANÁLISIS DE SALIDAS PRODUCIDAS POR EL SISTEMA

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ANÁLISIS DE REPORTES</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>REPORTES DE EXCEPCIÓN</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>PANTALLAZOS</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>COHERENCIA DE LOS MENSAJES PRODUCIDOS</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>ANÁLISIS DE ARCHIVOS GENERADOS</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>SUPERVISAR LA DESTRUCCIÓN DE AQUELLOS REPORTES NO NECESARIOS</td>
<td></td>
</tr>
</tbody>
</table>

**Diligenció**

**Fecha de Diligenciamiento**
<table>
<thead>
<tr>
<th>Nro</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE LLEVA A CABO UN ANÁLISIS GENERAL DE LOS REPORTES PRODUCIDOS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿ES CONTROLADA LA DISTRIBUCIÓN DE LOS REPORTES?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN PROCEDIMIENTOS PARA REVISAR LA EXACTITUD DE LAS SALIDAS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SE PRODUCEN LOS REPORTES ABSOLUTAMENTE NECESARIOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SE SUPERVISA LA DESTRUCCIÓN DE REPORTES NO NECESARIOS O QUE SON PRODUCTO DE PROCESOS ABORTADOS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SE INFORMA AL CENTRO DE INFORMÁTICA SOBRE AQUELLOS REPORTES QUE PRESENTAN INCONSISTENCIAS?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 3.6 CONTROLES DE SEGURIDAD EN ASPECTOS FÍSICOS Y TÉCNICOS

#### 3.6.1 ASPECTOS FÍSICOS DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE CONTROL SOBRE EL INGRESO DE FUNCIONARIOS A LA DEPENDENCIA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN PROGRAMAS DE PREVENCIÓN CONTRA DESASTRES?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTE SEÑALIZACIÓN DE LAS RUTAS DE EVACUACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN EXTINGUIDORES DENTRO DE LA INSTALACIÓN? REVISAR LA FECHA DE EXPIRACIÓN</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTE PLAN DE CONTINGENCIAS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿ESTÁN EL SOFTWARE Y EL HARDWARE AMPARADOS POR PÓLIZAS DE SEGUROS?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
### 3.6.2 ASPECTOS TÉCNICOS DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE CONTROL SOBRE CLAVES DE ACCESO AL SISTEMA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿TIENE LA APLICACIÓN MANuales TÉCNICOS, DE OPERACIÓN y DEL USUARIO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿CON QUÉ PERIODICIDAD SE LE SACA BACK-UP A LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿PUEDEN LOS OPERADORES O USUARIOS MODIFICAR LOS PROGRAMAS FUENTE DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SE PERMITE EL USO DE LA COMPUTADORA A PERSONAS EXTRANJERAS A LA DEPENDENCIA?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTE MÁS DE UN FUNCIONARIO QUE ESTÉ EN CAPACIDAD DE OPERAR LA APLICACIÓN?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
HOJA DE TRABAJO 4: ANÁLISIS ADMINISTRATIVO

4.1 CONTROLES ORGANIZACIONALES

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿LOS NIVELES JERÁRQUICOS DEL DEPARTAMENTO O UNIDAD PERMITEN UN DESENVOLVIMIENTO NORMAL DE SUS ACTIVIDADES?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE CUMPLEN LAS POLÍTICAS PARTICULARES IMPARTIDAS POR LA GERENCIA Y RELACIONADAS CON LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿LAS POLÍTICAS PARTICULARES RELACIONADAS CON LA APLICACIÓN ENCAJAN DENTRO DE LAS POLÍTICAS GENERALES DE LA EMPRESA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN POLÍTICAS DE CONTROL FISCAL CON RESPECTO A LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿CONOCE LA NORMATIVIDAD QUE COBija A LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTE MANUAL DE PROCEDIMIENTOS ESCRITO, RELACIONADO CON LA APLICACIÓN?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 4.2 TALENTO HUMANO

#### 4.2.1 ADMINISTRACIÓN Y ORGANIZACIÓN

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTEN POLÍTICAS SOBRE PLANEACIÓN DEL TALENTO HUMANO?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTE DENTRO DE LA EMPRESA LA FUNCIÓN DE AUDITORÍA APLICADA AL TALENTO HUMANO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTE DENTRO DE LA EMPRESA UN SISTEMA DE INFORMACIÓN DEL TALENTO HUMANO?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿CONoce el reglamento interno de trabajo?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿Existen políticas de salud ocupacional?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿Existe un programa de trabajo y se cumple a cabalidad?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CÓMO ES EL AMBIENTE LABORAL DEL ÁREA AUDITADA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN POLÍTICAS DE BIENESTAR LABORAL POR PARTE DE LA EMPRESA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿HAY ESTABILIDAD LABORAL EN LA EMPRESA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿ES ALTA LA ROTACIÓN DE PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN PROGRAMAS DE INDUCCIÓN?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SON PERIÓDICAS Y CONSECUTIVAS LAS VACACIONES DEL PERSONAL?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 4.2.3 ENTRENAMIENTO Y CAPACITACIÓN DEL PERSONAL DEL ÁREA AUDITADA

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTEN PLANES DE ENTRENAMIENTO Y CAPACITACIÓN PROGRAMADOS POR LA EMPRESA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SON EVALUADOS LOS PROGRAMAS DE ENTRENAMIENTO Y CAPACITACIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SON EVALUADAS LAS PERSONAS QUE RECIBIERON ENTRENAMIENTO Y CAPACITACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿CON QUÉ PERIODICIDAD SE IMPARTEN LOS CURSOS DE ENTRENAMIENTO Y CAPACITACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ESTÁN DIRIGIDOS LOS PROGRAMAS DE ENTRENAMIENTO Y CAPACITACIÓN A TODOS LOSFUNCIONARIOS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTEN PROGRAMAS DE INDUCCIÓN DIRIGIDOS A TODOS LOS FUNCIONARIOS?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**

162
### 4.2.4 DESEMPEÑO DEL PERSONAL DEL ÁREA AUDITADA

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CONOCÉ LOS ESTÁNDARES DE DESEMPEÑO Y LAS NORMAS QUE SE DEBEN SEGUIR?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE REALIZAN EVALUACIONES PERIÓDICAS DEL DESEMPEÑO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ES SUFICIENTE EL PERSONAL PARA EL CUMPLIMIENTO DE LAS FUNCIONES PROPIAS DEL ÁREA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTE EFICACIA EN EL CUMPLIMIENTO DE LAS FUNCIONES?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ES ADECUADA LA CALIDAD DEL TRABAJO EJECUTADO?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿HAY COOPERACIÓN POR PARTE DEL PERSONAL PARA LA REALIZACIÓN DE TAREAS?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
### 4.2.5 SUPERVISIÓN DEL PERSONAL DEL ÁREA AUDITADA

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CÓMO ES LA DISCIPLINA LABORAL DE LOS EMPLEADOS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SON FRECUENTES LOS CONFLICTOS LABORALES?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SON DEBIDAMENTE ATENDIDAS LAS QUEJAS Y RECLAMOS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿ES ALTO EL ÍNDICE DE AUSENTISMOS Y RETARDOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN POLÍTICAS INSTITUCIONALES RELACIONADAS CON LA SUPERVISIÓN DEL PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿CÓMO SE LLEVA A CABO LA SUPERVISIÓN DEL PERSONAL?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diligenció**

**FECHA DE DILIGENCIAMIENTO**
### 4.2.6 MOTIVACIÓN DEL PERSONAL DEL ÁREA AUDITADA

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿HAY MOTIVACIÓN AL INTERIOR DE LA EMPRESA U ORGANIZACIÓN?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN MECANISMOS DE ASCENSOS Y PROMOCIONES?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿CÓMO SE CONCEDEN LOS ASCENSOS, PROMOCIONES Y AUMENTOS SALARIALES?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿QUÉ FACTORES LO DESMOTIVAN PARA CUMPLIR CON SUS FUNCIONES?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diligenció**

**Fecha de diligenciamiento**
4.2.7 REMUNERACIÓN DEL PERSONAL DEL ÁREA AUDITADA

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE EN LA EMPRESA UNA POLÍTICA SALARIAL DEFINIDA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN INCENTIVOS SALARIALES?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ESTÁN ADECUADAMENTE REMUNERADOS LOS CARGOS DEL ÁREA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿LA REMUNERACIÓN ASIGNADA POR LA EMPRESA ES COMPETITIVA CON LOS SUELDOS Y SALARIOS PAGADOS EN EL MEDIO?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ADEMÁS DE LA REMUNERACIÓN DEL CARGO, QUÉ OTROS INCENTIVOS RECIBE?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
PUNTOS DE ATENCIÓN PARA FUTURAS REVISIONES

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
6.1 ASPECTOS CRÍTICOS

6.2 RECOMENDACIONES

6.3 RECOMENDACIONES ESPECÍFICAS FRENTE A LOS ASPECTOS CRÍTICOS

6.4 ENCARGADO DE LA PUESTA EN MARCHA

6.5 TIEMPO ESTIMADO DE LA PUESTA EN MARCHA

6.6 FECHA LÍMITE DE LA PUESTA EN MARCHA
6.7 OBSERVACIONES

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
ANEXO N° 10
GUÍA PARA LA DESCRIPCIÓN DE APLICACIONES EN DESARROLLO

ARCHIVO CORRIENTE. FORMULARIO H

EMPRESA AUDITADA:

EMPRESA AUDITORA:

NOMBRE DE APLICACIÓN:

HOJA DE TRABAJO 1: GENERALIDADES

1.1 OBJETIVOS DE LA AUDITORÍA DE SISTEMAS PARA APLICACIONES EN DESARROLLO

1.2 FECHA DE INICIO DEL DESARROLLO

OBSERVACIONES

1.3 DILIGENCIÓ:

1.4 FECHA DE DILIGENCIAMIENTO:
## HOJA DE TRABAJO 2: SESIONES DE TRABAJO

### 2.1 SESIONES DE TRABAJO CON DISEÑADORES/ADMINISTRADORES DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>FECHA</th>
<th>LUGAR</th>
<th>FUNCIONARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2 SESIONES DE TRABAJO CON USUARIOS DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>FECHA</th>
<th>LUGAR</th>
<th>FUNCIONARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.3 SESIONES DE TRABAJO CON AUDITORES DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>FECHA</th>
<th>LUGAR</th>
<th>FUNCIONARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.4 DILIGENCIACIÓN

### 2.5 FECHA DE DILIGENCIAMIENTO
## 3.1 ENTRADAS A LA APLICACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE CONSIDERARON TÉCNICAS PARA VALIDAR, PROBAR Y VERIFICAR LOS DATOS DE ENTRADA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE CONSIDERARON CONTROLES RAZONABLES RELACIONADOS CON LA GENERACIÓN DE DATOS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SON LOS FORMATOS DISEÑADOS PARA LA CAPTURA, LOS MÁS INDICADOS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SE CONSIDERARON MECANISMOS QUE RESTRINJAN EL ACCESO LÓGICO A LOS DISPOSITIVOS DE ENTRADA?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SE CONTEMPLÓ LA SEGREGACIÓN DE FUNCIONES ENTRE LA GENERACIÓN, REGISTRO Y ALMACENAMIENTO DE LOS DATOS DE ENTRADA?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿CONTEMPLA LA APLICACIÓN EN DESARROLLO LA MODIFICACIÓN DE DATOS ERRÓNEOS UNA VEZ HAN INGRESADO?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE REALIZÓ UN ANÁLISIS DE LOS REPORTES QUE SE DEBEN PRODUCIR?</td>
</tr>
<tr>
<td>2</td>
<td>¿CÓMO SE CONTROLARÁ LA DISTRIBUCIÓN DE LOS REPORTES?</td>
</tr>
<tr>
<td>3</td>
<td>¿CÓMO SE CONTROLARÁ LA EXACTITUD DE LAS SALIDAS?</td>
</tr>
<tr>
<td>4</td>
<td>¿QUÉ TRATAMIENTO SE LE DARÁ A LA INFORMACIÓN CONFIDENCIAL?</td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### HOJA DE TRABAJO 5: SOFTWARE DEL SISTEMA

#### 5.1 ASPECTOS GENERALES

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ES TENIDO EN CUENTA EL CRITERIO DEL USUARIO DURANTE EL DESARROLLO DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿CÓMO SE REGISTRARÁN LOS PROBLEMAS QUE SE PRESENTEN CON LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ES TENIDO EN CUENTA EL CRITERIO DEL AUDITOR DURANTE EL DESARROLLO DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN CONTROLES ADECUADOS PARA PROBAR LA NUEVA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SON AUDITADAS LAS APLICACIONES EN DESARROLLO?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SE ESTÁ CONFECCIONANDO LA DOCUMENTACIÓN A LA PAR CON EL DESARROLLO DE LA APLICACIÓN?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 5.2 PROGRAMAS DE LA APLICACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE PLANEACIÓN DE LAS PRUEBAS QUE DEBEN SER REALIZADAS A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN LIBRERÍAS ESPECÍFICAS PARA REALIZAR LAS PRUEBAS A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTE UNA AMPLIA DIFUSIÓN DE LAS PRUEBAS A REALIZAR?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN CIRCUNSTANCIAS ESPECÍFICAS QUE LIMITAN LA EJECUCIÓN DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿LA ETAPA DE DESARROLLO CONTEMPLA POSIBILIDAD DE REPROCESO PARA LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
PUNTOS DE ATENCIÓN PARA FUTURAS REVISIONES

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
7.1 ASPECTOS CRÍTICOS

7.2 RECOMENDACIONES

7.3 RECOMENDACIONES ESPECÍFICAS FRENTE A LOS ASPECTOS CRÍTICOS

7.4 OBSERVACIONES

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
ANEXO Nº 11
DESCRIPTOR Y EVALUACIÓN DE PROCEDIMIENTOS

ARCHIVO PERMANENTE. FORMULARIO I

EMPRESA AUDITADA:

EMPRESA AUDITORA:

1. GENERALIDADES

1.1 NOMBRE DEL FUNCIONARIO ENTREVISTADO

1.2 CARGO

1.3 DIVISIÓN / SECCIÓN

1.4 CARGO DEL JJEFE INMEDIATO

1.5 FECHA DE ANÁLISIS

2. ANÁLISIS DE ACTIVIDADES

2.1 ACTIVIDADES PRINCIPALES

(Señale el orden y periodicidad de las actividades principales que realiza normalmente)

<table>
<thead>
<tr>
<th>N°</th>
<th>ACTIVIDADES PRINCIPALES</th>
<th>D</th>
<th>S</th>
<th>Q</th>
<th>M</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2 SEÑALE LA PERIODICIDAD DE LAS ACTIVIDADES SECUNDARIAS QUE REALIZA NORMAMENTE EN SU TRABAJO

<table>
<thead>
<tr>
<th>Nº</th>
<th>ACTIVIDADES SECUNDARIAS</th>
<th>D</th>
<th>S</th>
<th>Q</th>
<th>M</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3 SEÑALE LA PERIODICIDAD DE LAS ACTIVIDADES ESPORÁDICAS U OCASIONALES QUE REALIZA NORMAMENTE EN SU TRABAJO

<table>
<thead>
<tr>
<th>Nº</th>
<th>ACTIVIDADES OCASIONALES</th>
<th>D</th>
<th>S</th>
<th>Q</th>
<th>M</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.4 ANÁLISIS DE DOCUMENTOS. RELACIONE LOS DOCUMENTOS EN CUYO PROCEDIMIENTO O TRÁMITE INTERVIENE Y SEÑALE LA PERIODICIDAD, ORIGEN, QUÉ TRÁMITE LE DA, DESTINO Y CONTROLES EJERCIDOS.

<table>
<thead>
<tr>
<th>NOMBRE DEL DOCUMENTO</th>
<th>FRECUENCIA</th>
<th>PROVIENE DE</th>
<th>TRÁMITES APLICADOS AL DOCUMENTO</th>
<th>A QUIÉN LO ENVÍA</th>
<th>CONTROLES EJERCIDOS AL DOCUMENTO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

181
3. RECOMENDACIONES O SUGERENCIAS FRENTE A LOS DOCUMENTOS MANEJADOS. IDENTIFIQUE EL NOMBRE Y LAS SUGERENCIAS QUE TIENE RESPECTO A LOS DOCUMENTOS MANEJADOS

<table>
<thead>
<tr>
<th>NOMBRE DEL DOCUMENTO</th>
<th>EXPLIQUE LA RECOMENDACIÓN</th>
<th>OTRAS</th>
<th>ELIMINAR SELLOS</th>
<th>ELIMINAR FIRMAS</th>
<th>SUPERVISAR COPIAS</th>
<th>CREARLO TOTALMENTE</th>
<th>REDISEÑAR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. ANÁLISIS RESPECTO A LA INFORMACIÓN CONFIDENCIAL. SI TIENE ACCESO A INFORMACIÓN CONFIDENCIAL, DESCRIBA SU CONTENIDO, FUENTE Y DESTINO

<table>
<thead>
<tr>
<th>MEDIO UTILIZADO</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPENDENCIA O PERSONA A QUIEN LA COMUNICA</td>
<td></td>
</tr>
<tr>
<td>DE QUÉ FUENTE LA OBTIENE</td>
<td></td>
</tr>
<tr>
<td>CONTENIDO, TIPO O NOMBRE DE LA INFORMACIÓN</td>
<td></td>
</tr>
</tbody>
</table>
5. QUE PASOS DE LOS PROCEDIMIENTOS EN LOS QUE USTED INTERVIENE, PODRÍAN 
SUPRIMIRSE O ADICIONARSE Y DE QUÉ FORMA?

6. CONOCE USTED LAS FUNCIONES OFICIALES ASIGNADAS A SU CARGO SI     NO
LAS CONOCIÓ EN FORMA VERBAL      ESCRITA
SI NO LAS CONOCE SE DEBE A

7. QUE INCONVENIENTES O DIFICULTADES AFRONTA EN EL CUMPLIMIENTO DE LAS 
ACTIVIDADES DE SU TRABAJO?

8. QUE SUGIERE PARA MEJORAR O SUPERAR LOS INCONVENIENTES MENCIONADOS?

9. OBSERVACIONES
ANEXO N° 12
PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

DIRIGIDO A JEFES Y DIRECTIVOS DEL CENTRO DE INFORMÁTICA
FORMULARIO J

DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

NOMBRE DEL ENTREVISTADO:

CARGO: FECHA:

1. CARACTERÍSTICAS GENERALES

1 ESTRUCTURA ORGÁNICA DE LA EMPRESA (ANEXAR)

2. POLÍTICAS Y OBJETIVOS DE LA EMPRESA

2.1 POLÍTICAS

2.2 OBJETIVOS

3. ESTRUCTURA ORGÁNICA DEL CENTRO DE INFORMÁTICA (ANEXAR)

4. PRINCIPALES OBJETIVOS DEL CENTRO DE INFORMÁTICA
4.1 OBJETIVOS GENERALES

4.2 OBJETIVOS ESPECÍFICOS

5. PERSONAL INTEGRANTE DEL CENTRO DE INFORMÁTICA

<table>
<thead>
<tr>
<th>Cargo</th>
<th>Nombre</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIRECTOR/JEFE/ANALISTA</td>
<td></td>
</tr>
<tr>
<td>ANALISTA/PROGRAMADOR</td>
<td></td>
</tr>
<tr>
<td>PROGRAMADOR</td>
<td></td>
</tr>
<tr>
<td>DIGITADOR</td>
<td></td>
</tr>
<tr>
<td>SECRETARIA</td>
<td></td>
</tr>
<tr>
<td>OTROS</td>
<td></td>
</tr>
</tbody>
</table>

2. RECURSOS INFORMÁTICOS

1. CONFIGURACIÓN DEL HARDWARE Y DISTRIBUCIÓN DENTRO DE LA EMPRESA
2. DESCRIBA EL SOFTWARE OPERATIVO Y SOFTWARE DE UTILIDAD ACTUALMENTE EN USO

<table>
<thead>
<tr>
<th>SOFTWARE OPERATIVO</th>
<th>SOFTWARE DE UTILIDAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. DESCRIBA BREVEMENTE LAS DISTINTAS APLICACIONES EN Funcionamiento

<table>
<thead>
<tr>
<th>APLICACIÓN</th>
<th>AMBIENTE</th>
<th>HERRAMIENTA/ LENGUAJE</th>
<th>Nº REGISTROS</th>
<th>ADQUIRIDA</th>
<th>DESARROLLADA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. DESCRIBA JERÁRQUITICAMENTE LAS DISTINTAS APLICACIONES EN DESARROLLO INDICANDO PORCENTUALMENTE EL ESTADO EN QUE SE ENCUENTRAN

<table>
<thead>
<tr>
<th>APLICACIÓN</th>
<th>AMBIENTE</th>
<th>LENGUAJE</th>
<th>ESTADO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. DESCRIBA LAS APLICACIONES QUE ESTÁN PENDIENTES POR DESARROLLAR Y TIEMPO ESTIMADO DE INICIACIÓN

<table>
<thead>
<tr>
<th>APLICACIÓN</th>
<th>TIEMPO (EN MESES)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. ASPECTOS DE AUDITORÍA

1. SE HA INVOLUCRADO AL PERSONAL DE AUDITORÍA EN ALGUNA DE LAS ETAPAS DEL DESARROLLO DE SOFTWARE?
   SI    NO

¿CUAL HA SIDO LA PARTICIPACIÓN?

2. SE HA INVOLUCRADO AL USUARIO EN ALGUNAS DE LAS ETAPAS DEL DESARROLLO DE SOFTWARE?
   SI
   NO    (PASE A LA PREGUNTA 4)

3. ¿EN QUÉ ETAPAS Y CÚAL HA SIDO SU PARTICIPACIÓN?

<table>
<thead>
<tr>
<th>ETAPA</th>
<th>DESCRIPCIÓN DE LA PARTICIPACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. EL SOFTWARE DESARROLLADO INCLUYE CONCEPTOS DE AUDITORÍA DE SISTEMAS?

SI NO

EXPLIQUE CUALES

5. DOCUMENTACIÓN DEL CENTRO DE INFORMÁTICA

<table>
<thead>
<tr>
<th>Documentación</th>
<th>SI</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan estratégico de sistemas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metodología y estándares formales para el desarrollo de software</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedimientos para copias de respaldo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan de contingencias</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan de mantenimiento</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pólizas/seguros</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual de funciones</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual de procedimientos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual técnico</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual del operador</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual del digitador (capturador)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. HA SIDO EL CENTRO DE INFORMÁTICA OBJETO DE AUDITORÍA DE SISTEMAS INTERNA O EXTERNA? INDIQUE QUIÉN LA HIZO Y CON QUÉ PERIODICIDAD SE HA EFECTUADO

<table>
<thead>
<tr>
<th>ENTIDAD</th>
<th>PERIODICIDAD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

189
4. OBSERVACIONES
ANEXO N° 13
PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS
AL CENTRO DE INFORMÁTICA

ESTIMACIÓN DE TIEMPOS
FORMULARIO K

<table>
<thead>
<tr>
<th>ACTIVIDAD</th>
<th>TIEMPO ESTIMADO EN HORAS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. CONOCIMIENTO-AMBIENTACIÓN</strong></td>
<td></td>
</tr>
<tr>
<td><strong>II. ASPECTOS ADMINISTRATIVOS</strong></td>
<td></td>
</tr>
<tr>
<td>• Evaluación del plan estratégico de sistemas de información</td>
<td></td>
</tr>
<tr>
<td>• Evaluación de políticas administrativas</td>
<td></td>
</tr>
<tr>
<td>• Análisis organizacional</td>
<td></td>
</tr>
<tr>
<td>• Análisis de estándares</td>
<td></td>
</tr>
<tr>
<td>• Análisis del talento humano</td>
<td></td>
</tr>
<tr>
<td><strong>III. ASPECTOS TÉCNICOS</strong></td>
<td></td>
</tr>
<tr>
<td>• Evaluación de políticas técnicas</td>
<td></td>
</tr>
<tr>
<td>• Evaluación del desarrollo de sistemas</td>
<td></td>
</tr>
<tr>
<td>• Evaluación de la implementación de sistemas</td>
<td></td>
</tr>
<tr>
<td>• Evaluación de controles de: entrada, salida, mantenimiento, software del sistema</td>
<td></td>
</tr>
<tr>
<td><strong>IV. ASPECTOS DE SEGURIDAD</strong></td>
<td></td>
</tr>
<tr>
<td>• Evaluación de políticas de seguridad</td>
<td></td>
</tr>
<tr>
<td>• Seguridad física</td>
<td></td>
</tr>
<tr>
<td>• Instalaciones</td>
<td></td>
</tr>
<tr>
<td>• Personal</td>
<td></td>
</tr>
<tr>
<td>• Equipos</td>
<td></td>
</tr>
<tr>
<td>• Documentación</td>
<td></td>
</tr>
<tr>
<td>• Back - ups</td>
<td></td>
</tr>
<tr>
<td>• Pólizas / seguros</td>
<td></td>
</tr>
<tr>
<td>• Plan de contingencias</td>
<td></td>
</tr>
<tr>
<td><strong>Total tiempo en horas profesional</strong></td>
<td></td>
</tr>
</tbody>
</table>

191
ANEXO N° 14
AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

ARCHIVO PERMANENTE. ASPECTOS ADMINISTRATIVOS. FORMULARIO L

DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

FECHA:

1. RESEÑA DEL CENTRO DE INFORMÁTICA

2. OBJETIVOS

2.1 OBJETIVOS A LARGO PLAZO

2.2 OBJETIVOS A CORTO PLAZO
3. ESTRUCTURA ORGÁNICA

3.1 ESTRUCTURA ORGÁNICA DE LA EMPRESA (ANEXAR)

3.2 ESTRUCTURA ORGÁNICA DEL CENTRO DE INFORMÁTICA (ANEXAR)

4. POLÍTICAS ADMINISTRATIVAS

5. PLANEACIÓN ESTRATÉGICA DE SISTEMAS DE INFORMACIÓN (P.E.S.I.)

5.1 COHERENCIA ENTRE OBJETIVOS ORGANIZACIONALES Y OBJETIVOS DE LA P.E.S.I.

5.2 OBJETIVOS A LARGO PLAZO

5.3 OBJETIVOS A CORTO PLAZO
5.4 COMPROMISO DE LA EMPRESA CON LA P.E.S.I.

5.5 PERSONAL PARTICIPANTE EN LA ELABORACIÓN Y PUESTA EN MARCHA DE LA P.E.S.I.

5.6 TIEMPO PROYECTADO DE LA P.E.S.I.

5.7 ANÁLISIS COSTO-BENEFICIO DE LA P.E.S.I.

5.8 BREVE DESCRIPCIÓN DE LAS HERRAMIENTAS Y COMPONENTES CONSIDERADOS EN LA ELABORACIÓN DE LA P.E.S.I.
6. NORMATIVIDAD

7. TALENTO HUMANO

7.1 INVENTARIO DEL TALENTO HUMANO (ANEXAR)

7.2 POLÍTICAS

7.3 DESCRIPCIÓN DE ESTÁNDARES DE DESEMPEÑO

7.4 REGLAMENTO INTERNO (ANEXAR)

7.5 PROGRAMA DE TRABAJO (ANEXAR)
7.6 RELACIONAR LOS PROGRAMAS DE ENTRENAMIENTO Y CAPACITACIÓN

7.7 ANEXAR MANUAL DE FUNCIONES

7.8 ANEXAR MANUAL DE PROCEDIMIENTOS

8. ELEMENTOS FINANCIEROS

8.1 EXPLIQUE BREVEMENTE EL SISTEMA EMPLEADO DE COSTEO POR APLICACIÓN

8.2 EXPLIQUE BREVEMENTE LA METODOLOGÍA PARA ESTIMAR TIEMPOS Y COSTOS APLICABLES A LOS PROYECTOS INFORMÁTICOS
ANEXO N° 15
AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

ARCHIVO PERMANENTE. ASPECTOS TÉCNICOS. FORMULARIO M

DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

FECHA:

1. POLÍTICAS DE ORDEN TÉCNICO

2. INVENTARIO DE SOFTWARE

2.1 SOFTWARE GENÉRICO

<table>
<thead>
<tr>
<th>NOMBRE DEL SOFTWARE</th>
<th>DESCRIPCIÓN</th>
<th>DESARROLLADO</th>
<th>ADQUIRIDO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

197
2.2 APLICACIONES EN FUNCIONAMIENTO

<table>
<thead>
<tr>
<th>NOMBRE DE LA APLICACIÓN</th>
<th>AMBIENTE</th>
<th>NÚMERO REGISTROS</th>
<th>LENGUAJE</th>
<th>ADQUIRIDA</th>
<th>DESARROLLADA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. INVENTARIO DE HARDWARE

<table>
<thead>
<tr>
<th>CONFIGURACIÓN</th>
<th>UBICACIÓN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4. DESARROLLO E IMPLEMENTACIÓN DE SISTEMAS

4.1 DEFINICIÓN DE ESTÁNDARES DE PRODUCCIÓN
4.2 DEFINICIÓN DE ESTÁNDARES DE CALIDAD

4.3 DEFINICIÓN DE ESTÁNDARES PARA APLICACIONES SOPORTADAS POR TELEPROCESO

5. ENTRADA DE DATOS

5.1 PROCEDIMIENTO PARA CAPTURA DE DATOS

5.2 PROCEDIMIENTO PARA REGISTRO DE TRANSACCIONES

5.3 PROCEDIMIENTO PARA REGISTRO DE DOCUMENTOS EN TRÁNSITO
5.4 PROCEDIMIENTO PARA TRATAMIENTO DE ERRORES

6. SALIDA DE DATOS

6.1 PROCEDIMIENTO PARA SALIDA DE DATOS

6.2 PROCEDIMIENTO PARA REPORTE DE INCONSISTENCIAS

7. SOFTWARE DEL SISTEMA

7.1 PROCEDIMIENTO PARA ASIGNACIÓN DE CUENTAS
7.2 PROCEDIMIENTO RELACIONADO CON LA BASE DE DATOS

7.3 PROCEDIMIENTO RELACIONADO CON EL SISTEMA OPERATIVO

7.4 PROCEDIMIENTO PARA CORRIDA DE PROGRAMAS

7.5 PROCEDIMIENTO PARA CORRIDA DE TRABAJOS ESPECIALES

7.6 CRITERIOS PARA ASIGNACIÓN DE CONTROLES
ANEXO N° 16
AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

ARCHIVO PERMANENTE. ASPECTOS DE SEGURIDAD. FORMULARIO N

DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

FECHA:

1. POLÍTICAS DE SEGURIDAD

2. INSTALACIONES

2.1 DESCRIPCIÓN DE LA UBICACIÓN DEL CENTRO DE INFORMÁTICA

2.2 ANEXAR PLANOS FÍSICOS

2.3 ANEXAR PLANOS ELÉCTRICOS

2.4 ANEXAR PLANOS HIDRÁULICOS
2.5 ANEXAR PLANOS DE DUCTOS DE AIRE

2.6 DESCRIPCIÓN DE LAS CONDICIONES FÍSICO-AMBIENTALES

3. EQUIPOS

3.1 ANEXAR CONVENIOS DE RESPALDO DE EQUIPOS CON OTRAS INSTITUCIONES O EMPRESAS

4. DOCUMENTACIÓN

4.1 ANEXAR MANUAL DEL OPERADOR

4.2 ANEXAR MANUAL DEL SISTEMA

4.3 ANEXAR MANUAL DEL AUDITOR

5. BACK-UPS

5.1 PROCEDIMIENTO DE BACK-UPS
6. PÓLIZAS

6.1 ANEXAR PÓLIZA DE SEGUROS DEL HARDWARE
6.2 ANEXAR PÓLIZA DE SEGUROS DEL SOFTWARE
6.3 ANEXAR PÓLIZA DE SEGUROS DE LAS INSTALACIONES

7. PROCEDIMIENTOS DE SEGURIDAD

8. PLAN DE CONTINGENCIAS

8.1 DESCRIPCIÓN DEL PLAN DE CONTINGENCIAS (ANEXAR)
## ANEXO N° 17
AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

ARCHIVO CORRIENTE. ASPECTOS ADMINISTRATIVOS. FORMULARIO O DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SON LOS OBJETIVOS DEL CENTRO DE INFORMÁTICA COHERENTES CON LOS OBJETIVOS DE LA ORGANIZACIÓN?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SON LOS PLANES A CORTO PLAZO DEL CENTRO DE INFORMÁTICA, COHERENTES CON LOS PLANES A LARGO PLAZO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTE COMPROMISO A NIVEL DE DIRECCIÓN CON AQUELLOS ASPECTOS INFORMÁTICOS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿QUIÉN DETERMINA LAS METAS A LARGO PLAZO DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ES CONSIDERADO EL CRONOGRAMA COMO HERRAMIENTA DE PLANEACIÓN?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿HAY AMPLIA PARTICIPACIÓN EN LA ELABORACIÓN DE LA P.E.S.I.?</td>
<td></td>
</tr>
</tbody>
</table>

Diligenció | Fecha de diligenciamiento
<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE CLARA DEFINICIÓN DE POLÍTICAS AL INTERIOR DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN POLÍTICAS CON RELACIÓN A LA INTEGRACIÓN DE LOS SISTEMAS DE INFORMACIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN POLÍTICAS RELACIONADAS CON LA LEGALIZACIÓN DEL SOFTWARE UTILIZADO?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN POLÍTICAS RELACIONADAS CON EL ENTRENAMIENTO Y CAPACITACIÓN DEL PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN POLÍTICAS RELACIONADAS CON EL DESEMPEÑO DE PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTEN POLÍTICAS RELACIONADAS CON LAS VACACIONES ANUALES DEL PERSONAL</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### HOJA DE TRABAJO 3: ANÁLISIS ORGANIZACIONAL

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ES EVALUADA PERIÓDICAMENTE LA ESTRUCTURA ORGÁNICA DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTE UNA ADECUADA SEPARACIÓN DE FUNCIONES PARA LOS DISTINTOS CARGOS DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN PROCEDIMIENTOS ESCRITOS QUE INDICEN COMO REALIZAR CAMBIOS O MODIFICACIONES A PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN MECANISMOS QUE PERMITAN LA SUSPENSIÓN INMEDIATA DE EMPLEADOS DESHONESTOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN PROCEDIMIENTOS ESCRITOS QUE SEÑALEN LA FORMA DE REPORTAR DIFICULTADES?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTEN POLÍTICAS DE CONTROL FISCAL CON RESPECTO AL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
</tbody>
</table>

 **Diligenció**

 **Fecha de diligenciamiento**
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTEN ESTÁNDARES ESCRITOS CLARAMENTE DEFINIDOS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE REALIZAN ANÁLISIS DE NECESIDADES PREVIO A LA ADQUISICIÓN DE SOFTWARE Y HARDWARE UTILIZADO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SE ACTUALIZA CON PERIODICIDAD EL SOFTWARE Y HARDWARE UTILIZADO?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SON AUTORIZADAS POR LOS USUARIOS LAS MODIFICACIONES A LAS APLICACIONES?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SE DESARROLLAN E IMPLEMENTAN SISTEMAS DE COSTEO POR APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTEN ESTÁNDARES PARA LA OPERACIÓN DE LOS SISTEMAS DE INFORMACIÓN?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### HOJA DE TRABAJO 5: TALENTO HUMANO

#### 5.1 ADMINISTRACIÓN Y ORGANIZACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTEN POLÍTICAS SOBRE PLANEACIÓN DEL TALENTO HUMANO DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿CONOCE EL REGLAMENTO INTERNO DE TRABAJO A NIVEL ORGANIZACIONAL Y A NIVEL DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN POLÍTICAS DE SALUD OCUPACIONAL AL INTERIOR DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTE UN PROGRAMA DE TRABAJO AL INTERIOR DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>VERIFICAR LA APLICACIÓN DE LA FUNCIÓN DE AUDITORÍA AL TALENTO HUMANO</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTE AL INTERIOR DEL CENTRO DE INFORMÁTICA UN SISTEMA DE INFORMACIÓN DEL TALENTO HUMANO?</td>
<td></td>
</tr>
</tbody>
</table>

### DILIGENCIÓ

### FECHA DE DILIGENCIAMIENTO
### 5.2 ENTRENAMIENTO Y CAPACITACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTEN PROGRAMAS PERMANENTES DE ENTRENAMIENTO Y CAPACITACIÓN?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE CONOCEN LAS NECESIDADES DE CAPACITACIÓN INMEDIATAS Y A LARGO PLAZO, REQUERIDAS POR EL PERSONAL DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SON EVALUADOS PERMANENTEMENTE LOS PROGRAMAS DE ENTRENAMIENTO Y CAPACITACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SON EVALUADAS LAS PERSONAS QUE RECIBIERON ENTRENAMIENTO Y CAPACITACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ESTÁ EL PERSONAL DEBIDAMENTE FORMADO PARA CUMPLIR A CABALIDAD CON SUS FUNCIONES?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTE MATERIAL BIBLIOGRÁFICO ACTUALIZADO Y DISPONIBLE?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**

210
### 5.3 AMBIENTE LABORAL

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CÓMO ES EL AMBIENTE LABORAL?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿ES ALTA LA ROTACIÓN DEL PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN POLÍTICAS SOBRE REEMPLAZAMIENTO DE PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SON EXIGIDOS EXÁMENES MÉDICOS Y PSICOLÓGICOS ESPECIALES COMO REQUISITO DE VINCULACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN POLÍTICAS CON RESPECTO A LAS VACACIONES DE PERSONAL?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SE REALIZA ANÁLISIS DE REFERENCIAS Y ANTECEDENTES PREVIO A LA VINCULACIÓN DE PERSONAL?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**

211
<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ES ALTO EL ÍNDICE DE AUSENTISMOS Y RETARDOS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CÓMO ES LA DISCIPLINA LABORAL DE LOS FUNCIONARIOS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN CONFLICTOS LABORALES AL INTERIOR DEL CENTRO DE INFORMÁTICA? FRECUENCIA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SON ATENDIDAS OPORTUNAMENTE LAS QUEJAS Y/O RECLAMOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SE CUMPLE POR PARTE DE LOS FUNCIONARIOS CON LA JORNADA LABORAL CONTRATADA?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿ES CONTROLADA LA CALIDAD DE TRABAJO DESARROLLADO?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 5.5 MOTIVACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE MOTIVACIÓN AL INTERIOR DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN POLÍTICAS DE ASCENSOS Y PROMOCIONES?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO

### 5.5 REMUNERACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ESTÁN ADECUADAMENTE REMUNERADOS LOS CARGOS DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿LA REMUNERACIÓN ASIGNADA POR LA EMPRESA ES COMPETITIVA CON LOS SUELDOS Y SALARIOS PAGADOS EN EL MEDIO?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### HOJA DE TRABAJO 6: ASPECTOS FINANCIEROS

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE UN SISTEMA DE COSTEO POR APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTE UNA METODOLOGÍA PARA ESTIMAR LOS TIEMPOS Y COSTOS DE CADA PROYECTO INFORMÁTICO?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**

---

### HOJA DE TRABAJO 7: PUNTOS DE ATENCIÓN PARA FUTURAS REVISIONES

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
ANEXO N° 18  
AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

ARCHIVO CORRIENTE. ASPECTOS TÉCNICOS. FORMULARIO P

DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SON FRECUENTEMENTE INTERRUMPIDOS LOS PROYECTOS DE SISTEMAS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTEN ESTÁNDARES DE PRODUCCIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTE INTEGRACIÓN ENTRE SUBSISTEMAS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿CÓMO SE EVALÚAN LOS SISTEMAS DE INFORMACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿CÓMO SE ADMINISTRAN LOS PROYECTOS INFORMÁTICOS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SE REVISAN PERIÓDICAMENTE LOS SISTEMAS EN funcionamiento?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ                                      FECHA DE DILIGENCIAMIENTO
### HOJA DE TRABAJO 2: ENTRADA DE DATOS

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE UTILIZAN TÉCNICAS DE VERIFICACIÓN DURANTE LA GRABACIÓN DE DATOS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SON VERIFICADOS LOS DATOS DE ENTRADA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿HAY LIBRE ACCESO AL CUARTO DE LA COMPUTADORA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿LOS ANALISTAS DE SISTEMAS TIENEN ACCESO A LOS DATOS Y PROGRAMAS DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN PROCEDIMIENTOS ESCRITOS PARA EL TRATAMIENTO DE ERRORES?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿PUEDEN LOS FUNCIONARIOS DEL CENTRO DE INFORMÁTICA ACCEDER A LOS EQUIPOS E INSTALACIONES POR FUERA DEL HORARIO OFICIAL?</td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ESTÁN PLENAMENTE IDENTIFICADOS LOS REPORTES GENERADOS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿ESTÁN TOTALMENTE FECHADOS Y PAGINADOS LOS INFORMES PRODUCIDOS POR EL SISTEMA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿LOS REPORTES GENERADOS SON ENTREGADOS CON OFICIO REMISORIO?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SE CONTROLA LA CALIDAD DE LA INFORMACIÓN PRODUCIDA?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿ESTÁ BIEN PROTEGIDA LA INFORMACIÓN CONFIDENCIAL?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿ES DESTRUIDA LA INFORMACIÓN CONFIDENCIAL ESCRITA NO UTILIZABLE?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE PROGRAMA LA UTILIZACIÓN DEL EQUIPO DE COMPUTACIÓN?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTE UN PLAN DE MANTENIMIENTO A LAS APLICACIONES?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SE LE AVISA OPORTUNAMENTE A LOS USUARIOS CUÁNDO SE VA A APAGAR EL EQUIPO CENTRAL?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿CÓMO SE CONTROLA EL MANTENIMIENTO DEL EQUIPO DE COMPUTACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿SE LLEVA UN REGISTRO DE MANTENIMIENTO DE LAS UPS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿SON PROGRAMADOS LOS MANTENIMIENTOS A LAS APLICACIONES?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO

218
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE UNA ADECUADA SEGREGACIÓN DE FUNCIONES AL INTERIOR DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE ENCUENTRAN VARIAS PERSONAS CAPACITADAS EN EL FUNCIONAMIENTO DE CADA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿PUEDEN LOS ANALISTAS Y DISEÑADORES DE SISTEMAS OPERAR EL EQUIPO DE COMPUTACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿CON QUÉ FRECUENCIA SON REPROCESADAS LAS APLICACIONES?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿PUEDE EL OPERADOR DE LA COMPUTADORA EJERCER FUNCIONES DE CONTROL DE SALIDAS?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿ES RESPONSABLE EL OPERADOR DE LA CUSTODIA DE LA CINTOTECA?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
### 6.1 Aspectos Generales

<table>
<thead>
<tr>
<th>N°</th>
<th>Descripción</th>
<th>Hallazgos</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿Cómo se administran las claves de acceso?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿Se cambian periódicamente las palabras clave (passwords)?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿Se controla el número de intentos fallidos al utilizar la clave de acceso?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿Cómo se controlan las violaciones a la seguridad del sistema?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿Se utilizan técnicas de criptografía?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿Con qué periodicidad se revisa el log del sistema?</td>
<td></td>
</tr>
</tbody>
</table>

**Diligenció**

**Fecha de diligenciamiento**
### 6.2 PROGRAMAS

<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CÓMO SE DETERMINAN LOS CONTROLES APLICABLES A LOS PROGRAMAS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTE UN PROCEDIMIENTO PARA LA CORRIDA DE TRABAJOS ESPECIALES O DELICADOS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN ESTÁNDARES DE CALIDAD DEL SOFTWARE PRODUCIDO?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SE LLEVA CONTROL DE LAS TRANSACCIONES GENERADAS POR EL SISTEMA?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿CÓMO SE CONTROLA LA EJECUCIÓN DE LAS APLICACIONES?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿CÓMO SE CONTROLAN LAS ACTIVIDADES DEL OPERADOR DEL EQUIPO DE COMPUTACIÓN?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
HOJA DE TRABAJO 7: PUNTOS DE ATENCIÓN PARA FUTURAS REVISIONES

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO

222
ANEXO N° 19
AUDITORÍA DE SISTEMAS AL CENTRO DE INFORMÁTICA

ARCHIVO CORRIENTE. ASPECTOS DE SEGURIDAD. FORMULARIO Q

DEPENDENCIA AUDITADA: CENTRO DE INFORMÁTICA

EMPRESA AUDITORA:

### HOJA DE TRABAJO 1: SEGURIDAD FÍSICA

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CÓMO ES LA UBICACIÓN FÍSICA DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ FECHA DE DILIGENCIAMIENTO

### HOJA DE TRABAJO 2: INSTALACIONES

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿CÓMO SON LAS INSTALACIONES DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿EXISTE SEÑALIZACIÓN DE RUTAS DE EVACUACIÓN AL INTERIOR DEL CENTRO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿HAY EXTINGUIDORES DENTRO DEL CENTRO? VERIFICAR LA FECHA DE EXPIRACIÓN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PREGUNTA</td>
<td>RESPUESTA</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>4</td>
<td>¿DÓNDE SE ENCUENTRA UBICADO EL PANEL DE CONTROL ELÉCTRICO?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTEN CABLES E INSTALACIONES ELÉCTRICAS SOBRE EL PISO?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿CÓMO ES LA VIGILANCIA DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>¿CÓMO SE REALIZA EL ALMACENAMIENTO DE LA PAPELERÍA?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>¿CÓMO SE REALIZA EL ASEO AL EQUIPO DE COMPUTACIÓN?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>¿CÓMO SON LAS CONDICIONES FÍSICO-AMBIENTALES DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
## HOJA DE TRABAJO 3: PERSONAL

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿QUIÉN ES EL RESPONSABLE DE LA SEGURIDAD DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿PUEDEN LOS ANALISTAS DE SISTEMAS INGRESAR AL CUARTO DE LA COMPUTADORA?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SE INHABILITA LA CLAVE DE ACCESO AL SISTEMA DE LOS FUNCIONARIOS RETIRADOS TEMPORAL O DEFINITIVAMENTE?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTEN PROGRAMAS DE PREVENCIÓN CONTRA DESASTRES?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿CÓMO SE CONTROLA EL ACCESO A LOS RECURSOS DEL SISTEMA?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿QUÉ CONTROLES SE APLICAN A LAS UPS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE DISPONE DE UPS DE RESPALDO?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTEN CONVENIOS CON OTRAS EMPRESAS PARA EL RESPALDO DE EQUIPOS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SE CUENTA CON PLANOS ELÉCTRICOS ACTUALIZADOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿POSEEN FORROS O CUBIERTAS QUE PROTEJAN EL EQUIPO DE COMPUTACIÓN?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
### HOJA DE TRABAJO 5: DOCUMENTACIÓN

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ESTÁN LAS APLICACIONES SISTEMATIZADAS COMPLETAMENTE DOCUMENTADAS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE ACTUALIZA PERMANENTEMENTE LA DOCUMENTACIÓN DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SE RESTRINGE EL ACCESO A LA DOCUMENTACIÓN?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SE DISPONE DE DUPLICADO DE LA DOCUMENTACIÓN DE LA APLICACIÓN?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>VERIFICAR EL LUGAR DE ALMACENAMIENTO DE LA DOCUMENTACIÓN Y SUS COPIAS</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTEN POLÍTICAS DEFINIDAS CON RESPECTO A LOS BACK-UPS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿CÓMO SE CONTROLA EL TRANSPORTE DE DISCOS Y CINTAS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ES REVISADO EL LOG DE LOS OBJETOS SALVADOS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿CON QUÉ FRECUENCIA SE SACA BACK-UP DEL SISTEMA OPERATIVO?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>VERIFICAR EL LUGAR DONDE SE GUARDAN LAS COPIAS DE LOS BACK-UPS</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO

228
**HOJA DE TRABAJO 7: PÓLIZAS-SEGUROS**

<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿ESTÁ EL SOFTWARE Y EL HARDWARE AMPARADOS POR PÓLIZAS DE SEGUROS?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE VERIFICAN LAS FECHAS DE VENCIMIENTO DE LAS PÓLIZAS DE SEGUROS?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿SE EXIGE FIANZA PARA AQUELLOS CARGOS QUE IMPLÍCAN RIESGOS AL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿LOS VALORES AMPARADOS DEL SOFTWARE Y HARDWARE, ESTÁN DEBIDAMENTE ACTUALIZADOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DILIGENCIÓ**

**FECHA DE DILIGENCIAMIENTO**
<table>
<thead>
<tr>
<th>N°</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿SE EVALÚAN PERIÓDICAMENTE LOS PLANES DE SEGURIDAD?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿ESTÁ CAPACITADO EL PERSONAL PARA LA APLICACIÓN DE CONTROLES Y PROCEDIMIENTOS DE SEGURIDAD?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿ESTÁ CAPACITADO EL PERSONAL DE SISTEMAS PARA MANEJAR LOS EQUIPOS DE EMERGENCIA?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿SON DETALLADOS Y COMPRENSIBLES LOS PLANES DE SEGURIDAD?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
<table>
<thead>
<tr>
<th>Nº</th>
<th>DESCRIPCIÓN</th>
<th>HALLAZGOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>¿EXISTE UN PLAN DE CONTINGENCIAS INFORMÁTICO DE AMPLIA COBERTURA?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>¿SE REALIZAN SIMULACROS CON PERIODICIDAD?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>¿EXISTE ALGUNA PERSONA RESPONSABLE DEL PLAN DE CONTINGENCIAS?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>¿EXISTE UN PROCEDIMIENTO QUE INDIQUE CÓMO REALIZAR SIMULACROS Y QUE ASPECTOS DEBEN SER CONSIDERADOS?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>¿EXISTE UN COMITÉ DE SEGURIDAD AL INTERIOR DEL CENTRO DE INFORMÁTICA?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>¿EXISTE UN CONVENIO DE RESPALDO CON OTRAS EMPRESAS O INSTITUCIONES?</td>
<td></td>
</tr>
</tbody>
</table>

DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO
DILIGENCIÓ

FECHA DE DILIGENCIAMIENTO

232