Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ciencias Matemáticas

Escuela Profesional de Computación Científica

Mejoramiento de calidad de auditoría a las tecnologías de información y comunicaciones

TESINA

Para optar el Título Profesional de Licenciado en Computación Científica

AUTOR

Carlos Alberto PAREDES CABRERA

Lima, Perú

2016

Referencia bibliográfica

Paredes, C. (2016). *Mejoramiento de calidad de auditoría a las tecnologías de información y comunicaciones*. [Tesina de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Escuela Profesional de Computación Científica]. Repositorio institucional Cybertesis UNMSM.

UNIVERSIDAD NACIONAL MAYOR DE SANMARCOS

(Universidad del Perú, DECANA DE AMERICA)

FACULTAD DE CIENCIAS MATEMATICAS

PROGRAMA DE ACTUALIZACIÓN PARA LA TITULACIÓN PROFESIONAL 2016-II
MODALIDAD EXAMEN DE SUFICIENCIA PROFESIONAL

(R.R. N° 03849-R-16

ESCUELA PROFESIONAL DE COMPUTACIÓN

ACTA DE EXPOSICIÓN DE TESINA

En la Ciudad Universitaria, Facultad de Ciencias Matemáticas, siendo las .....horas, del día 11 de Diciembre del 2016, se reunieron las docentes designadas como miembros del Jurado Evaluador:

- Dra. María Natividad Zegarra Garay — Presidenta
- Lic. José Luis Acuña Guillermo — Miembro

Para la exposición de Tesina titulada: «**MEJORAMIENTO DE CALIDAD DE AUDITORIA A LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES**», *presentada* por el Bachiller **Carlos Alberto Paredes Cabrera**

Luego de la exposición de la tesina, los Miembros del Jurado hicieron las preguntas correspondientes, a las cuales el Bachiller, **Carlos Alberto Paredes Cabrera** respondió con acierto y solvencia, demostrando pleno conocimiento del tema.

Hecha la evaluación correspondiente, según tabla adjunta, la Bachiller **Carlos Alberto Paredes Cabrera** mereció la aprobación obteniendo como calificativo promedio y la nota calificativo.....dieciocho (18).....(letras y números). Mereció

A continuación los miembros del Jurado, dan manifiesto que el Bachiller **Carlos Alberto Paredes Cabrera** APROBÓ la exposición de la tesina.

Siendo las 13:00 horas, se levantó la sesión, firmando para constancia la presente acta en dos (2) copias originales.

Lic. José Luis Acuña Guillermo
MIEMBRO

Dra. María Natividad Zegarra Garay
PRESIDENTA

INDICE

1. ANÁLISIS SITUACIONAL Y PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES

.

En el campo de la auditoria a los sistemas de información y comunicaciones (TIC), ya existe una cultura organizacional para realizar estas actividades y dado que el avance en las organizaciones de la automatización de sus procesos y la lenta adecuación en los criterios y lenguajes de los auditores financieros con los ingenieros especialistas en el area de las ciencias de la información y comunicaciones, surgió la necesidad de desarrollar una metodología para desarrollar auditorias de TIC sobre la base estándar Cobit 4.1 y la norma ISO/IEC 27002.

Esta tesina permite mostrar una metodología para mejorar la calidad de auditoría TIC, integrando auditores, ejecutivos de la organización y usuarios finales basándose para ello en el marco conceptual que entrega el estándar internacional COBIT y la norma técnica ISO/IEC 27002 de modo que se logre obtener una mayor cooperación entre los equipos de trabajo y se cumplan en forma oportuna y al menor costo los objetivos planificados.

1.2 OBJETIVOS DE LA INVESTIGACION

1.2.1 OBJETIVO GENERAL

El objetivo general es mejorar la calidad de las auditorias a las TIC realizadas a las organizaciones, empresas o entidades.

1.2.2 OBJETIVO ESPECIFICO

El objetivo específico es apoyar la realización de las auditorías a las tecnologías de la información y las comunicaciones utilizando para ello el marco conceptual que entrega el estándar internacional COBIT y la norma ISO/IEC 27002.

El logro de este objetivo específico permitirá entre otros:

- Desarrollar auditorias de manera estructurada y uniforme.
- Entregar normas y procedimientos actualizados para examinar los sistemas de información y la infraestructura tecnológica que los soportan.
- Especificar los objetivos de control para realizar las pruebas de cumplimiento y sustantivas.
- Promover la evaluación de los controles claves de los procesos y sistemas de información que soportan el negocio de la organización.
- Suministrar un marco de referencia para medir el desempeño de los auditores a cargo y en terreno.

2. RESULTADO DE LA INVESTIGACIÓN

2.1 MARCO TEÓRICO

2.1.1. DEFINICION DE AUDITORIA

Según Alvin A. Arens:

La auditoria es la recopilación y evaluación de datos, sobre información cuantificable de una entidad económica para determinar e informar sobre el grado de correspondencia entre la información y los criterios establecidos, la auditoria debe ser realizada por una persona independiente.

2.1.2 TIPOS DE AUDITORIA

AUDITORIA DE GESTION.

La auditoría de gestión, está orientada a la evaluación de aspectos relacionados con la eficiencia y productividad de las operaciones de una organización. Este tipo de auditoría puede ser desempeña tanto por auditores externos como internos.

Constituye objeto de la auditoria de gestión, el proceso administrativo, las actividades de apoyo y operativas, la eficiencia, efectividad y economía en el empleo de los recursos humanos, financieros, ambientales, tecnológicos y de tiempo; y el cumplimiento de las atribuciones institucionales.

AUDITORIA INTEGRAL

La auditoría integral, se realiza con el fin de evaluar en su totalidad los objetivos que existen en una organización, es decir, los relacionados con información financiera, salvaguardar los activos, eficiencia y normativa, entre otros. Este tipo de auditorías también pueden ser realizadas tanto por auditores externos como internos.

AUDITORIA A LAS TIC

Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos lleva a cabo los fines de la organización y utiliza eficientemente los recursos.

Cabe mencionar sobre la auditoria a las TIC, que todas las auditorias deben integrar a la auditoria en tecnologías de información para efectuar revisiones específicas derivadas del uso de la tecnología de información en las empresas.

2.1.3 LOS SISTEMAS DE INFORMACIÓN

Para adentrarse en el proceso de una auditoria a las tecnologías de la información y comunicaciones, es requisito imprescindible comprender los conceptos de sistemas, información y tecnologías de las comunicaciones. Al logar una visión y conocimientos del entorno informático, el auditor juzgara, de manera suficiente, la naturaleza de la problemática y riesgos a los cuales se verá enfrentado al planificar y realizar la auditoria.

CARACTERISTICAS DE LOS SISTEMAS DE INFORMACION.

Si se tuviera que resumir con una sola frese, el principal objetivo de un sistema de información dentro de una organización, se podría afirmar que este se encarga de entregar la información oportuna y precisa, con la presentación y el formato adecuados a la persona que la necesita dentro de la organización, para tomar una decisión o realizar alguna operación y justo en el momento en que esta persona necesita disponer de dicha información.

Actualmente, la información debe ser considerada como uno de los recursos más valiosos de una organización y el sistema de información es el encargado de que esta sea gestionada siguiendo criterios de eficiencia y eficacia.

La información será útil para la organización, en la medida que facilite la toma de decisiones, por lo que ha de cumplir una serie de requisitos, entre los cuales cabe destacar:

- **Exactitud:** La información ha de ser precisa y libre de errores.
- **Completitud:** La información debe contener todos aquellos hechos que pudieran ser importantes.
- **Economicidad:** El costo en que se debe incurrir para obtener la información debería ser menor que el beneficio proporcionado por esta a la organización.
- **Confianza:** Para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes de información.
- **Relevancia:** La información ha de ser útil para la toma de decisiones. En este sentido, conviene evitar todos aquellos hechos que sean superfluos o que no aporten ningún valor.
- **Nivel de detalle:** La información debe presentar el nivel de detalle indicado a la decisión a que se destina. Se debe proporcionar con la presentación y el formato adecuados para que resulte sencilla y fácil de manejar.
- **Verificabilidad:** La información ha de poder ser contrastada y comprobada en todo momento.

Por otra parte, no se debe olvidar que el exceso de información también puede ser causa de problemas, suponiendo un obstáculo en vez de una ayuda para la toma de decisiones.

Asimismo, cada función y nivel organizativo tiene diferentes necesidades de información, afectando a los formatos, origen, periodicidad, nivel de información que sirven de soporte a las primeras.

En el componente redes, se analizan la descentralización de la organización, la distribución de los restantes componentes elementales en los lugares más útiles (oficinas, dependencias, delegaciones, etc.), así como la comunicación y coordinación entre dichos lugares.

Por último, el componente tecnología, hace referencia tanto al hardware como el software de un sistema de información. Se pone de manifiesto la existencia de una interrelación entre los elementos propios de la organización y los sistemas de información.

PROCESOS DE LOS SISTEMAS DE INFORMACION

Un sistema de información, se puede definir como un conjunto de elementos interrelacionados (entre los que se pueden considerar los distintos medios técnicos, las personas y los procedimientos), cuyo cometido es capturar datos, almacenarlos y transformarlos de manera adecuada y distribuir la información obtenida mediante este proceso.

Su propósito es apoyar y mejorar las operaciones cotidianas de la organización, así como satisfacer las necesidades de información, para la resolución de problemas y la toma de decisiones, por parte de los directivos de la organización. Por lo tanto, se trata de un sistema que tiene entradas (datos) y salidas (información), procesos de transformación de las entradas en salidas y mecanismos de retroalimentación.

La captura de datos puede ser manual o automatizada y, en general, es conveniente realizarla en el momento en que se produce el hecho al que está asociado.

En la etapa de proceso, se transforman los datos de entrada del sistema en información útil, mediante una serie de operaciones de cálculo, agregación, comparación, filtrado, presentación, etc. Estas operaciones, generalmente son realizadas con la ayuda de sistemas informáticos.

Agregación y otras características. A medida que se asciende en el escalafón organizacional, se observa como la información requerida aumenta en nivel de

agregación (menor nivel de detalle), incorpora información del entorno y hace un mayor énfasis en el mediano y largo plazo, a diferencia de la información puramente operativa, que normalmente se refiere a los hechos ocurridos dentro de la propia organización y a un corto plazo.

Es así como la información y el conocimiento que acumulan las organizaciones, deben ser consideradas como un recurso más, al mismo nivel que el capital, los bienes, las instalaciones o el personal.

En consecuencia, es necesario protegerlo y controlarlo adecuadamente, para que pueda contribuir a la realización de los objetivos y metas fijadas por la organización.

ESTRUCTURA DE LOS SISTEMAS DE INFORMACION

Los sistemas de información están compuestos por diferentes elementos que interaccionan entre sí, entre los cuales se pueden encontrar cinco componentes fundamentales: personas, actividades, datos, redes y tecnología.

Las personas engloban a los propietarios del sistema (entendiendo como tales, a aquellas personas que patrocinan y promueven el desarrollo de los sistemas de información), a los usuarios (directivos, ejecutivos medios, jefes de equipo, personal administrativo), a los diseñadores y a los desarrolladores.

Los datos constituyen la materia prima empleada para crear información útil.

Dentro de las actividades, se incluyen los procesos que se llevan a cabo en la organización y las actividades de procesamiento de datos y generación.

La información útil se plasma en una serie de documentos, informes y gráficos, para ser distribuida a las personas adecuadas dentro de la organización. Esta información, así como los datos de partida, se almacenan generalmente, en un soporte informático para poder ser reutilizados en cualquier momento.

La retroalimentación (feedback) de la información obtenida en todo este proceso, se puede utilizar para realizar ajustes y detectar posibles errores en la captura de los datos y/o en su transformación.

CLASIFICACION DE LOS SISTEMAS DE INFORMACION

Por lo general, las clasificaciones más extendidas de los sistemas de información suelen agrupar estos en función de su propósito. De una forma muy global, puede considerarse que existen dos propósitos básicos para los sistemas.

- **Soporte a las actividades operativas:** Que da lugar a sistemas de información para actividades más estructuradas (aplicaciones contables, ventas, adquisiciones y, en general, lo que se denomina "gestión empresarial" o también sistemas que permiten el manejo de información menos estructurada: aplicaciones ofimáticas, programas técnicos para funciones de ingeniería, etc.
- **Soporte a las decisiones y el control de gestión:** Que puede proporcionarse desde las propias aplicaciones de gestión empresarial (mediante salidas de información existentes) o a través de aplicaciones específicas.

Los sistemas de soporte a las actividades operativas, surgen para automatizar actividades operacionales intensivas en el manejo de datos. Concretamente, se centran en áreas como administración (contabilidad y facturación) y gestión de personal, extendiéndose a otras actividades como la venta, la compra o la producción. Estos permiten recoger los datos básicos en los datos básicos en las operaciones y se les denomina sistema de procesamiento transaccional.

Actualmente, estos sistemas forman parte de lo que normalmente las organizaciones denominan como su "Sistema de Gestión Empresarial" o ERP (Enterprise Resource Planning).

Los sistemas de información para la toma de decisiones, permiten sacar provecho a los datos recogidos por los sistemas transaccionales, siendo capaces de proporcionar información para la gestión. Estos sistemas, permiten

generar informes para los directivos de la organización, con el propósito de mejorar el control de gestión de las distintas áreas funcionales. De este modo, se consigue agilizar el proceso de toma de decisiones, al proporcionar la información necesaria de forma rápida, precisa y fiable.

En los sistemas de información de control de gestión, los informes pueden ser generados de forma periódica, bajo demanda, en el momento en que se produzca una situación excepcional (posibilitando este último caso el control de excepción) y en ellos se comparan, para cada área funcional o centro de responsabilidad, los objetivos previstos con los resultados obtenidos, fruto de las distintas operaciones realizadas.

La dirección de una organización, además, requiere sistemas capaces de soportar decisiones de carácter menos estructurado, con frecuencia el directivo necesitara herramientas para diagnosticar un problema (análisis) y para elegir la mejor alternativa (simulación, planificación, etc.). Este tipo de herramientas se les denomina sistemas de “inteligencia de negocios”.

Los sistemas de soporte a la dirección son los que asisten a los directivos de las organizaciones en todos los aspectos de un proceso de toma de decisiones: generación de alternativas, análisis de ellas, simulación de resultados que se obtendrán con cada una de ellas, etc. Se puede afirmar que estos sistemas van un paso más allá que los sistemas de información tradicionales.

Por último, los sistemas de información para ejecutivos, combinan buena parte de las características de los sistemas anteriores, para servir de ayuda a los directivos en el proceso de toma de decisión y seguimiento de acciones.

2.2.4 COBIT 4.1

DEFINICION

COBIT es un acrónimo formado por las siglas derivadas de Control Objetives for Information and Related Technology (Objetivos de Control para la Información y Tecnologías Relacionadas)

Este conjunto de objetivos representa el producto de un proyecto de investigación desarrollado por la Information System Audit and Control Fundation (ISACF) que fue publicado inicialmente en el año de 1996.

Como su nombre lo indica, COBIT es un conjunto de objetivos de control aplicables a un ambiente de tecnologías de información que lograran definirse gracias a un trabajo de investigación y búsqueda de consenso entre la normatividad de distintos cuerpos colegiados, estándares técnicos, códigos de conducta, prácticas y requerimientos de la industria y requerimientos emergentes para industrias especificas (desde la banca hasta la manufactura). Este extenso trabajo de investigación realizado por equipos de expertos de América, Europa y Oceanía, dio como resultado un grupo estructurado de objetivos de control que la ser compatibles con las principales normas a nivel internacional, cuenta con una aceptación implícita como un estándar global en términos de control interno en tecnologías de información.

MISION

La misión de COBIT es: “investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnologías de información generalmente aceptados por el uso cotidiano de gerentes de organizaciones y auditores”.

Entonces, el propósito de COBIT se fundamenta en la idea de que los recursos de TI deben ser utilizados en forma adecuada mediante la ejecución de procesos de trabajo para satisfacer los requerimientos de (información del) negocio que existen en las organizaciones.

RECURSOS DE TI

La clasificación que propone COBIT sobre los recursos de tecnología de información es la siguiente:

- **Datos:** Incluye a los objetivos de información en su sentido más amplio, considerando información interna y externa, estructurada y no estructurada, grafica, sonidos, etc.
- **Sistemas de información:** Este concepto se entiende como los sistemas de información (aplicaciones) que integran tanto procedimientos manuales como procedimientos programados (basados en tecnología)
- **Tecnología:** Incluye hardware, sistemas operativos, sistemas de administración de base de datos, equipos de redes y telecomunicaciones, video conferencia, etc.
- **Instalaciones:** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- Recursos Humanos: Este concepto incluye, habilidades, conciencia y productividad del personal para planear, adquirir, prestar servicios, proporcionar soporte y monitorear los sistemas y servicios de información.

PROCESOS DE TRABAJO

COBIT clasifica los procesos de trabajo en tres niveles jerárquicos, dominios, procesos y actividades o tareas.

Los cuatro dominios definidos se estructuran de acuerdo con el esquema que se utiliza para representar el ciclo de vida de administración de recursos:

- Planeación y organización: Planning and organization (PO)
- Adquisición e implementación: Acquisition and implementation (AI)
- Entrega de servicios y soporte: Delivery and support (DS)
- Monitoreo: Monitoring (M)

Estos dominios a su vez se subdividen en procesos:

1. **Planeación y Organización (PO)**
   - PO1: Definir un plan estratégico de sistemas.
   - PO2: Definir la arquitectura de información.
   - PO3: Determinar la dirección tecnológica.
   - PO4: Definir la organización y sus relaciones.
   - PO5: Administrar las inversiones en TI.
   - PO6: Comunicar la dirección y objetivos de la gerencia.
   - PO7: Administrar los recursos humanos.
   - PO8: Asegurar el apego a disposiciones externas.
   - PO9: Evaluar riesgos.
   - PO10: Administrar proyectos.
   - PO 11: Administrar calidad.

2. **Adquisición e Implementación (AI)**

   AI1: Identificar soluciones de automatización.

   AI2: Adquirir y mantener software de aplicaciones.

   AI3: Adquirir y mantener la arquitectura tecnológica.

   AI4: Desarrollar y mantener procedimientos.

AI5: Instalar y acreditar sistemas de información.

AI6: Administrar cambios.

3. Prestación de Servicios y Soporte (DS)

DS1: Definir niveles de servicio.

DS2: Administrar servicios de terceros.

DS3: Administrar desempeño y capacidad

DS4: Asegurar la continuidad de servicio.

DS5: Garantizar la seguridad de sistemas.

DS6: Identificar y asignar costos.

DS7: Educar y capacitar usuarios.

DS8: Apoyar y orientar a clientes.

DS9: Administrar la configuración.

DS10: Administrar problemas e incidentes.

DS11: Administrar la información.

DS12: Administrar las instalaciones.

DS13: Administrar la operación.

4. Monitoreo (M)

M1: Monitorear el proceso

M2: Evaluar lo adecuado del control interno.

M3: Obtener aseguramiento independiente.

M4: Proporcionar auditoría independiente.

Posteriormente y como producto de un análisis más profundo, COBIT define las actividades o tareas en que se descompone cada uno de los 34 procesos e identifica los objetivos de control que deben existir en cada uno de ellos, tal como se muestra en el siguiente ejemplo:

DS.	Prestación de servicios y soporte (dominio)
DS2.	Administrar servicios de terceros (proceso)
2.3.	Contrato con terceros (actividad o tarea)

Objetivo de Control: “La Gerencia debe definir procedimientos específicos para asegurar que un contrato formal es definido y acordado para cada relación de servicios con un proveedor”.

REQUERIMIENTO DE NEGOCIO

Por lo que respecta a requerimiento de negocio COBIT, se orienta en forma exclusiva a requisitos relacionados con la información. En un primer análisis presenta la siguiente clasificación.

- **Requerimiento de calidad:**
  - Calidad.
  - Costo.
  - Prestación de servicio.
- **Requerimiento de confianza:**
  - Efectividad y confianza de operaciones.
  - Confiabilidad de la información.
  - Cumplimiento de leyes y regulaciones.
- **Requerimiento de seguridad de la información:**
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.

De acuerdo con esta clasificación preliminar y mediante un análisis de los conceptos que integra y de las áreas comunes de interés que se presentan entre los mismos, COBIT resume los requerimientos (de información) del negocio en las siguientes categorías:

- **Efectividad:** Se refiere a que la información debe ser relevante y pertinente para los procesos de negocia si como ser proporcionada en forma oportuna, correcta, consistente y utilizable.
- **Eficiencia:** Se refiere a proveer la información mediante el empleo optimo (la forma más productiva y económica impuestas en forma externa) de los recursos.

- **Confidencialidad:** Se refiere a la protección de la información sensitiva contra la divulgación no autorizada.
- **Integridad:** Se refiere a lo exacto y completo de la información así como a su validez de acuerdo a los valores y expectativas de la organización.
- Disponibilidad: Se refiere a la accesibilidad de la información cuando sea requerida por los procesos de negocio ahora y en el futuro. También se relaciona con la salvaguardia de los recursos necesarios y las capacidades asociadas a los mismos.
- **Cumplimiento:** Se refiere al cumplimiento de leyes, regulaciones y compromisos contractuales a los cuales está comprometida la organización, por ejemplo, criterios de negocio.
- **Confiabilidad de la información:** Se refiere a proveer la información apropiada para que la administración opere la organización y cumpla con sus responsabilidades de informes financieros y de cumplimiento normativo.

Los 34 procesos de TI definidos por COBIT esta orientado a la satisfacción de un rerquisito de negocio especifico, de acuerdo a la siguiente tabla:

PROCESOS COBIT Y SUS REQUISITOS DE NEGOCIO

PROCESOS COBIT DE TI	REQUISITOS DE NEGOCIO
PLANEACION Y ORGANIZACIÓN (PO)	
PO1: Definir un plan estratégico de sistemas	Obtener un balance óptimo de oportunidades en tecnología de información y requerimientos de negocio de TI, así como asegurar su logro futuro.
PO2: Definir la arquitectura de información.	Organizar adecuadamente los sistemas de información.
PO3: Determinar la dirección tecnológica.	Obtener beneficio de la tecnología existente y de la tecnología emergente.
PO4: Definir la organización y sus relaciones.	Proporcionar servicios de tecnología de información.
PO5: Administrar las inversiones en TI.	Asegurar la obtención de fondos y controlar el empleo de los recursos financieros.

PO6: Comunicar la dirección de la gerencia.	Asegurar la concientización de los usuarios y su entendimiento de las aspiraciones de la dirección.
PO7: Administrar los recursos Humanos.	Maximizar las contribuciones del personal a los procesos de TI.
PO8: Asegurar el apego a disposiciones externas.	Observar el cumplimiento de obligaciones legales, regulatorias y contractuales.
PO9: Evaluar riesgos.	Asegurar el cumplimiento de los objetivos de TI y la respuesta a amenazas a la prestación de servicio de TI.
PO10: Administrar proyectos.	Establecer prioridades y cumplir compromisos en tiempo y en costo.
PO11: Administrar calidad.	Satisfacer los requerimientos de los clientes de TI.
ADQUISICION E IMPLEMENTACION (AI)	
AI1. Identificar soluciones de automatización.	Asegurar el mejor enfoque para satisfacer los requerimientos del usuario.
AI2. Adquirir y mantener software de aplicación.	Proveer funciones automatizadas que efectivamente soporten los procesos de negocio.
AI3. Adquirir y mantener la arquitectura tecnológica.	Proveer la plataforma adecuada para proporcionar soporte a las aplicaciones de negocio.
AI4. Desarrollar y mantener procedimientos.	Asegurar el uso apropiado de las aplicaciones y de las soluciones de tecnología existentes.
AI5. Instalar y acreditar sistemas de información.	Verificar y confirmar que la solución corresponda al propósito pretendido.
AI6. Administrar cambios.	Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.
PRESTACION DE SERVICIO Y SOPORTE (DS)	
DS1. Definir niveles de servicio.	Establecer un entendimiento común del nivel de servicio requerido.
DS2. Administrar servicio de terceros.	Asegurar que los roles y responsabilidades de terceros están definidas claramente, son respetados y continúan satisfaciendo los requerimientos.
DS3. Administrar desempeño y capacidad.	Asegurar que la capacidad adecuada se encuentra disponible y se hace el mejor y optimo uso de la misma para satisfacer los requerimientos de desempeño.
DS4. Asegurar continuidad de servicio.	Contar con servicios disponibles de acuerdo con los requerimientos y mantener la prestación de los mismos en caso de una interrupción.

DS5. Garantizar la seguridad de sistemas.	Salvaguardar información contra uso no autorizado, divulgación o modificación, daño o pérdida.
DS6. Identificar y asignar costos.	Asegurar una concientización correcta de los costos atribuibles a servicios de TI.
DS7. Educar y capacitar usuarios.	Asegurar que los usuarios estén haciendo uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucradas.
DS8. Apoyar y orientar a clientes.	Asegurar que cualquier problema experimentado por los usuarios es manejado apropiadamente.
DS9. Administrar la configuración.	Dar razón de todos los componentes. Prevenir alteraciones no autorizadas, confirmar existencia física y proveer las bases para una sólida administración de cambios.
DS10. Administrar problemas e incidentes.	Asegurar que problemas e incidentes son resueltos y que las causas son investigadas para prevenir cualquier ocurrencia futura.
DS11. Administrar la información.	Asegurar que la información se mantiene completa, exacta y valida durante su entrada, actualización y almacenamiento.
DS12. Administrar las instalaciones.	Proporcionar una ubicación física conveniente que proteja al equipo y a las personas contra riesgos naturales y riesgos producidos por el hombre.
DS13. Administrar la operación.	Asegurar que las funciones importantes de TI son desarrolladas regularmente y en una forma ordenada.
MONITOREO (M)	
M1. Monitorear el proceso.	Asegurar el cumplimiento de los objetivos de desempeño establecidos para los procesos de TI.
M2. Evaluar lo adecuado del control interno.	Asegurar el logro de los objetivos de control interno establecidos para los procesos de TI.
M3. Obtener aseguramiento independiente.	Incrementar los niveles de confianza y beneficiarse con recomendaciones sobre mejores prácticas.
M4. Obtener auditoría independiente.	Incrementar la confianza y confiabilidad entre la organización, clientes y proveedores.

2.2.5 ISO / IEC 27002

Definición y objetivos.

El objetivo del estándar ISO/IEC 27002: 2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información.

En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios.

- La política de seguridad
- Organización para la seguridad de la información.
- Gestión de activos de información.
- Seguridad del personal.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de la seguridad de la información
- Gestión de la continuidad del negocio.
- Cumplimiento.

Los principios rectores en la norma ISO/IEC 27002 son los puntos de partida para la implementación de seguridad de la información. Se basan en los requisitos legales o en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en los requisitos legales son:

- La protección y la no divulgación de datos personales.
- Protección de la información interna.
- Protección de los derechos de propiedad intelectual.

as mejores prácticas mencionadas en la norma incluyen:

- La política de seguridad de la información.
- Asignación de la responsabilidad de seguridad de la información.
- Escalamiento de problemas.
- Gestión de la continuidad del negocio.

3. ENFOQUE METODOLÓGICO

El enfoque metodológico propuesto integra el conocimiento aportado por las organizaciones que lideran el desarrollo de los estándares y mejores prácticas en el ámbito de las tecnologías de la información reconocidas a nivel internacional, entregando un marco referencial para realizar auditorías a las tecnologías de información centradas en los procesos del negocio, los sistemas de información que los soportan y sus actividades de control.

3.1 METODOLOGÍA

Esta constituye una herramienta de apoyo que permite incorporar el uso del estándar COBIT y la norma técnica ISO/IEC 27002 a los programas de auditorías a las tecnologías de información y comunicaciones.

A continuación, se presentan las etapas que componen la metodología.

FASE I. Planificación de la auditoria.

1. Plan de auditoria preliminar.
2. Comprensión de la organización, procesos de negocio y sistemas.
3. Definición del programa y alcance de la auditoria.

FASE II. Ejecución de la auditoria.

4. Evaluación del control interno.
5. Diseño de las pruebas de auditoria.
6. Ejecución de las pruebas de auditoria.
7. Evaluación del resultado de las pruebas de auditoria.

FASE III. Comunicación de los resultados.

8. Elaboración del informe con los resultados de la auditoria
9. Seguimiento a las observaciones de la auditoria.

SINTESIS DE ACTIVIDADES Y PRODUCTOS ENTREGABLES POR ETAPAS

A continuación, se presenta un resumen de las actividades y productos que componen las etapas a cumplir para realizar una auditoría a las tecnologías de información y comunicaciones.

RESUMEN DE ACTIVIDADES Y PRODUCTOS DE LA METODOLOGÍA

ETAPAS DE LA METODOLOGÍA		ACTIVIDADES QUE SE EJECUTAN	PRODUCTOS DE LA ETAPA
N°	DESCRIPCION		
1	**Plan de auditoria preliminar.**	• Elaborar un plan de auditoria con objetivos generales. • Conformar el grupo de trabajo que realizara la auditoria. • Estimar tiempo necesario para realizar la auditoria.	• Plan de auditoria preliminar. • Definición del perfil del personal requerido y asignación de auditores. • Lista con horas estimadas por etapa para realizar la auditoria.
2	**Comprensión de la organización, procesos de negocio y sistemas.**	• Levantamiento de información sobre el estado actual y características de la organización, infraestructura, recursos humanos y técnicos, procesos de negocios y sistemas de información que los soportan. • Confeccionar flujograma de los procesos de negocio. • Realizar ficha técnica de los sistemas de información que soportan los procesos de negocio.	• Archivos de trabajo de la auditoria. • Documentos con definición de los procesos de negocio y diagramas descriptivos. • Ficha técnica de los sistemas de información que soportan los procesos de negocio.
3	**Definición del programa y alcance de la auditoria.**	• Seleccionar los objetivos de control aplicables a los procesos de negocio y sistemas de información. • Elaborar el programa de auditoria detallado. • Confeccionar Carta Gantt del programa de auditoria.	• Lista de objetivos de control que deben ser satisfechos por los procesos de negocio y sistemas de información. • Programa de auditoria detallado. • Carta Gantt del programa de auditoria.
4	**Definición del sistema de control interno.**	• Identificar y documentar los controles existentes en los procesos de negocio y sistemas de información. • Evaluar el diseño y grado de protección que ofrecen los controles existentes. • Identificar y documentar los controles deficientes.	• Lista de controles existentes para los procesos de negocio y sistemas de información. • Lista con el grado de protección de controles existentes para los procesos de negocio y los sistemas.

5	**Definición y diseño de las pruebas de auditoria.**	• Definir y diseñar pruebas de cumplimiento para los controles claves de los procesos de negocio y sistemas agrupados por técnicas de verificación. • Definir el diseño y alcance de las pruebas sustantivas para datos clave de los procesos y sistemas. .	• Lista de deficiencias y debilidades de control interno. • Definición del alcance de las pruebas de cumplimiento. • Diseño detallado de las pruebas de cumplimiento según técnica de verificación. • Definición del alcance de las pruebas sustantivas. • Diseño detallado de las pruebas sustantivas.
6	**Ejecución de las pruebas de auditoria.**	• Ejecutar pruebas de cumplimiento y sustantivas utilizando técnicas de verificación manuales o asistidas por computador.	• Lista de controles verificados por el auditor. • Soportes de las pruebas de auditoria realizadas.
7	**Evaluación de los resultados obtenidos en las pruebas de auditoria.**	• Evaluar los resultados de las pruebas efectuadas. • Desarrollar el análisis de las observaciones de auditoria y puntos mejorables par los controles y datos deficientes. • Identificar las causas, el impacto y las implicaciones de las observación para la organización y verificar los estándares y mejores prácticas que no se cumplen. • Diseñar las conclusiones de auditoria para los resultados no satisfactorios.	• Listado con análisis de observaciones de auditoria para pruebas de cumplimiento y sustantivas. • Conclusiones de los resultados obtenidos.
8	**Elaboración del informe con los resultados de la auditoria.**	• Elaborar resumen de observaciones. • Desarrollar y aprobar informe preliminar. • Emitir informe preliminar. • Analizar respuesta del servicio al informe preliminar. • Diseñar conclusiones generales y específicas de la auditoria. • Elaborar y aprobar informe final de auditoria. • Emitir informe final de auditoria. • Organizar y cerrar expediente y archivo con hojas de trabajo.	• Resumen de observaciones obtenidas. • Informe preliminar de auditoria. • Documento con el análisis de las respuestas emitidas por el servicio auditado al informe preliminar. • Informe final de auditoria. • Expediente de auditoria con observaciones organizadas y referenciadas adecuadamente.
		• Planificar seguimiento al	• Programa de seguimiento.

9	**Seguimiento a las observaciones de auditoria.**	cumplimiento de las observaciones de auditoria. • Efectuar seguimiento en fechas programadas. • Analizar y evaluar resultados del seguimiento. • Elaborar y aprobar informe de seguimiento. • Emitir informe de seguimiento.	• Listado con el resultado del cumplimiento de las observaciones. • Informe de seguimiento.

3.2 FASE I. PLANIFICACIÓN DE LA AUDITORÍA

La primera fase de la auditoria comprende la realización de un plan de auditoria preliminar con el propósito de definir los objetivos de la auditoria, asignar los recursos y estimar el tiempo necesario para efectuar la revisión.

Plan de auditoria preliminar

Como resultado de esta actividad se realiza el programa de trabajo para la auditoria, el que debe incluir:

- Objetivos de la auditoria.
- Definición del equipo de auditores requerido: perfil y habilidades.
- Tiempo estimado para efectuar la auditoria.

Programa de trabajo para el desarrollo de la auditoria.

Este documento consta de tres secciones:

- Objetivos de la auditoria. En esta sección se incluyen los objetivos de control generales que se buscan con la realización de la auditoria en tecnologías de la información.
- Alcance de la auditoria: En esta sección se definen los procesos de negocio y sistemas de información que serán revisados.
- Programación de actividades: Incluye la secuencia de pasos que deberán ejecutarse para desarrollar las etapas de la auditoria.

Asignación de recursos y estimación del tiempo requerido para efectuar la auditoria

Con base en la complejidad técnica de los procesos de negocio y sistema de información sujetos a auditoría y en el volumen de trabajo estimado para satisfacer los objetivos propuestos, es necesario definir las competencias necesarias del equipo de auditoría y estimar las necesidades de tiempo que se requerirán.

Suponga que se presupuestan 480 horas para todo el trabajo, las que podrían ser asignadas así: 15% para labores de supervisión, 20% para el auditor a cargo y el restante 65% para los auditores en terreno.

ASIGNACIÓN DE HORAS DE AUDITORÍA

No	NIVEL DE RESPONSABILIDAD	HORAS ASIGNADAS
1	Supervisor	72
2	Auditor a cargo	96
3	Auditores en terreno	312

Por cada una de las etapas de la metodología, un modelo de distribución de tiempo podría ser el siguiente:

ESTIMACION DE HORAS POR ETAPAS

No	ETAPAS DE LA METODOLOGIA	HORAS ESTIMADAS
1	Plan de auditoría preliminar	40
2	Comprensión del proceso de negocio	80

3	Definición del programa y su alcance	40
4	Evaluación del control interno	120
	Definición y diseño de las pruebas	80
6	Ejecución de las pruebas	40
7	Análisis de resultados de las pruebas	40
8	Elaboración informe con los resultados	40

Comprensión de los procesos de negocio y sistemas de información que los soportan

Esta etapa tiene como objetivos conocer y comprender el ambiente de organización, tecnológico y operativo de los procesos de negocio y los sistemas de información que los soportan. Implica para el auditor, realizar un levantamiento de la información detallada a través de entrevistas con las personas apropiadas, de observación de la forma como se ejecutan las operaciones y de la comprensión de la lógica del negocio, los flujos de información, el rol de las personas y dependencias que intervienen en el manejo de las operaciones y otros aspectos que el auditor considere importantes.

Cuando se realiza por primera vez la auditoría en un servicio, la información relevante obtenida en esta etapa se organiza en un documento conocido como archivo permanente o expediente continuo de auditoría. Si el archivo ya existe, es necesario su revisión y actualización con los cambios efectuados desde la última auditoría.

Este documento contiene información sobre los objetivos y procesos que soportan los sistemas de información y sobre los recursos de tecnología utilizados (instalaciones de procesamiento, infraestructura, personal, contratos, etc.) y la importancia relativa de las cifras que se procesan y otros datos de interés.

Levantamiento de la información básica y detallada

El levantamiento de información que se realiza en esta etapa, tiene como finalidad asegurar que el auditor comprenda la filosofía y las características de funcionamiento de los procesos de negocio y sistemas de información en estudio. Esto es imperativo dentro del proceso de la auditoría, puesto que toda la pericia y el conocimiento técnico del auditor serían inaplicables si antes no obtiene la comprensión de aspectos claves del universo que será auditado.

Como resultado de esta actividad, el auditor obtiene la siguiente información:

a) De los procesos de negocio

- Estructura organizacional
- Estructura de las áreas propietarias de la información de los procesos de negocio
- Clientes interno y externos
- Dependencias de la organización
- Tareas o actividades que realiza cada dependencia
- Terceros que intervienen en el manejo de la información
- Cuantificación de las cifras de operaciones que manejan los procesos de negocio (promedio durante un año)
- Políticas y procedimientos establecidos en la organización relacionados con los procesos de negocio
- .Normas legales e institucionales que rigen el funcionamiento del servicio
- Información sobre fraudes y otros antecedentes en las operaciones del servicio

b) De las tecnologías de información que soportan los procesos de negocio

- Funciones y operaciones del negocio que ejecutan los sistemas Modelo entidad/relación de las bases de datos de los sistemas
- Diccionario de datos de los modelos entidad/relación
- Inventario de documentos fuentes y otros medios de entrada de datos
- Personas claves que dan soporte técnico a la operación y mantención de los sistemas para cada dependencia.
- Terceros que prestan servicios de tecnologías de información para los procesos de negocio.
- Inventario de informes que producen los sistemas y destinatarios de los mismos
- Interfaces entre sistemas (información que reciben o proporcionan a otros sistemas)
- Manuales existentes con la documentación técnica y del usuario
- Plataforma en la que funcionan los sistemas de información (sistema operativo, software de desarrollo y motor de base de datos utilizados)
- Si el sistema de información fue adquirido; datos del proveedor, año de adquisición, versión en producción, cantidad de usuarios con licencia, poseen programas fuentes y contrato de mantención)
- Si el sistema de información fue desarrollado internamente (tipo de lenguaje utilizado, archivos fuentes y ejecutables, fecha de ingreso a producción, versión actual en producción).

Estructura y organización de los archivos de trabajo

Con la información obtenida en esta etapa se organiza el primero de dos archivos de trabajo de la auditoría, el "archivo permanente o expediente continuo de auditoría", que contiene la información que representa el estado actual del área objeto de auditoría. El otro archivo se denomina "archivo de

hojas de trabajo" y se construye con los resultados de cada una de las etapas de la metodología,

a) Archivo permanente

Es el archivo con los antecedentes que reflejan el estado de organización y funcionamiento de los procesos y sistemas auditados en una entidad.

Este archivo contiene información de la organización que es poco cambiante y, por consiguiente, tiene validez continua a través del tiempo. Generalmente, se elabora completamente en la primera auditoría y en las demás se reemplazan unos documentos por otros actualizados.

b) Archivo de hojas de trabajo

Es el archivo con las hojas de trabajo que contienen las evidencias del desarrollo de cada una de las etapas de la auditoría.

Los documentos de este archivo tienen validez por una sola vez, es decir, para cada auditoría realizada a las aplicaciones que están en proceso de evaluación. Por consiguiente, cada vez que se efectúe una auditoría se debe elaborar un nuevo archivo con la información recopilada.

Ficha técnica de los sistemas de información

La ficha técnica es un documento con el resumen gerencial de las principales características del proceso de negocio y de las tecnologías de información que soportan sus operaciones.

El objetivo principal de este documento es ubicar a los destinatarios de los informes de auditoría, proporcionándoles información que sirva de referencia para evaluar la importancia de las observaciones y conclusiones que se presentan en el informe de auditoría.

El contenido de la ficha técnica es un resumen del archivo permanente de los procesos de negocio y los sistemas de información que los soportan.

Definición del alcance de la auditoría

El objetivo de esta etapa es identificar, analizar y seleccionar los objetivos de control aplicables a los procesos de negocio y sistemas de información sujetos a auditoría. Estos objetivos de control serán incorporados al programa de auditoría detallado.

De esta etapa se obtiene lo siguiente:

- Programa de auditoría con objetivos detallados
- Carta Gantt de la auditoría
- Lista con la definición y análisis de los objetivos de control aplicables a los procesos del negocio y sistemas de información auditados.

Selección de los objetivos de control aplicables

En este paso de la metodología se deben seleccionar los objetivos de control que sean aplicables a la auditoría de los procesos de negocio y sistemas de información en revisión.

Para agrupar de forma más comprensiva los controles que proporcionan COBIT e ISO/IEC 27002, podemos recurrir a los objetivos de control básicos que define la Asociación de Auditores de Sistemas de Información y Control (ISACA) para realizar una revisión y evaluación de los sistemas de información.

1. Estrategia y dirección
2. Organización general
3. Acceso a los recursos de información
4. Metodología de desarrollo de sistemas y control de cambios 5, Procedimientos de operaciones
5. Programación de sistemas y funciones de soporte técnico
6. Procedimientos de aseguramiento de calidad
7. Controles de acceso físico
8. Planificación de la continuidad del negocio y recuperación de desastres
9. Redes y comunicaciones

10. Administración de la base de datos
11. Protección y mecanismos de detección contra ataques internos y externos

En la etapa "evaluación del sistema de control", se debe analizar si los controles establecidos por la administración se encuentran alineados con los objetivos de control seleccionados de los estándares. Posteriormente, en la etapa "Ejecución de pruebas de auditoría", se debe verificar si la protección de los controles es suficiente para asegurar razonablemente el cumplimiento de los objetivos del negocio.

OBJETIVOS DE CONTROL COBIT e ISO/IEC 27002

A continuación, se presenta la lista con la descripción de los objetivos de control COBIT e ISO/IEC 27002 que son aplicables a cada objetivo de control básico.

1. ESTRATEGIA Y DIRECCIÓN

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
P01.2 Alineación de TI con el negocio	
P01.4 Plan estratégico de TI	
P02.1 Modelo de arquitectura de información empresarial	
P03.1 Planeamiento de *la* orientación	
P03.2 Plan de infraestructura tecnológica	
P03.4 Estándares tecnológicos	
PO4.2 Comité estratégico de TI	
PO4.3 Comité directivo de TI	
P06.5 Comunicación de los objetivos y de la dirección de TI	

2. ORGANIZACIÓN GENERAL

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
PO4.4 Ubicación organizacional de la función de TI	
PO4.5 Estructura organizacional de Ti	
PO4.6 Establecer roles y responsabilidades	
PO4.7 Responsabilidades para el aseguramiento de la calidad de TI (QA)	
PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	
PO4.10 Supervisión	
PO4.11 Segregación de funciones	
PO4.12 Personal de TI	
PO4.13 Personal clave de TI	
P06.4 Implantación de políticas, estándares y procedimientos	

3. ACCESO A LOS RECURSOS DE INFORMACIÓN

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
P02.3 Esquema de clasificación de datos P06.2 Riesgo corporativo y marco de referencia del control interno de TI	11.1.1 Políticas de control de acceso
DS5.4 Gestión de cuentas de usuario D55.3 Gestión de identidad	11.2.1 Registro de usuarios
	11.2.2 Gestión de privilegios
	11.2.4 Revisión de derechos de acceso de
	11.2.3 Gestión de contraseñas de
	11.3.1 Uso de contraseñas
	11.5.1 Procedimientos seguros de inicio de sesión 11.6.1 Restricción de
DS5,9 Prevención, detección y corrección de software malicioso	11.4.2 Autenticación de usuario para conexiones externas
DS5.11 Intercambio de datos sensitivos DS9.2 Identificación y mantenimiento de elementos de la configuración	11.4.3 identificación de equipos en redes

4. METODOLOGÍA DE DESARROLLO DE SISTEMAS Y CONTROL DE CAMBIOS

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
AI2.1 Diseño a alto nivel	
AI2.2 Diseño detallado	
AI2.7 Desarrollo de software aplicativo	10.1.4 Separación de los entornos de desarrollo, pruebas y producción
AI2.9 Gestión de los requisitos de las aplicaciones	
AI2.10 Mantenimiento del software aplicativo	
AI2.8 Aseguramiento de la calidad del software A17.2 Plan de pruebas	
A17.3 Plan de implementación	
A17.4 Ambiente de prueba	
A17.5 Conversión de datos y sistemas	
A17.6 Pruebas de cambios	
AI7.7 Pruebas de aceptación final	10.3.2 Aceptación del sistema
AI7.8 Promoción a producción	
AI7.9 Revisión posterior a la Implementación	
AI6.1 Estándares y procedimientos para cambios	10,1,2 Gestión de cambios 12.5.1 Procedimientos de control de cambios 12,53 Restricciones en los cambios a los paquetes de software
AI6.2 Evaluación de impacto, priorizacIón y autorización	
AI6.4 Seguimiento y reporte de estado de los cambios	
AI6.5 Cierre y documentación del cambio	
AI6.3 Cambios de emergencia	

5.- PROCEDIMIENTOS DE OPERACIONES

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
AI4 Facilitar la operación y el uso D513 Gestionar las operaciones	10.1.1 Procedimientos operativos documentados
AI7 Instalar y acreditar soluciones y cambios	10,1.4 Separación de los entornos de desarrollo, pruebas y producción
DS1 Definir y gestionar los niveles de servicio DS2 Gestionar los servicios de terceros	10.2.1 Entrega de servicios
DS2 Gestionar los servicios de terceros	10,2.2 Monitore° y revisión de los servicios de terceros
	10.2.3 Gestión de cambios a los servicios de terceros
	10.3.1 Gestión de la Capacidad
DS11 Gestionar datos	10.5.1 Respaldo de la información
	10.7.2 Eliminación de medios de almacenamiento
ME1 Monitorear y evaluar el desempeño de TI	10.10.2 Monitoreo del uso de los sistemas
DS5 Garantizar la seguridad de los sistemas	10.10.4 Loqs de administrador y de operador
	10.10.5 logs de errores

6.- PROGRAMACIÓN DE SISTEMAS Y SOPORTE TÉCNICO

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
DS1.3 Acuerdos de niveles de servicio	
DS8.1 Mesa de servicios	10.2,1 Entrega de servicios
DS8.2 Registro de consultas de clientes	
DS10.3 Cierre de problemas	

7.- PROCEDIMIENTOS DE ASEGURAMIENTO DE CALIDAD

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
PO4.7 Responsabilidades para el aseguramiento de la calidad de TI (IDA)	
P08.1 Sistema de administración de	
P08.2 Estándares y prácticas de calidad	
P08,5 Mejora continua	
P08.6 Medición, monitoreo y revisión de la calidad	

8. CONTROLES DE ACCESO FÍSICO

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
DS12.1 Selección y diseño del centro de datos 0512.2 Medidas de seguridad física	9.1.1 Perímetro de seguridad física
DS12.3 Acceso físico	9.1.2 Controles físicos de Ingreso
D512,4 Protección contra factores ambientales	9.1.4 Protección contra amenazas externas y ambientales
PO4.14 Políticas y procedimientos para personal contratado P06.2 Riesgo corporativo y marco de referencia para el control Interno de TI	9,1.6 Áreas de acceso público, despacho y recepción
DS5.7 Protección de la tecnología de seguridad	9,2.1 Ubicación y protección de los equipos
	9.2.3 Seguridad del cableado
AI3.3 Mantenimiento de la Infraestructura DS12.5 Gestión de instalaciones físicas DS13.5 Mantenimiento preventivo del hardware	9.2.4 Mantenimiento de equipos
DS11,4 Desechar	9.2.6 Eliminación o reutilización segura de equipos

9. PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN DE DESASTRES

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
DS4.1 Marco de trabajo de continuidad de TI	6.1.6 Relación con las autoridades 6.1,7 Relación con grupos de interés especial 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.4Marco de planificación
DS4.2 Planes de continuidad de TI	14.1.3 Desarrollar e Implementarpl información
DS4.4 Mantenimiento del plan de continuidad de TI	14.1.2 Continuidad del negocio y evaluación de riesgos
DS4.5 Pruebas del plan de continuidad de TI	14.1,5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
DS4.6 Entrenamiento en el plan de continuidad de TI	
DS4.7 Distribución del plan de continuidad de TI	
DS4.8 Recuperación y reanudación de servicios Ti	14,1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la Información
DS4.9 Almacenamiento externo de respaldos	10.5.1 Respaldo de la información
DS4.10 Revisión post-reanudación	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio

10. REDES Y COMUNICACIONES

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
	11.4.1 Políticas de uso de los servicios
DS9.2 Identificación y mantenimiento de elementos de la configuración	11.4.3 identificación de equipos en redes
	11.4.4 Protección de puertos de configuración y diagnóstico remoto
	11.4.5 Segregacion en redes
	11.4.6 Control de conexiones en la red
	11.4.7 Control de enrutamiento en la red
DS5 Garantizar la seguridad de los sistemas	10.6.1 Controles de red
	10.6.2 Seguridad de los servicios de red

11. ADMINISTRACIÓN DE LA BASE DE DATOS

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
P02.1 Modelo de arquitectura	
P02.2 Diccionario de datos	
PO4.9 Propiedad de los datos y sistemas	7.1.2 Propiedad de los activos de información

12. PROTECCIÓN Y MECANISMO DE DETECCIÓN CONTRA ATAQUES INTERNOS Y EXTERNOS

OBJETIVOS DE CONTROL APLICABLES	
COBIT	**ISO/IEC 27002**
DS5 Garantizar la seguridad de los sistemas D59.2 Identificación y mantenimiento de elementos de la configuración	12.6.1 Control de vulnerabilidades técnicas
D55.6 Definición de incidente de seguridad	13.1.1 Reporte eventos de seguridad de información
P09.3 Identificación de eventos	
	13,1.2 Reporte de debilidades de seguridad de información
	13.2.1 Responsabilidades y procedimientos
AI2.3 Control y auditabilidad de las aplicaciones	13.2.2 Aprendiendo de los incidentes de seguridad de información
058.3 Escalamiento de incidentes D58.4 Cierre de incidentes	13.2.3 Recolección de evidencia

3.3 FASE II. EJECUCIÓN DE LA AUDITORÍA

La segunda fase de la auditoría comprende un análisis del sistema de control interno de la organización con el objetivo de planificar y realizar las pruebas de cumplimiento y sustantivas que evaluarán si los controles operan de forma adecuada y cumplen con resguardan el cumplimiento de los objetivos y requisitos del negocio.

EVALUACION DEL SISTEMA DE CONTROL INTERNO

En esta etapa los auditores deben evaluar el sistema de control interno existente en los procesos de negocio y sistemas de información objeto de la auditoría, como base para determinar la naturaleza y extensión de las pruebas de auditoría que se requieran.

Evaluar el sistema de control interno significa: "determinar si los controles establecidos en los procesos de negocio y los sistemas de información, ofrecen la protección apropiada para reducir los riesgos a niveles aceptables para la organización".

El propósito de la evaluación de control interno, es determinar si es suficiente y efectiva para proteger a la organización, contra los riesgos que podrían afectarla en los procesos de negocio y sistemas de información que se están auditando. Esto es, evaluar la confiabilidad de los controles utilizados para prevenir o detectar y corregir las causas de los riesgos y minimizar el impacto que estos tendrían en caso de llegar a materializarse.

La evaluación del sistema de control interno produce resultados intermedios, de valor importante para las etapas restantes del proceso de auditoría, estos son:

1) El auditor fundamenta su opinión sobre la confiabilidad que ofrecen los controles utilizados, para reducir la probabilidad de ocurrencia o el impacto de los riesgos. Los resultados de esta evaluación sirven al

auditor como base para determinar la naturaleza y extensión de las pruebas de auditoría que se consideren necesarias y apropiadas a las circunstancias.

2) El auditor identifica y soporta debilidades y oportunidades de mejoramiento (observaciones de auditoría) en la estructura de los controles. Estas observaciones son insumos para el informe de auditoría.
3) El auditor identifica los controles que deberán verificarse en la etapa de ejecución de pruebas de auditoría, para determinar que realmente existen, están operando y son entendidos por las personas encargadas de ejecutarlos (pruebas de cumplimiento).
4) El auditor identifica los datos críticos y actividades sobre las cuales es necesario aplicar pruebas para verificar la exactitud y confiabilidad de los cálculos y de la información que producen los sistemas de información para apoyar el desarrollo de las operaciones del negocio (pruebas sustantivas).

S) El auditor documenta las observaciones de auditoría para los procesos de negocio y los sistemas de información que los soportan. Esta presenta las debilidades y deficiencias de control interno y seguridad identificadas en la evaluación de controles,

Levantamiento de controles por procesos de negocio y sistemas de información

El propósito de esta actividad es identificar y documentar los controles existentes por cada proceso de negocio y sistemas de información. Los soportes de este levantamiento de controles, generalmente son flujogramas o la descripción narrativa de las actividades que se desarrollan en cada proceso.

Criterios para evaluar la protección que ofrecen los controles

Para que los controles existentes ofrezcan el nivel de protección apropiado, deben satisfacer al menos dos de los tres criterios que se mencionan a continuación:

- Que exista la mezcla de los tres tipos de controles. Es decir, que la causa de riesgo tenga al menos un control de cada tipo (preventivo, detectivo y correctivo). EL incumplimiento de este criterio significa que los controles existentes para la causa de riesgo o amenaza contra la seguridad, no cumplen el principio de las tres barreras o anillos de seguridad recomendado por los expertos.
- Que la calificación promedio de los controles, según su clase, sea mayor o igual que 3.5. Las calificaciones para cada clase de control son:
- 5.0: Para controles automáticos no discrecionales
- 4.0: Para controles automáticos y discrecionales
- 3.0: Para controles manuales

  El incumplimiento de este criterio significa que la mayoría de los controles existentes no están automatizados y por consiguiente, la confiabilidad de los controles depende significativamente de las personas que los ejecutan y supervisan.

- Que la relación costo/beneficio sea razonable, Es decir, que el costo de los controles sea menor que el valor de las pérdidas que originaría la ocurrencia de la causa del riesgo. Los controles, para que sean apropiados, siempre deben ser menos costosos que el riesgo para el cual se establecen.

  Para estimar la razonabilidad de los costos de los controles, el auditor debe tener en cuenta lo siguiente:

  - Costo de adquisición del control
  - Costo de instalación del control
  - Costo de operación del control
  - Costo de mantenimiento del control

El incumplimiento de este criterio significa que la inversión en controles y seguridad está por encima del valor de las pérdidas que se pretende reducir con los controles. En este caso los costos de los controles exceden los beneficios que podrían obtenerse.

En forma cualitativa, se evalúa la efectividad de los controles existentes utilizando dos rangos de valoración: satisfactoria o insatisfactoria.

Evaluar la satisfacción de los objetivos de control

Al terminar el levantamiento de los controles de los procesos de negocios y sistemas de información que los soportan, se procede a evaluar la satisfacción de los objetivos de control identificados en la etapa anterior. Para este fin es necesario ejecutar las siguientes actividades:

1) Consultar la lista de los controles levantados indicando sus atributos (tipo y clase)
2) Distribuir los controles existentes entre los objetivos de control COBIT e 1SO 27002. Para este fin el auditor aplica su experiencia y criterio profesional para determinar la aplicabilidad de los controles a cada objetivo de control. Esto requiere del análisis cuidadoso del auditor
3) Evaluar el grado de satisfacción que ofrecen los controles asignados a cada objetivo de control
4) Resumir la evaluación de satisfacción de los objetivos de control

Observaciones de control interno

Las observaciones de auditoría en la evaluación de control interno, se refieren a desviaciones que se presentan respecto a los estándares de seguridad y control o a las normas internas de la organización. En la práctica, se refieren a debilidades o deficiencias que se detectan cuando los controles no satisfacen los criterios de evaluación antes mencionados.

Para los controles evaluados con efectividad inapropiada se generan una o más observaciones de auditoría. Las observaciones de auditoría se registran

y posteriormente se analizan y se desarrollan como se especifica a continuación.

Primero se describe la observación o desviación identificada respecto a los objetivos y estándares que identificó el auditor.

Luego, se presenta el estándar de comparación que no se cumple y que debería aplicarse para evitar o resolver el problema.

Posteriormente, se describe el impacto o perjuicios a que se expone la organización como consecuencia de la deficiencia o debilidad de control identificada.

Definición y diseño de las pruebas de auditoría

El objetivo de esta etapa es definir y diseñar los procedimientos de auditoría para obtener evidencia válida y suficiente de la operación de los controles existentes (pruebas de cumplimiento) y de la integridad de la información (pruebas sustantivas). Las pruebas pueden ser realizadas con procedimientos manuales o asistidas por computadora.

Estas pruebas se aplican sólo a los controles que en la evaluación de control interno presentaron un nivel de protección apropiado.

El auditor debe verificar que:

- Los controles identificados y evaluados en la etapa anterior están operando como se previó. Estas se denominan pruebas de cumplimiento.
- La información manejada, procesada o producida por el proceso de negocio o sistema de información, es exacta y confiable, es decir, refleja la realidad. Estas son las pruebas sustantivas.

De la ejecución de esta etapa se obtienen los siguientes productos:

- **Para pruebas de cumplimiento:** Por cada técnica de comprobación a emplear, un documento con las especificaciones de diseño de cada

prueba, indicando los controles a probar, el procedimiento y los recursos requeridos para ejecutar la prueba.

- **Para pruebas sustantivas:** Por cada técnica de comprobación a utilizar, un documento con las especificaciones de diseño de cada prueba, indicando los datos a verificar, el procedimiento y los recursos requeridos para ejecutar la prueba.

Identificación de controles claves que serán verificados

Las pruebas de cumplimiento y sustantivas no se aplican para todos los controles existentes, identificados y evaluados satisfactoriamente en la etapa anterior. Por razones de efectividad y eficiencia, es suficiente con probar solamente una muestra de controles seleccionados cuidadosamente, aplicando criterios que consulten su importancia para asegurar calidad, seguridad, cumplimiento con aspectos legales y confiabilidad de los procesos de negocio y sistemas de información sujetos a auditoría.

Tales controles se denominarán claves.

Un control clave se define como el control que es vital o de la mayor importancia para asegurar el correcto funcionamiento de los procesos, sistemas y las actividades del negocio sujetas a auditoría.

Los controles claves son aquellos que, a juicio del auditor, son indispensables para evitar o detectar y corregir el efecto o la probabilidad de ocurrencia de las causas de riesgo que generan riesgo alto. También, pueden considerarse claves aquellos controles que con mayor frecuencia actúan sobre varias causas de riesgo, es decir, tienen efecto múltiple. Se asume que entre mayor frecuencia tenga un control, mayor será su importancia y por consiguiente podrá ser considerado clave.

Otro criterio que podría emplear el auditor para seleccionar los controles clave es la clase de control. Por ejemplo, podría decidir seleccionar una muestra de controles automatizados y otra muestra de controles manuales.

Agrupamiento de controles por técnica de comprobación

Este método consiste en asignar individualmente las técnicas de comprobación a cada uno de los controles y posteriormente agruparlos bajo el nombre de ésta.

Los pasos a seguir para definir las pruebas de cumplimiento utilizando el método de agrupamiento de controles por técnica de comprobación son:

- Asignar la técnica de comprobación para cada control
- Agrupar los controles a verificar por técnica de comprobación
- Definir el alcance de las pruebas de cumplimiento
- Diseñar las pruebas de cumplimiento (diseño detallado) a ejecutar
- Planificar la ejecución de las pruebas de cumplimiento
- Ejecutar el plan de pruebas de cumplimiento

La aplicabilidad de cada técnica de comprobación depende de la naturaleza del control, por lo que el auditor debe analizar sus características y optar por la técnica que a su criterio permita la correcta ejecución y comprobación de las pruebas a realizar. En la siguiente etapa de la auditoría se detallan las técnicas y procedimientos de mayor aceptación para realizar las pruebas de cumplimiento y sustantivas en ambientes informáticos.

Definición y diseño de pruebas de cumplimiento

Las pruebas de cumplimiento tienen como objetivo comprobar (obtener evidencia) que los controles establecidos están implantados y que las personas encargadas de las operaciones los entienden, ejecutan y supervisan (monitorean) continuamente. Estas pruebas también son necesarias para evaluar si los procedimientos empleados satisfacen las políticas y procedimientos de la organización.

Para efectuar las pruebas de cumplimiento se utiliza una lista de comprobación de controles claves ordenados por técnica de comprobación para los procesos de negocio y sistemas de información auditados.

Este método de diseñar pruebas de cumplimiento consiste en asignar individualmente las técnicas de comprobación a cada uno de los controles claves y, posteriormente, agrupar bajo el nombre de cada técnica a todos los controles que serán verificados con ella. Entonces, se está en capacidad de planear detalladamente el uso de cada técnica de prueba considerando todos los controles que serán verificados con ella.

Los pasos a seguir para definir las pruebas utilizando este método se explican a continuación:

a) Asignar técnicas de verificación para cada control clave

En este primer paso se agrupan los controles claves que serán verificados y se escogen las técnicas de prueba a emplear. Una misma técnica puede ser asignada a diferentes controles.

b) Agrupar los controles clave a verificar por técnica de comprobación asignada

Realizar el agrupamiento de controles que utilicen la misma técnica de comprobación.

Al agrupar globalmente los controles por técnica de comprobación se debe tener presente que una misma técnica puede ser utilizada para verificar controles de distintos procesos de negocio o sistemas de información.

c) Definir el alcance de las pruebas por técnica de comprobación

El alcance de cada técnica de comprobación se puede definir globalmente para todo el proceso de negocio y sistema de información que lo soporta, el que incluye los siguientes aspectos a considerar:

- Los controles a probar con la técnica de comprobación
- Los criterios de la información de negocio impactados por los controles a probar
- Los recursos de tecnología que son impactados por los controles a probar

d) Diseño detallado de las pruebas de auditoría a ejecutar

El diseño detallado implica determinar los recursos necesarios (infraestructura, datos y personal), el procedimiento a emplear y los responsables de ejecutarlos.

e) Planificar la ejecución de las pruebas

El objetivo de este paso es planificar y coordinar con el personal de sistemas y de las áreas de negocio la ejecución de las pruebas de auclitoría (manual y asistida por computador) en el lugar de trabajo.

Como factor crítico de éxito de las pruebas de auditoría, es necesario programar su ejecución considerando la disponibilidad de los recursos necesarios para aplicarlas, el sitio de ejecución, los auditores asignados para ejecutarlas y la periodicidad de ejecución.

Para este fin se elabora un cronograma de pruebas, considerando las fechas que sean más oportunas, especialmente cuando para su ejecución se requieran equipos de procesamiento que no son administrados por la auditoría y la colaboración del personal de sistemas.

Definición y diseño de las pruebas sustantivas

Las pruebas sustantivas tienen como objetivo verificar (obtener evidencia) la integridad de la información y se aplican sobre datos críticos que representan saldos de activos o de pasivos o, gastos importantes en las operaciones del negocio objeto de la auditoría. Esta información comúnmente reside en bases de datos y, son producto de cálculos efectuados por el sistema de información que soporta la operación del negocio.

El objetivo de esta actividad es asignar individualmente las técnicas de prueba a cada uno de los datos claves que serán verificados, sólo entonces se está en capacidad de planear detalladamente el uso de cada técnica de prueba.

Los pasos a seguir por el auditor son:

a) Agrupar los datos clave a verificar por técnica de comprobación asignada

Se confecciona una lista con los datos clave para cada una de las técnicas a utilizar. En este caso, debe considerarse que una misma técnica puede ser utilizada para verificar varios datos claves.

b) Definir el alcance de las pruebas por cada técnica de comprobación

El alcance de cada técnica de comprobación se define de la siguiente forma:

- Datos claves a probar con la técnica de comprobación
- Los criterios de la información de negocios afectados por los datos a probar
- Los recursos de tecnología que son impactados por los controles a probar

c) **Diseñar las pruebas de auditoría a ejecutar con cada técnica de comprobación**

El diseño detallado implica determinar los recursos necesarios (infraestructura, datos y personal), los objetivos y el procedimiento de análisis a emplear.

d) **Planificar la ejecución de las pruebas sustantivas**

El objetivo de este paso es planear y coordinar la ejecución de las pruebas de auditoría con el personal de sistemas y del área de negocio en el lugar de trabajo (manuales y asistidas por computador).

Como factor crítico de éxito de las pruebas de auditoría, es necesario programar su ejecución considerando la disponibilidad de los recursos necesarios para aplicarlas, el sitio de ejecución y su periodicidad.

Para este fin, se elabora un plan de pruebas, considerando las fechas que sean más oportunas, especialmente cuando para su ejecución se requiera de los equipos de procesamiento, que no son administrados por la auditoría y la colaboración del personal de sistemas.

Cuando se requiere desarrollar aplicaciones computacionales para realizar las pruebas sustantivas, las actividades correspondientes y el tiempo deben incluirse en este plan.

Ejecución de las pruebas de auditoría

La siguiente etapa del proceso de auditoría consiste en ejecutar el plan de pruebas de auditoría especificado en la etapa anterior. Estas pruebas pueden ser asistidas por computador o completamente manuales. Por cada prueba que se ejecute deben adjuntarse los soportes correspondientes. Estos consisten en documentos, archivos, programas de computador y cualquier otra evidencia que compruebe la ejecución de la prueba y muestre los resultados obtenidos.

Como resultado de las pruebas de auditoría ejecutadas, se obtienen entre otros los siguientes soportes:

- Lista de comprobación de controles revisados por el auditor
- Documentación sobre los procedimientos y controles establecidos en los procesos de negocio o sistemas de información sujetos a auditoría
- Muestras de documentos, listados y cualquier otro material de evidencia relacionado con deficiencias, debilidades o irregularidades identificadas por la auditoría
- Archivos de datos utilizados por el auditor en las pruebas de auditoría asistidas por computador
- Documentos con la preparación de las entrevistas y con las notas tomadas por el auditor durante su realización
- Documentación de los programas o scripts desarrollados por el auditor para realizar las pruebas asistidas por computador

Técnicas y herramientas de auditoría

Los auditores pueden utilizar diferentes métodos para revisar los controles de las aplicaciones en funcionamiento y las operaciones en el centro de

servicios informáticos. A continuación se describe en qué consiste cada técnica o herramienta.

a) Técnicas para probar los controles en los sistemas

- Método de los datos de prueba
- Evaluación del sistema de caso base
- Operación paralela
- Simulación paralela

b) Técnicas para analizar sistemas

- Snapshot
- Mapping y tracing manuales
- Mapping y tracing asistidos por el computador
- Flujogramas de control (control flowcharting)

c) Técnicas para verificar datos

- Software multipropósito para auditoría
- Software de auditoría para terminales
- Programas de auditoría de propósito especial

d) Técnicas para seleccionar y monitorear transacciones

- Selección de transacciones de entrada
- Módulos de auditoría integrados en los sistemas de información
- Registros extendidos

Técnicas para probar los controles en los sistemas

Se utilizan para probar cálculos, programas o aplicaciones completas con el propósito de evaluar los controles, verificar la exactitud del procesamiento y el cumplimiento con los procedimientos de procesamiento establecidos.

Tales técnicas son usadas para dos propósitos: evaluar los sistemas de aplicación y probar el cumplimiento.

a) Método de datos de prueba

Este procedimiento ejecuta programas de aplicación de computador utilizando archivos de datos de prueba y verifica la exactitud del procesamiento comparando los resultados del procesamiento de los datos de prueba con los resultados predeterminados para la prueba.

Los auditores usan esta técnica para probar la lógica del procesamiento seleccionado, las rutinas de cálculos y las características de control dentro de los sistemas de información.

Los datos de prueba son transacciones simuladas que incluyen idealmente todo tipo de condiciones posibles, incluyendo aquellas que el sistema es incapaz de manejar, debido a la carencia de controles apropiados. Quiere decir esto, que la lista de transacciones simuladas debería probar condiciones tanto válidas como inválidas. Los datos de prueba deben ser procesados con los programas regulares del sistema.

1) Propósito de los datos de prueba

El auditor no puede ver físicamente las operaciones y los controles dentro de la caja negra (sistema de información) pero puede ver un listado de los resultados de la prueba donde por ejemplo, algunas transacciones que deberían ser rechazadas no lo fueron o donde condiciones de desbordamiento causaron errores o transacciones fuera de límite fueron procesadas como si fueran correctas (ejemplo transacciones de dientes que exceden el límite de crédito).

El auditor también puede determinar si la caja negra está procesando apropiadamente las transacciones válidas. El uso de los datos de prueba abre ventanas en la caja negra, porque las transacciones simuladas se procesan en el sistema de computador y generan resultados que son comparados por el auditor con resultados esperados, preparados

manualmente con anterioridad. Es decir, antes de ejecutar los datos de prueba, el auditor calcula los resultados que debería obtener y luego los compara con los obtenidos en la prueba.

2) ¿Cómo preparar los datos de prueba?

Generalmente, los datos de prueba se aplican de la siguiente manera:

- Se debe revisar todo el sistema de controles.
- Sobre la base de esta revisión se diseñan las transacciones para probar aspectos seleccionados del sistema o el sistema completo.
- Los datos de prueba se transcriben a los formatos de entrada al sistema.
- Los datos se convierten (graban) a medios utilizables por el computador. El auditor debe verificar la conversión mediante rutinas de balanceo o en los listados de validación que se produzcan. Además, debe guardar el medio magnético que contiene la información hasta cuando realice la prueba.
- Los datos deben procesarse con los programas de la aplicación que están vigentes. El auditor debería estar presente durante el proceso de los datos para asegurar que:
  - No se introduzca información adicional.
  - Se utilizan los procedimientos de operación de máquina estándar.
  - No ocurra alguna irregularidad cuando se efectúa la prueba.
  - Todos los documentos impresos que se produzca sean retenidas por el auditor.
- Los resultados obtenidos en el punto cinco se deben comparar con los resultados predeterminados.

3) Controles de auditoría sobre los sistemas en producción

El principal objetivo del uso de datos de prueba es verificar la operación de los sistemas de información de los clientes para ver si operan como se piensa (desea).

El auditor debe asegurarse que el programa que se está probando es el mismo que está actualmente en producción. No existe una forma segura de garantizar esta situación pero hay muchas cosas que puede hacer el auditor para sentirse más seguro de estar probando el sistema real.

4) Aplicaciones de los datos de prueba

El auditor debe tener el diseño de los registros de transacciones para preparar sus transacciones de prueba. Este diseño debe contener el nombre de cada campo, el tamaño y el tipo (numérico o alfanumérico). El auditor incluye sus propios datos en los campos apropiados para producir resultados predeterminados. Si los resultados de las pruebas no están de acuerdo a los resultados esperados se debe hacer una investigación más profunda para determinar la razón para las variaciones.

Los siguientes son algunos elementos que normalmente deberían ser incluidos en la aplicación de datos de prueba:

- Verificar si se producen totales de control y se devuelven a la mesa de control
- Tratar de procesar una transacción sensitiva sin la debida autorización y observar si el sistema la rechaza (por ejemplo, cambiar el límite de crédito)
- Hacer chequeos numéricos, alfabéticos y de caracteres especiales
- Entrar a un campo con signo negativo y observar si se procesa realmente con este signo
- En algunos sistemas sin controles apropiados, el signo negativo se convierte a positivo
- Hacer comprobaciones de validez. Por ejemplo, entrar un código inválido o un departamento con número equivocado
- Hacer pruebas de razonabilidad y de límite
- Cuando las transacciones deben estar ordenadas por número de secuencia, entrar transacciones en desorden
- Incluir un número de cuenta dígito de chequeo predeterminado y ver si se procesa normalmente

- Incluir diversos campos de datos incompletos o inexistentes
- Insertar caracteres en campos que causen condiciones de desbordamiento
- Tratar de leer o escribir un archivo equivocado

Los archivos que se van a probar, deben ser copiados corno archivos especiales de trabajo con el fin de permitir todo tipo de pruebas.

5) Ventajas y desventajas de los datos de prueba

- **Ventajas:**
  - Su uso puede limitarse a funciones específicas del programa, minimizando el alcance de la prueba y su complejidad
  - Es una buena herramienta de aprendizaje para los auditores porque su uso requiere mínimos conocimientos de informática
  - No se requiere que el auditor tenga grandes conocimientos técnicos
  - Tiene buena aplicación donde son pocas las variaciones y combinaciones de transacciones
  - Da una evaluación y verificación objetiva de los controles de programa y de otras operaciones que serían impracticables por otros medios
  - Los datos de prueba se podrían correr sorpresivamente para descubrir la posible modificación de programas sin autorización e incrementar la efectividad de otras pruebas realizadas

- **Desventajas:**
  - Se requiere bastante cantidad de tiempo y esfuerzo para preparar y mantener un lote de datos de prueba representativo. Cualquier cambio en programas, diseño de registros y sistema implican cambiar los datos de prueba
  - En algunos casos el auditor puede no probar el sistema que realmente está en producción

- En un sistema complejo con gran variedad de transacciones es difícil anticipar todas las condiciones significativas y las variables que deberían probarse
- El auditor debe estar bastante relacionado 'con la lógica de programación que está probando
- La prueba en si misma no detecta todos los errores. Cuando los programas son muy complejos, pueden existir infinidad de rutas y es muy difícil seguirlas todas
- Hay una probabilidad muy alta que los datos de prueba no detecten manipulaciones inadecuadas de una cuenta o cantidad específica

6) Sugerencias para desarrollar datos de prueba

- **Para archivos maestros:**
  - Duplicar registros.
  - Proceso de registros fuera de secuencia.
  - Montar e intentar procesar archivos equivocados.
- **Para registros nuevos:**
  - Crear un registro nuevo antes del primer registro existente en el maestro
  - Crear un registro nuevo después del último registro existente en el maestro
  - Crear tres o cuatro registros nuevos con llaves consecutivas dentro de registros que no existen
  - Crear un registro para una división inexistente, un departamento, una planta, un elemento de inventario, empleado, cliente y así sucesivamente
  - Crear dos o más registros de cabecera, uno inmediatamente después del otro
  - Crear un registro nuevo con llave cero
  - Crear un registro nuevo con llaves nuevas
  - Crear un registro nuevo pero incompleto. (por ejemplo sólo uno o dos campos de diez posibles)

- **Para transacciones:**

- Crear transacciones para el primer registro del archivo
- Crear transacciones para el último registro del archivo
    - Crear transacciones para otros registros diferentes al primero y último del archivo
    - Crear transacciones para un registro nuevo creado en la misma corrida
    - Crear transacciones para varios registros consecutivos
    - Crear varios tipos de transacciones para un mismo registro
    - Intentar crear transacciones para registros inexistentes que fueran menores en secuencia que el menor registro existente, mayores en secuencia que el último registro existente y entre registros existentes, así como para varios registros consecutivos no existentes
    - Crear transacciones de tal manera que los totales se hagan negativos y verificar el efecto en otros campos del registro
    - Crear cantidades demasiado grandes para crear desbordamiento. Examinar los resultados
    - Si se utiliza un registro de encabezado seguido por registros de detalle, crea registros detallados para el primer registro del archivo, el último registro, dos registros consecutivos, un registro no existente y varios registros inexistentes.

- **Para registros borrados e inactivos:**

- Eliminar el primer registro de cada archivo
- Eliminar el último registro de cada archivo
- Eliminar tres o cuatro registros consecutivos de cada archivo
- Intentar accesar un registro inexistente
    - Codificar un registro como inactivo e intentar grabar datos al mismo registro en la misma corrida
    - Volver activo un registro inactivo y crearle transacciones en la misma corrida
    - **Para fechas:**

- Asegurarse que todos los campos de datos de fechas se han actualizado correctamente.
- Crear fechas con meses 00 y 13, días O y 32 y un año inválido
- Crear fechas que estén fuera de los intervalos de actualización. Ejemplo en un período mensual, hacer intervalo de más de 30 días
- Hacer dos corridas de actualización con la misma fecha

- **Para pruebas de lógica y proceso:**
  - Verificar todos los cálculos que proceden promedios o porcentajes con pequeños medianos y grandes valores
  - Crear una condición para todas las rutinas de división con cero como denominador
  - Crear datos de prueba para valores menores que el mínimo y mayores que el máximo permitidos
  - Crear datos para todas las excepciones y errores
  - Crear datos que incluyan excepciones múltiples y errores en la misma transacción
  - Crear datos para los valores mínimos y máximos de cada campo
- **Para programas de edición, los datos de prueba para campos alfabéticos incluirán:**
  - Campo completamente lleno
  - Campo completamente en blanco
  - Únicamente la primera posición
  - Primera posición en blanco
  - Mezcla de caracteres numéricos y alfabéticos
- **Datos de prueba para los campos de cantidad o valor que incluirán:**
  - Campo lleno de nueves
  - Campo lleno de ceros
  - Campo lleno de blancos
  - Exacto el límite inferior, si lo hay
  - Exacto el límite superior, si lo hay
  - Una cantidad o valor típico entre los límites

- Valor superior al límite, si lo hay (diferente de nueves) Valor inferior al límite, si lo hay (diferente de ceros)
- Valor con un signo errado (+ o -)
- Datos alfabéticos en cada campo

- **Para programas de actualización:**

- Diseñar datos para crear varios registros maestros completos
- Crear datos para cambiar un registro maestro inexistente
    - Diseñar datos para crear un registro con la misma llave de otro existente
    - Crear datos con un registro cuya llave sea cero
    - Crear datos con un registro cuya llave sea nueve
    - Crear uno o dos elementos para establecer un registro del archivo maestro nuevo pero incompleto
    - Diseñar datos para crear un nuevo registro en el archivo maestro y hacerle cambios posteriores en la misma corrida

- **Para programas de proceso:**
    - Entrar datos que produzcan resultados de cálculos con valores pequeños, medianos y muy grandes
    - Entrar datos que creen condiciones de división o multiplicación por cero
    - Entrar datos que originen desbalanceo del registro de control de lote. Examinar los resultados
    - Diseñar varias entradas contables ilógicas (ejemplo: crédito a gastos de depreciación y debido a cuentas por cobrar)

Entrar datos que causen desbordamiento.

- **Para programas de informes:**
    - Incluir datos de prueba con valores negativos para asegurar que se impriman los signos para cada campo, en cada línea de detalle y en las líneas de total
    - Crear datos con nueves en todo el campo para asegurar que se impriman y que no se ponen en otros

- Entrar datos de prueba con sólo ceros para probar la supresión de ceros no significativos en la impresión
- Verificar todas las sumas y resultados de los cálculos

b) Evaluación del sistema de caso base

Este procedimiento ejecuta programas de sistemas de información, usando archivos de datos de prueba desarrollados como una parte de la prueba general del programa que verifica la exactitud del procesamiento, comparando los resultados del procesamiento con los resultados predeterminados para los datos de prueba.

Esta técnica usa datos de prueba desarrollados por auditores y usuarios de aplicaciones de computador, en cooperación con el personal del centro de datos, para proporcionar una prueba completa al sistema. El archivo de datos del caso base está destinado a verificar la correcta operación del sistema antes de su aceptación en producción, así como para verificar periódicamente la integridad del procesamiento después de su aceptación en producción.

Los archivos de prueba del sistema de caso base, por definición, son creados para proveer una prueba selectiva de todas las características y funciones dentro de un sistema de información.

Aunque esta técnica proporciona la ventaja de efectuar pruebas de cumplimiento y verificar el sistema completo, el esfuerzo requerido para mantener los archivos de datos después de su instalación inicial requiere de estrecha cooperación entre usuarios, auditores y el personal del centro de datos para la preparación de los datos de prueba y la validación de los resultados.

c) Operación paralela

Este es un procedimiento para verificar la exactitud de sistemas de aplicación nuevos o revisados, mediante el procedimiento de datos y archivos en producción, usando tanto los procedimientos existentes como

los nuevamente desarrollados, para luego comparar los resultados de ambos procesamientos e identificar diferencias no esperadas.

Este procedimiento es ampliamente utilizado por el personal del centro de datos para verificar sistemas nuevos o revisados, antes de remplazar los procedimientos existentes.

Tiene la ventaja de verificar los nuevos programas del sistema de información antes de discontinuar los existentes. Períodos extensos de operación paralela implican, como desventaja, los costos resultantes del procesamiento adicional.

d) Simulación paralela

En este procedimiento, las transacciones y los archivos de producción son procesados usando programas de computador que simulan la lógica de los programas de aplicación. Las funciones de procesamiento seleccionadas pueden, entonces, ser verificadas mediante la comparación de los resultados simulados con los resultados del procesamiento de producción.

Esta técnica de prueba tiene la ventaja de verificar los procedimientos de procesamiento seleccionados, usando datos de producción, obviando así el tiempo consumido en la preparación de los datos de prueba.

Los auditores que usen esta técnica, sin embargo, deben preparar programas de computador que simulen las funciones de producción a ser verificadas. Programas de auditoría especialmente preparados o software generalizado de auditoría pueden ser usados para este propósito. El software generalizado de auditoría ha simplificado la preparación de programas de simulación paralela.

Técnicas para analizar los sistemas

En esta sección, se incluyen las técnicas y herramientas de auditoría usadas para evaluar la lógica de procesamiento y, los procedimientos internos en programas de aplicación y en programas del sistema. Estas técnicas se usan durante el desarrollo de los sistemas de aplicación así como durante

las pruebas de cumplimiento periódicos en la etapa post instalación. Estas técnicas son snapshot, tracing, mapping y flowcharting (flujogramas de control).

a) Snapshot

Son instrucciones de programa o subrutinas que reconocen y registran el flujo de transacciones señaladas, durante todo el camino lógico seguido por tales transacciones dentro de los sistemas de información. Esta técnica es usada por los auditores para rastrear (localizar el paradero) transacciones específicas mediante programas de computador para conseguir evidencia, documentar el recorrido lógico, las condiciones de control y de las secuencias de procesamiento.

La técnica tiene la ventaja de verificar el flujo lógico del programa y, consecuentemente, ayuda al auditor a entender los pasos de procesamiento dentro de programas de aplicación. Tiene la desventaja de requerir bastante conocimiento de sistemas y de programación por lo que con frecuencia consume bastante tiempo para el uso de los auditores.

Tracing y mapping manual

Estos procedimientos identifican el flujo de transacciones y sus controles de aplicación asociados, incluyendo la elaboración, aprobación y procesamiento de documentos fuente, así como el procesamiento de transacciones de entrada, procesamiento en el computador, la distribución y uso de los informes.

El tracing y mapping manual pueden incluir el análisis de listados de programas de aplicación, para identificar y evaluar la lógica y las funciones de control de los programas de aplicación. Sin embargo, el énfasis es sobre la identificación y evaluación de los procedimientos manuales y de controles externos a los programas de aplicación.

Las técnicas de tracing y mapping ayudadas por computador se usan para analizar programas de aplicación, complementando los métodos manuales.

b) Tracing y mapping asistido por computador

Estas son subrutinas de programas de computador que identifican los segmentos y/o subrutinas de programa usadas en el procesamiento de transacciones de prueba. El tracing asistido con el computador proporciona evidencia documentaria de las instrucciones del programa utilizadas para procesar transacciones específicas.

Mapping es una técnica que proporciona evidencia de las secuencias de procesamiento usadas en la subrutina, más que a nivel de instrucción en el programa de computador.

Estas técnicas y herramientas de auditoría son usadas para verificar la lógica de procesamiento de las transacciones e identificar las porciones de programa no utilizadas. Dos desventajas están asociadas con el uso de éstas por parte del auditor: se requiere extenso conocimiento de programación de aplicaciones y, segunda, consume bastante tiempo e implican análisis detallado.

c) Control flowcharting (Flujograma de control)

Este procedimiento usa técnicas de diagramación de programas de computador para identificar y presentar el recorrido lógico y los puntos de control dentro de los sistemas informático.

Símbolos y técnicas estándar de auditoría analítica, son usados para desarrollar diagramas de los sistemas de información. Esos esquemas proporcionan información con el objeto de analizar con los usuarios y el personal de informática los controles internos de los sistemas de información. Además, los flujogramas de control sirven como un excelente mecanismo para entrenar a nuevos auditores.

Técnicas para verificar los datos

Estas técnicas son usadas posteriormente al procesamiento de la producción, para seleccionar datos de archivos basados en requerimientos lógicos o de muestreo estadístico; para totalizar y balancear archivos o

secciones lógicas de archivos, tales como divisiones organizacionales o clases de cuentas; para dividir archivos por valores de excepción; para ignorar datos o entradas duplicadas o para formatear informes para uso de auditoría.

a) Software general de auditoría (SGA)

El SGA accesa, extrae, manipula y presenta datos y resultados de pruebas en un formato apropiado para los objetivos de la auditoría. Tal archivo generalizado generador de software, generalmente es controlado por parámetros o instrucciones simplificadas que requieren un mínimo de conocimientos de informática. Tiene la ventaja de permitir al auditor manipular el procesamiento de datos de archivos maestros sin preparar programas especiales. Una desventaja asociada con esta técnica es que su evidencia se limita a los archivos de datos y en consecuencia no es utilizable (funcional) para pruebas de cumplimiento en los programas, para condiciones que no se reflejan en los archivos.

b) Software de auditoría para terminales

Este software de propósito general accesa, extrae, manipula y despliega datos de bases de datos en línea, usando comandos de terminales remotas.

Esta técnica tiene la ventaja de permitir la investigación interactiva y rápida y de proporcionar acceso completo a los archivos de datos, permitiendo periódicamente examinar archivos sin excesiva preparación o procesamiento separado. Este es, sin embargo, utilizado únicamente en situaciones donde se utilizan bases de datos en línea.

c) Programas de auditoría de propósito especial

Son especialmente desarrolladas para extraer y presentar datos de los archivos de un sistema de aplicación específico, generalmente en formato invariable.

Las desventajas asociadas con estos programas son su limitada aplicabilidad, inflexibilidad, costos de preparación y el alto nivel de expertos

en programación de computador que es requerido. Debido a la naturaleza específica de cada programa de auditoría de propósito especial no se profundiza más sobre esta herramienta.

Técnicas para seleccionar y monitorear transacciones

Las técnicas y herramientas usadas para seleccionar y capturar datos de producción para su posterior verificación y auditoría manual son indicadas bajo esta clasificación. Se utilizan generalmente para supervisar actividades de producción y seleccionar muestras como parte de una continua actividad de auditoría dentro del proceso de producción normal.

Los criterios de selección son generalmente parámetros controlados por el auditor y usan pruebas de rango, técnicas de muestreo o condiciones de error para implicar la selección de registros para su posterior evaluación por parte del auditor. Tales técnicas se usan en pruebas de cumplimiento para monitorear el procesamiento de transacciones y seleccionar datos para su verificación.

Esta categoría incluye: programas de selección de transacciones de entrada, los cuales son independientes de los programas del sistema de información, módulos de auditoría integrados en los sistemas de información y la técnica de registros extendidos.

a) Selección de transacciones de entrada

Utiliza software de auditoría para separar y seleccionar transacciones, que son entrada para sistemas de información, como parte del ciclo de procesamiento de producción regular.

Las capacidades de este software incluyen: monitoreo de niveles de actividad y razones de error por transacción, seleccionando sistemáticamente muestras de transacciones para subsiguiente verificación manual y, la identificación y selección de condiciones de excepción especificadas por el auditor. El software es controlado por parámetros y totalmente independiente de su correspondiente software de aplicación en

producción. Como resultado, éste es independientemente controlado por el auditor y puede ser instalado sin requerir modificaciones del software del sistema de aplicación. El costo de desarrollo y mantenimiento es la desventaja primaria asociada con esta técnica.

b) Colección de datos de auditoría integrados en los sistemas de información

Este procedimiento usa software de auditoría para marcar y seleccionar transacciones de entrada y transacciones generadas dentro del sistema de aplicación durante el procesamiento de producción. Tales subrutinas de auditoría son integradas como huéspedes dentro de los sistemas de nforrnación.

Actividad de supervisión (monitoreo), muestreo y reportes de excepción son todos controlados por parámetros. El diseño y la implementación de tales módulos son altamente dependientes de la aplicación y generalmente son ejecutados como parte integral del proceso de desarrollo de aplicaciones. Con frecuencia este método es referido como SCARF (System Control AuditingReview File). Tiene la ventaja de proporcionar muestreo y producción estadística incluyendo transacciones, tanto de entrada como generadas internamente. La desventaja primaria es el alto costo de desarrollo y mantenimiento y la dificultad asociada con la independencia del auditor.

c) Registros extendidos

Esta técnica selecciona, por medio de uno o más programas creados especialmente, todos los datos significativos que han afectado el procesamiento de una transacción individual. Esto incluye la acumulación, dentro de un único registro, de los resultados del procesamiento sobre el mismo período de tiempo requerido para el procesamiento completo de la transacción. El registro extendido incluye datos de todos los sistemas de aplicación de computador que contribuyeron al procesamiento de una transacción. Tales registros extendidos, son compilados dentro de archivos que proporcionan una fuente convenientemente accesible para los datos de

las transacciones. Este tiene la desventaja del incremento de los requerimientos y costos de almacenamiento de datos y los costos adicionales de desarrollo del sistema.

Análisis del resultado de las pruebas de auditoría

El objetivo de esta etapa es analizar y evaluar los resultados de las pruebas de cumplimiento y sustantivas, efectuadas en la etapa anterior, con el propósito de obtener conclusiones de la auditoría sobre el funcionamiento de los procesos de negocio y sistemas de información objeto de la auditoría.

En esta etapa, se analizan los resultados de las pruebas de auditoría que fueron ejecutadas por medios manuales o asistidas por computador y se generan indicadores de la protección existente para cada control clave asociado con los procesos de negocio y sistemas sujetos a auditoría. Los resultados pueden ser satisfactorios o insatisfactorios y de ellos se generan observaciones que son analizadas para determinar su impacto en el negocio.

Las observaciones se refieren a desviaciones que se detectan en las pruebas de auditoría, respecto a los estándares, de la tecnología de información, a la normativa legal y las políticas y procedimientos establecidos en la organización.

Como resultado del análisis y evaluación de los resultados de las pruebas de auditoría ejecutadas, se obtienen los siguientes productos:

- Lista de controles clave comprobados por el auditor en terreno.
- Documentación de las observaciones de auditoría obtenidas como resultado de las pruebas de cumplimiento y sustantivas, el análisis de las deficiencias identificadas y/o oportunidades de mejoramiento.

Análisis del resultado de las pruebas de cumplimiento

El análisis de los resultados de las pruebas de cumplimiento se realiza utilizando la agrupación de controles por técnica de comprobación.

Por cada técnica de comprobación utilizada, para todo el proceso de negocio o el sistema de información, el auditor procede a analizar los resultados obtenidos como se indica a continuación:

- Por el grupo de controles verificados con una misma técnica de comprobación, establecer globalmente si los resultados de la prueba son satisfactorios o no satisfactorios y generar una conclusión de la auditoría.
- Desarrollar las observaciones de auditoría. Por cada técnica de comprobación utilizada se pueden generar una o más observaciones.
- Consolidar los resultados de las pruebas de auditoría.

El análisis del grado de satisfacción de los objetivos de control para las pruebas de cumplimiento se realiza utilizando la agrupación de controles por objetivo de control.

Las respuestas obtenidas para cada uno de los objetivos de control sustanciados por el auditor, se procesan siguiendo los pasos que se indican a continuación:

1. **Por cada objetivo de control seleccionado, calificar el grado de satisfacción según los resultados de las pruebas efectuadas**

Para evaluar el grado de protección de los controles agrupados por objetivo de control, es necesario registrar al menos una observación por cada control verificado con resultado insatisfactorio.

Un control verificado con resultado insatisfactorio puede estar asociado a varios objetivos de control. Por consiguiente, una observación puede impactar a varios objetivos de control.

Un objetivo de control es satisfecho por los controles verificados cuando la protección existente es superior al 70%, es decir, cuando el significado cualitativo de la protección existente es Media Alta o Alta.

2. **Para cada control verificado con resultado insatisfactorio, desarrollar una observación de auditoría**

A cada objetivo de control pueden corresponder varias observaciones, al menos uno por cada control que presenta resultado insatisfactorio.

Si un control que presenta resultado insatisfactorio está asociado con varios objetivos de control, es suficiente con desarrollar una sola vez la observación, analizando su impacto en todos los objetivos relacionados con el control.

Esta última etapa permite consolidar las calificaciones del grado de satisfacción de los objetivos de control para cada proceso de negocio y sistema de información.

Análisis de los resultados de las pruebas sustantivas

Para analizar los resultados de las pruebas sustantivas, el auditor procede como se indica a continuación:

1. **Establecer si los resultados de la prueba sustantivas son satisfactorios o no**

Para los datos claves verificados por cada proceso de negocio o sistema de información, se debe concluir si los resultados de las pruebas son satisfactorios o no y generar una observación de auditoría por cada prueba con resultado negativo.

2. **Desarrollar las observaciones de auditoría**

Por cada dato verificado se pueden generar una o varias observaciones.**4.4**

3.4 FASE III. COMUNICACIÓN DE LOS RESULTADOS

Esta es la última fase de la auditoría, en ella se resumen los resultados más significativos obtenidos en las etapas anteriores.

Estos son los insumos para elaborar el informe de auditoría con el cual se comunicará a la alta dirección y a los demás interesados, las observaciones y conclusiones sobre las características de seguridad, calidad y confiabilidad de la información y de los recursos tecnológicos y humanos que intervienen en las actividades de control de los procesos de negocio y sistemas de información.

Elaboración de los informes con los resultados de la auditoría

Los informes tienen como objetivo comunicar al servicio sobre el resultado de la auditoría, que éste conteste cada una de las observaciones con los antecedentes pertinentes y posteriormente se elabore y envíe el informe final con las conclusiones de la auditoría.

Estructura y contenido de los informes

El objetivo del informe preliminar es comunicar al servicio las observaciones encontradas, suscitar la respuesta con las acciones de mejoramiento para solucionar los problemas detectados.

El propósito del informe final es atender las respuestas del servicio a las observaciones y desarrollar las conclusiones de auditoría.

El informe preliminar consta de las siguientes tres secciones:

a) Objetivos y alcance de la auditoría

Breve descripción de los objetivos que se propuso la auditoría, de los aspectos de seguridad examinados, los objetivos de controles y las dependencias en las que se efectuó la revisión. También, se mencionan el período de tiempo que cubrió la revisión y el rango de las fechas durante las cuales se efectuó la auditoría.

Se describen los objetivos específicos fijados en el programa de auditoría. Para definir el alcance, se detallan los aspectos de control generales revisados (objetivos de control básicos) por la auditoría. Este párrafo es importante como punto de referencia para que el destinatario evalúe la importancia de las observaciones detectadas por la auditoría.

b) Antecedentes generales

Este capítulo contiene una breve descripción de las características y atributos del área auditada. El objetivo es ubicar al destinatario del informe dentro de un marco de referencia que le ayude a comprender el informe y la importancia de las observaciones de la auditoría.

c) Observaciones de la auditoría

Esta parte del informe presenta, para cada proceso y sistema evaluado, las observaciones y debilidades de control identificados por la auditoría que debe contestar la administración.

Para elaborar el informe final de auditoría, se realiza lo siguiente:

Luego de recibir la respuesta al informe preliminar, el auditor analiza los descargos y antecedentes enviados por el servicio y desarrolla las conclusiones para cada observación y la conclusión general de la auditoría.

4.4.3 Aseguramiento de la calidad de los informes de auditoría

Verificar que la forma y el contenido del informe con los resultados de la auditoría cumplan con el mínimo exigidos por los estándares y las mejores prácticas recomendados por los expertos. Si alguna de las respuestas a las preguntas que se incluyen a continuación es negativa, significa que el informe necesita más trabajo de revisión.

Lista de comprobación de calidad de los informes de auditoría.

1. ¿Todos los puntos del informe atañen al destinatario del mismo?
2. ¿Todas las observaciones incluidas en el informe fueron respondidas por el auditado para determinar su exactitud?

3. ¿Todas las observaciones y conclusiones incluidas en el informe son suficientemente explícitas, para que las áreas entiendan su significado e importancia y se motiven a tomar acciones correctivas?
4. ¿Todas las observaciones incluidas en el informe son lo suficientemente importantes como para justificar el tiempo que el auditado dedique a su lectura?
5. ¿En los papeles de trabajo existe suficiente evidencia para soportar las observaciones y conclusiones de la auditoría?
6. ¿Todas las conclusiones incluidas en el informe fueron evaluadas con suficiente detalle para determinar su costo/beneficio?
7. 7, ¿Si las conclusiones incluidas no son viables por costo/beneficio, otras circunstancias justifican su inclusión en el informe?
8. ¿En el informe se incluyen únicamente puntos que tienen alto potencial de pérdidas y bajo costo correctivo?
9. ¿Tienen sentido los títulos utilizados para encabezar las observaciones?
10. ¿El informe cumple con las expectativas de la jefatura?
11. ¿Existe claridad en los beneficios para los auditados que justifican la incorporación de las observaciones de control interno especificadas en el informe final?
12. ¿El informe se emite oportunamente de modo que el máximo beneficio pueda obtenerse de él?

Las observaciones y puntos mejorables deberán incluir exclusivamente aspectos que sean importantes, de beneficio para el servicio y factibles de implantar sin causar costos significativos. Cada punto tendrá asignado un número de secuencia y un título que exprese de manera resumida lo que se detectó, utilizando un lenguaje positivo y constructivo.

A continuación, se deben presentar los beneficios que obtendrá el servicio auditado al solucionar la deficiencia o problema observado. Es aquí donde el

auditor debe mostrar que su trabajo contribuye al mejoramiento de los procesos y sistemas de la organización.

Para cada observación de la auditoría siempre se deberán expresar los beneficios para la organización. Como por ejemplo, para incrementar la eficiencia, prestar un mejor servicio a los usuarios, ahorrar costos, evitar que los errores pasen inadvertidas, mejorar la información que recibe la alta dirección, etc.

- El beneficio debe enfocarse para el usuario, no para el auditor
- No decir que el beneficio es mejorar el control interno. Tampoco que es para mejorar los procedimientos
- Evitar decir: "Es necesario que se establezcan controles de acceso", es decir "es necesario establecer controles de acceso"
- Deberá expresarse con palabras que describan la realidad de la manera más exacta posible y con un lenguaje simple
- Se escribe en infinitivo
- Evitar el uso de superlativos

La conclusión de la auditoría debe expresar su concepto sobre la protección que ofrecen los controles y procedimientos utilizados por la organización para asegurar la confiabilidad de los procesos y sistemas auditados.

Organizar y cerrar la carpeta con archivos de trabajo

La expresión archivos de trabajo se refiere al conjunto organizado de papeles y archivos computacionales, que contiene:

- La documentación del trabajo realizado por los auditores asignados al desarrollo de un trabajo particular de auditoría
- Las evidencias válidas y suficientes de los trabajos de auditoría
- Las evidencias de las actividades y procedimientos de planeación, ejecución y control de cada una de las etapas de la auditoría

La documentación de auditoría es el registro del trabajo y la evidencia que soporta las observaciones y conclusiones del auditor. La documentación

demuestra la extensión con la que el auditor cumplió con los estándares generales para realizar la auditoría.

La documentación debería incluir, como mínimo, un registro de:

- La planificación y preparación del alcance y objetivos de la auditoría
- El programa de auditoría
- Los pasos de auditoría ejecutados y reunidos
- Las observaciones y conclusiones de la auditoría
- Cualquier reporte producido como resultado del trabajo de auditoría
- Las respuestas del auditado a las observaciones del informe preliminar

La extensión de la documentación del auditor, dependerá de las necesidades para una auditoría particular y deberá incluir:

- El entendimiento del auditor sobre el área que fue auditada
- El entendimiento del auditor sobre los sistemas de información y su infraestructura
- La fuente de la documentación de auditoría y la fecha de su elaboración
- La evidencia de revisión y supervisión del trabajo de auditoría

La documentación debería incluir información de auditoría que es exigida por las regulaciones o cualquier estándar aplicable.

Las políticas y procedimientos que en efecto pueden estar para asegurar la custodia apropiada y retención de la documentación que soporta observaciones y conclusiones de auditoría, por un tiempo prudente para satisfacer los requerimientos legales, profesionales y organizacionales.

La documentación debería ser organizada, almacenada y asegurada de una manera apropiada para el medio en el cual se retiene.

Seguimiento a las observaciones de la auditoría

El objetivo de esta etapa es establecer las fechas de compromiso para verificar que los responsables de las observaciones detectadas, inicien e implementen las acciones correctivas,

En esta etapa se acuerda con los auditados, las fechas de compromiso para atender las observaciones de la auditoría. También, se definen los responsables de atender estos compromisos y se registran los datos de planeación del seguimiento, además de las fechas específicas para verificar dicho seguimiento, junto con los cargos de los responsables de verificar el seguimiento y los resultados del mismo. Con las actividades de esta etapa se termina el trabajo de auditoría.

Los productos de esta etapa son los siguientes:

- Programa de seguimiento del informe final
- Listado con verificación de cada observación pendiente
- Emisión del informe con los resultados del seguimiento

Planificar el seguimiento a las observaciones de la auditoría

Elaborar tabla con los siguientes encabezados:

- Observación
- Cargo responsable de tomar la acción
- Fecha de compromiso para implantar la acción de mejoramiento
- Fecha de seguimiento prevista

Establecer fechas de compromiso de común acuerdo con el encargado de cada observación:

- Fijar una fecha de compromiso
- Fijar una fecha de seguimiento
- Fijar una alerta de compromiso y seguimiento

Ejecutar el seguimiento a las observaciones de la auditoría

El objetivo es verificar que se hayan implantado las acciones correctivas requeridas para atender las observaciones informadas por la auditoría. Con el fin de establecer políticas, normas y procedimientos acordes a mejorar las deficiencias encontradas en los procesos de negocio y sistemas de información.

Establecer una descripción detallada de la acción implantada y la opinión del auditor al respecto, así como los comentarios del auditado y sus respectivas conclusiones con respecto a la acción implantada.

Informe de seguimiento de la auditoría

Al finalizar el seguimiento se elabora el informe con la información definida en la planificación del seguimiento.

- Observaciones corregidas, pendientes de implementar y no implementadas.
- Porcentajes total de observaciones implementadas.
- Conclusión del proceso de seguimiento.

4. CONCLUSIONES

Las auditorías a las tecnologías de información y comunicaciones realizadas utilizando la metodología expuesta en este trabajo de investigación permiten al auditor y su equipo utilizar un criterio uniforme para seleccionar los objetivos de control y herramientas de auditoría que los conducirá a la obtención de un informe fundamentado en estándares conocidos a nivel internacional.

Por otro lado, la incorporación del estándar COBIT y la norma técnica ISO/IEC 27002 es una fortaleza que ayuda a los auditores a orientarse de mejor forma respecto a los requisitos del negocio que tienen relación con el uso de la tecnología. Cada día surgen nuevas tendencias y productos que aparentemente ayudan a cumplir de forma más eficiente y eficaz los objetivos planteados por la organización pero que, por otro lado, aumentan la complejidad con la cual deben lidiar los directores y ejecutivos a cargo de la administración.

El nivel de complejidad con el cual deben convivir las organizaciones ha aumentado en los últimos años a raíz de la explosiva masificación del uso de sistemas de información que soportan la mayoría los procesos del negocio. La adopción de nuevas tecnologías al interior de una organización impacta directamente en la manera de hacer las cosas, siendo común encontrar una gran cantidad de proyectos que fracasan debido a la resistencia al cambio que manifiestan los empleados y usuarios en la organización.

Ahora bien, si esta problemática fuese abordada por auditores que conocen y entienden los problemas y desafíos que conlleva el uso de tecnologías de información, la realidad actual que viven las organizaciones podría mejorar de manera positiva.

BIBLIOGRAFÍA

Gómez Viertes, Álvaro. "Sistemas de Información, Herramientas Prácticas para la Gestión Empresarial". Editora RAMA. Madrid. España. 196 pp.

Information System Auditor and Control Association, "COBIT® Marco Referencial", "COBIT® Objetivos de Control" y "COBIT® Guías de Auditoría". Atlanta, USA. 512 pp.

IT Governance Institute. "Control Practice". Atlanta. USA. 698 pp.

Warren Gorham & Lamont."Practica] IT Auditing".RIA. New York. USA. 870 pp.

Weber, Ron. "Information System Control and Audit". Pearson Education Inc. New York. USA. 543 pp.

PLATTEN, Mario. DEL PESO NAVARRO, Emilio. (2008). Auditoría Informática enfoque práctico 2a ed. México: Alfa omega Grupo Editor.

HERNÁNDEZ HERNANDEZ, Enrique. (2000). Auditoría en Informática, Un enfoque metodológico y práctico. r ed. México: GRUPO PATRIA CULTURAL.

ECHENIQUE GARCÍA, José Antonio.

(2001). Auditoría en Informática, 2a ed. México: Mc GRAW-HILL/INTERAMERICANA