Sistemas de Información para la Gestión
Gestión de TI

Unidad 7:
CONTROL DE LA GESTION DE TECNOLOGIAS DE INFORMACIÓN

U.N.Sa. – Facultad de Cs.Económicas

Unidad 7: CONTROL DE LA GESTION DE TECNOLOGIAS DE INFORMACIÓN
Control de los Sistemas de Información: Las funciones de control y auditoria en entornos informáticos**.** Sistema de control interno informático: Tipos y metodologías.
Revisiones de auditoría: Entorno jurídico nacional y normativo (nacional e internacional) de la auditoría de los Sistemas.
Herramientas para auditoría de SI. **Principales áreas de la auditoría:** Del outsourcing, de la seguridad física, de la dirección informática, de la explotación, de bases de datos, de la seguridad, de redes, de Internet, de aplicaciones, del desarrollo y mantenimiento de sistemas, del sistema de vigilancia y sobre los datos de carácter general.
Informe de control de sistemas de información

Objetivos específicos:

- **Evaluar los principios básicos que fundamentan la función de la Auditoria de Tecnología de Información**

  Conocer la evolución y las características particulares de la realización de las Auditorias de Tecnologías de la información.

  Evaluar el control interno de la organización y, en base en su examen, proporcionar recomendaciones orientadas a fortalecer las debilidades reveladas.

Bibliografía Básica:

Sistemas de información para la gestión empresaria - Procedimientos, seguridad y auditoría / Lardent, Alberto R.. - Buenos Aires : Pearson Educación, 2001. . ISBN 987-9460-51-0.

Seguridad y auditoría informática : Cap. 25. Auditoría del desarrollo de sistemas - 26. Auditoría de sistemas de aplicación instalados - 27. Técnicas de auditoría y evaluación - 28. Técnicas de auditoría asistidas por computadoras.

Auditoría de Tecnologías y Sistemas de Información, Mario G. Piattini, Emilio del Peso, Mar del Peso, Abril 2008, Editorial Alfa Omega Grupo Editorial, México, ISBN 978-970-15-1378-1.

Material actualizado al momento del dictado de Information Systems Audit and Control Association (ISACA) que es actualmente la organización líder en gobernabilidad en tecnologías de información, aseguramiento, seguridad y control. www.isaca.org

Normas de BCRA, CNV, FACPCE aplicables como sensores de auditorías de TIC especificas según el Ente.

Control de los Sistemas de Información

Control Interno

Conjunto de métodos coordinados y medidas adoptadas dentro de una organización con el fin de:

- Salvaguardar activos,
- Asegurar la confiabilidad y corrección de los datos contables y extracontables
- Promover la eficacia y eficiencia de las operaciones
- Promover la adhesión a las políticas vigentes

Control de los Sistemas de Información

El Control Interno se instrumenta a partir de:

a) Funciones Preventivas
- Políticas Gerenciales
- Misiones y Funciones
- Esquemas de organización
- Normas y procedimientos
- Políticas de personal
- Etc.

b) Funciones de Control/Verificación
- La función de línea, en todos sus niveles (control operativo)
- La función staff (auditoría)

Control de los Sistemas de Información

Auditoría

Es una función de control independiente del sistema controlado, que en forma sistemática y organizada debe:
- Comparar la característica o condición controlada, con respecto a las pautas, normas o elementos utilizados para medirla. Es decir comparar el objeto con respecto al sensor.
- Determinar los desvíos, e
- Informar a quien ordena o contrata la auditoría, que jerárquicamente debe estar por encima del sistema auditado.

Control de los Sistemas de Información

Concepto Moderno de Auditoría

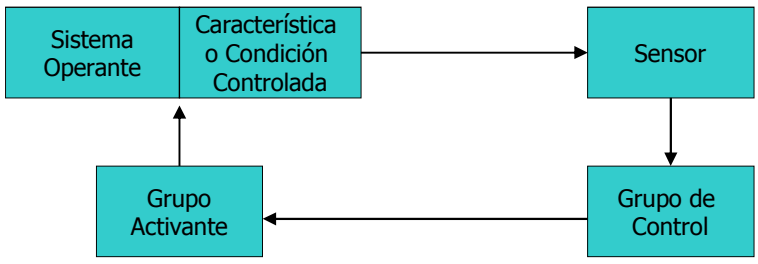
La Auditoría ha cambiado de un enfoque de viejas nociones reactivas hacia una actitud proactiva, con una fuerte inclinación hacia detección de fraudes, monitoreo continuo y capacidad para mejorar procesos del negocio

Concepto

Proceso formal llevado adelante por especialistas en auditoría y en informática a efectos de verificar y asegurar que los recursos y procesos involucrados en la construcción y explotación de los sistemas de información cumplen con los procedimientos establecidos y se ajustan a criterios de integridad, eficiencia, seguridad, efectividad y legalidad.

Control de los Sistemas de Información

Componentes de un Sistema de Control RT7 CECyT (reemplazada por RT 37)



Control de los Sistemas de Información

Sensor

Unidad de medida, el estándar o la norma con la cual voy a medir o comparar el sistema de información.

Normas internas:

Algunas organizaciones de cierta envergadura suelen generar su propio conjunto de normas de funcionamiento materializadas en manuales de procedimientos, cursogramas, flujogramas, organigramas, documentación de sistemas, etc.

Normas externas:

Profesionales:

• Informe 6 Area de Auditoría del CECyT: Pautas para el Examen de Estados Contables en un Contexto Computadorizado

• Informe 15 Area de Auditoría del CECyt: Auditoría en Ambientes Computadorizados.

Organismos de Control:

• Comunicación A 2659 del Banco Central de la República Argentina

• Pautas de Control Interno para Sistemas Computadorizados y Tecnología de Información de la SIGEN (Sindicatura Gral.de la Nación)

•Internacionales

C.O.B.I.T Objetivos de control para la información y la tecnología Relacionada, desarrollado por la I.S.A.C.A. Asociación de Auditoría y Control de Sistemas de Información.

Control de los Sistemas de Información

Sensor

Criterio del Auditor:

Es el menos recomendable y en general el más utilizado.

La principal crítica que se le puede hacer como sensor es la falta de objetividad, ya que es la opinión del auditor sobre lo que debería ser, y por lo general suele ser muy discutida, salvo casos de observaciones muy evidentes, o una muy buena fundamentación del criterio utilizado.

Control de los Sistemas de Información

Componentes del riesgo de Auditoría

Riesgo inherente: aquel que es propio de la actividad del ente o sistema, su naturaleza, estructura, actividad, magnitud, etc.

Está fuera de poder ser controlado por el auditor como para poder eliminarlo.

Riesgo de Control: son los que resultan de un sistema de control deficiente, incapaz de evitar o detectar fallas o irregularidades en forma oportuna.

Está fuera de poder ser controlado por el auditor como para poder eliminarlo, pero sus recomendaciones deben contribuir a reducirlo.

Riesgo de Detección: son los que resultan de un deficiente planeamiento y/o ejecución de la auditoría, sea tanto en la evaluación y categorización de los riesgos, como en la selección y/o aplicación de los procedimientos de auditoría.
Es del ámbito y tarea exclusiva del auditor.

Etapas para el Desarrollo de la Auditoría

Principales Areas de Actividad de la A.S.I.

Objeto de la Auditoría de Sist.de Información

El ámbito de la ASI se refiere al entorno informático entendiéndose por tal a todo lo que conforma:

• Auditoría de la dirección (Plan Estratégico de Sistemas)

• Auditoría del desarrollo (gestión de proyecto) / Adquisición

•Auditoría del Hardware, Software, Comunicaciones, B.de Datos

• Auditoría Seguridad (Seguridad Física, Seguridad Lógica, Evaluación de Riesgos, Plan de Contingencias)

• Auditoría de la explotación y Mantenimiento (Utilización de sistemas, puesta en marcha, cambios de programas)

Principales Areas de Actividad de la A.S.I.

Funciones de la A.S.I.

- Evaluación y verificación de controles y procedimientos relacionados con la función de informática
- Verificación del uso eficiente de los SI.
- Desarrollo de las actividades del área de auditoría informática de acuerdo a estándares normativos.
- Evaluación de las áreas de riesgo y en consecuencia planificación de las tareas del área.
- Realizar el monitoreo permanente de las actividades del área.
- Realizar el monitoreo de la seguridad.
- Monitoreo de la aplicación de procedimientos.
- Realizar una adecuada información y seguimiento de las observaciones realizadas.

Principales Areas de Actividad de la A.S.I.

Auditoría del Plan Estratégico de Sistemas

Objetivo de Control	Riesgos Asociados	Verificaciones a Realizar
El Plan de sistemas contempla las necesidades organizaciones y el crecimiento del negocio y se encuentra adecuadamente aprobado por la dirección y es periódicamente revisado ante cambios en la planificación de la organización.	• Los sistemas no responden a las necesidades de la organización. • Inflexibilidad de los sistemas ante nuevos requerimientos organizacionales. • Desvinculación entre los distintos sistemas. • Comportamiento desordenado y errático en el desarrollo y adquisición de aplicaciones. • Desconocimiento de la existencia o alcance del plan por parte de las distintas áreas organizacionales. • La asignación de recursos no es la adecuada dado la dimensión del proyecto.	• Existencia de un plan formalizado y aprobado por el nivel máximo de la organización. • Verificación de la actualización periódica del plan. • Revisión de la documentación del directorio (actas de reuniones, instrucciones de la dirección, existencia de un responsable de la formulación, etc. • Los cambios de los proyectos impactan en el plan de sistemas.

Principales Areas de Actividad de la A.S.I.

Auditoría del Impacto sobre el Negocio

Objetivo de Control	Riesgos Asociados	Verificaciones a Realizar
El proyecto se encuentra dentro del marco del plan de negocios de la empresa.	Los sistemas no responden a las necesidades del negocio.	El plan estratégico de sistemas es coordinado con el plan de negocios.
Las especificaciones establecidas contemplan los factores esenciales del negocio.	La habilidades propias del negocio no se encuentran apoyadas por los nuevos sistemas.	En la documentación de los requerimientos se identifican las habilidades principales que distinguen a la empresa.
El sistema tiene la capacidad de adaptarse a nuevas reglas del negocio.	El sistema se muestra inflexible ante nuevos cambios.	Se ha previsto que el o los sistemas sean parametrizables y flexibles para adaptarse a los cambios.
Se ha medido adecuadamente el impacto del proyecto en el negocio	El negocio se ve seriamente cuestionado ante el fracaso del proyecto de sistemas.	Se ha previsto el alcance e impacto del proyecto como así también las consecuencias del fracaso del mismo.

Principales Areas de Actividad de la A.S.I.

Auditoría del Desarrollo, Compra o Implementación de SI

Adquisición de Software: Actividades a Auditar

Principales Areas de Actividad de la A.S.I.

Auditoría del Desarrollo, Compra o Implementación de SI

Ejemplo de Plan para Revisión de Requerimientos

Objetivo de Control	Riesgos Asociados	Verificaciones a Realizar
Se han establecido en forma clara todos los requerimientos de todos los usuarios.	• El sistema no contempla todas las necesidades de los sectores usuarios. • Algunos aspectos funcionales no se encuentran soportados. • Las necesidades de información de los niveles directivos no se encuentran totalmente cubiertas. • El sistema no contempla aspectos de control interno. • El sistema no contempla aspectos legales o normativos propios de la actividad de la organización.	• Existe un documento adonde se establecen cuales son los usuarios que representan a cada sector. • Existe un documento donde se establece como se realizará el contacto con los áreas usuarias. • Se ha analizado el sistema actual y se han identificado las fortalezas y debilidades del mismo. • Existe un documento donde se establecen los requerimientos funcionales de control, legales y de información. • Dicho documento fue aceptado por las áreas intervinientes.

Principales Areas de Actividad de la A.S.I.

Auditoría del Desarrollo, Compra o Implementación de SI

Ejemplo de Plan para Revisión de la Instalación

Objetivo de Control	Riesgos Asociados	Verificaciones a Realizar
La instalación del Hardaware necesario se cumplimentó en tiempo y forma.	• Existen demoras en la implementación debido a que el hardaware no está disponible en tiempo y forma establecidos.	• Se ha establecido un plan de instalación del hardware acorde con los tiempos establecidos para el proyecto.
La instalación de software de base se cumplimento en tiempo y forma	• Existe demoras en la instalación debido a que no se ha realizado la instalación del software de base o el mismo está mal instalado.	• Se ha establecido un plan de instalación del software de base y se han contemplado los requerimientos establecidos por el proveedor.
Todos los parámetros de funcionamiento se encuentran adecuadamente definidos.	• Existen parámetros no definidos que provocan el mal funcionamiento del sistema. • La definición de los parámetros no es la adecuada y provoca el malfuncionamiento del sistema.	• Los parámetros han sido adecuadamente establecidos y los usuarios participan en su definición. • Se ha realizado la capacitación suficiente para la adecuada definición de los parámetros.

Principales Areas de Actividad de la A.S.I.

Auditoría del Procesamiento de la Información

Aspecto	Riesgo	Problemas
Segregación de Funciones	Personas no autorizadas pueden tener acceso a funciones de procesamiento de transacciones, permitiéndoles leer, ingresar, modificar o eliminar datos o ingresar transacciones no autorizadas para su procesamiento.	• Inadecuada separación de funciones dentro del Dpto.de Sistemas • Inadecuada ubicación del área de Seguridad Informática • Inadecuado esquema de seguridad lógica-perfiles de usuarios • Problemas con la puesta en funcionamiento de nuevas versiones
Ingreso de Datos	Los datos ingresados pueden ser imprecisos, incompletos o ingresados más de una vez	• Falta de controles de edición y validación (tipos de campos, campos faltantes, límites y validación) • Inadecuada codificación • Falta de controles por lotes
Ítems rechazados o en suspenso	Los datos rechazados y las partidas en suspenso pueden ser no identificadas, analizadas y corregidas	• Inexistencia de aviso de rechazo • Identificación inadecuada de datos rechazados • Inexistencia de reportes de excepción • Falta de seguimiento de datos rechazados
Procesamiento	Las transacciones ingresadas para su procesamiento pueden perderse o ser procesadas incorrectamente	• Duplicación del procesamiento • Falta de controles operativos • Falta de informes de problemas de proceso • Problemas de reenganche de procesos • Problemas de administración de procesos (secuencia)

Principales Areas de Actividad de la A.S.I.

Auditoría del Plan de Continuidad del Negocio

Aspectos a Auditar

Plan de Contingencia

- ✓ Integridad (completo)
- ✓ Divulgación
- ✓ Actualización

Plan de Recuperación

Informe de Control de Sistemas de Información

Objetivos del Informe

Objetivo	Propósito	Medios
Informar	Brindar conocimientos oportunos y apropiados	Clara y comprensible identificación de dificultades y oportunidades de mejora
Persuadir	Lograr aceptación y respaldo de las acciones	Real y persuasivo respaldo de las conclusiones y evidencia de su importancia
Obtener Resultados	Originar Cursos de Acción	Propósitos claros , prácticos y constructivos para realizar los cambios necesarios

Informe de Auditorías de Sistemas de Información

Estructura del Informe

Introducción	Se indica: **Objetivo, Alcance y Posición** de la auditoría frente al objeto auditado
Resultados	Se indica: **Evidencias y hallazgos claves** obtenidos durante la revisión, que sean significativos y que sirvan de base para las conclusiones
Conclusiones	Se expone: el **diagnóstico** en función de los resultados obtenidos. Ordenar: problema y causalidad (causa-efecto) Incluir **siempre** opinión del personal auditado.
Recomenda-ciones	Cursos de acción que se estimen pertinentes. Importante: **participación** del personal auditado
Anexos	Incluir: **El detalle** que respalda los hallazgos y explica el método empleado.

Informe de Control de Sistemas de Información

Pautas para desarrollar el Informe de Auditoría

Aspecto (Qué)	Característica (Cómo)
Directo	Título Informativo Priorizar lo importante Oraciones concluyentes sin enunciaciones elípticas
Preciso	Seleccionar y presentar los temas de mayor importancia Acompañar resúmenes de documentación respaldatoria Realizar una redacción precisa
Persuasivo	Llevar convencimiento con la información que se expone Desarrollar las consecuencias de las situaciones descriptas
Prudente y Constructivo	Propender a una razonable interpretación de los hechos y exponer las causas no los síntomas Presentar una visión del conjunto balanceando lo positivo y lo negativo Trasuntar confianza en el auditado para solucionar el o los problemas
Oportuno	Para lograr la pronta solución de los problemas Anticipar informes en casos de gravedad
Expuesto conforme al destinatario	Resúmenes para los niveles superiores Exposición que potencie la interpretación (relaciones %, tablas, gráficos) Atractivos (presentación, distinta tipografía para resaltar temas)
Orientado a Resultados	Recomendaciones prácticas, factibles y específicas Descripción de los cursos de acción a tomar

Herramientas para Auditoría de TI

TAAC's (Técnicas de Auditoria asistidas por computador)

Son un conjunto de técnicas y herramientas
utilizadas para el desarrollo de auditoria de sistemas informáticos
con el fin de mejorar la eficiencia, alcance y confiabilidad de los análisis.

Proporcionan suficiente evidencia para sustentar observaciones y recomendaciones, lo que obliga a desarrollar destrezas especiales en el uso de estas técnicas, tales como:

- Mayores conocimientos informáticos
- Discernimiento en el uso adecuado de herramientas informáticas y analíticas
- Eficiencia en la realización de los análisis

Sin dejar de lado técnicas tradicionales de auditoria como inspección, observación, confirmación, revisión, entre otros.

Herramientas para Auditoría de TI

Proceso de Auditoría de la Información

1. Si los controles computadorizados son débiles o no existen, los auditores necesitan realizar mas pruebas sustantivas.

Las pruebas sustantivas son pruebas de detalle de transacciones y balanceo de cargas

2. Las pruebas de cumplimiento son realizadas para asegurar que los controles están establecidos y trabajan correctamente.

Esto puede implicar el uso de las TAAC's

Herramientas para Auditoría de TI

Ventajas de las TAAC's

1. Incrementan o amplían el alcance de la investigación y permiten realizar pruebas que no pueden efectuarse manualmente

2. Incrementan el alcance y calidad de los muestreos, verificando un gran número de elementos

3. Elevan la calidad y fiabilidad de las verificaciones a realizar

4. Reducen el periodo de las pruebas y procedimientos de muestreo a un menor costo

5. Garantizan el menor número de interrupciones posibles a la entidad auditada

6. Disminución considerable del riesgo de no-detección de los problemas

Herramientas para Auditoría de TI

Tipos de Software

a) Paquete de auditoria

Son programas generalizados diseñados para desempeñar funciones de procesamiento de datos que incluyen leer bases de datos, seleccionar información, realizar cálculos,
crear archivos de datos e imprimir informes en un formato especificado por el auditor.

Usados para control de secuencias, búsqueda de registros, detección de duplicaciones, selección de datos, revisión de operaciones lógicas y muestreo, algunos de ellos son IDEA, ACL, etc.

Herramientas para Auditoría de TI

Tipos de Software

b) Software para un propósito específico o diseñado a medida

Son programas de computadora diseñados para desempeñar tareas de auditoria en circunstancias especificas.
Estos programas pueden ser desarrollados por el auditor, por la entidad, o por un programador externo contratado por el auditor.
Por ejemplo programas que permitan generar check-list adaptados a las características de la empresa y de los objetivos de la auditoría.

Herramientas para Auditoría de TI

Tipos de Software

c) Los programas de utilería

Son usados por la organización auditada para desempeñar funciones comunes de procesamiento de datos, como clasificación, creación e impresión de archivos.
Ejemplo planillas de calculo, procesadores de texto, etc.

d) Rutinas de auditoria en programas de aplicación

Módulos especiales de recolección de información incluidos en la aplicación y diseñados con fines específicos.
Se trata de módulos que permiten obtener pistas de auditorías en muchos casos generados a través de triggers programados en las propias bases de datos

Herramientas para Auditoría de TI

Tipos de Software

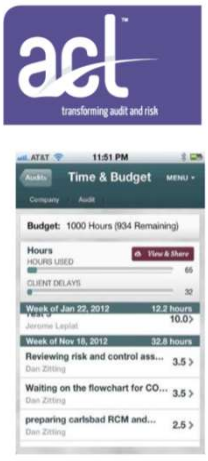
e) Los programas de administración del sistema

Son herramientas de productividad sofisticadas que son típicamente parte de los sistemas operativos sofisticados, por ejemplo software para recuperación de datos o software para comparación de códigos.

Como en el caso de los programas de utilería estas herramientas no son específicamente diseñadas para usos de auditoria.

Existen en el mercado una gran variedad de este tipo de herramientas como por ejemplo los que permiten controlar las versiones de un sistema.

Ejemplo Software para Auditoría TI



ACL Audit Management
www.acl.com

Software para Gestión de Auditorías

CARACTERISTICAS:

- Control integral del proceso de auditoría
- Colaboración con partes interesadas
- Listas de auditoría basadas en riesgo y estándares de la industria
- Dashboard de seguimiento
- Puede funcionar como SaaS *(Software as a Service)*

Ejemplo Software para Auditoría TI

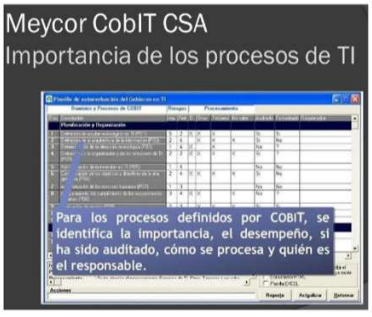
ACL Analytics
www.caseware.com

Software de análisis de datos

CARACTERISTICAS:

- Acceso a múltiples formatos de datos *(Excel, PDF, Oracle, SQL, SAP, ERPs)*
- Análisis exhaustivo de datos
- Automatización de rutinas de auditoría *(calendarización de extracción y pruebas)*
- Puede funcionar como SaaS *(Software as a Service)*

Ejemplo Software para Auditoría TI



Meycor CobiT
www.meycor-soft.com

Apoyo a gobierno de IT basado en COBIT

CARACTERISTICAS:

- Evaluación del cumplimiento de procesos definidos por COBIT
- Gestión de proyectos de auditoría de TI
- Diagnóstico del estado de la organización respecto a la seguridad, calidad, eficacia y eficiencia de TI