ILUMNO

LA AUDITORÍA INFORMÁTICA - CASOS PRÁCTICOS

Elaborado por:

LIC. MARÍA DEL PILAR UGALDE HERRERA. MAF

LA AUDITORÍA INFORMÁTICA

NORMAS INTERNACIONALES DE AUDITORÍA

Las principales normas de auditoría que un auditor de sistemas de información debe dominar, son:

- Normas Internacionales de Auditoría emitidas por IFAC (*International Federation of Accountants*) en la NIA (Norma Internacional de Auditoría o *International Standards on Auditing*, ISA) 15 y 16
- Norma ISA 401, sobre Sistemas de Información por Computadora. SAS No. 94 *(The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement audit)*
- La norma SAP 1009 (Statement of Auditing Practice) denominada Técnicas de Auditoría Asistidas por Computador
  - SAP 1009 los define como programas de computadora y datos que el auditor usa como parte de los procedimientos de auditoría para procesar datos de significancia en un sistema de información.

EL CONTROL INTERNO EN UNA AUDITORÍA INFORMÁTICA Y NIA-401

La NIA-401 establece los procedimientos a seguir para evaluar el control interno cuando se lleva a cabo una auditoría informática, en la evaluación preliminar es muy importante, que el auditor encargado analice el ambiente de control, ya que con este análisis puede determinar los procedimientos a seguir, determinar el riesgo tanto de la auditoría como del auditor, y por último definir las pruebas que utilizará .

Una auditoría de tecnologías de información, permite planificar procesos comunes, roles y actividades con relación y líneas de comunicación que permita mejorar la gestión de servicios TI, es proporcionar una solución que permita una visión de los puntos clave de la Gestión de TI

EL ROL DE LA AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN

El rol de la auditoría es muy significativo, se debe contar con buen dominio del tema para las recomendaciones, para la calidad y eficiencia, ya que la auditoría informativa, permite asegurar el cumplimiento como el monitoreo continuo. En esta y todas las auditorías se debe reportar al más alto nivel como la Junta Directiva, Comité Ejecutivo, Dirección Ejecutiva y la Gerencia de la seguridad de la información. En la siguiente figura 1, Relaciones Gobierno de Seguridad, es donde se establece en cual nivel de gerencia el auditor puede realizar las evaluaciones y la obtención de las pruebas o evidencias.

RELACIONES GOBIERNO DE SEGURIDAD

Nivel de gerencia	Alineamiento estratégico	Gestión del riesgo	Generación de valor	Medición del desempeño	Gestión de recursos	Aseguramiento del proceso
Consejo de dirección	Requerir Alineamiento Demostrable	- Establecer tolerancia al riesgo. - Supervisar una política de gestión del riesgo. - Asegurar el cumplimiento de las regulaciones	Requerir reporte de costos de actividad de seguridad	Requerir el reporte de efectividad de la seguridad	Supervisar una política de gestión de los conocimientos y utilización de los recursos	Supervisar una política de integración del proceso de aseguramiento
Dirección ejecutiva	Responsable de procesos para integrar la seguridad con los objetivos del negocio	- Asegurar que los roles y responsabilidad se incluyan en la administración del riesgo en todas las actividades - Monitorear el cumplimiento regulatorio	Requerir estudios de caso de negocio de iniciativas de seguridad	Requerir el monitoreo y medición de las actividades de seguridad	Asegurar los procesos para la captación de los conocimientos y medidas de eficiencia	Proveer supervisión de todas las funciones de aseguramiento y planes para la integridad
Comité directivo	- Revisar y asistir en la estrategia de seguridad y los esfuerzos de integración - Asegurar que los propietarios del negocio respalden la integración	Identificar los riesgos que surjan, promover prácticas de seguridad de la unidad de negocio e identificar los problemas de cumplimiento	Revisar la adecuación de las iniciativas de seguridad para servir las funciones de negocio.	Revisar y asesorar las iniciativas respecto a seguridad y asegurar que satisfacen los objetivos de negocio.	Revisar los procesos para captación y divulgación del conocimiento	- Identificar los procesos críticos de negocio y los proveedores de aseguramiento. - Dirigir los esfuerzos de integración de aseguramiento.

* Tabla continua en la siguiente página

RELACIONES GOBIERNO DE SEGURIDAD						
Nivel de gerencia	Alineamiento estratégico	Gestión del riesgo	Generación de valor	Medición del desempeño	Gestión de recursos	Aseguramiento del proceso
Gerencia de seguridad de la información	Desarrollar una estrategia de seguridad, supervisar el programa de seguridad y las iniciativas, y vincular con los propietarios de los procesos del negocio para asegurar alineación continua	- Asegurar valoración del riesgo y el impacto sobre el negocio. - Desarrolla estrategias de mitigación del riesgo - Hacer cumplir las políticas y regulaciones	Monitorear la utilización y la efectividad de los recursos de seguridad	Desarrollar e implementar los métodos de monitoreo y medición y dirigir y monitorear las actividades de seguridad	Desarrollar método para la captación y divulgación de los conocimientos y desarrollar métricas de efectividad y eficiencia	- Vincularse con otros proveedores de aseguramiento. - Asegurar que se identifiquen y resuelvan las brechas y las superposiciones.
Promotores de auditoria	Evaluar y reportar sobre el grado de alineación	Evaluar y reportar sobre las prácticas y resultados de la gestión de riegos de la organización.	Evaluar y reportar sobre la eficiencia.	Evaluar y reportar sobre el grado de efectividad de las medidas vigentes y le métrica que está en uso	Evaluar y reportar sobre la eficiencia o la gestión de recursos	Evaluar y reportar sobe la efectividad de los procesos de aseguramiento realizados por diferentes áreas de la gerencia.

Figura 1. Relaciones gobierno de seguridad
Fuente: Elaboración propia con base en Garita, L. (2015) Formación y actualización profesional gobernanza de las TIC y tecnologías afines

EL AUDITOR DE SISTEMAS Y TIPO DE AUDITORÍAS

El auditor informático debe asegurar los responsables de la informática, donde puedan certificar que la estructura establecida se encuentra correctamente, así como la ejecución y el seguimiento. Para esto, le corresponde dominar conocimientos generales como:

- Obtener conocimientos informáticos de manera actualizada y especializada
- Normas estándares para la auditoría interna.
- Políticas organizacionales sobre la información y las tecnologías de la información
- Características de la organización respecto a la ética, estructura organizacional, tipo de supervisión existente
- Normativa legal y de la actividad en la que se desevuelve la empresa, por ejemplo si es una actividad de alimentos, la normativa relacionada con alimentos.

La auditoría informativa, surge de la necesidad de evaluar los sistemas y todo lo relacionado con estos, para que el auditor pueda garantizar que el uso de los recursos es adecuado, o si es del caso, realizar algunas correcciones, así como la evaluación de las funciones, actividades y operaciones que realiza el personal involucrado. Dentro de las auditorías más comunes de sistemas informáticos se encuentran:

AUDITORÍA INFORMÁTICA

Esta auditoría busca realizar la revisión de toda la gestión informática; evalúa los equipos de cómputo, programas y cualquier actividad relacionada con el sistema informático.

AUDITORÍA EN LA COMPUTADORA

Es analizar y evaluar las propias actividades administrativas e informáticas de la empresa, como puede ser su uso, las aplicaciones, entre otros.

AUDITORÍA AL SISTEMA DE CÓMPUTO

Esta auditoría se enfoca en el funcionamiento y el uso correcto de los equipos. Aquí se clasifican las características de los sistemas computacionales en estudio.

AUDITORÍA SOBRE LA SEGURIDAD SISTEMAS

Esta auditoría trata todo lo relacionado con la seguridad en los sistemas, así como las funciones preventivas y correctivas que le permitan a la empresa salvaguardar sus activos, así como identificar si cuenta con planes de contingencia.

AUDITORÍA AL SISTEMA DE REDES

En esta auditoría se debe evaluar la arquitectura, topología, protocolos de comunicación, las conexiones, privilegios y otros.

AUDITORÍA ISO-9000

Esta auditoría únicamente puede ser realizada por un auditor certificado con la ISO-9000, ya que la evaluación se debe realizar con base a los estándares y requerimientos de la norma, como lo es el grado de cumplimiento, si las pruebas generan conformidad o no conformidad, si todo se encuentra debidamente documentado.

Para lograr el objetivo de una auditoría informática es necesario que el auditor utilice una serie de herramientas y técnicas que permitan realizar de manera especializada, evaluar el cumplimiento, verificar el control, seguridad y el seguimiento de las actividades, para lo cual es importante aplicar técnicas como:

- Técnicas de evaluación de riesgos
- Muestreo
- Calculo pos operación
- Monitoreo de actividades
- Recopilación de grandes cantidades de información
- Verificación de desviaciones en el comportamiento de la data.
- Análisis e interpretación de evidencia
- Información de salida

ÁREAS QUE SE DEBEN AUDITAR EN UNA AUDITORÍA INFORMÁTICA

El auditor siempre debe considerar algunos puntos de partida al iniciar la auditoria en sistemas. En esta parte, desde la solicitud o la necesidad que expone la gerencia y lo establecido en las normas de auditoría a (NIAS), generalmente se debe evaluar:

- Hardware:
- Software
- Gestión informática
- Información
- Diseño de los sistemas
- Base datos
- Seguridad del sistema
- Redes de cómputo
- Alguna otra evaluación que sea muy especializada como la ISO-9000, internet, multimedia.

PROGRAMA DE TRABAJO

Establecer el programa permite al auditor mantener un orden de los recursos que le han sido asignados tanto en material, financiero, y permite lograr el conocimiento inicial de las actividades del sistema y evaluarlas en relación con los objetivos de auditoría, a fin de determinar el alcance preliminar y determinar el grado de participación del auditor en cada fase del ciclo de vida del sistema.

EL AUDITOR DEBE TENER UN GRADO DE PARTICIPACIÓN MEDIANTE UN ACUERDO Y REVISIÓN DE LAS FASES.

El auditor debe tener un grado de participación mediante un acuerdo y revisión de las fases.

Acuerdo: Es el acuerdo formal con el contenido del producto tangible. En caso de desacuerdo, la persona responsable de evaluar el producto tangible prepara un memorando indicando su posición y los ítems que requieren solución y lo envía o remite al siguiente nivel superior gerencial.

Revisión: Los productos tangibles son presentados para información solamente; pueden hacerse comentarios, pero ellos no son decisivos.

Revisión de productos finales: Acordar y revisar las actividades y el producto final en cada fase del ciclo de vida del desarrollo del sistema.

Revisar que las firmas de aprobación para todos los productos tangibles están consideradas en el control de aceptación de etapas.

Elaborar los papeles de trabajo para evidenciar y documentar los resultados de la investigación del proyecto.

Identificar las fuentes de información para las revisiones y/o pruebas de auditoría; estas fuentes de información entregan los medios para la revisión y documentación de las actividades de auditoría y verificación de controles.

LISTADO DE VERIFICACIÓN DE AUDITORÍA INFORMÁTICA

Una vez que el auditor tenga definido el tipo de auditoria que realizará, se debe elaborar un listado de verificación, donde pueda dar un valor sea excelente, bueno, regular, mínimo , no cumple, según lo considera, ya que esto es una referencia para determinar posibles hallazgos. En la figura 3, Lista de verificación de auditoría, se puede observar un ejemplo de una auditoría de gestión administrativa y de acuerdo a los valores seleccionados, se puede determinar que se presentan tres hallazgos.

Estos tres hallazgos, según auditor, considera que debe proceder con procedimientos y pruebas en el caso de:

- Se identifican los componentes físicos
- Existen todos los protocolos de comunicación
- Cuenta con un sistema de seguridad

Logo del despacho

Listado de verificación de auditoría de gestión administrativa

Empresa auditada _____

VERIFICACIÓN	EXC	BUENO	REGULAR	MÍNIMO	NO CUMPLE
Cuenta con objetivos la red de cómputo			X		
Tiene claras las características		X			
Se identifican los componentes físicos				X	
Existen todos los protocolos de comunicación					X
Cuenta con un sistema de seguridad				X	

Figura 3. Lista de verificación de auditoría
Fuente: Elaboración propia

FORMATO DE HALLAZGOS DE UNA AUDITORÍA INFORMÁTICA

El utilizar un formato estándar para plasmar las situaciones o hallazgos de la auditoría, permite al auditor una identificación más certera de lo que realizó, así como de la recomendación o propuesta que debe hacer en el informe final. En la figura 4, Papel de trabajo de hallazgos de una auditoría informática, se debe considerar tanto el día que se realiza el hallazgo, quién lo realizó, quién lo supervisó y las posibles propuestas de solución y por qué, además de quién debe ser el responsable del cumplimiento y por último, verificar ese cumplimiento.

Logo del despacho

No hallazgo _____

Empresa auditada _____

Área, programa auditar _____

Fecha _____

REFE #	HALLAZGO	CAUSA	SOLUCIÓN	FECHA SOLUCIÓN	RESPONSABLE	SEGUIMIENTO

Auditor responsable _____

Auditor supervisor _____

Figura 4. Papel de trabajo de hallazgos
Fuente: Elaboración propia

INFORME DE AUDITORÍA

En él se debe informar cuáles son las situaciones encontradas durante la evaluación, así como las posibles causas y sugerencias. Siempre se debe mantener un formato estándar para la presentación de informes, incluyendo:

- Aplicar instrumentos de recopilación.
- Registrar las situaciones encontradas.
- Explicar las situaciones encontradas con los auditados.
- Analizar, depurar y corregir las desviaciones encontradas.
- Presentar informe y dictamen final a los directivos de la empresa.

REFEREMCIAS BIBLIOGRÁFICAS

Isaca org (2012) Cobit 5. *Un marco de negocio para el gobierno y la gestión de las TI de la empresa.* Algonquin Road Suite 1010 Rolling Meadws, IL 60008 E.E.U.U.

Contraloría General de la República. *Normas técnicas para la gestión y el control de las Tecnologías de Información* (N-2-2007-CO-DFOE) San José: Costa rica

Garita, L. (2015). *Gestión de Auditoria en sistemas de información.* Escuela Ciencias Exactas y Naturales, Ingeniería Informática UNED. San José: Costa Rica

McLeod Jr, R. (2000). *Sistemas de información gerencial 7a. ed* Editorial Prentice Hall Hispanoamericana S.A. Mexico DF.

Muñoz, Carlos (2002) *Auditoria en sistemas computacionales.* Editorial Pearson Educación. México DF.

ILUMNO