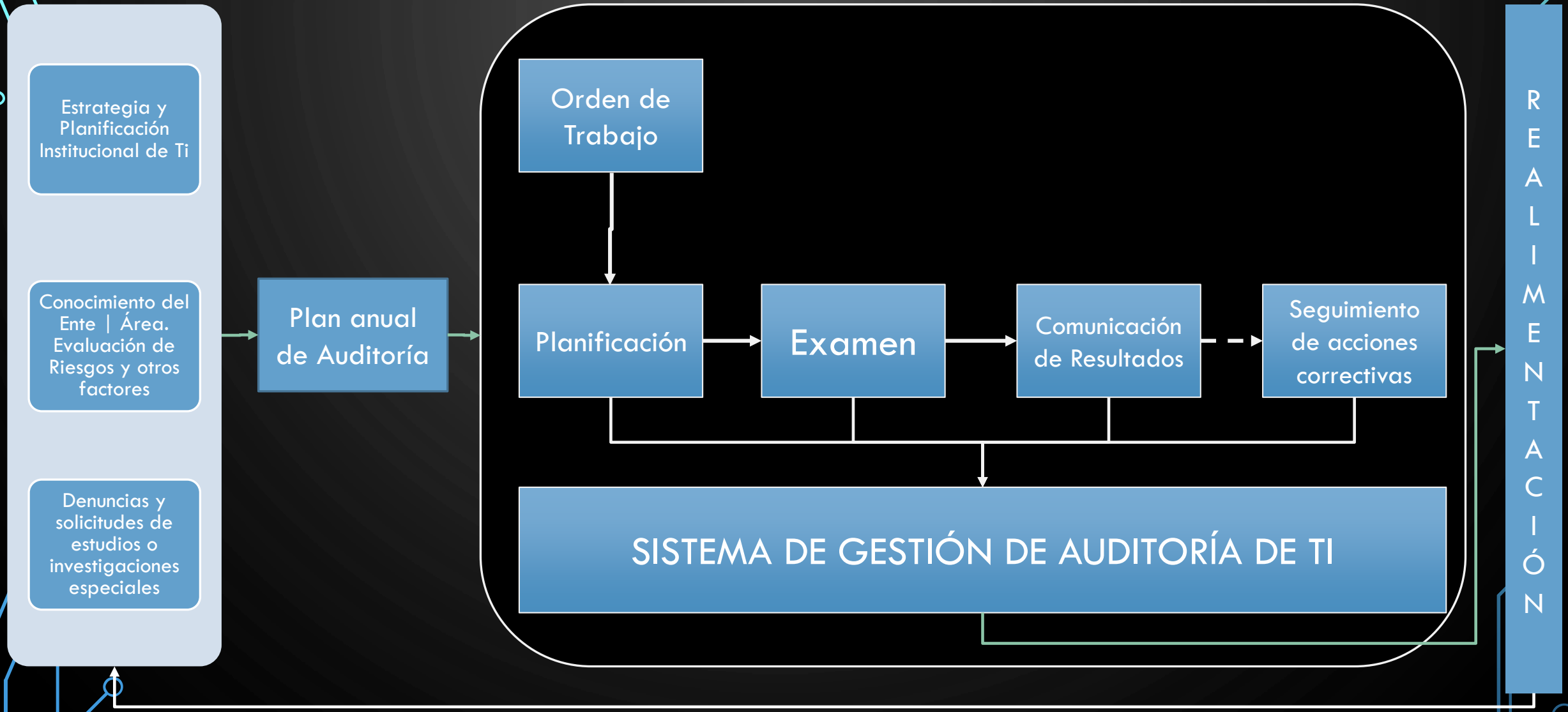
AUDITORÍA INFORMÁTICA

PROFESOR: BAYRON ESPINOZA ORTIZ

AUDITORÍA INFORMÁTICA

- La Auditoría de TI es el PROCESO mediante el cual se evalúa el cumplimiento de los criterios de gestión y control de los recursos tecnológicos de información de una empresa o entidad, con el propósito de concluir sobre el grado de economía y eficiencia en la adquisición y uso y sobre la eficacia para producir información pertinente al negocio, íntegra, correcta, confiable, confidencial y oportuna para la toma de decisiones de la organización, bajo criterios de ética, legalidad y cuidado por el ambiente. Como resultado de este proceso se espera coadyuvar con los miembros de la organización para un desempeño efectivo de sus responsabilidades.

SISTEMA DE GESTIÓN DE AUDITORÍA DE TI



¿POR QUÉ ES IMPORTANTE?

- Para realizar evaluaciones oportunas y completas de la función informática, a cargo de personal calificado, consultores externos, auditores en informática o evaluaciones periódicas realizadas por el mismo personal de informática.
- También es un conjunto de tareas realizadas por un especialista para la evaluación o revisión de políticas y procedimientos relacionados con las diferentes áreas de una empresa:
  - Administrativas
  - Financieras
  - Operativas
  - Informática
  - Crédito
  - Fiscales

CAMPOS DE ACCIÓN

- La evaluación administrativa del área de informática. Esto comprende la evaluación de:
  - Los objetivos del departamento, dirección o gerencia.
  - Metas, planes, políticas y procedimientos de procesos electrónicos estándares.
  - Organización del área y su estructura orgánica.
  - Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
  - Integración de los recursos materiales y técnicos.
  - Dirección.
  - Costos y controles presupuestales.
  - Controles administrativos del área de procesos electrónicos.

CAMPOS DE ACCIÓN

- La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información, lo cual comprende:
  - Evaluación del análisis de los sistemas y sus diferentes etapas.
  - Evaluación del diseño lógico del sistema.
  - Evaluación del desarrollo físico del sistema.
  - Facilidades para la elaboración de los sistemas.
  - Control de proyectos.
  - Control de sistemas y programación.
  - Instructivos y documentación.
  - Formas de implantación.
  - Seguridad física y lógica de los sistemas.
  - Confidencialidad de los sistemas.
  - Controles de mantenimiento y forma de respaldo de los sistemas.
  - Utilización de los sistemas.
  - Prevención de factores que puedan causar contingencias; seguros y recuperación en caso de desastre.
  - Productividad.
  - Derechos de autor y secretos industriales.

CAMPOS DE ACCIÓN

- La evaluación del procesamiento de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones), la cual comprende:
  - Controles de los datos fuente y manejo de cifras de control.
  - Control de operación.
  - Control de salida.
  - Control de asignación de trabajo.
  - Control de medios de almacenamiento masivo.
  - Control de otros elementos de cómputo.
  - Control de medios de comunicación.
  - Orden en el centro de cómputo.

CAMPOS DE ACCIÓN

- La seguridad y confidencialidad de la información, que comprende:
  - Seguridad física y lógica.
  - Confidencialidad.
  - Respaldos.
  - Seguridad del personal.
  - Seguros.
  - Seguridad en la utilización de los equipos.
  - Plan de contingencia y procedimiento de respaldo para casos de desastre.
  - Restauración de equipos y de sistemas.

CAMPOS DE ACCIÓN

- Los principales objetivos de la auditoria informática son los siguientes:
  - Salvaguardar los activos. Se refiere a la protección del hardware, software y recursos humanos.
  - Integridad de datos. Los datos deben mantener consistencia y no duplicarse.
  - Efectividad de sistemas. Los sistemas deben cumplir con los objetivos de la organización.
  - Eficiencia de sistemas. Que se cumplan los objetivos con los menores recursos.
  - Seguridad y confidencialidad.

CAMPOS DE ACCIÓN

- La auditoría en informática debe evaluar todo (informática, organización del centro de cómputo, computadoras, comunicación y programas), con auxilio de los principios de la auditoria administrativa, auditoria interna, auditoría contable/financiera y, a su vez, puede proporcionar información a esos tipos de auditoria. Las computadoras deben ser una herramienta para la realización de cualquiera de las auditorias.

EL AUDITOR: PERFIL REQUERIDO

- Especialización en función de la importancia económica que tienen distintos componentes financieros dentro del entorno empresarial
- Debe conocer técnicas de administración de empresas y de cambio, ya que las recomendaciones y soluciones que aporte deben estar alineadas a los objetivos de la empresa y a los recursos que se poseen
- El auditor debe tener un enfoque de calidad total, lo cual hará que sus conclusiones y trabajo sean reconocidos como un elemento valioso dentro de la empresa

EL AUDITOR: PRINCIPIOS ÉTICOS

- Principio de calidad
- Principio de capacidad
- Principio de comportamiento profesional
- Principio de confianza
- Principio de criterio propio
- Principio de legalidad
- Principio de secreto profesional
- Principio de veracidad
- Principio de información suficiente
- Principio de cautela

CERTIFICACIÓN CISA

- CISA, por sus siglas en inglés, significa Certified Information System Auditor, o en su traducción: Auditor Certificado en Sistemas de Información.
- Esta certificación dada por la organización internacional ISACA (Information Systems Audit and Control Association, o, Asociación de Auditoría y Control de Sistemas de Información) que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control de sistemas de información.

CERTIFICACIÓN CISA

- La certificación CISA es reconocida a nivel mundial que reconocer aptitudes y conocimientos de un profesional en las tareas de:
  - Auditoría en Sistemas de Información.
  - Gobierno y mantenimiento de tecnología de información.
  - Adquisición, desarrollo e implementación de sistemas de información.
  - Operaciones, mantenimiento y soporte de sistemas de información.
  - Protección de activos de información.
- La certificación demuestra la experiencia, habilidades y conocimientos en auditoría, capaz de evaluar las vulnerabilidades, informes de cumplimiento y establecer controles dentro de una empresa.

CERTIFICACIÓN CISA: BENEFICIOS

- Conocimiento y experiencia
- Nivel de conocimientos necesarios para afrontar los retos dinámicos de una empresa moderna.
- Reconocimiento mundial como profesional de auditoría de sistemas de información.
- Combinación de la teoría, el trabajo y la experiencia educativa que proporciona credibilidad en el mercado.
- Ayuda a lograr un alto nivel profesional a través de ISACA para la educación continua y la conducta ética.

CONCEPTOS GENERALES

RIESGO

- Según la RAE, un riesgo es “Contingencia o proximidad de un daño.”, es decir, riesgo es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. Cuanto mayor es la vulnerabilidad mayor es el riesgo, pero cuanto más factible es el perjuicio o daño, mayor es el peligro.

RIESGO DE AUDITORÍA

- Un riesgo de auditoría es aquel que existe en todo momento por lo cual se genera la posibilidad de que un auditor emita una información errada por el hecho de no haber detectado errores o faltas significativas que podría modificar por completo la opinión dada en un informe.
- La posibilidad de existencia de errores puede presentarse en distintos niveles, por lo tanto, se debe analizar de la forma más apropiada para observar la implicación de cada nivel sobre las auditorias que vayan a ser realizadas.

RIESGO INHERENTE

- Este tipo de riesgo tiene ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando.
- Entre los factores que llevan a la existencia de este tipo de riesgos esta la naturaleza de las actividades económicas, como también la naturaleza de volumen tanto de transacciones como de productos y/o servicios, además tiene relevancia la parte gerencial y la calidad de recurso humano con que cuenta la entidad.

RIESGO DE CONTROL

- Aquí influye de manera muy importante los sistemas de control interno que estén implementados en la empresa y que en circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por esto la necesidad y relevancia que una administración tenga en constante revisión, verificación y ajustes los procesos de control interno.
  - Cuando existen bajos niveles de riesgos de control es porque se están efectuando o están implementados excelentes procedimientos para el buen desarrollo de los procesos de la organización.
  - Entre los factores relevantes que determina este tipo de riesgo son los sistemas de información, contabilidad y control.

PRUEBA DE CUMPLIMIENTO

- Es el examen de la evidencia disponible de que una o más técnicas de control interno están operando durante el periodo de auditoría.
- El auditor deberá obtener evidencia de auditoría mediante pruebas de cumplimiento de:
  - Existencia: el control existe
  - Efectividad: el control está funcionando con eficiencia
  - Continuidad: el control ha estado funcionando durante todo el periodo.

PRUEBA SUSTANTIVA

- Stiene como pruebas sustantivas, los procedimientos de auditoría dirigidos o examinados a obtener evidencia de validez y corrección del manejo contable de las transacciones y los estados financieros y detección de errores o irregularidades en ellos.

INSTRUMENTAL BÁSICO

PROGRAMA DE AUDITORÍA

Etapa de examen

- Un programa de auditoría, también llamado plan de auditoría, es un plan de acción que documenta qué procedimientos seguirá un auditor para validar que una organización cumple con las regulaciones de cumplimiento.
- El objetivo de un programa de auditoría es crear un marco que sea lo suficientemente detallado como para que cualquier auditor externo entienda qué exámenes oficiales se han completado, a qué conclusiones se ha llegado y cuál es el razonamiento detrás de cada conclusión

→ Que va hacer, cuando y como?

PAPELES DE TRABAJO

todo lo que el auditor
haga, escriba, capte y evidencia

- Los papeles de trabajo son el conjunto de documentos que contienen la información obtenida por el auditor en su revisión, así como los resultados de los procedimientos y pruebas de auditoría aplicados; con ellos se sustentan las observaciones, recomendaciones, opiniones y conclusiones contenidas en el informe correspondiente.

EVIDENCIA

¿Y Qué es eso?

- En la NIA 500, se define el concepto de Evidencia:
  - Información utilizada por el auditor para alcanzar las conclusiones en las que basa su opinión. La evidencia de auditoría incluye tanto la información contenida en los registros contables de los que se obtienen los estados financieros, como otra información.
- Para que sea valiosa la evidencia, debe contar con las siguientes características:
  - **Relevante** - Cuando ayuda al auditor a llegar a una conclusión respecto a los objetivos específicos de auditoría.
  - **Autentica** - Cuando es verdadera en todas sus características.
  - **Verificable** - Es el requisito de la evidencia que permite que dos o más auditores lleguen por separado a las mismas conclusiones, en iguales circunstancias.
  - **Neutral** - Es requisito que esté libre de prejuicios. Si el asunto bajo estudio es neutral, no debe haber sido diseñado para apoyar intereses especiales.

CARACTERÍSTICAS DE LA EVIDENCIA AUDITORÍA

Competente	• La evidencia es competente si es apta para sustentar satisfactoriamente los resultados de la auditoría.
Pertinente	• La pertinencia significa que la evidencia se ajusta al propósito de los asuntos sujetos a revisión.
Suficiente	• La evidencia es suficiente si no es excesiva ni escasa para sustentar con toda propiedad los hallazgos, conclusiones y las recomendaciones resultantes de la exposición de la evidencia que se realiza en la descripción de los hallazgos.
Relevante	• Que sea importante al lector o interesados

TÉCNICAS PARA LA OBTENCIÓN DE EVIDENCIA

Verbales	• Indagación, encuesta, cuestionario, entrevista • Estudio de Mercados, grupos de enfoque
Oculares	• Observación, comparación, revisión selectiva, rastreo
Documentales	• Cálculos, comprobaciones • Revisión de archivos, lectura y análisis de legislación
Físicas	• Observación de las operaciones • Toma de fotografías y videos
Escritas	• Análisis, tabulación, confirmación, conciliación, solicitudes de información, estadísticas

INFORME DE AUDITORÍA

- Es el resultado del trabajo realizado por el auditor, donde se exponen los hallazgos, recomendaciones sobre los hallazgos para reducir o eliminar dichas situaciones y también están las conclusiones del auditor respecto al trabajo realizado. Por lo general, se incluye un resumen ejecutivo del informe.

ESTRUCTURA DEL INFORME DE AUDITORÍA

- Información introductoria
  - Antecedentes
  - Objetivos de la Auditoría
  - Alcance de la Auditoría
  - Base legal, Objetivos y estructura orgánica de la entidad
  - Principales funcionarios
- Control Interno
- Observaciones de Auditoría
- Conclusiones
- Recomendaciones
- Firmas responsables (únicamente borrador)

INDIZACIÓN

- La indización es el hecho de asignar índices o claves de identificación las cuales permitirán localizar y conocer el lugar exacto donde se encuentra el expediente, este procedimiento representa grandes ventajas para el auditor tales como simplificar: la localización de algún asunto en específico dentro de los papeles de trabajo.