

AUDITORIA DE SISTEMAS

AUDITORIA EN INFORMATICA

Antecedentes Terminología Referencias





Antecedentes

- Inicialmente la informática apoyó las áreas de contabilidad, nóminas, etc., lo que originó la necesidad de conocer y medir dicho apoyo a estas áreas y a toda la empresa.
-> Se origina el proceso de la auditoría a sistemas de información o auditoria de sistemas.
- Luego cubrió las áreas de negocio en todos los niveles, por medio de productos y servicios variados, con el uso de computadoras personales, redes locales, telecomunicaciones y una diversidad de componentes de tecnología, contribuyendo con la integración empresarial.

Estado actual

- Todas las actividades de la sociedad buscan apoyarse en la tecnología informática.
- El control y seguridad de los recursos de informática es una necesidad creciente.
- La Informática se enfocó hacia la sistematización de las áreas de un negocio.
(Tecnologías y Sistemas de Información).
- Tendencia a obtener una solución integrada y actualizada.

- Las entidades deben contar con controles, políticas y procedimientos que aseguren a los niveles directivos, que los recursos humanos, materiales y financieros están adecuadamente orientados a la rentabilidad y competitividad del negocio.
- La improductividad, mal servicio y carencia de soluciones totales de la función informática, fueron, son y seguirán siendo mal de muchas organizaciones.

¿Qué se espera de Informática?

■ SATISFACCIÓN de la demanda de SISTEMAS y TECNOLOGIAS de INFORMACIÓN



- Personas
- Datos
- Aplicativos
- Tecnología
(Hard., Soft., BD, Comunics.)
- Procesos

Problemas:

- Debilidades en la planeación del negocio (informática)
- Resultados negativos (improductividad, duplicidad de funciones, etc) de los SI (Desarrollo, Mantenimiento. Operación).
- Falta de actualización de personal informático.
Capacitación deficiente de los usuarios de los SI
- Deficiente involucramiento de los usuarios en el desarrollo e implantaciones de soluciones informáticas.
- Administración deficiente de los proyectos (Falta de un proceso de *análisis costo/beneficio, metodologías de planeación y desarrollo* no estandarizadas, poco uso de *técnicas formales*, falta proceso formal de *planeación*)
- Involucramiento mínimo de la alta dirección

Importancia de la auditoria en informática

- La tecnología informática es una herramienta que brinda rentabilidad y ventaja competitiva; pero puede originar costos y desventajas si no es bien llevada.
 - *¿Cómo saber si se está administrando y dirigiendo de manera correcta la función informática?*
 - *¿Es necesario auditar o evaluar la función de informática?*
 - *¿Quiénes lo harían?*

- La solución es realizar evaluaciones oportunas y completas de la función informática, a cargo de personal calificado (consultores externos, auditores en informática).
- La función informática se ha convertido en una herramienta permanente y necesaria, en un aliado confiable y oportuno, de los procesos principales de los negocios.
- Es posible auditar la función informática, si se implementan los controles y esquemas de seguridad requeridos para su aprovechamiento óptimo.

- => Evaluar, formal y periódicamente, la función de informática integrada al proceso de negocios.
- La función del auditor no es ser un policía; se orienta a ser un punto de control, confianza y un facilitador de soluciones.
- Orientación del auditor:

“Conducir a la empresa a la búsqueda permanente de la salud óptima de los recursos de informática y de todos los elementos relacionados con ella”.

II. Terminología de la auditoria en informática

Informática

❖ Campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionados con las computadoras y el manejo de la información por medios electrónicos.

Se divide en grandes ramas o se integra a otros elementos tecnológicos y administrativos para fortalecer las empresas.

- Sistemas de información
- Redes y comunicaciones
- Bases de datos
- Desarrollo de sistemas
- Soporte a usuarios
- Planeación informática
- Investigación de nuevas tecnologías

❖ Sistemas de Información:

Conjunto de módulos computacionales organizados e interrelacionados de manera formal para la administración y uso eficiente de todos los recursos (humanos, materiales, tecnológicos, etc.) de un área de la empresa (manufactura, administración, dirección, etc.); para representar los procesos reales y orientar los procedimientos, políticas y funciones inherentes al logro eficientemente las metas y objetivos del negocio.

Pueden orientarse al apoyo de:

- Niveles operativos.
- Niveles tácticos.
- Niveles estratégicos.

❖ Sistemas de Información Estratégicos:

Proporcionan a la alta dirección una serie de parámetros y acciones encaminadas a la toma de decisiones que apoyarán en el seguimiento de la rentabilidad y eficiencia respecto de la competencia.

❖ **Metodología:** Conjunto de etapas estructuradas de manera que brinden a los interesados los parámetros de acción, en el desarrollo de sus proyectos, siguientes:

Plan general y detallado, tareas y acciones, tiempos, aseguramiento de calidad, involucrados, etapas, revisiones, responsables, recursos, etc.

❖ **Técnicas:** Procedimientos y pasos ordenados que se usan en el desarrollo de un proyecto con el propósito de finalizar las etapas definidas en el procesos metodológico, tales como: Análisis de sistemas, Diseño de sistemas, Análisis costo beneficio, Gráficas de control tiempos, etc.

❖ **Herramientas:** Elementos físicos utilizados para llevar a cabo las acciones y pasos definidos en la técnica.

Auditoria

- Proceso formal y necesario para las empresas con el fin de asegurar que todos sus activos sean protegidos adecuadamente.
- Conjunto de tareas realizadas por un especialista para la evaluación o revisión de políticas y procedimientos relacionados con las áreas Administrativa, Financiera, Operativa, Informática y/o de gestión de una empresa.
- Tareas:
 - Estudiar y actualizar permanentemente las áreas susceptibles de revisión
 - Apegarse a las normas, políticas, procedimientos y técnicas de auditoria establecidas por los organismos aceptados a nivel internacional.
 - Evaluación y verificación de las áreas requeridas, por la alta dirección o responsables directos del negocio.
 - Elaboración del informe (debilidades y recomendaciones).

Auditoria en informática

- ❖ Proceso formal ejecutado por especialistas del área de auditoria y de informática; orientado a la **verificación** y **aseguramiento** de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología informática, se lleven a cabo de forma oportuna y eficiente.
- ❖ *Actividades ejecutadas por profesionales del área de informática y auditoria para evaluar el grado de cumplimiento de políticas controles y procedimientos correspondientes al uso de recursos de informática; asegurando que operen en un ambiente de seguridad y control eficientes.*
- ❖ Proceso metodológico cuyo propósito principal es **evaluar** todos los recursos (humanos, financieros, tecnológicos, etc.) relacionados con la función de informática, para garantizar al negocio que éstos operan con criterios de integración y desempeño altamente satisfactorios, que apoyen la productividad y rentabilidad de la organización.

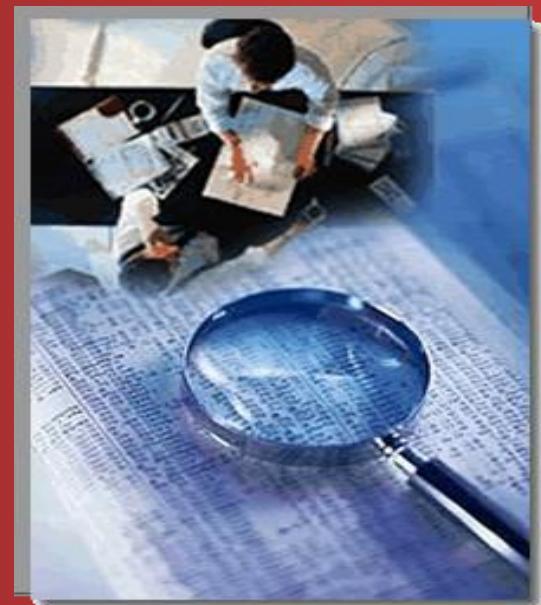
III. La Auditoría en informática y su entorno

1. Entorno en Informática.
2. Objetivos auditor informático
3. Apoyo a la estrategia del negocio.

El Entorno en Informática

Las actividades de una organización afectan sectores específicos de la sociedad; asimismo, los hechos y actividades externas al negocio tienen un grado de impacto en el mismo.
Tales hechos ó factores externos pueden ser:

- Económicos
- Políticos
- Culturales
- Tecnológicos
- Sociales
- Otros.



Los negocios definen estrategias de planeación con las que afrontar los factores externos, para minimizar su impacto negativo o sacar ventaja estratégica de los mismos.

La Auditoría en informática siendo un proceso básico de evaluación y control en el uso de los recursos tecnológicos para el logro de las estrategias; debe contemplar el entendimiento del entorno del negocio como parte de sus actividades primarias.

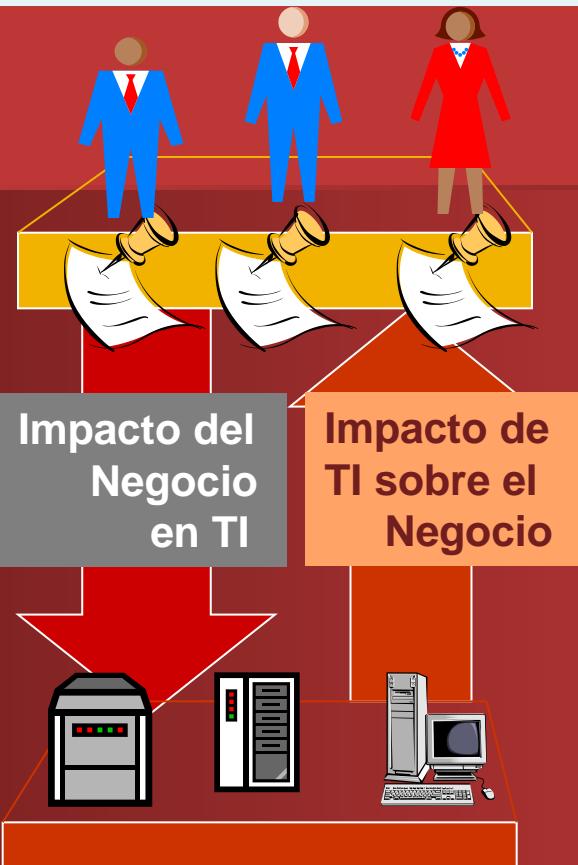
Entorno del negocio (ejemplos)

Factor Externo	Acciones de la empresa	Responsabilidad del auditor informática	Comentarios
Adecuación al uso de nuevos mercados (e-commerce)	Es política de la empresa la expansión y adaptación de los procedimientos y recursos al uso de nuevos mercados	Verificar que los sistemas de información contemplen esta disposición de manera formal y oportuna	Emana como una necesidad, dentro de la globalización
Auge en el uso de las tecnologías de comunicación y computación móviles	Se define como estratégico que exista una red privada virtual entre empresas y entidades de la organización por este medio	Constatar que existe un proyecto de costo-beneficio para desarrollar la infraestructura tecnologica e implementar los servicios de computación móvil que se requieran	Con esta acción se obtiene una ventaja competitiva. Permite una integración más eficiente entre las entidades del negocio.

Alinear TI con el Negocio

OPERACIONES DE TI

- “ Como afectan los cambios y las fallas de TI al Negocio? ”
- “ Cuál es el impacto ? ”
- “ Cuál es el costo para el negocio? ”

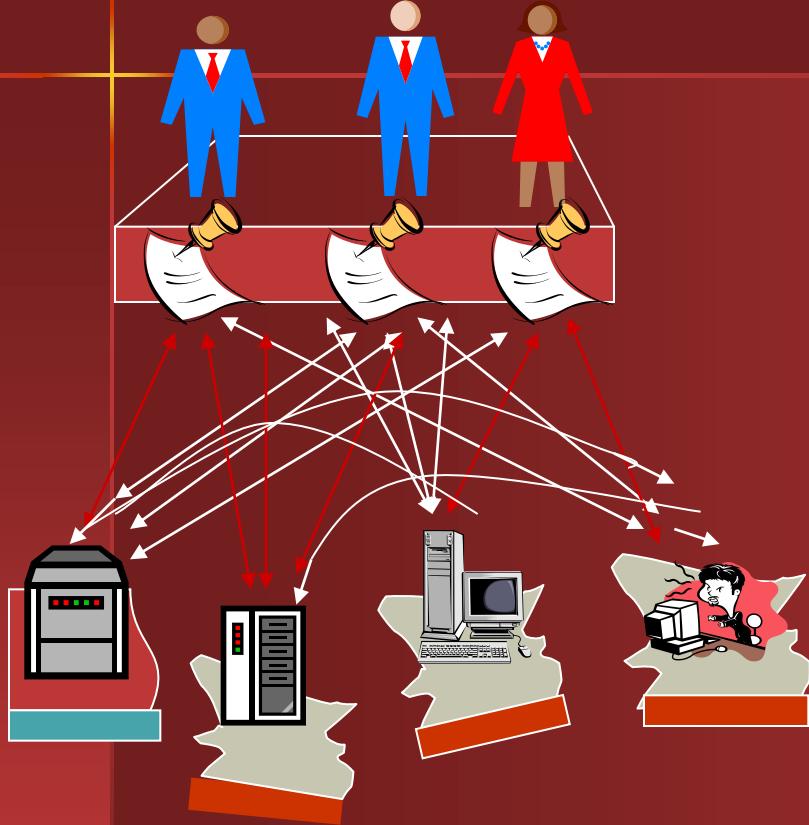


Operaciones del Negocio

- “ Cómo los cambios del Negocio afectan los sistemas de TI ”
- “ TI está listo y capacitado para soportar las iniciativas estratégicas del negocio? ”

“ No hay más proyectos de TI , solo proyectos del Negocio soportados por la Tecnología ”

Adoptar una Perspectiva de Servicio



De: Focalizada en los
Componentes de Tecnología

A : Focalizada en Servicios de TI
Soportando el Negocio



El entorno en la informática (I)

La función de informática debe estructurar sus servicios y proyectos con base en los requerimientos específicos o **estrategias del negocio**, apoyándose en el uso de TICs.

- El auditor en informática deberá verificar la existencia de un análisis costo-beneficio y el empleo de estándares en cada proyecto de inversión orientado a la implementación de nueva tecnología.



El entorno en la informática (II)

- Mantendrá un proceso de seguimiento de los recursos de tecnología, metodologías, técnicas, procedimientos y políticas de informática que aseguren calidad y productividad en esta área.
- Las TICs están desarrollando continuamente soluciones más eficientes; por lo que el área involucrada en su empleo, deberá ejecutar las acciones que aseguren el mejor uso de la información, cumpliendo los requisitos de control esperados: exactitud, totalidad, autorización, actualización, etc. para brindar a la organización resultados eficientes y de calidad.

Principales Controles físicos y lógicos

Autenticidad.- Permiten verificar la identidad (Passwords, Firma digital)

Exactitud.- Aseguran la coherencia de los datos (Validación de campos, Validación de excesos)

Totalidad.- Evitan la omisión de registros así como garantizan la conclusión de un proceso de envío (Conteo de registros, Cifras de control)

Redundancia.- Evitan la duplicidad de datos (Cancelación de lotes, Verificación de secuencias)

Privacidad.- Aseguran la protección de los datos (Compactación, Encriptación)

Existencia.- Aseguran la disponibilidad de los datos (Bitácora de estados, Mantenimiento de activos)

Protección de Activos.- Destrucción o corrupción de información o del hardware (Extintores, Passwords)

Efectividad.- Aseguran el logro de los objetivos (Encuestas de satisfacción, Medición de niveles de servicio)

Eficiencia.- Aseguran uso óptimo de los recursos (Análisis costo-beneficio)

En el entorno de la informática se han desarrollado:

- Mejores equipos de cómputo.
- Lenguajes de programación y aplicaciones de Software más flexibles y dinámicos.
- Innovaciones tecnológicas en redes y telecomunicaciones.
- Metodologías, técnicas y herramientas para la administración de la función informática y la planeación y desarrollo de sistemas.
- Integración de especialidades profesionales en asociaciones reconocidas formalmente.

Concepto	Características	Impacto en el proceso de AI
<p>Hardware</p> <ul style="list-style-type: none"> • Servidores • Redes • Computadoras portátiles • Impresoras • Dispositivos de almacenamiento • Telecomunicaciones <ul style="list-style-type: none"> - datos - voz - video 	<ul style="list-style-type: none"> • Permiten alimentar, procesar, generar, transmitir y almacenar los datos de los SI (estratégicos, tácticos y operativos del negocio) • El Hw sufre cambios de manera dinámica, su desempeño y performance han mejorado : <ul style="list-style-type: none"> ▪ Almacenamiento ▪ Procesamiento ▪ Portabilidad ▪ Escalabilidad ▪ Conectividad ▪ Otros 	<ul style="list-style-type: none"> • Utilización de los equipos de computo para consulta, captura, proceso y generación de reportes a fin de evaluar y diagnosticar la situación de los sistemas. • Evaluación de SI a través de accesos remotos y en línea. • Auditar cada tarea en el lugar de los hechos, • Registrar y monitorear gran cantidad de actividades inherentes al uso de TICs.

Concepto	Características	Impacto en el proceso de auditoria en informática
<p>Software</p> <ul style="list-style-type: none"> • Base y Aplicado • (Herr. Gestión y comunicación) • Especializado Auditoría Seguridad Desempeño • CASE Método Técnicas Herramientas 	<ul style="list-style-type: none"> • Son los elementos lógicos • Permiten la sistematización computacional de los procesos de negocio. • Se ha conseguido la automatización de actividades de desarrollo de sistemas a través de las computadoras y en gran medida la planeación de sistemas. 	<ul style="list-style-type: none"> • El personal de informática, programa rutinas de control y evaluación de procesos en los sistemas o genera reprocesos y respaldos de la información por auditar. • El auditor en informática domina ambos campos – auditoria e informática-, es el enlace ideal para la evaluación de SI y el uso eficiente de todos los recursos, servicios y productos de TICs en el negocio.

Una organización, también está afectada por otros factores del entorno, por lo que se hace necesario que la función de auditoría en informática se mantenga actualizada y enterada de los aspectos que rodean a los negocios.

Es necesario documentarse mediante:

- lecturas de boletines, periódicos o revistas especializadas y acceso a BD nacionales e internacionales
- participación en conferencias, eventos y en asociaciones especializadas
- contacto permanente con proveedores líderes de productos y servicios de la tecnología informática
- análisis permanente de los procesos básicos de negocio y de sus competidores clave.

En general, hay que considerar elementos formales para aplicar oportunamente el cambio organizacional, cultural y tecnológico, que conlleve a facilitar el reposicionamiento y la competitividad del negocio, tales como:

- Planeación estratégica
- Evaluación permanente de los procesos y flujos de datos.
- Reingeniería de negocios, Investigación de mercados.
- Estudio y asimilación del aspecto social, cultural, político, económico y tecnológico del entorno.
- Compromiso de todos los niveles de la empresa con la calidad y satisfacción del cliente.
- Orientar los recursos a los procesos fundamentales del negocio.
- Considerar el recurso humano como la pieza clave de la organización.

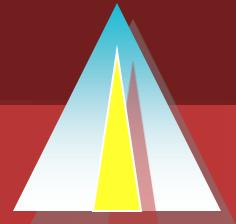
La Dirección de TI



5 dimensiones

Alineamiento estratégico con el negocio

concordantes con visión, misión y lineamientos estratégicos de la organización



Entrega de valor

- de acuerdo a intereses del cliente, considerando costos, plazos y otras restricciones

Gestión de recursos

personas, aplicaciones, información, infraestructura



Gestión de rendimiento

medición, seguimiento y mejora



Gestión de riesgos

identificados, priorizados, cuantificados, comunicados



Factores que propician la Auditoría Informática

- ✓ Leyes gubernamentales.
- ✓ Políticas internas de la empresa.
- ✓ Necesidad de controlar el **uso** de equipos computacionales.
- ✓ Altos **costos** debido a errores.
- ✓ Pérdida de **información** y de **capacidades** de procesamiento de datos, aumentando el riesgo de **toma de decisiones** incorrectas.
- ✓ **Valor** del hardware, software y personal.
- ✓ Necesidad de mantener la **privacidad y confidencialidad de las transacciones** de la organización.



Objetivos generales de la Auditoría en Informática



- Asegurar la **integridad, confidencialidad y confiabilidad** de la información.
- **Minimizar existencias de riesgos** en el uso de Tecnología de información
- Conocer la **situación actual** del área informática para lograr los objetivos.
- **Seguridad, utilidad, confianza, privacidad y disponibilidad** en el ambiente informático, así como también seguridad del personal, los datos, el hardware, el software y las instalaciones.



Objetivos generales de la Auditoría en Informática



- Incrementar la **satisfacción de los usuarios** de los sistemas informáticos.
- **Capacitación y educación** sobre controles en los Sistemas y Tecnologías de Información.
- Buscar una mejor **relación costo-beneficio** de los sistemas informáticos y tomar decisiones en cuanto a inversiones en TICs.

Objetivo del auditor en informática al estudiar el entorno y su impacto en el negocio

- Evaluar y dar seguimiento oportuno a los proyectos de auditoria en informática programados, enfocándose al control, seguridad y auditoría en contacto con las TICs; con el fin de apoyar las estrategias del negocio, considerando los factores externos e internos que se relacionan con la organización.

Garantizar el apoyo directo a las estrategias del negocio (i)

- La Auditoria en informática debe evitar la interrupción de las operaciones del negocio y al mismo tiempo salvaguardar los activos relacionados con las TICs.
- Los auditores en informática dirigirán la participación directa del personal y usuarios involucrados durante el proceso de auditoría.
- Cada proyecto de la auditoría se orienta al cumplimiento de normas, procedimientos y estándares -tanto de auditoría como de informática-, comúnmente aceptados.



Garantizar el apoyo directo a las estrategias del negocio (ii)

- El responsable de la función de auditoría en informática ha de coordinar con:
 - la *alta dirección* (director o gerente general),
 - el *responsable de la auditoría* tradicional (operativa, administrativa, financiera, etc.), y
 - el *responsable de informática*.

IV. ORGANIZACION

1. Estrategias y cursos de acción para la AI.
2. Estructura organizacional y funciones AI.
3. Administración de la función de AI.
4. Elementos de la administración.
5. Hacia una auditoría informática eficiente.

4.1 Estrategias y cursos de acción para la función de AI

- **Estrategias.-**

- 1. Formalizar la AI en la organización, mediante :**

- Documentos de justificación para la Alta Dirección
- Difusión de la AI en las Áreas relacionadas
- Desarrollo del proceso de AI

- 2. Auditoria Permanente para garantizar a la Alta Dirección:**

- Políticas y procedimientos para el uso, eficiente y confiable de los recursos de informática.
- Verificación del uso adecuado de TICs.
- Evaluación y justificación de los Pys Informáticos.
- Planeación informática orientada al plan de negocio.
- Uso de Metodologías, Técnicas, Herramientas.
- Profesionalismo y productividad del personal
- Apoyo a los objetivos del negocio

■ Cursos de Acción (i)

1. Alta Dirección, usuarios y personal deben ser conscientes de la necesidad de AI para el uso eficiente de los recursos.
2. Formalizar un procedimiento que divulgue los planes, objetivos, beneficios y áreas de oportunidad de la AI.
3. Compromiso del personal y usuarios con el proyecto de AI.
4. Planeación y desarrollo del proceso de AI :
Proyectos, Prioridades, Calidad/eficiencia
 - *Justificar expectativas: involucrar áreas
 - *Planear detalladamente: responsables directos
 - *Responsable AI: Presentación ejecutiva
 - *Reunión formal: Jefes de Área, exponer:
 - a) Antecedentes b) Justificación c) Objetivos y alcances
 - d) Etapas e) Productos Terminados f) Fechas de Revisión formales e informales g) Funciones y responsabilidades h) Costes-Beneficios

Cursos de Acción (ii)

5. Coordinar reuniones con los responsables e involucrados.
6. Ejecutar cada PY, de manera formal y oportuna.
7. Informes ejecutivos y detallados a la alta dirección.
8. Investigar, actualizar y formalizar la metodología de AI:
considerar requerimientos, procedimientos y estándares.
9. Capacitar permanentemente al personal de AI.
10. Orientar los esfuerzos al objetivo del negocio.

4.2 Estructura Organizacional y funciones de la AI

■ Ubicación jerárquica de la función

1. La AI es independiente jerárquicamente: control y seguridad.
2. Apoyo y participación de todas las áreas
3. La AI se establece en un nivel Estratégico, nunca Operativo.
4. AI Externa: Seguimiento, coordinación y apoyo alta dirección.

■ Tipos de estructuras donde se ubica la AI

1. En el alto nivel Organizacional
2. Se subordina jerárquicamente a una dirección (administracion/informatica)
3. Objetivo de la Alta Dirección: Asegurar el desempeño oportuno y eficiente de las actividades de AI.

Grado de soporte por parte de la función de auditoria en informática (i)

Nivel	Características	Ventajas	Desventajas
Nivel estratégico	<ol style="list-style-type: none">1. Independencia funcional2. AI opera estratégicamente.3. Compromiso permanente con la alta dirección4. Se halla en instituciones financieras y de gobierno5. Visión del negocio	<ol style="list-style-type: none">1.Comunicación formal y permanente con alta dirección2.Apoyo y soporte constante3. Objetividad en el desempeño de la función4.Se establecen a nivel directivo, las políticas, controles y procedimientos sugeridos por la función de A I	<ol style="list-style-type: none">1. Seguimiento de la alta dirección al desempeño de la función, puede ser un proceso complejo.2. En gran parte de las empresas no se acepta la AI3. Faltan profesionales con experiencia y capacidades requeridas para la función de A I

Grado de soporte por parte de la función de auditoría en informática (ii)

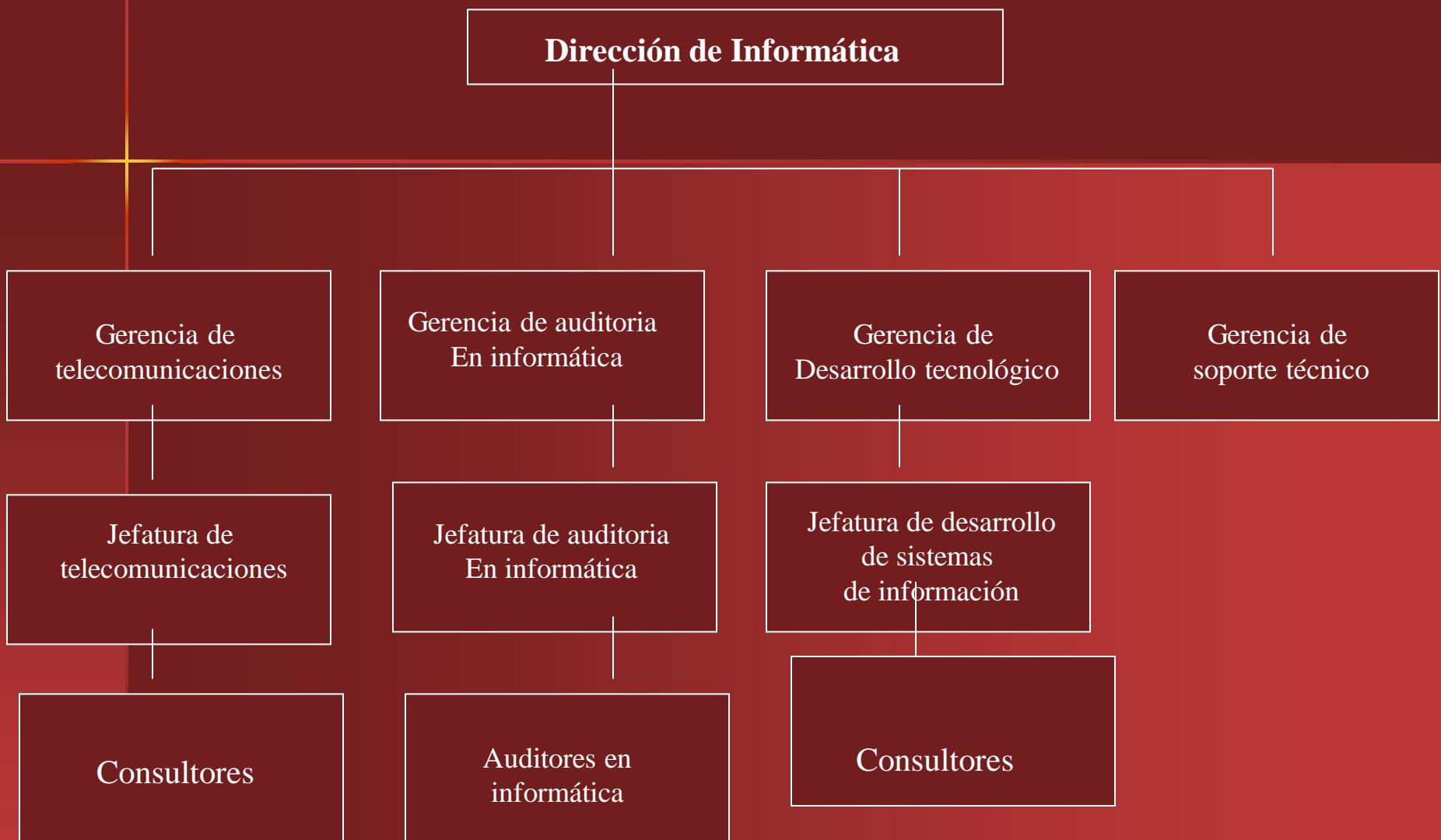
Nivel	Características	Ventajas	Desventajas
Nivel táctico	<p>1.No hay independencia funcional respecto a otras gerencias.</p> <p>2.Se encuentra en diversos sectores, instituciones financieras, gubernamentales, industriales y educativo.</p> <p>3.Limitada al estilo de trabajo del nivel superior al que le reporta.</p>	<p>1. Función indispensable para el cumplimiento de políticas y procedimientos de informática en el negocio.</p> <p>2.Tiene contacto con los responsables para la toma de decisiones.</p> <p>3.Existen asociaciones, consultores y escuelas profesionales que impulsan la formalización de la función.</p>	<p>1. Débil compromiso y soporte de la alta dirección.</p> <p>2. Porcentaje de empresas que considera importante contar con una función a este nivel es mínimo.</p> <p>3. Faltan profesionales con experiencia, técnicas y habilidades .</p>

Funciones de la Auditoría en Informática

- Evaluación, implantación y verificación del cumplimiento de los controles y procedimientos, para el uso eficiente de los recursos y de la función de informática
- Evaluación de las áreas de riesgo de la función de informática y su justificación con la alta dirección.
- Elaborar un plan de auditoria en informática en los plazos determinados.
- Obtener la aprobación formal de los proyectos de AI y difundirlos entre los involucrados para su compromiso.
- Desarrollar la auditoria den informática conforme normas y políticas estandarizadas.
- Administrar o ejecutar eficientemente los proyectos contemplados en el plan de la auditoria en informática.

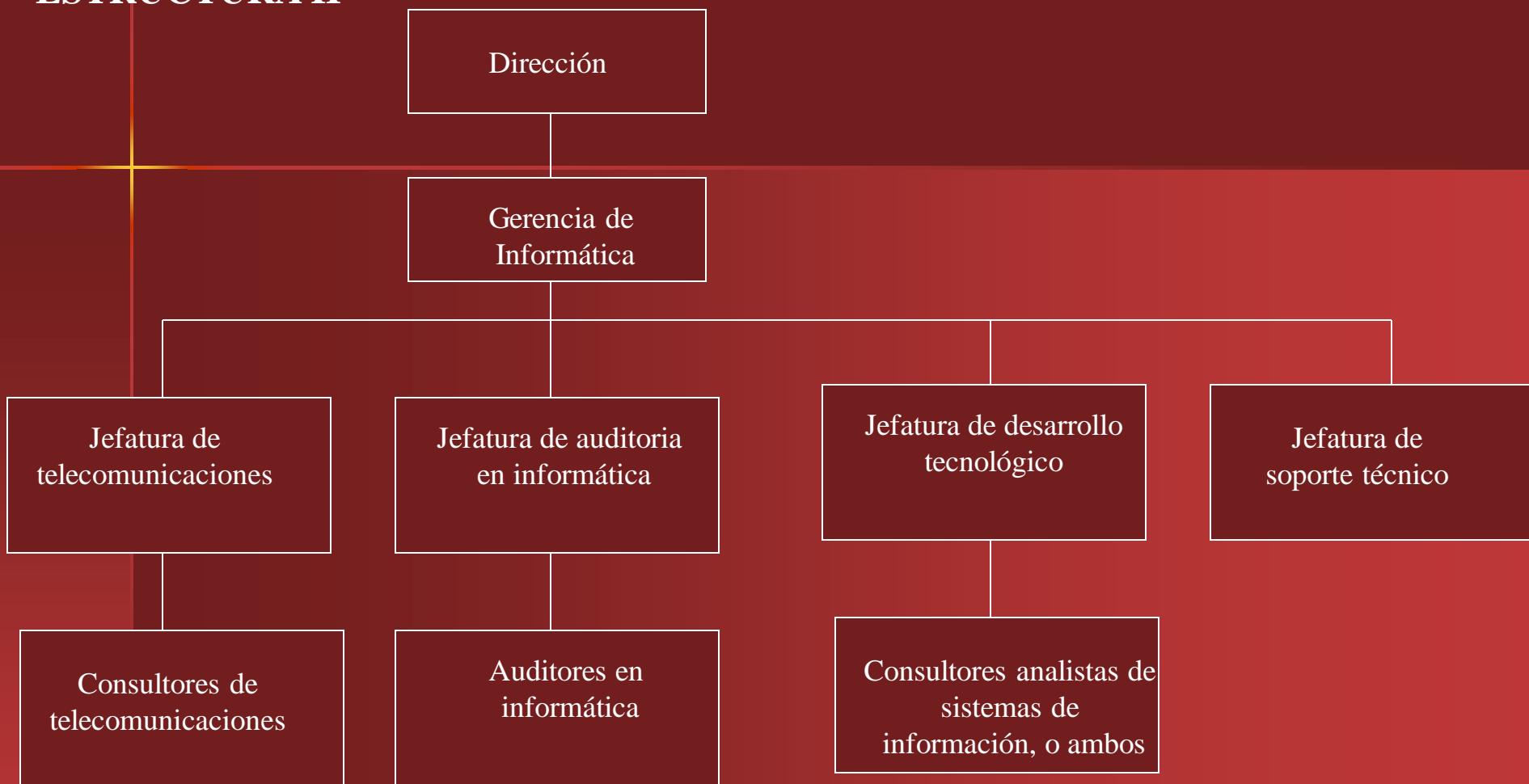
ESTRUCTURA ORGANIZACIONAL DE LA AI

ESTRUCTURA I



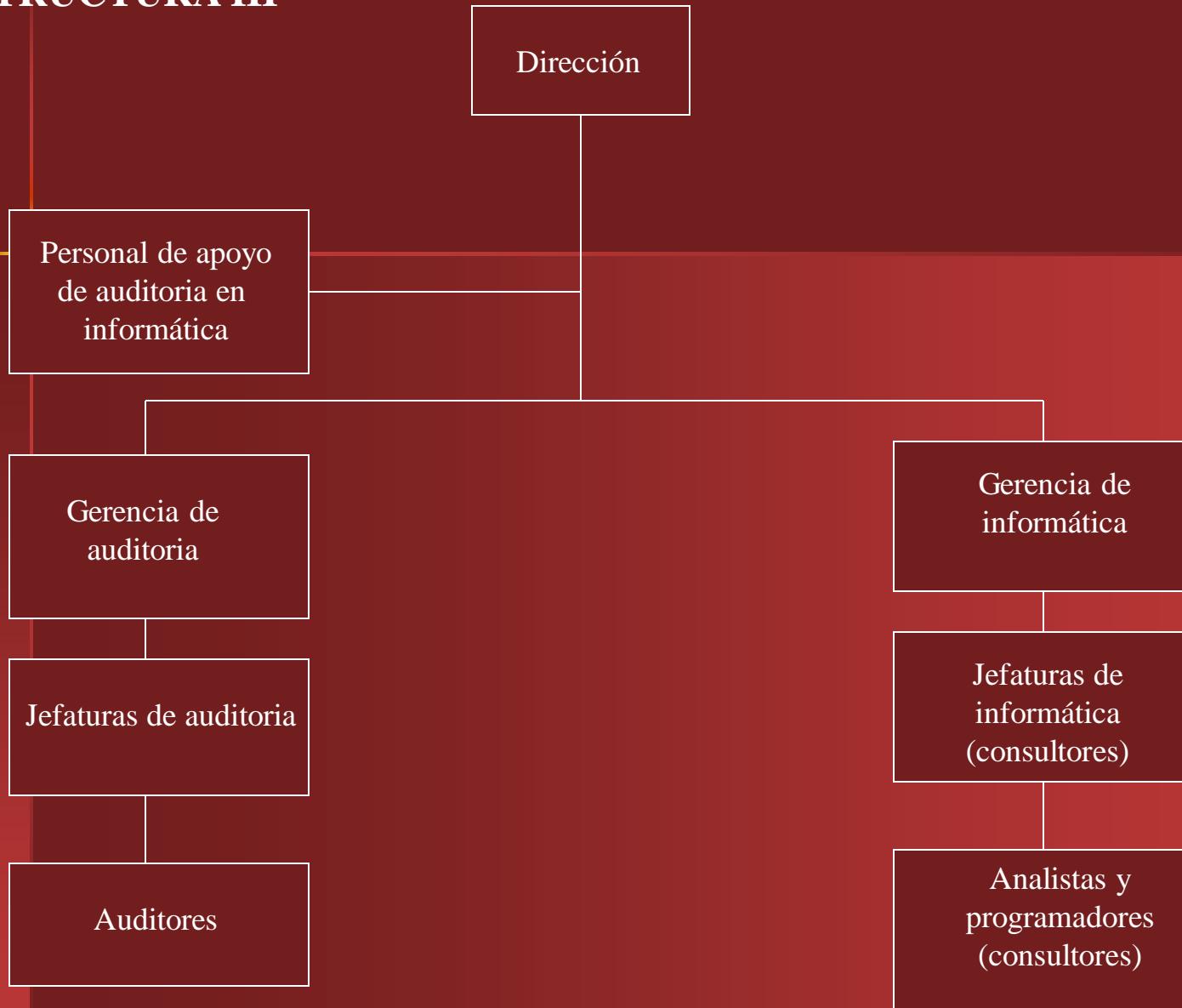
Soporte al director de informática (estructura I)

ESTRUCTURA II



Soporte directo a nivel gerencial de informática (estructura II)

ESTRUCTURA III



Asesoría y soporte a la alta dirección (estructura III)

ESTRUCTURA IV



Soporte directo a nivel gerencial de auditoria (estructura IV)

CLASES Y TIPOS DE AUDITORÍA INFORMÁTICA

- Auditoria informática como soporte a la auditoria tradicional, financiera, etc.
- Auditoria informática con el concepto anterior, pero añadiendo la función de auditoria de la función de gestión del entorno informático.
- Auditoria informática como función independiente, enfocada en la situación actual del entorno informático, en aspectos de seguridad y riesgo, eficiencia y veracidad e integridad.
- Auditoria como función de control dentro de un Departamento de sistemas

Organización de la función de auditoría informática

- La función de Auditoría Informática pasa de ser una función de apoyo a ser una función estratégica en beneficio del negocio.
- El Auditor Informático, es un auditor y consultor empresarial, desempeñándose como analista, auditor y asesor en materia de:
 - Seguridad
 - Control interno operativo
 - Eficiencia y eficacia
 - Tecnología informática
 - Continuidad de operaciones
 - Gestión de negocios

- La ubicación del auditor informático dentro de una organización, debe estar ligada a la de la auditoría interna operativa y financiera, con independencia de objetivos, planes de formación y presupuesto.
- La dependencia organizacional debe ser del máximo responsable operativo de la organización.
- El personal de Auditoría Informática, debe contemplar su certificación CISA o ISACA como auditor informático.
- Una organización interna típica del área de auditoria informática debería considerar:
 - Jefe de departamento
 - Gerente o supervisor de auditoría informática
 - Auditor informático

- El tamaño del área de AI se puede precisar un función de los objetivos de la función.
- Se podría considerar:
 - Especialista en el entorno informático a auditar
 - Especialista en comunicación y/o redes
 - Responsables de gestión de riesgos operativo y aplicaciones
 - Responsables de la auditoria de sistemas de información
 - Especialista para la elaboración de programas de trabajo conjuntos con la auditoría administrativa

4.3 Administración de la Función de Auditoria en informática

Garantiza que los recursos involucrados obedezcan los principios básicos de un proceso administrativo, como: la planeación, el personal , el control y el seguimiento del desempeño.

- Objetivos principales de la administración de AI:
 1. Cubrir y proteger los riesgos informáticos
 2. Asegurar los recursos sean orientados al logro de objetivos
 3. Asegurar la formulación, elaboración, difusión y cumplimiento de las políticas, funciones y procedimientos
 4. Asegurar resultados esperados por el negocio
 5. Para el éxito: Elaborar y formalizar planes, organizar la función, dirigir, revisar y evaluar el desempeño.

Conocimiento o Habilidades requeridas para la función de la Auditoria en informática

Concepto	Responsable de Auditoria	Supervisor de Auditoria	Auditor
Metodología			
•Planeación de sists	Alto	Alto	Bueno
•Desarrollo de sists.	Mínimo	Alto	Alto
Técnicas			
•Análisis			
1.Organizacional	Alto	Alto	Regular
2.Sistemas	Bueno	Alto	Alto
3.Computacional	Regular	Bueno	Alto
•Diseño			
1.Conceptual	Regular	Alto	Alto
2.Computacional	Mínimo	Alto	Alto

•Costo/Beneficio	Alto	Alto	Alto
•Mod. Datos y Procesam.	Mínimo	Bueno	Alto
•Documentación			
1.Ejecutiva	Alto	Alto	Bueno
2.Detallada	Mínimo	Bueno	Alto
•Entrevista	Alto	Alto	Alto
•Cuestionarios	Bueno	Alto	Bueno
•Controles , políticas y estándares	Alto	Alto	Alto
•Áreas de Especializac.			
1. Redes y Comunicaciones	Regular	Bueno	Alto
2. Ing. De Software	Regular	Bueno	Alto
3. Base de Datos	Regular	Bueno	Alto
4. Desarrollo Web	Regular	Bueno	Alto
5.Otros	Regular	Bueno	Alto
•Habilidades/virtudes			
1.Creatividad	Bueno	Bueno	Bueno
2.Abstracción	Alto	Bueno	Bueno
3.Responsabilidad	Alto	Alto	Alto

4.4 Elementos de la administración de la función de AI

■ **Planificación**

1. Desarrollar una matriz de la planeación de AI para determinar las áreas que serán evaluadas.
2. Tener información de los sistemas, equipos, Sw, planes de informática y de auditoria, actuales.
3. Coordinar los planes con Gerencia de Auditoria interna
4. Componentes de éxito de la Planeación:
 - *Juntas formales de discusión de planes periódicas.
 - *Seguimiento de deficiencias y debilidades
 - *Reportes de Auditoria y aseguramiento de calidad
 - *Capacitación conjunta
 - *Metodología, técnicas y herramientas comunes.

■ **Personal**

1. Políticas de selección y reclutamiento
2. Preparación suficiente y confiable Informática/Auditoría
3. Personal con experiencia, educación, adaptabilidad, entendimiento, determinación y diligencia.
4. Establecer el número de auditores y horas de auditoría

■ **Control**

1. Supervisión oportuna garantiza un producto consistente
2. Ayuda en el desarrollo y control de los presupuestos
3. Es un proceso continuo, desde la planeación hasta el informe final
4. Verificación con los estándares y procedimientos.

■ **Reportes de desempeño**

1. Herramientas muy importantes para evaluar:
 - Productividad y calidad de los proyectos
 - Resultados y Avances de los proyectos
 - Áreas susceptibles de control y seguimiento individual y de grupo.

ACTIVIDADES CRITICAS DE LA AUDITORÍA INFORMÁTICA (i)

- Verificación del control interno, tanto de las aplicaciones como de los sistemas informáticos, centrales y periféricos.
- Análisis de la gestión de los sistemas de información desde una vista de riesgo de seguridad y de efectividad de la gestión.
- Evaluación de la integridad, fiabilidad y certeza de la información, a través del análisis de las aplicaciones.
- Análisis del nivel de actualización de las TICs en la organización
- Análisis de la gestión de los riesgos de la información y de la seguridad informática.

ACTIVIDADES CRÍTICAS DE LA AUDITORÍA INFORMÁTICA (ii)

- Verificación del nivel de continuidad de las operaciones (campos de revisión : riesgo de la información, continuidad de las operaciones, gestión del centro de información, efectividad y actualización de las inversiones).
- Diagnóstico sobre la contribución de las aplicaciones y recursos a las necesidades estratégicas y operativas de información de la organización.
- el auditor interno debe convertirse en consultor y apoyo del auditado, sugiriendo procedimientos de control interno, efectividad y eficacia y medición del riesgo empresarial.

4.5 Hacia una Auditoria en Informática eficiente

Clave:

- **Conocimiento, habilidades y capacidades profesionales y personales del auditor informático.**
- **Conocer teóricamente normas, políticas y estándares de auditoría/informática, no son garantía de seguridad y confianza.**
- **Experiencia: Práctica, Disciplina, Orden y Objetividad.**
- **Facultades apropiadas de: análisis objetivo, habilidades de comunicación y modelación conceptual, observación y capacidad para tomar decisiones.**

FUNCION DEL AUDITOR INFORMÁTICO

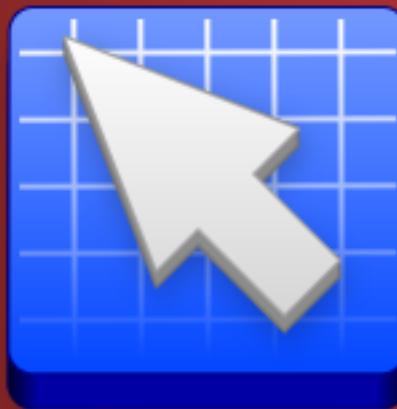
- Un profesional dedicado al análisis de sistemas informáticos, especializado en alguna de las ramas de la auditoría informática e integrado en las corrientes organizacionales actuales.
- Posee las características necesarias para actuar como consultor.
- Puede actuar como asesor de la organización en la que está desarrollando su labor.

Perfil profesional del auditor informático (i)

1. Formación universitaria en informática, que contemple conocimientos en:
 - Desarrollo de sistemas de información
 - Gestión de sistemas.
 - Análisis de riesgos informáticos.
 - Sistemas operativos
 - Telecomunicaciones y Redes locales.
 - Gestión de base de datos.
 - Seguridad informática
 - Operaciones y planificación informática.
 - Gestión de la seguridad de los sistemas de información.
 - Gestión de entornos y proyectos informáticos.
 - Administración de datos, ofimática, herramientas web

Perfil profesional del auditor informático (ii)

- 1.
2. Dominio de las técnicas de auditoria computacional.
3. Actuación anterior en estudios de Auditoría o en auditorias internas.
4. Especialización en función del entorno empresarial, gestion del cambio, calidad total, la importancia económica, etc.
5. Excepcionales condiciones personales para tratar con los sectores auditados.
6. Comunicación adecuada entre el auditado y el auditor.
7. Alta adaptación a los cambios tecnológicos y metodológicos



Tipos de Auditoría

- Auditoría Interna
- Auditoría Externa





Auditoría Externa

- Es realizada por personas afines a la empresa auditada.
- Se presupone una mayor objetividad y credibilidad que en la auditoría interna debido al distanciamiento entre auditores y auditados.

■ Se realiza una Auditoría Externa porque:



- Se necesita auditar un área de gran especialización, para lo que los servicios propios no están suficientemente capacitados.
- Se debe contrastar algún Informe interno en casos de graves hallazgos o conclusiones que afecten la opinión o situación de la propia empresa.
- Se desea tener una visión objetiva en relación a alguna situación problemática, cada cierto tiempo, como salvaguardar información o infraestructura importante, inversión realizada en proyectos, etc.



Auditoría Interna

- Se realiza con recursos materiales y humanos que pertenecen a la empresa auditada, por expresa decisión de esta.
- Puede actuar periódicamente realizando revisiones globales, como parte de su plan anual y de su actividad normal.
- Si es realizada en forma eficiente y objetiva, su resultado y recomendaciones beneficiarán el trabajo de los auditados, dando como valor agregado un servicio de calidad mejorado constantemente.

Ambos tipos de auditoría deben estar ajenos a cualquier tipo de intereses o tendencias sociales, políticas, de la misma empresa, “compañerismo”, filiación, etc.



Control

- Los datos son de los recursos más valiosos de las organizaciones y, aunque intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás activos.

- **Definición :** Controles son todos aquellos mecanismos existentes dentro del sistema y de la organización, que tienen como objetivo asegurar la veracidad e integridad de la información que maneja el sistema tanto aquella que entra y sale de él, como la que se almacena y se manipula internamente dentro del proceso computacional.

Control Interno Informático vs. Auditoría Informática



Análisis de los controles
día a día.



Análisis de un momento informático
determinado

Informa a la dirección informática

Informa a la dirección general de la
organización

Solo personal interno

Personal interno o externo

Alcance de funciones solo
sobre el departamento informático

Cobertura sobre todos los componentes
de los sistemas informáticos de la
organización



CONTROL INTERNO Y AUDITORIA INFORMATICA



El personal debe estar altamente capacitado en lo que concierne a las tecnologías de la información, verificación del cumplimiento de controles internos, normativas y procedimientos establecidos por la gerencia para los sistemas informáticos.

- Un buen control debe contar con las siguientes características:
 - Completo.
 - Simple.
 - Revisable.
 - Adecuado.
 - Fiable.
 - Actualizado.
 - Rentable .

Tipos de Controles Internos

- En general, existen tres tipos de controles que es posible implementar en un sistema:
 - Preventivos
 - Detectores o detectivos
 - Correctivos
- Es necesario definir en qué etapas o procesos del sistema es aplicable cada tipo de control, y qué etapas es necesario controlar.



Tipos de Controles Internos

- **Preventivos** : Evitar el hecho, por ejemplo, los software de seguridad de acceso al sistema.
- **Detectores** : Poder detectar lo antes posible fallas en el sistema, por ejemplo, registro de actividad diaria.
- **Correctivos** : Volver a un estado normal después de una falla, por ejemplo, el mantenimiento de una BD con la réplica existente de respaldo.



CLASES DE CONTROLES

- Controles Generales
- Controles de Aplicación
- Controles Especiales



Controles Generales

- **Definición :** Son los que se realizan para asegurar que la organización y sistemas operen en forma normal.
- **Ejemplos :**
 - Separación de funciones.
 - Acceso y Seguridad.
 - Procedimientos escritos.
 - Controles sobre software de sistemas.
 - Control sobre la continuidad del procesamiento.
 - Control sobre el desarrollo y modificación de sistemas.



Controles de Aplicación

■ **Definición :** Son los que se realizan para asegurar la exactitud, integridad y validez de la información procesada.

■ Ejemplos :

- Control sobre los datos de entrada.
- Control sobre los datos constantes o fijos.
- Control sobre el procesamiento.
- Control sobre los datos rechazados.
- Control sobre los datos de salida.





Controles Especiales

- **Definición :** Son los que se realizan para asegurar la integridad, seguridad y aspectos operacionales.
- **Ejemplos :**
 - Control sobre la entrada de datos en línea.
 - Procedimientos de recuperación y reestablecimiento de sistemas en línea.
 - Control sobre la modificación de programas.
 - Control sobre el procesamiento distribuido.
 - Control sobre sistemas integrados.
 - Control sobre bases de datos.

Principales Controles físicos y lógicos en auditorías

Autenticidad

- Permiten verificar la identidad
- Passwords
- Firmas digitales

Exactitud

- Aseguran la coherencia de los datos
- Validación de campos
- Validación de excesos

Totalidad

- Evitan la omisión de registros así como garantizan la conclusión de un proceso de envío
- Conteo de registros
- Cifras de control





V. PLANEACIÓN

1. Proceso de planeación del negocio.
2. Proceso de planeación en informática.
3. Proceso de planeación de la auditoría.
4. Proceso de planeación de la auditoría en informática.

Planeación

- La función de auditoria en informática debe generar un plan de proyectos que justifique su trabajo durante cierto tiempo, con parámetros lo más tangibles y mensurables posibles.
- Cada proyecto de A I, respalda los objetivos y requerimientos de tres entidades del negocio: Alta Dirección, Auditoria e Informática.

- La comunicación entre la función de auditoria en informática y la alta dirección, así como las direcciones o gerencias de auditoria o informática, son muy importantes .
- Para elaborar un plan maestro de auditoria que asegure un apoyo permanente y eficiente, se debe:
 - Crear un comité de control y seguimiento
 - Analizar los proyectos de negocio en forma conjunta.
 - Establecer fechas de reuniones formales e informales

Proceso de Planeación del Negocio

- Consiste en establecer las metas y cursos de acción del negocio, a través de entrevistas y del análisis detallado de cada uno de los procesos básicos de la organización:
 - Empresa manufactura (producción, ventas, rr. hh., ó administración).
 - Institución financiera (créditos, ahorros y RR.HH.).
 - Otras empresas con giros bien definidos.

- Cualquier entidad, privada o pública, de distintos tamaños y estructura organizacional debe formalizar el plan del negocio, ya que aquí se define el rumbo del mismo.
- Los proyectos que se deriven de este proceso deben contemplar:
 - Se involucre todas las áreas del negocio.
 - Se evalúe el medio externo en sus diferentes entornos.
 - Se apoye en asesores externos o especialistas del negocio.
 - Detectar fortalezas, debilidades, amenaza y oportunidades.
 - Determinar metas y estrategias del negocio.
 - Se establecen a corto, mediano y largo plazo.
 - Son aprobados por los accionistas o responsables del negocio.

Proceso de Planeación en Informática

- Consiste en definir los proyectos relacionados con el área de informática, a corto, mediano y largo plazo.

Cada proyecto debe estar orientado a las metas y estrategias específicas del negocio.

Actividades del proceso de planeación en informática y responsabilidades

Actividad	Responsable de ejecución	Respons. de seguimiento	Comentarios
Determinación de las áreas apoyadas por informática	Coordinador o Supervisor de planeación de informática	Director o gerente de informática	Las áreas se derivan del plan de negocios
Elaboración del plan de informática	Coordinador o Supervisor de planeación de informática	Director o gerente de informática	Involucrarse en cada tarea
Presentación del plan a la alta dirección	Director o gerente de informática	Alta dirección del negocio	Verificar el análisis costo-beneficio de cada proyecto
Ejecución del plan de informática	Funciones de informática: Desarrollo, investigación, otros	Gerente o Supervisores	Funciones hechas por el mismo personal o externos

Proceso de la Planeación de la Auditoría

- Definir un conjunto de proyectos de evaluación y verificación de políticas, controles y procedimientos inherentes a las áreas administrativas, financieras, operativas, etc. del negocio, con objeto de asegurar el buen manejo y administración de los recursos de la organización.
- Los diferentes planes emanados del plan de auditoria son implantados y llevados a cabo en diferentes periodos, de acuerdo con los requerimientos y características del negocio.

Proceso de Planeación de la Auditoría

- Los negocios deben tener un conjunto de políticas, emanadas por la alta dirección, que establezcan la necesidad de contar con una función externa o interna, que asegure la congruencia de todos los estados financieros y contables con las operaciones y transacciones que se realicen en la empresa.
- Esta función debe ser un área de control y aseguramiento, entidad independiente y capacitada.
- La función de auditoria se ocupa de la planeación, ejecución y seguimiento de tales políticas, controles y procedimientos.

Actividades del proceso de planeación de la auditoría y responsabilidades

Actividad	Responsable Ejecución	Responsable Seguimiento
Determinación de las áreas por auditar en el negocio	Coordinador o supervisor de auditoria	Director o Gerente de Auditoria
Elaboración del Plan de Auditoria	Coordinador o supervisor de auditoria	Director o Gerente de Auditoria
Presentación del Plan a la Alta Dirección	Director o Gerente de Auditoria	Alta Dirección del Negocio
Ejecución del Plan de Auditoria	Supervisor o Auditores (externos o internos)	Gerente o Supervisores

Proceso detallado de la Planeación de la Auditoría Informática

- Depende del diagnóstico previo que haga el auditor en informática de la situación que prevalece en cada una de las áreas o servicios de la función de informática.
- El diagnóstico de la situación informática previo, deberá ser breve y objetivo.
- El objetivo principal es determinar las áreas de mayor riesgo de la función de informática con base a diferentes criterios.

Actividades sugeridas para el proceso (i)

- Elaboración, Documentación, Autorización y Difusión Formal del Plan de Auditoria en Informática.
- Identificar el nivel de Riesgo de cada uno de los elementos que integran la función de informática (diagnóstico de la situación actual).
- Las áreas a ser diagnosticadas pueden variar de acuerdo al tamaño y estructura del negocio.

Actividades sugeridas para el proceso (ii)

■ Algunos Servicios:

- Sistemas de Información en operación.
- Administración de Hardware y software.
- Desarrollo de Sistemas de Información.
- Soporte a Usuarios (capacitación, asesoría, etc.)
- Administración de Telecomunicaciones.
- Investigación y desarrollo tecnológico.
- Otros.

Actividades sugeridas para el proceso (iii)

Consideraciones a tener en cuenta para efectuar el diagnóstico de la situación actual:

- El auditor en informática ha de conocer de manera aceptable los aspectos relativos a auditoría e informática que deben tener cada una de las áreas de Informática.
- Se apoyará en la visión de los principales Usuarios del negocio y del responsable de Informática.

Diagnóstico de la Situación actual de los SI en Operación.

- Obtener una lista de los principales SI y de sus usuarios principales.
- Obtener comentarios positivos y negativos de los usuarios de cada SI.
- Registrar fallas más comunes del Sistema.
- Anotar fecha de liberación de Sistemas y su última auditoría.
- Revisar la configuración del equipo donde fue instalado.
- Estudiar su integración a otros SI.
- Evaluar otros aspectos de interés del auditor.

Debilidades que pueden motivar la Auditoria de un SI

- **Primerº:** Que el sistema no haya sido liberado formalmente, lo que ocasiona desconocimiento.
- **Segundo:** Que el sistema nunca haya sido auditado, esto sugiere una auditoria inmediata, intermedia o final.

Clasificación del Nivel de Riesgo que Representa el Uso de Hw y Sw

Los SI y los datos deben ser procesados en un ambiente tecnológico confiable, seguro y eficiente.

- Equipos o Aplicaciones de Sw.
- Mantenimiento de la tecnología del Equipo y Sw.
- Diversos factores motivan la intensidad de la auditoria de Hw.

Evaluación del nivel de Riesgo que representa el uso inadecuado de Productos y Servicios

- Se refiere al grado de conocimiento sobre uso de servicios, Sw y equipos.
- Información de apoyo: Organigramas, descripción de puestos y políticas relacionadas a productos y servicios de informática.
- Se debe determinar el grado de confianza del usuario con el manejo del sistema, paquetes de Sw y equipos.

Otros Aspectos: Telecomunicaciones, redes, automatización de procesos.

- Estos se evalúan en base a los estándares establecidos.
- Considerar la proyección de uso que piensa darle el negocio a corto, mediano y largo plazo.
- Tener en cuenta comentarios de personal especializado en el área.

Clasificación de Riesgos según criterios de la Función de Auditoria en Informática

- Cumplimiento de Estándares.
- Cumplimiento formal de políticas y procedimientos.
- Grado de Satisfacción: Alta Dirección y personal usuario.
- Prioridades de la alta dirección.
- Prioridades de la función de auditoria en informática.
- Otros de interés del auditor.

Elaboración de una matriz de Riesgos

- Muestra las áreas de la función de informática susceptibles de auditoría.
- Resultados en forma descendente.
- Entidades o áreas con mayor y menor riesgo.

Elaboración de un Plan consolidado de Proyectos.

Considera:

- Fechas de inicio y final de cada Auditoria.
- Etapas de cada auditoria.
- Tareas principales de cada etapa.
- Equipo de Trabajo (auditor, representantes, ...)
- Requerimientos (recursos, apoyo, capacitación, ...)

Revisión de la Matriz de Riesgos

- Pronosticar proyectos de auditoria en informática con la gerencia.
- Visto bueno antes de presentarlo a la alta dirección.

Se cubren los siguientes Aspectos:

- Área por auditar, prioridad, Fechas de inicio y final, involucrados, responsables, fechas de revisión y otros.

Presentación del plan de proyectos a la alta dirección.

Finalidad:

- Conocer los proyectos de auditoria informática.
- Verificar la consideración de áreas fundamentales.
- Compromiso de la alta dirección con los auditores.
- Obtener la aprobación del plan de auditoria en informática por parte de la alta dirección.

Realización de cada proyecto de acuerdo con el plan de Auditoria en Informática.

- Ejecución de actividades de seguimiento.
- Revisión formal de cada proyecto.

Integración y formalización de Equipos de trabajo.

Equipos Integrados por:

- Gerente (s) de las áreas usuarias que se evaluarán.
- Gerente de la Función de Informática.
- Líder del proyecto de la función de AI.

Aprobación formal de la alta dirección, del informe final de la auditoría en informática realizada

- Se dará seguimiento oportuno y formal a cada una de las recomendaciones contempladas en dicho informe
- Se aplicarán políticas y controles estandarizados a nivel internacional.
- La implantación del proceso de planeación en auditoría en informática, será permanente.

Tipo de proyectos, responsables e involucrados

Tipo de Proyectos	Responsables	Involucrados
Negocio		
Adquirir empresas	Accionistas	Gobierno, asesores
Reducción de costos	Directores	Gerencias, asesores
Reingeniería	Accionistas, directores	Asesores, gerencias, clientes y proveedores
Informática		
Automatización de oficinas	Informática	Proveedores, áreas usuarias
Red Local	Informática	Proveedores, usuarios de la red
Desarrollo de sistemas	Informática	Áreas usuarias, asesores

Tipo de Proyectos	Responsables	Involucrados
Auditoría		
Financiera	Auditores internos o externos	Áreas de la empresa
Fiscal	Auditores internos o externos	Áreas de la empresa
Operativa	Auditores internos o externos	Áreas de la empresa
Auditoría en informática		
Auditoría a sistemas de información	Auditores en informática internos o auditores externos	Informática, usuarios de los sistemas de información
Auditoría en seguridad	Auditores en informática internos o auditores externos	Informática, áreas usuarios de los recursos de informática
Auditoría en el mantenimiento de Hw y Sw	Auditores en informática internos o auditores externos	Áreas de operación informática y áreas usuarias

Planeación de la AI

- Un proceso formal contiene los siguientes elementos:
 - Etapas
 - Tareas
 - Actividades
 - Costos/Beneficios
 - Resultados esperados por actividad, tarea y etapa
 - Responsables de cada actividad ó tarea
 - Involucrados ó participantes
 - Revisiones Formales e informales
 - Técnicas para ejecutar actividades
 - Herramientas para realizar las actividades

Planeación de la AI

- Requisitos mínimos para que la planeación en auditoría informática sea formal, permanente y exitosa:
 - Involucramiento directo del auditor en informática en el proceso de planeación estratégica
 - Requerimientos
 - Tiempos
 - Prioridades de cada proyecto
 - Compromiso del responsable de auditoría para implementar un esquema de control y seguridad preventivo y completo.

Planeación de la AI

- Participación en el proceso de **planeación de auditoría tradicional**, para hacer control y medidas correctivas.
- Beneficios de la participación, supresión:
 - Riesgos de no planear la auditoría
 - Responsables de tareas inadecuados
 - Falta de compromiso de los involucrados en el proyecto
 - Aparición de costos imprevistos
 - Retrasos en la obtención de beneficios
 - Mala calidad en los resultados
 - Rotación del personal clave
 - Inadecuada segregación de tareas y actividades, Etc.

Dimensiones del Trabajo del Auditor Informático - 1

Revisión de Controles de las Aplicaciones (19%)

- Determinar que los sistemas producen la información a tiempo, exacta y completa

Revisión de Integridad de Datos (13%)

- Compleción, consistencia y exactitud

Revisión de C.V. de Desarrollo (5%)

- Determinar la adherencia a los estándares de CV de desarrollo aceptados

Revisión de Controles Generales de los Procedimientos Operacionales (12%)

- Determinar que las aplicaciones se procesan en un entorno controlado

Revisión de Seguridad (14%)

- Asegurar la protección adecuada de los programas, de los datos y de la instalación de procesamiento de datos

Dimensiones del Trabajo del Auditor Informático - 2

Revisión Software de los Sistemas (5%)

- Determinar el cumplimiento con las políticas de la organización

Revisión de Mantenimiento (6%)

- Determinar que los sistemas se han modificado de acuerdo con las políticas de la organización

Revisión de Adquisición (3%)

- Determinar que los recursos de la organización se están utilizando de forma económica

Revisión de la Gestión de Recursos del Procesamiento de Datos (5%)

- Determinar su adecuación en el cumplimiento de los objetivos organizativos

Gestión de Auditoría Informática (9%)

- Utilizar de forma efectiva los recursos disponibles de la función de la auditoría informática y para cumplir el requisito de auditoría informática de la organización

EVOLUCIÓN DE S.T. I.

VALOR PARA LA EMPRESA

SOCIO
TECNOLÓGICO

PROVEEDOR DE
SERVICIOS

PROVEEDOR DE
TECNOLOGÍA

MADUREZ DEL SERVICIO

STI DEBERÁ FOCALIZAR SU ESFUERZO,
COMO CUALQUIER EMPRESA DE
SERVICIOS, EN LOS 3 NIVELES BÁSICOS
DE SU GESTIÓN:



ALINEAMIENTO
CON EL NEGOCIO

VALOR

SERVICIOS

INFRAESTRUCTURAS

POR QUÉ DE LA GESTIÓN DE S.T.I. COMO UN NEGOCIO

VISION

MISION

ESTRATEGIA ORGANIZACIONAL

OBJETIVOS del NEGOCIO

OPERACIONES

- Planific.
- Gestión

PORTAFOLIO

- Planific.
- Gestión

OPERACIONES
en CURSO

Actividades
recurrentes

PROGRAMAS
y PROYECTOS
autorizados

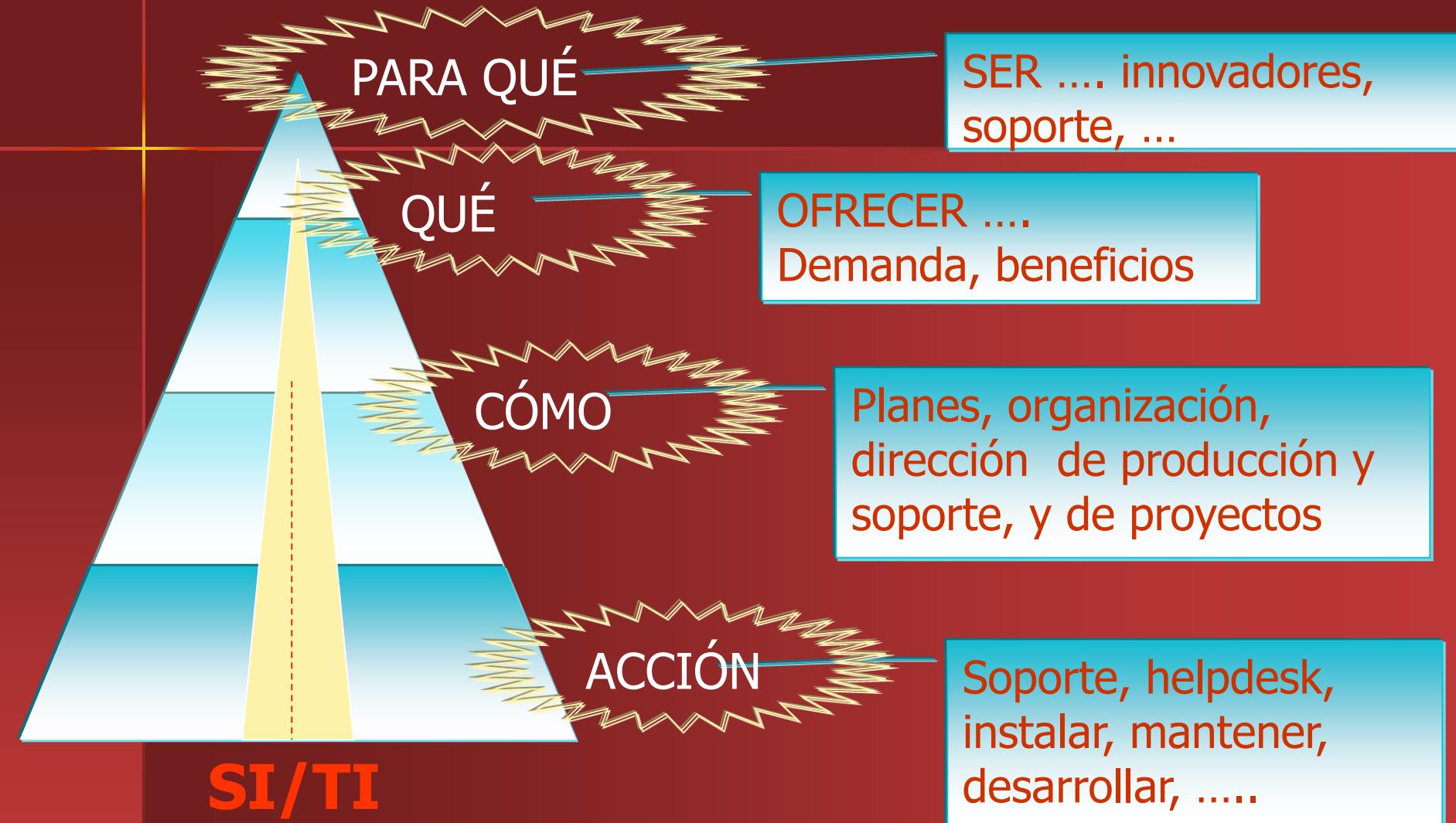
Actividades de
proyectos

Producen
valor

Aumentan capacidad
de producir valor

Productos y Servicios





Probables escenarios de la función de auditoría en informática

Área supeditada	Consideraciones de la función	Ventajas	Desventajas
Dirección o Gerencia de auditoria	<ul style="list-style-type: none">•Independiente de la función informática•Integración de los controles y políticas de informática al resto	<ul style="list-style-type: none">•Objetividad en el desempeño•Planeación y desarrollo conjunto de las auditorías•Control y seguimiento de recursos.	<ul style="list-style-type: none">•No aceptación de la evaluación•Puede desconocer el alcance y misión del área informática.
Dirección o Gerencia de informática	<ul style="list-style-type: none">•Dependencia funcional con el Director•Director: Negociador / impulsador de la AI	<ul style="list-style-type: none">•Se facilita apoyo•Concientización políticas y control•Conocimiento proyecto	<ul style="list-style-type: none">•Incertidumbre por los problemas de la función informática.•Enfoque limitante.

Probables escenarios de la función de auditoria en informática

Área supeditada	Consideraciones de la función	Ventajas	Desventajas
Personal de Apoyo de la Dirección General	<ul style="list-style-type: none">•Responsable: visión negocio•Compromiso, valor agregado•Función estratégica	<ul style="list-style-type: none">•Apoyo Alta dirección•Compromiso formal de las áreas•Justifica perfil AI	<ul style="list-style-type: none">•Alta dirección autoriza y da seguimiento al desempeño informático•Orientan los proyectos Informáticos.
Función de AI Externa	<ul style="list-style-type: none">•Coordina Alta Dirección•Amplia experiencia•Evaluar su desempeño	<ul style="list-style-type: none">•Técnicas y estandares•Nivel profesional+•Independencia/ética•Exige resultados	<ul style="list-style-type: none">•Fugas de información•Mayor costo y tiempo•Soluciones no adecuadas•Compromiso Formal

Resumen i

- Las empresas han tenido durante un tiempo relativamente corto una transición de duros cambios, como son los de pasar de un enfoque (operativo) totalmente manual a otro parcial o íntegramente sistematizado.
- La toma de decisiones hace que una empresa sea líder o una más del montón, es por ello que se necesita de un flujo de información mucho más dinámico y en línea; para posibilitar tomar una decisión correcta en el momento adecuado.

Resumen ii

- La manera de tomar una decisión dejó de ser un proceso intuitivo y basado en la experiencia; para estar basado en una sólida base, fruto de la adecuada información al alcance de los niveles estratégicos, medios y operativo de un negocio.

La administración de toda esta información permitirá encaminar adecuadamente la organización y llevar a cabo cambios para su mejora; con el uso de enfoques, herramientas y técnicas existentes, tales como reingeniería o gestión del conocimiento.

Resumen iii

- Dado que vivimos ante una comunidad global, la tecnología informática y su adecuado tratamiento es pieza clave que debe de ayudarnos a ser miembros dinámicos de esta.
- En este punto el perfil del Auditor de Sistemas se encargará de mantener las metas del negocio basadas en la tecnología.
- Estas metas son: ser líder, mantenerse en el mercado o crecer a corto o mediano plazo a través de la eficiencia de los recursos y la especialización del personal con un enfoque claro de servicio al cliente.

Resumen iv

- Las metas relacionadas con la seguridad y control de la infraestructura tecnológica de las empresas y los canales de información carecen, en su mayoría, de un responsable directo.
 - ¿Qué ocurre con la protección de los recursos una vez realizada cada inversión en informática?
 - ¿Quién implantará y revisará los controles de la información alimentada, procesada, almacenada y distribuida por medio de los recursos tecnológicos?
 - ¿Quién será el facilitador entre lo que debe de ser y lo que se esta haciendo en cuanto a controles preventivos y correctivos que brinden la confianza en la toma de decisiones que emana de los sistemas de información?
 - ¿Quién proporcionará y dará seguimiento formal a la formulación, elaboración, difusión implementación y mejora del plan total de informática?

Resumen v

- *No existe una respuesta clara a esas interrogantes por parte de muchos gerentes.*
- Las funciones de prevención y aseguramiento de la calidad normalmente se dejan de lado en nuestros países; a excepción de grandes corporaciones o el estado en algunos casos.
- La gran mayoría de las medianas empresas no tienen un compromiso claro con el control permanente y la calidad de la empresa. (i.e. dedicando una gerencia a ello, o agrega un área de control de calidad)

Resumen vi

- Es imperativo formalizar una función que revise, evalúe y recomiende acciones de mejora para lograr que cada recurso de informática contribuya a conseguir los objetivos de auditoria en cuanto a información:
 - Totalidad
 - Exactitud
 - Oportunidad
 - Actualización Oportuna
 - Autorización de las transacciones
 - Seguridad
- Finalmente, es importante señalar que para tener una estructura de auditoria informática eficiente y acorde con las necesidades del negocio, se debe considerar la organización de otras dos áreas que serán su punto de referencia: AUDITORIA E INFORMATICA

Resumen vii

Auditoría

- Tareas
- Proyectos de revisión a sistemas de información
- Apoyo requerido para el uso de la informática en las funciones de evaluación y control
- Proyectos
- Otros

Informática

- Servicios
- Puestos
- Funciones
- Equipos de Computo
- Redes y Comunicaciones
- Aplicaciones y Desarrollo de Sistemas
- Proyectos a corto y mediano plazo

Resumen viii

- **La auditoría informática no es un concepto reciente sino data desde tiempos remotos.**
- **El auditor informático no solo puede realizar auditoría informática sino también auditoría de apoyo en otras áreas, como la financiera, donde haya flujo de información.**
- **La función de auditor informático requiere de competencias especializadas en la función informática, conocimientos de auditoria y de gestión empresarial.**

Actividades del proceso de planeación del negocio y responsabilidades

Actividad	Responsable de ejecución	Respons. de seguimiento	Comentarios
Determinación de las áreas de oportunidad para el negocio.	Gerente o coordinador de planeación	Alta dirección o director de planeación	FODA, y proyectos de cada área del negocio.
Elaboración del plan del negocio	Gerente o coordinador de planeación	Alta dirección o director de planeación	Cada proyecto justifica su inversión
Presentación del plan a los accionistas o director general	Director o gerente de planeación	Accionistas o alta dirección del negocio	Se realice al inicio del periodo fiscal y se autoriza formalmente
Ejecución del plan de negocio	Gerente o coordinadores de cada área o proceso básico del negocio.	Alta dirección o gerente de planeación	Cada área ejecuta los proyectos

- El periodo de elaboración o actualización del plan de negocio depende de las estrategias y formalidades que tenga este proceso en cada negocio.
- Después de haber sido aprobado de manera formal por los accionistas, se debe ejecutar con eficiencia y actualizar al menos cada año; de acuerdo con las estrategias y metas del negocio y autorizado por la alta dirección.

Resumen

- El Proceso de Planeación es el pilar de todas las actividades que se ejecutan en la organización

Pérdidas Irreparables - Decepciones

- “Planear es una pérdida de tiempo y un recipiente de buenos deseos”.
- Si no se planea el trabajo, es lógico pensar que tampoco se planean las anomalías y decepciones que dicho trabajo acarreará.

Resumen ii

- **Problema**, proyectos mediano-largo plazo:
- Falta de definición de función, responsabilidad, tiempos y resultados.

“Dejemos de depender de la buena suerte”

- No se vive de buenos deseos sino de metas claras, medibles y factibles.
- **Principal Beneficio:** Poder asegurar, con alto grado de credibilidad, cuánto invertir y cuánto se obtendrá de beneficio; plazos claros y establecidos.