

Auditoría Informática

Prof. César Molina

Ciclo 2018-I

AGENDA

- Introducción al Curso
- Conceptos
- T.G.S.
- La organización
- Tipos de auditoría
- La Empresa como un sistema
- Fase de control
- Examen Parcial

Introducción

- En la actualidad la Informática conforma el apoyo tecnológico más importante en cualquier tipo de Empresa, lo que obliga a tener procedimientos de evaluación y control sobre el proceso administrativo que se ejerce sobre el mismo.
- De acuerdo a lo anterior, la importancia de dar al alumno los conocimientos necesarios sobre las principales metodologías y técnicas para realizar la Auditoría de Sistemas en la organización.

Introducción (cont.)

- Considerando el carácter contralor de la auditoría, ésta tiene tuición sobre todas áreas de la empresa.
- Una de ellas es el área computacional (Sistemas, T.I., etc.) donde, debido al problema de la especialización, fue necesario crear una nueva especialidad: la **Auditoría Informática**, que controla toda la gestión del Centro de Procesamiento de Datos (CPD), incluyendo la parte administrativa de los sistemas de información que de allí se generan y, más en particular, se encarga del control sobre la protección de información.

Introducción (cont.)

- El Departamento de Informática requiere fiscalización similar a la de cualquier otra área de la organización, ya que en ella:
 - Se manejan todos los activos de la empresa.
 - Se generan y almacenan activos de valor muy considerable.
 - Se genera la información operativa y para toma de decisiones.

Concepto de Auditoría (1)

Es un examen crítico para evaluar la eficacia y eficiencia de una sección u organismo.

INEFICAZ + INEFICIENTE

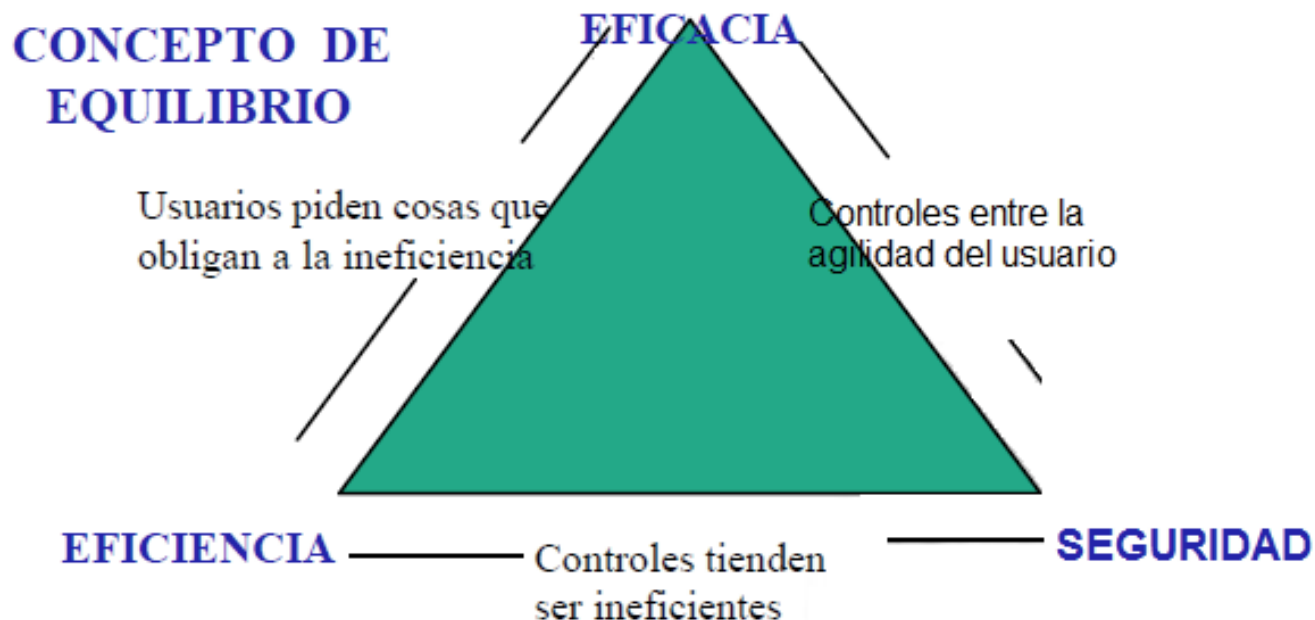
EFICAZ + INEFICIENTE

INEFICAZ + EFICIENTE

EFICAZ + EFICIENTE = **EFFECTIVO**

Objetivos en la Gestión en T.I.

- **Eficacia** - Cumplir requerimientos de usuarios.
- **Eficiencia** - Utilizar recursos en forma óptima.
- **Seguridad** - Mitigar adecuadamente los riesgos.



Factores a considerar...

Necesidad y justificación de una evaluación formal y exhaustiva depende de:

- Importancia estratégica de la gestión para la empresa.
- Nivel de inversión y costo que representa.
- Grado de dependencia operativa.
- Naturaleza de transacciones procesadas.

Síntomas de la necesidad...

- Discrepancia continua entre personal de informática y usuarios.
- Aumentos presupuestarios significativos sin aparente razón.
- Percepción por parte de usuarios de servicio inadecuado.
- Desorientación respecto de acciones futuras a tomar.
- Cambios drásticos o períodos de fuerte crecimiento de la gestión.

Objetivos específicos

Debe considerarse el problema o la decisión principal que dio lugar a la evaluación.

- Solicitud por parte de Informática de ampliar capacidad de equipamiento.
- Problemas empresariales causados por recepción de información inadecuada, poco confiable o inoportuna.
- Solicitud de aumentos en planta de personal.
- Antecedente reciente de falla, error, fraude o siniestro.

Oportunidad de la Aplicación

¿Cuándo debo evaluar y con qué frecuencia?

¿Cuándo se suele evaluar?

- Condiciones de crisis en el procesamiento.
- Después de grandes inversiones.

¿Cuándo se debiera evaluar?

- En cambios gerenciales
- Antes de decisiones importantes
- En cambios estratégicos empresariales

En general la evaluación debiera ser un proceso, no un proyecto.

Razones para Auditar

- Mayor cantidad de funciones dentro de la organización que están siendo computarizadas.
- Existencia de grandes volúmenes de datos que pueden ser accesados por varios programas.
- Implementación de procesamiento de datos distribuidos.
- El uso de computadores personales cuyas características los hacen más vulnerables a la fuga de información.

Definición de Auditoría

La **Auditoría** es un proceso mediante el cual el auditor obtiene evidencias que le permiten formarse una opinión acerca de la responsabilidad de la información elaborada.

La **Auditoría de Sistemas** es la revisión y la evaluación de:

- los controles, sistemas, procedimientos de informática
- los equipos de cómputo, su utilización, eficiencia y seguridad
- la organización que participan en el procesamiento de la información.

Definición de Auditoría (cont.)

- Debe evaluar los sistemas de información, en general, desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.
- Es de vital importancia para el buen desempeño de los sistemas de información, que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.
- Además, debe evaluar todo (informática, organización, *hardware y software*).

I - T.G.S.

1. TEORIA GENERAL DE SISTEMAS (TGS)

La TGS fue creada por el biólogo alemán Ludwig Von Bertalanffy, desde sus trabajos publicados en 1950 hasta su General Systems Theory (1979), con el fin de establecer principios para la unificación de las ciencias.

Sistema: Grupo de elementos interdependientes que forman un todo organizado.

La TGS se fundamenta en tres premisas básicas:

- 📄 La función de un sistema la da su estructura.
- 📄 Los sistemas son abiertos
- 📄 Los sistemas existen dentro de otros sistemas

La interacción del sistema con su ambiente, generan dos fenómenos internos de importancia:

✉ **ENTROPIA:** tendencia al caos, al desorden, al aumento de la aleatoriedad, al desgaste total.

✉ **HOMEOSTASIS:** es el equilibrio dinámico entre las partes del sistema, tendencia de adaptarse para lograr el equilibrio interno.

Existe una tendencia general de los eventos de la Naturaleza en dirección a un estado de máximo desorden.

1. CONCEPTOS PREVIOS

Por su naturaleza los sistemas son:

📄 **Cerrados:** mínimo intercambio con el medio ambiente, con comportamiento determinístico.

✉ Un sistema cerrado evita el aumento de la entropía.

📄 **Abiertos:** constante intercambio y reajuste de sus relaciones con el medio ambiente.

✉ Un sistema abierto posee un continuo flujo de entrada-salida y una adaptabilidad de sus componentes, a través de la homeostasis.

2. LA ORGANIZACIÓN COMO UN SISTEMA

Una organización es un sistema incluido en otro sistema mas amplio que es la sociedad, con la que interactúa influyéndose mutuamente.

Una organización está formada por:

-  **RR.HH.,**
-  **Activos logísticos, y**
-  **Funciones o relaciones**

Morgan (1986) señala que la visión de las organizaciones como totalidades dinámicas es resultado de la Teoría General de Sistemas y de la Cibernética.

2. LA ORGANIZACIÓN COMO UN SISTEMA

Cibernética: es la ciencia de las regulaciones, del mando, del control y del gobierno que permite al sistema mantener su equilibrio dinámico.

Por ello: Lo que estabiliza la funcionalidad de los sistemas es el CONTROL, porque elimina los riesgos.

Control: es todo aquello que anula o minimiza un riesgo, en forma planificada y alineado a los objetivos del negocio. El Control minimiza la entropía.

Riesgo: todo evento que genera o causa daño. Es el que genera la entropía, puede ser:

📄 **Riesgo Inherente** (o de generación aleatoria)

📄 **Riesgo de Control** (o de ausencia de control)

II. TEORÍA DEL CONTROL

II. LA TEORIA DEL CONTROL

1. EL PROCESO DE CONTROL

EL CONTROL:

- Es el proceso para determinar lo que se está llevando a cabo, valorizándolo y si es necesario, aplicando medidas correctivas de manera que la ejecución se lleve a cabo de acuerdo a lo planeado. (George Terry).
- El control es la acción necesaria para asegurar que se están logrando los propósitos, los planes, las políticas y los estándares o normas. (Glenn Welsh).

II. LA TEORIA DEL CONTROL

1. EL PROCESO DE CONTROL

En una organización, el Control es el grupo de normas, técnicas y procedimientos, a través de los cuales se mide y corrige el desempeño de una actividad para asegurar el éxito.

Simbiosis: es la convivencia, en un lugar común, con organismos diferentes en beneficio mutuo.

Bajo este concepto, el Control es el conjunto de actividades reguladoras mediante las cuales los sistemas logran un estado estable (**Homeostasis simbiótica**).

II. LA TEORIA DEL CONTROL

1. EL PROCESO DE CONTROL

El Control posee como características:

- **Estar identificados con el objetivo**
- **Ser económicos**
- **Ser apropiados**
- **Ser sencillos y comprensibles**
- **Ser flexibles**
- **Concentrados en puntos críticos**
- **Deben provocar acción**

II. LA TEORIA DEL CONTROL

2. FASES DEL PROCESO DE CONTROL

El Proceso de Control comprende las siguientes fases:

- **Definición del objeto a controlar**
- **Desarrollo de normas de actuación**
- **Medición y comparación de resultados**
- **Corrección de inconsistencias**

Estas fases o componentes del proceso de control tienen aplicación en cualquier actividad empresarial y/o personal y pueden orientarse a cantidad, calidad, costos y tiempo.

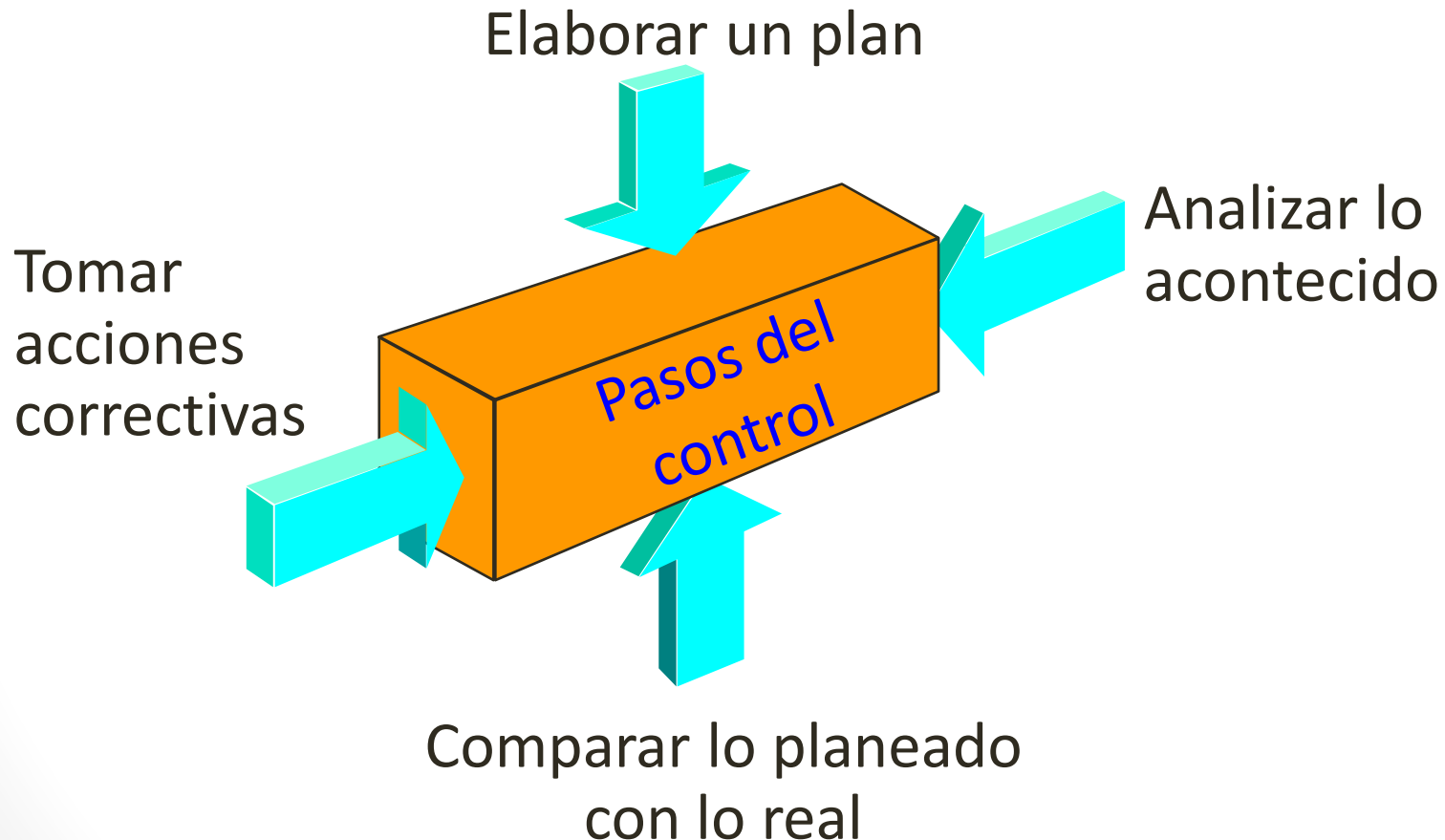
II. LA TEORIA DEL CONTROL

2. FASES DEL PROCESO DE CONTROL



II. LA TEORIA DEL CONTROL

2. FASES DEL PROCESO DE CONTROL



II. LA TEORIA DEL CONTROL

3. EL CONTROL EN EL ESTADO DE DERECHO

El Estado de Derecho es el ejercicio del poder público a través de un régimen de legalidad previamente definido. Posee un sistema de controles que previene, corrige y sanciona las fallas en el ejercicio del poder público.

Comprende:

- **Control Legal:** basado en un ordenamiento jurídico.
- **Control Político:** derivado de los órganos políticos del Estado. (Congreso, JNE, TC, Municipalidad, etc.)
- **Control Gubernamental:** en la mayoría de países americanos, a cargo de una Contraloría General.

II. LA TEORIA DEL CONTROL

4. EL CONTROL EN EL SECTOR PÚBLICO

Tiene como objetivo la protección del patrimonio de la Nación y la garantía de la correcta y legal utilización de los recursos públicos.

Se le denomina Control Gubernamental, y en el Perú está a cargo del Sistema Nacional de Control, presidido por la Contraloría General de la República.

Se clasifica en:

- **Control previo**
- **Control perceptivo**
- **Control posterior**

II. TEORIA DEL CONTROL

5. EL CONTROL EN EL SECTOR PRIVADO

- ✓ **Control Estratégico:** Ejercido por la alta Dirección e implica una visión general de las actividades empresariales. El instrumento técnico de control es el Presupuesto.
- ✓ **Control Táctico:** a cargo de las Gerencias con una visión detallada de las actividades, y actúa sobre las áreas funcionales y operativas. Se basa en el Control Interno.
- ✓ **Control Operativo:** a cargo de la administración de nivel bajo con una visión específica y actúa a nivel operativo. Se ejecuta aplicando Técnicas de Supervisión.

II. LA TEORIA DEL CONTROL

5. EL CONTROL EN EL SECTOR PRIVADO

Las organizaciones privadas, sociales o económicas, establecen sus objetivos y los condicionan con políticas y planes de acción. Estos planes, se detallan en programas que que deben concretarse en hechos coherentes con el objetivo empresarial.

Esta secuencia del proceso Administrativo, se compone de tres tipos de control:

 **Control Estratégico**

 **Control Táctico**

 **Control Operativo**

II. TEORIA DEL CONTROL

5. EL CONTROL EN LA ORGANIZACION



III. AUDITORIA - GENERALIDADES

1. ANTECEDENTES

📄 **En el Tahuantinsuyo:** El Inca para administrar el imperio tenía los Capac Apo (Gobernadores).

Tucuyricuy (el que todo lo ve), realizaba el control y verificaba la información remitida al Inca.

📄 **En el Virreynato:** El Virrey en la Colonia, contaba con el Cabildo, el Corregidor y la Real Audiencia

Oidores (el que todo lo escucha), realizaban el control e informaba al Virrey.


📄 **En la República:** El Estado Peruano cuenta con el Sistema Nacional de Control.


Auditores, realizan el control e informan a las direcciones correspondientes.

III. AUDITORIA - GENERALIDADES

2. CONCEPTOS DE AUDITORIA

 Auditoría es el examen crítico que se realiza con el objeto de evaluar la eficiencia y la eficacia de una organización.

 La Auditoría informática es el examen que verifica la existencia de controles a fin de minimizar o anular los riesgos a los sistemas de información.

 La Auditoría es el examen que tiene como objetivo verificar la existencia de controles internos que permitan anular o minimizar los riesgos de manera eficaz y con base en los objetivos de la empresa.

III. AUDITORIA - GENERALIDADES

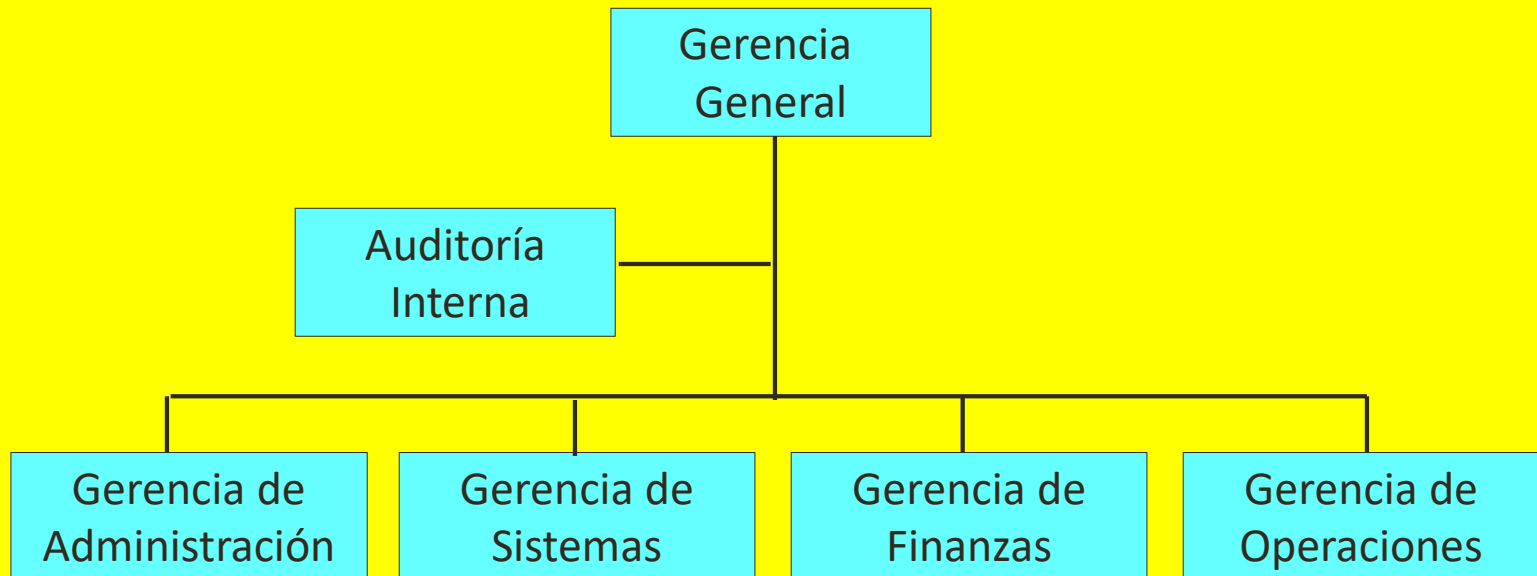
3. TIPOS DE AUDITORIA

- ✓ En razón a su competencia, las auditorias se dividen en dos grandes grupos (Por el sujeto quien lo evalúa):
 - Auditoría interna, y
 - Auditoría externa.
- ✓ La función de auditoría informática puede existir en cualquiera de los citados entornos.
- ✓ La auditoría interna es una evaluación independiente dentro de la organización y depende de la máxima autoridad.
- ✓ La función principal del auditor interno es apoyar a la Dirección en el logro de sus objetivos estratégicos, tácticos y operativos.

III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

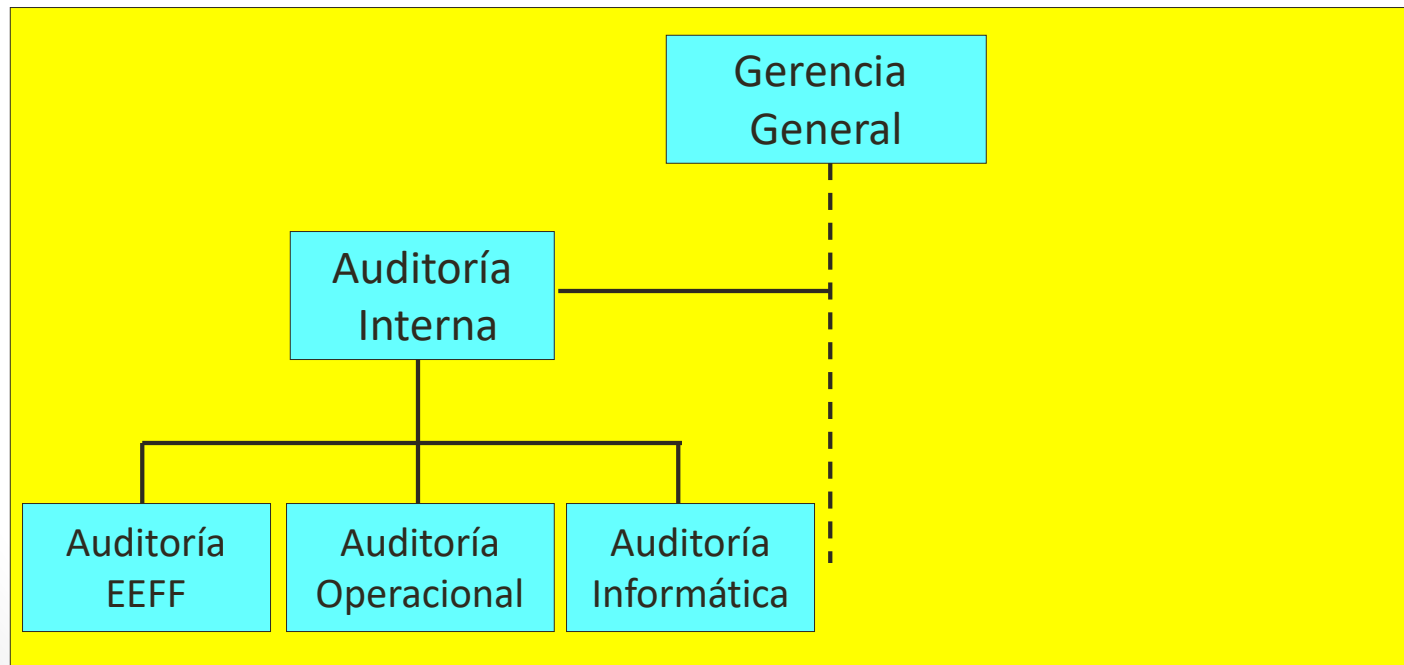
- ✓ La **Auditoría Interna**, dependen únicamente del más alto nivel de dirección.
- ✓ Ejerciendo su acción de control de manera independiente en toda la organización.



III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

- ✓ La **Auditoría Interna**, dependen únicamente del más alto nivel de dirección.
- ✓ Ejerciendo su acción de control de manera independiente en toda la organización.



III. AUDITORIA - GENERALIDADES

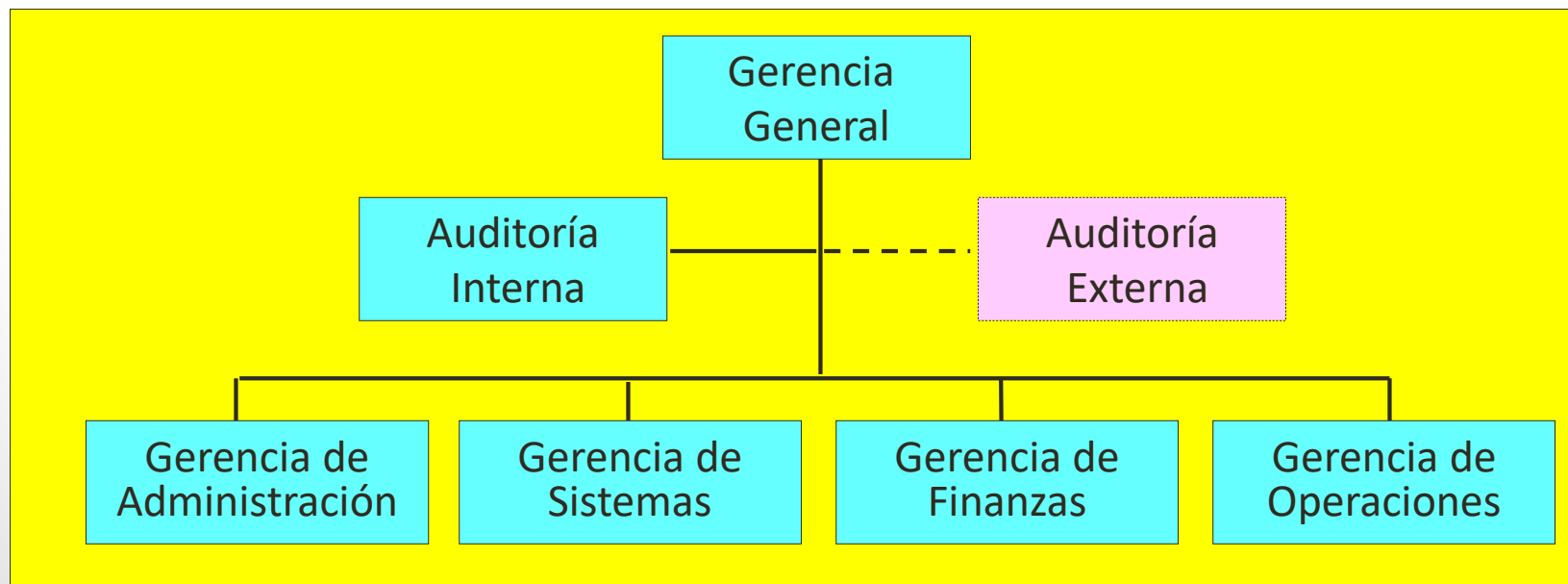
3. TIPOS DE AUDITORIA

- ✓ La auditoría externa es una evaluación independiente y es externa a la entidad que se examina.
- ✓ En la mayoría de las empresas, se realiza anualmente una auditoría de los EE.FF. por parte de una empresa auditora externa, bien voluntariamente o bien por obligación legal.
- ✓ El objetivo principal de una auditoria externa es tener una opinión independiente respecto de la calidad de los estados financieros y/o de la gestión de la entidad.

III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

- ✓ La **Auditoria Externa** reporta al Sistema Nacional de Control, informando únicamente al más alto nivel de dirección.
- ✓ Coordina su acción de control de manera independiente en toda la organización, y sus conclusiones las deriva a la Auditoría Interna.



III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA - Los grandes externos

- Arthur Andersen
- Arthur Young & Co.
- Coopers & Lybrand (hasta 1973 Cooper Brothers (Reino Unido) y Lybrand, Ross Bros., & Montgomery (EE.UU.)
- Ernst & Whinney (hasta 1979 Ernst & Ernst (EE.UU.) y Whinney Murray (Reino Unido)
- Deloitte Haskins & Sells (hasta 1978 Haskins & Sells (EE.UU.) y Deloitte & Co. (Reino Unido)
- Peat Marwick Mitchell (Peat Marwick y KPMG)
- Price Waterhouse Coopers
- Touche Ross

III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

Diferencias entre auditoria interna y externa:

- La interna es realizada por personas de la misma empresa, mientras que la externa exige, como condición esencial de credibilidad, que los profesionales no formen parte de la empresa.
- Generalmente, los objetivos de la externa es expresar una opinión sobre los EE.FF. y su gestión, mientras que los objetivos de la auditoría interna son múltiples y variados, no limitándose sólo a una área.

III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

Diferencias entre auditoria interna y externa:

- En la auditoría interna, el sujeto que la realiza es un empleado de la empresa; mientras que en la auditoría externa, es un profesional independiente.
- En la auditoría interna, la independencia está limitada; mientras que en la auditoría externa, la independencia es total.
- En la auditoría interna, la responsabilidad del sujeto que la realiza es de tipo laboral; mientras que en la auditoría externa, es de tipo profesional, que puede llegar a ser penal.

III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

Diferencias entre auditoria interna y externa:

- En la auditoría interna, el objetivo de la auditoría es el examen de la gestión; mientras que en la auditoría externa, el objetivo es el examen de los estados financieros para determinar si representan la situación real de la entidad auditada.
- En la auditoría interna, el informe emitido es un informe con recomendaciones para la gerencia; mientras que en la auditoría externa, está dirigido también a terceros.
- En la auditoría interna, el uso del informe está restringido al ámbito de la propia empresa; mientras que en la auditoría externa, el uso trasciende la propia empresa.

III. AUDITORIA - GENERALIDADES

3. TIPOS DE AUDITORIA

Diferencias entre auditoria interna y externa:

- Ambos tipos de auditoría no son excluyentes. El auditor externo debe tener en cuenta el trabajo efectuado por el auditor interno a la hora de fijar la naturaleza y extensión de los procedimientos.
- Se debe establecer una colaboración entre ambos. Con este propósito, el auditor externo debe considerar la objetividad y competencia de los auditores internos y evaluar el trabajo realizado por los mismos.

III. AUDITORIA - GENERALIDADES

3. CLASES DE AUDITORIA

- ✓ Las auditorías se pueden clasificar en:
 - Financieras,
 - Verificativas o de cumplimiento,
 - Operativas o de Gestión,
 - Técnicas o de métodos,
 - Informáticas.
- ✓ Es admisible que existan otros enfoques, atendiendo a su finalidad específica.

III. AUDITORIA - GENERALIDADES

4. BASE JURIDICA EN EL PERU

En el Perú, se han creado normas a fin de dar solución en la sociedad peruana, a los problemas que en ella genera el control de la Información. Por ejemplo:

📄 La Ley del Habeas Data o Derecho a la Intimidad e Informática (Ley 26470 y Ley 26301).

📄 Ley 29733 – Ley de Protección de Datos Personales

📄 Las Disposiciones sobre Protección Jurídica del Software (Decisión 351, R.S. 001- 89 y R.S. 01- 94).

📄 El Valor Probatorio del Documento Informático (D. L. 768 y D.L. 681).





📄 Las Normas Técnicas de Control Interno y su Norma 500 “Normas de Control para Sistemas Computarizados”.

📄 Las Normas y Recomendaciones dictadas por el INEI como órgano rector en el ámbito informático, etc.

III. AUDITORIA - GENERALIDADES

4. BASE JURIDICA EN EL PERU

Asimismo, existen Normas Técnico-Administrativas que enmarcan el accionar de toda organización; definiendo las funciones, responsabilidades y procedimientos de cada trabajador. Las principales son:

-  El Reglamento de Organización y Funciones (ROF)
-  El Manual de Descripción de Puestos (MOF)
-  Las Políticas, Estándares, Normas y Metodologías implantadas en la empresa
-  Las Directivas, Procesos y Procedimientos para el control de procesos.

III. AUDITORIA - GENERALIDADES

Ejemplo 1: El Banco “A” y su Problemática

Entorno: El Banco “A” está con problemas con el sector financiero, que generó un masivo retiro de ahorros y juicios de embargo a las cuentas de sus dueños y directivos.

Delito: Para minimizar los embargos judiciales a las cuentas de sus dueños, algunos gerentes del Banco “A” coordinan con la Gerencia de Sistemas, la simulación con fecha atrasada de fuertes retiros de dinero, generando las respectivas pistas de auditoría en sus S/I.

Pista de Control: La información sobre las cuentas remitida en meses anteriores a la CONASEV, era diferente a la que arrojaba el sistema informático.

(El Valor Probatorio del Documento Informático)

III. AUDITORIA - GENERALIDADES

Ejemplo 2: El Banco “B” y el Pago de Interés

Entorno: Las altas tasas de interés en ahorros que se daban, creaban constantes cambios en el aplicativo de Ahorros que estaba en Area de Producción.

Acción: El Jefe de Sistemas, para agilizar los procesos ordena que el mantenimiento y la explotación del aplicativo de Ahorros sean realizadas por la misma persona que da el mantenimiento.

Delito: El programador a cargo de las modificaciones y de la explotación coloca en los programas, altos intereses y favorece a 12 cuentas de sus familiares previamente aperturadas.

Pista de Control: Auditoría detecta el delito por muestreo. *Si el programador hubiera cancelado las cuentas nadie lo descubriría*, porque el Programa de Auditoría sólo analizaba las cuentas activas. (La adecuada separación de funciones)

III. AUDITORIA - GENERALIDADES

5. CONCLUSIONES

Si la Auditoría informática es el examen que verifica la existencia de controles internos que minimicen o anulen los riesgos a los S/I, y así alcanzar la eficiencia y la eficacia de una organización.

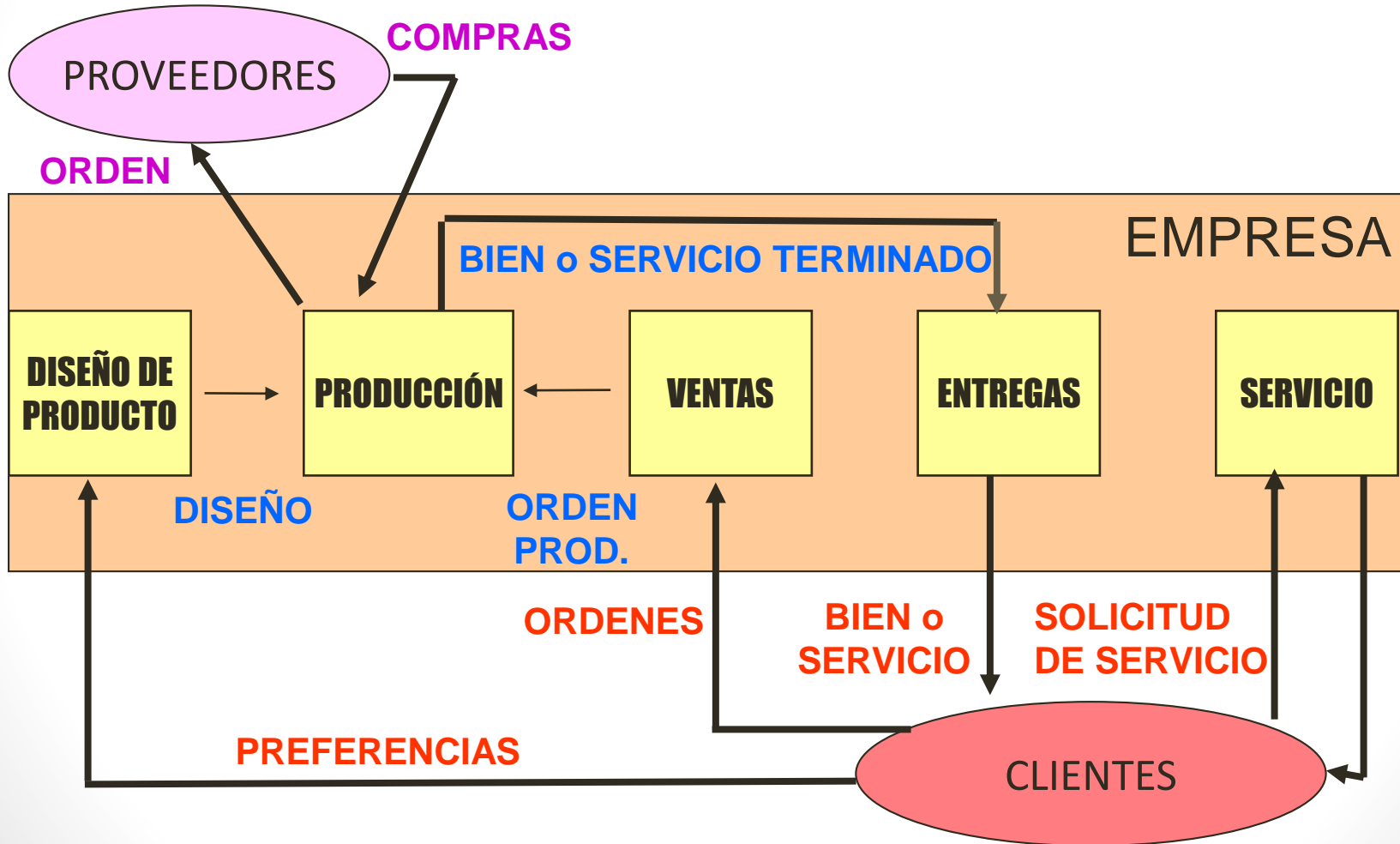
Cabe preguntarse:

...¿Cómo la realizamos? ...¿Qué pasos dar? ¿Qué enfoque o metodología utilizar?

Realmente no hay soluciones únicas, sino que dependen de la organización, de los recursos y del momento .

IV. LA EMPRESA Y LOS S/I

1. LA EMPRESA COMO UN SISTEMA



IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

- ✓ Las empresas, para sobrevivir, necesitan desarrollar estrategias que les permitan adaptarse a un entorno fuertemente inestable y competitivo.
- ✓ Esto justifica la necesidad de disponer de un Sistema de Información, eficaz y eficiente, que desarrolle mecanismos de adaptabilidad con el entorno y potencie la explotación de sus recursos y capacidades, a fin de obtener ventajas competitivas (Porter, 1985).

IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

Modelo contemporáneo

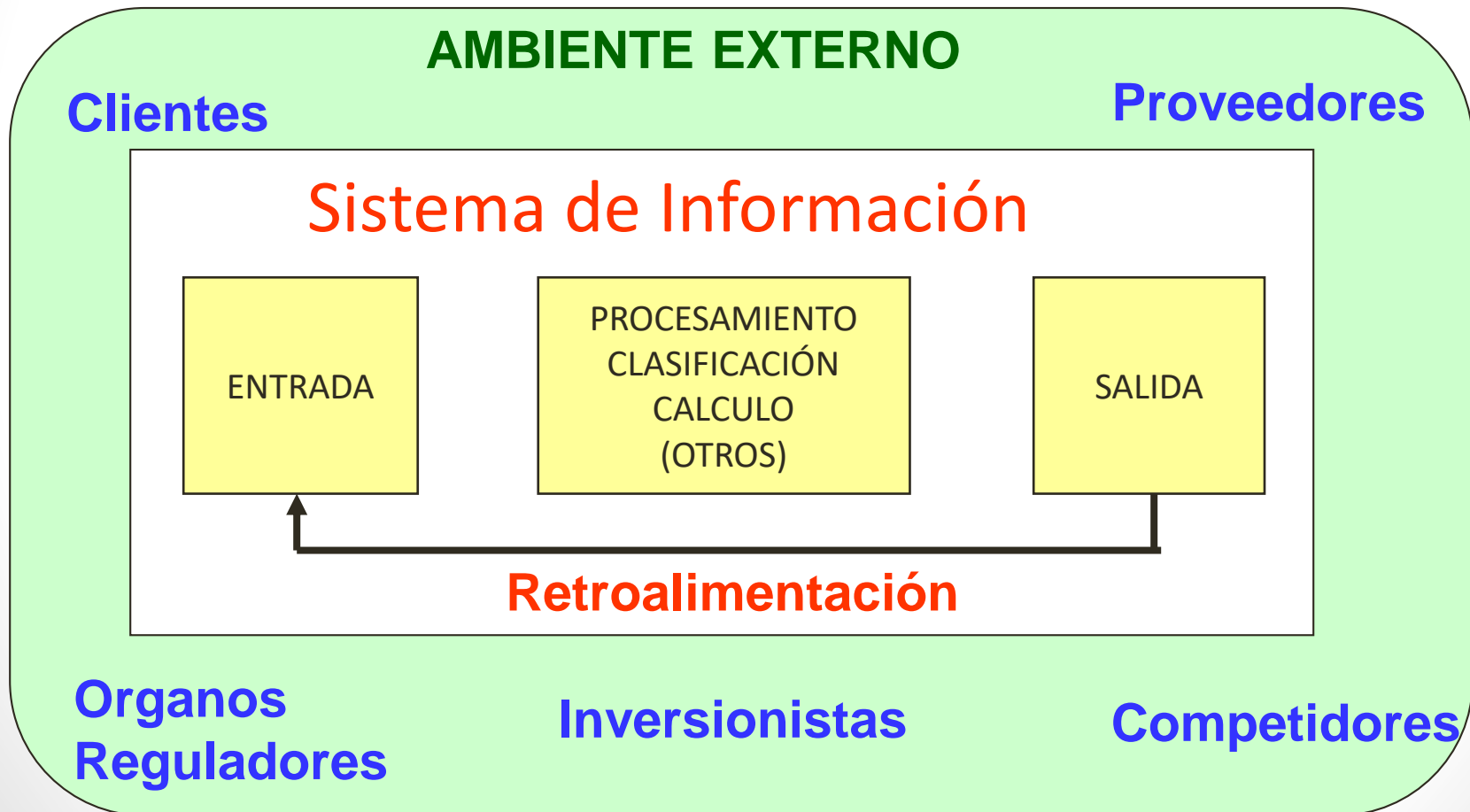
Definición de Sistema de Información

“Un sistema de información definido técnicamente es un conjunto de componentes interrelacionados que recopilan, procesan, almacenan, distribuyen y recuperan información para soportar la toma de decisiones y el control en la organización” [Laudon & Laudon](#)

IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

Los S/I como estructuras sistémicas



IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

- ✓ Las empresas, para producir sus productos y/o servicios desarrollan Sistemas de Trabajo, los cuales necesitan Sistemas de Información soportados por determinadas Tecnologías de la Información.
- ✓ Sin embargo, es muy común el utilizar el mismo termino y dar el mismo significado a estos conceptos.
- ✓ Debemos definir cada término

IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

✓ Tecnología de Información

Es el hardware y el software usado por los sistemas de información

✓ Sistema de Información

Es un tipo particular de sistema de trabajo que usa TI para capturar, almacenar, manipular, desplegar, transmitir y recuperar información; y que soportan uno o más sistemas de trabajo

✓ Sistema de Trabajo

Es un sistema en el que las personas participantes desempeñan el proceso de negocios usando la información, la tecnología y otros recursos para producir productos y/o servicios para clientes internos o externos.

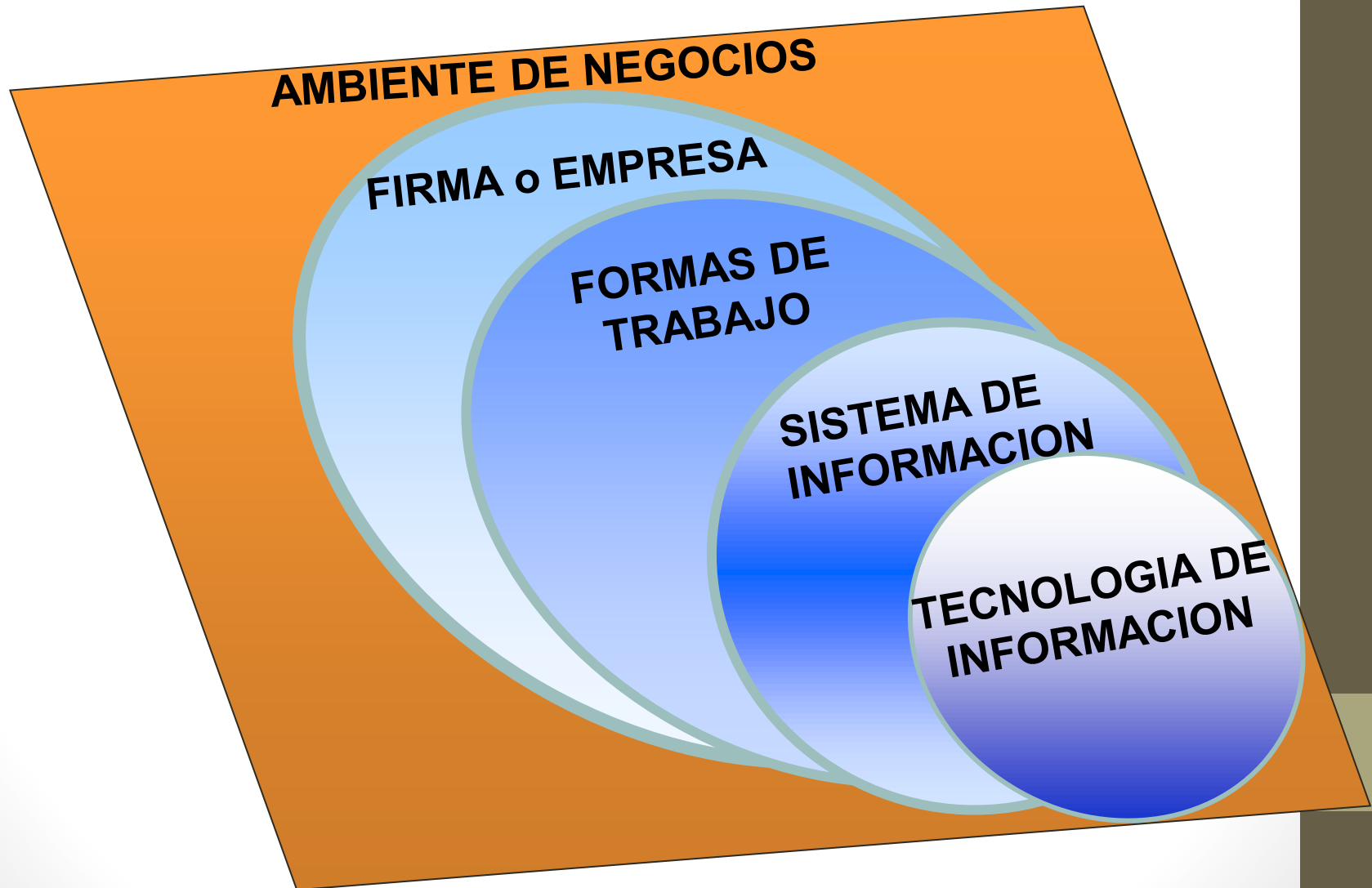
IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

- ✓ **La Firma o Empresa** consiste en la interrelación de sistemas de trabajo, los cuales operan para generar los productos o servicios para los clientes que se encuentran en el ambiente de negocios
- ✓ **El Ambiente de Negocios** incluye a la misma empresa o firma y todo lo que afecta su éxito como: competidores, proveedores, clientes, Instituciones reguladoras, condiciones sociales, demográficas y económicas, etc.

IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I



IV. LA EMPRESA Y LOS S/I

2. LA EMPRESA Y LA IMPORTANCIA DE LOS S/I

Ejemplos de Roles de los SI y Sistema de Trabajo

- Sistema de Ahorros con retiros por Cajeros Automáticos
- Scanner de código de barras que captura los datos del producto
- Sistema de Identificación de empleados que utiliza tarjeta con banda magnética
- Pide clave confidencial y compara con archivo de claves encriptadas
- Ejecuta la transacción con el cliente y verifica la captura de datos
- Prevé que una persona no autorizada acceda a un área determinada

IV. LA EMPRESA Y LOS S/I

5. WORK-CENTER ANALYSIS (WCA)

Es un esquema que identifica los Sistemas de Trabajo soportado por S/I. Este esquema combina recursos como: administración de la calidad, reingeniería de procesos y teoría general de sistemas.

Consiste en seis (6) elementos interrelacionados

- Clientes internos o externos al sistema de trabajo
- Productos generados por el sistema de trabajo
- Los procesos de negocios, razón de la empresa
- Los participantes en el sistema de trabajo
- La información que el sistema de trabajo utiliza
- La tecnología que el sistema de trabajo usa


IV. LA EMPRESA Y LOS S/I


5. WORK-CENTER ANALYSIS (WCA)




V. EL CONTROL INTERNO

1. EL CONTROL INTERNO EN LA EMPRESA

 Control es cualquier acción que lleva a cabo una persona para aumentar la probabilidad de que se logren las metas y objetivos propuestos.

 El propósito final del control es, preservar la existencia de cualquier organización y apoyar a su desarrollo; su objetivo es contribuir con los resultados esperados.


 No debe ser aislado, sino un todo, relacionado con los planes estratégicos de la empresa y su gestión organizacional.


V. EL CONTROL INTERNO

1. EL CONTROL INTERNO EN LA EMPRESA

Para las Organizaciones se han creado diversos Modelos de Control, a fin de proteger sus bienes. Así tenemos:

 **COSO:** COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. (COMITÉ DE ORGANIZACIONES QUE PATROCINAN LA COMISIÓN DE TREADWAY)

 **COCO:** CRITERIA OF CONTROL COMMITTEE: THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS. (CRITERIOS DEL COMITÉ DE CONTROL DEL INST. CANADIENSE DE CONTABLES ENCARGADOS)

 **CADBURY:** UK CADBURY COMMITTEE- INTERNAL CONTROL WORKING GROUP, INST. OF CHARTERED ACCOUNTANTS IN ENGLAND AND WALES. (GRUPO DEL CONTROL INTERNO DEL COMITÉ DE CADBURY, INST. DE CONTABLES DE INGLATERRA Y PAÍS DE GALES).

V. EL CONTROL INTERNO

2. EL INFORME COSO

En los EE.UU. en 1985, se forma una Comisión patrocinada por la American Accounting Association y otras firmas, se llamo National Commission on Fraudulent Financial Reporting, también conocida como comisión Treadway.

Se creó con el objetivo de identificar las causas de la presentación de información financiera en forma fraudulenta o falsificada y emitir recomendaciones que llevaran a garantizar la máxima transparencia en lo que se refiere a la información financiera.

V. EL CONTROL INTERNO

2. EL INFORME COSO

Este informe, publicado en 1987, contenía una serie de recomendaciones en relación con el control interno de cualquier empresa u organización.

En base a estas recomendaciones, las empresas patrocinadoras de la Comisión Treadway, debatieron durante más de cinco años y finalmente en 1992, se emite el Informe COSO, el cual tuvo gran aceptación.

V. EL CONTROL INTERNO

2. EL INFORME COSO

Actualmente es el principal documento de estudio que define un nuevo marco conceptual del control interno, capaz de integrar las diversas definiciones y conceptos que hasta ese momento se habían venido utilizando sobre este tema.



La misión de COSO es:

"... Proporcionar liderazgo intelectual a través del **desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude**, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones."

V. EL CONTROL INTERNO

2. EL CONTROL INTERNO SEGÚN INFORME COSO

CONTROL INTERNO se define de manera amplia como un proceso llevado a cabo por el Consejo de Administración, la Gerencia y otro personal de la organización, que está diseñado para proporcionar una garantía razonable sobre el logro de objetivos en una o más de las siguientes categorías:

- 📄 Efectividad y eficiencia de las operaciones
- 📄 Confiabilidad de la información financiera
- 📄 Cumplimiento con las leyes y normas.

V. EL CONTROL INTERNO

2. EL CONTROL INTERNO SEGÚN INFORME COSO

La definición tiene conceptos fundamentales:

- El control interno es un **proceso**. Es un medio para lograr un fin, no un fin en sí mismo.
- Es llevado a cabo por **personas**. No se trata de manuales, normas y políticas, sino de personas que lo ejecutan en cada nivel de la organización.
- Sólo aporta un grado de **seguridad razonable**, no total, a la dirección y al consejo de administración.
- Diseñado para facilitar la consecución de los **objetivos y metas institucionales**, no para obstaculizarlos (menos y mejores controles).

V. EL CONTROL INTERNO

2. EL CONTROL INTERNO SEGÚN INFORME COSO

EL CONTROL COMO PROCESO ADMINISTRATIVO

¿EL CONTROL ES PARTE INTEGRAL DE LA EMPRESA?



V. EL CONTROL INTERNO






2. EL CONTROL INTERNO SEGÚN INFORME COSO

- El Control Interno es el medio que las empresas aplican para asegurar de manera razonable que se cumplan las Metas y Objetivos.
- Es un frente en el combate a la corrupción.
- Aporta una estructura adecuada para la rendición de cuentas y fomenta la transparencia.
- Es responsabilidad de la administración, a todos los niveles y en todos los ámbitos.
- Previene **riesgos** que pueden impedir el logro de las Metas y Objetivos.
- Promueve la eficiencia, eficacia y economía en el manejo y aplicación de recursos.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

El proceso del Control Interno en una empresa, según COSO, está conformado por:

-  **Entorno de Control**
-  **Evaluación de los Riesgos**
-  **Actividades de Control**
-  **Comunicación e Información**
-  **Monitoreo**

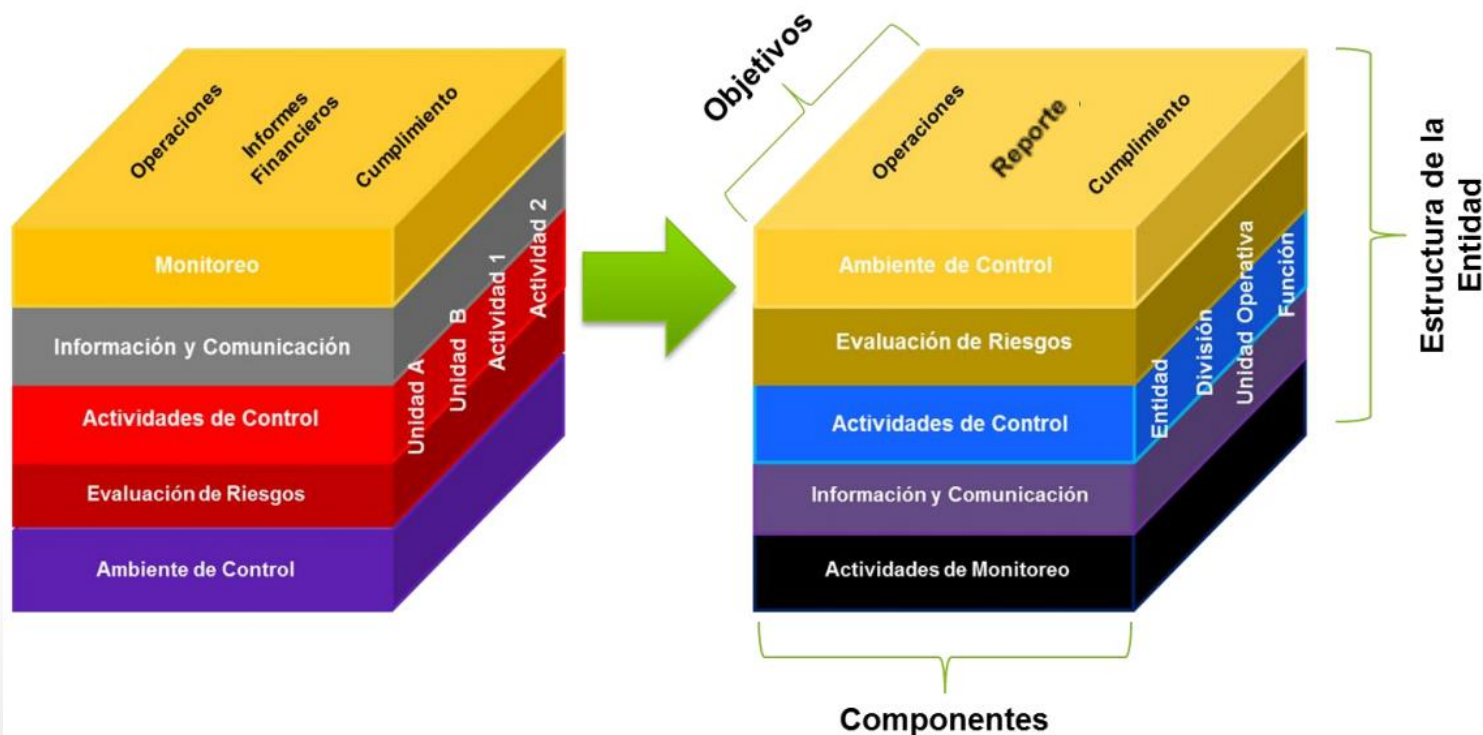
V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)



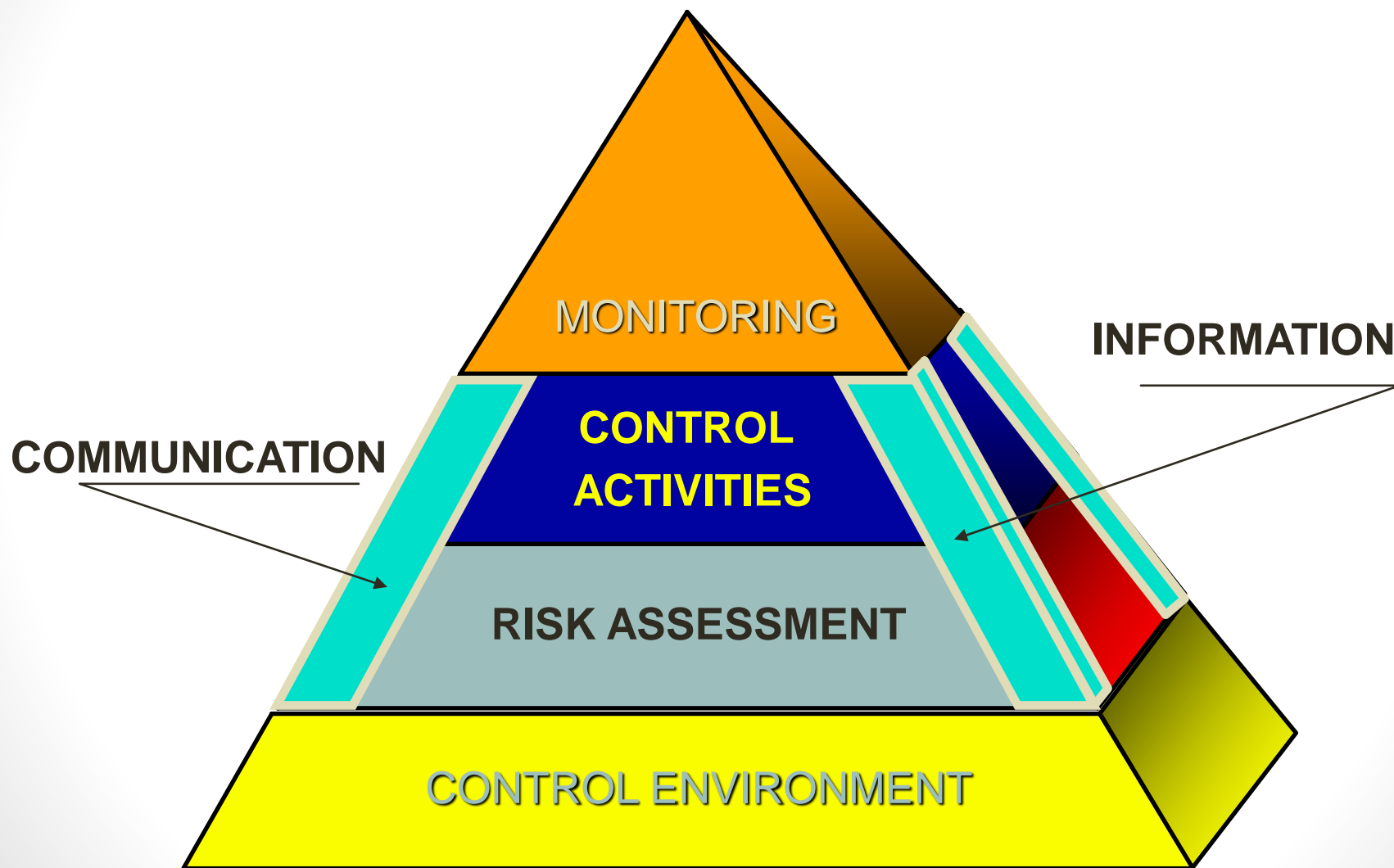
COSO 1992

COSO 2013



V. EL CONTROL INTERNO

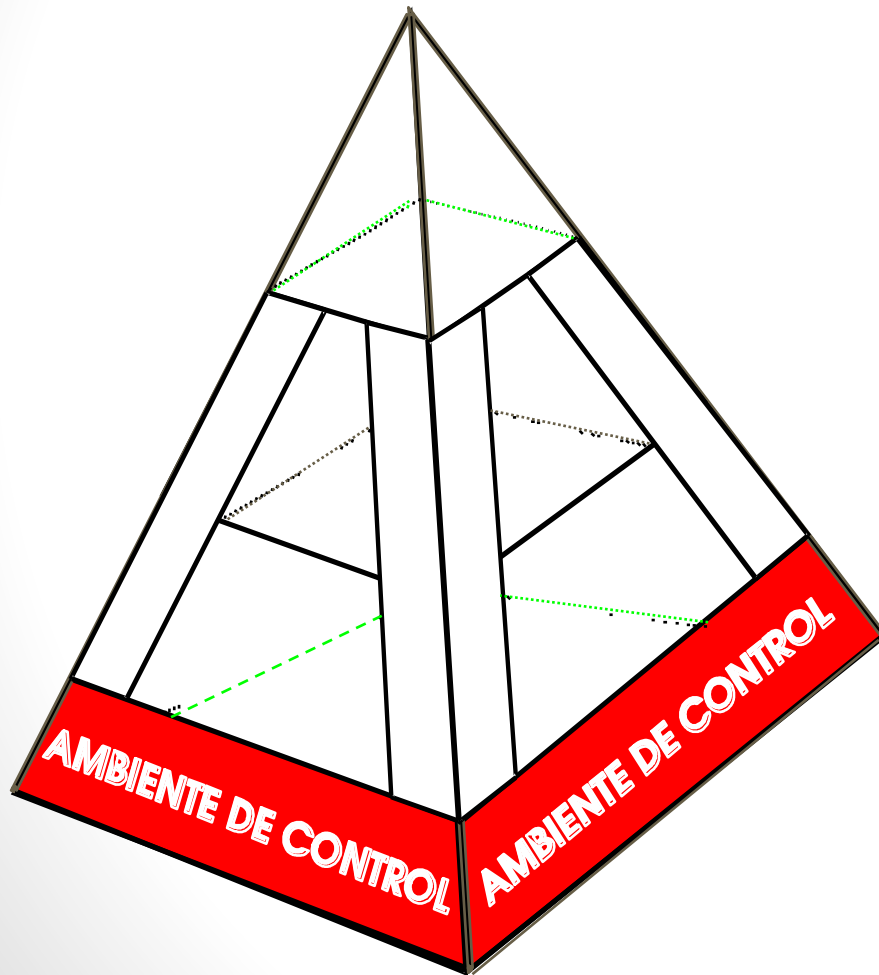
3. COMPONENTES DEL CONTROL INTERNO (COSO)



V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

EL AMBIENTE DE CONTROL










- 📄 INTEGRIDAD Y VALORES ETICOS
- 📄 COMPETENCIA PROFESIONAL
- 📄 COMITÉ DE AUDITORÍA
- 📄 FILOSOFÍA ADMVA. Y ESTILO DE DIRECCIÓN
- 📄 ESTRUCTURA ORGANIZACIONAL
- 📄 ASIGNACIÓN DE AUTORIDAD Y RESPONSABILIDAD
- 📄 POLÍTICA DE RECURSOS HUMANOS

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

EL AMBIENTE DE CONTROL...

-  Es la personalidad de la organización.
-  Estimula y promueve el compromiso de control de su personal.
-  Genera orden y disciplina.
-  Incluye la integridad, valores éticos, capacidad y competencia de su personal.
-  Es la filosofía y el estilo del mando directivo.
-  Delegación de responsabilidad y de autoridad.
-  Estructura organizacional.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

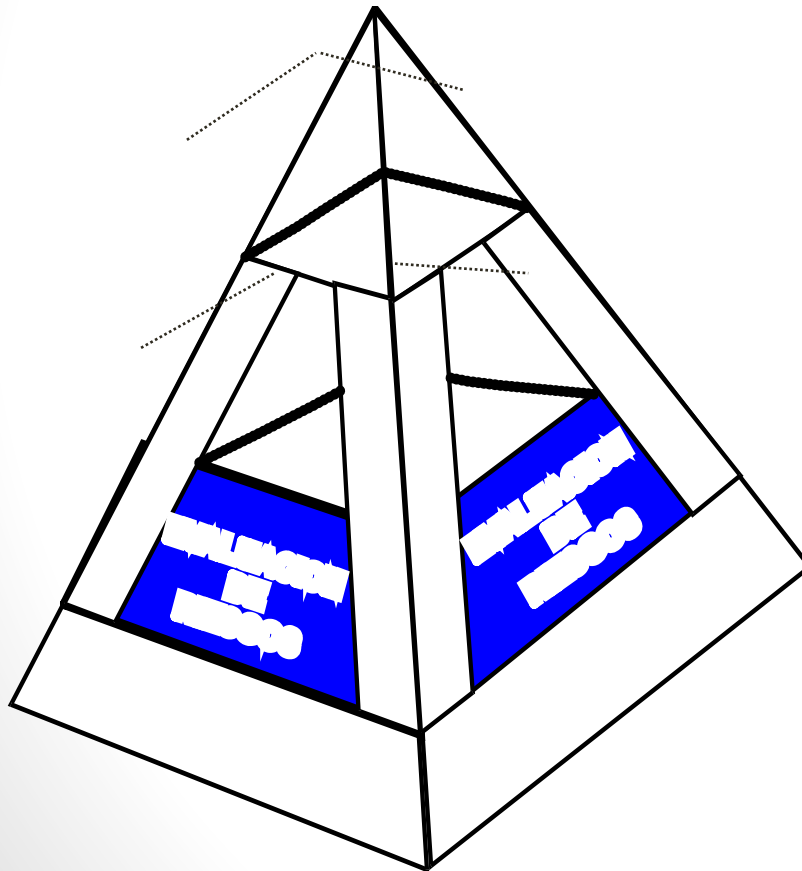
EL AMBIENTE DE CONTROL...

- 01/ La organización demuestra compromiso por la **integridad y valores éticos**.
- 02/ El Consejo de Administración demuestra una independencia de la administración y **ejerce una supervisión del desarrollo y el rendimiento** de los controles internos.
- 03/ La Administración establece, con la aprobación del Consejo, las **estructuras, líneas de reporte y las autoridades y responsabilidades** apropiadas en la búsqueda de objetivos.
- 04/ La organización demuestra un **compromiso a atraer, desarrollar y retener personas** competentes en alineación con los objetivos.
- 05/ La organización **retiene individuos comprometidos** con sus responsabilidades de control interno en la búsqueda de objetivos.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

EVALUACION DE RIESGOS






- 📁 OBJETIVOS ESPECÍFICOS
 - 📁 OPERATIVOS
 - 📁 INFORMACIÓN FINANCIERA
 - 📁 CUMPLIMIENTO
- 📁 ANÁLISIS DE RIESGOS
 - 📁 ORGANIZACIÓN (EXTERNOS / INTERNOS)
- 📁 OBJETIVOS INSTITUCIONALES
 - 📁 ACTIVIDAD
 - 📁 ANÁLISIS (TRASCENDENCIA / PROBABILIDAD / CONTROL)
- 📁 MANEJO DE CAMBIOS
 - 📁 (REORGANIZACIONES / POLÍTICAS / SISTEMAS Y PROCEDIMIENTOS)

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

La Evaluación de Riesgos:

-  Todas las organizaciones están expuestas a riesgos, tanto internos como externos, los que deben ser advertidos y diagnosticados.
-  El análisis de riesgo consiste identificar y analizar los peligros más significativos que puedan afectar el cumplimiento de los objetivos establecidos, con el fin de diseñar un plan que permita decidir cómo administrar dichos riesgos.
-  Se deben realizar a través de toda la empresa, a todos sus niveles y en todas sus funciones.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

Evaluación de Riesgos:

- 📖 Identificar y analizar las condiciones que hayan cambiado y dar atención a las mismas.
- 📖 Existen riesgos según su naturaleza (operacionales /financieros/cumplimiento)
- 📖 Los riesgos deben ser analizados, estimando su impacto y probabilidad de ocurrencia.
- 📖 Los riesgos son administrados con actividades de control.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

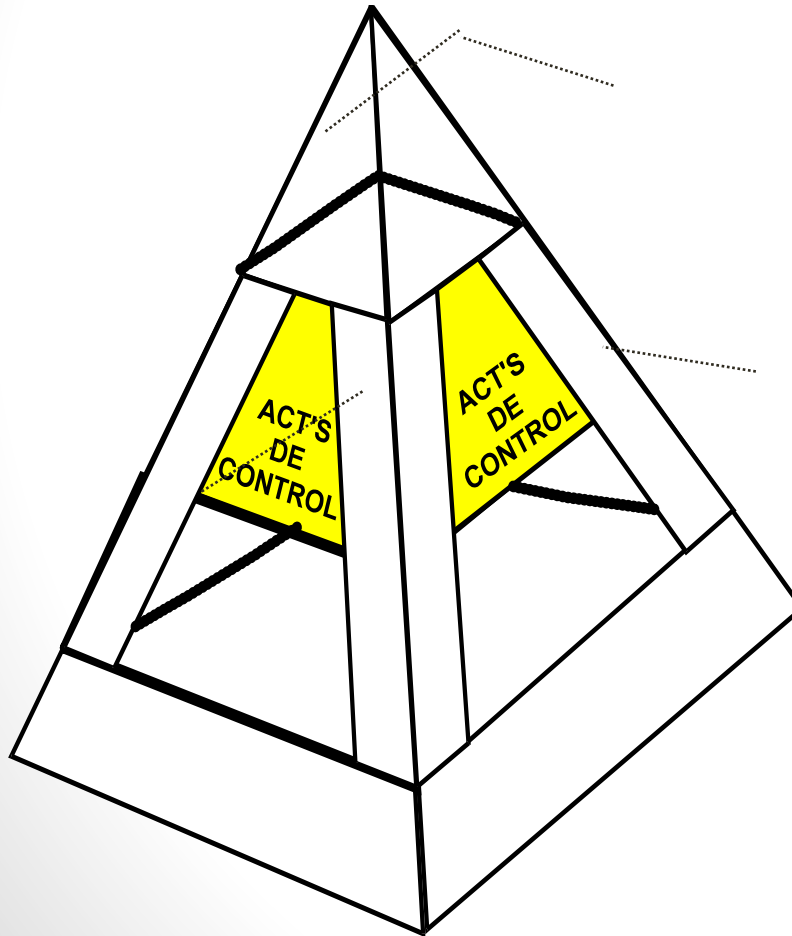
Evaluación de Riesgos:

- 06/ La organización **especifica objetivos** con suficiente claridad para permitir **la identificación y valoración de los riesgos** relacionados a los objetivos.
- 07/ La organización **identifica** los riesgos sobre el cumplimiento de los objetivos a través de la entidad **y analiza los riesgos** para determinar cómo esos riesgos deben de administrarse.
- 08/ La organización **considera la posibilidad de fraude** en la evaluación de riesgos para el logro de los objetivos.
- 09/ La organización **identifica y evalúa cambios** que pueden impactar significativamente al sistema de control interno.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

ACTIVIDADES DE CONTROL



ACTIVIDADES DE CONTROL:

- ▣ ANÁLISIS DIRECTIVO
 - ▣ GESTIÓN DE FUNCIONES
 - ▣ PROCESO DE INFORMACIÓN
 - ▣ CONTROLES FÍSICOS
 - ▣ INDICADORES DE RENDIMIENTO
 - ▣ SEGREGACIÓN DE FUNCIONES
 - ▣ SISTEMAS DE INFORMACIÓN

TIPOS DE CONTROL:

- ▣ PREVENTIVOS / CORRECTIVOS
- ▣ MANUALES / AUTOMATIZADOS
- ▣ GERENCIALES

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

ACTIVIDADES DE CONTROL

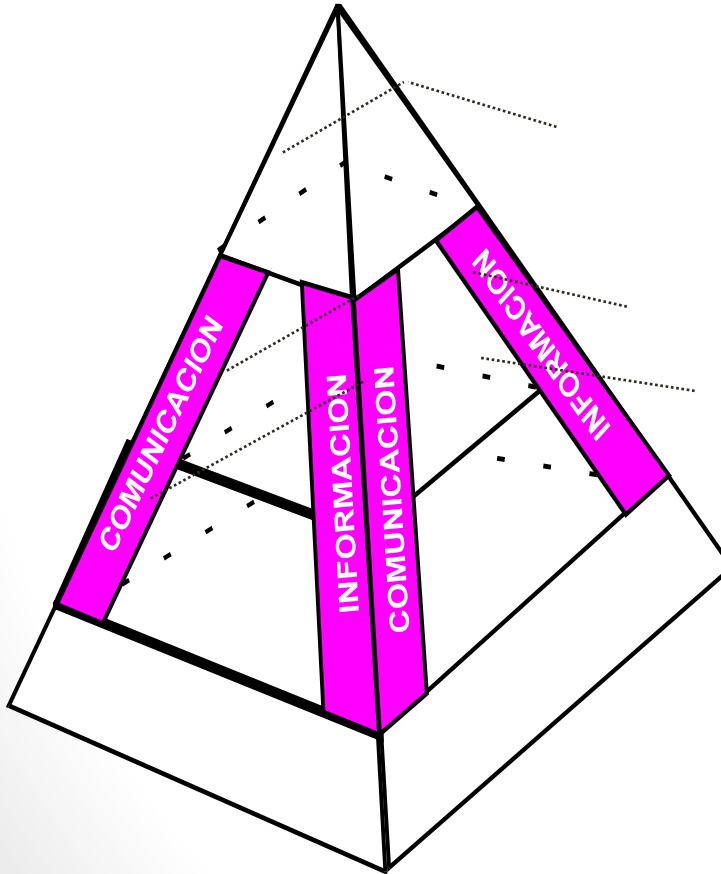
- 10/ La organización elige y desarrolla **actividades de control que contribuyen a la mitigación de riesgos** para el logro de objetivos a niveles aceptables.
- 11/ La organización elige y desarrolla **actividades de control generales sobre la tecnología** para apoyar el cumplimiento de los objetivos.
- 12/ La organización **despliega actividades de control a través de políticas** que establecen lo que se espera y **procedimientos** que ponen dichas políticas en acción.







V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

INFORMACION Y COMUNICACION



SISTEMAS DE INFORMACIÓN :

-  APOYO ACTIVIDADES ESTRATÉGICAS
-  INTEGRACIÓN CON LAS OPERACIONES
-  COEXISTENCIA DE TECNOLOGÍAS
-  CALIDAD

COMUNICACIÓN :

-  INTERNA / EXTERNA
-  MEDIOS

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

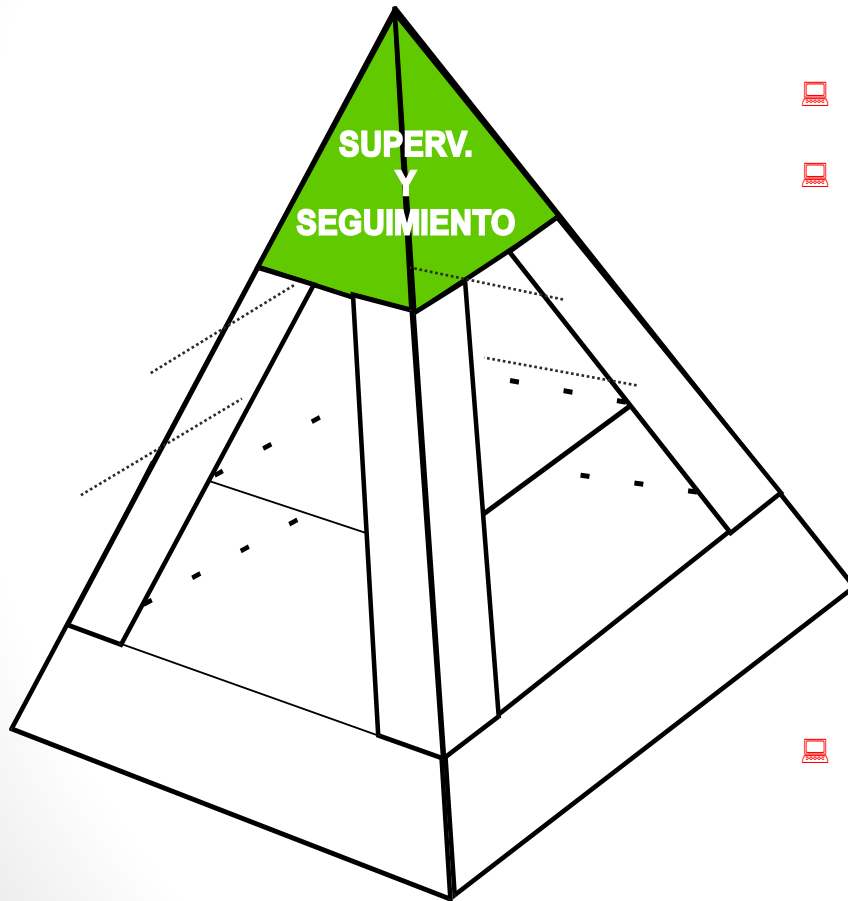
INFORMACION Y COMUNICACION










- 13/ La organización obtiene o genera y usa **información relevante y de calidad** para apoyar el funcionamiento del control interno.
- 14/ La organización **comunica información internamente, incluyendo objetivos y responsabilidades sobre el control interno**, necesarios para apoyar funcionamiento del control interno.
- 15/ La organización **se comunica con grupos externos** con respecto a situaciones que afectan el funcionamiento del control interno.

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

SUPERVISION Y SEGUIMIENTO (MONITOREO)



-  **SUPERVISIÓN CONCURRENTE**
-  **EVALUACIONES INDEPENDIENTES**
-  **ALCANCE Y FRECUENCIA**
-  **QUIÉNES EVALÚAN**
-  **PROCESO DE EVALUACIÓN**
-  **METODOLOGÍA**
-  **DOCUMENTACIÓN**
-  **PLAN DE ACCIÓN**
-  **REPORTES DE DEFICIENCIAS**

V. EL CONTROL INTERNO

3. COMPONENTES DEL CONTROL INTERNO (COSO)

SUPERVISION Y SEGUIMIENTO (MONITOREO)

- 16/ La organización **selecciona, desarrolla, y realiza evaluaciones** continuas y/o separadas para comprobar cuando los componentes de control interno están presentes y funcionando.
- 17/ La organización **evalúa y comunica deficiencias de control interno** de manera adecuada a aquellos grupos responsables de tomar la acción correctiva, incluyendo la Alta Dirección y el Consejo de Administración, según sea apropiado.

V. EL CONTROL INTERNO

4. MARCO INTEGRADO DEL CONTROL (COSO)



Resumen...

El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO) es una iniciativa conjunta de cinco organizaciones del sector privado, establecidas en los Estados Unidos , dedicada a proveer el liderazgo de pensamiento a la dirección ejecutiva y las entidades de gobierno en los aspectos críticos del gobierno, la ética empresarial , la organización interna el control , la gestión del riesgo empresarial , el fraude y la información financiera.

Resumen...

COSO ha establecido un modelo de control interno común contra el cual las empresas y las organizaciones pueden evaluar sus sistemas de control.

COSO con el apoyo de cinco organizaciones de apoyo, incluyendo el Institute of Management Accountants (IMA) , la Asociación Americana de Contabilidad (AAA) , el Instituto Americano de Contadores Públicos Certificados (AICPA), el Instituto de Auditores Internos (IIA) y Ejecutivos Financieros Internacionales (FEI) .

Resumen...

Siguientes pasos para iniciar con la aplicación del nuevo enfoque de COSO

Estudiarlo y entenderlo



Evaluar el estado actual



Definir un plan de implementación



Comunicarlo en la organización



Recordar...

El control interno es la acción humana, que introduce la posibilidad de errores en el procesamiento o el juicio . El control interno también puede ser anulado por la colusión entre los empleados o la coacción por la alta dirección .

V. EL CONTROL INTERNO

5. RIESGO DEL NEGOCIO Y RIESGO PREVISTO

EVALUACIÓN DE RIESGOS A NIVEL ORGANIZACIONAL



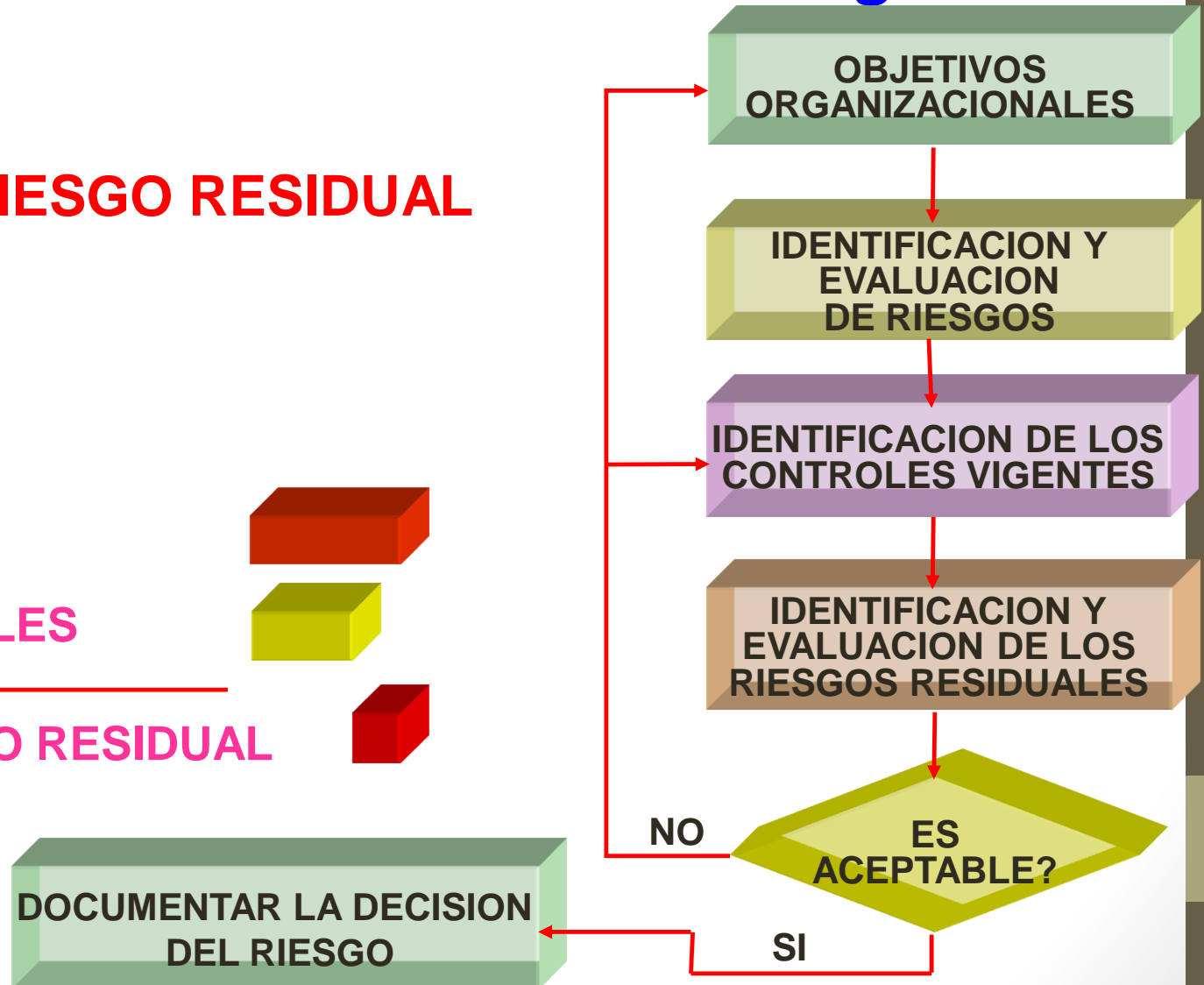
EVALUACIÓN DE RIESGOS DENTRO DE LA AUDITORÍA

-  **RIESGO DEL NEGOCIO**
-  **EXAMEN DEL MANEJO DE RIESGOS**
-  **EVALUACIÓN DEL RIESGO RESIDUAL**

V. EL CONTROL INTERNO

6. Proceso de Administración de Riesgos

EL RIESGO RESIDUAL



VI. AMBITO DE CONTROL

EVALUACION DE LA FUNCION INFORMÁTICA

- **La administración del procesamiento de datos es la primera gran área de interés para el auditor.**
- **Esto porque son dependientes de la forma en que se esté administrando la función informática:**
 - **La calidad de los sistemas.**
 - **En nivel de aprovechamiento de la TI.**
 - **El desenvolvimiento del personal de cómputo.**

VI. AMBITO DE CONTROL

EVALUACION DE LA FUNCION INFORMÁTICA

- **Dentro de ésta área es importante que el auditor llegue a conocer con profundidad:**
 - **La forma en que se está administrando la función informática.**
 - **El rumbo que se le está dando.**
 - **Las directrices que se han dictado.**
 - **Las prioridades que se han establecido.**
 - **La normativa que rige la actividad.**
 - **El nivel de motivación que posee el personal involucrado.**
 - **Las inversiones que se piensan realizar.**
 - **Los planes de capacitación, entre otros.**

VI. AMBITO DE CONTROL

DIVISIÓN DE LA EVALUACIÓN DE LA FUNCIÓN INFORMÁTICA

- Se pueden evaluar cinco grandes áreas:
 1. Evaluación de la participación gerencial en el proceso informática.
 2. Evaluación de los procesos de planeamiento.
 3. Evaluación de la organización.
 4. Evaluación de la dirección.
 5. Evaluación de los mecanismos de control.

1. EVALUACIÓN DE LA PARTICIPACIÓN GERENCIAL EN EL PROCESO INFORMÁTICO

- **En la actualidad, la tecnología de la información tiene una connotación estratégica en casi toda la organización.**
- **El uso apropiado de la informática puede ayudar a la gerencia a proyectar la empresa dentro de un mundo altamente competitivo.**
- **En su día a día, muchas de las grandes organizaciones del mundo tienen una alta dependencia de los sistemas automatizados.**

1. Evaluación de la participación gerencial en el proceso informático

- **En esencia, la informática cumple una función de apoyo.**
- **El rumbo que se dé a la función informática dentro de una organización debe estar totalmente dirigido a apoyar el cumplimiento de los objetivos y las metas planteadas en la organización.**

1. Evaluación de la participación gerencial en el proceso informático

- **El auditor debe:**
 - **Verificar que quienes administran la función informática conozcan con claridad la misión, los objetivos y metas de la organización.**
 - **Que el rumbo que se esté dictando con respecto al uso de la tecnología esté dirigido a facilitar o propiciar el alcance de dichos propósitos.**

2. EVALUACIÓN DE LOS PROCESOS DE PLANEAMIENTO

- **En materia informática la existencia de un proceso ordenado y sistemático de planeamiento resulta esencial para la buena marcha de todos los proyectos que se desarrollan.**
- **Es indispensable que el planeamiento se de a muchos niveles:**
 - **Planeamiento del marco general que establezca el rumbo de la informática y que fije la estrategia en esta materia.**
 - **Planes operativos anuales que delimiten las actividades que se ejecutarán en el corto plazo.**

2. Evaluación de los Procesos de Planeamiento

- **Planes para llevar el control a todos los proyectos de desarrollo de aplicaciones.**
- **Planes de capacitación tanto para usuarios como para el personal de cómputo.**
- **Planes específicos en materia de adquisición de software hardware.**
- **Planes para todos los procesos de conversión que se produzcan.**
- **Y por último un plan que permita asegurar la continuidad del servicio informático.**

2.1 Plan Estratégico Informático

- **Son establecidos con el propósito de definir la visión a largo plazo con respecto a la función informática.**
- **Mediante este tipo de plan se puede llegar a definir la orientación que tendrá la empresa en materia de Hardware y Software, el inventario de aplicaciones a desarrollar, opciones para el desarrollo y el establecimiento de prioridades.**
- **Establece el rumbo que debe tener la empresa en materia informática para un periodo de 3 a 5 años.**

2.1 Plan Estratégico Informático

- **La existencia de un plan estratégico le permite al auditor conocer:**
 - **Cual es la arquitectura básica de hardware que planea introducirse en la empresa,**
 - **Las herramientas básicas de software que se utilizarían para el desarrollo de S/I,**
 - **La cartera de S/I que es necesario construir y establecer prioridades en el tiempo,**
 - **Las decisiones en materia de desarrollo de S/I que han sido tomadas y la estrategia a seguir: desarrollo interno, contratación externa, entre otros.**

2.1 Plan Estratégico Informático

- **La inexistencia de un plan estratégico implica que el área informática en una empresa está sin un rumbo establecido.**
- **Dada la importancia de la tecnología de la información para las empresas, el auditor debe promover la creación de un plan estratégico el cual marque la dirección que se dará a la informática.**

2.2 Plan operativo anual

- **Este tipo de plan busca definir el conjunto de actividades que se desarrollarán en una empresa en materia informática en un período de un año.**
- **Debe tener una estrecha vinculación con el Plan Estratégico**
- **Requiere que la dirección de informática establezca coordinaciones con las áreas usuarias para que exista coherencia entre las actividades que cada una debe realizar como parte del desarrollo de los proyectos de automatización.**

2.2 Plan operativo anual

- **El auditor debe:**
 - **Evaluar la consistencia que presenta el plan operativo con respecto al plan estratégico.**
 - **Comparar los planes operativos de las áreas usuarias contra el que elabore la dirección de informática con el propósito de medir el nivel de coordinación existente.**
 - **Analizar el avance de la ejecución de estos planes y alertar a la administración sobre los atrasos detectados, los cuales pueden perjudicar el logro de las metas y objetivos.**

2.3 Planeamiento de los procesos de desarrollo

- Resulta muy común que durante el desarrollo de una aplicación se deban replantear sus alcances como producto de necesidades no previstas y que esto provoque atrasos en la culminación del proyecto.
- Es en este nivel donde se requiere una mayor participación de los usuarios.
- El planeamiento de los proyectos debe contemplar una estimación de costos y la utilización de herramientas automatizados para el control del proyecto.

2.3 Planeamiento de los procesos de desarrollo

- **El auditor debe:**
 - **Verificar que el planeamiento de los proyectos permita medir los costos estimados contra los reales y que detecte de manera oportuna los atrasos en la ejecución de actividades.**
 - **Recomendar la utilización de herramientas de planeamiento para cada proyecto, lo cual permitirá controlar el avance del proyecto, detectar a tiempo los problemas en el avance y tomar las decisiones pertinentes.**

2.4 Planes de capacitación

- **Como la tecnología evoluciona a una velocidad vertiginosa, obliga a quienes se encuentran involucrados con ella, a mantener un nivel de actualización muy alto.**
- **Por lo anterior, la dirección de informática debe proponer periódicamente planes de capacitación que permitan tanto a los usuarios como al personal de cómputo mantener un nivel de conocimientos acorde con la tecnología existente en el mercado y con las exigencias del negocio.**

2.4 Planes de capacitación

- **El auditor debe:**
 - **Analizar los programas de capacitación a la luz de las tendencias que se presentan en el mercado.**
 - **Asesorar a la dirección de informática sobre temas específicos en los cuales resulte importante adiestrar al personal.**

2.5 Planes de adquisición

- **La dirección debe establecer un planeamiento adecuado de compra de hardware y software que responda a sus necesidades de automatización.**
- **Es necesario que exista una calendarización precisa del momento en el cual es necesario que se adquiera cada nuevo componente.**
- **Los planes de adquisición permiten mantener un nivel de actualización tecnológica y prudente.**
- **Deben analizarse medidas de rendimiento y estudios que permitan determinar las nuevas demandas de Hw y Sw con anticipación.**
- **La compra de nuevos equipos debe estar fundamentada en información referente al respaldo que ofrecen los proveedores.**

2.5 Planes de adquisición

- **El auditor debe:**
 - **Evaluar si los presupuestos de nuevas adquisiciones, los procesos de formulación de Bases para invitar a los proveedores, las evaluaciones de ofertas, la adjudicación y entrega de los productos adquiridos están de acuerdo con planes previamente establecidos.**
 - **Alertar a la administración cuando detecte que las adquisiciones se están realizando de manera improvisada.**
 - **Asesorar a la dirección de informática en la definición de procesos de compra de Hw y Sw que sean ordenados y controlados.**

2.6 Planes de conversión

- Los siguientes eventos generan procesos de conversión básicos en un ambiente de cómputo:
 - Cambio del computador
 - Cambio de versión del software.
 - Cambio de versión de una aplicación.
- Cualquiera de estos tres tipos de eventos tienen en común que implican un cambio en la forma actual de operación de algún componente.
- Cualquier conversión requiere de un adecuado planeamiento que asegure la posibilidad de que exista continuidad en el servicio informático.

2.6 Planes de conversión

- **El plan debe contemplar, al menos, lo siguiente:**
 - **Calendarización correcta del momento en el cual debe llevarse a cabo la conversión**
 - **Realización de respaldos de las aplicaciones.**
 - **Definición de las pruebas mínimas**
 - **Convocatoria a los usuarios, analistas, personal de soporte, funcionarios de los proveedores para la realización de las pruebas**
 - **Preparación de charlas y boletines para comunicar el cambio.**
 - **Definición clara y concreta de las responsabilidades de los diferentes participantes.**

2.6 Planes de conversión

- **El auditor debe:**
 - **Estar atento a los cambios que se piensen realizar en el área informática para alertar y asesorar sobre los aspectos mínimos que hay que considerar en los procesos de conversión.**

2.7 Planes de contingencia

- **La gran dependencia de las empresas hacia los medios automatizados crea la necesidad de elaborar planes de contingencia cuyo propósito sea asegurar un alto grado de disponibilidad de los servicios informáticos que permitan la continuidad de las operaciones de las empresas.**
- **Por lo anterior, las instituciones deben realizar un esfuerzo por identificar los posibles riesgos que pueden presentarse, cuya ocurrencia provoque trastornos en la operación diaria y elaborar planes concretos para minimizar el impacto de dichas contingencias en el accionar del negocio.**

2.7 Planes de contingencia

- **El auditor debe:**
 - **Evaluar el grado de preparación que existe en la organización para actuar en caso de contingencias y la eficacia de los planes existentes para restaurar los servicios informáticos en un tiempo prudencial.**
 - **Medir si el presupuesto asignado para la creación y mantenimiento de un plan de este tipo está acorde con la importancia que tiene la TI para el accionar de la empresa.**
 - **Participar activamente en los procesos de prueba de los planes definidos para evaluar la eficacia de las acciones que se ejecutan y sugerir las mejoras pertinentes.**



3. EVALUACIÓN DE LA ORGANIZACIÓN

- **Todo el esfuerzo de planeamiento del área informática luego debe traducirse en métodos y esquemas de trabajo que faciliten la consecución de objetivos.**
- **La forma en que esté organizado el área de cómputo de la empresa es también de interés para la auditoría.**
- **El proceso de organizar sirve para estructurar los recursos, los flujos de información y los controles que permitan alcanzar los objetivos marcados durante la planificación.**

3.2 Ubicación dentro del organigrama

- **Debido a que la función informática es una función de apoyo al resto de la organización, requiere un nivel razonable de independencia funcional con respecto a los usuarios.**
- **La ubicación idónea del área informática de la empresa es en el nivel staff, dependiendo de la gerencia general de la compañía.**
- **Siempre que el departamento de informática esté integrado en algún departamento usuario, puede surgir dudas razonables sobre su ecuanimidad a la hora de atender las peticiones del resto de departamentos de la empresa.**

3.2 Ubicación dentro del organigrama

- **El auditor debe:**
 - **Analizar si la ubicación que posee el área informática en el organigrama le permite alcanzar suficiente independencia para actuar con autonomía con respecto a las áreas usuarias a las cuales brinda servicios.**
 - **Sugerir, en aquellos casos donde se detecten problemas de autoridad, la reubicación del área informática.**

3.3 Definición de funciones y responsabilidades

- Como en el área informática existe una serie de tareas que pueden ser fácilmente diferenciadas y para las cuales se requieren diferentes niveles de especialización y de experiencia:
 - Es posible efectuar una clasificación de puestos de manera que queden claramente definidas las funciones y responsabilidades de cada puesto. *Esto permitirá establecer el área de responsabilidad de cada individuo.*
- La existencia de una definición de las tareas y responsabilidades permite definir las cargas de trabajo de cada uno de los puestos y ayuda al establecimiento de un sistema de control interno adecuado.

3.3 Definición de funciones y responsabilidades

- **Para el auditor resulta de ayuda la existencia de una definición concreta y actualizada de las funciones de cada uno de los puestos del área informática.**
- **Las descripciones de los puestos de trabajo deben delimitar claramente la autoridad y responsabilidad en cada caso. Deben incluir los conocimientos técnicos y/o experiencia necesarios para cada puesto.**
- **Se debe llegar a conocer la operación del área de cómputo, las interrelaciones existentes, el nivel de centralización o descentralización de las tareas, el ámbito de toma de decisiones de cada puesto, los mecanismos de comunicación y la autoridad.**

3.3 Definición de funciones y responsabilidades

- **Además, una forma ideal de transmitir al personal la actitud hacia los controles necesarios es con la existencia de estándares de funcionamiento y procedimientos.**
- **Estos estándares deberían estar documentados, actualizados y ser comunicados a todos los departamentos afectados**
- **La gestión de los recursos humanos es uno de los elementos críticos en la estructura general informática. Seleccionarlos y mantenerlos adecuadamente es crucial para la buena marcha de la informática y su papel en la empresa.**

3.3 Definición de funciones y responsabilidades

- El departamento de informática debe organizarse para lograr una adecuada separación de funciones y así asegurar que las transacciones estén salvaguardadas.
- Cuando las funciones están separadas, el acceso a la computadora, los datos de producción, los programas fuente y objeto, la documentación el sistemas operativo y otros puede ser limitado.
- El daño potencial por las acciones de cualquier persona queda por lo tanto reducido.

3.3 Definición de funciones y responsabilidades

- **El auditor debe:**
 - **Evaluar el proceso por el que los estándares y procedimientos son desarrollados, aprobados, distribuidos y actualizados**
 - **Revisar los puestos para evaluar si reflejan las actividades realizadas en la práctica**
 - **Contrastar la definición formal de las funciones para medir si alguno de los funcionarios se está excediendo con respecto a las funciones que tiene encomendadas.**
 - **Evaluar si algunas funciones importantes para la correcta del control interno se están dejando de realizar sin que existan justificaciones claras.**

3.3 Definición de funciones y responsabilidades

- **Recomendar a la dirección de informática la actualización de las funciones de cada individuo de acuerdo con las tareas asignadas.**
- **Evaluar que la selección de personal se basa en criterios objetivos y tiene en cuenta la formación y experiencia anteriores.**
- **Revisar que se evalúe el rendimiento de cada empleado con base en estándares establecidos.**
- **Revisar que en el departamento de informática se esté aplicando una adecuada separación de funciones o en su defecto que existan los controles que reduzcan el riesgo.**

3.3 Definición de funciones y responsabilidades

- **El auditor debe:**
 - **Identificar aquellas actividades del área de cómputo que requieren de una definición clara de los procedimientos de operación y verificar que estos se encuentren debidamente documentados y se estén poniendo en práctica.**
 - **Poner especial atención a los procedimientos de operación ligados a las labores de mantenimiento de sistemas.**
 - **Poner atención sobre aquellos procedimientos de operación que involucren la actualización del contenido de las bases de datos por parte del personal de cómputo.**

3.3 Definición de funciones y responsabilidades

- **Evaluar con detenimiento los procedimientos que tienen relación con el área de operaciones, en especial los relacionados con la ejecución de respaldos, corrida de procesos especiales e impresión de listados con información clave.**
- **Revisar los procedimientos aplicados en la cinto teca.**
- **Revisar el nivel de automatización existente en el área de cómputo.**
- **Poner especial énfasis en la evaluación de la separación de funciones, en los mecanismos de supervisión existentes y en el grado de automatización que estos poseen.**

3.5 Normativa, metodologías y estándares

- **Las organizaciones deben dedicarse a crear la normativa de carácter interno que sirva para definir políticas de carácter general en materia informática**
- **Como, por ejemplo, para el tratamiento de los datos, confidencialidad de la información, cuido del equipo, entre otros, lo cual ayudará a regular el accionar de los diferentes participantes en la actividad informática.**

3.5 Normativa, metodologías y estándares

- **La normativa debe regular aspectos como:**
 - **Clasificación de datos según su sensibilidad y criterios para su acceso a personal autorizado.**
 - **Responsabilidad de los trabajadores en el uso de sus códigos de acceso a los sistemas.**
 - **Políticas institucionales para evitar contagio contra virus.**
 - **Mecanismos de archivo y destrucción de reportes.**
 - **Regulaciones para el uso apropiado de los equipos.**
 - **Procedimientos para compra, alquiler o sustitución de equipos.**

3.5 Normativa, metodologías y estándares

- **El auditor debe:**
 - **Revisar la normativa existente para el desarrollo y mantenimiento de aplicaciones. Por ejemplo, que se cuente con metodologías de desarrollo y mantenimiento de S/I, y clara definición de estándares (motor de base de datos, lenguajes de programación, herramientas de modelado, documentación, diseño de reportes, pantallas, menús, nomenclatura de variables, tablas, etc.)**
 - **Revisar periódicamente que el personal de cómputo esté cumpliendo con los estándares y con la metodología vigente.**

3.6 Distribución física

- **Existen factores que inciden en el rendimiento del personal de cómputo:**
 - **Ruido,**
 - **Temperaturas fuertes**
 - **Cantidad de luz**
 - **Alto tráfico de personas por la zona donde labora el personal**
 - **Ubicación de las estaciones de trabajo**
 - **Distribución de las líneas eléctricas y de comunicación.**
 - **Nivel de hacinamiento del personal.**

3.6 Distribución física

- **El auditor debe:**
 - **Verificar que las instalaciones, en el área de informática, reúnan condiciones mínimas para lograr que el personal alcance los niveles de concentración y productividad necesarios.**

VII. CONTROL INTERNO y AUDITORIA y RIESGOS

1. CONTROL INTERNO vs AUDITORIA INFORMATICA

AREA DE CONTROL INTERNO INFORMATICO

AREA DE AUDITORIA INFORMATICA

SIMILITUDES

- Conocimiento especializados en T/I y S/I.
- Verificación del cumplimiento de controles internos, normas y procedimientos establecidos por entes rectores.
- Técnicas, métodos, procedimientos de análisis y evaluación de riesgos.

DIFERENCIA

- | | |
|---------------------------------|-----------------------------|
| ➤ Evaluación diaria / constante | ➤ Evalúa en un momento |
| ➤ Sólo personal interno | ➤ Personal interno/externo |
| ➤ Criterio dependiente | ➤ Criterio independiente |
| ➤ Informa al Jefe Informático | ➤ Informa a Alta Dirección |
| ➤ Limitado al Dpto de Sistemas | ➤ Sin límites en la empresa |

VII. CONTROL INTERNO y AUDITORIA y RIESGOS

2. PRINCIPALES CONTROLES INFORMATICOS

➤ Controles organizativos y de dirección:

- Plan Estratégico Empresarial,
- Plan de S/I, Planes Operativos Anuales, etc.

➤ Controles para desarrollo, implantación, adquisición y mantenimiento de S/I:

- Políticas y arquitecturas de S/I
- Estándares de desarrollo y de adquisición de S/I
- Estándares de implantación y mantenimiento de S/I

➤ Controles de explotación de S/I:

- Políticas de planificación y gestión de recursos
- Procedimientos de seguridad física
- Procedimientos de seguridad lógica, etc.

VII. CONTROL INTERNO y AUDITORIA y RIESGOS

2. PRINCIPALES CONTROLES INFORMATICOS

➤ Controles de Aplicaciones:

- Control de entrada de datos,
- Control de procesos,
- Control de salida de datos, etc.

➤ Controles específicos de ciertas tecnologías:

- Controles de gestión de Bases de Datos,
- Controles de redes, ofimática,
- Controles en Telecomunicaciones,
- Controles en Internet, Intranet, Extranet, etc.

Examen Parcial