# Presentación 1

## ¿Porque nació la Auditoria de Sistemas?

Ejercer control sobre

* Manejo de información
* Integridad de los datos
* Operaciones

## Que es la Auditoria?

* Proceso sistematico → Obtener → Evaluar → Objetivamente -→Afirmaciones vs hechos.
* Afirmaciones relativas a actos y eventos → Auditoria evalua el grado de correspondencia entre las afirmaciones vs los hechos.
* Posteriormente comunica los resultados.

## Actividades

# Definir el alcance

Encerrar el espacio a verificar, establecer el área precisa (puede aumentarse), definir el espacio de tiempo en que se indagara

# Análisis de Información

Recopilar, analizar información general de (actividades-procesos) → Adquirir conocimiento sobre las funciones de la unidad a evaluar.

# Construir esquemas y modelos

Construir el entendimiento del tema auditado → Lograr mayor comprensión del entorno y su relación con las estrategias del negocio.

Establecer responsables de ejecutar pruebas

Definición de roles y sus respectivos ejecutores

# Documentación y flujogramas

Permite al auditor distinguir los documentos, datos con trascendencia para obtener evidencia. Ejemplo: Papeles de Trabajo

# Eficacia en técnicas de observación

Permiten observar de manera critica los elementos tales como condiciones internas o externas (inventarios, accesos, colocación de elementos, seguridad)

# Papeles de Trabajo

Conllevan la rigurosidad de una investigación criminalista → Desde el punto de vista de (Colección, numeración, conservación, resguardo

Deben ser suficientes en calidad y cantidad → Deben respaldar el informe ya que son el fundamento de la evidencia de lo examinado

# Resultados de Pruebas de

Observaciones, visitas, entrevistas →Estos son detallados en los resultados del auditor (Cedula Resumen)

# Construcción de informe de Auditoria

Toma en cuenta – Papeles de Trabajo, el análisis, evidencias, juicio del equipo de trabajo

# Hallazgos

Resultados de aplicación de pruebas y procedimientos → Sus elementos: condición, criterio, causa y efecto.

Deben estar por escrito para comunicar los resultados-→ Reduce la malinterpretación y facilita el seguimiento y recomendaciones

## Auditoria de Sistemas de Información

**¿Como se define?** -- Abarca la revisión, evaluación de los aspectos de sistemas automáticos de procesamiento de información (incluidos procedimientos ligados a ellos e interfaces)

**¿Que es?** --Una rama especializada que aplica conceptos de auditoria en TI

**Conceptos de Auditoria**

Al hablar de auditoria se tienes 2 fases (programas de trabajo según su fase, procedimientos). Finalmente, hallazgos que se detallan en un informe.



## Etapas de la Auditoria

# Planificación

Contempla los hallazgos, el borrador e informe final

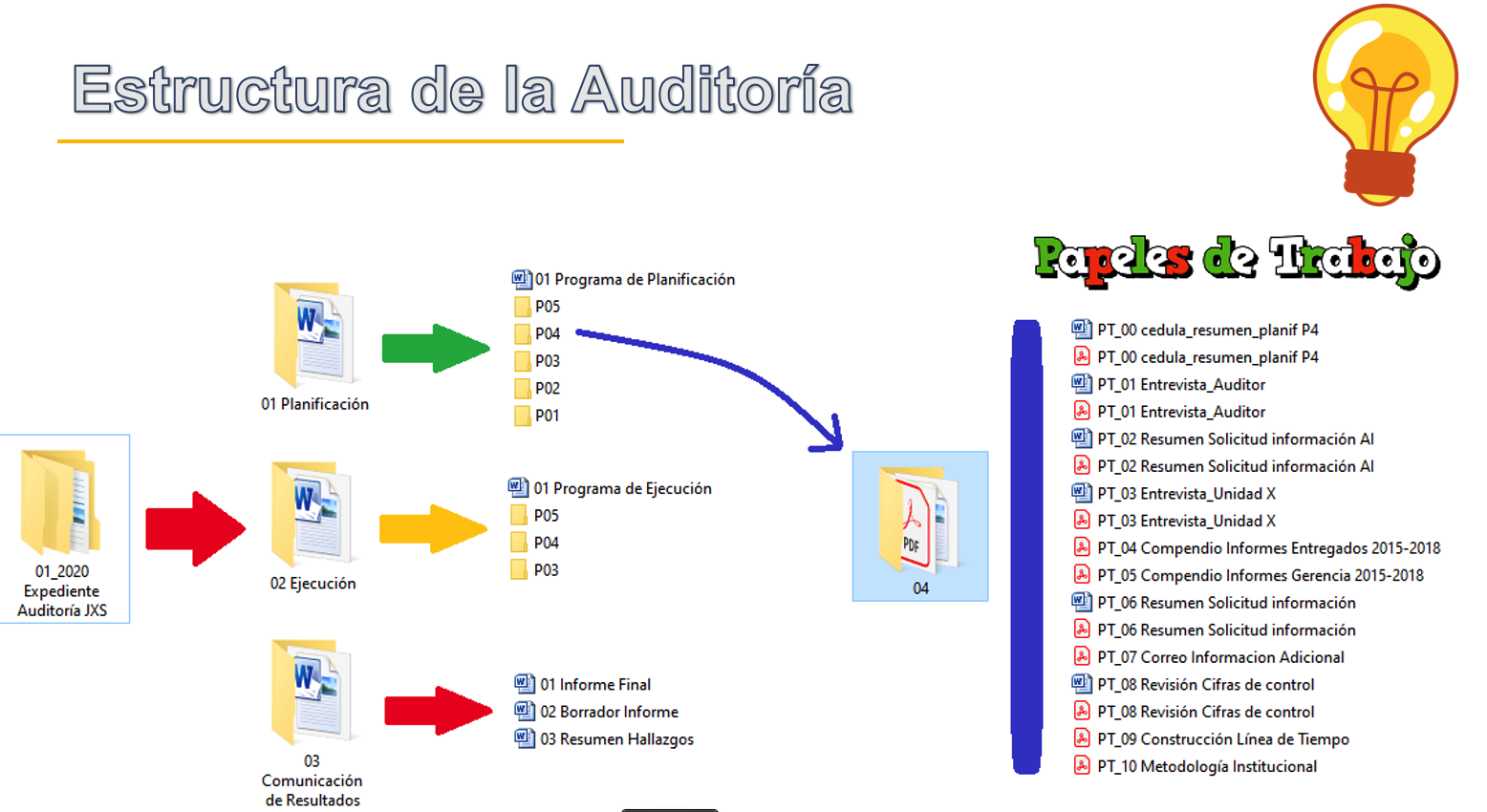
# Ejecución o Examen

Compuesto por un programa de trabajo y procedimientos de VERIFICACION

# Planificación

Compuesto por un programa de trabajo y procedimientos de CONOCIMIENTO

## Estructura de la Auditoria



## Programa de Auditoria

Permite al auditor → Ejecutar, establecer indagaciones para conocer a la empresa y perfilar las áreas de estudio para la fase de ejecución

## Ejecución del Programa y Elaboración de Informe

El auditor debe obtener evidencia suficiente, relevante y útil para lograr los objetivos de la auditoria.

Conclusiones hallazgos → deben estar sustentados por un análisis e interpretación apropiados



\*\* El trabajo queda anotado en los papeles de trabajo que es la prueba documental del trabajo\*\*

* Los papeles de trabajo se registran Cronológicamente
* Contienen los datos e informaciones obtenidos,
* Los resultados de las pruebas hechas y técnicas, procedimientos utilizados

## Importancia de los Papeles de Trabajo

Aspectos como:

* Historia de labor realizada
* Fuentes de informacion indagadas
* Registro de resultados
* Respaldo en procesos legales

## ¿Que es la evidencia en Auditoria?

Conjunto de hechos comprobados que sustentan las conclusiones del auditor

**¿Como se obtiene?**

Observación, Inspección, Entrevistas, Pruebas detalladas de registros, datos, eventos

**¿Donde esta recopilada?** --Papeles de Trabajo

**Cambios en Paradigmas de Control**

Los objetivos de control se aplican a todas las áreas (manuales, automatizadas)

Pero la manera de como se implementan puede variar en TI respecto a otras áreas

Debe abarcar los cambios del mundo globalizado (internet, redes, virtualización, etc.)

# Presentación 2

## Implementación de Controles

Los controles abarcan diferentes realidades de diferentes organizaciones-→ Supone desafíos para el auditor en su función (cambio en paradigmas)

Retos para el diseñador de controles

## Retos para el Diseño de Controles

* La inclusión de políticas y tareas para proveer una certeza razonable de que se logren los objetivos
* Generación de controles generales para todas las áreas de la organización
* Un sistema de información bien diseñado debería contar con controles

## Controles especificos de TI

* Implica traducir controles generales a un control de TI
* Todo sistema bien construido debería contar con controles hechos para sus funciones sensitivas o criticas
* El auditor de TI debería entender los procedimientos generales para cada función

# Los procedimientos de Control de SI incluyen:

* Estrategia y dirección de las funciones de TI general y gestión de las funciones de TI
* Acceso a los recursos de TI, incluyendo datos y programas
* Metodologías de desarrollo de sistemas y control de cambios
* Procedimientos de operaciones
* Programación de sistemas y funciones de soporte técnico
* Procedimientos de aseguramiento de calidad (QA)
* Controles de acceso físico
* Planificación de continuidad del negocio (BCP)/recuperación en caso de desastre (DRP)

## Controles específicos de TI

Después de identificar el riesgo se pueden evaluar controles existentes o diseñar nuevos controles para reducir vulnerabilidades.

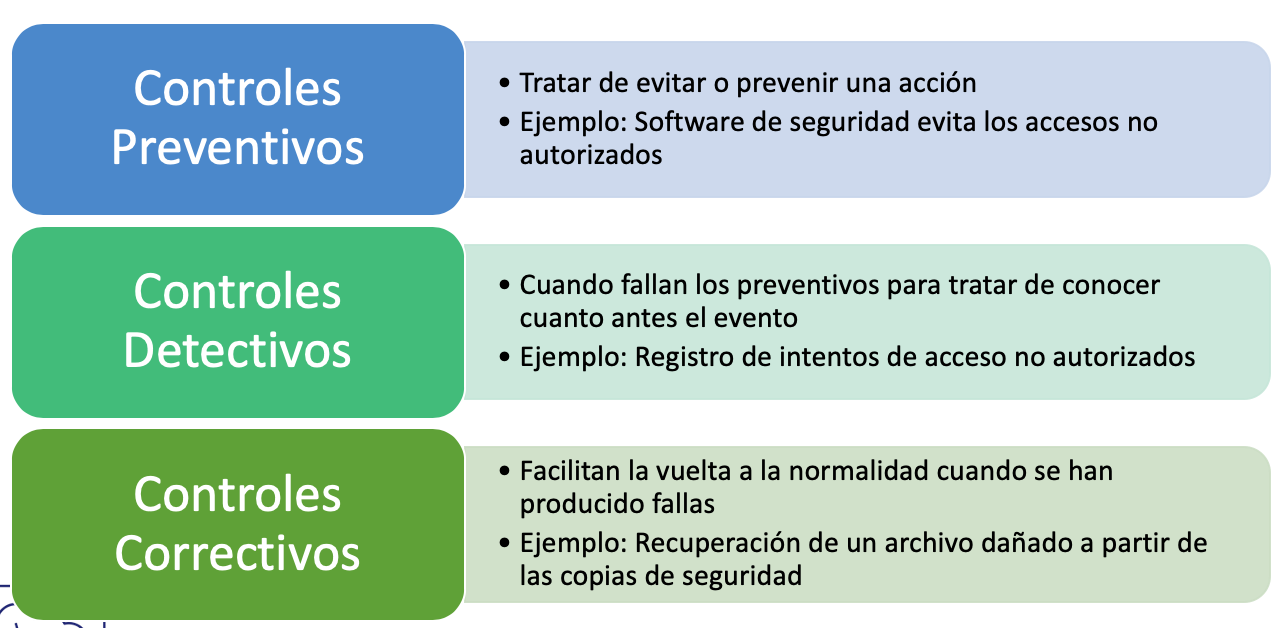
**Estos controles se llaman** → CONTRAMEDIDAS O SALVAGUARDAS

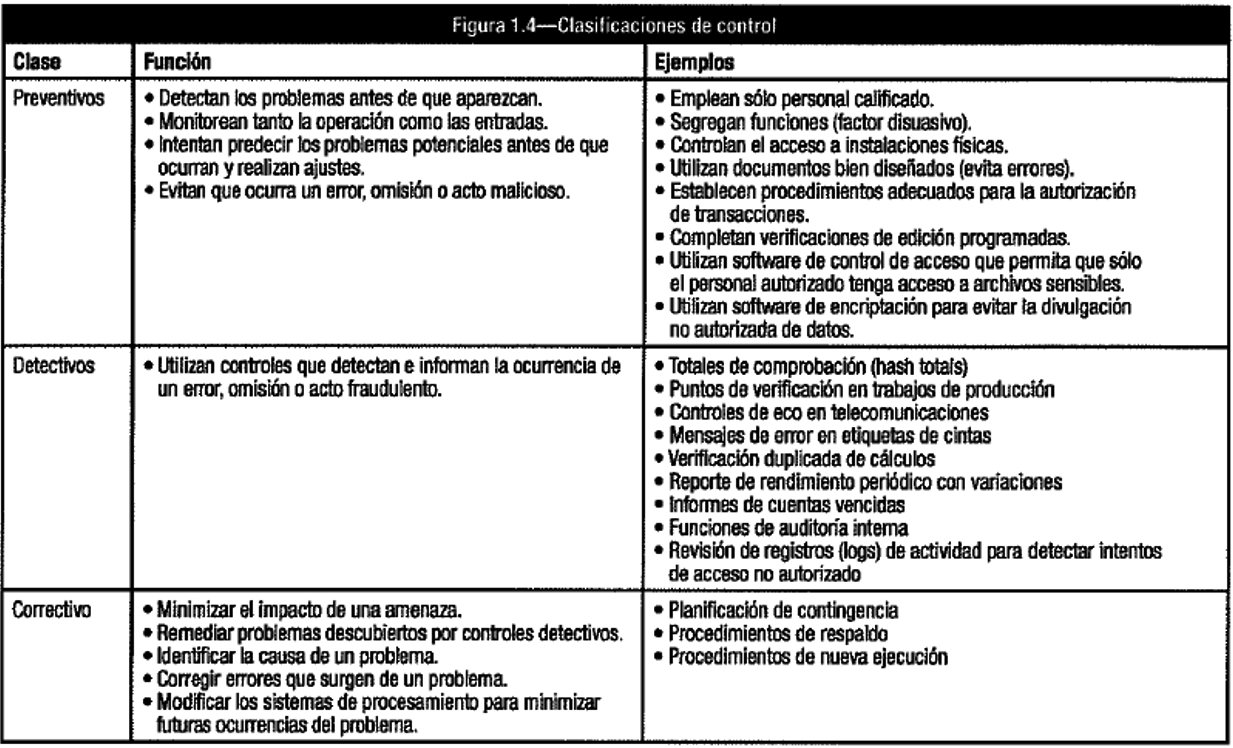
**Incluyen** → acciones, técnicas, medidas

**La fortaleza de un control se mide**→ En términos de su diseño y probabilidad de efectividad

**Entre las características para evaluar su solidez**→ Si son preventivos, detectivos o correctivos

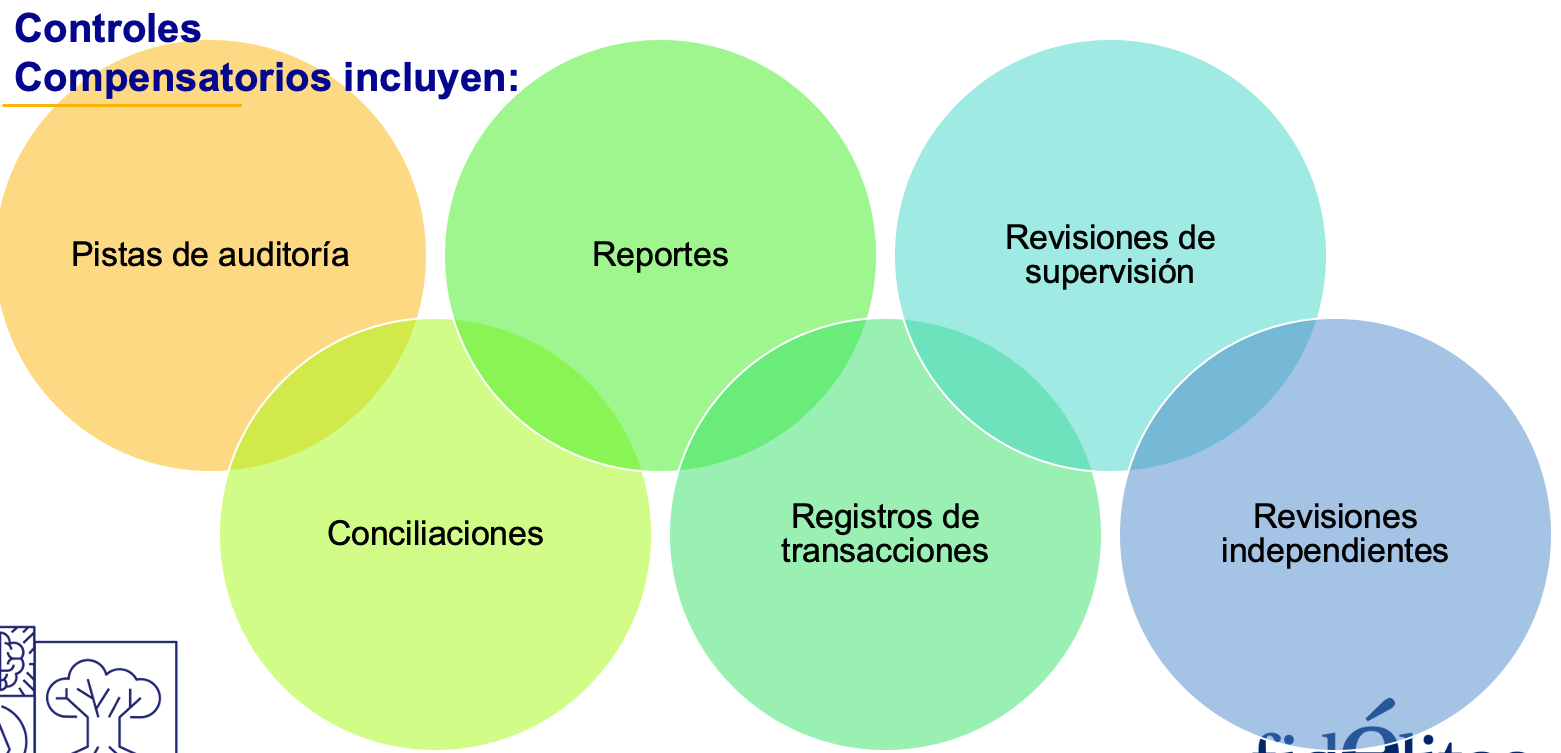
## Importancia y clasificación





## Controles compensatorios y segregación de funciones

* En negocios pequeños deben existir medidas de control compensatorio para mitigar el riesgo de una falta de segregación de funciones.
* Antes de basarse en reportes generados por el sistema o en funciones como controles compensatorios, el auditor de SI debe evaluar cuidadosamente los reportes, las aplicaciones y los procesos relacionados con SI (sistema de información)

s.**.**

# Presentación 3

## Gobierno Corporativo

Relacionado a como la organización mediante ROLES Y RESPONSABILIDADES DE LOS DIRECTORES Y ADMINISTRACION logra:

* Fijar obetivos corporativos
* Ejecutar operaciones diarias
* Monitorear el desempeño
* Integrar a los interesados
* Alinear las actividades
* Cumplir regulaciones

## Expectativas

**Logra TI sus objetivos?** → Desempeño

**Se puede adaptar TI? →** Adaptabilidad

**¿Conoce TI los riesgos, los administra? →** Comprensión

**¿Existe alineación de objetivos vs esfuerzos de TI?** → Sintonía

## Riesgo asociado a TI

* Seguridad de sistemas
* Continuidad de servicio
* Fraudes
* Integridad de datos
* Incidentes
* Aplicativos que no cumplen expectativas

## Ausencia de Gobierno de TI

* Impacta en la aparición de actividades de TI informales en la organización
* Retrabajos
* Baja calidad
* Percepción de un área de gasto sin retorno de inversión

## Administración del Riesgo

Gestión de Riesgo-- Proceso de → Identificar → Vulnerabilidades o amenazas a los recursos de información → decidir contramedidas (protecciones) para reducir el riesgo a niveles aceptables (riesgo residual) basándose en el valor del recurso de información para la organización (ISACA, 2011)



1. Evitar (cuando sea factible) no implementar actividades o procedimientos que generen un riesgo (eliminar el riesgo)

2. Mitigar – definir, implementar, monitorear controles apropiados para reducir el impacto del riesgo

3. Transferir- Compartir el riesgo con socios o cobertura de seguros, acuerdos contractuales

4. Aceptar – reconocer formalmente la existencia del riesgo

## Gestion del Riesgo

* Proceso de identificar y clasificación de recursos o activos que requieren protección
* Puede clasificarse según el valor del activo o modelos estándar de protección

## Perdidas a raíz del riesgo

* Perdida de dinero
* Violacion a lesgislacion
* Perdida de reputacion
* Peligro al personal
* Perdida de oportunidades
* Interrupcion del servicio

En resumen, gestión del riesgo debe lograr un BALANCE ENTRE COSTO DE APLICACION DE CONTROLES DE SEGURIDAD Y LAS AMENAZAS.