

**U**niversidad **T**ecnológica **N**acional **F**acultad **R**egional **R**esistencia

**I**ngeniería en **S**istemas de **I**nformación **Administración de Sistemas de Información** 4° Nivel

**Cuestionarios de estudio Subsistema de Seguridad y Auditoría de los SI/TI**

Elaborado por la cátedra:

* **Ing. Claudia A. SORIA OJEDA** – Responsable de Cátedra
* **Ing. Rosina A. RAMIREZ** – Jefe de Trabajos Prácticos
* **Ing. Raúl A. MONTIEL** – Auxiliar Docente



**ISI**

**UNIDAD DE REFERENCIA: *Seguridad y Auditoría de los SI/TI*.**

**Cuestionario**

# Parte I. Seguridad de SI/TI.

## Bibliografía de Referencia:

* + ROBSON, Wendy. (1999) *Decisiones Estratégicas en Sistemas de Información II*. Tomo 5, Cap. 13: Management responsable de IS. Colección Management Estratégico de Sistemas de Información. MP Ediciones. 2ª edición. Argentina. (Material de Estudio N°7).
  + LARDENT, Alberto R. (2001) *Sistemas de Información para la Gestión Empresaria -Procedimientos, Seguridad y Auditoría*. Editorial Prentice Hall Pearson Educación. Brasil.
  + PIATTINI, Mario ; DEL PESO Emilio. (2006) *Auditoría Informática. Un enfoque práctico.*

## Material sistematizado disponible en el aula.

**PREGUNTAS.**

1. ¿Qué cuestiones determinan el management de los SI de un modo “seguro”?.

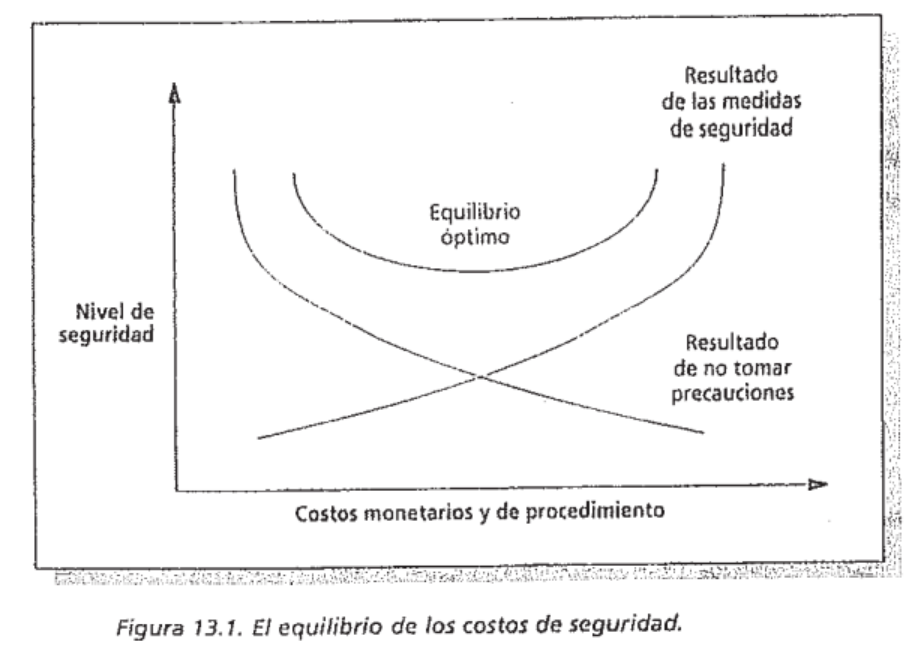
* desde el punto de vista organizacional(técnico)- la vamos a ver en el resto de las materias ‘
* desde el punto de vista social (ético)
* desde el punto de vista judicial (legal)
* estas tres cuestiones pueden superponerse

1. ¿Qué es la pérdida de seguridad?. Cuando esto ocurre, ¿cuáles son los aspectos involucrados?

* puede definirse como la falla de un SI computarizado para realizar la función o brindar el o los servicios para los cuales estaba destinado
* dicha falla puede referirse a la pérdida de uno de los siguientes aspectos
  + disponibilidad
  + integridad
  + confiabilidad

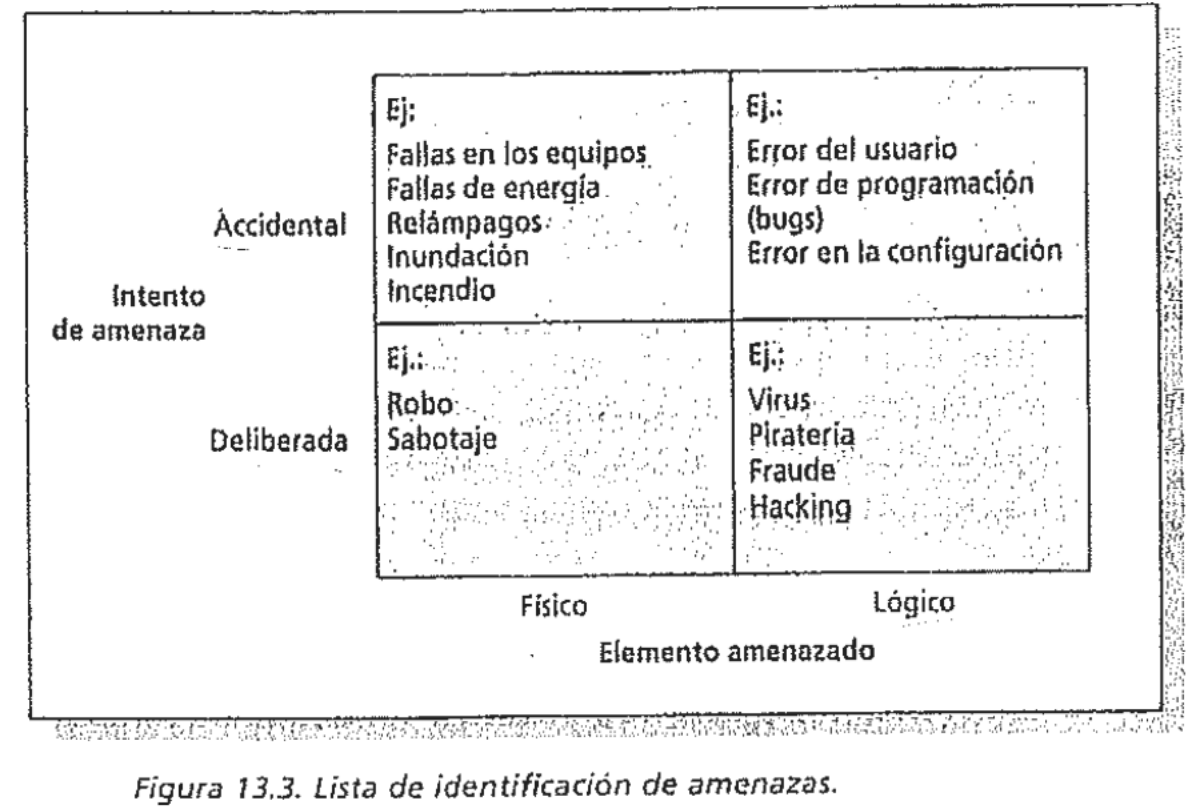
1. ¿Qué es la administración del riesgo?. ¿Cómo se relaciona con la seguridad este concepto?.

* Es el análisis del equilibrio entre los costos resultantes de una falla de seguridad y los costos resultantes de las medidas necesarias para aumentar la seguridad. Este management deberá considerar el equilibrio entre los costos resultantes de una falla en la seguridad y los costos resultantes de las medidas necesarias para aumentar la seguridad. busca el equilibrio óptimo



* El costo de seguridad queda relativamente claro de antemano, mientras que el costo de no tener seguridad puede ser difícil de definir, aun cuando las fallas ocurran. El management del riesgo intenta reducir estas pérdidas. Un enfoque sistemático del management del riesgo permitirá que los IS de seguridad sean administrados de tal forma que reconozcan las vulnerabilidad y la sensibilidad de los sistemas de la empresa, y los datos que estos contienen, pero también los costos en términos sociales financieros técnicos de los controles y las medidas para el manejo del riesgo. ningún sistema puede ser completamente seguro. el management sistemático permite elegir e implementar las contramedidas de una forma planeada y administradas

1. Enumerar y sintetizar las etapas de la administración del riesgo.
2. Identificación del riesgo:
   * la organización busca identificar todos los riesgos a los que está potencialmente expuesta, es decir a los que es vulnerable. para esto se necesitan dos cosas
     1. conocimiento detallado del trabajo de la organización (consultores internos)
     2. conocimiento de las áreas que tienden a la vulnerabilidad es decir la comprensión del riesgo probable (consultores externos)
   * se trata de encontrar los puntos débiles, es decir la identificación de
     1. fuertes amenazas potenciales
     2. activos que son vulnerables a la pérdida
     3. ubicación de esos riesgos



* + un método alternativo de identificación del riesgo es considerar las amenazas sistemáticamente a través de la vulnerabilidad de
    1. activos específicos: ¿que le puede pasar a este activo en particular?
    2. riesgo genérico: ¿como somos vulnerables a este tipo de riesgo?
  + muchas amenazas potenciales provienen de algun punto débil en alguna de las siguientes áreas
    1. fabricación
    2. mantenimiento
    3. diseño
    4. capacitación del usuario
    5. procedimientos de operación

1. Análisis del riesgo: aquí la organización debe cuantificar la probabilidad y la frecuencia esperada de ocurrencia de cada riesgo identificado, y también evaluar la probable gravedad de las consecuencias

fOrmulas 147 y 148

1. Manejo del riesgo: una vez identificado y analizado el patrón de exposición al riesgo, la organización prosigue con la selección de controles y contramedidas a fin de alcanzar la posición de seguridad óptima

buscar el mejor metodo de manejo de riesgo

1. Recuperación del desastre: ya que ningún proceso de management de seguridad puede ser absoluto, debería existir paralelamente a las otras tres etapas un planeamiento de contingencia para la recuperación después de un desastre. el plan de recuperación se controla, revisa y pone a prueba en forma continua
2. ¿Cómo se clasifican las políticas de seguridad? → permisiva y prohibitiva

* Seguridad informática en general: Se menciona la seguridad de los sistemas de información. El objetivo es manejar los riesgos relacionados con la visualización y el management de los IS. La política de seguridad define el nivel de seguridad adecuado para lo que se debe proteger.
* Seguridad de acceso lógico y físico: Se discuten controles para proteger el acceso a los sistemas y datos. Las políticas en esta área buscan asegurar la confidencialidad y la integridad de la información.
* Seguridad en la red e Internet: Las fuentes abordan la seguridad en redes y sistemas distribuidos. Se mencionan controles para la transmisión de datos y la comunicación entre dispositivos.
* Seguridad en sistemas de base de datos: Se trata de la seguridad en los datos almacenados en bases de datos, incluyendo el control de acceso y la modificación de datos y programas.
* Seguridad de aplicaciones instaladas: Se mencionan controles aplicados a los programas de aplicación para asegurar la integridad de los datos de entrada, el procesamiento y la generación de reportes.
* Seguridad organizacional y administración del ambiente informático: Se refiere a la estructura, políticas y procedimientos generales de seguridad dentro de la organización, incluyendo la segregación de funciones y la gestión de recursos

1. ¿Qué es el delito informático?. ¿Quienes son los artífices del mismo y con qué modalidad operan?.

* El delito informático se presenta como una de las causas de violaciones contra el acceso lógico. Se clasifica dentro de las amenazas deliberadas contra los sistemas de información. Estas amenazas deliberadas buscan dañar la información almacenada electrónicamente
* En cuanto a quienes cometen el delito informático (los "artífices"), las fuentes no ofrecen una clasificación detallada de perfiles de delincuentes (como internos, externos, etc.). Sin embargo, mencionan a los "hackers" específicamente en el contexto de los intentos de acceso no autorizado. Las fuentes también distinguen claramente entre los "riesgos accidentales o colapsos (errores) del sistema" (como errores humanos o fallas de equipo) y los "riesgos deliberados", lo que implica que los delitos informáticos son resultado de acciones intencionadas llevadas a cabo por individuos o grupos.
* Respecto a la modalidad con la que operan, las fuentes identifican el delito informático con las amenazas deliberadas. Estas amenazas pueden tomar varias formas:
  + Robo.
  + Fraude
  + Sabotaje
  + Hacking: Intentos de acceso no autorizado a un sistema. Parte de estos intentos pueden estar impulsados por la curiosidad, careciendo de finalidad delictiva, pero la intención de dañar es lo que los convierte en delito.
  + La implantación de virus también se menciona como una modalidad. Los virus pueden ser creados por errores de programación o de forma deliberada.
  + Otras acciones deliberadas incluyen el acceso a programas sin autorización y la modificación de resultados.
* En resumen, se define el delito informático como una violación del acceso lógico derivada de acciones deliberadas que buscan dañar los sistemas de información. Aunque no perfilan a los perpetradores en detalle, mencionan a los "hackers" y listan las modalidades de operación como robo, fraude, sabotaje, hacking y la implantación de virus.

# Parte II. Auditoría de SI/TI.

1. ¿Qué es la auditoría de sistemas de información?

Según las fuentes proporcionadas, podemos definir la **Auditoría de Sistemas de Información** de la siguiente manera:

* Es una **disciplina independiente de la Auditoría General**.
* Se define como la **revisión imparcial de las operaciones empresarias y los controles relacionados a la utilización de los Sistemas de Información (IS)**.
* Tiene como **objetivo** asegurar propiedades como la **integridad, operatividad y confidencialidad de la información**.
* Desde el punto de vista del auditor, se enfoca en la visión de los Sistemas de Información, el **cumplimiento de los objetivos gerenciales** y la **eficiencia del sistema**.
* El objetivo de la auditoría de sistemas de información es **identificar, analizar y evaluar los requerimientos del usuario**, basando el análisis en **riesgos** y **puntos de control**.

La auditoría de sistemas de información puede referirse o enfatizar distintos aspectos, incluyendo, pero no limitándose a, las siguientes áreas o revisiones:

* **Revisión de controles generales:** Afectan las estructuras de la organización, las políticas y procedimientos, y el ambiente de control de los sistemas de información.
* **Revisión de procedimientos de procesamiento de información:** Se refiere a las operaciones que se ejecutan dentro del Centro de Procesamiento de Información y aquellas realizadas fuera de él.
* **Revisión de seguridad:** Abarca la revisión de la **calidad del acceso lógico, del acceso físico y de los controles del ambiente informático**. También incluye la revisión de las políticas de seguridad formuladas por la empresa.
* **Revisión del software del sistema operativo:** Se relaciona con la revisión de las políticas y procedimientos de desarrollo, y con la adquisición y mantenimiento del software del sistema operativo.
* **Revisión de la metodología para el desarrollo de sistemas:** Abarca la metodología empleada, las normas y los procedimientos para el desarrollo, adquisición y mantenimiento del software.
* **Revisión de los controles del software de aplicación:** Comprende la revisión y evaluación de las fortalezas y debilidades de los puntos de control y procedimientos de control que deben permanecer intactos en los sistemas de aplicación de la organización.
* **Plan de organización:** Consiste en verificar la existencia y aplicación de políticas y procedimientos referentes a la recuperación de desastres y la continuidad de operaciones en caso de presentación de desastres.

En la práctica, una auditoría de sistemas de información implica la **verificación de la evidencia de auditoría** y la aplicación de **técnicas de auditoría asistidas por computadora (CAATs)**. El proceso de ejecución de una auditoría de sistemas de información sigue diversas etapas.

1. ¿Qué es el control interno? Desarrolle las clasificaciones de control. Ejemplifique cada una.

**¿Qué es el Control Interno?**

El control interno es definido como **el plan de organización, la asignación y separación de funciones, y el conjunto coordinado de medios y métodos adoptados dentro de una empresa** [141, p. 266]. Su propósito es **proteger los activos, verificar la exactitud y fiabilidad de los datos contables y operativos, promover la eficiencia en la operación y estimular la adhesión a la política de la empresa** [141, p. 266]. Desde la perspectiva de la auditoría de sistemas de información, los tipos de control constituyen los **componentes de un sistema de control interno** [135, p. 266]. Los objetivos del control interno son válidos sin importar el ambiente [142, p. 268].

**Clasificaciones de Control**

Las fuentes presentan o implican varias formas de clasificar los controles, principalmente en el contexto de la auditoría de sistemas de información y la seguridad. Dos clasificaciones principales que se derivan de las fuentes son:

1. **Según el momento de actuación o propósito:**
   * **Controles Preventivos:** Buscan **evitar errores o sucesos no deseados antes de que ocurran** [143, p. 270]. En el ámbito de la seguridad, la "Prevención" es la primera etapa que busca evitar la amenaza [217, p. 162].
     + *Ejemplo según las fuentes:* El control de software, la aplicación de control de software [143, p. 270]. Controles de acceso virtual o físico [143, p. 270].
   * **Controles Detectivos:** Buscan **identificar errores o sucesos no deseados una vez que han ocurrido** [143, p. 270]. En seguridad, la "Detección" es la segunda etapa, buscando detectar fallas o errores después de que la prevención falla [217, p. 162].
     + *Ejemplo según las fuentes:* La corrección de errores [143, p. 270]. El análisis de errores ya realizados [143, p. 270]. La verificación de evidencia de violación [143, p. 270].
   * **Controles Correctivos:** Buscan **subsanar (corregir) errores o sucesos no deseados una vez que han sido identificados** [143, p. 270]. En el contexto de la seguridad, la "Recuperación" es la tercera etapa, que se ocupa de la recuperación de fallas de seguridad o errores [217, p. 162]. Estos controles se aplican *después* de que un suceso o acto ha ocurrido o para subsanar su aparición [143, p. 270].
     + *Ejemplo (basado en el concepto de Recuperación en seguridad):* Un procedimiento de recuperación de desastres que involucra restaurar sistemas y datos a partir de copias de seguridad [223, p. 176; 224, p. 177]. (Aunque el ejemplo específico de "Acceso a la seguridad a través de la validación del acceso" dado en para Correctivos parece más relacionado con la detección).
2. **Según el alcance o área de aplicación:**
   * **Controles Generales:** Afectan las **estructuras de la organización, las políticas y procedimientos, y el ambiente de control de los sistemas de información** [144, p. 272; 136, p. 257]. Se relacionan con los procedimientos de control que permanecen intactos en los sistemas de aplicación de la organización [144, p. 272].
     + *Ejemplo según las fuentes:* El plan de organización de la empresa [141, p. 267]. La segregación de funciones [141, p. 267; 159, p. 306; 160, p. 309]. Las políticas y procedimientos generales de seguridad [144, p. 272].
   * **Controles Específicos (o de Aplicación):** Se refieren a los **procedimientos de procesamiento de información**, es decir, las operaciones que se ejecutan *dentro* y *fuera* del Centro de Procesamiento de Información [144, p. 272]. Comprenden la revisión y evaluación de los puntos y procedimientos de control específicos de los sistemas de aplicación [144, p. 272].
     + *Ejemplo según las fuentes:* Controles aplicados a los programas de aplicación para asegurar la integridad de los datos de entrada, el procesamiento y la generación de reportes [141, p. 267]. Controles de entrada [141, p. 267], de procesamiento [141, p. 267], de salida [141, p. 267].

Las fuentes también mencionan "controles de organización" en relación con la estructura, políticas y procedimientos [143, p. 270], y listan áreas como "Revisión de controles generales", "Revisión de seguridad", "Revisión de software del sistema operativo", "Revisión de la metodología para el desarrollo de sistemas", "Revisión de los controles del software de aplicación" y "Plan de organización" como revisiones de control importantes en una auditoría de sistemas de información [144, p. 272].

1. ¿Cuáles son los tipos de prueba que se requieren en la Auditoría de SI?.

Basándonos en la información de las fuentes proporcionadas y nuestra conversación previa, podemos describir los tipos de prueba que se requieren en la Auditoría de Sistemas de Información.

Según las fuentes, en el contexto de la Auditoría de Sistemas de Información, existen principalmente dos categorías o **tipos de pruebas** [143, p. 270]:

1. **Pruebas de Cumplimiento** [143, p. 270]
   * **Objetivo:** Estas pruebas están diseñadas para determinar si se han **cumplido los requisitos** [143, p. 270]. Buscan comprobar que los **controles generales y específicos funcionan eficazmente** [143, p. 270].
   * **Foco:** Se centran en verificar que los **procedimientos preventivos fueron ejecutados**, que los **reparos (correcciones) fueron ejecutados**, y que estas acciones fueron llevadas a cabo por **alguien que cumple con los principios de separación de funciones** [143, p. 270].
   * **Ejemplo (según las fuentes):** Un ejemplo de prueba de cumplimiento en el Departamento de Cuentas a Pagar y Recepción implica la **aplicación de control de software** [143, p. 271].
2. **Pruebas Sustantivas** [143, p. 270]
   * **Objetivo:** El propósito principal de estas pruebas es **verificar la evidencia de auditoría** [143, p. 270; 148, p. 281]. Se aplican a los **saldos o al detalle de las transacciones** [146, p. 277; 147, p. 277].
   * **Base:** Estas pruebas se basan en un **análisis de riesgos** y con frecuencia implican la aplicación de **Técnicas de Auditoría Asistidas por Computadora (CAATs)** [143, p. 270]. Las CAATs son herramientas que permiten a los auditores examinar grandes volúmenes de datos y registros del sistema de información [135, p. 255; 148, p. 282; 149, p. 283].
   * **Aplicación en SI:** En el contexto de la auditoría de sistemas de información, las pruebas sustantivas implican verificar la información y los datos procesados por los sistemas, como el **saldo de las transacciones** [149, p. 283].

En la práctica de la auditoría de sistemas de información, la **verificación de la evidencia de auditoría** y la aplicación de **Técnicas de Auditoría Asistidas por Computadora (CAATs)** son componentes esenciales de la ejecución de una auditoría [135, p. 255]. Las CAATs pueden incluir programas específicos para verificar la integridad y corrección de programas de aplicación, o software de auditoría general para examinar datos [149, p. 283]. Esto subraya que las pruebas sustantivas, al requerir la verificación de datos y transacciones, a menudo dependen de herramientas tecnológicas en un ambiente de sistemas de información [137, p. 258; 149, p. 283].

1. Para cada área de Auditoría determine:
   1. Concepto
   2. Funciones del Auditor
   3. Síntesis de los elementos a auditar

Claro, con base en la información de las fuentes proporcionadas, podemos detallar las principales áreas de la Auditoría de Sistemas de Información y, para cada una, su concepto, las funciones del auditor y una síntesis de los elementos a auditar. Las fuentes [144, p. 272] listan las siguientes áreas principales:

**I) Revisión de Controles Generales**

* **Concepto:** Afectan las **estructuras de la organización, las políticas y procedimientos, y el ambiente de control de los sistemas de información (IS)** [144, p. 272]. Se relacionan con los procedimientos de control que deben permanecer intactos en los sistemas de aplicación de la organización [144, p. 272]. Son la base sobre la cual operan los controles de aplicación [141, p. 267].
* **Funciones del Auditor:** El auditor debe verificar que los controles generales y específicos **funcionan eficazmente** [143, p. 270]. Debe verificar que los **procedimientos preventivos fueron ejecutados**, que los **reparos (correcciones) fueron ejecutados**, y que estas acciones fueron llevadas a cabo por **alguien que cumple con los principios de separación de funciones** [143, p. 270]. El objetivo es evaluar la efectividad de los controles generales [151, p. 286]. Se debe verificar la existencia y aplicación de políticas y procedimientos relacionados con la administración del procesamiento de información [152, p. 288].
* **Síntesis de los elementos a auditar:**
  + Plan de organización de la empresa [141, p. 267; 152, p. 288].
  + Segregación y asignación de funciones y responsabilidades [141, p. 267; 152, p. 288; 160, p. 306; 159, p. 306].
  + Políticas y procedimientos generales (seguridad, administración del procesamiento de información, etc.) [144, p. 272; 152, p. 288; 163, p. 310].
  + Ambiente de control de los sistemas de información [144, p. 272].

**II) Revisión de Procedimientos de Procesamiento de Información**

* **Concepto:** Se refiere a las **operaciones que se ejecutan dentro y fuera del Centro de Procesamiento de Información** [144, p. 272]. Implica la revisión de la **secuencia natural de operaciones** y los procedimientos administrativos y de sistemas de información [8, p. 3]. Esta área abarca el flujo de datos y las operaciones dentro de los sistemas empresariales [6, p. ix].
* **Funciones del Auditor:** El auditor debe evaluar las fortalezas y debilidades de los **puntos de control** y los **procedimientos de control** dentro de los sistemas [144, p. 272]. Se deben verificar los procedimientos de procesamiento de información [152, p. 288]. Se busca verificar la existencia y aplicación de políticas y procedimientos referentes a este procesamiento [152, p. 288]. El auditor examina los controles de entrada, procesamiento y salida de datos [141, p. 267; 156, p. 299].
* **Síntesis de los elementos a auditar:**
  + Operaciones y procedimientos ejecutados en el Centro de Procesamiento de Información y fuera de él [144, p. 272].
  + Controles de entrada de datos [141, p. 267; 156, p. 299; 199, p. 382].
  + Controles de procesamiento de datos [141, p. 267; 156, p. 299].
  + Controles de salida de información y reportes [141, p. 267; 156, p. 299].
  + Flujos de datos y diagramas de procesos (DFD) [192, p. 369].
  + Modalidades de procesamiento (ej. en línea, por lotes) [164, p. 313].

**III) Revisión de Seguridad**

* **Concepto:** Abarca la revisión de la **calidad del acceso lógico, del acceso físico y de los controles del ambiente informático** [144, p. 272]. Incluye la revisión de las **políticas de seguridad** formuladas por la empresa [144, p. 272]. El objetivo de la seguridad informática es asegurar la **integridad, operatividad y confidencialidad** de la información [6, p. ix; 132, p. 249; 135, p. 254]. Implica la gestión de los riesgos [132, p. 249].
* **Funciones del Auditor:** Verificar la calidad del acceso lógico y físico [144, p. 272]. Revisar los controles del ambiente informático [144, p. 272]. Examinar las políticas de seguridad formuladas [144, p. 272; 163, p. 310]. Evaluar las medidas de seguridad [157, p. 301]. Verificar el cumplimiento de las políticas de seguridad [162, p. 309; 163, p. 310; 189, p. 361]. Revisar la calidad de los accesos (lógico y físico) [162, p. 309; 163, p. 310]. Analizar los riesgos [206, p. 139].
* **Síntesis de los elementos a auditar:**
  + Controles de acceso lógico (contraseñas, validación de usuarios) [144, p. 272; 162, p. 309; 169, p. 322; 178, p. 340].
  + Controles de acceso físico (seguridad del edificio, centros de cómputos) [144, p. 272; 162, p. 309; 178, p. 340].
  + Controles del ambiente informático (ej. ambiente físico del centro de cómputos) [144, p. 272; 162, p. 309].
  + Políticas de seguridad [144, p. 272; 163, p. 310; 157, p. 301].
  + Seguridad en sistemas de base de datos [178, p. 340].
  + Seguridad de redes y sistemas distribuidos [185, p. 355].
  + Integridad, operatividad y confidencialidad de la información [6, p. ix; 132, p. 249].
  + Manejo de riesgos de seguridad [132, p. 249; 204, p. 137].

**IV) Revisión del Software del Sistema Operativo**

* **Concepto:** Se relaciona con las **políticas y procedimientos de desarrollo, adquisición y mantenimiento del software del sistema operativo** [144, p. 272]. El software del sistema operativo es fundamental para el funcionamiento del hardware y software de aplicación [180, p. 345; 158, p. 303].
* **Funciones del Auditor:** Revisar las políticas y procedimientos para el desarrollo, adquisición y mantenimiento [144, p. 272]. Verificar la integridad y corrección de los programas del sistema operativo [29, p. 29; 176, p. 337]. Comprobar que las modificaciones al software del sistema operativo estén autorizadas y documentadas [176, p. 337; 177, p. 338; 183, p. 350]. Verificar la seguridad relacionada con el sistema operativo [176, p. 337; 177, p. 338].
* **Síntesis de los elementos a auditar:**
  + Políticas y procedimientos de desarrollo, adquisición y mantenimiento del sistema operativo [144, p. 272].
  + Integridad y corrección de los programas del sistema operativo [29, p. 29; 176, p. 337].
  + Modificaciones al software del sistema operativo [176, p. 337; 177, p. 338; 183, p. 350].
  + Aspectos de seguridad del sistema operativo [176, p. 337; 177, p. 338].
  + Documentación del software del sistema operativo [176, p. 337].
  + Software de sistema [158, p. 303].

**V) Revisión de la Metodología para el Desarrollo de Sistemas**

* **Concepto:** Abarca la **metodología empleada, las normas y los procedimientos para el desarrollo, adquisición y mantenimiento del software** [144, p. 272; 191, p. 366]. Se centra en el **ciclo de vida del desarrollo de sistemas** [190, p. 363]. Busca asegurar la calidad y confiabilidad de los sistemas implementados [190, p. 363].
* **Funciones del Auditor:** Revisar y evaluar la metodología, normas y procedimientos [144, p. 272; 191, p. 366]. Verificar el cumplimiento de la metodología [191, p. 366]. Revisar la documentación de cada etapa del ciclo de vida [191, p. 366; 194, p. 373]. Revisar las pruebas realizadas durante el desarrollo [192, p. 369; 193, p. 370]. Evaluar la planificación y la viabilidad del proyecto [190, p. 363; 191, p. 366]. Revisar el diseño lógico y físico [191, p. 366; 192, p. 369]. Evaluar la implementación [193, p. 370]. Revisar los procedimientos de mantenimiento [194, p. 373]. Identificar riesgos asociados [195, p. 375].
* **Síntesis de los elementos a auditar:**
  + Metodología de desarrollo de sistemas [144, p. 272; 191, p. 366].
  + Normas y procedimientos de desarrollo, adquisición y mantenimiento [144, p. 272; 191, p. 366; 196, p. 376].
  + Ciclo de vida del desarrollo de sistemas [190, p. 363].
  + Requisitos del sistema [191, p. 366].
  + Diseño lógico y físico del sistema [191, p. 366; 192, p. 369].
  + Programación y pruebas (testing) [192, p. 369; 193, p. 370].
  + Documentación del sistema (requisitos, diseño, programación, pruebas, usuario) [194, p. 373; 191, p. 366].
  + Implementación del sistema [193, p. 370].
  + Procedimientos de mantenimiento [194, p. 373].
  + Riesgos asociados a la metodología [195, p. 375].

**VI) Revisión de los Controles del Software de Aplicación**

* **Concepto:** Comprende la **revisión y evaluación de las fortalezas y debilidades de los puntos de control y procedimientos de control que deben permanecer intactos en los sistemas de aplicación de la organización** [144, p. 272; 197, p. 379]. Los sistemas de aplicación capturan, procesan, almacenan y suministran información [197, p. 379]. Los controles buscan asegurar la **integridad, validez y exactitud** de los datos [197, p. 379].
* **Funciones del Auditor:** Revisar y evaluar los puntos y procedimientos de control en las aplicaciones [144, p. 272]. Identificar y analizar las debilidades [198, p. 380]. Evaluar los controles de entrada, procesamiento y salida de datos en las aplicaciones [198, p. 380; 199, p. 382; 200, p. 384]. Verificar el funcionamiento de las funciones de control [198, p. 380]. Comprobar la eficiencia de las operaciones y los controles [198, p. 380]. Verificar el cumplimiento de los objetivos de la aplicación [198, p. 380]. Revisar el código fuente o ejecutable de los programas [196, p. 376; 197, p. 379]. Verificar las modificaciones realizadas a los programas [196, p. 376; 197, p. 379]. Revisar la documentación [197, p. 379].
* **Síntesis de los elementos a auditar:**
  + Puntos de control en los sistemas de aplicación [144, p. 272; 197, p. 379].
  + Procedimientos de control en los sistemas de aplicación [144, p. 272; 197, p. 379].
  + Controles de entrada, procesamiento y salida específicos de cada aplicación [198, p. 380; 199, p. 382; 200, p. 384].
  + Código fuente o ejecutable de los programas de aplicación [196, p. 376; 197, p. 379].
  + Documentación de los sistemas de aplicación [197, p. 379].
  + Modificaciones a los programas de aplicación [196, p. 376; 197, p. 379].

**VII) Plan de Organización (Relacionado con Continuidad del Negocio y Recuperación de Desastres)**

* **Concepto:** Consiste en verificar la **existencia y aplicación de políticas y procedimientos referentes a la recuperación de desastres y la continuidad de operaciones en caso de presentación de desastres** [144, p. 272]. Se relaciona con el plan general de la empresa para la asignación de funciones y procesamiento de información [152, p. 288]. El objetivo es minimizar el impacto de un desastre y asegurar la continuidad del negocio [223, p. 176; 224, p. 177].
* **Funciones del Auditor:** Verificar la existencia y aplicación de políticas y procedimientos de recuperación de desastres y continuidad [144, p. 272]. Revisar el plan de organización general [152, p. 288]. Evaluar el plan de recuperación de desastres y continuidad del negocio [223, p. 176; 224, p. 177]. Verificar que existan procedimientos para recuperar operaciones críticas [223, p. 176]. Evaluar si el plan es adecuado y probado (aunque las pruebas pueden ser difíciles) [224, p. 177].
* **Síntesis de los elementos a auditar:**
  + Políticas y procedimientos de recuperación de desastres [144, p. 272; 223, p. 176].
  + Políticas y procedimientos de continuidad del negocio [144, p. 272; 223, p. 176].
  + Plan de recuperación de desastres [223, p. 176].
  + Plan de continuidad de operaciones [223, p. 176].
  + Procedimientos de recuperación de datos y sistemas [223, p. 176].
  + Ubicaciones de respaldo (cold sites, hot sites) [223, p. 176; 224, p. 177].
  + Personal clave y responsabilidades en caso de desastre [223, p. 176].

1. Auditoría del desarrollo: efectúe un cuadro comparativo entre el enfoque de Lardent y el de Piattini&Del Peso.

La auditoría es una evaluación, es decir que tiene un patrón de comparación, es uno de los dos procesos de gestión de seguridad de los SI/TI

objeto de audito: área a auditar

cualquier auditoria es una actividad consistente en

* contenido
* condición
* justificación
* objeto
* finalizad

los tipos de auditoria, segun su naturaleza

* financiera
* administrativa
* de gestión de recursos humanos, de calidad
* de sistemas de información

definición y tipo de controles internos

preventivos: se realizan para evitar los problemas o fallas

detectivos: cuando fallan los preventivos se intentan detectar lo antes posible las razones

correctivos: facilitan el retorno al funcionamiento “correcto”

implantacion de un sistema de controles internos informáticos

para esto es necesario

* entorno de red
* configuración del entorno

...

para esto hay que definir

* gestión del sistema de información
* administración de sistemas
* seguridad
* gestión de cambio

Aspectos procedimentales claves de la auditoría

1. no puedo empezar una auditoría si no defino el alcance y los objetivos, es decir, el objeto a estudiar
2. realizar el estudio del entorno a auditar
3. ejecución del programa de revisión
4. cierre de revisión
5. realizar el informe final
6. seguimiento

evaluaiocn de la funcion inf

de sistemas y proc

audit desarrollo

y no se q mas

riesgos del auditor (etapa inicial)

la posibilidad que la información obtenida tenga algún tipo de error que no se puede detectar un error que ha ocurrido

* inherentes: propios de la naturaleza de la actividad
* de control: no puede ser evitado o detectado por el sistema de control interno
* de detección: pruebas exitosas con las pruebas erróneas

El concepto está relacionado con el de materialidad, que se refiere a la magnitud del error en términos del impacto potencial para el conjunto de la organización. En general, esa materialidad es expresada en términos monetarios

principio de independencia

independencia de criterio

el auditor interno tiene que auditar el control interno y no puede estar involucrado con las aplicaciones que el mismo puede auditar, pero si puede proponer