

Cuestionario N° 9: Seguridad y Auditoría de Sistemas de Información

Indicación: La respuesta a los puntos 2, 3, 8 y 13 requieren de la elaboración de conceptos, de investigación bibliográfica y en Internet por parte del alumno. Las restantes consignas se refieren temas que constituyen los conceptos principales del Subsistema de Control de SW y HW y tienen como fin establecer el orden temático desarrollado en clase y guiar el estudio de los mismos.

Laura

Referencias:

No importante

Importante (Lo que pide la preguntante)

Bel

PARTE I. Seguridad en el ambiente informático.

1. Conceptualizar el proceso de control de SI/TI.

Sacado del capítulo 2 del libro de auditoría informática.

El proceso de control de SI/TI se puede conceptualizar como un conjunto de actividades y procedimientos diseñados para garantizar que los sistemas informáticos y las tecnologías utilizadas en una organización operen de manera eficiente, segura y alineada con los objetivos estratégicos de la empresa. Cíclico y repetitivo.

Este proceso incluye varias etapas:

- **Definición de objetivos de control:** Se establecen metas claras que los controles deben alcanzar, basadas en los riesgos y necesidades de la organización.
- **Identificación de riesgos:** Se evalúan los riesgos asociados a los SI y las TI. Se identifican vulnerabilidades y amenazas que podrían afectar la integridad y confidencialidad de la disponibilidad de la información.
- **Diseño de controles:** Controles específicos para mitigar riesgos. Pueden ser preventivos o detectivos.
- **Implementación de controles:** Se incluye aquí, además de la implementación en los sistemas y procesos, a la capacitación del personal y la creación de documentos que guíen su uso.

- **Monitoreo y evaluación:** Se realiza un seguimiento continuo de la efectividad de los controles. Aquí se incluyen las auditorías internas y revisiones periódicas para asegurar que los controles estén funcionando como se espera y que cumplan con los objetivos de control establecidos.
- **Mejora continua:** Ajustes y mejoras en los controles y procesos.

2. Elabore un concepto de ambiente informático. Ejemplifique.

Página 32 del capítulo 2 del libro de auditoría informática. No habla específicamente pero se puede relacionar la Info con el concepto armado a continuación:

Ambiente informático: Conjunto de elementos y condiciones que interactúan en un sistema de información. Este ambiente incluye tanto los componentes físicos como los lógicos que permiten el funcionamiento de los SI/TI facilitando el procesamiento y la gestión de la información en una organización. Soporta las operaciones diarias, facilita la comunicación y la gestión de información, y permite la automatización de procesos. *Osea sus recursos y todos los sectores de la organización asociados al procesamiento de la información.*

Ejemplos:

- **Hardware:** Un servidor que aloja una base de datos de clientes y una impresora que genera informes de ventas.
- **Software:** Un ERP (Sistema de gestión empresarial) que ayuda a la organización a gestionar sus recursos y procesos como SAP.
- **Redes:** Una red LAN que conecta las computadoras de una oficina y permite el acceso a un servidor central.
- **Procedimientos:** Un proceso que establece cómo se deben manejar los datos sensibles de clientes para cumplir con las regulaciones de privacidad.
- **Personas:** Un equipo de soporte técnico que ayuda a los empleados a resolver problemas con el software.
- **Entorno físico:** Un centro de datos diseñado para mantener condiciones óptimas de temperatura y humedad para los servidores.

Otro ejemplo más completo:

Ejemplos:

En una empresa de comercio electrónico, el ambiente informático incluiría:

- **Hardware:** Servidores, ordenadores, dispositivos móviles y periféricos.
- **Software:** Aplicaciones de gestión de inventario, plataformas de comercio electrónico, sistemas de gestión de relaciones con clientes (CRM), y software de análisis de datos.
- **Redes:** Conexiones de red internas, acceso a internet, y redes de comunicación entre sucursales.

- **Datos:** Bases de datos de clientes, registros de ventas, información de inventarios y datos financieros.
- **Procedimientos:** Políticas de seguridad, protocolos de backup, y procedimientos de recuperación ante desastres.

3. ¿Por qué se “controla” el ambiente informático?

El control del ambiente informático es una práctica crucial para mantener la integridad, seguridad y eficiencia de los recursos tecnológicos en una organización, alineándolos con sus objetivos estratégicos y asegurando su funcionamiento continuo y fiable. Algunas razones puntuales son:

- Seguridad de la información: Proteger la confidencialidad, integridad y disponibilidad de la información.
- Cumplimiento normativo: Existen leyes de protección de datos y estándares de seguridad de la información que se deben cumplir, u otras regulaciones a las que esté sujeta la organización sobre sus sistemas de información.
- Eficiencia operativa: Los controles ayudan a optimizar los procesos y asegurar que funcionen eficientemente.
- Gestión de riesgos: Permiten a las organizaciones anticipar y responder a posibles amenazas.
- Mejora continua: Permite a las organizaciones mejorar continuamente sus procesos y sistemas y esto es vital porque el entorno tecnológico está en constante cambio.
- Protección de activos: Los SI son activos valiosos para la organización.
- Responsabilidad y auditoría: Los controles facilitan la rendición de cuentas y de auditoría de los si.
- Costos???? :Gestionar y reducir los costos asociados con el mantenimiento y la operación de los sistemas informáticos. (Este lo agregué yo)

ROBSON, Wendy. “Decisiones Estratégicas en Sistemas de Información II”. Tomo 5, Cap. 13:

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

La gestión de seguridad de los Sistemas de información consisten en la administración de modo seguro, son seguros si poseen:

Seguridad desde los puntos de vista

- organización(seguridad técnica),
- social (éticos)
- y judicial (legal)

ROBSON, Wendy. “Decisiones Estratégicas en Sistemas de Información II”. Tomo 5, Cap. 13.

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

La pérdida de seguridad se da cuando se produce una falla de los elementos de un SI o a la pérdida de unos o todos los siguientes aspectos:

- **Disponibilidad:** Cuando debido a fallas en HW/SW se interrumpe el normal curso de actividades, o se pierde, aunque no es necesaria actualmente, la posibilidad de realizar alguna tarea.
- **Integridad:** Si los datos almacenados no se condicen con los elementos de la realidad a los que hacen referencia.
- **Confiability:** Cuando la información no pierde integridad, la operatividad/disponibilidad no se afecta, pero hay acceso NO AUTORIZADO a información vital d la empresa y debe mantenerse privada

ROBSON, parte ii Tomo 5, Cap. 13.1

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

extra contexto:

Las organizaciones deberán considerar el equilibrio entre costos resultantes de una falla de seguridad y los costos de las medidas necesarias para aumentarla, ya que un fallo podría comprometer su funcionamiento durante un cierto tiempo.

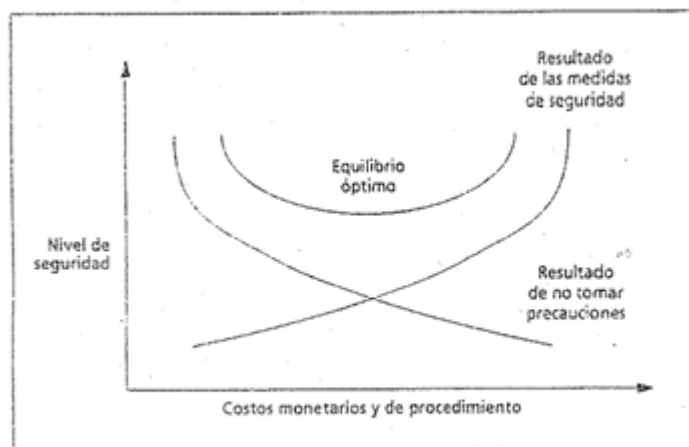


Figura 13.1. El equilibrio de los costos de seguridad.

El management/gestión del riesgo intenta:

- reducir las pérdidas producidas por las fallas de seguridad de un SI,
- administran los SI de forma que reconozcan:
 - la vulnerabilidad
 - y sensibilidad de los sistemas y los datos que contienen,
 - costos (sociales, financieros y técnicos) del control y las medidas para el manejo del riesgo
- Ningún sistema puede ser completamente seguro, el management permite elegir e implementar medidas de forma planeada y administrada.

La administración del riesgo busca reducir estas pérdidas, obtener el mejor equilibrio entre el costo producido por una pérdida de seguridad y el costo que implica implementar medidas que disminuyan las posibilidades de ocurrencia.

RELACION SEGURIDAD Y ADM DE RIESGO: La relación con la seguridad es que como “la seguridad total es imposible”, no se puede asegurar la seguridad al 100%, pero se puede buscar un nivel razonable de seguridad, y EL MECANISMO que busca la mejor opción a la hora de obtener un nivel razonable de seguridad ES LA ADMINISTRACIÓN DEL RIESGO,

- ROBSON, parte ii Tomo 5, Cap. 13.1.1

7. Enumerar y sintetizar las etapas de la administración del riesgo.

extra contexto:

Existen distintas metodologías para la administración de riesgos (análisis cualitativo o análisis cuantitativo, GRAMM, Riskpac, SRA)

Independientemente de la metodología, **el management de seguridad de los si se reduce a cuatro etapas:**

- 1. Identificación del riesgo**
- 2. Análisis del riesgo**
- 3. Manejo del riesgo**
- 4. Recuperación del desastre**

1 Identificación del riesgo: la organización busca identificar todos los riesgos a los que está potencialmente expuesto.

Para ello se debe tener conocimiento detallado de la organización y las áreas que tienden a la vulnerabilidad, a través de consultores internos y externos.

- Consultores Internos: identifican las amenazas específicas con una profunda comprensión de la empresa.
- Consultores Externos: poseen amplio conocimiento.

Un análisis sistemático y organizado de riesgos se trata de encontrar puntos débiles:

- Fuentes de amenazas potenciales (clasificarlas según los tipos)
- **Activos que son vulnerables a la pérdida (recursos financieros, software: datos, informacion, codigo, sist op de pc y servidores, aplicaciones de gestion o offmatica, hardware:estaciones de trabajo, servidor, rack de comunicaciones)**
- Ubicación de los riesgos.

Existen categorías de **Tipos de amenazas:** (HACER CUADRITO)

- Física: robo, incendios, energía
o
- Lógica: virus, hacking.
y
- deliberadas: robo, fraude, daño malicioso.
o
- accidentes: como inundaciones, incendios, errores humanos.

Ej tp samsung Filtración de información confidencial.

	ELEMENTO AMENAZADO		
INTENTO DE AMENAZA		LÓGICO	FÍSICO
	ACCIDENTAL	Filtración de información confidencial. (Pasivo) Error del usuario: Filtración de información confidencial a ChatGPT porque los usuarios no son conscientes de las implicancias en el uso de la herramienta.(Pasivo) Error de configuración: Uso indebido de herramientas de IA por falta de controles adecuados para prevenir accesos no autorizados.(Pasivo)	
	DELIBERADO	Robo de información confidencial para el uso de competidores.(Pasivo)	

Muchas **amenazas potenciales** provienen de algún **punto débil** como

- fabricación.
- mantenimiento.
- diseño.
- capacitación del usuario.
- procedimientos de operación.

Si se elimina ese punto débil significa que la amenaza puede reducirse.

Hacking: acceso o intento no autorizado a ciertas áreas en un sistema, es un riesgo frente a agresores externos con mentalidad delictiva. Las actividades de los hackers van desde robo de datos, modificación de resultados, manipulación de un virus.

La **vulnerabilidad depende de los siguientes factores**:

- El personal de la organización: la protección del acceso puede ser quebrantada en cualquier elemento de la red.
- El tamaño de la red: mientras más amplia sea, mayor será el potencial de riesgo.
- La calidad de la transmisión de datos: mientras más alto sea el valor de los datos, mayor será el riesgo de amenazas, ya que el valor obtenido por el hacker por el abuso deliberado justificara su inversión de tiempo y dinero.

Virus: Son creados como abuso deliberado, se propagan accidentalmente por desconocimiento del peligro. Son frecuentes en instituciones educativas o en organizaciones cuando el personal descarga software pirata (además de los problemas legales). Los virus generan altos costos de prevención.

2 Análisis del riesgo: cuantificar la probabilidad y la frecuencia esperada de ocurrencia de cada riesgo identificado y también evaluar la posible gravedad de las consecuencias.

Se debe analizar el impacto, evaluar la **pérdida esperada producida por una amenaza particular.**

Pérdida esperada= pérdida potencial x frecuencia de pérdida.

El análisis de impacto potencial requiere dos etapas:

- 1 Evaluar costos empresariales que surgen de una brecha en la seguridad.
- 2 Estimar la frecuencia de ocurrencia de cualquier falla de seguridad a través de la probabilidad de falla de seguridad y probabilidad falla de seguridad prospere.

El producto de costo y frecuencia da como resultado la pérdida anual esperada para cada amenaza: (*Costo de las consecuencias*)×*Frecuencia de los cálculos*) = *Exposición anual de pérdidas.*

El análisis del riesgo establece un lado del *punto de equilibrio óptimo entre el costo de pérdidas y el costo de medidas de seguridad.* El manejo del riesgo identifica contra medidas posibles y luego elige el conjunto adecuado para ese trueque óptimo.

Un análisis de riesgo efectivo requiere una apreciación de la verdadera magnitud de las pérdidas resultantes de cada amenaza, lo cual es difícil de determinar. El management efectivo del riesgo también requiere una valoración realista de la posibilidad de que la amenaza se convierta en realidad.

Perdida: el análisis de riesgo de los SI debe considerar el método de cuantificación de pérdidas resultantes por una falla de seguridad en los elementos de un SI.

Elementos(Los activos vulnerables a pérdidas debido a una amenaza pueden ser)

- Hardware: pérdida relativamente fácil de evaluar y estos elementos están a menudo asegurados.
- Datos e información: es la pérdida más seria y la más difícil de cuantificar.
- Software: la principal complicación cuando se evalúa la pérdida de software es que el valor intrínseco o costo de reemplazo, del software no tiene relación con el costo original de desarrollo. Para sumar complicaciones, la pérdida de software genera una pérdida de la capacidad de procesamiento y, entonces, el factor debe incluirse en la cuantificación de pérdida del software.
- Capacidad de procesamiento: la duración de la interrupción es la variable clave al determinar el valor de la pérdida.
- Personal: esta pérdida puede ser significativa ya sea por su conocimiento teórico o por su competencia práctica.
- Fondos.

Todas las pérdidas que resultan de una falla en la seguridad se relacionan con los atributos de valor agregado de la información y se las puede dividir en tres **categorías**:

1. Pérdida de disponibilidad: la pérdida de la seguridad destruye, total o parcialmente, la habilidad de la empresa para acceder a datos e información.

2. Falla en la integridad/precisión: la pérdida de seguridad destruye la capacidad de una empresa para confiar en sus datos, o peor, de contar con datos de precisión incierta.

3. Pérdida de confidencialidad/seguridad: la pérdida de seguridad destruye la posesión exclusiva de datos, lo que provoca que la organización pierda poder y confianza. Una vez más, el peor caso es el de la incertidumbre.

Para evaluar la magnitud de la pérdida resultante de una falla en la seguridad es **considerar las consecuencias primarias**, es decir, aquellas cosas que se desprenden directamente, y por lo general en forma inmediata, de un problema en la seguridad.

- Interrupción de procesamiento a corto o largo plazo.
- Corrupción de los registros de datos.
- Destrucción de los medios de almacenamiento.
- Uso de software no autorizado.
- Relevación de información confidencial.
- Desaparición de equipos, datos, sw, robo o piratería.
- Pérdida de los registros de contabilidad u otros.

Las pérdidas secundarias (que surgen como consecuencia de las pérdidas primarias, y no de una falla en sí misma) revisten gran importancia en los cálculos de pérdidas.

La magnitud de la pérdida total de una falla en la seguridad es la suma de las consecuencias primarias y secundarias.

En el caso de que las consecuencias primarias puedan ser minimizadas, entonces habría una doble ganancia, porque si se reducen las pérdidas primarias, entonces las secundarias también se minimizan.

Riesgo: es el potencial de que una amenaza determinada explote las vulnerabilidades de un activo o de un grupo de activos, ocasionando su pérdida o daño (ISACA). El concepto de riesgo está relacionado con el de materialidad, que se refieren 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. Consiste en analizar el impacto potencial, para determinar la pérdida esperada producida por una amenaza particular. Donde $\text{Frecuencia de pérdida} = \text{probabilidad agresión} \cdot \text{probabilidad de éxito}$

3 Manejo del riesgo: una vez identificado y analizado el patrón de exposición, la organización prosigue con la selección de controles y contra medidas a fin de alcanzar la proposición de seguridad óptima.

- Prevenir el riesgo: Si se puede, debe evitarse la amenaza II. III. IV.
- Asumir el riesgo: Si los costos son bajos las consecuencias de las pérdidas son menores, se podría usar esta estrategia, aunque por lo general se la adopta inadvertidamente.
- Reducir el riesgo: Es la más común por razones obvias. Sólo es efectivo si la reducción en costos es mayor que los costos que origina. Debe considerarse que todas las contra medidas suman costos a: El desarrollo, La operación, El mantenimiento, La flexibilidad.
- Transferir el riesgo: transfiere los costos resultantes de una falla en la seguridad a un tercero, que en general implica pólizas de seguros o contratos de mantenimiento.

Luego se definen en base a esos 4 las políticas, marcos y alineaciones.

4 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 de forma continua. Niveles de emergencia: desastre no desastre catástrofe.

No se tiene un solo plan de contingencia, para cada situación de desastre se plantea uno diferente.

Por ej sistemas críticos, tener una reserva paralela de sistemas críticos aparte con hw y aplicaciones críticas, la empresa hará las inversiones necesarias.

Definir la creatividad, los responsables y los roles con actividades de cada uno. Por ej en un incendio quien llama al bombero, quien agarra el matafuego, etc.

ROBSON, parte ii Tomo 5, Cap. 13.1

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

Fraude: es engaño, acción contraria a la verdad,

Delito: acción antijurídica realizada por el ser humano tipificado como culpable y sancionado con una pena.

Elementos Delito: Es una acción humana, este acto es antijurídico y pone en peligro un interés jurídico protegido, corresponde a un tipo legal definido por la ley. El acto es culpable, intencional o negligencia cuando se pone a cargo una determinada persona. La ejecución u omisión del acto puede ser sancionada con una pena.

DELITO INFORMÁTICO: toda acción culpable realizada por un ser humano que cause perjuicio a personas sin necesariamente se beneficie el autor o que por el contrario produce un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley que se realiza en el entorno informático y está sancionado con una pena.

TIPOS:

- 1 Delitos contra la intimidad:
- ,2 Contra el patrimonio:
- 3 Falsedades documentales:

Capítulo 6.5 Piattini "Auditoría informática: un enfoque práctico". PAG 136

CHAT GEPETO:

Artífices del delito informático y modalidades de operación

Los **artífices** del delito informático suelen ser individuos o grupos que poseen conocimientos avanzados en tecnología y ciberseguridad. Estos pueden ser:

1. **Hackers:** Personas con habilidades técnicas que, motivados por diversas razones (económicas, políticas, ideológicas, o simplemente por el desafío), acceden de manera no autorizada a sistemas informáticos. Acceso no autorizado a sistemas con el fin de robar o manipular información.

2. **Phishers:** Delincuentes que utilizan técnicas de ingeniería social para engañar a las personas y obtener información sensible, como contraseñas o datos bancarios. engaños a través de correos electrónicos o sitios web falsos que imitan a entidades legítimas para obtener información personal.
3. **Crackers:** Similar a los hackers, pero con intenciones maliciosas específicas, como dañar sistemas, robar información o cometer fraude.
4. **Estafadores en línea:** Personas que utilizan internet para cometer fraudes, como el robo de identidad, estafas financieras o venta de productos falsos.
5. **Grupos de cibercrimen organizado:** Organizaciones que operan de manera profesional y coordinada para llevar a cabo delitos informáticos a gran escala.
6. **Ataques DDoS (Denegación de servicio distribuida):** Saturación de un sistema o red para hacerla inoperativa.
7. **Malware:** Uso de software malicioso para robar datos, controlar sistemas o causar daños.
8. **Ransomware:** Bloqueo de acceso a sistemas o datos mediante cifrado, exigiendo un rescate para liberarlos.

PARTE II. Auditoría en el ambiente informático.

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

Auditoría: actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y o cumple las condiciones que le han sido prescritas. Es una función que se acomete a posteriori en relación a actividades ya realizadas, sobre las que hay que emitir una opinión.

Elementos fundamentales:

- 1 Contenido: una opinión.
- 2 Condición: profesional.
- 3 Justificación sustentada en determinados procedimientos
- 4 Objeto: una determinada información obtenida en un cierto soporte
- 5 Finalidad: determinar si presenta adecuada la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

Clases de auditorías:

- 1 Financiera
- 2 Informática
- 3 Gestión
- 4 Cumplimiento

Auditoría Informática: El objeto es el sistema de aplicación, recursos informáticos, planes de contingencia, etc. La finalidad es la operatividad eficiente y según las normas establecidas.

Capítulo 1.3 Piattini “Auditoría informática: un enfoque práctico”.

La **Auditoría Informática** es el proceso de:

- recoger,
- agrupar
- y evaluar evidencias

para determinar si un sistema informatizado:

- salvaguarda los activos (Objetivo de protección),
- mantiene la integridad de los datos (Objetivo de protección),
- lleva a cabo eficazmente los fines de la organización (Objetivo de gestión)
- y utiliza eficientemente los recursos (Objetivo de gestión).

AUDITOR INFORMÁTICO:

El **auditor** evalúa y comprueba en determinados momentos los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, se deberá emplear software de auditoría y otras técnicas asistidas por computador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Las funciones del auditor son:

- 1 Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes.
- 2 Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- 3 Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

Capítulo 2..2.2 Piattini “Auditoría informática: un enfoque práctico”.

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

Extra introducción de donde sale el control interno :

El concepto de control interno surge inicialmente en el ámbito de la auditoría financiera. Sin embargo, debido a diversos problemas en numerosas organizaciones, se hizo evidente la falta de conciencia sobre la necesidad de implementar controles efectivos para evitar la aparición y el crecimiento de problemas.

Muchas organizaciones han emprendido iniciativas como:

- la reestructuración de procesos empresariales (BPR - Business Process Re-engineering),
- la gestión de la calidad total (TQM - Total Quality Management),
- el redimensionamiento organizacional,
- la contratación externa (outsourcing)
- y la descentralización.

Estas acciones son impulsadas por fuerzas externas como la creciente necesidad de acceder a **mercados globales, la consolidación industrial, la intensificación de la competencia y el avance de nuevas tecnologías.**

Ante la rapidez de estos cambios, los directivos han tomado conciencia de la importancia de reevaluar y reestructurar sus sistemas de **control interno para evitar fallos significativos**. Es crucial que actúen de manera proactiva, implementando medidas audaces no solo para su propia tranquilidad, sino también para garantizar a los consejos de administración, accionistas, comités y al público en general que los controles internos de la empresa están adecuadamente diseñados para enfrentar los retos futuros y asegurar la integridad en el presente.

Capítulo 2.1 Piattini “Auditoría informática: un enfoque práctico”.

CONTROL INTERNO INFORMATICO:

Control Interno Informático **controla diariamente** que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y no normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales.

La **misión es** asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Control Interno Informático suele ser un **órgano staff de la Dirección del Departamento de Informática** y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Objetivos Control Interno:

- 1 Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- 2 Asesorar sobre el conocimiento de las normas.
- 3 Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al Grupo.
- 4 Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informática, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos ni se les ubiquen exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

Realizar en:


los diferentes sistemas (centrales, departamentales, redes locales. PCs. etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:

- El cumplimiento de procedimiento, normas y controles dictados. Merece resaltar la vigilancia sobre el control de cambios y versiones del software.

- Controles sobre la producción diaria.
- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del sw y del servicio informática.
- Controles en las redes de comunicaciones.
- Controles sobre el sw de base.
- Controles en los sistemas microinformáticos.
- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):
 - - Usuarios, responsables y perfiles de uso de archivos y bases de datos.
 - - Normas de seguridad.
 - - Control de información clasificada.
 - - Control dual de la seguridad informática.
- Licencias y relaciones contractuales con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

Capítulo 2.2.1 Piattini "Auditoría informática: un enfoque práctico".

CONTROL INTERNO INFORMATICO VS AUDITORIA INFORMATICA:

	Control interno informatico	Auditoria informatica
Similitudes	<ul style="list-style-type: none"> ● Personal interno. ● Conocimiento especializado en Tecnología de la información. ● Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los Sistemas de Información. 	IGUAL PUE SI DICE SIMILITUDES, daaaa 
Diferencias	<ul style="list-style-type: none"> ● Análisis de controles en el día a día. ● Informa a la Dirección del Departamento de Informática. ● Solo personal interno. ● El alcance de sus funciones es únicamente sobre el Departamento de informática. 	<ul style="list-style-type: none"> ● Análisis de un momento informático determinado. ● Informar a la Dirección General de la Organización. ● Personal interno y/o externo. ● Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.

Capítulo 2.2.3 Piattini "Auditoría informática: un enfoque práctico".

CONTROL INTERNO DEFINICIÓN: "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos".

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos, simples, fiables, revisables. adecuados y rentables (habrá que analizar el coste-riesgo de su implantación).

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos.

CLASIFICACIÓN DE CONTROLES INFORMÁTICOS:

- **Controles preventivos:** para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- **Controles detectivos:** cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc..
- **Controles correctivos:** facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad.

Capítulo 2.3.1 Piattini “Auditoría informática: un enfoque práctico”.

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

Extra introducción de donde salen las pruebas:

(Objetivo general auditoría: Asegurarse de que las funciones que sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada, y satisfacen los requisitos empresariales.)

Para alcanzar el objetivo general de la auditoría, se puede dividir este objetivo en diversos objetivos específicos sobre los que se realizarán las pruebas oportunas para asegurarse de que el objetivo general se alcanza.

*El **procedimiento** o sea el trabajo a realizar es:*

- *Pruebas de cumplimiento.*
- *Pruebas sustantivas.*

TIPOS DE PRUEBAS:

1. Pruebas de cumplimiento: Hacer pruebas de cumplimiento para determinar si los controles que están instalados funcionan según lo establecido, de manera consistente y continua.

El **objetivo** de las pruebas de cumplimiento consiste en analizar el nivel de cumplimiento de las normas de control que tiene establecidas el “auditorio”. Se supone que esas normas de control establecidas son eficientes y efectivas.

Comprobar que el personal de explotación conoce y comprende :

- Los procedimientos de explotación de los que es responsable.
- Las expectativas de funcionamiento como las normas, de los proveedores y los procedimientos de la empresa y el nivel de servicio acordado de la empresa que se vaya a suministrar a los usuarios.
- Los planes de emergencia.
- Requisitos de los diarios de explotación y su revisión por parte de la dirección.
- Procedimientos por la solución de problemas.

- Las comunicaciones en los cambios de turno y las responsabilidades de cada uno de los turnos.
- La interacción de los equipos de proceso remoto con los equipos de proceso central.

2. Pruebas sustantivas: *Hacer pruebas sustantivas para aquellos objetivos de control cuyo buen funcionamiento con las pruebas de cumplimiento no nos ha satisfecho.*

El objetivo de las pruebas sustantivas consiste en realizar las pruebas necesarias sobre los datos para que proporcionen la suficiente seguridad a la dirección sobre si se ha alcanzado su objetivo empresarial.

- *Revisar las estadísticas de explotación de equipo y personal para determinar si su uso es el adecuado, comparar con otras empresas similares, con las normas de los proveedores, con normas internacionales, apropiadas y con las prácticas y ratios de las mejores industrias.*
- *Revisar una muestra representativa de los manuales del servicio de información y determinar si cumplen con las normas y los procedimientos*
- *Examinar la documentación sobre el arranque y terminación de los procesos para confirmar que los procedimientos se someten a pruebas y que se actualizan con periodicidad.*
- *Examinar el horario de proceso para asegurarse de su adecuación y suficiencia de funcionamiento con el programa.*
- *Seleccionar usuarios y determinar si es suficiente el rendimiento operativo de las operaciones de las actividades en curso y en relación con los acuerdos de nivel de servicio.*
- *Seleccionar una muestra de terminación anormales de los trabajos y determinar la solución a problemas que ocurrieron.*
- *Identificar los cursos de formación práctica de los operadores, los cambios de turnos y lo ocurrido con las vacaciones.*
- *Seleccionar una muestra de los diarios de la consola para comprobar la exactitud, tendencias en su funcionamiento, y la revisión por parte de la directiva de la resolución de problemas, evaluar el esquema de solución de problemas donde sea aplicable.*
- *Identificar a los usuarios para determinar si el nivel de servicio es satisfactorio.*
- *Identificar los procedimientos de mantenimiento preventivo que se han realizado en todos los equipos por sugerencia de los proveedores.*

Extra que pasa despues de las pruebas:

El auditor debería haber realizado las suficientes pruebas sobre los resultados de las distintas tareas y actividades de la explotación del sistema de información como para poder concluir si los objetivos de control se han alcanzado o no. Con esa información debe elaborar un informe y si procede hacer las recomendaciones oportunas.

Capítulo 11.5 Piattini “Auditoría informática: un enfoque práctico”.

12. Para cada área de Auditoría determine:

- Concepto**
- Funciones del Auditor**

Capítulo 5.3.3 Piattini “Auditoría informática: un enfoque práctico”.

- Síntesis de los elementos a auditar.**

Las demás auditorías a chequear

1. Auditoría Financiera

- Concepto: Evaluación de los estados financieros de una organización para asegurar que reflejan de manera fiel su situación económica y financiera.
- Funciones del Auditor:
 - Revisar y verificar la exactitud de los registros contables.
 - Evaluar la conformidad con las normas contables aplicables.
 - Emitir un informe sobre la razonabilidad de los estados financieros.
- Elementos a Auditar:
 - Libros contables y registros financieros.
 - Activos y pasivos.
 - Ingresos y gastos.
 - Políticas contables y su aplicación.

2. Auditoría Informática (libro)

- Concepto:

La auditoría informática es una evaluación sistemática de los sistemas de información de una organización, con el objetivo de asegurar la integridad, confidencialidad y disponibilidad de la información. Esta auditoría se centra en la revisión de los controles internos relacionados con la tecnología y la eficacia de los sistemas informáticos en el soporte de las operaciones empresariales.
- Funciones del Auditor Informático:
 - Ejecutar el trabajo de auditoría: Los auditores informáticos son responsables de llevar a cabo la auditoría, lo que incluye la obtención de información, realización de pruebas y documentación del trabajo.
 - Evaluar la seguridad de los sistemas: Deben revisar la seguridad de los sistemas informáticos y la efectividad de los controles internos.
 - Diagnosticar resultados: Evaluar y diagnosticar los resultados de las auditorías, asegurando que las recomendaciones estén alineadas con los objetivos empresariales.
 - Colaborar con otros auditores: Trabajar en conjunto con la auditoría financiera para garantizar que los datos utilizados sean precisos y confiables.
- Elementos a Auditar:
 - Seguridad de la información: Evaluar las políticas y procedimientos de seguridad implementados para proteger la información.
 - Control interno: Revisar los controles internos relacionados con la informática y su efectividad en la mitigación de riesgos.
 - Eficiencia y eficacia de los sistemas: Analizar la eficiencia de los sistemas de información y su capacidad para cumplir con los objetivos organizacionales.
 - Integridad de los datos: Asegurar que los datos utilizados en los informes financieros sean precisos y estén libres de manipulaciones.
 - Gestión de riesgos: Evaluar la gestión de riesgos operativos y la efectividad de los controles implementados para mitigarlos.

3. Auditoría Operativa

- Concepto: Evaluación de la eficiencia y efectividad de las operaciones de una organización.
- Funciones del Auditor:
 - Analizar procesos y procedimientos operativos.
 - Identificar áreas de mejora y optimización.
 - Evaluar el cumplimiento de políticas y procedimientos internos.
- Elementos a Auditar:
 - Procesos operativos y flujos de trabajo.
 - Uso de recursos (humanos, materiales, financieros).
 - Indicadores de rendimiento y resultados.

4. Auditoría de Cumplimiento

- Concepto: Evaluación de la conformidad de una organización con leyes, regulaciones y políticas internas.
- Funciones del Auditor:
 - Revisar el cumplimiento de normativas aplicables.
 - Evaluar la efectividad de los controles internos para asegurar el cumplimiento.
 - Emitir recomendaciones para mejorar el cumplimiento.
- Elementos a Auditar:
 - Políticas y procedimientos de cumplimiento.
 - Documentación y registros relacionados con el cumplimiento.
 - Capacitación y concienciación del personal sobre normativas.

5. Auditoría de Riesgos

- Concepto: Evaluación de los riesgos que enfrenta una organización y la efectividad de los controles para mitigarlos.
- Funciones del Auditor:
 - Identificar y evaluar riesgos potenciales.
 - Revisar la gestión de riesgos y los controles implementados.
 - Proporcionar recomendaciones para mejorar la gestión de riesgos.
- Elementos a Auditar:
 - Análisis de riesgos y su impacto potencial.
 - Controles internos relacionados con la gestión de riesgos.
 - Planes de contingencia y respuesta ante crisis.

13. ¿Por qué se habla de desarrollo y mantenimiento de los RRHH y no de los SI?.

ChatPDF:

La referencia al desarrollo y mantenimiento de los Recursos Humanos (RH) en lugar de los Sistemas de Información (SI) puede deberse a varios factores que se relacionan con la gestión organizacional y la importancia de ambos aspectos en el contexto de la auditoría y la administración empresarial. A continuación, se presentan algunas razones:

1. Enfoque en el Capital Humano: Los Recursos Humanos son fundamentales para el éxito de cualquier organización. La gestión del talento, la capacitación y el

desarrollo de habilidades son esenciales para asegurar que los empleados estén alineados con los objetivos estratégicos de la empresa. Esto puede ser un enfoque prioritario en la auditoría, ya que el rendimiento de los empleados impacta directamente en la eficacia de los Sistemas de Información.

2. Interacción entre RH y SI: Aunque los Sistemas de Información son cruciales para la operación de una organización, su efectividad depende en gran medida de cómo los Recursos Humanos los utilizan. La capacitación y el desarrollo de los empleados en el uso de estos sistemas son vitales para maximizar su potencial. Por lo tanto, se puede argumentar que el desarrollo de los RH es un componente clave para el mantenimiento y la mejora de los SI.

3. Gestión del Cambio: En un entorno empresarial en constante evolución, la gestión del cambio es crítica. Los auditores pueden enfocarse en cómo los Recursos Humanos manejan la transición hacia nuevas tecnologías y sistemas, asegurando que los empleados estén preparados y capacitados para adaptarse a estos cambios. Esto puede ser más relevante en ciertos contextos donde la resistencia al cambio puede afectar la implementación de nuevos Sistemas de Información.

4. Normativas y Cumplimiento: En algunos casos, las auditorías pueden centrarse más en el cumplimiento de normativas relacionadas con la gestión de personal y la ética laboral, que son aspectos críticos en la gestión de Recursos Humanos. Esto puede llevar a una menor atención a los Sistemas de Información, a menos que haya un vínculo directo con la gestión de personal.

5. Perspectiva Estratégica: La auditoría puede adoptar una perspectiva más amplia que incluya la alineación de los Recursos Humanos con la estrategia organizacional. Esto puede llevar a un enfoque en el desarrollo de los RH como un medio para mejorar la efectividad general de la organización, incluyendo sus Sistemas de Información.

En resumen, aunque los Sistemas de Información son esenciales para la operación de una organización, el desarrollo y mantenimiento de los Recursos Humanos son igualmente importantes, ya que el éxito de los SI depende en gran medida de cómo los empleados interactúan con ellos. La auditoría puede reflejar esta interdependencia al enfocarse en el desarrollo de los RH como un componente crítico para el éxito organizacional.

Bibliografía de Referencia:

Bibliografía obligatoria:

- - PIATTINI, Mario y DEL PESO, Emilio. “Auditoría informática: un enfoque práctico”. Editorial Alfaomega- RA-MA. 2ª Edición ampliada y revisada. Noviembre 2006.
- - LARDENT, Alberto R.. “Sistemas de Información para la Gestión Empresaria-Procedimientos, Seguridad y Auditoría”. Editorial Prentice

Hall Pearson Educación. 2001. Brasil.- ISACA. "Manual de Información Técnica para CISA". 2001

no obligatoria creo

- - ROBSON, Wendy. "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. 1999. Argentina.
- - ECHENIQUE GARCÍA, José Antonio. "Auditoría en Informática". Editorial McGraw-Hill. 2ª edición. 2003. México.- Anexos complementarios y conceptos dictados por la cátedra.