AUDITORÍA DE SOFTWARE

Ing. Kerly Hernández

Julio, 2022

ÍNDICE GENERAL

INTRODUCCIÓN

Hablar de avances tecnológicos hoy día es algo indiscutible y muy certero, pues desglosar el ritmo acelerado que ha tenido el sector tecnológico y en la manera en la que ha incursionado y/o afectado en nuestras vidas y en todos los ámbitos es prácticamente no decir nada. Actualmente podemos decir que desde hace un siglo se pueden describir los grandes cambios que se han dado con el pasar del tiempo de este último, pues se han visto muchos más grandes avances que en anteriores aspectos de la humanidad y absolutamente todo parece asomar que dichos cambios serán dados más rápido a medida del tiempo aunque menos duraderos. Es por ello que vemos presente los cambios en los ámbitos sociales, económicos, políticos, comercial y sin más el tecnológico, llevar a las empresas y/o organizaciones a una dirección, a un horizonte distinto donde el auge es compaginar la globalización tecnológica dentro de las necesidades de cada cual en adaptarse a estos cambios como medio para obtener grandes ventajas competitivas.

A esto se añade el acceso y la manipulación de información, que como bien se sabe, actualmente se encuentra de fácil acceso desde cualquier sitio por medio de cualquier dispositivo, y es que, a diferencia de años anteriores esto se daba de forma limitada. De aquí se desprende un sin fin de desventajas a pesar de las grandes ventajas, pues la información que tratamos en nuestros procesos productivos es el activo más importante de nuestros despachos y el de nuestros clientes. Y, como tal, debe protegerse adecuadamente. Esto es lo que busca mantener presente todo encargado del área desde lo que conocemos como seguridad de la información cómo los auditores informáticos dentro de sus procesos en cuanto a controles internos dentro de cada organización. Que a pesar de que sus objetivos difieren entre unas y otras buscan un mismo fin, garantizar la disponibilidad, integridad y confidencialidad de la información de la empresa y de la que es custodio, tanto la que se encuentra en soporte digital, como la que se gestiona en papel cómo veremos a continuación.

PLANEACIÓN

Antes de dar comienzo a las auditorías informáticas y controles internos se refiere, es importante mencionar que las primeras auditorías eran muy limitadas y restringidas en cuanto a controles internos, ya que se dió a conocer con la información financiera por lo que les interesaba grandemente y de cierto punto como prioridad el manejo de la información para con su personal financiero a pesar de que contaban con herramientas de gestión que facilitarán el objetivo de prevenir los riesgos efectivos y potenciales que se enfrentan día a día las organizaciones, no era llevado correctamente y como consecuencia de una serie de eventos ajenos a los fines y necesidades de cada cual, tales como la inexistencia de concientización de las necesidades de los controles se dieron cuenta que la buena planeación de controles internos auditados era y es la solución en pro de mejoras de cada departamento u organización.

Para aquel entonces estos procesos tomaron mayor atención por parte de las entidades encargadas de dirigirlas como por cada empresa reestructurando sus procesos internos. Así pues, las auditorías crecieron y cambiaron considerablemente en los últimos años de la mano con las tecnologías nacientes, ejecutando nuevos métodos informáticos en cuanto a la manera de procesar la información para los superiores, supliendo de esta manera las necesidades de obtener y mantener conocimientos actualizados. Cabe acotar que, hoy día en relación planeación, metodologías y planes de auditoría las hay de distintos tipos, cada uno enfocado en puntos específicos dependiendo del tipo de organización y su función a llevar a cabo. Es por ello que cada planeación requiere una planificación adecuada para definir claramente los objetivos y el alcance del trabajo a realizar, así como también las técnicas y herramientas necesarias como también las horas hombre para llevar a cabo dicha auditoría en mención.

Objetivos.

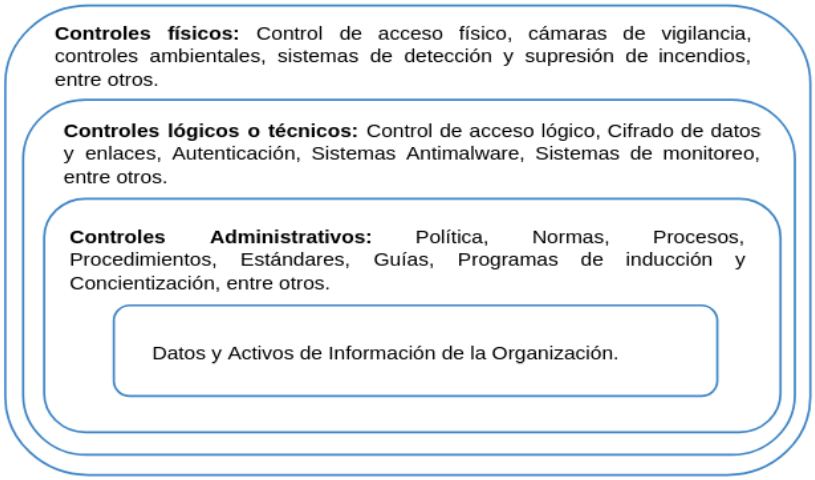
Sobre la base de las consideraciones anteriores mantenemos el hecho de que el objetivo difiere en cuánto al tipo de organización a auditar, sin embargo todas y cada una de ellas siguen cumplir los procesos de recopilar, agrupar y evaluar desde sistemas automatizados como manuales, para determinar si dicho tipo de sistema llevado actualmente es el más seguro, certero, y de herramientas efectivas para la empresa. Todo auditor tiene la responsabilidad de revisar e informar a la gerencia de las empresas relacionado al diseño y funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada, manteniendo con ello la protección de activos e integridad de datos de manera eficaz y eficiente.

Antes de seguir adelante conviene saber que, es importante dentro de toda organización mantener ciertos niveles tanto de protección como de gestión y soporte, todo ello viene de la teoría de defensa en profundidad del área militar desempeñada de años anteriores ellos resaltan el hecho de usar varias líneas de defensa de forma consecutiva con cierto grado incremental en cada una de ellas.

La idea de usar esta forma de protección y/o defensa es servir de señuelo para “debilitar” al enemigo con el fin de mejorar las estrategías y centrar sus esfuerzos en la reorganización y acción estratégica. En el área de informática, se toma esta teoría como base a aplicar dentro de los sistemas informáticos.

Figura 1.

Secuencia de organización y contención de controles.



Nota: Estos conceptos son muy importantes, no solo desde la perspectiva del responsable del auditor interno de toda empresa o en su defecto del área de seguridad de la información de la organización, el cual es el responsable de garantizar que todos los controles funcionen correctamente.

Metodología.

Como bien se ha dicho anteriormente, las metodologías dependen de cada auditor, pero esto lo conocerán mejor más adelante. A pesar de que actualmente existen muchos tipos de metodologías de auditoría informática, podemos decir, en resumidas cuentas que, las únicas que encajan perfectamente son las auditorías de controles generales usadas generalmente por auditores profesionales como también las metodologías de los auditores internos.

El enfoque que buscan estas metodologías es probar la fiabilidad de los datos del computador, generados por los usos y procesos de las herramientas implementadas internamente en cada empresa u organización, la obtención de los datos que sirven para valer la fiabilidad son generados por los cuestionarios y pruebas de vulnerabilidades que se realizan tanto a los sistemas en funcionamiento actual como al personal encargado.

Es importante recalcar que, para aplicar las metodologías es necesario que el auditor cuente con mucha experiencia con el fin de que saber actuar al momento de cómo utilizarlas y de qué manera hacerlo ante imprevistos, se hace énfasis en este aspecto debido a que actualmente se están desprestigiando el uso de estas metodologías por el simple hecho que, las han llevado a práctica profesionales sin ningún tipo de experiencia buscando asumir la función auditora de forma fácil que le permita realizar su trabajo rápidamente. Es por ello que se espera y requiere que el auditor informático tenga una larga experiencia y formación tanto en el campo de auditorías como el de informática, adquirida por medio del estudio y la práctica de la misma.

Para poder entender mejor estas metodologías es importante identificar estos conceptos dentro de cada sistema informático tales como:

- **Amenazas:** Puede ser identificado como una persona o cosa vista como posible fuente de peligro o catástrofe.
- **Vulnerabilidad:** Es la situación creada debido a la falta de un o varios controles que amenazan con afectar al entorno informático.
- **Riesgo:** Posibilidad que exista el momento en que una amenaza se convierta en vulnerabilidad.
- **Impacto:** Evaluación del efecto de riesgo.

Cabe mencionar que tanto el análisis de riesgos como las auditorías informáticas tienen enfoques distintos ya que la primera busca evaluar los riesgos y recomendar acciones mientras que la segunda identifica el nivel de vulnerabilidad por la falta de controles. Es por ello que las metodologías deben ser diseñadas y desarrolladas por el propio auditor, de ello vale su experiencia.

Ejemplo de metodología de auditoría de una aplicación.

Según Piattini G, Mario y del Peso, Emilio comparten el ejemplo claro de una auditoría de aplicación de la siguiente forma:

Objetivo

Determinar que los sistemas producen informaciones exactas y completas en el momento oportuno. Esta área es tal vez la más importante en el trabajo de auditoría informativas.

Programa de revisión.

1. *Identificar el área a revisar (por ejemplo, a partir del calendario de revisiones notificar al responsable del área y prepararse utilizando papeles de trabajo de auditorías anteriores.*
2. *Identificar las informaciones necesarias para la auditoría y para las pruebas.*
3. *Obtener informaciones generales sobre el sistema. En esta etapa, se definen los objetivos y el alcance de la auditoría, y se identifican los usuarios específicos que estarían afectados por la auditoría (plan de cuestionarios y/o entrevistas).*
4. *Obtener un conocimiento detallado de la aplicación/sistema. Se pasan las entrevistas y/o cuestionarios con los usuarios y el personal implicado en el sistema a revisar, se examina la documentación de usuarios, de desarrollo y de operación, y se identifican los aspectos más importantes del sistema (entrada, tratamiento, o lida de datos, etc.), la periodicidad d e procesos, los programas fuentes, características y estructuras d e archivos de datos, así como pistas de auditoría.*

5. *Identificar los puntos de control críticos en el sistema. Utilizando organigramas de flujos de informaciones, identificar los puntos de control críticos en entrevistas con los usuarios con el apoyo de la documentación sobre el sistema. El auditor tiene que identificar los peligros y los riesgos que podrían surgir en cada punto. Los puntos d e control críticos son aquellos donde el riesgo es más grave, es decir, donde la necesidad de un control es más importante. A menudo, son necesarios controles en los puntos de interfaz entre procedimientos manuales y automáticos.*
6. *Diseño y elaboración de los procedimientos de la auditoría.*
7. *Ejecución de pruebas en los puntos críticos de control. Se podría incluir la determinación de las necesidades de herramientas informáticas de ayuda a la auditoría no informática. Se revisa el cumplimiento de los procedimientos para verificar el cumplimiento de los estándares y los procedimientos formales, así como los procesos descritos por los organigramas de flujos. Así se verifican los controles internos del cumplimiento de: a) planes. políticas, procedimientos, estándares, b) del trabajo de la organización. c) requerimientos legales, d) principios generales de contabilidad y e) prácticas generales de informática.*

Se hacen revisiones sustantivas y pruebas, como resultado de la revisión del cumplimiento de procedimientos. Si las conclusiones d e la revisión de cumplimentación fuesen generalmente positivas, se podrían limitar las revisiones sustantivas.

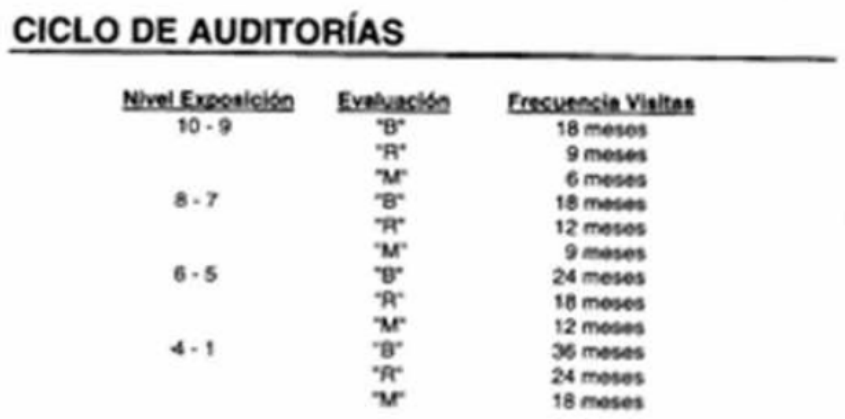
Plan de Auditoría.

El esquema metodológico en el que se basa en el plan del propio auditor en el cual se desarrolla todo sobre la función a aplicar y el trabajo que realiza en cada entidad, es importante recalcar que si hay más de un auditor entonces todos los planes deben llevar una secuencia dónde al menos debe constar de las siguientes partes:

- Funciones: Tener clara la figura del organigrama de la empresa, ya que debe de existir una división de funciones y control interno informático el cual debe ser auditado también. Se deben describir las funciones de manera precisa y organización interna del departamento con sus respectivos recursos.
- Procedimientos: Para cada una de las distintas tareas de las auditorías, desde el procedimiento de apertura, entrega y discusión de vulnerabilidades, entrega del informe preliminar, cierre de auditoría y la redacción del informe final, entre otros.
- Tipos de auditorías: Que se van a realizar desde metodologías y cuestionarios.
- Sistema de evaluación: Independientemente de que exista un plan de acciones en el informe final, se debe evaluar en distintos aspectos como el nivel de gestión de recursos humanos, cumplimiento de normas, así como realizar una evaluación global como resumen para toda la auditoría. Esto nos ayudará para definir la próxima fecha para repetir la misma auditoría según los datos arrojados en la actual.
- Nivel de Exposición: Esto se refiere subjetivamente a permitir como base la evaluación final de la última auditoría realizada y definir la fecha de repetición de la misma. En este caso el valor del nivel de exposición significa la suma de factores como impacto, peso del área, situación de control en el área.

Figura 2.

Ciclo de auditorías.



CICLO DE AUDITORÍAS

Nivel Exposición	Evaluación	Frecuencia Visitas
10 - 9	"B"	18 meses
	"R"	9 meses
	"M"	6 meses
8 - 7	"B"	18 meses
	"R"	12 meses
	"M"	9 meses
6 - 5	"B"	24 meses
	"R"	18 meses
	"M"	12 meses
4 - 1	"B"	36 meses
	"R"	24 meses
	"M"	18 meses

Nota: En la figura 2 se observa un ciclo de auditoría por nivel de exposición esta evaluación suele hacerse en tres niveles que son "Bien", "Regular" o "Mal", significando la visión de grado, d e gravedad. lista evaluación final nos servirá para definir la fecha de repetición de la misma auditoría en el futuro según el nivel de exposición que se le haya dado a este tipo de auditoría en cuestión.

- Lista de Distribución de informes:

  Seguimiento de las acciones correctoras:

  - ➔ Plan quincenal: Es indispensable que dentro de todas las áreas a revisar deben corresponder al cuestionario de metodología y deben distribuirse en un plazo de cuatro o cinco años.
  - ➔ Plan de trabajo anual: El tiempo debe estimarse razonablemente por medio de un calendario, y una vez completado, nos proporcionará las horas de trabajo planificadas y los resultados previstos necesarios para utilizar los recursos.

CONTROL INTERNO (Cuestionarios de Control)

Dentro de este contexto hay que tener claro que tanto el auditor de TI interno ó externo debe revisar diferentes controles, tales como definir y cumplir internamente en cada función de TI, todo acorde a la normativa interna y externa, según nivel de riesgo y según objetivos, definidos por el consejo interno empresarial y el consejo de TI de cada ente u organización. Notificar a la escala de gerencia sobre los hechos observados y cuando existan deficiencias aplicar las debidas medidas de control y recomendar reglas para minimizar los posibles riesgos que pudieran existir a futuro, a pesar de que nunca se podrá eludir totalmente, lo que se busca es maximizar de alguna u otra forma las amenazas y/o vulnerabilidades. Es por ello que en toda organización debe existir un sistema de control informático de responsabilidad de la gerencia para mantener las políticas dentro de todo entorno informático.

Continuando con la teoría, según Piattini G, Mario y del Peso, Emilio afirman que el control interno es cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento d e un sistema para conseguir sus objetivo.(p 30). Los mismos controles utilizados actualmente en el entorno informático continúan desarrollándose al mismo tiempo que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Los objetivos que buscan los controles internos se pueden clasificar de la siguiente manera:

- Controles preventivos: Software de seguridad que limita los accesos no autorizados al sistema.
- Controles detectivos: Registro diarios de intentos fallidos de acceso al sistema no autorizados para detectar errores u omisiones.
- Controles correctivos: La recuperación de archivos dañados.

A continuación se detallan los siguientes controles internos informáticos que ayudan a evaluar el cumplimiento y validez con el fin de mantener y asegurar la integridad, disponibilidad y eficacia de los sistemas, todo ello se consigue por medio de cuestionarios de control interno.

- **Controles de preparación de datos.**
  - Revisar procedimientos escritos para iniciar, autorizar, recoger, preparar y aprobar los datos de entrada mediante un manual de usuario para poder verificar que los usuarios entienden y siguen los procedimientos.
  - Revisar que se dé la inducción para utilizar la terminal necesaria a los usuarios.
  - Revisar los documentos fuentes para determinar si son numerados
  - Determinar los usuarios totales de control de los datos de entrada por terminales y comprobar que los de entrada sean igual que los de salida.
  - Determinar que todos los datos de entrada dentro de un sistema siguen la secuencia de validación y registro.
  - Comprobar la existencia y seguimientos de calendarios de entrada de datos y distribución de informes listados.
  - Revisar los procedimientos para solventar fallos.

- Comprobar la existencia de los períodos de retención de documentos fuentes y soportes magnéticos.

- **Controles de entrada a la aplicación.**
  - Establecer procedimientos de entrada y control de datos con fechas límites y criterios de validación de los mismos tales como códigos, mensajes, detección y corrección de errores, y reentrada de datos.
  - Revisar logs de acceso por medio de E.R para obtener de forma eficaz de accesos no autorizados de posibles accesos y entradas de telecomunicaciones.
  - Revisar los programas para poder saber si tienen internamente procesos de validación
  - Comparar, validar, apuntar y calcular elementos de datos críticos
  - Comprobar los usuarios si revisan gradualmente las tablas internas del sistema
  - Revisar funciones para validar implicaciones negativas.
  - Determinar la existencia de auditorías adecuadas dentro del diccionario de datos.
  - Revisar procedimientos de corrección de errores.
  - Identificar con los usuarios cualquier código de errores críticos que deberían aparecer en momentos específicos.

- **Controles de salida a la aplicación.**
  - Determinar si los usuarios comparan totales de control de datos de entrada contra los totales de control de datos de salida.
  - Determinar si el control de datos evalúa los informes listados para detectar errores evidentes.
  - Verificar que se hace una identificación adecuada de los informes
  - Comparar listas de distribución de informes.

- Verificar que los informes que pasan de aplicabilidad se destruyan y que simplemente no pasen a la papelera.
- Revisar la justificación de informes.
- Verificar la existencia de períodos de retención de informes.

- **Seguridad en aspectos físicos y en aspectos técnicos de la aplicación.**

Esta fase es la complementaria al proceso del auditor ya que incluye desde los controles fundamentales implementados en el software, integridad y confidencialidad del sistema dentro de cada uno de los aspectos físicos y técnicos, tales como:

- Definir un grupo de seguridad de la información priorizando sus funciones tales como: la administración y gestión del software de seguridad, revisiones constantes, informes de violaciones para identificar y resolver incidencias.
- Controles físicos para asegurar el acceso a las instalaciones internas de las compañías, restringiendo a las personas no autorizadas.
- Acceso controlado, todas aquellas personas deberán ir acompañadas por un miembro de la plantilla cuando se requiera movilizarse por las instalaciones restringidas.
- Acceso restringido a las máquinas por medio de identificadores personales de cada usuario de forma intransferible.
- Crear y aplicar normas que vigilen y regulen el acceso a todos los recursos informáticos.
- Instalación de medidas que ayuden a facilitar la aplicación de los mismos
- Formar y concientizar al personal responsables de los sistemas como todos los demás dentro la empresa
- Normas que regulen el control para el responsable de todo el departamento.
- Crear y mantener planes de contingencias.

- **Controles generales organizativos.**

  Engloban los siguientes:

  - Planificación: Consta de cuatro aspectos fundamentales:
    - Plan estratégicos de Información: Se hace uso de tecnologías para definir los procesos corporativos, este plan es realizado por los órganos de la alta gerencia.
    - Plan Informático: Determina los caminos precisos para suplir las necesidades de la organización por medio de proyectos informáticos
    - Plan General de Seguridad: Maneras que garanticen la confidencialidad, integridad y disponibilidad de la información.
    - Plan de emergencia ante desastres que garanticen la disponibilidad de todos los sistemas informáticos ante eventos.
  - Estándares: Regulen la adquisición de recursos, diseños, desarrollo, modificación y explotación de sistemas.
  - Procedimientos: para describir de forma responsable las relaciones entre el departamento de TI y los demás departamentos.
  - Organización: Del departamento de TI dentro del marco superior de la estructura organizativa para asegurar la independencia con los demás departamentos.
  - Descripción: Determinar las funciones y responsabilidades del departamento.
  - Políticas: Aplicar políticas al personal desde la selección, inducción, vacaciones, evaluación y promoción.
  - Asegurar: Que los departamentos superiores revisen todos los informes de control y resuelvan las incidencias.
  - Asegurar: La existencia de políticas de organización y clasificación del personal autorizado y qué información maneja cada cual.

- Designación: Designar de acuerdo a la experiencia y tamaño del departamento a la figura principal responsable del control interno informático.

- **Talento Humano de la aplicación.**

La integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa, Este aspecto es el más importante, ya que sin él,no sería posible llevar todo a cabo. Se pueden establecer controles sin alguno de los demás aspectos, pero nunca sin personas, ya que son estas las que realizan los procedimientos y desarrollan los Planes (Plan de Seguridad. Plan de contingencias, auditorías, etc.).

CONCLUSIÓN

Cómo se ha podido observar a lo largo del desglose de este documento, se pudo demostrar que desde la planeación en cuanto a objetivos de la realización de auditorías, metodologías, Planes del mismo, dentro del marco de los controles internos de aplicación han nacido para quedarse, a pesar de que en principios las auditorías se enfocaban hacia el campo financiero, sin embargo con el avance tecnológico ha ayudado a evolucionar estos mecanismos desde lo tradicional aportando grandes beneficios para todos aquellos que lo utilicen dentro la auditoría informática, en cualquiera de las escalas, en proyectos de micro a macro ya que su característica más resaltante como lo es el poder de la “adaptabilidad” a cualquier tipo de organización y en la manera en la que se pueden trabajar en conjunto, dos metodologías con uno o más auditores informáticos a la vez facilita y aporta un mejor y más fluido flujo de trabajo, con el fín de evaluar y gestionar de manera eficaz y eficiente las vulnerabilidades que presenta cada ente . Como por ejemplo los controles de análisis de riesgos y las metodologías de los auditores. Claro, que a pesar de ello, todo debe constar de compromiso, entender y mantener lo que significa la confidencialidad y responsabilidad de los recursos corporativos y que, no solo con ello los datos de los usuarios finales son muy importantes a la hora de gestionar y preservar desde el Auditor en jefe y todos los concernientes como el Team IT. Manteniendo siempre la vista y actos dinámicos el enfoque de cada proceso sin perderlo, por el simple hecho de aplicar de manera muy rígida estos marcos de trabajo, con el objeto de obtener una solución no viable sino fácil y rápida de llevar a cabo por profesionales no especializados, desprestigian a los métodos llevados desde tiempos remotos. Es por ello que el Auditor especializado es de suma importancia en toda organización, ya que de él depende la seguridad de los datos tanto internos como el de los clientes finales, una buena gestión de procesos y organización de los mismos en conjunto con herramientas que aseguren la integridad de la empresa.

BIBLIOGRAFÍA

Piattini Velthuis, Mario Gerardo, del Peso Navarro, Emilio. 2001. Auditoría Informática. Un enfoque práctico. 2da ed.