METODOLOGÍA DE UNA AUDITORÍA DE SISTEMAS

Existen algunas metodologías de Auditorías de Sistemas y todas dependen de lo que se pretenda revisar o analizar, pero como estándar analizaremos las cuatro fases básicas de un proceso de revisión:

- Estudio preliminar
- Revisión y evaluación de controles y seguridades
- Examen detallado de áreas criticas
- Comunicación de resultados

Estudio preliminar.- Incluye definir el grupo de trabajo, el programa de auditoría, efectuar visitas a la unidad informática para conocer detalles de la misma, elaborar un cuestionario para la obtención de información para evaluar preliminarmente el control interno, solicitud de plan de actividades, Manuales de políticas, reglamentos, Entrevistas con los principales funcionarios del PAD.

Revisión y evaluación de controles y seguridades.- Consiste de la revisión de los diagramas de flujo de procesos, realización de pruebas de cumplimiento de las seguridades, revisión de aplicaciones de las áreas criticas, Revisión de procesos históricos (backups), Revisión de documentación y archivos, entre otras actividades.

Examen detallado de áreas criticas.-Con las fases anteriores el auditor descubre las áreas criticas y sobre ellas hace un estudio y análisis profundo en los que definirá concretamente su grupo de trabajo y la distribución de carga del mismo, establecerá los motivos, objetivos, alcance Recursos que usará, definirá la metodología de trabajo, la duración de la auditoría, Presentará el plan de trabajo y analizará detalladamente cada problema encontrado con todo lo anteriormente analizado.

Comunicación de resultados.- Se elaborará el borrador del informe a ser discutido con los ejecutivos de la empresa hasta llegar al informe definitivo, el cual se presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría.

El informe debe contener lo siguiente:

- Motivos de la Auditoría
- Objetivos
- Alcance
- Estructura Orgánico-Funcional del área Informática
- Configuración del Hardware y Software instalado
- Control Interno
- Resultados de la Auditoría

PROCEDIMIENTOS Y TECNICAS DE AUDITORIA.

Se requieren varios pasos para realizar una auditoría. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos. ***El proceso de auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia.*** Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

<u>Planificación de la auditoría</u>

Una planificación adecuada es el primer paso necesario para realizar auditorías de sistema eficaces. El auditor de sistemas debe comprender el ambiente del negocio en el que se ha de realizar la auditoría así como los riesgos del negocio y control asociado. A continuación se menciona algunas de las áreas que deben ser cubiertas durante la planificación de la auditoría:

a. **Comprensión del negocio y de su ambiente.**

Al planificar una auditoría, el auditor de sistemas debe tener una comprensión de suficiente del ambiente total que se revisa. Debe incluir una comprensión general de las diversas prácticas comerciales y funciones relacionadas con el tema de la auditoría, así como los tipos de sistemas que se utilizan. El auditor de sistemas también debe comprender el ambiente normativo en el que opera el negocio. Por ejemplo, a un banco se le exigirá requisitos de integridad de sistemas de información y de control que no están presentes en una empresa manufacturera. Los pasos que puede llevar a cabo un auditor de sistemas para obtener una comprensión del negocio son: Recorrer las instalaciones del ente. Lectura de material sobre antecedentes que incluyan publicaciones sobre esa industria, memorias e informes financieros. Entrevistas a gerentes claves para comprender los temas comerciales esenciales. Estudio de los informes sobre normas o reglamentos. Revisión de planes estratégicos a largo plazo. Revisión de informes de auditorías anteriores.

b. **Riesgo y materialidad de auditoría.**

Se puede definir los riesgos de auditoría como aquellos riesgos de que la información pueda tener errores materiales o que el auditor de sistemas no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera: Riesgo inherente: Cuando un error material no se puede evitar que suceda por que no existen controles compensatorios relacionados que se puedan establecer. Riesgo de Control: Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno. Riesgo de detección: Es el riesgo de que el auditor realice pruebas exitosas a partir de un procedimiento inadecuado. El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad los hay. La palabra "material" utilizada con cada uno de estos componentes o riesgos, se refiere a un error que debe considerarse significativo cuando se lleva a cabo una auditoría. En una auditoría de sistemas de información, la definición de riesgos materiales depende del tamaño o importancia del ente auditado así como de otros factores. El auditor de sistemas debe tener una cabal comprensión de estos riesgos de auditoría al planificar. Una auditoría tal vez no detecte cada uno de los potenciales errores en un universo. Pero, si el tamaño de la muestra es lo suficientemente grande, o se utiliza procedimientos estadísticos adecuados se llega a minimizar la probabilidad del riesgo de detección. De manera similar al evaluar los controles internos, el auditor de sistemas debe percibir que en un sistema dado se puede detectar un error mínimo, pero ese error combinado con otros, puede convertiré en un error material para todo el sistema. La materialidad en la auditoría de sistemas debe ser considerada en términos del impacto potencial total para el ente en lugar de alguna medida basado en lo monetario.

c. **Técnicas de evaluación de Riesgos**.

Al determinar que áreas funcionales o temas de auditoría que deben auditarse, el auditor de sistemas puede enfrentarse ante una gran variedad de temas candidatos a la auditoría, el auditor de sistemas debe evaluar esos riesgos y determinar cuales de esas áreas de alto riesgo debe ser auditada. Existen cuatro motivos por los que se utiliza la evaluación de riesgos, estos son: Permitir que la gerencia asigne recursos necesarios para la auditoría. Garantizar que se ha obtenido la información pertinente de todos los niveles gerenciales, y garantiza que las actividades de la función de auditoría se dirigen correctamente a las áreas de alto riesgo y constituyen un valor agregado para la gerencia. Constituir la base para la organización de la auditoría a fin de administrar eficazmente el departamento. Proveer un resumen que describa como el tema individual de auditoría se relaciona con la organización global de la empresa así como los planes del negocio.

d. **Objetivos de controles y objetivos de auditoría**.

El objetivo de un control es anular un riesgo siguiendo alguna metodología, el objetivo de auditoría es verificar la existencia de estos controles y que estén funcionando de manera eficaz, respetando

las políticas de la empresa y los objetivos de la empresa. Así pues tenemos por ejemplo como objetivos de auditoría de sistemas los siguientes: La información de los sistemas de información deberá estar resguardada de acceso incorrecto y se debe mantener actualizada. Cada una de las transacciones que ocurren en los sistemas es autorizada y es ingresada una sola vez. Los cambios a los programas deben ser debidamente aprobados y probados. Los objetivos de auditoría se consiguen mediante los procedimientos de auditoría.

e. **Procedimientos de auditoría.**

Algunos ejemplos de procedimientos de auditoría son: Revisión de la documentación de sistemas e identificación de los controles existentes. Entrevistas con los especialistas técnicos a fin de conocer las técnicas y controles aplicados. Utilización de software de manejo de base de datos para examinar el contenido de los archivos de datos. Técnicas de diagramas de flujo para documentar aplicaciones automatizadas.

Desarrollo del programa de auditoría.

Un programa de auditoría es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoría planificados. El esquema típico de un programa de auditoría incluye lo siguiente:

Tema de auditoría: Donde se identifica el área a ser auditada.

Objetivos de Auditoría: Donde se indica el propósito del trabajo de auditoría a realizar.

Alcances de auditoría: Aquí se identifica los sistemas específicos o unidades de organización que se han de incluir en la revisión en un período de tiempo determinado.

Planificación previa: Donde se identifica los recursos y destrezas que se necesitan para realizar el trabajo así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar.

Procedimientos de auditoría para:

Recopilación de datos.

Identificación de lista de personas a entrevistar.

Identificación y selección del enfoque del trabajo

Identificación y obtención de políticas, normas y directivas.

Desarrollo de herramientas y metodología para probar y verificar los controles existentes.

Procedimientos para evaluar los resultados de las pruebas y revisiones.

Procedimientos de comunicación con la gerencia.

Procedimientos de seguimiento.

El programa de auditoría se convierte también en una guía para documentar los diversos pasos de auditoría y para señalar la ubicación del material de evidencia. Generalmente tiene la siguiente estructura:

Procedimientos de Auditoría	Lugar	Papeles de Trabajo Referencia:	Hecho Por: Fecha:

Los procedimientos involucran pruebas de cumplimiento o pruebas sustantivas, las de cumplimiento se hacen para verificar que los controles funcionan de acuerdo a las políticas y procedimientos establecidos y las pruebas sustantivas verifican si los controles establecidos por las políticas o procedimientos son eficaces.

Asignación de Recursos de auditoría.

La asignación de recursos para el trabajo de auditoría debe considerar las técnicas de administración de proyectos las cuales tienen los siguientes pasos básicos: Desarrollar un plan detallado: El plan debe precisar los pasos a seguir para cada tarea y estimar de manera realista, el tiempo teniendo en cuenta el personal disponible. Contrastar la actividad actual con la actividad planificada en el proyecto: debe existir algún mecanismo que permita comparar el progreso real con lo planificado. Generalmente se utilizan las hojas de control de tiempo. Ajustar el plan y tomar las acciones correctivas: si al comparar el avance con lo proyectado se determina avances o retrasos, se debe reasignar tareas. El control se puede llevar en un diagrama de Gantt

Diagrama de Gantt.	Nro.	Fecha	Fecha	Real	Real	Sem1	Sem2	Sem3	Sem4
Auditoría 1	Pers.	Inicio	Termino	Inicio	Termino				
Actividad 1	X	dd/mm/aa	dd/mm/aa	dd/mm/aa	dd/mm/aa				
Actividad 2	Y	dd/mm/aa	dd/mm/aa	dd/mm/aa	dd/mm/aa				
Actividad 3	S	dd/mm/aa	Dd/mm/aa	dd/mm/aa	dd/mm/aa				
Actividad 4	Y	dd/mm/aa	Dd/mm/aa	dd/mm/aa	dd/mm/aa				
Actividad 5	X	dd/mm/aa	Dd/mm/aa	dd/mm/aa	dd/mm/aa				

Así mismo las hojas de control de tiempo son generalmente como sigue:

HOJA DE CONTROL DE TIEMPO – SEMANAL

SEMANA DEL __/__/__ AL __/__/__
NOMBRE : Auditor 1
REGISTRO : nnnnn

GENERAL	DETALLE	L dd	M dd	M dd	J dd	V dd	S dd	D Dd
Auditoría 1	Actividad 1							
Auditoría 1	Actividad 2							
Auditoría 1	Actividad 3							
Auditoría 2	Actividad 1							
Auditoría 2	Actividad 4							

Hecho por : Auditor 1
Revisado Por: Director de auditoría.

Los recursos deben comprender también las habilidades con las que cuenta el grupo de trabajo de auditoría y el entrenamiento y experiencia que estos tengan. Tener en cuenta la disponibilidad del personal para la realización del trabajo de auditoría, como los períodos de vacaciones que estos tengan, otros trabajos que estén realizando, etc.

Técnicas de recopilación de evidencias.

La recopilación de material de evidencia es un paso clave en el proceso de la auditoría, el auditor de sistemas debe tener conocimiento de cómo puede recopilar la evidencia examinada. Algunas formas son las siguientes:

Revisión de las estructuras organizacionales de sistemas de información.

Revisión de documentos que inician el desarrollo del sistema, especificaciones de diseño funcional, historia de cambios a programas, manuales de usuario, especificaciones de bases de datos, arquitectura de archivos de datos, listados de programas, etc.; estos no necesariamente se encontrarán en documentos, sino en medios magnéticos para lo cual el auditor deberá conocer las formas de recopilarlos mediante el uso del computador.

Entrevistas con el personal apropiado, las cuales deben tener una naturaleza de descubrimiento no de acusatoria.

Observación de operaciones y actuación de empleados, esta es una técnica importante para varios tipos de revisiones, para esto se debe documentar con el suficiente grado de detalle como para presentarlo como evidencia de auditoría.

Auto documentación, es decir el auditor puede preparar narrativas en base a su observación, flujogramas, cuestionarios de entrevistas realizados. Aplicación de técnicas de muestreo para saber cuÁndo aplicar un tipo adecuado de pruebas (de cumplimiento o sustantivas) por muestras.

Utilización de técnicas de auditoría asistida por computador CAAT, consiste en el uso de software genérico, especializado o utilitario.

Evaluación de fortalezas y debilidades de auditoría.

Luego de desarrollar el programa de auditoría y recopilar evidencia de auditoría, el siguiente paso es evaluar la información recopilada con la finalidad de desarrollar una opinión. Para esto generalmente se utiliza una matriz de control con la que se evaluará el nivel de los controles identificados, esta matriz tiene sobre el eje vertical los tipos de errores que pueden presentarse en el área y un eje horizontal los controles conocidos para detectar o corregir los errores, luego se establece un puntaje (puede ser de 1 a 10 ó 0 a 20, la idea es que cuantifique calidad) para cada correspondencia, una vez completada, la matriz muestra las áreas en que los controles no existen o son débiles, obviamente el auditor debe tener el suficiente criterio para juzgar cuando no lo hay si es necesario el control. Por ejemplo:

Riesgo de Control en	Ctrl. Integr	Ctrl. Duplic.	Ctrl. Valid	Ctrl. Limit	Ctrl. Exist	Ctrl. Tablas	Ctrl. Autoriz	Ctrl. Dig-chk
Despacho ítem de almacén	0	10	0	0	0	0	0	5
Ingreso Código de cliente	0	0	10	10	10	0	5	0
Código de ítem.	2	0	0	0	0	0	0	0
Ingreso de cantidad	0	10	0	10	0	5	10	5

En esta parte de evaluación de debilidades y fortalezas también se debe elegir o determinar la materialidad de las observaciones o hallazgos de auditoría. El auditor de sistemas debe juzgar cuales observaciones son materiales a diversos niveles de la gerencia y se debe informar de acuerdo a ello.

Informe de auditoría.

Los informes de auditoría son el producto final del trabajo del auditor de sistemas, este informe es utilizado para indicar las observaciones y recomendaciones a la gerencia, aquí también se expone la opinión sobre lo adecuado o lo inadecuado de los controles o procedimientos revisados durante la auditoría, no existe un formato específico para exponer un informe de auditoría de sistemas de información, pero generalmente tiene la siguiente estructura o contenido:

Introducción al informe, donde se expresara los objetivos de la auditoría, el período o alcance cubierto por la misma, y una expresión general sobre la naturaleza o extensión de los procedimientos de auditoría realizados.

Observaciones detalladas y recomendaciones de auditoría.

Respuestas de la gerencia a las observaciones con respecto a las acciones correctivas.

Conclusión global del auditor expresando una opinión sobre los controles y procedimientos revisados.

Seguimiento de las observaciones de auditoría.

El trabajo de auditoría es un proceso continuo, se debe entender que no serviría de nada el trabajo de auditoría si no se comprueba que las acciones correctivas tomadas por la gerencia, se están realizando, para esto se debe tener un programa de seguimiento, la oportunidad de seguimiento dependerá del carácter crítico de las observaciones de auditoría. El nivel de revisión de seguimiento del auditor de sistemas dependerá de diversos factores, en algunos casos el auditor de sistemas tal vez solo necesite inquirir sobre la situación actual, en otros casos tendrá que hacer una revisión más técnica del sistema.

PLANEACIÓN DE LA AUDITORÍA EN INFORMÁTICA

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

En el caso de la auditoría en informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

Evaluación de los sistemas y procedimientos.

Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de informática a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

INVESTIGACIÓN PRELIMINAR

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar:

A NIVEL DEL ÁREA DE INFORMÁTICA.- Objetivos a corto y largo plazo.

RECURSOS MATERIALES Y TECNICOS.- Solicitar documentos sobre los equipos, número de ellos, localización y características.

Estudios de viabilidad.

Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)

Fechas de instalación de los equipos y planes de instalación.

Contratos vigentes de compra, renta y servicio de mantenimiento.

Contratos de seguros.

Convenios que se tienen con otras instalaciones.

Configuración de los equipos y capacidades actuales y máximas.

Planes de expansión.

Ubicación general de los equipos.

Políticas de operación.

Políticas de uso de los equipos.

SISTEMAS

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

Manual de formas.

Manual de procedimientos de los sistemas.

Descripción genérica.

Diagramas de entrada, archivos, salida.

Salidas.

Fecha de instalación de los sistemas.

Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

No tiene pero es necesaria.

No se tiene y no se necesita.

Se tiene la información pero:

No se usa.

Es incompleta.

No esta actualizada.

No es la adecuada.

Se usa, está actualizada, es la adecuada y está completa.

En el caso de *No se tiene y no se necesita*, se debe evaluar la causa por la que no es necesaria. En el caso de *No se tiene pero es necesaria*, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)

Investigar las causas, no los efectos.

Atender razones, no excusas.

No confiar en la memoria, preguntar constantemente.

Criticar objetivamente y a fondo todos los informes y los datos recabados.

PERSONAL PARTICIPANTE

Una de las partes más importantes dentro de la planeación de la auditoría en informática es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la auditoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la auditoría, proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de informática, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la auditoría se deben tener personas con las siguientes características:

Técnico en informática.

Experiencia en el área de informática.

Experiencia en operación y análisis de sistemas.

Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como base de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

Una vez que se ha hecho la planeación, se puede utilizar el formato señalado en el anexo 1, el figura el organismo, las fases y subfases que comprenden la descripción de la actividad, el número de personas participantes, las fechas estimadas de inicio y terminación, el número de días hábiles y el número de días/hombre estimado. El control del avance de la auditoría lo podemos llevar mediante el anexo 2, el cual nos permite cumplir con los procedimientos de control y asegurarnos que el trabajo se está llevando a cabo de acuerdo con el programa de auditoría, con los recursos estimados y en el tiempo señalado en la planeación.

El hecho de contar con la información del avance nos permite revisar el trabajo elaborado por cualquiera de los asistentes. Como ejemplo de propuesta de auditoría en informática.

CONTROLES

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, ordenes impartidas y principios admitidos.

Clasificación general de los controles

Controles Preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones.
Sistemas de claves de acceso.

- **Controles detectivos:** Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los mas importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Ejemplo: Archivos y procesos que sirvan como pistas de auditoría.
Procedimientos de validación.

- **Controles Correctivos:** Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Principales Controles físicos y lógicos

Controles particulares tanto en la parte física como en la lógica se detallan a continuación

Autenticidad: Permiten verificar la identidad

Passwords
Firmas digitales

Exactitud: Aseguran la coherencia de los datos
Validación de campos
Validación de excesos

Totalidad**:** Evitan la omisión de registros así como garantizan la conclusión de un proceso de envío
Conteo de registros
Cifras de control

Redundancia: Evitan la duplicidad de datos
Cancelación de lotes
Verificación de secuencias

Privacidad: Aseguran la protección de los datos
Compactación
Encriptación

Existencia: Aseguran la disponibilidad de los datos
Bitácora de estados
Mantenimiento de activos

Protección de Activos: Destrucción o corrupción de información o del hardware
Extintores
Passwords

Efectividad: Aseguran el logro de los objetivos
Encuestas de satisfacción
Medición de niveles de servicio

Eficiencia: Aseguran el uso óptimo de los recursos
Programas monitores
Análisis costo-beneficio
Controles automáticos o lógicos

Periodicidad de cambio de claves de acceso

Los cambios de las claves de acceso a los programas se deben realizar periódicamente. Normalmente los usuarios se acostumbran a conservar la misma clave que le asignaron inicialmente.

El no cambiar las claves periódicamente aumenta la posibilidad de que personas no autorizadas conozcan y utilicen claves de usuarios del sistema de computación.

Por lo tanto se recomienda cambiar claves por lo menos trimestralmente.

Combinación de alfanuméricos en claves de acceso

No es conveniente que la clave este compuesta por códigos de empleados, ya que una persona no autorizada a través de pruebas simples o de deducciones puede dar con dicha clave.

Para redefinir claves es necesario considerar los tipos de claves que existen:

Individuales: Pertenecen a un solo usuario, por tanto es individual y personal. Esta clave permite al momento de efectuar las transacciones registrar a los responsables de cualquier cambio.

Confidenciales: De forma confidencial los usuarios deberán ser instruidos formalmente respecto al uso de las claves.

No significativas: Las claves no deben corresponder a números secuenciales ni a nombres o fechas.

Verificación de datos de entrada

Incluir rutinas que verifiquen la compatibilidad de los datos mas no su exactitud o precisión; tal es el caso de la validación del tipo de datos que contienen los campos o verificar si se encuentran dentro de un rango.

Conteo de registros

Consiste en crear campos de memoria para ir acumulando cada registro que se ingresa y verificar con los totales ya registrados.

Totales de Control

Se realiza mediante la creación de totales de línea, columnas, cantidad de formularios, cifras de control, etc. , y automáticamente verificar con un campo en el cual se van acumulando los registros, separando solo aquellos formularios o registros con diferencias.

Verificación de límites

Consiste en la verificación automática de tablas, códigos, limites mínimos y máximos o bajo determinadas condiciones dadas previamente.

Verificación de secuencias

En ciertos procesos los registros deben observar cierta secuencia numérica o alfabética, ascendente o descendente, esta verificación debe hacerse mediante rutinas independientes del programa en si.

Dígito auto verificador

Consiste en incluir un dígito adicional a una codificación, el mismo que es resultado de la aplicación de un algoritmo o formula, conocido como MODULOS, que detecta la corrección o no del código. Tal es el caso por ejemplo del décimo dígito de la cédula de identidad, calculado con el modulo 10 o el ultimo dígito del RUC calculado con el módulo 11.

Utilizar software de seguridad en los microcomputadores

El software de seguridad permite restringir el acceso al microcomputador, de tal modo que solo el personal autorizado pueda utilizarlo.

Adicionalmente, este software permite reforzar la segregación de funciones y la confidencialidad de la información mediante controles para que los usuarios puedan acceder solo a los programas y datos para los que están autorizados.

Programas de este tipo son: WACHDOG, LATTICE, SECRET DISK, entre otros.

Controles administrativos en un ambiente de Procesamiento de Datos

La máxima autoridad del Área de Informática de una empresa o institución debe implantar los siguientes controles que se agruparan de la siguiente forma:

1.- Controles de Preinstalación
2.- Controles de Organización y Planificación
3.- Controles de Sistemas en Desarrollo y Producción
4.- Controles de Procesamiento
5.- Controles de Operación
6.- Controles de uso de Microcomputadores

1.- Controles de Preinstalación

Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes.

Objetivos:

- Garantizar que el hardware y software se adquieran siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
- Garantizar la selección adecuada de equipos y sistemas de computación
- Asegurar la elaboración de un plan de actividades previo a la instalación

Acciones a seguir:

- Elaboración de un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio.
- Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación
- Elaborar un plan de instalación de equipo y software (fechas, actividades, responsables) el mismo que debe contar con la aprobación de los proveedores del equipo.
- Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales. Este proceso debe enmarcarse en normas y disposiciones legales.
- Efectuar las acciones necesarias para una mayor participación de proveedores.
- Asegurar respaldo de mantenimiento y asistencia técnica.

2.- Controles de organización y Planificación

Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades del área PAD, en labores tales como:

Diseñar un sistema
Elaborar los programas
Operar el sistema
Control de calidad

Se debe evitar que una misma persona tenga el control de toda una operación.

Es importante la utilización óptima de recursos en el PAD mediante la preparación de planes a ser evaluados continuamente

Acciones a seguir

- La unidad informática debe estar al mas alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.
- Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.
- Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.
- Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultado del procesamiento.
- El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.
- Las actividades del PAD deben obedecer a planificaciones a corto, mediano y largo plazo sujetos a evaluación y ajustes periódicos "Plan Maestro de Informática"
- Debe existir una participación efectiva de directivos, usuarios y personal del PAD en la planificación y evaluación del cumplimiento del plan.
- Las instrucciones deben impartirse por escrito.

3.- Controles de Sistema en Desarrollo y Producción

Se debe justificar que los sistemas han sido la mejor opción para la empresa, bajo una relación costo-beneficio que proporcionen oportuna y efectiva información, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados.

Acciones a seguir:
Los usuarios deben participar en el diseño e implantación de los sistemas pues aportan conocimiento y experiencia de su área y esta actividad facilita el proceso de cambio

- El personal de auditoría interna/control debe formar parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de control
- El desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías estándares, procedimientos y en general a normatividad escrita y aprobada.
- Cada fase concluida debe ser aprobada documentadamente por los usuarios mediante actas u otros mecanismos a fin de evitar reclamos posteriores.
- Los programas antes de pasar a Producción deben ser probados con datos que agoten todas las excepciones posibles.
- Todos los sistemas deben estar debidamente documentados y actualizados. La documentación deberá contener:
    - Informe de factibilidad
    - Diagrama de bloque
    - Diagrama de lógica del programa
    - Objetivos del programa
    - Listado original del programa y versiones que incluyan los cambios efectuados con antecedentes de pedido y aprobación de modificaciones
    - Formatos de salida
    - Resultados de pruebas realizadas
- Implantar procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.
- El sistema concluido será entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos

4.- Controles de Procesamiento

Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información, lo que conlleva al establecimiento de una serie de seguridades para:

- Asegurar que todos los datos sean procesados
- Garantizar la exactitud de los datos procesados
- Garantizar que se grabe un archivo para uso de la gerencia y con fines de auditoría
- Asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.

Acciones a seguir:

- Validación de datos de entrada previo procesamiento debe ser realizada en forma automática: clave, dígito autoverificador, totales de lotes, etc.
- Preparación de datos de entrada debe ser responsabilidad de usuarios y consecuentemente su corrección.
- Recepción de datos de entrada y distribución de información de salida debe obedecer a un horario elaborado en coordinación con el usuario, realizando un debido control de calidad.
- Adoptar acciones necesaria para correcciones de errores.
- Analizar conveniencia costo-beneficio de estandarización de formularios, fuente para agilitar la captura de datos y minimizar errores.
- Los procesos interactivos deben garantizar una adecuada interrelación entre usuario y sistema.
- Planificar el mantenimiento del hardware y software, tomando todas las seguridades para garantizar la integridad de la información y el buen servicio a usuarios.

5.- Controles de Operación

Abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento, la administración de la cintoteca y la operación de terminales y equipos de comunicación por parte de los usuarios de sistemas online.

Los controles tienen como fin:

- Prevenir o detectar errores accidentales que puedan ocurrir en el Centro de Cómputo durante un proceso
- Evitar o detectar el manejo de datos con fines fraudulentos por parte de funcionarios del PAD
- Garantizar la integridad de los recursos informáticos.
- Asegurar la utilización adecuada de equipos acorde a planes y objetivos.

Acciones a seguir:

- El acceso al centro de computo debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado
- Implantar claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado.
- Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y como responder ante esos eventos.
- Mantener un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.
- Los operadores del equipo central deben estar entrenados para recuperar o restaurar información en caso de destrucción de archivos.
- Los backups no deben ser menores de dos (padres e hijos) y deben guardarse en lugares seguros y adecuados, preferentemente en bóvedas de bancos.
- Se deben implantar calendarios de operación a fin de establecer prioridades de proceso.
- Todas las actividades del Centro de Computo deben normarse mediante manuales, instructivos, normas, reglamentos, etc.
- El proveedor de hardware y software deberá proporcionar lo siguiente:
  - Manual de operación de equipos
  - Manual de lenguaje de programación
  - Manual de utilitarios disponibles
  - Manual de Sistemas operativos
- Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, asi como extintores de incendio, conexiones eléctricas seguras, entre otras.
- Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía.
- Contratar pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación.

6.- Controles en el uso del Microcomputador

Es la tarea más difícil pues son equipos mas vulnerables, de fácil acceso, de fácil explotación pero los controles que se implanten ayudaran a garantizar la integridad y confidencialidad de la información.

Acciones a seguir:

- Adquisición de equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo
- Vencida la garantía de mantenimiento del proveedor se debe contratar mantenimiento preventivo y correctivo.

- Establecer procedimientos para obtención de backups de paquetes y de archivos de datos.
- Revisión periódica y sorpresiva del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa.
- Mantener programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos.
- Propender a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y mantener actualizadas las versiones y la capacitación sobre modificaciones incluidas.

Analizados los distintos tipos de controles que se aplican en la Auditoría de Sistemas efectuaremos a continuación el análisis de casos de situaciones hipotéticas planteadas como problemáticas en distintas empresas , con la finalidad de efectuar el análisis del caso e identificar las acciones que se deberían implementar .

PLANES DE CONTINGENCIA:

Por ejemplo, la empresa sufre un corte total de energía o explota, ¿Cómo sigo operando en otro lugar? Lo que generalmente se pide es que se hagan Backups de la información diariamente y que aparte, sea doble, para tener un Backup en la empresa y otro afuera de ésta. Una empresa puede tener unas oficinas paralelas que posean servicios básicos (luz, teléfono, agua) distintos de los de la empresa principal, es decir, si a la empresa principal le proveía teléfono Telecom, a las oficinas paralelas, Telefónica. En este caso, si se produce la inoperancia de Sistemas en la empresa principal, se utilizaría el Backup para seguir operando en las oficinas paralelas. Los Backups se pueden acumular durante dos meses, o el tiempo que estipule la empresa, y después se van reciclando.

Dentro de las áreas generales, se establecen las siguientes divisiones de Auditoría Informática: de Explotación, de Sistemas, de Comunicaciones y de Desarrollo de Proyectos.

Cada Área Especifica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno.
- Desde el apoyo que recibe de la Dirección y, en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- Desde la perspectiva de los usuarios, destinatarios reales de la informática.
- Desde el punto de vista de la seguridad que ofrece la Informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

Estas son las Áreas Especificas de la Auditoría Informática más importantes.

Áreas Específicas	**Áreas Generales**			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo				
Sistemas				
Comunicaciones				
Seguridad				

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de Controles Técnicos Generales de Operatividad y Controles Técnicos Específicos de Operatividad, previos a cualquier actividad de aquel.

Los Controles Técnicos Generales son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el Software de base con todos los subsistemas existentes, así como la compatibilidad del Hardware y del Software instalados. Estos controles son importantes en las instalaciones que cuentan con varios competidores, debido a que la profusión de entornos de trabajo muy diferenciados obliga a la contratación de diversos productos de Software básico, con el consiguiente riesgo de abonar más de una vez el mismo producto o desaprovechar parte del Software abonado. Puede ocurrir también con los productos de Software básico desarrollados por el personal de Sistemas Interno, sobre todo cuando los diversos equipos están ubicados en Centros de Proceso de Datos geográficamente alejados. Lo negativo de esta situación es que puede producir la inoperatividad del conjunto. Cada Centro de Proceso de Datos tal vez sea operativo trabajando independientemente, pero no será posible la interconexión e intercomunicación de todos los Centros de Proceso de Datos si no existen productos comunes y compatibles.

Los Controles Técnicos Específicos, de modo menos acusado, son igualmente necesarios para lograr la Operatividad de los Sistemas. Un ejemplo de lo que se puede encontrar mal son parámetros de asignación automática de espacio en disco* que dificulten o impidan su utilización posterior por una Sección distinta de la que lo generó. También, los periodos de retención de ficheros comunes a varias Aplicaciones pueden estar definidos con distintos plazos en cada una de ellas, de modo que la pérdida de información es un hecho que podrá producirse con facilidad, quedando inoperativa la explotación de alguna de las Aplicaciones mencionadas.

Una vez conseguida la Operatividad de los Sistemas, el segundo objetivo de la auditoría es la verificación de la observancia de las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa. Para ello, habrán de revisarse sucesivamente y en este orden:

Las Normas Generales de la Instalación Informática. Se realizará una revisión inicial sin estudiar a fondo las contradicciones que pudieran existir, pero registrando las áreas que carezcan de normativa, y sobre todo verificando que esta Normativa General Informática no está en contradicción con alguna Norma General no informática de la empresa.

Los Procedimientos Generales Informáticos. Se verificará su existencia, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de Explotación. Tampoco el alta de una nueva Aplicación podría producirse si no existieran los Procedimientos de Backup y Recuperación correspondientes.

Los Procedimientos Específicos Informáticos. Igualmente, se revisara su existencia en las áreas fundamentales. Así, Explotación no debería explotar una Aplicación sin haber exigido a Desarrollo la pertinente documentación. Del mismo modo, deberá comprobarse que los Procedimientos Específicos no se opongan a los Procedimientos Generales. En todos los casos anteriores, a su vez, deberá verificarse que no existe contradicción alguna con la Normativa y los Procedimientos Generales de la propia empresa, a los que la Informática debe estar sometida.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*). Mientras que las Aplicaciones de Teleproceso están permanentemente activas y la función de Explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de Explotación. En muchos Centros de Proceso de Datos, éste órgano recibe el nombre de Centro de Control de Batch. Este grupo determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

*Batch y Tiempo Real:

Las Aplicaciones que son Batch son Aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente.

Las Aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son Sistemas que tienen que responder en Tiempo Real.

Operación. Salas de Computadoras:

Se intentarán analizar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verificará la existencia de un responsable de Sala en cada turno de trabajo. Se analizará el grado de automatización de comandos, se verificara la existencia y grado de uso de los Manuales de Operación. Se analizará no solo la existencia de planes de formación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada Operador desde el último Curso recibido. Se estudiarán los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real. Se verificarán las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

Centro de Control de Red y Centro de Diagnosis (Help Desk):

El Centro de Control de Red suele ubicarse en el área de producción de Explotación. Sus funciones se refieren exclusivamente al ámbito de las Comunicaciones, estando muy relacionado con la organización de Software de Comunicaciones de Técnicas de Sistemas. Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al Sistema. El Centro de Diagnosis (Help Desk) es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de Software como de Hardware. El Centro de Diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la Informática de la empresa. Debe ser auditada desde esta

perspectiva, desde la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del Centro, es necesario analizarlo simultáneamente en el ámbito de Usuario.

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.

Control Interno de las Aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:

- Estudio de Vialidad de la Aplicación. [importante para Aplicaciones largas, complejas y caras]
- Definición Lógica de la Aplicación. [se analizará que se han observado los postulados lógicos de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto]
- Desarrollo Técnico de la Aplicación. [Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles]
- Diseño de Programas. [deberán poseer la máxima sencillez, modularidad y economía de recursos]
- Métodos de Pruebas. [Se realizarán de acuerdo a las Normas de la Instalación. Se utilizarán juegos de ensayo de datos, sin que sea permisible el uso de datos reales]
- Documentación. [cumplirá la Normativa establecida en la Instalación, tanto la de Desarrollo como la de entrega de Aplicaciones a Explotación]
- Equipo de Programación. [Deben fijarse las tareas de análisis puro, de programación y las intermedias. En Aplicaciones complejas se producirían variaciones en la composición del grupo, pero estos deberán estar previstos]

Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aquiescencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

Control de Procesos y Ejecuciones de Programas Críticos: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podríase provocar, desde errores de bulto que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc. Por ende, hay normas muy rígidas en cuanto a las Librerías de programas; aquellos programas fuente que hayan sido dados por bueno por Desarrollo, son entregados a Explotación con el fin de que éste:

1. Copie el programa fuente en la Librería de Fuentes de Explotación, a la que nadie más tiene acceso
2. Compile y monte ese programa, depositándolo en la Librería de Módulos de Explotación, a la que nadie más tiene acceso.
3. Copie los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc. en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente por el punto 1.

Como este sistema para auditar y dar el alta a una nueva Aplicación es bastante ardua y compleja, hoy (algunas empresas lo usarán, otras no) se utiliza un sistema llamado U.A.T (User Acceptance Test). Este consiste en que el futuro usuario de esta Aplicación use la Aplicación como si la estuviera usando en Producción para que detecte o se denoten por sí solos los errores de la misma. Estos defectos que se encuentran se van corrigiendo a medida que se va haciendo el U.A.T. Una vez que se consigue el U.A.T., el usuario tiene que dar el Sign Off ("Esto está bien"). Todo este testeo, auditoría lo tiene que controlar, tiene que evaluar que el testeo sea correcto, que exista un plan de testeo, que esté involucrado tanto el cliente como el desarrollador y que estos defectos se corrijan. Auditoría tiene que corroborar que el U.A.T. prueba todo y que el Sign Off del usuario sea un Sign Off por **todo**.

Es aconsejable que las Empresas cuenten con un Departamento QA (Quality Assurance – Aseguramiento de la Calidad) que tendría la función de controlar que el producto que llegue al usuario sea el correcto en cuanto a funcionamiento y prestaciones, antes del U.A.T.

Auditoría Informática de Comunicaciones y Redes

Para el informático y para el auditor informático, el entramado conceptual que constituyen las Redes Nodales, Líneas, Concentradores, Multiplexores, Redes Locales, etc. no son sino el soporte físico-lógico del Tiempo Real. El auditor tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico que presta el soporte. Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios).

El auditor de Comunicaciones deberá inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la Red de Comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. La inexistencia de datos sobre cuantas líneas existen, cómo son y donde están instaladas, supondría que se bordea la Inoperatividad Informática. Sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas. La contratación e instalación de líneas va asociada a la instalación de los Puestos de Trabajo correspondientes (Pantallas, Servidores de Redes Locales, Computadoras con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y de ser posible, dependientes de una sola organización.

Auditoría de la Seguridad informática:

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

La seguridad informática se la puede dividir como Área General y como Área Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Ejemplo:

Impacto	Amenaza				
	Error	Incendio	Sabotaje	……..	1: Improbable
Destrucción de Hardware	-	1	1		2: Probable
Borrado de Información	3	1	1		3: Certeza
					-: Despreciable

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

HERRAMIENTAS Y TÉCNICAS PARA LA AUDITORÍA INFORMÁTICA

Cuestionarios:

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando el llenado de cuestionarios preimpresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos preimpresos hubieran proporcionado.

Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Aparte de algunas cuestiones menos importantes, la entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular

Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para el llenado sistemático de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist. Salvo excepciones, las Checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de Auditoría Informática guardan sus Checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente. No debe olvidarse que la función auditora se ejerce sobre bases de autoridad, prestigio y ética.

El auditor deberá aplicar el Checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las Checklists utilizadas para cada sector, deben ser repetidas. En efecto, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes. De este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas. El auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango.
   Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo)

   Ejemplo de Checklist de rango:

   Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al Centro de Cálculo. Podrían formularse las preguntas que figuran a continuación, en donde las respuestas tiene los siguientes significados:

   1: Muy deficiente.
   2: Deficiente.
   3: Mejorable.
   4: Aceptable.
   5: Correcto.

   Se figuran posibles respuestas de los auditados. Las preguntas deben sucederse sin que parezcan encorsetadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño guión. El llenado del Checklist no debe realizarse en presencia del auditado.

-¿Existe personal específico de vigilancia externa al edificio?
-No, solamente un guarda por la noche que atiende además otra instalación adyacente.

<Puntuación: 1>

-Para la vigilancia interna del edificio, ¿Hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?
-Si, pero sube a las otras 4 plantas cuando se le necesita.

<Puntuación: 2>

-¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
-Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.

<Puntuación: 2>

-El personal de Comunicaciones, ¿Puede entrar directamente en la Sala de Computadoras?
-No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente salvo causa muy justificada, y avisando casi siempre al Jefe de Explotación.

<Puntuación: 4>

El resultado sería el promedio de las puntuaciones: (1 + 2 + 2 + 4) /4 = 2.25 Deficiente.

b. Checklist Binaria.
Es la constituida por preguntas con respuesta única y excluyente: Si o No. Aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Ejemplo de Checklist Binaria:

Se supone que se está realizando una Revisión de los métodos de pruebas de programas en el ámbito de Desarrollo de Proyectos.

-¿Existe Normativa de que el usuario final compruebe los resultados finales de los programas?

<Puntuación: 1>

-¿Conoce el personal de Desarrollo la existencia de la anterior normativa?

<Puntuación: 1>

-¿Se aplica dicha norma en todos los casos?

<Puntuación: 0>

-¿Existe una norma por la cual las pruebas han de realizarse con juegos de ensayo o copia de Bases de Datos reales?

<Puntuación: 0>

Obsérvese como en este caso están contestadas las siguientes preguntas:

-¿Se conoce la norma anterior?

<Puntuación: 0>

-¿Se aplica en todos los casos?

<Puntuación: 0>

Los Checklists de rango son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones. Permiten una mayor precisión en la evaluación que en los checklist binarios. Sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

Los Checklists Binarios siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta. Una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen Checklists estándar para todas y cada una de las instalaciones informáticas a auditar. Cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

ACTIVIDADES PROPIAMENTE DICHAS DE LA AUDITORÍA

La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Técnicas de Trabajo:
- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

Herramientas:
- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

CONFECCIÓN Y REDACCIÓN DEL INFORME FINAL

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

ESTRUCTURA DEL INFORME FINAL:

El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

Definición de objetivos y alcance de la auditoría.
Enumeración de temas considerados:
Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.
Cuerpo expositivo:
Para cada tema, se seguirá el siguiente orden a saber:

a. Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
b. Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
c. Puntos débiles y amenazas.
d. Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
e. Redacción posterior de la Carta de Introducción o Presentación.

MODELO CONCEPTUAL DE LA EXPOSICIÓN DEL INFORME FINAL

- El informe debe incluir solamente hechos importantes.
  La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

El hecho debe poder ser sometido a cambios.

Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.

No deben existir alternativas viables que superen al cambio propuesto.

La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

1 – Hecho encontrado.
- Ha de ser relevante para el auditor y pera el cliente.
- Ha de ser exacto, y además convincente.
- No deben existir hechos repetidos.

2 – Consecuencias del hecho
- Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

3 – Repercusión del hecho
- Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

4 – Conclusión del hecho

- No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

5 – Recomendación del auditor informático

- Deberá entenderse por sí sola, por simple lectura.
- Deberá estar suficientemente soportada en el propio texto.
- Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.
- La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe final:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo 4 folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no se escribirán nunca recomendaciones.

A su vez, las actividades auditoras se realizan en el orden siguiente:

1. Comienzo del proyecto de Auditoría Informática.
2. Asignación del equipo auditor.
3. Asignación del equipo interlocutor del cliente.
4. Llenado de formularios globales y parciales por parte del cliente.
5. Asignación de pesos técnicos por parte del equipo auditor.
6. Asignación de pesos políticos por parte del cliente.
7. Asignación de pesos finales a segmentos y secciones.
8. Preparación y confirmación de entrevistas.
9. Entrevistas, confrontaciones y análisis y repaso de documentación.
10. Cálculo y ponderación de sub-secciones, secciones y segmentos.
11. Identificación de áreas mejorables.
12. Elección de las áreas de actuación prioritaria.
13. Preparación de recomendaciones y borrador de informe
14. Discusión de borrador con cliente.
15. Entrega del informe.

Fase 0. Causas de realización de una Auditoría de Seguridad

Esta constituye la FASE 0 de la auditoría y el orden 0 de actividades de la misma.
El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad. Puede haber muchas causas: Reglas internas del cliente, incrementos no previstos de costes, obligaciones legales, situación de ineficiencia global notoria, etc.
De esta manera el auditor conocerá el entorno inicial. Así, el equipo auditor elaborará el Plan de Trabajo.

Fase 1. Estrategia y logística del ciclo de Seguridad

Se desarrolla en las siguientes actividades:

1. Designación del equipo auditor.
2. Asignación de interlocutores, validadores y decisores del cliente.
3. Llenado de un formulario general por parte del cliente, para la realización del estudio inicial.

Con las razones por las cuales va a ser realizada la auditoría (Fase 0), el equipo auditor diseña el proyecto de Ciclo de Seguridad con arreglo a una estrategia definida en función del volumen y complejidad del trabajo a realizar, que constituye la Fase 1 del punto anterior.

Para desarrollar la estrategia, el equipo auditor necesita recursos materiales y humanos. La adecuación de estos se realiza mediante un desarrollo logístico, en el que los mismos deben ser determinados con exactitud. La cantidad, calidad, coordinación y distribución de los mencionados recursos, determina a su vez la eficiencia y la economía del Proyecto.

Los planes del equipo auditor se desarrollan de la siguiente manera:

1. Eligiendo el responsable de la auditoria su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a especialidad, pero compacto.
2. Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas, etc.
3. Mediante un estudio inicial, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su llenado.

Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar la "tarea de campo", la operativa auditora del Ciclo de Seguridad.

Fase 2. Ponderación de los Sectores Auditados

Engloba las siguientes actividades:

1. Asignación de pesos técnicos. Se entienden por tales las ponderaciones que el equipo auditor hace de los segmentos y secciones, en función de su importancia.
2. Asignación de pesos políticos. Son las mismas ponderaciones anteriores, pero evaluadas por el cliente.
3. Asignación de pesos finales a los segmentos y secciones. El peso final es el promedio del peso técnico y del peso político. Las sub-secciones se calculan pero no se ponderan.

Se pondera la importancia relativa de la seguridad en los diversos sectores de la organización informática auditada.
Las asignaciones de pesos a secciones y segmentos del área de seguridad que se audita, se realizan del siguiente modo:
Pesos técnicos
Son los coeficientes que el equipo auditor asigna a los segmentos y a las secciones.
Pesos políticos
Son los coeficientes o pesos que el cliente concede a cada segmento y a cada sección del ciclo de seguridad.

Ciclo de Seguridad. Suma Pesos Segmentos = 100 (con independencia del número de segmentos consideradas)			
Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg1. Normas y Estándares	12	8	10
Seg2. Sistema Operativo	10	10	10
Seg3. Software Básico	10	14	12
Seg4. Comunicaciones	12	12	12
Seg5. Bases de Datos	12	12	12
Seg6. Procesos	16	12	14
Seg7. Aplicaciones	16	16	16
Seg8. Seguridad Física	12	16	14
TOTAL	**100**	**100**	**100**

Pesos finales

Son el promedio de los pesos anteriores.

El total de los pesos de los 8 segmentos es 100. Este total de 100 puntos es el que se ha asignado a la totalidad del área de Seguridad, como podría haberse elegido otro cualquiera. El total de puntos se mantiene cualquiera que hubiera sido el número de segmentos. Si hubieran existido cinco segmentos, en lugar de 8, la suma de los cinco habría de seguir siendo de 100 puntos.

Suma Peso Secciones = 20 (con independencia del número de Secciones consideradas)			
Secciones	**Pesos Técnicos**	**Pesos Políticos**	**Pesos Finales**
Secc1. Seg. Física de Datos	6	6	6
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
TOTAL	20	20	20

Puede observarse la diferente apreciación de pesos por parte del cliente y del equipo auditor. Mientras éstos estiman que las Normas y Estándares y los Procesos son muy importantes, el cliente no los considera tanto, a la vez que prima, tal vez excesivamente, el Software Básico.

Del mismo modo, se concede a todos los segmentos el mismo valor total que se desee, por ejemplo 20, con absoluta independencia del número de secciones que tenga cada segmento. En este caso, se han definido y pesado cinco secciones del segmento de seguridad física. Cabe aclarar, solo se desarrolló un solo Segmento a modo de ejemplo.

Fase 3. Operativa del ciclo de Seguridad

Una vez asignados los pesos finales a todos los segmentos y secciones, se comienza la Fase 3, que implica las siguientes actividades:

1. Preparación y confirmación de entrevistas.
2. Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma.

Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.

La realización de entrevistas adecuadas constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado. Si esta no se produce, el responsable lo hará saber al cliente.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.

La entrevista concreta suele abarcar sub-secciones de una misma sección tal vez una sección completa. Comenzada la entrevista, el auditor o auditores formularán preguntas al/los entrevistado/s. Debe identificarse quien ha dicho qué, si son más de una las personas entrevistadas.

Las Checklist's son útiles y en muchos casos imprescindibles. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede al levantamiento de la información correspondiente.

Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y reverificar los resultados de las pruebas auditoras.

La evaluación de las Checklists, las pruebas realizadas, la información facilitada por el cliente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoria, que se materializarán en el informe final.

A continuación, un ejemplo de auditoría de la sección de control de accesos del segmento de seguridad física:

Vamos a dividir a la sección de control de accesos en cuatro sub-secciones:

1. Autorizaciones
2. Controles Automáticos
3. Vigilancia
4. Registros

En las siguientes Checklists, las respuestas se calificarán de 1 a 5, siendo 1 la más deficiente y 5 la máxima puntuación.

Control de Accesos: **Autorizaciones**

Preguntas	Respuestas	Puntos
¿Existe un único responsable de implementar la política de autorizaciones de entrada en el Centro de Cálculo?	Si, el Jefe de Explotación, pero el Director puede acceder a la Sala con acompañantes sin previo aviso.	4
¿Existe alguna autorización permanente de estancia de personal ajeno a la empresa?	Una sola. El técnico permanente de la firma suministradora.	5
¿Quiénes saben cuales son las personas autorizadas?	El personal de vigilancia y el Jefe de Explotación.	5
Además de la tarjeta magnética de identificación, ¿hay que pasar otra especial?	No, solamente la primera.	4
¿Se pregunta a las visitas si piensan visitar el Centro de Cálculo?	No, vale la primera autorización.	3
¿Se preveen las visitas al Centro de Cálculo con 24 horas al menos?	No, basta que vayan acompañados por el Jefe de Explotación o Director	3
TOTAL AUTORIZACIONES		**24/30 80%**

Control de Accesos: **Controles Automáticos**		
Preguntas	Respuestas	Puntos
¿Cree Ud. que los Controles Automáticos son adecuados?	Si, aunque ha de reconocerse que a pie puede llegarse por la noche hasta el edificio principal.	3
¿Quedan registradas todas las entradas y salidas del Centro de Cálculo?	No, solamente las del personal ajeno a Operación.	3
Al final de cada turno, ¿Se controla el número de entradas y salidas del personal de Operación?	Sí, y los vigilantes los reverifican.	5
¿Puede salirse del Centro de Cálculo sin tarjeta magnética?	Si, porque existe otra puerta de emergencia que puede abrirse desde adentro	3
TOTAL CONTROLES AUTOMATICOS		**14/20 70%**

Control de Accesos: **Vigilancia**		
Preguntas	Respuestas	Puntos
¿Hay vigilantes las 24 horas?	Sí.	5
¿Existen circuitos cerrados de TV exteriores?	Sí.	5

Identificadas las visitas, ¿Se les acompaña hasta la persona que desean ver?	No.	2
¿Conocen los vigilantes los terminales que deben quedar encendidos por la noche?	No, sería muy complicado.	2
TOTAL VIGILANCIA		**14/20 70%**

Control de Accesos: **Registros**		
Preguntas	Respuestas	Puntos
¿Existe una adecuada política de registros?	No, reconocemos que casi nunca, pero hasta ahora no ha habido necesidad.	1
¿Se ha registrado alguna vez a una persona?	Nunca.	1
¿Se abren todos los paquetes dirigidos a personas concretas y no a Informática?	Casi nunca.	1
¿Hay un cuarto para abrir los paquetes?	Si, pero no se usa siempre.	3
TOTAL REGISTROS		**6/20 30%**

Fase 4. Cálculos y Resultados del Ciclo de Seguridad

1. Cálculo y ponderación de Secciones y Segmentos. Las Sub-secciones no se ponderan, solo se calculan.
2. Identificación de materias mejorables.
3. Priorización de mejoras.

En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoría de Seguridad.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Solo faltaría calcular el porcentaje de bondad de cada área; éste se obtiene calculando el sumatorio de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes.

Una vez realizado los cálculos, se ordenaran y clasificaran los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Sub-secciones de la Sección de Control de Accesos:

Autorizaciones 80%
Controles Automáticos 70%
Vigilancia 70%
Registros 30%
Promedio de Control de Accesos 62,5%

Cabe recordar, que dentro del Segmento de Seguridad Física, la Sección de Control de Accesos tiene un peso final de 4.

Prosiguiendo con el ejemplo, se procedió a la evaluación de las otras cuatro Secciones, obteniéndose los siguientes resultados:

Ciclo de Seguridad: **Segmento 8, Seguridad Física.**		
Secciones	Peso	Puntos
Sección 1. Datos	6	57,5%
Sección 2. Control de Accesos	4	62,5%
Sección 3. Equipos (Centro de Cálculo)	5	70%
Sección 4. Documentos	3	52,5%
Sección 5. Suministros	2	47,2%

Conocidas los promedios y los pesos de las cinco Secciones, se procede a calcular y ponderar el Segmento 8 de Seguridad Física:

> Seg. 8 = PromedioSección1 * peso + PromedioSecc2 * peso + PromSecc3 * peso + PromSecc4 * peso + PromSecc5 * peso / (peso1 + peso2 + peso3 + peso4 + peso5)
>
> ó
>
> Seg. 8 = (57,5 * 6) + (62,5 * 4) + (70 * 5) + (52,5 * 3) + (47,2 * 2) / 20
>
> Seg. 8 = 59,85%

A continuación, la evaluación final de los demás Segmentos del ciclo de Seguridad:

Ciclo de Seguridad. Evaluación y pesos de Segmentos		
Segmentos	Pesos	Evaluación
Seg1. Normas y Estándares	10	61%
Seg2. Sistema Operativo	10	90%
Seg3. Software Básico	12	72%
Seg4. Comunicaciones	12	55%
Seg5. Bases de Datos	12	77,5%
Seg6. Procesos	14	51,2%
Seg7. Aplicaciones	16	50,5%
Seg8. Seguridad Física	14	59,8%
Promedio Total Área de Seguridad	**100**	**63,3%**

Sistemática seguida para el cálculo y evaluación del Ciclo de Seguridad:

a. Valoración de las respuestas a las preguntas específicas realizadas en las entrevistas y a los cuestionarios formulados por escrito.

b. Cálculo matemático de todas las sub-secciones de cada sección, como media aritmética (promedio final) de las preguntas específicas. Recuérdese que las sub-secciones no se ponderan.
c. Cálculo matemático de la Sección, como media aritmética (promedio final) de sus Subsecciones. La Sección calculada tiene su peso correspondiente.
d. Cálculo matemático del Segmento. Cada una de las Secciones que lo componen se afecta por su peso correspondiente. El resultado es el valor del Segmento, el cual, a su vez, tiene asignado su peso.
e. Cálculo matemático de la auditoría. Se multiplica cada valor de los Segmentos por sus pesos correspondientes, la suma total obtenida se divide por el valor fijo asignado a priori a la suma de los pesos de los segmentos.

Finalmente, se procede a mostrar las áreas auditadas con gráficos de barras, exponiéndose primero los Segmentos, luego las Secciones y por último las Sub-secciones. En todos los casos se referenciarán respecto a tres zonas: roja, amarilla y verde.

La zona roja corresponde a una situación de debilidad que requiere acciones a corto plazo. Serán las más prioritarias, tanto en la exposición del Informe como en la toma de medidas para la corrección.

La zona amarilla corresponde a una situación discreta que requiere acciones a medio plazo, figurando a continuación de las contenidas en la zona roja.

La zona verde requiere solamente alguna acción de mantenimiento a largo plazo.

Fase 5. Confección del Informe del Ciclo de Seguridad

Preparación de borrador de informe y Recomendaciones.

Discusión del borrador con el cliente.

Entrega del Informe y Carta de Introducción.

Ha de resaltarse la importancia de la discusión de los borradores parciales con el cliente. La referencia al cliente debe entenderse como a los responsables directos de los segmentos. Es de destacar que si hubiese acuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado. Esta acta se incorporará al Informe Final.

Las Recomendaciones del Informe son de tres tipos:

Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.

Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.

Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.