Apuntes de Auditoría de Sistemas

Profesor : Alejandro Covacevich

Versión marzo de 2006

Apuntes de Auditoría de Sistemas

Alejandro Covacevich

Se dice que la gran mayoría de las instituciones está consciente de la importancia de la información en el éxito o fracaso de su misión. Sin embargo, las verdaderamente exitosas lo están también de los riesgos que entraña la inseguridad de aquélla.

Capítulo 1: Conceptos de Auditoría

Podemos definir Auditoría como un proceso voluntario o forzado para verificar que se están cumpliendo ciertos estándares técnicos, legales, laborales, sanitarios u otros relativos a la gestión institucional. El producto de una auditoría es un diagnóstico. Este puede ser una simple expresión de conformidad, o una señal de alerta destinada a inducir a los altos ejecutivos de la institución, a tomar medidas conducentes a cumplir con dichos estándares.

Un proceso de Auditoría puede ser forzado o voluntario. Es forzado cuando un organismo externo a la institución impone a ésta un cateo en el interior. Por ejemplo, cuando un perito fiscal indaga si un restorán está cumpliendo con las normas de higiene o cuando un detective inspecciona los computadores para determinar si no está instalado software pirata. En tal caso el diagnóstico puede concluir -no con una recomendación- sino con una orden perentoria, una multa o –peor aún- con una clausura.

Las auditorías voluntarias -como su nombre lo indica- son decididas por los propios ejecutivos de la institución. Muchas veces su objetivo es justamente anticiparse al riesgo que implican las auditorías forzadas, y funcionalmente se parecen a éstas, sólo que no terminan con una orden perentoria ni con una multa. En otros casos, la auditoría se orienta a prevenir otros riesgos, no necesariamente legales, o a detectar y corregir defectos crónicos que restan eficiencia a la operatividad de la institución.

Los siguientes son ejemplos de los riesgos que se pueden descubrir mediante un proceso de auditoría:

- No hay extintores de incendio
- No hay seguridad contra robos
- No existe control de calidad sobre las materias primas
- No se está cumpliendo con la normativa del SII
- Etc.

Algunos males crónicos:

- Se está incurriendo en costos excesivos
- La información actual no es la más adecuada
- El nivel de ruido disminuye la productividad
- Los operarios hurtan la materia prima

- Etc.

Aspectos y áreas a auditar

En una institución los rubros y las áreas operativas susceptibles de ser auditadas son muchísimos. De hecho no existe un profesional que pueda establecer un diagnóstico global acerca de una institución abarcando todas sus disciplinas o aspectos, ni aún tratándose de una empresa pequeña. En algunos casos, de hecho, se forman equipos multidisciplinarios que después se reúnen para conformar un diagnóstico más integral y consensuado.

Gestación de una auditoría voluntaria

En caso de contratar una auditoría voluntaria. lo primero que debe estar claro por parte de los ejecutivos de la empresa es:

1. Sobre qué disciplinas o aspectos se va a investigar y
2. Qué áreas, lugares físicos o lapsos van a ser inspeccionados.

Respecto al primer punto, algunos ejemplos son:

3. Auditoría Financiera
4. Auditoría Contable
5. Auditoría Sanitaria
6. Auditoría Laboral
7. Auditoría de Sistemas de Información
8. Auditoría del proceso productivo
9. Etc.

Cuando la empresa a auditar es mediana o grande, y dependiendo naturalmente de su estructura organizacional, la auditoría podría abarcar a sólo algunas de las secciones o algunas de las instalaciones, o corresponder a una auditoría transversal, por ejemplo, que abarque a todas las secciones pero en un aspecto específico. Cabe hacer notar que un aspecto puede estar conformado por varios sub-aspectos o aspectos de segundo nivel y cada una de éstos, por varios de tercer nivel. Un campo de auditoría en que esta complejidad se hace más patente es el que se refiere a la Auditoría de Sistemas, donde –como veremos- los aspectos a auditar son múltiples y sus interrelaciones, bastante complejas.

Objetivos Específicos de un Proceso de Auditoría

Desde el punto de vista del auditor (nos referimos a un profesional individual o a un equipo multidisciplinario) los sub-objetivos u objetivos específicos a alcanzar son globalmente los siguientes.

1. Delimitar el ámbito de la auditoría en cuanto a:.
    a) Aspectos a auditar
    b) Áreas funcionales

c) Lapso
d) Lugar físico

2. Definir los elementos críticos de cada uno de los aspectos a auditar y asociar a ellos los estándares usualmente aceptados. Si no existen estándares, el auditor debe aplicar su criterio profesional.

3. Elegir los tipos de herramientas de indagación para cada uno de los aspectos. Las herramientas pueden ser de 4 tipos.

   - Entrevistas
   - Cuestionarios
   - Listas de chequeo
   - En el caso de investigar información guardada en medios computacionales suele aplicarse también herramientas de software.

4. Adecuar las herramientas acorde a los elementos considerados críticos en el pto.2. La mayoría de los libros de auditoría contienen cuestionarios o check-list genéricos en los que el auditor se podría basar, eliminando las preguntas improcedentes o irrelevantes, adaptando otras al caso en cuestión, y agregando nuevas preguntas. Un auditor debería guardar los check-lists y cuestionarios como materia prima para obtener los instrumentos más adecuados a cada nuevo caso.

5. Aplicar en terreno las herramientas construidas. Podría pensarse que la auditoría consiste en aplicar un conjunto de plantillas (cuestionarios, entrevistas, checklists, etc.) preconcebidas y luego procesar la información para obtener el diagnóstico. En realidad –dada la gran diversidad de casos posibles- la adecuación de herramientas y su aplicación son actividades iterativas. En ningún caso la auditoría es una labor meramente mecánica. Más bien, el auditor debe internalizar los antecedentes que recoja y formarse un diagnóstico personal

   Respecto a los cuestionarios y checklists la aplicación puede ser

   a) Presencial, cuando el auditor se reúne con alguien de la empresa para recoger tanto datos precisos como impresiones que logren orientar la investigación.
   b) Masivo, se aplica en formularios orientados a recoger opiniones. En cualquier caso estos cuestionarios ayudan a orientar la posterior confección de checklists específicos
   c) Activa, cuando es el propio auditor quien va obteniendo las respuestas a partir de su observación de las instalaciones y tareas diarias, la lectura de los procedimientos (si es que los hay y están escritos) el muestreo de documentos y el análisis de la información de las bases de datos.

6. Analizar la información recogida.

7. Verificar en terreno la veracidad de la información, según algunos de los siguientes métodos:
    a) Entrevistas personales
    b) Observación
    c) Inspección de documentos

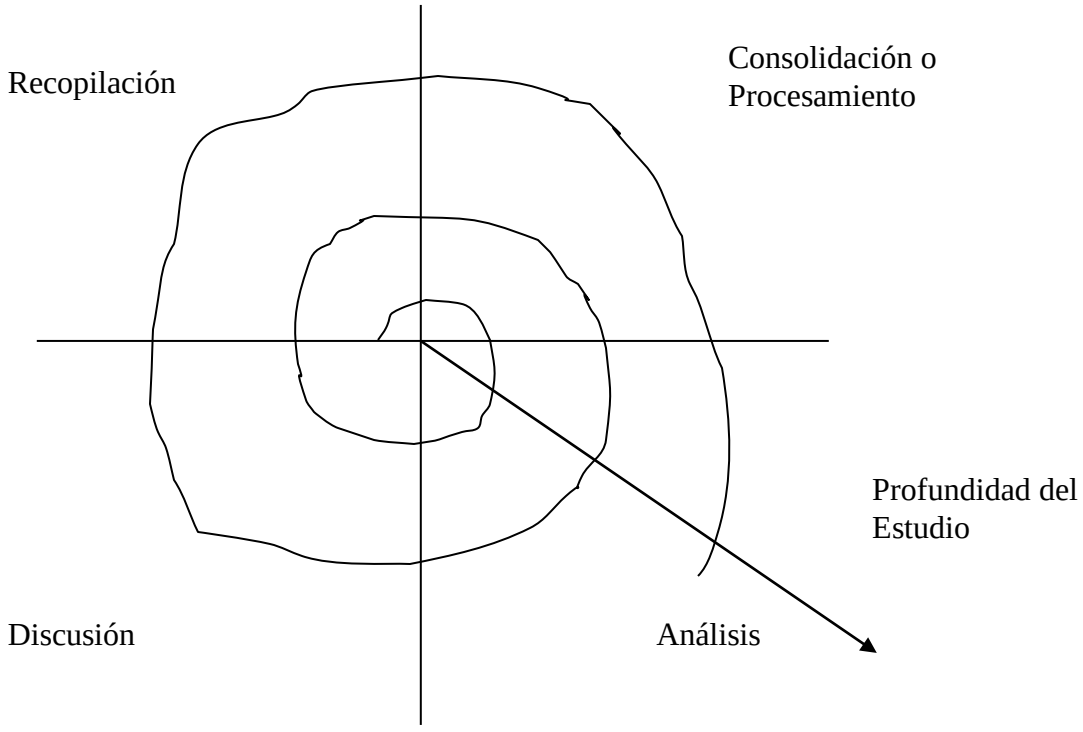
    La etapa de Verificación permite además dilucidar eventuales contradicciones de la información de base.

8. Confeccionar el diagnóstico, estableciendo los riesgos que se corren y recomendando las medidas a tomar. Todas las conclusiones de la auditoría y las recomendaciones pertinentes se entregan en un informe.

9. Exponer el informe ante las autoridades de la institución

10. Discutir con el cliente las conclusiones y recomendaciones hasta llegar a un documento consensuado.

Se aprecia que estas actividades corresponden a un típica metodología en cascada, la cual regularmente simplifica las cosas hasta un extremo utópico. En realidad las auditorías suelen ser iterativas, pareciéndose más a un modelo en espiral:



En el diagrama anterior, a medida que la curva se aleja del origen el estudio va ganando en profundidad iterando cuatro actividades básicas:

10. Recopilación, ya sea por observación, entrevistas, cuestionarios o checklists.
11. Consolidación, que consiste en ordenar los datos extraídos de acuerdo a algún modelo estadístico.
12. Análisis, consiste en el estudio estadístico de los resultados de la etapa anterior a fin de llegar a una conclusión
13. Discusión, es una etapa de intercambio de ideas con el cliente, que origen a la siguiente vuelta.

Recopilación

En las primeras vueltas la aproximación al problema requiere de preguntas relativamente simples, a fin de conocer:

14. Misión de la Institución
15. Mercado
16. Tamaño
17. Factores críticos de éxito
18. Sistemas de Información que están actualmente ocupándose
19. Usuarios
20. Nivel de criticalidad de cada sistema
21. Configuración computacional
22. Cantidad de Operadores
23. Cantidad de usuarios
24. Cantidad de transacciones
25. Efectos posibles de la eventuales fallas en cada sistema
26. Etc.

La técnica más adecuada para recabar información en las primeras vueltas, es la entrevista. A medida que el estudio va siendo más específico, en las siguientes vueltas, las preguntas requieren mayor precisión y son aconsejables los cuestionarios y checklists. La etapa de Recopilación incluye también una actividad de Verificación, que puede ejecutarse mediante investigación activa (analizando documentos o archivos computacionales) o simplemente verificando consistencia de las evidencias.

Consolidación o Procesamiento

Consiste en tabular o graficar los datos obtenidos a fin de obtener finalmente indicadores que señalen cómo continuar en las siguientes vueltas del espiral. Por supuesto, tras las primeras vueltas no hay una etapa de consolidación sino que la simple lectura de la información recopilada induce el área a investigar, o el camino a seguir en la siguiente bifurcación.

Análisis de Resultados

Los resultados corresponden a una simple tabulación o a una consolidación a primer nivel de los datos recopilados. En la etapa de Análisis se obtienen indicadores que conducen en forma más o menos directa a las conclusiones y recomendaciones. El análisis en las primeras vueltas del espiral es prácticamente inexistente pero a medida que la investigación avanza aumenta el vínculo entre los resultados y las conclusiones.

Discusión

La Discusión es una instancia de entrega parcial que exige la participación y el aporte del cliente tanto para corroborar los resultados (en las primeras vueltas) como para internalizar conclusiones y/o aceptar u objetar las recomendaciones. Si las conclusiones son consensuadas se vacian a un informe final que contiene el Diagnóstico de Auditoría.

Capítulo 2: Auditoría Tradicional de Sistemas

Cuando hablamos de Auditoría de Sistemas nos referimos a procesos voluntarios ejercidos sobre los activos de información, esto es hardware, software, instalaciones, personal y procedimientos humanos que permiten capturar, almacenar, procesar y distribuir la información que requiere la empresa. Por extensión también abarca las comunicaciones que se ejecutan mediante estos activos, esto es, los mensajes de correo electrónico aunque su contenido no provenga directa ni indirectamente de las bases de datos del sistema

En todo caso el primer requisito del profesional que ejerce una auditoría de sistemas es un conocimiento formal de los riesgos que conlleva para la institución un fallo de los sistemas, y de los estándares de calidad que deben ser tomados como patrones de comparación para el diagnóstico.

Si bien los objetivos específicos de cada proceso de auditoría informática requiere ser analizado exhaustivamente (de hecho este curso resta relevancia a las normas generales en beneficio del análisis de casos específicos) , en el último tiempo la demanda de auditoría de sistemas ha aumentado notablemente, debido a 4 razones (COBIT):

a) La creciente dependencia que experimentan las empresas respecto de la información.
b) La creciente vulnerabilidad y amplitud del espectro de amenazas
c) El incremento en el costo del software
d) La potencial capacidad de las TI de cambiar radicalmente la organización y las prácticas de negocio.

A modo de ilustración, algunos de los posibles efectos perjudiciales que podrían emanar de una falla en los sistemas de información son los siguientes:

27. Dejar de producir
28. Producir un producto equivocado
29. Dejar de cobrar
30. Tomar decisiones estratégicas erróneas (por ejemplo adquirir maquinaria no apta)
31. Dejar de vender

Aspectos de primer nivel de la Aditoría de Sistemas

La Auditoría de Sistemas se divide tradicionalmente en los siguientes aspectos

1. Auditoría de Seguridad. Se orienta a recoger y analizar indicios (también se les llama evidencias) de que la información que normalmente ingresa, se almacena, se procesa y sale del sistema es:
    a) Verídica
    b) Oportuna
    c) Está protegida de ataques externos
    d) Está protegida contra accidentes

e) Llega a los que la necesitan
f) No llega a quien no debe conocerla

2. Auditoría de Contingencia. Comprueba que existen resguardos que reducen la probabilidad de caída de un sistema de información y que la empresa está preparada para seguir operando, al menos por un tiempo prudencial, en caso de que cualquiera de sus partes (esto es captura, almacenamiento, proceso o rescate de información) deje de funcionar.

3. Auditoría de Gestión. Se orienta a determinar si la información –en cuanto a contenido, nivel de consolidación y formato- es realmente aquélla que los usuarios requieren para su gestión.

4. Auditoría de Desarrollo. Determina si el proceso de construcción de los sistemas de la institución cumple con ciertas normas básicas de calidad.

5. Auditoría Legal. Verifica que el software que se está empleando ha sido obtenido legalmente.

6. Auditoría de Costos. Determina si los costos de desarrollo, operación y mantenimiento de sistemas de información de una compañía no exceden los niveles aceptables.

7. Auditoría de Adquisiciones, se refiera a si la incorporación de nuevo hardware y software de base es necesaria y suficiente y está alineada con la misión de la institución.

Fases de la Auditoría

Considerando lo expresado en el apartado referente a Objetivos Específicos todo proceso de Auditoría debe tener un plan inicial, independientemente del hecho casi inevitable de que éste vaya variando a medida que se va conformando el diagnóstico definitivo.

Caso de aplicación

Por ejemplo, como el objetivo del estudio desarrollado por Femenías, Millar y Zúñiga "Seguridad del Sistema Operativo para una Compañía de Seguros" (UCINF 2003), estaba orientado esencialmente a establecer la veracidad de la información contenida en la base de datos y detectar posibles intervenciones maliciosas. Se consideró inicialmente las siguientes etapas:

1. Definición y Acotación de los Objetivos. En este caso se trató de acotar el entorno sujeto de auditoría tal como se muestra en el punto del apartado de Objetivos, esto es:

a) Aspectos a auditar

b) Áreas funcionales
c) Lapso
d) Lugar físico

Considerando la precisión del objetivo del trabajo se dio relevancia al aspecto c), esto es el lapso de transacciones que se debía investigar, debido a que un error consistente en incluir dentro del lapso a investigar una anomalía que se produjo fuera de este lapso, podría distorsionar gravemente las conclusiones del informe.

2. Catalogar y cubicar las posibles fuentes de evidencias. En este caso, lo fueron los documentos fuente y los archivos de transacciones.
3. Confección del plan de Trabajo. Esta actividad consiste en asignar entre los participantes la carga de trabajo considerando el volumen de información, y la disgregación documental en el interior de la base de datos.
4. Confección de Herramientas. Si bien se adaptaron cuestionarios a fin de delimitar bien el problema, la herramienta esencial fue un conjunto de programas listadores que presentaron la información transaccional en forma ordenada para una revisión comparativa versus los documentos físicos.
5. Revisión. La revisión involucró -además del cotejo mecánico de la información de base versus sus respectivas fuentes, conocer los mecanismos de consolidación, y en general cada uno de los algoritmos de procesamiento lo cual indujo entrevistas aclaratorias.
6. Análisis de Resultados y Valoración de Riesgos. En cada caso de anomalía se cuantificó subjetivamente el impacto sobre la organización. Ello implicó por cierto sostener entrevistas con ejecutivos de los niveles táctico y estratégico.
7. Presentación y Discusión del informe preliminar

Capítulo 3: CobiT

La auditoría de sistemas es una actividad compleja por varias razones:

1. No está claro qué se entiende por sistema de información. De hecho en el interior de una empresa los entes que manipulan la información son los mismos que la utilizan para gestionar el negocio. En consecuencia ¿qué aspectos debe abarcar la auditoría de sistemas?
2. Los aspectos a auditar aumentan y se hacen más complejos constantemente. Cuando la computación era centralizada, los procedimientos eran relativamente pocos y lo computacional estaba nítidamente separado de lo que llamamos gestión, comunicándose con ésta a través de procedimientos humanos de interfaz. Hoy, los controles hacen hincapié en las comunicaciones electrónicas a nivel mundial.
3. Consecuentemente la mayoría de los libros de auditoría están obsoletos y prestan escasa utilidad.
4. Han surgido históricamente numerosos modelos de auditoría, tales como ITSEC, TCSEC, ISO-9000 y otros que no consiguen formar una base estable. Esta cantidad de enfoques más que brindar un bagaje sólo consigue confundir a los aspirantes a auditores.

El especialista en informática que se inicia como auditor de sistemas -a pesar de su formación- rara vez está mentalmente organizado para una función de ese tipo. Tiene una vaga idea de algunos indicios dispersos que le hablan de la confiabilidad de una instalación, pero carece de una visión global sobre los sistemas en todos sus aspectos auditables. Si un gerente le encargase realizar una auditoría de sus sistemas carecería de método. No sabría cómo segmentar el estudio ni menos qué cuestionarios hacer o qué preguntar en las entrevistas.

Como ente unificador de las diversas corrientes de auditoría ha surgido CobiT (Control Objectives on Information Technologie). CobiT es un estándar generalmente aceptado y aplicable para las buenas prácticas de seguridad y control en Tecnologías de Información, fundamentado en los Objetivos de Control de la Information Systems Audit. and Control Foundation (ISACF) . CobiT no es excluyente y de hecho recoge elementos, como estándares técnicos de ISO, EDIFACT, y otros organismos, unifica códigos de conducta y criterios de clasificación de ITSEC, ISO9000, SPICE, TickIT, etc. (Lectura recomendada “Antecedentes de CobiT” en internet).

Algunas definiciones de CobiT:

Control se define como:

Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

Objetivo se define como:

Una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

De hecho la segregación de una auditoría en un conjunto de Objetivos clasificados permite, por una parte, el esencial ordenamiento mental y –por otra- brinda una base para construir la herramientas de control que, por supuesto, tendrán diferente nivel de profundidad según sea el tamaño de la empresa. Por último constituye una base para conversar con el cliente acerca de los aspectos que se desea auditar.

Como se ha dicho *Cobit* es un organismo de la la *Information System Audit and Control Fondation (ISACF)* cuya misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de compañías auditoras.

En su 2da Edición, de 1998, Cobit hace referencia a 4 grandes dominios (Planeación y Organización, Adquisición e Implementación, Entrega de Servicio y Monitoreo) de la Auditoría, que se disgregan en 34 objetivos. Como se verá, los objetivos se disgregan a su vez en un conjunto de 302 sub-objetivos. A partir de estos sub-objetivos, y conociendo las características esenciales de la institución auditada, su configuración y la organización interna, el auditor puede construir las herramientas (cuestionarios, checklists y entrevistas) aplicables a cada caso específico. El promedio de preguntas por cada sub-objetivo es alrededor de 10, por lo que una auditoría exhaustiva de Sistema en una institución se podría conducir respondiendo a unas 3000 preguntas. Algunas de ellas se pueden rescatar de cuestionarios masivos, otras de entrevistas personales y otras de la observación y el análisis de los documentos existentes.

Una síntesis de los Dominios y Objetivos de primer nivel sustentados por CobiT es la siguiente:

P Planeación y Organización: Se refiere fundamentalmente a la existencia de planes informáticos en la institución. Estos planes –si es que existen- marchan alineados con el plan de Desarrollo global de la Compañía.

P01 Desarrollo de un Plan Estratégico de Tecnología de Información
P02 Definición de la Arquitectura de Información
P03 Determinación de la Dirección Tecnológica
P04 Definición de la Organización y Relaciones de TI
P05 Manejo de la Inversión en TI
P06 Comunicación de la Dirección y Aspiraciones de la Gerencia
P07 Administración de Recursos Humanos
P08 Aseguramiento de Cumplimiento de Requerimientos Externos
P09 Evaluación de Riesgos
P10 Administración de Proyectos
P11 Administración de Calidad

A Adquisición e Implementación: Se refiere a la adquisición de nuevos recursos en al área informática, ya sea mediante, compras, leasing, arriendo o desarrollo propio. Incluye la incorporación de profesionales y la capacitación del personal existente. Las adquisiciones deberían estar alineadas con el Plan Estratégico

A01 Definición de Requerimientos de Información
A02 Software de Aplicación
A03 Adquisición y Mantenimiento de Arquitectura de Tecnología
A04 Desarrollo y Mantenimiento de Procedimientos relacionados con TI
A04 Instalación y Acreditación de Sistemas
A05 Administración de Cambios

S Entrega de Servicios y Soporte: Comprende todos los aspectos relativos al servicio actual, incluyendo seguridad, eficiencia, efectividad, confiabilidad, disponibilidad, integridad y cumplimiento.

S01 Definición de Niveles de Servicio
S02 Administración de Servicios Prestados por Terceros
S03 Administración de Desempeño y Capacidad
S04 Asegurar la Continuidad del Servicio
S05 Garantizar la Seguridad de los Sistemas
S06 Identificación y Asignación de Costos
S07 Educación y Entrenamiento de Usuarios
S08 Apoyo y Asistencia a los Clientes de TI
S09 Administración de la Configuración
S10 Administración de Problemas e Incidentes
S11 Administración de Datos
S12 Administración de Instalaciones
S13 Administración de Operaciones

M Monitoreo: Se orienta principalmente al seguimiento del desempeño a través de indicadores de gestión incluyendo indicadores clave, factores críticos de éxito, etc.

M01 Monitoreo del Proceso
M02 Evaluar lo Adecuado del Control Interno
M03 Obtención de Aseguramiento Independiente
M04 Proveer Auditoría Independiente

Construcción de una herramienta de Auditoría a partir del Instrumento CobiT

Por supuesto, que el estudio exhaustivo del método y su ulterior aplicación in extenso es un bagaje que no se puede dictar en pocas semanas sin pecar de superficialidad. En este curso trataremos con cierta profundidad sólo el Dominio S, esto es Entrega de Servicio, que es –por lo demás- el más cercano al enfoque tradicional de auditoría informática.

Vamos a partir por el primer objetivo del dominio S, esto es:

S01 Definición de Niveles de Servicio

Este nivel pretende establecer Niveles de Servicio a fin de establecer una comprensión común del nivel de servicio requerido en una caso específico. Esto se hace posible a través del establecimiento de niveles de desempeño contra los cuales se medirá la calidad y la cantidad del servicio entregado.

Para ello toma en consideración los siguientes aspectos:

5. Convenios formales
6. Definición de Responsabilidades
7. Tiempos y volúmenes de respuesta
8. Dependencias
9. Cargos
10. Garantías de Integridad
11. Convenios de Confidencialidad

El primer sub-objetivo se refiere a:

1.1 Marco de Referencia para el Convenio de Niveles de Servicio.

El instrumento Cobit dicta en ese aspecto, los siguientes criterios:

"La alta Gerencia deberá establecer un Marco de Referencia en donde presente la definición de los convenios sobre niveles formales de servicio y determine el contenido mínimo, disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de Contingencia/Recuperación, nivel mínimo aceptable de funcionalidad de cada sistema liberado satisfactoriamente, restricciones (esto es límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central, (disponibilidad), distribución de impresión central y administración de cambio. Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos. El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y cantidad de los servicios ofrecida y los usuarios deberán ajustar los servicios solicitados a los límites acordados"

El texto anterior constituye un patrón que indica al auditor qué es lo que tiene que investigar en caso que su contrato de auditoría incluya el aspecto descrito (en realidad en

empresas medianas y pequeñas no es usual que se exija), en base a éste es –desde luego- posible empezar a formular ciertas preguntas. Será función ulterior del auditor resolver mediante qué herramienta buscará la respuesta respectiva.

Veamos, a modo de ejemplo, cómo podemos construir un cuestionario vía análisis del texto de CobiT detallado más arriba.

Texto: "La alta Gerencia deberá establecer un Marco de Referencia...

Pregunta 1: ¿Existe un Marco de Referencia elaborado por la Gerencia respecto a los Servicios que debe entregar Informática? Si ( ) No ( )

Si la respuesta es negativa, debe saltarse a la pregunta 8

Texto: "...en donde presente la definición de los convenios sobre niveles formales de servicio..."

Pregunta 2: El marco de referencia ¿establece cuáles son los niveles de servicio por parte de Informática indicando los mínimos aceptables en cada caso?

Si ( ) No ( ) Sí pero insuficiente ( )

Texto "...disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario... "

En este caso vale la pena formular una pregunta múltiple con los aspectos que se señalan, colocando una nota (de 1 a 3) por el grado de satisfacción que involucra cada aspecto. Dejar el casillero en blanco implica que el Marco de Referencia no toca el aspecto señalado:

Pregunta 3

El Marco de Referencia de la Gerencia establece los mínimos indicados a continuación?

Disponibilidad	**3**
Confiabilidad	**2**
Desempeño	
Capacidad de Crecimiento	
Nivel de soporte proporcionado al usuario	**2**

Texto: " ... plan de Contingencia/Recuperación..."

Pregunta 4

¿Existen en el Marco de Referencia especificaciones acerca del alcance del Plan de Contingencia/Recuperación.? Si ( ) No ( ) Sí pero insuficiente ( )

Texto: "...nivel mínimo aceptable de funcionalidad de cada sistema liberado satisfactoriamente..."

Pregunta 5

¿Existen especificaciones acerca del nivel mínimo aceptable de funcionalidad de cada sistema liberado satisfactoriamente? Si ( ) No ( ) Sí pero insuficiente ( )

Texto: "...restricciones (esto es límites en la cantidad de trabajo) "

Pregunta 6

¿Especifica el Marco de Referencia alguna restricción a la jornada laboral?
Si ( ) No ( ) Sí pero insuficiente ( )

Texto: "...instalaciones de impresión central..."

Pregunta 7

¿Especifica el Marco de Referencia algunas características operacionales respecto de las instalaciones de impresión? Si ( ) No ( )

¿Cuáles? _____

Texto: "...Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos..."

Pregunta 8

¿Existe un Convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos?

Si ( ) No ( ) Sí pero insuficiente ( )

En caso negativo saltarse a la Pregunta 10

Texto "...El convenio definirá las responsabilidades de ambas partes...."

Pregunta 9

¿El convenio de servicio define las responsabilidades de ambas partes (personal de informática y usuarios)?

Si ( ) No ( ) Sí pero insuficiente ( )

Texto: "La función de servicios de información deberá prestar la calidad y cantidad de los servicios ofrecida..."

En este caso se trata obviamente de una encuesta de opinión que debe formularse a los usuarios

Pregunta 10: ¿Considera Ud. que los niveles de servicio de informática son los adecuados en términos de calidad y cantidad?

Si ( ) No ( )

Especificar por qué no_____

Texto: "...los usuarios deberán ajustar los servicios solicitados a los límites acordados"

En este caso se trata obviamente de una encuesta de opinión que debe formularse al personal de informática.

Pregunta 11: ¿Considera Ud. que las solicitudes de los usuarios se ajustan a los límites acordados en el convenio?

Si ( ) No ( )

Especificar por qué no_____

Ejercicio: Con en método descrito desarrolle cuestionarios para los sub-objetivos S 2 a S 13.

De Cobit A13

Adquisición y Mantenimiento de arquitectura de Software:

¿Se evalúa el impacto de nuevo hardware y software sobre el rendimiento del sistema en general?

¿Existe algún procedimiento de evaluación?

Analizar el procedimiento y proponer mejoras.

Existen instancias prefijadas de mantenimiento rutinario del hardware

Analizar la rutina establecida

¿Cuál es la frecuencia de fallas?

¿Se mantiene alguna estadística acerca del origen de las fallas?

Al instalar nuevo software ¿Existe algún procedimiento que asegure que no se vulnere la integridad de los datos?

Se hacen pruebas del software antes de su instalación.

Se siguen las normas establecidas por el fabricante?

Etc.

Capítulo 4: Auditoría de Procedimientos

Ver Consultoría Informacional

Capítulo 5: El Delito Informático

Ley Relativa a Delitos Informáticos
LEY 19223

Artículo 1º.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 28 de Mayo de 1993.- ENRIQUE KRAUSS RUSQUE, Vicepresidente de la República.- Francisco Cumplido Cereceda, Ministro de Justicia.

Identificación de la Norma : LEY-19223
Fecha de Publicación : 07.06.1993
Fecha de Promulgación : 28.05.1993
Organismo : M JUSTICIA

Fuente: Biblioteca del Congreso Nacional

Trabajo para un alumno: Efectuar una comparación con la ley que existe en otros países.

Capítulo 6: Casos de Análisis

Estimar el alcance de la auditoría según diversos factores.

Hacer una auditoría de sistemas es un término demasiado amplio como punto de partida de un proceso Recordemos, por ejemplo algunos accidentes informáticos que se podrían haber previsto se hubiera aplicado previamente un proceso de auditoría:

1. A fines de 2005 el Ministerio de Educación adjudicó una beca universitaria a los 14.000 alumnos de mayores ingresos de una lista de 50.000. La causa fue un "error del computador". Las consecuencias: escándalo político, reasignación de becas a todos los estudiantes, desprestigio de la cartera entre otros,
2. En 1985 el zócalo de ECOM se inundó por una crecida del Mapocho, destruyendo la instalación computacional y la información de respaldo. Consecuencias: quiebra de la empresa y pérdidas cuantiosas para sus clientes.
3. En 1997 una secretaria del Banco Central entregó a la empresa Inverlink información reservada vía e-mail. Consecuencias: Escándalo político, procesamiento de los responsables, renuncia de Massad, director del banco, pérdidas cuantiosas entre los clientes de Inverlink, entre otros
4. En 2000 una clienta demostró que en su cartola bancaria había un error de suma. Consecuencias: Desprestigio para el banco, indemnizaciones, despidos, revisión de todos los procesos informáticos. No obstante lo anterior, no se logró reproducir el error por lo que el caso se archivó sin solución.
5. En 1997 el Servicio de impuestos internos puso a disposición del público un sistema que permitía hacer las declaraciones de renta desde la casa. El sistema tenía una falla que hacía posible evadir impuestos. Consecuencias: muchas personas evadieron impuestos con pérdidas cuantiosas para el estado pero el asunto nunca salió a la luz pública.
6. En 2001 dos aviones de pasajeros destruyeron el World Trade Center donde operaban cientos de empresas y compañías transnacionales. Consecuencias (en el terreno informático por supuesto): destrucción de todo el hardware. En cuanto a software e información, casi ninguna. Toda la información y los sistemas que la procesaban estaban respaldados en servidores externos.
7. En Abril de 1978 se borró por razones eléctricas el disco duro de la Municipalidad de Peñalolén. Consecuencias: Hubo que reconstruir la información pero el proceso de patentes de vehículos pudo continuar en forma manual ya que se había previsto cómo proceder en caso de caída del sistema o corte de energía.
8. En 2002 el computador de la compañía de gas de San Felipe dio por saldadas las cuentas de varios clientes. El asunto se detectó por casualidad varios meses después y se comprobó que el hecho estaba ocurriendo desde hacía tiempo. Consecuencias: incuantificables.
9. En 2000 el virus Sigmund destruyó toda la información del disco duro en un juzgado argentino. Varias causas quedaron inconclusas. No había antivirus ni ningún tipo de repaldo.
10. En 1997 un paquete de recibos de pago de patentes de la Municipalidad de Conchalí no se ingresó al computador pero se dio por ingresada suscitando cobranzas judiciales indebidas y ocasionando el cierre de algunos establecimientos.

11. En 1983 un ingeniero informático de un banco londinense modificó un programa ocasionando que las diferencias de centavos al procesar los movimientos se abonar a una cuenta específica. El fraude operó durante varios meses antes de ser descubierto.
12. En 1983 el encargado de la contabilidad de un sistema en red informó diferencias entre las cuadraturas reales y las cuadraturas teóricas. Investigado el caso, se detectó que los miembros de una sección de la empresa (el departamento de Producción) tenían habilitada la opción de hacer ajustes a los datos que para Contabilidad representaba los cierres periódicos.
13. Una empresa detectaba que el **rendimiento de los trabajadores** había baja bajado considerablemente. Solución y actuación de AuditoriaSistemas.
Creamos unas **políticas de seguridad** informática y unas **normas de uso informático** para la empresa. Todos los trabajadores se comprometieron a cumplirlas. Además instalamos dos sistemas de control interno. Un sistema de **control del correo electrónico** que emitían y recibían los trabajadores. Y otro sistema de **control de las páginas web** que se visitaba cada trabajador de la empresa. Beneficio: La empresa **incrementó la productividad** de sus trabajadores y disminuyó el **riesgo de perdidas**

14. El día 24 de Febrero de 1998 FAVAT (Familiares de Víctimas de Tránsito) interpuso una demanda contra una empresa importadora del juego Carmageddon, por instigación a cometer delitos, incitación a la violencia y apología del crimen. Es un juego violento, el entretenimiento demanda arrollar a peatones para sumar puntos que varía de acuerdo con el peatón. Arrollar a una embarazada reditúa más, en cambio eliminar a un anciano otorga menos puntos, porque se presume más indefenso.

15. Recientemente la Compañía informática Omega, despidió a un empleado que hacía 11 años dirigía la red de computación. Antes de dejar la empresa colocó una "bomba de tiempo lógica" y además destruyó todas las copias de seguridad.

La desaparición de todos los datos de la empresa causó un perjuicio que se estima en 10 millones de dólares.

16. Un hacker atacó la página del diario La República de Lima reemplazando la información por una diatriba contra el presidente Toledo. El diario tuvo que pedir disculpas.

Indicar cuáles de los casos anteriores son delictuales según la ley.
Cuáles son no accidentales.

Análisis de los casos.

Caso 1:

No está claro si el efecto público se debió a un error de los programas, a falta de entrenamiento de quienes debían decidir basándose en la información del computador o a presiones externas (Alguien puede verse favorecido si se garantiza que los alumnos acreditados podrán efectivamente pagar su deuda). No resulta muy verosímil que todo el

origen resida en un error del computador o que no existieran los procedimientos para comprobar el error.

Si realmente se trata de presiones externas, habría que poner mucho ojo en el control de aquéllas medidas que restringen las leyes del mercado (por ejemplo, la norma de este establece que quienes más tienen más tienen más crédito tendrán). También podría ser que todo fuera una maniobra a fin de presionar al gobierno para otorgar más créditos. ¿Qué cree Ud.?

Trabajo para un alumno: Investigar qué pasó y establecer los controles necesarios.

Caso 2:

Aquí hay obviamente una política de respaldo inadecuada. Toda la información y los programas estaban respaldados pero en la misma instalación y sin ninguna protección física: no existían cámaras de seguridad ni caja fuertes. De hecho los manuales de explotación que se generaban en esa época hacían bastante hincapié en mantener cintas abuelo-padre-hijo pero no decían dónde había que guardarlas.

Trabajo para un alumno: Describir el caso ECOM incluyendo sus causas.

Caso 3:

Se trata de un atentado a la privacidad de la información y está tipificado en la

Caso 4:

Dada la amplitud del mercado bancario, no se puede suponer que se trate de un error frecuente. A veces los programas pasan por situaciones coyunturales muy infrecuentes que generan errores que no se pueden reproducir "en laboratorio". Con todo, los sistemas valóricos requieren pruebas y vigilancia exhaustivas. Por ejemplo un sistema que emite cheques para pagar a proveedores. Está claro que estos van a reclamar si los cheques salen por una cantidad menor a la factura pero no la harán si la cantidad es mayor. Un sistema bancario además es masivo

Caso 5:

Dicho sistema entra en la categoría de Sistemas Perfectos. Es decir, de aquello que no pueden liberar versiones Beta. Las características residen en el ámbito general del sistema:

a) Es un sistema valórico, como el de los bancos, esto es que la realidad es lo que muestra el sistema. No existe una realidad "real" como en un sistema de stock, donde eventualmente se puede compara la información sobre los saldos, contra lo que efectivamente hay en bodega.

b) Es un sistema conversacional abierto al público a través de la red y no existe ningún criterio para seleccionar usuarios.

En este ámbito las pruebas del SC deben ser exhaustivas

Caso 6:

Describir los tipos de respaldo que existían en el WTC indicando los daños informáticos reales que se produjeron

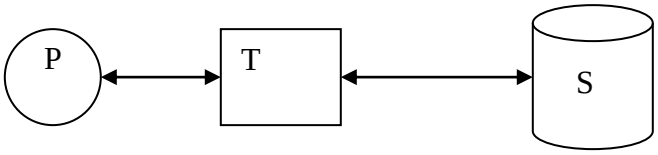
Caso 12:

Se trata de una falla del sistema interno de seguridad. Un sistema no puede permitir que una parte de sus usuarios tenga acceso a modificar información que otra parte (el departamento de Contabilidad, en este caso) considera información histórica inamovible. Un sistema debe conciliar el modus operandi de diversas culturas de usuarios, ciñéndose a las reglas del más exigente. El tipo de información -en el sentido de "histórica o actual"- debe especificarse en forma homogénea para todos los usuarios. En ese sentido, es recomendable aplicar el concepto de "dueño de los datos".

Transacciones externas

Uno de los factores que inciden sobre la profundidad y relevancia de un plan de auditoría es la intensidad de la relación del sistema con entes externos, sean estos clientes, proveedores, contribuyentes, etc. Existen varios esquemas para las transacciones externas, por ejemplo:

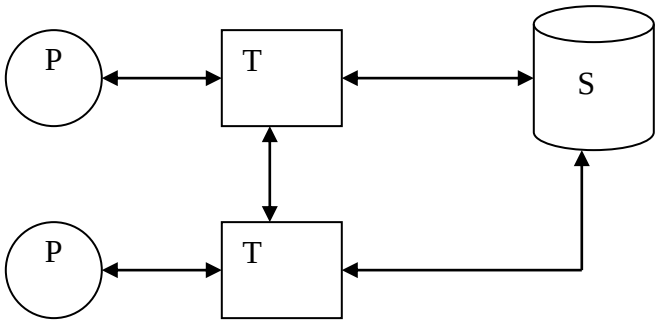
a) Público-Terminal-Sistema



El público ingresa sus transacciones a través de un terminal (generalmente su propio computador conectado al sitio del sistema) y el terminal le devuelve la conformidad o el comprobante. Esta modalidad de conexión es la que utiliza, por ejemplo, el SII de Impuestos internos para capturar las declaraciones de renta. Otros casos:

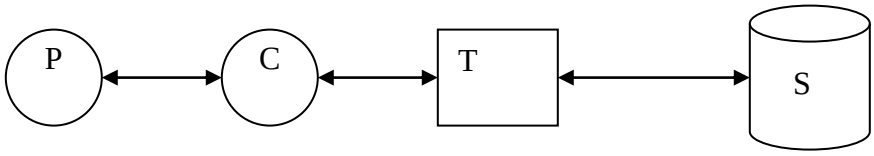
- Amazon.com
- Despegar.com
- Etc

b) Público-Terminal-Público- Sistema



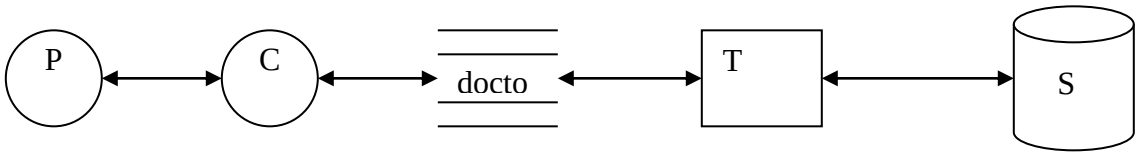
Corresponde a una transacción tripartita entre dos entes públicos y el Sistema. Por ejemplo el envío y recepción de una boleta o una factura electrónica.

c) Público-Cajero-Terminal-Sistema



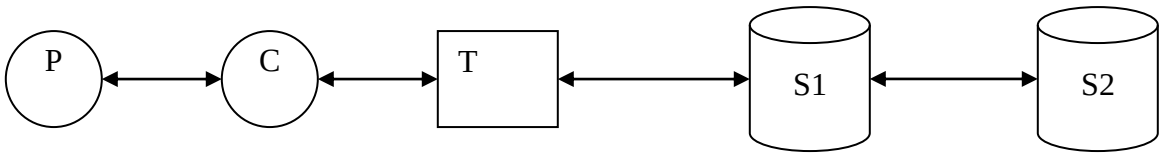
El público acude a una ventanilla y se relaciona con un cajero (persona), que recibe la transacción y la ingresa al sistema. Por ejemplo, los depósitos o giros en un banco, el pago de las patentes de vehículos, una reserva de hora en un centro de salud. Es el esquema más tradicional de transacciones en línea.

d) Transacciones Batch



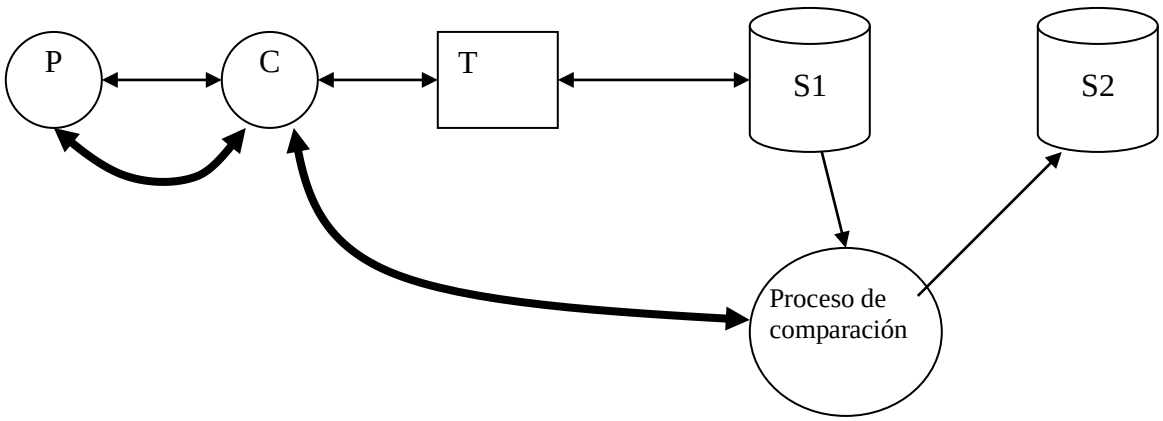
El cajero genera documentos en papel que después se incorporan al sistema a través de un terminal. Esta modalidad ya es poco usada.

e) Transacciones a través de una institución de servicio



Los datos son recogidos por un cajero a través de un terminal y transmitidos a un sistema externo a la institución. El envío hacia el sistema de la institución es batch y periódico. Por ejemplo, el pago de contribuciones a través de un banco, pagos a través de Servipag o Sencillito, etc.

Debe cosiderarse que en muchos casos la comunicación externa requiere –además del datp digital- el envío de un papel. Comparar los totales de los papeles y los de la transmisión electrónica es uno de los controles más usuales.



Como se muestra en la figura anterior, en el esquema e) antes de ingresar los datos al sistema se valida que cuadren con los documentos.

Tarea: Representar el flujo de documentos (si es que existe) y las correspondientes validaciones para los casos a, b, c y d. Indicar otros esquemas de captura de transacciones desde el público.

Otros tópicos a desarrollar

Política de respaldos

El único remedio infalible para evitar la pérdida de información valiosa dentro de su computadora es mantener una política de respaldos regulares. Estos respaldos pueden ser llevados a cabo con programas “espejo”, que crean una imagen de su disco duro desde la cual pueden recuperar la totalidad de los datos o mediante el simple procedimiento de guardar una copia en un medio extraíble, alejado de las contingencias cotidianas.

Aunque muchos usuarios conocen esta metodología segura, pocos optan por ella, bien sea por falta de tiempo o porque son víctimas de alguna eventualidad imprevista durante el trabajo, que limita las oportunidades de salvar lo que se está haciendo en el momento. Las más célebres son los “cuelgues” de los sistemas operativos, seguidos por las fallas en el suministro eléctrico, errores a la hora de guardar el trabajo y otros cientos de problemas que pueden hacerle perder incontables horas de esfuerzo.

Algunos estudios señalan que un usuario regular de computadoras personales sufre entre cuatro y cinco “incidentes” anuales, en los que se ven comprometidos archivos o datos importantes; en casi todos ellos, la pérdida de información tiene orígenes poco claros para el afectado, quien se limita a sufrir los males derivados del extravío sin saber que en la mayoría de los casos, la solución a su problema se encuentra a escasos clics de distancia.

Como primer paso para cualquier proceso de rescate de datos: ¡No reescriba el disco!, almacenar datos nuevos en un medio que ha sufrido pérdidas de archivos ó documentos, comprometerá seriamente las posibilidades de recuperarlos. Como referimos en una edición anterior, el procedimiento habitual usado por los sistemas operativos en el proceso de borrado de un archivo, consiste en eliminar la ruta de acceso a un determinado sector del disco duro donde están depositados los datos; una vez eliminado el acceso directo, el sistema supone que dicho espacio está disponible para reescritura y hará uso de él cuando lo considere necesario.

Utilidades para rescate especializado de datos como: Data Recovery Software, Easy File Recovery y File Rescue; detienen la escritura en discos duros afectados por pérdidas, reestableciendo los accesos directos a los archivos y ordenando los datos para su posterior examen y selección. Aunque son necesarios tiempo y conocimientos técnicos para su manejo, estos programas son realmente útiles en aquellos casos en los que la pérdida de información no está comprometida por daños físicos en las unidades de almacenamiento y en muchos casos son capaces de recuperar directorios completos, aún después de un formateo total del disco duro.

En la mayoría de los casos no es necesario llegar a utilizar herramientas experimentadas en rescate de datos, ya que los programas que usamos rutinariamente, (entre ellos los pertenecientes a la suite Office, como Word, Excel, PowerPoint, Outlook, OneNote, etc.), incluyen opciones que efectúan respaldos regulares de datos mientras se trabaja, lo más importante es saber dónde buscar y cómo acceder a estos respaldos automáticos que en muchos casos le ayudarán a recobrar un porcentaje importante de su trabajo.

En primer lugar, ubique la carpeta donde el programa en el que trabaja almacena los respaldos temporales; en el caso de las utilidades de Office, puede ver dicha ubicación en la pestaña de >Herramientas, >Opciones, >Ubicación de Archivos, >Archivos de Autorrecuperación. En esa carpeta encontrará los datos que el sistema almacena de manera periódica. Lo invitamos a establecer tiempos convenientes para guardar información de manera automática, para esto vaya hasta la pestaña de >Herramientas, >Opciones, >Guardar, >Guardar Info. de Autorrecuperación cada (1 ó 2) Minutos. Si su computadora es muy lenta, probablemente pierda mucho tiempo almacenando los datos cada minuto, pero recomendamos que como mínimo lo configure a cinco minutos, de esta manera, si se produce una contingencia, perderá apenas una pequeña parte de su trabajo.

Si conoce la extensión o el tipo de archivo que ha perdido, lo más cómodo bajo ambiente Windows es ir a la opción >Inicio, >Buscar; esta opción le permite localizar inmediatamente todos los archivos creados o modificados en el lapso que usted establezca, de un tamaño o tipo específico en las ubicaciones que crea convenientes. Hay tres cosas fundamentales en la búsqueda de datos perdidos: 1) normalmente se encuentran como archivos ocultos, por lo que deberá ir a >Inicio, >Panel de Control, >Opciones de Carpeta, >Ver, >Mostrar Todos los Archivos y Carpetas Ocultos; esta opción le permitirá ver archivos que normalmente no son visibles en el Explorador, 2) Cuando establezca parámetros de búsqueda, incluya opciones avanzadas como >Incluir Archivos Ocultos y de Sistema y >Buscar en Sub-Carpetas; y 3) muchas veces los datos de autorecuperación se guardan con nombres precedidos por símbolos como (&,%,$ ó ~), estas variables le indican al sistema que el espacio ocupado por ese archivo está disponible, en cuanto localice el archivo que busca, renómbrelo inmediatamente y guárdelo

(www.pc-news.com)

Seguridad ante ataques externos (virus, gusanos, hackers, bombas de tiempo)
Controles posibles para cautelar la privacidad

Plan de contingencia

Un Plan de Contingencia define los **procedimientos de resolución y procesos alternativos que se han de acometer en una organización cuando ocurre una disRrupción** por culpa de un desastre o incidente de fuerza mayor (force majeure) **en los procesos de negocio habituales.**

En tal caso (pongamos una inundación o un desplome de un edificio) se realiza una activación del Plan de Contingencia ("paso a contingencia"). En ese momento se lanzan tres

actividades principales, encargadas de coordinar el manejo de la crisis, asegurar la utilización de procesos alternativos que permitan la continuidad del negocio, y resolver el incidente, para restituir la normalidad en los procesos y operaciones.

No hay que olvidar que tan complejo como el paso a contingencia es la vuelta a la normalidad, ya que durante el período transitorio se habrán realizado operaciones que hacen que la vuelta a la normalidad no deba realizarse restituyendo el sistema al punto en que se pasó a contingencia, sino que deberá actualizarse para reflejar los resultados de los procesos alternativos ejecutados durante la crisis. Es lo que se llama "sincronización y restitución".

Es normal encontrar otras definiciones en las que estos términos adquieren otro significado. Aunque muchas veces es solamente una cuestión semántica, es importante estar de acuerdo en lo que se está hablando. Igualmente conviene no olvidar que la definición del Plan de Contingencia sólo es una parte del trabajo. La actualización y prueba del mismo es aún más importante para asegurar la correcta continuidad del negocio.

Un Plan de Actuación ante Incidentes no tiene por qué requerir el paso a contingencia. La mayoría de los incidentes, tanto de seguridad como de otro tipo, tienen un impacto en los procesos corporativos pero no se requiere de la utilización, al menos a nivel global, de procesos alternativos. Los pasos usuales de un Procedimiento para el Tratamiento de Incidentes son la detección del incidente, la clasificación del mismo, las tareas de restitución del servicio (en caso de ser requerido) y de resolución, la documentación de dicha resolución y el cierre del incidente, tras comprobar que la resolución es adecuada. Hay que considerar además en el proceso las tareas de supervisión de la resolución y las posibles situaciones en las que el proceso de decisión se vea alterado (por ejemplo, situaciones de incidentes fuera de horario habitual, en los que los responsables no están localizables).

(www.germinus.com)

Controles y registro de los accesos