



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

**UNA METODOLOGÍA DE AYUDA
PARA AUDITAR TECNOLOGÍAS
DE INFORMACIÓN**

T E S I S

**QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN**

**PRESENTA:
ISABEL FANG MA
LUCIA ADRIANA MÉNDEZ HERNÁNDEZ
ULISES ANDRÉS SANDOVAL HERNÁNDEZ**

**DIRECTOR DE TESIS:
ING.HERIBERTO OLGUÍN ROMO**

MÉXICO, D.F.

2009



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

AGRADECIMIENTOS

A mis padres Rubén y María Elena por darme la posibilidad de estudiar en esta gran casa de conocimientos y brindarme lo necesario para poder realizar mi carrera.

A mi novia y futura esposa Yasmín, por creer en mí y por estar siempre a mi lado dándome fortaleza en momentos difíciles.

Y a todas las personas que me apoyaron en algún momento de mi desarrollo académico les dedico ésta tesis.

ULISES

A mi Papá y Mamá por todo, por su amor, su comprensión, por estar siempre cuando los necesite, y por brindarme la oportunidad de estudiar y seguir apoyándome.

A mis hermanos Carlos y Gaby que son los mejores y me dieron ánimo y apoyo cuando estuve en problemas.

A Miguel Ángel por su paciencia y ayuda en todo momento.

A Karlita por ser la mayor motivación para seguir adelante.

A todos mis amigos y amigas que me apoyaron y vivieron experiencias inolvidables.

A mí querida universidad porque en ella aprendí, conocí, y viví lo mejor.

LUCÍA

Mi más profundo agradecimiento a nuestro equipo por la perseverancia, dedicación y entusiasmo para la terminación de esta tesis: Ing. Heriberto Olgún Romo, Lucía Adriana Méndez Hernández y Ulises Andrés Sandoval Hernández.

Agradezco el apoyo para la revisión y corrección al Ing. Gabriel Alejandro Jaramillo Morales, Ing. Lucila Patricia Arellano Mendoza, Ing. Gabriela Betzabé Lizarraga Ramírez y M.I. Ángel César Govantes Saldivar.

ISABEL

INTRODUCCIÓN

INTRODUCCIÓN

Las tecnologías de información (TI) han tenido un gran auge en las últimas décadas, debido a que las empresas cada vez necesitan de su diversidad y buen funcionamiento para poder ser competentes y estar a la vanguardia del mercado, que cada vez es mayor y requiere que satisfagan sus necesidades.

Para poder estar a dicha altura es necesario que se realice minuciosamente la revisión de las tecnologías de información incluyendo sus procedimientos y controles, que basados en normas, reglamentos y leyes, nos permite tener un óptimo funcionamiento empresarial, para lo cual surge la auditoría a tecnologías de información.

Existen variadas razones para la existencia de la función de Auditoría a Tecnologías de Información (TI), de entre las cuales podemos citar:

1. La información es un recurso clave en la empresa para:
 - ◆ Planear el futuro, controlar el presente y evaluar el pasado.
2. Las operaciones de la empresa dependen cada vez más de las Tecnologías de Información (TI).
3. Los riesgos tienden a aumentar, debido a:
 - ◆ Pérdida de información
 - ◆ Pérdida de activos.
 - ◆ Pérdida de servicios/ventas.
4. Las Tecnologías de Información (TI) representan un costo significativo para la empresa en cuanto a personal y costos tanto del hardware como del software.
5. Las políticas, normas y procedimientos de operación y administración se tornan rutinarias, por lo que ya no se les da importancia y algunas ya no se toman en cuenta.
6. Los problemas se identifican sólo al final.
7. El permanente avance tecnológico.

El lector encontrará como contenido, de esta primera parte, un listado con doce temas, de tecnologías de información que incluyen una descripción general de la misma.

En el primer y segundo capítulo (tecnologías de información y auditoría a tecnologías de información, respectivamente) presentan el punto de partida para poder analizar a cada tecnología de información, y de manera general, se definen conceptos básicos sobre lo que es TI y auditorías a TI.

En el III capítulo, “outsourcing”, se presenta la definición, características, así como también, sus ventajas y desventajas, entre algunos otros puntos de importancia.

En el capítulo IV se presenta lo relacionado a la calidad del software, como lo es, el aseguramiento, control y gestión de la calidad mencionando los aspectos que deben considerarse para poder evaluar con buena calidad al software.

El capítulo V trata la contratación de servicio de outsourcing, mediante el uso de un documento en donde la parte que solicita y la parte que presta el servicio se comprometen a cumplir lo acordado en el contrato, bajo ciertas condiciones y/o limitantes.

Para el capítulo VI lo que se aborda es el qué hacer para prevenir y afrontar situaciones que ponen en riesgo a la institución, principalmente a la información y los recursos humanos; es decir, que cuente con un plan de contingencia que permita afrontar dichas situaciones de manera eficiente.

Dentro del capítulo VII se tratará el tema de comercio electrónico, el cual es parte fundamental para que una empresa pueda extender el mercado de sus bienes y/o servicios que busca comercializar en otros territorios nacionales o extranjeros; y realizado con base a medidas de seguridad y privacidad para el manejo de información de sus clientes.

Como contenido del capítulo VIII se menciona lo relacionado con los almacenes de datos o data warehouses, que son de vital importancia para poder tomar decisiones a nivel gerencial.

Con el fin de facilitar la toma de decisiones dentro de una organización, es necesario el uso de la tecnología, así como también el manejo de estrategias, para poder recolectar, integrar, analizar y presentar los datos, que permitan comprender el funcionamiento de la empresa y anticipar acciones que den como resultado una buena operación al negocio. Todo esto está relacionado con la inteligencia del negocio (Business Intelligence, BI) y se podrá encontrar en el capítulo IX.

Para dar soporte a las tecnologías de información, se necesita de un área especializada, que tenga como finalidad la administración, coordinación y resolución de incidentes, y asegurar que los problemas que se presenten sean resueltos. Dicha área es nombrada Help Desk o mesa de ayuda y se podrá leer en el capítulo X.

El proceso de búsqueda de información valiosa en grandes cantidades de datos, con la finalidad de descubrir patrones, relaciones, asociaciones, etc. y que es de utilidad para la toma de decisiones se expone de manera breve en el capítulo XI, a éste proceso se le llama minería de datos.

Para finalizar, en el capítulo XII, se menciona a grandes rasgos que es un sitio web, y de los factores a tomarse en cuenta cuando se requiere la creación de alguno.

Todos los capítulos, a excepción de los tres primeros, contienen una serie de preguntas o acciones, así como sus respectivas sugerencias y recomendaciones.

Las preguntas o acciones y sugerencias están encaminadas al profesional que revisará cada tecnología de información; es decir, a la función auditora.

Las recomendaciones están dirigidas al cliente o dueño que solicite el servicio de auditoría.

Cabe aclarar que los temas fueron escogidos arbitrariamente y que no solamente existen esas tecnologías de información.

Si se desea información sobre más TI, ésta podrá encontrarse posteriormente en consecutivas partes.

Este trabajo también formara parte de un proyecto cuyo propósito será ayudar a auditores y empresas que soliciten ayuda al realizar auditorías de información, el nombre del proyecto es Sistema de Auditoría Informática y Control de Centros de Tecnología de Información en software libre (SAICOCETI) y podrá ser consultado en línea mediante una página web.

ÍNDICE

Agradecimientos.....	iii
Introducción.....	ix
CAPÍTULO I. TECNOLOGÍAS DE INFORMACIÓN.....	1
1.1. Introducción.....	3
1.2. Definición de tecnología de información (TI).....	4
1.3. El valor de las tecnologías de información.....	4
1.4. Ventajas del uso de las tecnologías de información.....	5
1.4.1. Reducción del tamaño de la organización jerárquica.....	6
1.4.2. Incremento del flujo de información horizontal.....	6
1.4.3. Ventaja competitiva.....	6
1.5. Planeación estratégica de tecnologías de información.....	7
1.6. Control y gobierno de tecnologías de información.....	8
1.7. Optimización del desempeño de tecnologías de información.....	9
1.8. Las tecnologías de información en México.....	10
CAPÍTULO II. AUDITORÍA A TECNOLOGÍAS DE INFORMACIÓN.....	13
2.1. Introducción.....	15
2.2. Auditoría a tecnologías de información.....	17
2.3. Definición de auditoría integral a tecnologías de información.....	17
2.4. Concepto de auditoría de sistemas de información (SI).....	18
2.5. Objetivos generales de una auditoría a tecnologías de información.....	19
2.6. Razones para efectuar una auditoría a tecnologías de información.....	19
2.7. Planeación de la auditoría a tecnologías de información.....	20
2.7.1. Investigación preliminar.....	20
2.8. Tipos de auditoría.....	21
2.9. Líneas de defensa del entorno en tecnologías de información.....	21
2.9.1. Control y control interno en TI.....	21
2.9.2. Auditoría interna a Tecnologías de Información.....	24
2.9.3. Auditoría externa a Tecnologías de Información.....	25
2.10. Perfil del auditor en tecnologías de información.....	26
2.11. El equipo humano.....	26
2.12. Funciones de los auditores de TI.....	26
2.13. Conducta profesional de un auditor en TI.....	27
CAPÍTULO III. OUTSOURCING.....	29
3.1. Introducción.....	31

3.2. Evolución histórica.....	31
3.3. Definición.....	33
3.4. Características.....	34
3.5. Ventajas.....	38
3.5.1. Ventajas operacionales.....	39
3.5.2. Ventajas tecnológicas.....	39
3.5.3. Ventajas financieras.....	40
3.6. Problemática del outsourcing.....	40
3.6.1. Problemas operacionales.....	41
3.6.2. Problemas en el servicio.....	41
3.6.3. Problemas de capacidades.....	42
3.6.4. Problemas de costos.....	42
3.7. Otros conceptos.....	44
3.7.1. Cosourcing.....	44
3.7.2. Out-tasking.....	44
3.7.3. Gestión de sistemas.....	45
3.7.4. Gestión de instalaciones.....	45
3.7.5. Integración de sistemas.....	45
3.7.6. Rightsourcing.....	46
3.7.7. On-site.....	46
3.7.8. Off-site.....	46
3.7.9. Insourcing.....	46
3.7.10. Offshore outsourcing.....	46
3.7.11. Nearshore outsourcing.....	47
3.8. Outsourcing creativo.....	47
3.8.1. La organización enlazada con outsourcing.....	47
3.8.2. Autopreservación con objetividad.....	48
3.8.3. Recursos humanos.....	48
CAPÍTULO IV: AUDITORÍA A LA CALIDAD DEL SOFTWARE.....	49
4.1. Introducción a los conceptos de calidad del software.....	51
4.1.1. Definiciones de calidad del software.....	51
4.1.2. Definición del aseguramiento de calidad del software (Software Quality Assurance).....	51
4.1.3. Definición del control de la calidad del software (software Quality control)	51
4.1.4. Definición de Gestión de la calidad del software (Software Quality Management).....	52
4.1.5. Definición de Sistema de calidad	52
4.2. Estándares y modelos de evaluación y mejora de los procesos de software.....	52

4.2.1. Certificación de la calidad (Quality certification).....	52
4.3. Factores que determinan la calidad del software.....	53
4.3.1. Métricas de la calidad del software.....	54
4.4. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 4.4.PAA-001, 4.4.GSA-001, 4.4.RC-001, hasta 4.4.PAA-024, 4.4.GSA-024, 4.4.RC-024 (C=Capítulo, I=Índice)	54
CAPÍTULO V: AUDITORÍA A CONTRATOS DE OUTSOURCING.....	65
5.1. Introducción.....	67
5.2. Tipos de outsourcing en TI.....	67
5.2.1. Tipo1.....	67
5.2.2. Tipo2.....	68
5.2.3. Tipo 3.....	69
5.2.4. Tipo 4.....	70
5.2.5. Tipo 5.....	71
5.2.6. Tipo 6.....	72
5.3. Tomar la decisión del outsourcing en tecnologías de información.....	73
5.4. Aspectos por considerar en el proceso de contratación del servicio de outsourcing.....	74
5.4.1. Análisis de las necesidades del comprador.....	74
5.4.1.1. Racionalización Financiera.....	75
5.4.1.2. Fortalecimiento de competencias.....	75
5.4.1.3. Captura de valor agregado.....	75
5.4.1.4. Diseño de la estrategia de la organización.....	75
5.5. Objetivo de la auditoría a contratos de outsourcing.....	76
5.6. Servicios del Outsourcing.....	76
5.7. Características de un contrato de Outsourcing.....	77
5.8. Aspectos clave para tomarse en cuenta en los contratos de outsourcing.....	77
5.8.1. Precio.....	77
5.8.2. Seguridad de la información.....	77
5.8.3. Nivel de servicio.....	78
5.8.4. Planes de contingencia.....	78
5.8.5. Disposición.....	78
5.8.6. Planes de pago.....	78
5.8.7. Otros elementos por considerar.....	78
5.8.8. Terminación del contrato.....	79
5.8.9. Confidencialidad.....	79
5.8.10. Rescisión del contrato por incumplimiento del SLA.....	79

5.9.	Factores relevantes en el proceso de contratación.....	79
5.9.1.	Transferencia de activos o recursos.....	80
5.9.2.	Flexibilidad.....	80
5.9.3.	Reversibilidad.....	81
5.9.4.	Experiencia en el entorno.....	81
5.9.5.	Seguridad.....	81
5.9.6.	Inversión continua en tecnología.....	82
5.9.7.	Coincidencia en estrategia tecnológica con la organización.....	82
5.10	Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 5.10.PAA-001, 5.10.GSA-001, 5.10.RC-001, hasta 5.10.PAA-030, 5.10.GSA-030, 5.10.RC-030 (C=Capítulo, I=Inciso)	82
CAPÍTULO VI. AUDITORIA A PROCEDIMIENTOS DE CONTINGENCIA.....		91
6.1.	Introducción.....	93
6.2.	Auditoría a Procedimientos de Contingencia.....	93
6.3.	Requerimientos de un Plan de Contingencias.....	93
6.3.1.	Plan de Reducción de Riesgos (Plan de Seguridad).....	94
6.3.2.	Plan de Recuperación de Desastres.....	94
6.3.3.	Actividades Previas al Desastre.....	95
6.3.4.	Establecimiento del Plan de Acción.....	95
6.3.4.1.	Sistemas de información.....	95
6.3.4.2.	Equipos de cómputo.....	95
6.3.4.3.	Personal.....	95
6.3.5.	Formación de Equipos Operativos.....	96
6.3.6.	Formación de Equipos de Evaluación (auditoría interna de los procedimientos sobre seguridad).....	96
6.3.7.	Actividades durante el Desastre.....	96
6.3.8.	Plan de Emergencias.....	96
6.3.9.	Formación de Equipos.....	97
6.3.10.	Entrenamiento.....	97
6.3.11.	Actividades después del Desastre.....	97
6.3.12.	Evaluación de Daños.....	97
6.3.13.	Priorización de Actividades del Plan de Acción.....	98
6.3.14.	Ejecución de Actividades.....	98
6.3.15.	Evaluación de Resultados.....	98
6.3.16.	Realimentación del Plan de Acción.....	98
6.4.	Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX)	

De 6.4.PAA-001, 6.4.GSA-001, 6.4.RC-001, hasta 6.4.PAA-027, 6.4.GSA-027, 6.4.RC-027 (C=Capítulo, I=Inciso)	99
CAPÍTULO VII. AUDITORÍA AL COMERCIO ELECTRÓNICO	117
7.1. Introducción al comercio electrónico.....	119
7.2. Concepto de uso frecuente del comercio electrónico.....	120
7.3. Obligaciones de información.....	120
7.4. Contenidos.....	121
7.5. Comunicaciones comerciales.....	121
7.6. Contratación electrónica.....	121
7.7. Responsabilidad civil.....	123
7.8. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 7.8.PAA-001, 7.8.GSA-001, 7.8.RC-001, hasta 7.8.PAA-030, 7.8.GSA-030, 7.8.RC-030 (C=Capítulo, I=Inciso).....	125
CAPÍTULO VIII. AUDITORÍA AL DATAWAREHOUSE (DW)	133
8.1. Introducción.....	135
8.2. Concepto de Data Warehouse.....	136
8.3. Características de un Data Warehouse.....	137
8.4. Elaboración de un Data Warehouse.....	139
8.5. Software en un Data Warehouse.....	140
8.6. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 8.6.PAA-001, 8.6.GSA-001, 8.6.RC-001, hasta 8.6.PAA-028, 8.6.GSA-028, 8.6.RC-028 (C=Capítulo, I=Inciso).....	141
CAPÍTULO IX AUDITORÍA A BUSINESS INTELLIGENCE (BI)	151
9.1. ¿Qué es la inteligencia del negocio?.....	153
9.2. Características de las herramientas de la inteligencia del negocio.....	153
9.3. Herramientas de Business Intelligence.....	154
9.3.1. Query y reporting.....	154
9.3.2. Cuadro de mando analítico.....	154
9.3.3. Cuadro de mando integral o estratégico (Balanced Scorecard).....	154
9.3.4. OLAP (on-line analytical processing).....	154
9.3.5. Datamining.....	155
9.4. Algunas soluciones de BI.....	156
9.5. Elementos que intervienen en la toma de decisiones.....	156
9.6. Sistema analítico.....	156
9.7. Funcionalidad de los sistemas analíticos.....	157

9.8. Aplicaciones de los sistemas analíticos.....	157
9.9. ¿Cómo elegir una aplicación BI?.....	158
9.10. ¿Por qué fallan muchos proyectos de Business Intelligence?.....	159
9.11. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 9.11.PAA-001, 9.11.GSA-001, 9.11.RC-001, hasta 9.11.PAA-020, 9.11.GSA-020, 9.11.RC-020 (C=Capítulo, I=Inciso).....	160
CAPÍTULO X AUDITORÍA AL SISTEMA HELP DESK.....	167
10.1. Introducción.....	169
10.2. Mecanismos de reporte.....	170
10.3. Participantes en un Help Desk.....	170
10.4. Funcionamiento ideal de un Help Desk.....	171
10.5. Características del Help Desk.....	171
10.6. Criterios de dimensión de un Help Desk.....	171
10.7. Tecnologías aplicadas en un Help Desk.....	172
10.8. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 10.8.PAA-001, 10.8.GSA-001, 10.8.RC-001, hasta 10.8.PAA-024, 10.8.GSA-024, 10.8.RC-024 (C=Capítulo, I=Inciso).....	173
CAPÍTULO XI AUDITORÍA A MINERÍA DE DATOS.....	185
11.1. Introducción a la minería de datos.....	187
11.2. Aplicaciones de minería de datos.....	187
11.3. Técnicas de minería de datos.....	188
11.4. Algoritmos de Minería de datos.....	188
11.5. Etapas principales del proceso de Minería de datos.....	189
11.6. Extensiones del data mining.....	189
11.6.1. Algunos Software.....	190
11.7. ¿Por qué usar la minería de datos?.....	190
11.8. Conclusiones.....	191
11.9. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 11.9.PAA-001, 11.9.GSA-001, 11.9.RC-001, hasta 11.9.PAA-030, 11.9.GSA-030, 11.9.RC-030 (C=Capítulo, I=Inciso).....	191
CAPÍTULO XII AUDITORÍA A SITIOS WEB.....	201
12.1. Introducción.....	203
12.2. Objetivo de una auditoría a sitios web.....	203
12.3. Planificación del sitio.....	203

12.4. Tipos de promoción.....	203
12.5. Formas de publicación de sitios web.....	204
12.6. Preguntas o acciones para el auditor (CI-PAA-XXX); guía o sugerencias para el auditor (CI-GSA-XXX) y recomendaciones para el cliente (CI-RC-XXX) De 12.6.PAA-001, 12.6.GSA-001, 12.6.RC-001, hasta 12.6.PAA-033, 12.6.GSA-033, 12.6.RC-033 (C=Capítulo, I=Inciso).....	204
Conclusiones.....	221
Glosario.....	225
Bibliografía.....	233

CAPÍTULO

I

TECNOLOGÍAS DE INFORMACIÓN (TI)

CAPÍTULO I

TECNOLOGÍAS DE INFORMACIÓN (TI)¹

1.1. Introducción

La relación angosta que existe entre tecnología e información resulta variada e interesante. La información permite que la tecnología evolucione y la tecnología, por su parte, hace más eficiente el manejo de la información; es decir, optima las formas de su almacenamiento, acceso y transmisión. El primer concepto fundamental que debemos definir es el de dato. Un dato representa un elemento fundamental que sirve de base a un razonamiento o a una investigación². Los datos pueden ser cuantitativos o cualitativos, se utilizan para describir o representar ideas, objetos o eventos del mundo real y generalmente se manifiestan mediante palabras, letras, sonidos o imágenes.

Otro concepto importante es el de información. Muchas personas entienden como información al conjunto de datos ordenados o estructurados. En realidad la información es más que eso. Si consultamos el significado en una enciclopedia veremos que: *información* es la acción y efecto de informar. En este sentido, llama la atención el hecho de que la información no es simplemente un conjunto de datos, sino que implica la acción de darlos a conocer a alguien.

Para que un conjunto de datos se considere como información, estos datos deberán estar organizados, procesados y tener un significado para quien los utilice o posea.

Los datos son uno de los recursos más valiosos de cualquier organización, se pueden considerar como uno de los activos de una empresa o institución. Muchas de las organizaciones valoran más los datos que su propio equipo de cómputo, ya que en caso de pérdida de datos, su recuperación puede resultar imposible. Por ser tan importantes los datos es necesario contar con *tecnologías de información* (TI) que permitan su uso eficiente, con objeto de proporcionar información oportuna, específica, relevante, ordenada y veraz.

Las tecnologías de información, definidas como la convergencia tecnológica entre las telecomunicaciones, los microcontroladores y la computación para el proceso, transmisión y almacenamiento de información en formato digital, ofrecen a las empresas una plataforma a fin de lograr una ventaja competitiva. Gracias a las TI y al procesamiento de datos se puede considerar como información a una extraordinaria cantidad de datos, tales como: texto, cifras, imágenes, voz y vídeo.

Las TI son la sangre vital que nutre a los negocios, que pone en contacto a los empleados para colaborar, compartir información y proporcionar los vínculos necesarios para

¹. **OLGUÍN** Romo Heriberto. Adaptado de Outsourcing en Tecnologías de Información. México. Facultad de ingeniería. UNAM. 1.ª ed. 2007, P.5.

². **SOLÍS** Montes Gustavo Adolfo. Tomado de reingeniería de la auditoría informática. México. Trillas. 2002, P. 17.

establecer una comunicación efectiva con los clientes, socios y proveedores. Las empresas dependen de estas aplicaciones para obtener un acceso fácil y rápido a la información que necesitan con el fin de tomar decisiones fundamentadas y mantener los niveles más altos de satisfacción del cliente.

Podemos ver como las TI han venido a ocupar una parte medular en cualquier corporación que pretende sobresalir en los mercados tan competidos actualmente. Por ello es necesario implementar a las TI no sólo en los procesos de producción o distribución sino en todas las actividades de la empresa.

1.2. Definición de tecnología de información (TI)

Las TI son las metodologías, técnicas y dispositivos utilizados en el manejo y proceso de la información. De forma general, comprenden todas las tecnologías que son usadas para adquirir, almacenar, manipular y transmitir información a diferentes áreas, que al mismo tiempo permiten a la organización mejorar su manejo e integración de las necesidades de procesamiento de información.

Las TI incluyen varios campos como electrónica, comunicaciones, administración e informática. Su estudio proporciona las herramientas necesarias que proveen habilidades para analizar, definir, diseñar, desarrollar, probar, implementar y mantener una solución integrada de TI.

1.3. El valor de las tecnologías de información

En la actualidad las TI están presentes en todas las actividades de la empresa, es decir, en las etapas de entrada, conversión y salida.

En la etapa de entrada, las TI contienen todas las habilidades, procedimientos y técnicas que permiten a las organizaciones manejar con eficiencia las relaciones que existen con los grupos de interés (clientes, proveedores y público en general) y el entorno en el que se desenvuelven.

En la función de recursos humanos, por ejemplo, existen técnicas especializadas, como entrevistas o exámenes psicológicos con el objetivo de seleccionar al personal con el mejor perfil para satisfacer las necesidades de la empresa. Además de que actualmente, gracias a Internet se puede tener acceso a bolsas de trabajo de cualquier parte del mundo.

En el manejo de recursos, existen técnicas de entrega con los proveedores de entrada (como los estándares de intercambio electrónico de datos, Electronic Data Interchange, EDI) que permiten obtener recursos de calidad a un costo menor.

En la etapa de conversión, las TI combinadas con el equipo, técnicas y procedimientos, transforman las entradas en salidas. Una mejor tecnología permite a la organización añadir valor a las entradas para disminuir el consumo, así como el desperdicio de recursos.

En la etapa de salida, las TI facilitan a la empresa ofrecer y distribuir tanto servicios como productos terminados.

Las TI en los procesos de entrada, conversión y salida dan a la compañía una gran ventaja competitiva, ya que pueden sobresalir en el desarrollo, administración del entorno organizacional y crear valor para toda la compañía.

Lo que hace diferente a las TI de otros activos de producción en los que invierten las empresas es que, una inversión significativa en TI puede corresponder a un proyecto estratégico, con efectos a mediano plazo no sólo sobre la cuenta de resultados, sino sobre el propio modelo de negocio en el que se asienta la actividad de la empresa.

También existen determinadas inversiones en TI que las empresas efectúan para evitar incurrir en desventajas. Hay ocasiones en que no se invierte en TI para ganar más sino para evitar pérdidas de competitividad con el resto del sector, por lo que la rentabilidad de la inversión se debe considerar a partir de la valoración de las pérdidas en que incurriría la empresa si practicase una política tecnológica basada en la abstención o el desinterés.

Un valor que aportan las TI es la eficacia. La tecnología contribuye al desarrollo empresarial cuando se convierte en una variable cuantificable; es decir, cuando permite que los procesos de gestión empresariales logren maximizar la rentabilidad de su operación y la minimización de sus gastos operativos, administrativos y productivos.

Las soluciones de TI permiten lograr a las empresas rentabilidad, exactitud y rapidez en la toma de decisiones al interior de su organización, mientras que en el exterior, otorgan una integración real gracias a su capacidad de respuesta ante los requerimientos de sus relaciones con socios tales como: proveedores, clientes, aliados, competidores y prospectos, pues logran una ventaja significativa si no se contara con una solución de TI.

Para que la implementación de nueva tecnología produzca rentabilidad hay que cumplir varios requisitos, por ejemplo, tener un conocimiento profundo de los procesos de la empresa, planificar detalladamente las necesidades de TI e incorporar paulatinamente los sistemas tecnológicos, empezando por los más básicos.

Las TI ayudan a desarrollar productos, servicios, procesos y capacidades que dan a una empresa ventaja estratégica sobre las fuerzas competitivas que enfrenta su industria. La ventaja sobre las fuerzas competitivas se puede obtener al implementar mediante TI: estrategias de costos, de diferenciación del producto y de innovación.

1.4. Ventajas del uso de las tecnologías de información

Las TI se han convertido en una parte medular para cualquier corporación que pretenda sobresalir en los mercados tan competidos actualmente. Para ello es necesario implementarlas no solamente en los procesos de producción o distribución sino en todas las actividades de la empresa.

Las TI pueden soportar actividades rutinarias o procesamiento de transacciones.

Actividades rutinarias como pueden ser: facturación, embarque, pago de nómina y ventas, etc., y procesamiento de transacciones como: cálculo, clasificación, ordenamiento, almacenamiento, recuperación, transmisión y generación de información, las cuales forman parte del nivel operacional de cualquier organización.

La información nos permite optimar todos los procesos internos de nuestra empresa, conocer mejor a nuestra competencia, así como el mercado por el que se compete. En general, podemos interpretar mejor el medio de nuestro negocio, para así detectar nuestras debilidades y potencialidades y lograr una ventaja sobre la competencia.

No olvidemos que las TI son un medio y no un fin, donde siempre habrá un usuario o cliente que necesita la información con un propósito determinado en el menor tiempo posible.

La revolución de las TI ha tenido un profundo efecto en la administración de las organizaciones, mejorando la habilidad del personal directivo para coordinar y controlar las actividades de la organización y ayudándolos en la toma de decisiones. Algunas ventajas del uso de las TI son las siguientes:

1.4.1. Reducción del tamaño de la organización jerárquica

Esto se logra al proveer a los administradores y ejecutivos información de calidad, oportuna y completa, lo cual reduce la necesidad de varios niveles de burocracia y jerarquía administrativa. Los sistemas de información al reducir estos niveles jerárquicos, actúan como dispositivos de control en las actividades de la empresa o negocio. Cabe señalar que los sistemas de información también reducen la necesidad de los administradores de coordinar e integrar las actividades de la empresa, además las TI actualmente pueden coordinar completamente el flujo de producción de una empresa.

1.4.2. Incremento del flujo de información horizontal

El cual es facilitado por el crecimiento de los sistemas cliente-servidor de tres capas, que permiten la conexión de computadoras personales a potentes servidores o minicomputadoras y éstos a su vez enlazados a un mainframe.

1.4.3. Ventaja competitiva

El implementar apropiadas TI puede significar que incremente el potencial competitivo de la empresa o negocio. Actualmente, la búsqueda de competitividad ha aumentado el uso de TI, por ejemplo, al reducir la necesidad de muchas jerarquías, los sistemas de información ayudan a reducir los gastos burocráticos, ya que los directivos se basan en las TI para coordinar y controlar las actividades de la empresa.

Gracias a los canales de comunicación que proveen las TI, podemos tener información clara y oportuna de todos los movimientos del entorno industrial, como son: precios, clientes, impuestos, tipos de cambio, regulaciones, estándares y movimientos de la competencia, lo cual ayuda a los ejecutivos al momento de diseñar estrategias competitivas, aunado a esto, los grandes corporativos pueden mantener un flujo de información constante en todas sus unidades de negocios sin importar la distancia física a la que éstos se encuentren distribuidos.

Las TI pueden ser usadas para mejorar la respuesta de una empresa o negocio hacia los requerimientos de los clientes, lo cual es una fuente muy importante de competitividad, ya que permiten a las compañías crear "productos virtuales", productos que pueden ser personalizados de acuerdo con las necesidades específicas de algún cliente en particular, sin cargos adicionales.

Se propone que los factores de importancia para las aplicaciones de las TI en una organización deben orientarse a:

- ◆ **Objetivo de la organización:** es de gran importancia definir el objetivo de la organización, el cual se establece en la misión.
- ◆ **Beneficios por obtener:** los beneficios esperados a la puesta en marcha del producto final. Con la finalidad de definir claramente la cantidad de recursos y en cuanto tiempo se obtendrán los beneficios del proyecto.
- ◆ **Recursos necesarios:** que se deben tener en cuenta tanto la fuente y el origen del financiamiento del proyecto de TI, lo cual marca la disposición de los recursos que se tendrá durante el proyecto.
- ◆ **Limitación del área de influencia sobre la cual debe tener impacto las TI dentro de la organización:** esto implica qué áreas de la organización modificarán sus procedimientos cotidianos al entrar en función la nueva TI, teniendo en cuenta el impacto que puede resultar en otras áreas de la organización.
- ◆ **Nivel de flexibilidad que se desea:** que las TI sean adaptables a las futuras exigencias que la organización pueda tener en un futuro, esto es, tomar en cuenta el tiempo de vida de la necesidad y que la infraestructura que se invierta pueda continuar aprovechándose en un futuro.

1.5. Planeación estratégica de tecnologías de información

La planeación estratégica consiste en relacionar las metas de una organización, determinar las políticas y programas necesarios para lograr objetivos específicos y establecer los métodos necesarios para asegurar que sean ejecutados. Otros propósitos son:

- ◆ Alinear la estrategia tecnológica con la institución.
- ◆ Crear un marco de arquitectura tecnológica que integre, ordene y dicte el desarrollo en TI, además de brindar servicios en cualquier lugar y en todo momento.
- ◆ Aprovechar sus oportunidades para incrementar la productividad y eficiencia empresarial.
- ◆ Generar una cultura de análisis y evaluación del uso de las TI.
- ◆ Compartir recursos, experiencias y mejores prácticas en su aprovechamiento.

Es necesario analizar las fortalezas, oportunidades, debilidades y amenazas tecnológicas sobre cuestiones de seguridad, conectividad, uso de metodologías, características del personal, criterios de calidad, etc., que junto con los objetivos de la institución y estrategia tecnológica permitirá definir una agenda de proyectos priorizada.

Internet, con su arquitectura multiplataforma y estándares abiertos, ha contribuido al surgimiento de nuevos paradigmas organizacionales y de negocios gracias a su facilidad para implementar comercio electrónico, comunicación, colaboración, mercadotecnia interactiva y alianzas estratégicas. Los nuevos paradigmas implican nuevas formas de relación entre clientes, proveedores, socios comerciales, subcontratistas y competidores que pueden representar para las empresas oportunidades y que facilitan su camino al éxito si son usadas apropiadamente, pero también pueden ser amenazas a su permanencia si no se les da un uso adecuado.

Las TI juegan un papel estratégico en la nueva manera de hacer negocios, sin embargo, la tecnología no es valiosa por sí misma sino por los beneficios que se pueden obtener de su correcta utilización, por lo que no basta con adquirir modernos equipos de cómputo y comunicaciones e implementar sofisticados sistemas de información (SI), sino que se requiere que la plataforma tecnológica de información que soporta los procesos empresariales se genere a partir de un cuidadoso proceso de planeación.

La planeación de TI no debe ser vista como un proceso independiente y aislado, sino como parte fundamental de la planeación estratégica de la empresa, debiendo originarse a partir de la visión empresarial que busca el logro de sus objetivos, y es el primer paso para ofrecer servicios de mejor calidad a un menor costo.

1.6. Control y gobierno de tecnologías de información

Son pocos los que pueden darse el lujo de tolerar fallas en la obtención de resultados relacionados con TI. La necesidad de obtener los beneficios esperados por la organización conduce directamente a los conceptos de control y gobierno de TI. Todas las dependencias que consideren a la competitividad como uno de sus objetivos deberán establecer procedimientos de control y gobierno en TI.

Por *control* se entienden las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para asegurar razonablemente, que los objetivos del negocio serán alcanzados y que los eventos no deseables serán evitados, detectados y corregidos.

Por eso, el control es un elemento de la administración que tiene un alcance muy amplio, y que no interesa únicamente a los auditores, sino a diversos grupos dentro de la organización que persiguen los objetivos para los cuales fue constituida, tal es el caso de: los responsables de diseñar e implementar el control, los usuarios y quienes evalúan su correcto funcionamiento.

El gobierno de TI es un término que abarca los SI, la tecnología y las comunicaciones; los aspectos comerciales, legales y de otra índole; y todos las personas involucrados de alguna forma como son: accionistas, directores, gerencia, administradores de procesos, proveedores, usuarios y auditores, que ayuda a asegurar que los objetivos de TI y de la empresa coincidan realizando los beneficios prometidos.

En 1995 la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association, ISACA) dio a conocer un marco de referencia para

la seguridad y el control de TI, el cual es utilizado por la mayoría de los auditores ya que goza de aceptación general y aporta mayor valor a la alta gerencia de las organizaciones.

De manera general, lo que debe realizar el auditor de TI es:

- ◆ Enfocar su trabajo a los aspectos estratégicos de la empresa u organización, y ser capaz de traducir sus hallazgos y recomendaciones a un lenguaje comprensible para las audiencias que típicamente manejan términos de negocio y no tecnológicos.
- ◆ Orientar su trabajo a apoyar los objetivos de negocio y no únicamente a la cobertura de riesgos.
- ◆ Reemplazar las tradicionales recomendaciones teóricas y ambiguas por propuestas de valor orientadas al negocio.
- ◆ Concebirse y proyectarse como un generador de valor y no como un minimizador de costos.
- ◆ Ser altamente productivo en su desempeño profesional y apoyar la competitividad de la organización.
- ◆ Dedicar parte de sus recursos a la investigación y desarrollo de herramientas de trabajo de alta productividad para dar soporte a todo el ciclo de vida de sus auditorías de manera integrada.
- ◆ Participar en ambientes de colaboración de trabajo, aprovechando las facilidades de las redes de telecomunicación.
- ◆ Contar con procedimientos y tecnologías para la administración del conocimiento y generar inteligencia de negocios de auditoría.
- ◆ Mantenerse actualizado en cuanto a métodos, técnicas y herramientas de trabajo, y procurar el desarrollo de actividades de capacitación profesional continua.

1.7. Optimación del desempeño de tecnologías de información

La *medición del desempeño de TI* es un proceso dinámico. Los sistemas tradicionales de medición pueden dar señales equivocadas a administradores de sistemas, en especial cuando se trata de evaluar información relacionada con la contribución de la tecnología a la misión de la organización. Con frecuencia muchas variables afectan el desempeño de los SI y por eso la medición del desempeño de TI puede ser un requisito establecido en los estatutos de una empresa.

La *optimación del desempeño* es un proceso impulsado por indicadores de efectividad.

Estos indicadores se definen sobre la base de complejidad de las operaciones y procesos de negocios de una organización, su solución estratégica de TI y los objetivos corporativos primarios de su implementación. Esta optimación se refiere al proceso de mejorar la productividad de los SI al máximo nivel posible sin inversión adicional en infraestructura de TI.

Las fases genéricas para obtener el desempeño de TI son:

- ◆ Establecer, actualizar y responsabilizar las medidas de desempeño

- ◆ Recolección y análisis de los datos del desempeño
- ◆ Reporte y uso de la información del desempeño

Las advertencias de la medida del desempeño incluyen:

- ◆ **Error de medición:** Las medidas convencionales no son representativas de los verdaderos datos y resultados.
- ◆ **Retrasos:** Los retrasos de tiempo entre la ejecución de la inversión y el reconocimiento del beneficio no son debidamente reportados en las medidas convencionales.
- ◆ **Redistribución:** Las TI se utilizan para redistribuir la fuente de los costos en las empresas.
- ◆ **Mala administración:** La falta de medidas explícitas del valor de la información lo hacen vulnerable a una asignación equivocada y al consumo excesivo de parte de los gerentes. Como resultado, las técnicas adecuadas de medición del desempeño jugarán un papel cada vez mayor para los directivos y juntas de revisión de inversiones.

Generalmente hay cinco usos de las medidas de desempeño:

1. Medir productos o servicios
2. Administrar productos o servicios
3. Asegurar la responsabilidad
4. Tomar decisiones de presupuesto
5. Optimizar el desempeño

Un sistema efectivo de administración del desempeño debe tener liderazgo, un marco conceptual, una comunicación interna y externa efectiva, responsabilidad por los resultados e inteligencia en la toma de decisiones. También es de gran importancia compartir los resultados y avances con los empleados, clientes y accionistas.

1.8. Las tecnologías de información en México

No hay duda que el ambiente en los negocios a escala mundial está cambiando. Las condiciones económicas y las demandas de la población buscan productos con calidad y a un precio accesible. Las empresas incorporan sistemas para la administración de recursos y el uso de Internet aumenta cada vez más.

Dentro de este medio, difícil para los que se oponen a los cambios, pero prometedor y lleno de oportunidades para quienes están dispuestos a integrarse hacia una dinámica de negocios más activa, la importancia de los sistemas de información y los programas orientados al control de recursos empresariales influyen de manera positiva en el desarrollo de nuevos mercados en el ámbito mundial, principalmente por dos cuestiones: la primera es que la integración de las empresas con proveedores y clientes emplea sistemas de información y para éstos se desarrollan aplicaciones en Internet; la segunda razón es que las empresas han comenzado la integración de sistemas como medida de control interno.

En este contexto, las empresas requieren de herramientas tecnológicas que les ayuden a competir. Sin embargo, actualmente la aplicación de las TI en las empresas presenta dos retos importantes: por un lado, los factores internos de la compañía, donde los costos generados por capacitación y la poca aceptación del personal hacia los cambios en los procesos, representan un severo conflicto para las organizaciones; por otro lado, los factores externos son muy costosos y requieren demasiado tiempo para su implementación. Entre los factores externos podemos mencionar las TI relacionadas a la administración integral de las empresas.

Una implementación exitosa de los sistemas de información en las empresas mexicanas brinda eficiencia, reducción de costos y la capacidad de competir con compañías internacionales; sin embargo, una implementación desarrollada de manera incorrecta representa gastos y provoca un cambio negativo en la filosofía de cómo hacer negocios.

Los proveedores de sistemas de información deben darse cuenta que el desarrollar tecnologías de información más accesibles para las pequeñas y medianas empresas (PyMES) significa un mercado excelente que se podría traducir en millonarias utilidades.

CAPÍTULO

II

AUDITORÍA A TECNOLOGÍAS DE INFORMACIÓN

CAPÍTULO II

AUDITORÍA A TECNOLOGÍAS DE INFORMACIÓN³

2.1. Introducción

Auditoría informática es el nombre que se le dio a la auditoría en tecnologías de información en sus primeros años en México y en otros países latinoamericanos.

En la década de los sesenta, los auditores financieros terminaban enfrentándose con la PC en el seguimiento de sus investigaciones, pero, en grandes empresas donde existía la auditoría informática, el proceso de revisión no incluía la PC y su entorno. Aquella modalidad se le llamó después *auditoría “alrededor de la PC”*, porque el auditor verificaba los documentos que se almacenaban en la PC y los informes producidos, pero no entendía lo que pasaba dentro de la PC, por tanto no podía certificar nada acerca del proceso. En esa época, no se había producido la revolución en las comunicaciones, los procesos eran en su mayoría por lotes y la función del auditor (normalmente, auditor financiero que realizaba funciones de auditor informático) solamente se limitaba a verificar la seguridad física, como por ejemplo, contra incendios, existencia de copias de seguridad, etc.

Tiempo después, los auditores financieros comenzaron a utilizar la PC como medio para acceder a los datos mediante la utilización de paquetes: llamada la fase de *auditoría “a través del ordenador”*.

La tercera fase de esta evolución se le puede nombrar como auditoría “con el ordenador”, ya que utiliza sus posibilidades, utilidades, etc.

Con frecuencia no es fácil de encontrar una definición de la auditoría a tecnologías de información y, lo que es de gravedad, el concepto que tienen muchos auditores financieros, consultores, informáticos y profesionales, en general, no es adecuado y a menudo es confundido con la auditoría de cuentas con ayuda de la computadora, si bien es claro que el objeto a examinar en ese caso son los estados de cuenta, balances, etc., y que la computadora no es más que el medio o la herramienta.

En resumen, auditoría a tecnologías de información es la revisión de la propia tecnología de información y de su entorno, y esto no implica la utilización de la PC (puede tratarse de una auditoría de funciones, de gestión de proyectos, etc.). Algunas de las actividades que puede comprender la auditoría a TI son:

³ **SOLÍS** Montes Gustavo Adolfo. Adaptado de reingeniería de la auditoría informática. México, trillas. 1.ª ed, 2002, p.17,43,47,49,127

MANZANO Villalón José Antonio Calvo. Adaptado de Introducción a la auditoría informática. España, Fundación General de la U. P. M. 1.ª ed, 2002, p 1.1,1.3, 2.33, 4.1, 4.19.

OLGUÍN Romo Heriberto. Adaptado de Dirección, Organización y Administración de Centros de Tecnología de Información. México. Facultad de ingeniería, UNAM. 1.ª ed, 2005, pp. 507-520.

- ◆ **Análisis de riesgos.** Suele ligarse con el concepto de prevención y detección de fraudes informáticos y virus.
- ◆ **Existencia de planes de contingencia.** Un incendio, una inundación o sabotaje que no se hayan previsto pueden paralizar las actividades de una empresa, temporal o definitivamente.
- ◆ **Participación en el desarrollo de aplicaciones** (auditoría preventiva).
- ◆ **Asesoramiento** en la instalación de paquetería de seguridad, así como revisión de parámetros y perfiles de usuario.
- ◆ **Revisión y cumplimiento de controles**, así como de las normas legales aplicables.
- ◆ **Evaluación de la gestión de los recursos informáticos**, así como existencia y cumplimiento de políticas y estándares
- ◆ **Apoyo técnico e informático en auditorías generales** (financieras, de cuentas, etc.).

Otro error, principalmente de los no informáticos, es asociar auditoría a TI con ordenadores personales, confundiendo la herramienta con el objetivo principal de dicha auditoría. Se da el caso de considerar erróneamente como auditoría a TI la que realiza un auditor de cuentas que se ayuda de un ordenador para escribir su informe.

De forma general, la auditoría a tecnologías de información comprende la revisión y la evaluación objetiva (por parte de personas independientes y competentes) del entorno de TI de una empresa, abarcando:

- ◆ **Todas o algunas de sus áreas** (equipos, sistemas operativos y paquetería, aplicaciones y su desarrollo, organización y funciones, comunicaciones, etc.).
- ◆ **Los estándares y procedimientos** en vigor, su idoneidad y cumplimiento.
- ◆ **El grado en el cual los usuarios y directivos están satisfechos.**
- ◆ **Los controles existentes.**
- ◆ **Análisis de riesgos.**

En consecuencia de la revisión y evaluación se emite un informe escrito que resume la situación desde un punto de vista independiente y objetivo, y según los casos, el informe ha de incluir las deficiencias y recomendaciones para mejoras.

2.2. Auditoría a tecnologías de información.

Vale la pena conocer la definición de auditoría en general, ya que ésta hereda muchos de sus preceptos generales a la auditoría a TI.

Se puede entender a la auditoría como:

La disciplina que mediante técnicas y procedimientos aplicados en una organización por personas independientes a la operación de la misma, evalúan el cumplimiento de los objetivos institucionales, emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de cumplimiento de dichos objetivos.

Dependiendo del tipo de auditoría del cual se trate, las definiciones reflejarán sus particularidades correspondientes, alineadas fundamentalmente con los objetivos que cada auditoría pretenda conseguir.

Por ser una especialización (de la auditoría general), la auditoría a TI hereda todas las características de la definición anterior. Se considera que la auditoría a TI es:

La disciplina que mediante técnicas y procedimientos aplicados en una organización por personas independientes a la operación de la misma, evalúa la función de tecnología de información y su aportación al cumplimiento de los objetivos institucionales; emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de cumplimiento de dichos objetivos.

La auditoría a TI debe visualizarse a un nivel de institución, y con mucha amplitud para establecer la relación entre la función de TI y los objetivos de la empresa.

Sin duda, este tipo de auditoría se enfocará de manera específica a los aspectos relacionados a sistemas de información (normalmente con un componente alto de tecnología) pero sin perder de vista su contexto institucional, puesto que le dará los elementos para proporcionar un valor agregado en sus servicios.

2.3. Definición de auditoría integral a tecnologías de información.

La auditoría integral a TI es un proceso objetivo e independiente de evaluación a las TI, orientado al desarrollo organizacional de una empresa, en un entorno de cambio permanente, cuya gestión puede ser llevada a cabo desde la misma empresa, a través de servicio de terceros, o mediante una combinación de ellos. Dicha auditoría se guía por una filosofía de servicio y calidad, que busca dar seguridad al proceso administrativo en su integridad (planificación, organización, dirección y control) en relación con la administración del riesgo para la organización.

El alcance de la auditoría integral a TI es variable y puede aplicarse a toda la organización de la empresa o solamente a algunos de sus procesos o actividades.

La auditoría integral podría fijar su alcance en un período tan extenso que sea de varios años, o tan corto que comprenda sólo algunas semanas.

La auditoría integral exige un equipo integrado por profesionales con una gama amplia de habilidades gerenciales que pueden o no incluir a profesionales con habilidades contables.

2.4. Concepto de auditoría de sistemas de información (SI).

Un sistema es una unidad que funciona en un ambiente y tiene muchas partes que trabajan juntas para lograr una meta común. Las partes mayores del sistema son llamados subsistemas y comparten algunas o todas las características del sistema. Además, las fronteras que separan los sistemas, subsistemas y sus entornos son lógicas, no físicas.

Hablando sobre auditoría a tecnologías de información y siendo los SI una de las aplicaciones más representativas de dicha tecnología, se propone dar la definición de sistemas de información.

Sistema de información es un conjunto de datos, de elementos humanos, de procedimientos de trabajo y de tecnología que en forma coordinada y alineada a una estrategia institucional, proporciona soporte a la operación, a la toma de decisiones y al servicio de los clientes de una empresa.

Como definición de auditoría a SI se tiene como: la disciplina que se encarga de evaluar y comprobar los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software.

La auditoría de los sistemas informáticos tiene como objetivo auditar los sistemas que ya están funcionando y no su desarrollo.

Dentro de cada sistema los tratamientos pueden variar, dependiendo de la parte concreta de que se trate, y del área y procedimientos administrativos que lo soporten.

El auditor puede verificar:

- ◆ La totalidad de la aplicación o una serie de programas, según donde se haya detectado el problema.
- ◆ Los controles que afectan a todas las aplicaciones y verificar si existe un nivel de control suficiente en cada una de las áreas, para garantizar que el entorno en donde se envuelven las aplicaciones es seguro y adecuado.
- ◆ El grado de eficiencia y utilidad de los sistemas, así como la fiabilidad y seguridad de la información que proporcionan.

En conclusión, la finalidad de la auditoría de un sistema de información es evaluar en qué medida se garantiza el control interno con la utilización de esa aplicación, la seguridad de los datos y programas, así como el rendimiento de la misma con relación a la finalidad con la que fue diseñada, en términos de costo-eficiencia.

Por tal motivo es necesario, en primer lugar, llegar a conocer el proceso, detectar los controles existentes y probar su funcionamiento.

2.5. Objetivos generales de una auditoría a tecnologías de información.

El auditor debe comprender exactamente los deseos y pretensiones del cliente, de forma que los objetivos perseguidos sean susceptibles para ser cumplidos. Algunos de los objetivos más comunes de los clientes son:

- ◆ Necesidad de auditar una materia de gran especialización.
- ◆ Contrastar algún informe interno con el resultado de uno externo.
- ◆ Evaluar el funcionamiento de las áreas de TI en un determinado departamento.
- ◆ Aumentos de seguridad y fiabilidad.
- ◆ Aumento de calidad.
- ◆ Disminución de costos.

Una vez determinados los objetivos específicos del cliente, el auditor deberá tener siempre presente los dos objetivos generales y comunes a toda auditoría a TI: la operatividad de los SI y los controles generales de la gestión en TI.

La operatividad de los sistemas se refiere al funcionamiento, aunque sea mínimo, de la organización y sus máquinas (computadoras, mainframes, etc.) La operatividad debe conseguirse tanto a escala general como particular.

Los controles Generales de la gestión en TI consisten en verificar las normas teóricas existentes en el departamento de TI y observar su consistencia con el resto de la empresa.

2.6. Razones para efectuar una auditoría a tecnologías de información.

- ◆ Aumento considerable e injustificado del presupuesto.
- ◆ Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- ◆ Descubrimiento de fraudes efectuados con la computadora.
- ◆ Falta de una planificación informática.
- ◆ Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración.
- ◆ Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados.
- ◆ Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción.

2.7. Planeación de la auditoría a tecnologías de información.

Aunque la planeación se presenta como la primera actividad de la auditoría, en realidad el auditor debió haber recibido previamente un requerimiento para desarrollar el trabajo de auditoría. En este requerimiento se deben especificar los objetivos y condiciones generales del trabajo. Ya obtenida la información, el auditor debe continuar con la obtención de un conocimiento general de la empresa que será auditada, sus características de negocio, su infraestructura tecnológica, sus sistemas de información, sus áreas de riesgo, sus objetivos estratégicos y cualquier asunto de interés específico sobre la auditoría a realizar.

Con dicha información, el auditor debe realizar un trabajo de planeación con el cual determine el tipo de procedimientos de revisión que desee emplear, el personal que será responsable para desarrollar las actividades, así como las fechas y duración del trabajo.

2.7.1. Investigación preliminar.

Dicha investigación consiste en examinar la situación general de las funciones y actividades de la informática. Para esto, es necesario conocer la organización, el entorno de operación y las aplicaciones informáticas (con sus bases de datos y archivos).

1. **Organización.** El equipo de auditores, para poder llevar a cabo su trabajo, necesita conocer cual es la estructura organizativa del departamento de TI a auditar, es decir saber quien ordena, quien diseña y quien ejecuta las diferentes actividades del departamento
2. **Entorno operativo.** El equipo auditor debe tener una adecuada referencia del entorno en el que va a trabajar. Para ello debe determinar:
 - ◆ Situación geográfica de los sistemas.
 - ◆ Arquitectura y configuración de hardware y software.
 - ◆ Inventario de hardware y software
 - ◆ Comunicaciones y redes de comunicación
3. **Aplicaciones informáticas con sus bases de datos y archivos.** La investigación previa termina con una idea general sobre los procesos informáticos realizados en la empresa auditada. Por ello se recomienda conocer:
 - ◆ Volumen, antigüedad y dificultad de las aplicaciones.
 - ◆ Metodología a la hora de desarrollar dichas aplicaciones.
 - ◆ Documentación de las aplicaciones.
 - ◆ Cantidad y complejidad de bases de datos y archivos

2.8. Tipos de auditoría.

Existen muchas formas de clasificar a la auditoría; simplemente al pensar en las áreas de especialización, ésta nos resultaría una clasificación extensa y válida.

Clasificación con base en quien realiza la auditoría

En este sentido, la clasificación presenta dos grupos definidos claramente, *la auditoría externa y la auditoría interna*.

1. **La auditoría externa** es aquella que realiza un auditor o grupo de auditores que son independientes a la empresa auditada y su relación con ésta está limitada con un contrato o convenio de servicios profesionales establecido entre la empresa auditada y su auditor.
2. **La auditoría interna** es aquella que realiza un auditor o grupo de auditores empleados formalmente por una empresa, pero cuyas funciones son ajenas totalmente a la operación de la misma.

Clasificación con base en los objetivos que se persiguen.

1. **La auditoría financiera.** Es realizada con el objetivo primario de emitir una opinión sobre los estados financieros de una organización; en consecuencia, se dirige a la evaluación de aspectos de integridad y veracidad de la información.

Dicha opinión se llama “dictaminación de estados financieros”, y únicamente es válida cuando se emite por auditores externos.

2. **La auditoría administrativa** la cual se dirige a la evaluación de aspectos relacionados con la eficiencia y productividad de las operaciones de una empresa.

Este tipo de auditoría puede ser desempeñada por auditores externos e internos.

3. **La auditoría integral** se realiza con la finalidad de evaluar en su totalidad los objetivos que existen en una organización; es decir, los que se relacionan con información financiera, salvaguarda de activos, eficiencia y normatividad, etc. Este tipo de auditoría puede ser realizada por auditores externos y auditores internos.

Sin embargo, debido a la estrecha relación con la empresa, los auditores internos tienen mejores elementos para efectuar este trabajo de manera más eficiente.

2.9. Líneas de defensa del entorno en tecnologías de información.

Comúnmente se habla de tres líneas de defensa las cuales se muestran en la figura 2.1. Las tres se complementan y suelen ser necesarias

2.9.1. Control y control interno en TI

En la figura 2.1. el primer anillo que rodea al núcleo del entorno de TI es el control.

Un *control* es una actividad o acción, o un grupo de actividades, realizadas por uno o varios elementos, humanos o máquinas, para prevenir, detectar y corregir errores o irregularidades que afecten el funcionamiento de algo.

Es muy difícil saber cuánto control y mediante qué procedimiento es necesario aplicar, para que a la vez que se garantiza una situación razonablemente fiable, no se disparen los costos, no disminuya la productividad ni se caiga en una situación de burocracia. Es necesario encontrar un equilibrio.

Es apropiado evaluar los riesgos derivados de la inexistencia del control y del incumplimiento de los procedimientos relacionados.

Objetivos de control. Son declaraciones sobre el resultado final deseado o del propósito a ser alcanzado mediante la implantación de procedimientos de control.

Sistemas de control interno. Un sistema de control es un conjunto de procesos, funciones, actividades, subsistemas y dispositivos cuya misión, total o parcial, es garantizar que se alcancen los objetivos de control.

Control y auditoría. La implantación de los controles es, en última instancia, una responsabilidad de la dirección, si bien cada directivo en su área es corresponsable de la existencia de controles al nivel determinado.

En informática el control lo realizan los supervisores a los diferentes niveles: jefes de proyecto, jefes de turno y otros.

Los auditores verifican que existan controles adecuados y que sean eficientes.

Fig. 2.1. Líneas de defensa del entorno informático



Antes de introducirse al tema de control interno en TI es conveniente hablar sobre Cobit.

Cobit (Objetivos de control para la información y tecnologías relacionadas) fue desarrollado para representar un estándar a nivel internacional sobre conceptos de control en TI. Como se menciona, Cobit es un conjunto de objetivos de control aplicables a un ambiente de TI que se lograron definir gracias al trabajo de investigación y búsqueda de consenso entre la normatividad de distintos grupos colegiados, estándares técnicos, códigos de conducta, prácticas y requerimientos de industria y requerimientos emergentes para industrias específicas. Este extenso trabajo de investigación realizado por expertos dio como resultado un grupo de objetivos de control estructurados que al ser compatibles con las normas principales a nivel internacional, cuenta con aceptación implícita como un estándar global en términos de control interno en TI.

Control interno en tecnologías de información es el conjunto de elementos de administración que una empresa establece en forma coordinada para que el empleo de sus recursos de tecnología de información apoye en forma efectiva a los objetivos institucionales de la empresa.

Los factores críticos de éxito son los elementos de los cuales depende una empresa para la obtención de sus objetivos como institución. Los objetivos de control buscan apoyar el cumplimiento de dichos factores críticos de éxito desde el punto de vista de tecnología de información.

Los objetivos de control deberán ser evaluados por el auditor para determinar su nivel de cumplimiento y, consecuentemente, su nivel de aportación a los factores críticos de éxito (FCE).

A continuación se definen los objetivos de control en TI que apoyan directamente a los FCE.

1. **Preservar atributos de la información.** Asegurar que la información que se genera y se almacena mediante el empleo de TI conserve los atributos necesarios para ser confiable y útil a la empresa.
2. **Apoyar la protección del patrimonio.** Apoyar las medidas de protección para inversiones y bienes de la empresa utilizando adecuadamente las TI.
3. **Proteger la infraestructura de tecnología.** Proteger toda la infraestructura para preservar su funcionalidad e integridad.
4. **Apoyar la eficiencia operativa.** Utilizar la TI como soporte a la eficiencia de la operación de la compañía.
5. **Emplear los recursos de TI adecuadamente.** Utilizar todos los recursos de TI de manera legal, eficiente, efectiva.

6. **Brindar apoyo competitivo.** Dar soporte tecnológico competitivo a la operación y toma de decisiones de la empresa enfocadas a las políticas establecidas por la administración de la misma.
7. **Mantener una cultura informática adecuada.** Contar con una cultura informática competitiva y acorde con las expectativas derivadas de los objetivos institucionales.
8. **Mantener una cultura organizacional adecuada.**
9. **Habilitar mecanismos de equilibrio.** Utilizar las TI para adecuar el medio y mantener el equilibrio interno de la empresa.
10. **Mantener la continuidad y consistencia del soporte tecnológico.**
11. **Preservar las condiciones de la información.** Mantener la confidencialidad, integridad y disponibilidad de la información de la empresa.

Si un área de TI logra alcanzar los objetivos de control en forma satisfactoria, significará que su “misión” dentro de la empresa probablemente será cumplida.

El alcance satisfactorio de algunos de estos objetivos puede no estar bajo control total de la dirección de TI de una empresa. Las áreas de SI ocupan normalmente posiciones staff en las organizaciones, lo que limita de alguna manera su nivel de autoridad para concretar cambios que afecten a otras áreas de la empresa. Por tal motivo, es necesaria la interacción con otras áreas con suficiente nivel de autoridad y, sin duda, contar con el apoyo de la dirección general para impulsar acciones y asegurar obtener los objetivos de control.

Lo que sí es responsabilidad directa del área de sistemas es establecer los procedimientos de control que permitan las herramientas necesarias para lograr los objetivos.

2.9.2. Auditoría interna a Tecnologías de Información.

Se le llama Auditoría interna a TI cuando dicha actividad se lleva a cabo por empleados de la organización. Los auditores internos están en la capacidad de revisar trabajos ajenos al suyo garantizando la independencia y la objetividad del procedimiento. Ocupan una posición de asesoría y deben presentar sus informes directamente al responsable en las áreas administrativas más altas de la empresa.

Hoy en día la auditoría interna a TI es:

- ◆ Una unidad con atribuciones y facultades para auditar todas las operaciones de las organizaciones.
- ◆ Situada en el organigrama en dependencia directa de la alta dirección.

- ◆ Con la finalidad de asegurar el control interno influyendo en la gestión de las organizaciones.
- ◆ Realizada por personal altamente calificado, con un conocimiento global de las organizaciones y una visión de los problemas gerenciales.
- ◆ Actuando como control de los restantes controles de la empresa.
- ◆ Independiente para la formulación de sus opiniones y recomendaciones.
- ◆ Trabajando con arreglo a la previa y autorizada planificación anual de sus informes y actividades.

El alcance de la auditoría interna debe abarcar el examen y evaluación de la adecuación y efectividad del sistema de control interno y la calidad de la ejecución en la realización de las responsabilidades asignadas.

2.9.3. Auditoría externa a Tecnologías de Información.

La auditoría externa es aquella que se lleva a cabo por profesionales independientes, cuyos servicios son solicitados por una empresa, para analizar lo relacionado con las TI y posteriormente presentar un informe de auditoría que exprese su opinión acerca del adecuado funcionamiento de la misma. Dicho informe no está desviado por las necesidades o deseos de algún grupo o miembro de la organización en particular.

La auditoría externa es una actividad muy antigua, algunas firmas tienen más de 100 años de operaciones. El éxito de este tipo de organizaciones se debe a varios factores, como pueden ser:

Las firmas de auditores independientes, han alcanzado un nivel técnico elevado, acumulando experiencia profesional en diversas industrias y perfeccionando métodos de trabajo eficientes que con dificultad podrían desarrollarse en forma interna por la mayoría de las empresas.

Al ser independientes a las empresas que son auditadas, les da mayor nivel de credibilidad a su opinión profesional, ya que muchas empresas recurren a sus servicios como forma de contar con un aval que sea reconocido por la sociedad y autoridades.

Muchos gobiernos, a través de su legislación tributaria o de los requisitos de participación en bolsa de valores, hacen obligatorio que las empresas utilicen los servicios de auditores independientes para la presentación de estados financieros dictaminados o informes especiales.

2.10. Perfil del auditor en tecnologías de información

De manera general el auditor que se dedique a auditar TI debe tener:

- ◆ Entendimiento de los equipos, incluyendo componentes, y sus capacidades (hardware).
- ◆ Entendimiento de la programación (software), incluyendo sistemas operativos, programas de aplicaciones, paquetes comerciales.
- ◆ Familiarizado con las técnicas de proceso de archivos y estructuras de datos.
- ◆ Conocimiento suficiente del uso de paquetes de auditoría.
- ◆ Habilidad para el análisis de procesos e interpretación de la documentación inherente (programas, definiciones de registros, políticas, procedimientos, estándares, etc.)
- ◆ Conocimiento de los controles de TI:
 - ◆ Identificar y evaluar.
 - ◆ Determinar hasta dónde deben probarse y evaluar los resultados.
- ◆ Entender y conocer los sistemas de información para desarrollar un plan de auditoría y supervisar su ejecución.
- ◆ Familiarizado con la dinámica que encierra el desarrollo y mantenimiento de sistemas de información.

2.11. El equipo humano

Tanto los auditores informáticos internos como externos han de planificar su trabajo de acuerdo al enfoque y profundidad de sus investigaciones. Deben realizar su trabajo de acuerdo con las normas de su entidad, y cuando se trate de un equipo humano han de trabajar como tal y no como una individualidad, sobre todo porque lo que haga cada uno han de entenderlo los demás, previendo sustituciones, enfermedades y continuidad para otras revisiones en épocas sucesivas.

La organización de los equipos y el número de personas dependerá de la experiencia de sus componentes. Podrá haber un gerente por proyecto, dependiendo de éste uno o dos jefes de equipos y a su vez de éstos uno o dos auditores.

Si se integran en el equipo auditores *novatos*, hay que considerar que su aportación inicial no será importante y que al principio más que ayudar se estarán formando.

2.12. Funciones de los auditores de TI

El auditor en TI debe jugar un rol proactivo a través de todas las etapas del proceso de sistematización de la empresa. Adicionalmente debe apoyar a la Auditoría Financiera en su proceso de obtención de evidencia y validación de procedimientos de control.

Las funciones serán las que se determinen en cada entidad, debiendo estar definidas por escrito, las más generales son las siguientes:

- ◆ Realización del trabajo de *campo* mediante:
 - ◆ Entrevistas.
 - ◆ Pruebas y verificaciones.
 - ◆ Análisis de documentación.
 - ◆ Organización y archivo de los “papeles de trabajo”.

- ◆ Propuesta de sugerencias. Por ejemplo: verificaciones complementarias.
- ◆ Propuesta de recomendaciones.
- ◆ Colaboración con los jefes de equipo.

Las actividades típicas de un auditor en TI se clasifican en cuatro grupos:

- ◆ Auditoría de la gestión de los SI y de las TI.

- ◆ Auditoría de los sistemas en desarrollo.

- ◆ Auditoría de los centros de procesos de datos.

- ◆ Apoyo a los demás auditores.

2.13. Conducta profesional de un auditor en TI

El auditor en TI deberá asegurar la adherencia a los códigos aplicables de ética profesional (por ejemplo, Código de Ética Profesional de la Asociación de Auditoría y Control de sistemas de la información (ISACA) y estándares de auditoría de ISACA).

Debe ejercer cuidado profesional en todos los aspectos del trabajo de auditoría, incluyendo la observación de la auditoría aplicable y estándares de TI.

La auditoría es una actividad profesional cuyos compromisos éticos rebasan en muchas ocasiones las obligaciones que tiene con sus clientes directos. Para dar más entendimiento, puede recurrirse a un término en inglés que refleja con mayor fidelidad la magnitud de dicho concepto, el término es *stake holder*.

Stake holder es la persona, grupo de personas o institución que se interesa por el buen funcionamiento de una empresa.

Adicionalmente, una compañía a su concepción como empresa generadora de utilidades o satisfactores para sus dueños, es una entidad que agrupa seres humanos, proporcionándoles empleo y la posibilidad de desarrollo profesional y personal; es una entidad que puede tener impacto económico en una comunidad generando empleos directos e indirectos; que contribuye al gasto público por medio del pago de sus impuestos; es un socio con los proveedores y clientes que establecen relaciones comerciales y puede ser una alternativa para inversionistas que deseen adquirir acciones de la compañía y, en última instancia, representa una serie de recursos asignados a una

administración para que sean utilizados en forma adecuada para alcanzar los objetivos de la empresa.

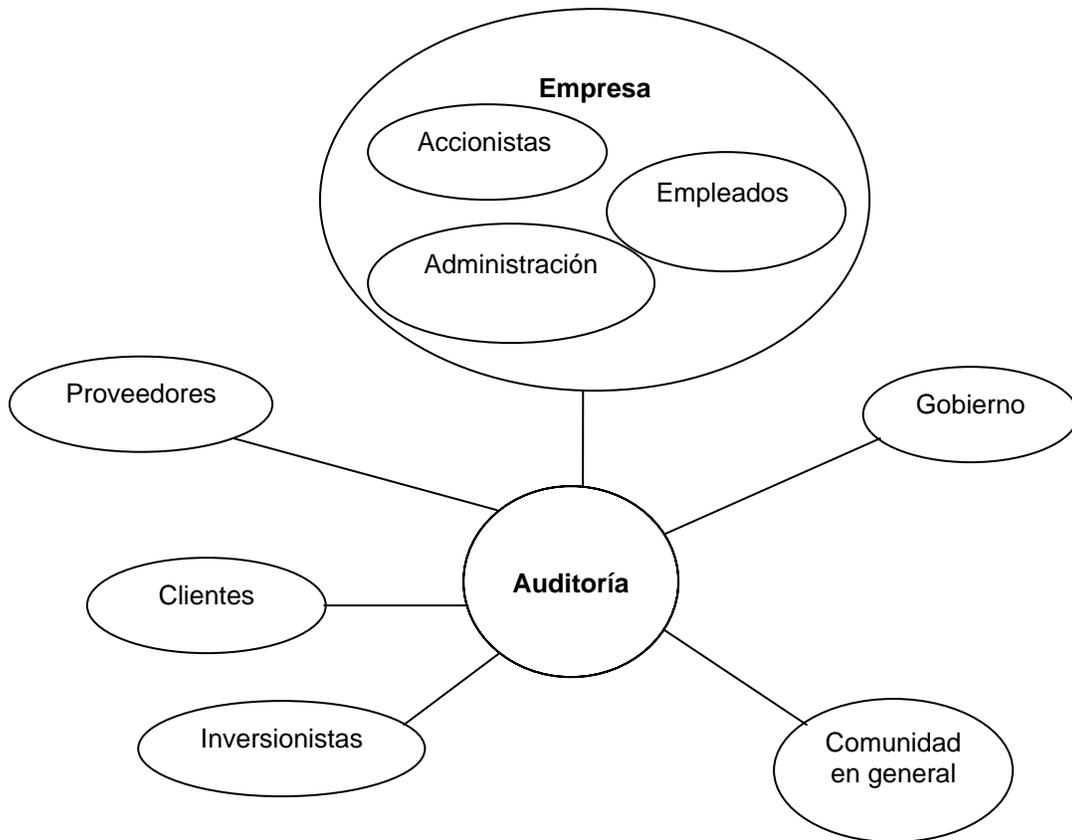


Fig. 2.2. Stake holders

Cada uno de los stake holder, bajo su propia perspectiva, tiene intereses en que la empresa se desempeñe de manera adecuada. La figura 2.2. ejemplifica un modelo en el cual los stake holders se relacionan entre si para poder lograr el bienestar de una empresa.

El informe de un auditor puede utilizarse por cualquiera de estos grupos de interés para tomar decisiones que resulten fundamentales dentro de su contexto de actuación. Por tal motivo, la responsabilidad y compromiso ético de un auditor sobrepasa las obligaciones de un contrato laboral o de prestación de servicios profesionales.

CAPÍTULO

III

OUTSOURCING

CAPÍTULO III

OUTSOURCING⁴

3.1. Introducción

Recientemente el *outsourcing* se ha dado a conocer en el mercado y en nuestro país, está teniendo un gran auge porque nos ha incorporado en el mundo de los negocios.

Esta modalidad se ha hecho cada vez más atractiva para los empresarios, ya que se presenta como una alternativa que les ayuda a mejorar su competitividad al bajar sus costos de operación y maximizar la utilización del capital, gracias a que las empresas ya no se encargan de actividades ajenas al cumplimiento de sus objetivos (“zapatero a tus zapatos”).

El outsourcing es cada vez más la respuesta común a la pregunta “¿producir o adquirir?” que se hacen los empresarios para proporcionar un mejor servicio a los clientes. El outsourcing está creando un ambiente sofisticado, totalmente nuevo, en la correlación proveedor-productor-cliente. A través de esta relación se busca que exista una cooperación intensa entre los tres, por la cual los proveedores adoptan los mismos sistemas que los productores, proporcionando así una mejor relación de trabajo y obteniendo siempre la satisfacción del cliente.

3.2. Evolución histórica

Al iniciar la competencia en los mercados globales las empresas deciden que otros asuman responsabilidades, debido a que su capacidad de servicios no era suficiente para su crecimiento. La necesidad de delegar responsabilidades y compromisos que no son inherentes a la esencia del negocio, han servido para conceptualizar el outsourcing como una visión de los negocios enfocada hacia una estrategia más determinada, en donde los directivos empezaron a darse cuenta de la importancia de una especialización para desarrollar mejor sus funciones.

En un principio, el desarrollo tecnológico se limitó a grandes empresas capaces de costear la implementación del equipo necesario para dicho avance. No obstante, algunas firmas especializadas prestaban el servicio de procesamiento de datos a empresas externas (*service bureau*).

Después de la Segunda Guerra Mundial, las empresas trataron de concentrar en sí mismas la mayor cantidad posible de actividades, para no tener que depender de los proveedores. Sin embargo, esta estrategia que en principio resultara efectiva, fue

⁴ **OLGUÍN** Romo Heriberto. Tomado de Outsourcing en Tecnologías de Información. México, Facultad de ingeniería. UNAM. 1.ª ed. 2007, P.39.

haciéndose obsoleta con el adelanto de la tecnología, ya que nunca los departamentos de una empresa podían mantenerse tan actualizados y competitivos como lo hacían las agencias independientes especializadas.

El concepto de outsourcing comienza a ganar credibilidad en 1970, sobre todo en las áreas de información tecnológica de las empresas. Las primeras en implementar modelos de outsourcing fueron, entre otras: International Business Machines (IBM), Electronic Data Systems (EDS), Arthur Andersen y Price Waterhouse.

En 1990 la tendencia organizacional iba cambiando hacia la reubicación de recursos y servicios que permitían el crecimiento de la parte esencial o principal del negocio. Con esto último, el término outsourcing va tomando fuerza con el desarrollo de tecnologías de información (TI), y es que precisamente con la revolución tecnológica que vivimos, muchas empresas están redefiniendo su negocio que por lo general comprende tecnología.

En 1993 surge The Outsourcing Institute, una red ejecutiva de recursos con la misión de ir evolucionando hasta llegar a ser un foro profesional que dispone información y servicios a compradores, vendedores y observadores del mercado del outsourcing a escala mundial.

A pesar de no ser una práctica común entre las empresas, el outsourcing se ha convertido en una herramienta de competitividad que genera una oportunidad de desarrollo. La crisis económica de 1995 en México constituyó la plataforma de desarrollo para que los servicios externos se llevaran a cabo, dado que para muchas compañías el reducir costos e incrementar la productividad se convirtió en la diferencia entre el éxito y el fracaso.

La progresiva especialización de las TI ha ido provocando un aumento de los conocimientos necesarios para utilizarlas, un mecanismo adecuado para atenuar la falta de éstos, fue la capacitación del personal dentro de las estrategias de las organizaciones. Sin embargo, una de las dificultades principales ha radicado en que las TI están en continua y creciente evolución, por tanto, se ha hecho incuestionable también el proceso de actualización.

En la medida que el volumen de operaciones de una empresa aumenta, aparece la oportunidad de procesarlas en el exterior para hacerlas más flexibles, es allí donde se empieza a dar el verdadero outsourcing. En un entorno globalizado y altamente competitivo como el actual, el outsourcing representa una herramienta que facilita la gestión gerencial para las diversas organizaciones. Es el procedimiento estratégico que permite afrontar los cambios, a fin de ofrecer nuevas ideas para competir mejor, acceder a nuevos mercados, reafirmarse en los ya establecidos y optimar los costos en las funciones internas.

Prácticamente todo se ha podido integrar de manera externa, y las instituciones consideran hacer justo eso en muchas áreas que no son sus ejes principales de negocio (*core business*) además, se han estado integrando las actividades que requieren habilidades especiales. Cada empresa ahora no sólo compite contra sus

semejantes en su propio país, sino también con cualquier otra que desempeñe un servicio similar en el extranjero, por lo que el crecimiento y desarrollo en las TI nos brindan herramientas necesarias para lograr calidad y productividad.

El mensaje es claro, el outsourcing no sólo tiene que ver con la reducción de costos, también puede proporcionar mejoras en el negocio y en servicios de tecnología. Debe ser estudiado como un proceso de largo plazo, en el cual se contratan servicios con la función básica de integrarlos a la empresa, pero sin que esto intervenga en su misión o en sus procesos medulares. Además, al llevar a cabo un proceso de este tipo, la empresa puede ofrecer un valor agregado en términos de una estrategia competitiva de diferenciación que supere las expectativas de los clientes, tales como la aportación de tecnología, la adquisición de una metodología de trabajo, estándares de calidad internacionales, aumento en los beneficios operativos y disposición de un grupo multidisciplinario de especialistas que van a ayudar al logro de sus metas.

3.3. Definición

El término “outsourcing” proviene del neologismo de origen norteamericano que está compuesto por las siguientes palabras: *out* que significa “afuera o externo de”; *source* que representa “recurso o fuente” y, usándose el sufijo *-ing* se sugiere una acción “continua”. El término se puede traducir como “tercerización”, “externalización” o “contratación externa”.

El objetivo principal al incorporar el outsourcing es lograr una mayor productividad. A continuación presentamos las siguientes definiciones formales:

- ◆ Contratación y delegación a largo plazo de uno o más procesos no críticos para nuestro negocio, a un proveedor más especializado, para conseguir una mayor efectividad que permita orientar nuestros mejores esfuerzos para el cumplimiento de una misión.
- ◆ Práctica de adquirir servicios o equipos de TI de un distribuidor externo, lo cual puede incluir tanto personal técnico informático como equipo físico y lógico, de modo que todas o parte de las tareas de carácter informático y de comunicaciones de la organización pasan a ser realizadas por la empresa contratista.
- ◆ Contratación de servicios externos para resolver procesos o funciones necesarias en las empresas, pero no estrictamente relacionadas con el objetivo principal de éstas. Su finalidad no es la de resolver problemas para los cuales hay otras empresas especializadas, sino enfocar la atención en su objetivo principal.

3.4. Características

Existen diferentes características asociadas a las modalidades de outsourcing. Estas características permiten analizar cada uno de los distintos servicios en sus componentes. La tabla 3.1 se refiere a la relación de las características asociadas de servicios de apoyo que decida la empresa con respecto a las modalidades de servicio.

Estas modalidades se basan en relaciones estratégicas con una orientación de mediano a largo plazo y un nivel de riesgo compartido, donde prevalece la confianza y la seguridad mutua.

Tabla 3.1. Matriz de outsourcing. Modalidades de servicio *versus* características asociadas

Características asociadas	Modalidades de servicios				
	Motivos para contratarlo	Reducción de costos	Potenciar recursos internos y tecnológicos	Posicionamiento con visión hacia el futuro	Estrategia futura con proyectos compartidos
Manera de seleccionarlos	Concurso	Negociación	Alianza estratégica	Alianza	Alianza
Método de medición	Por su economía o velocidad en el proceso	Productividad o valor agregado	Retorno esperado y balance presente-futuro	Retorno esperado y balance presente-futuro	Retorno esperado y balance presente-futuro
Orientación y términos	Corto plazo	Mediano y largo plazo	Largo plazo	Largo plazo abierto	Largo plazo abierto
Estructura de la relación	Transaccional	Transaccional y relacional	Relacional	Administrar la relación	Unidad de negocio
Método de costos	Precios más bajos	Análisis en la relación costo-beneficio	Riesgo compartido ganar-ganar	Riesgo compartido ganar-ganar	Riesgo compartido ganar-ganar
Planificación estratégica	Pequeña	Compromiso de recursos	Buena planificación	Alineada con la visión de la empresa	Desarrollo de nuevos negocios
Formalidad de control	Alta y enfocada	Flexible y cooperativa	Por objetivos y logros compartidos	Colaborativo	Medio bajo
Nivel de riesgo	Bajo	Asociación	Alto nivel de confianza mutua	Alto nivel de confianza basada en desempeño	Alto nivel de confianza basada en expansión de oportunidades

Es importante destacar que uno de los primeros pasos en un proyecto de outsourcing, y quizás el más importante, es aquel en donde se seleccionan los procesos que podrían ser contratados. Basándose en su experiencia, las empresas han justificado sus decisiones para adoptar proyectos de outsourcing en áreas generales que consideran las siguientes características:

- ◆ Aquellas que hacen uso más intensivo de recursos.
- ◆ Las que son relativamente independientes.

- ◆ Las que brindan servicios especializados y de apoyo.
- ◆ Las que se caracterizan por patrones de trabajo fluctuantes en carga y rendimiento.
- ◆ Las sujetas a un mercado inestable.
- ◆ Las que poseen una tecnología cambiante que requiere una gran inversión.

De lo anterior deducimos que las siguientes áreas específicas son susceptibles para la aplicación del outsourcing:

En tecnologías de información:

- ◆ Mantenimiento de sistemas
- ◆ Comunicaciones
- ◆ Entrenamiento y capacitación
- ◆ Desarrollo de aplicaciones
- ◆ Consultoría y reingeniería
- ◆ Manejo de centros de datos
- ◆ Gestión de redes
- ◆ Soporte directo a usuarios y servicios *help-desk*
- ◆ Servicio completo de sistemas
- ◆ Internet
- ◆ Correo electrónico

En administración:

- ◆ Impresión y reproducción de formatos
- ◆ Correo y mensajería tradicional
- ◆ Archivos y biblioteca
- ◆ Suministros e inventarios
- ◆ Nómina
- ◆ Compras
- ◆ Contabilidad
- ◆ Impuestos

En servicio a clientes:

- ◆ Visitas y mantenimiento
- ◆ Despacho
- ◆ *Call center*
- ◆ Servicio de información al cliente

En finanzas:

- ◆ Tesorería
- ◆ Manejo y relación de bancos
- ◆ Cobranzas

En recursos humanos:

- ◆ Selección de personal
- ◆ Capacitación
- ◆ Sistema de información

En planta física:

- ◆ Cafetería
- ◆ Mantenimiento de instalaciones (conserjería)
- ◆ Seguridad

En ventas:

- ◆ Mercadeo directo
- ◆ Publicidad
- ◆ Telemercadeo
- ◆ Estudios estadísticos de campo

En distribución:

- ◆ Almacenes
- ◆ Distribución y logística

En transporte:

- ◆ Manejo de flota
- ◆ Distribución de personal
- ◆ Mantenimiento

Cuando se está evaluando la posibilidad de aplicar outsourcing a una función o proceso, lo primero que se debe responder es si el proceso en cuestión es uno de los procesos clave para la empresa (*core processes*).

Por otra parte, se recomienda realizar un examen cuidadoso antes de aplicar outsourcing para los siguientes servicios:

- ◆ Administración de planeación estratégica
- ◆ Administración de finanzas
- ◆ Administración de la consultoría gerencial
- ◆ Control de proveedores
- ◆ Administración ambiental y de calidad
- ◆ La supervisión de la satisfacción de los requisitos reglamentarios del mercado, tales como:
 - ◆ Responsabilidad del producto
 - ◆ Publicidad engañosa

- ◆ Calidad
- ◆ Regulaciones ambientales

El primer paso será identificar si el proceso en cuestión en la empresa es o no core business, una vez identificado el proceso, se deben evaluar los siguientes criterios:

- ◆ ¿Debería invertir en este proceso? Si la respuesta es sí, entonces, la siguiente pregunta es ¿Cómo haré para enriquecerlo?
- ◆ ¿Debo retener este proceso dentro de la empresa?
- ◆ ¿Debería darlo en outsourcing?
- ◆ ¿Sería mejor vender o eliminar este proceso?

La experiencia del prestador del servicio es muy importante, pues las ventajas del negocio están en evitar la curva de aprendizaje y contratación de gente nueva, reducción de costos y gastos, optimar la inversión en actualización tecnológica y potenciar recursos existentes.

Las contrataciones con terceros deben ser muy precisas en cuanto a los resultados esperados, responsabilidades y alcance del trabajo; preferiblemente se debe discriminar cada servicio y sus componentes, preservando la flexibilidad de los contratos en cuanto a los ajustes futuros que deban aplicarse. Además de manera general se presentan las siguientes características.

Relativas al contrato entre las partes:

- ◆ Su elaboración es compleja, puesto que debe establecer claramente las responsabilidades de ambas partes en cualquier aspecto, no sólo del nivel de servicio actual sino también del nivel de servicio futuro.
- ◆ Suele tener una duración de varios años. En el sector privado tiene una duración no menor a cinco o siete años, siendo habitual un período de diez años.
- ◆ Uno de los aspectos más importantes del contrato es la definición de su conclusión, el establecimiento de terminaciones anticipadas al plazo acordado, así como los períodos de preaviso en caso de reversión del servicio.
- ◆ Junto con los conceptos financieros, a lo largo de todo el proceso de evaluación se deben establecer criterios de transferencia de personal.
- ◆ El alcance del contrato podrá ser tan amplio como lo acuerden las partes.
- ◆ El contrato debe ser flexible para que puedan cambiarse los requisitos del servicio y el proveedor pueda cambiar los medios con los que lo proporciona, dado que la tecnología es cambiante.

Relativas a la organización demandante del servicio:

- ◆ Es una decisión estratégica para la organización, puesto que cede el total o parte de sus activos informáticos a la empresa de outsourcing.
- ◆ Permite el acceso a nuevas tecnologías y centrarse en la realización de actividades de mayor valor para la organización (“zapatero a tus zapatos”).

- ◆ Permite a la organización alcanzar un mayor nivel de competitividad sin realizar inversiones en equipamiento tecnológico o en formación del personal informático propio.
- ◆ Transforma a nivel contable los conceptos de costos fijos en costos variables y las inversiones en gastos desapareciendo los activos. Son menores los costos de operación y se evitan las decisiones de invertir en infraestructura.

Relativas a la empresa de outsourcing:

- ◆ Adquiere un compromiso muy importante con la organización que la contrata, puesto que de ella dependerá que se proporcione un adecuado nivel de servicio.
- ◆ El servicio prestado debe ser suficientemente flexible como para adaptarse a cambios de negocio, organizativos o funcionales en la organización, así como al entorno tecnológico.

Es importante tener en cuenta que en el contexto de outsourcing se necesitan de otras habilidades además de motivar, orientar y controlar al personal. Emitir órdenes y delegar a colaboradores dejará de ser lo principal en la función directiva. El liderazgo exige negociar resultados y asignar trabajos hacia afuera, más que hacia abajo. Los directivos de la función informática deberán reunir las siguientes habilidades básicas:

Pensamiento estratégico

Para decidir cómo materializar procesos de outsourcing que mejoren las ventajas competitivas de su unidad de negocios, su equipo de trabajo o su organización.

Negociación

Para lograr simultáneamente en cada proceso de outsourcing dos fines: asegurar los servicios o productos adecuados de los proveedores y lograr la utilización de los mismos por parte de sus gerentes y personal.

Mantenimiento de la relación

Para efectuar un seguimiento óptimo de los procesos y crear relaciones permanentes y sólidas en el tiempo.

Reto a la transición

Para llevar a cabo los cambios que los procesos de outsourcing producen en el personal.

3.5. Ventajas

La adopción de un servicio de outsourcing debe estar cimentada desde el principio en una serie de propósitos y beneficios esperados. Particularmente la alta dirección o la gerencia de TI puede decidir contratar los servicios de outsourcing por varias razones, las más importantes implican las ventajas operacionales, tecnológicas y financieras que se derivarán.

3.5.1. Ventajas operacionales

Las ventajas operacionales del outsourcing transfieren la entrega del servicio de las actividades de TI a un especialista, de tal modo que permita que la gerencia se centre en las actividades base de la organización, lo cual reduce al mínimo los recursos dedicados a las actividades que no son la esencia del negocio, de esta manera se mejora el funcionamiento de la organización.

Dentro de estos beneficios podemos encontrar los siguientes:

- ◆ Mejorar el enfoque de la empresa
- ◆ Aumentar la velocidad de acceso al mercado
- ◆ Fortalecer los procesos de la organización
- ◆ Estimular el desarrollo de la reingeniería
- ◆ Obtener recursos no disponibles internamente
- ◆ Flexibilidad tanto a la organización como a la estructura
- ◆ Acceder a servicios especializados

3.5.2. Ventajas tecnológicas

El outsourcing brinda acceso a tecnología avanzada, lo cual da lugar a distintas técnicas que ayudan a la obtención de las prioridades de la organización siguiendo distintas direcciones, esto puede ser una manera de continuar en el camino de los cambios tecnológicos y acceder a ellos y, con esto, mejorar la calidad de los servicios de TI proporcionados al negocio y a los clientes.

Los departamentos de tecnología de las empresas se enfrentan a un nuevo y crucial reto: abarcar cada vez más ámbitos de actuación con enormes procesos de racionalización y reducción de costos. Se enfrentan a la vez al problema de ser eficientes y productivos, retos extremadamente complejos si no se aplican soluciones imaginativas, aunque a veces sólo sean de sentido común, como es centrarse en el campo que constituye la competencia diferencial de la compañía y confiar el resto de funciones a proveedores externos.

La descentralización de los sistemas de información y la complejidad administrativa resultante, ha hecho aún más atractivas las alianzas profesionales. Redes avanzadas, comercio electrónico, integración de soluciones y migración/evolución de los sistemas existentes, son algunas de las actividades que más se contratan bajo la modalidad de outsourcing de TI.

Hoy en día, los sistemas de información son estratégicos para la mayoría de las organizaciones y las posiciones competitivas dependen de la habilidad para satisfacer la demanda creciente de los clientes con una respuesta inmediata. El outsourcing a mediano y largo plazo es la forma más apropiada de brindar un servicio con una multiplicidad de requerimientos en TI. En estos casos la empresa se preocupa exclusivamente por definir la funcionalidad de las áreas prioritarias de

su organización, dejando que la empresa proveedora de outsourcing se ocupe de decisiones de tipo tecnológico, implementación, administración y operación de la infraestructura tecnológica.

3.5.3. Ventajas financieras

En un mundo cada día más competitivo, complicado y orientado hacia la globalización, las pequeñas, medianas y grandes corporaciones saben que para sobrevivir en un mercado con enormes amenazas, habrá que reconocer con frecuencia las oportunidades existentes en su entorno.

Las ventajas financieras que ofrece el outsourcing son perseguidas a menudo por la gerencia de TI, entre las cuales se pueden mencionar:

- ◆ Tener disponibilidad de fondos de capital
- ◆ Reducir y controlar costos operativos
- ◆ Adquirir nuevos socios de negocios
- ◆ Transparencia y flexibilidad
- ◆ Compartir riesgos
- ◆ Destinar recursos para otros propósitos
- ◆ Presión sobre los márgenes de ganancias

El outsourcing ofrece la posibilidad de disminuir los costos de control. Esto depende de la eficiencia que pudiera ofrecer el proveedor de servicio o también se podrían compartir costos comunes entre los servicios que considera el contrato de outsourcing. Además, se puede reducir el riesgo de la inversión en tecnología incorrecta o limitar notablemente la inversión de capital y obtener así recursos financieros disponibles para actividades más estratégicas.

Para que el lector pueda profundizar en el tema del por qué recurrir al outsourcing, el apéndice A, “Las diez razones principales para que las instituciones o empresas elijan al outsourcing”, contiene información adicional; las primeras cinco razones son tácticas, aspectos a un plazo cercano, y las otras cinco son más estratégicas, beneficios a largo plazo.

3.6. Problemática del outsourcing

Aunque el outsourcing a menudo parece atractivo, puede ocasionar algunos problemas. Un estudio realizado en EE.UU. demostró que en el 60% de los contratos de outsourcing, el cliente resultó beneficiado, mientras que el 36% experimentaron problemas.

A continuación, se describen posibles problemas al utilizar outsourcing. Se recomienda que en el clausulado del contrato se especifiquen las acciones que se deben seguir cuando se presenten.

3.6.1 Problemas operacionales

Entre los problemas operacionales se encuentran amenazas en: la disponibilidad, la integración de los sistemas y recursos, la confidencialidad de la información y la falta de regulación de la conformidad de los sistemas. Además, puede existir una carencia en las cualidades de la información o datos como lo es la confiabilidad, la exactitud y el acceso no autorizado.

Estas situaciones pueden ocasionar graves daños, como la pérdida del negocio, una mala reputación, pérdidas financieras, pleitos, multas y penalizaciones. Las amenazas existen en cualquier ambiente del proceso, pero se incrementan a corto plazo, cuando se introducen los cambios, ya que en un contrato de outsourcing, las operaciones de una organización son realizadas por diversas personas, con diferentes gerencias, usando diversas técnicas y métodos en un ambiente de funcionamiento versátil.

Otra dificultad que se presenta es que una organización no puede, a pesar de sus mejores esfuerzos, identificar que existen los problemas operacionales o el grado de severidad que pueden ocasionar si es que se sospechan. Generalmente, la organización solicita al proveedor de servicio una relación de los tipos de informes que pueden presentarse antes del contrato, los cuales se pedirán mientras se lleve a cabo el outsourcing. Esto en muchos casos será adecuado; sin embargo, en otros, los acuerdos de reportes no anticiparán todas las necesidades que se presenten, además de que no pueden ser suficientes para identificar los problemas a la hora de tomar las acciones correctivas.

3.6.2. Problemas en el servicio

Uno de los problemas en el servicio es que no se resuelvan las expectativas o las necesidades de la organización. El desafío del outsourcing es tender un puente sobre la brecha que pueda existir entre el estándar de servicio que la organización espera y los servicios entregados realmente. Los siguientes puntos son problemas comunes que contribuyen a esta deficiencia:

- ◆ Primero, la organización podría acostumbrarse a un cierto estándar y estilo del funcionamiento que fue proporcionado anteriormente al outsourcing por el departamento de TI, mismo estándar que en ocasiones no se puede seguir ofreciendo. El grado de diferencia puede ser un punto de contención, por lo menos a corto plazo, hasta que ambas partes crecen acostumbradas al nuevo ambiente de funcionamiento.
- ◆ Un segundo problema es que el proveedor de servicio podría no apreciar completamente las prioridades operacionales de la organización u otras expectativas prioritarias. Una vez más éste puede ser un problema a corto plazo

que se resuelve con la evolución del cambio de ambiente o puede ser un síntoma de una carencia de la gerencia.

- ◆ Un tercero y significativo problema es que la empresa outsourcer no puede proveer los estándares definidos en la calidad del funcionamiento, lo que provoca una interrupción en el servicio.
- ◆ Finalmente, el contrato de outsourcing puede no ser suficientemente robusto para implementar y ejecutar los cambios oportunos y rentables que son necesarios para soportar los proyectos y actividades de la empresa.

Muchos factores son la base de estos problemas sin olvidar la posible inhabilidad de la organización para definir sus objetivos y necesidades de outsourcing en las TI o de comunicarlos adecuadamente, también de la inhabilidad del proveedor de servicio de entender esas necesidades y los objetivos, así como los procesos del negocio y los sistemas; de la falta de predeterminar las medidas de funcionamiento, de la no asignación de roles y responsabilidades para supervisar el funcionamiento y la falta de confianza de todas las partes para remediar las deficiencias operacionales.

3.6.3. Problemas de capacidades

En muchos contratos de outsourcing, los activos y el personal de TI son transferidos al proveedor de servicio. Esta acción da lugar a la transferencia del personal capacitado y bien formado, que contribuyó previamente al capital intelectual de la organización. Con el outsourcing una organización puede comprometer, tanto su capacidad de funcionamiento como el control para manejarse con eficiencia en el conocimiento profundo de sus sistemas y operaciones en puntos relevantes.

El outsourcing crea una necesidad de nuevas habilidades de gerencia. Anteriormente la organización tenía el control directo sobre los recursos de TI, ahora con el contrato debe ejecutar el control indirecto a través de una gerencia eficiente.

Las nuevas necesidades de capacidad de la gerencia pueden no estar disponibles dentro de la organización, por lo menos a corto plazo, mientras se implanta una eficiente administración, supervisión y resolución de procesos problemáticos. La carencia de estas capacidades puede comprometer la toma de decisiones sobre los cambios en los servicios de TI, el manejo de las relaciones administrativas o de comunicación con los clientes, los cuales son la base de la organización.

3.6.4. Problemas de costos

La principal razón para transferir procesos a un tercero es el costo. A veces se pierde de vista que al delegar en un proveedor experto alguna área operativa se esperan ciertas economías o mejoras en el servicio, ya que con la excusa de que el proveedor utiliza tecnología muy especializada, en ocasiones se termina pagando

más por el proyecto de outsourcing que lo que costaría hacerlo internamente. De la misma manera, el nivel de servicio que prometió el proveedor puede no cumplirse, o bien, no tiene el impacto esperado en las ventas o utilidades, con lo que solamente se habrán incrementado los costos.

Es importante considerar los siguientes puntos relacionados con problemas de costos:

- ◆ Costos que excedan las expectativas del cliente
- ◆ Costos por terminación de contrato
- ◆ Costos relacionados con disputas y litigios

Costos que excedan las expectativas del cliente

Cuando el outsourcing no se planea adecuadamente, la organización puede incurrir en los costos imprevistos relacionados con la transición y la directiva, los cuales pueden afectar significativamente los beneficios de la decisión del outsourcing. Al pensar en un proyecto de este tipo, debe quedar claro qué parte del negocio se quiere ceder a un tercero, tanto en TI como en personal.

El beneficio esperado debe ser claro y mensurable, la inversión inicial y los precios del servicio deben ser menores al costo interno real. Si lo anterior no se cumple, el objetivo de dedicarse a lo fundamental del negocio no será suficiente para mejorar la economía de la empresa. Investigaciones demuestran que la carencia de la claridad y entendimiento de los costos relacionados con los muchos aspectos del servicio de outsourcing son los problemas más grandes del mismo. La claridad entre la organización y el proveedor con respecto a los servicios que se incluyen en el contrato y cuáles representan adiciones, es muy importante porque a menudo existen diferencias. Los proveedores pueden asumir una carga extra de servicios tal como la organización desee, pero debe ser incluido en el precio base, por ejemplo, la capacitación al personal o soporte a computadoras.

Por último, los servicios, los volúmenes de procesos y la tecnología cambian durante el ciclo de vida de un contrato de outsourcing; estos cambios lo afectan directamente en porcentajes de disponibilidad sobre el nivel de servicio y en última instancia, en la carga de trabajo del proveedor. También podría convertirse en un conflicto significativo la falta de exactitud y justificación de costos, por lo que es importante identificar las consecuencias de cada uno de estos cambios.

Costos por terminación de contrato

Algunas veces las situaciones inesperadas, no dejan otra opción que terminar el contrato. Tal decisión se podría justificar por el cierre de una unidad, por el cambio en la misión o la estrategia de negocio, por falta de calidad en el servicio o por la insolvencia del proveedor de servicio. Terminar

un contrato puede implicar altos costos, particularmente si el contrato no contiene alguna cláusula que considere este punto o la opción de otro proveedor externo. Al terminar con el proveedor de servicio o regresar a una solución interna también implica altos costos. Algunas organizaciones pueden sentirse atrapadas en los contratos de outsourcing y perpetuar malas relaciones para evitar los costos de cambiar o de terminar. Esta encrucijada de situaciones son más probables cuando hay pocos proveedores que compiten para ofrecer estos servicios.

Costos relacionados con disputas y litigios

Una mala relación entre la organización y el proveedor de servicio aumenta el riesgo de conflictos y pleitos, que distraen a la directiva de actividades importantes y pueden implicar altos costos en los litigios jurídicos.

3.7. Otros conceptos

Al outsourcing se le suele confundir o identificar a menudo con conceptos como gestión o integración de sistemas; sin embargo, a continuación se comparan las diferencias que existen entre estos términos.

3.7.1. Cosourcing

Una evolución del outsourcing es el *cosourcing*, el cual pretende que la empresa prestadora del servicio comparta riesgos con aquella que lo contrató. En general, el *cosourcing* designa un proceso que se basa en la colaboración entre recursos internos y externos con vistas a desarrollar y optimar las tareas más sólidas dentro de la empresa. A diferencia del outsourcing que consiste en la contratación de servicios especializados externos, el *cosourcing* utiliza recursos propios y de terceros.

3.7.2. Out-tasking

Es una modalidad de outsourcing enfocado hacia tareas específicas. El *out-tasking* (externalización de tareas) permite a las empresas contratar partes específicas de sus labores sin perder el control ni la propiedad de sus entornos informáticos. Entre las características del *out-tasking* tenemos:

- ◆ Son contratos de escala reducida
- ◆ Se confían menos funciones a la empresa proveedora del servicio

3.7.3. Gestión de sistemas

Es un servicio de gran alcance que se ocupa de integrar, planificar y controlar los aspectos técnicos, humanos, organizativos, comerciales y sociales del proceso completo (desde el análisis y el diseño hasta la operación) del sistema. Los objetivos principales de la gestión de sistemas suelen ser:

- ◆ Planificar y controlar el proceso completo de análisis, diseño y operación del sistema dentro del presupuesto, plazo, calidad y restantes condiciones convenidas.
- ◆ Controlar la validez de los criterios de diseño.
- ◆ Controlar la adecuación del producto del diseño a los requisitos establecidos en el análisis.
- ◆ Planificar y desarrollar las necesidades de mantenimiento y formación del personal que va a operar el sistema.
- ◆ Desarrollar la supervisión del funcionamiento del sistema.

3.7.4. Gestión de instalaciones

Es el servicio que tiene como objetivo realizar las tareas propias de un centro de proceso de datos de una organización, que consiste básicamente en:

- ◆ Operación de sistemas de información
- ◆ Gestión de redes
- ◆ Soporte técnico

Este servicio puede proporcionarse vía remota desde las instalaciones de la empresa contratada o en la organización misma. El concepto de gestión de instalaciones se confunde generalmente con el de outsourcing aunque este último es más amplio y lo engloba.

3.7.5. Integración de sistemas

La *integración* es el proceso a través del cual la organización aprende a introducir criterios y especificaciones en sus procesos y sus sistemas de modo que satisfagan a todos sus usuarios. En este sentido, es necesario mantener de forma sólida y accesible toda la información que se dispone, lo cual permite la unificación y seguimiento de todo el ciclo de relación a través de los sistemas corporativos.

De esta manera, es un servicio que considera el desarrollo y puesta en marcha de las aplicaciones de una organización, cuyo alcance incluye todas las tareas relacionadas con un proyecto de desarrollo de sistemas de información.

3.7.6. Rightsourcing

Se define con el término *rightsourcing* la solución óptima entre los recursos e inversiones propias de la compañía, incluyendo las ventajas que aporta una empresa externa especializada outsourcer.

Como el outsourcing incluye diferentes servicios, la elección óptima posiblemente supondría no adjudicar el contrato a una sola empresa, sino a varias, de modo que cada una efectuase la parte del servicio de forma más efectiva.

3.7.7. On-site

El concepto *on-site* se aplica cuando el servicio de outsourcing se produce en las instalaciones de la organización contratante del mismo. Una de las principales ventajas es el mayor control y la supervisión que se tiene sobre los resultados.

Por otro lado, una desventaja es que la implementación será más lenta, ya que no se tienen todos los recursos disponibles para ejecutarla tan rápido como lo puede hacer una empresa que presta el servicio de outsourcing.

Los resultados no se observarán claramente antes de seis meses, lo cual hace que la operación se vuelva cara, e inclusive hay empresas que en el quinto mes al no ver resultados positivos claudican. También representa una mayor inversión inicial, considerando que para empezar una operación de este tipo se tienen que efectuar gastos, tanto de recursos materiales como humanos, además de los costos que trae la curva de aprendizaje.

3.7.8. Off-site

A diferencia del anterior, el *off-site* se utiliza cuando el servicio de outsourcing se produce en las instalaciones de la propia empresa que presta este servicio.

3.7.9. Insourcing

El término *insourcing* no es más que el uso consciente y planificado del recurso interno que poseen las organizaciones; es decir, es el procesamiento interno ejecutado por el mismo personal, típicamente es lo que sucede en cualquier empresa.

3.7.10. Offshore outsourcing

Se utiliza la expresión *offshore outsourcing* para indicar la externalización de servicios a compañías localizadas en otras regiones.

3.7.11. Nearshore outsourcing

Se emplea *nearshore outsourcing* para señalar que la única diferencia es la afinidad cultural o cercanía geográfica y similitud cultural entre el país proveedor y el país usuario.

3.8. Outsourcing creativo

3.8.1. La organización enlazada con outsourcing

Una institución se ve generalmente como una organización integrada, que directamente tiene y maneja la mayoría (si no es que todas) de sus fuentes requeridas de producción. El crecimiento ha sido considerado siempre como una señal de buena salud, de fortaleza y de éxito. Las empresas que crecen proyectan en los mercados una imagen de dinamismo y vitalidad que les capacita para abordar mejor el futuro.

Por otro lado, cuando el entorno en el que la empresa lleva a cabo su actividad se encuentra inmerso en una fase de desarrollo, el crecimiento de la empresa se convierte en una necesidad, ya que en estas condiciones tiene que crecer por lo menos al mismo ritmo que el mercado para mantener su posición relativa en el mismo.

Para que el crecimiento suponga ventajas importantes a las empresas, éste debe ser sostenido y equilibrado, consiguiéndose a través de una correcta definición e implantación de las estrategias de crecimiento o estrategias de desarrollo.

Conforme las empresas se vuelven más complejas, sus recursos se especializan y se dirigen hacia varias piezas de las operaciones de la organización: diseño de producción, administración, manufactura, recursos humanos, información tecnológica, distribución y ventas, sólo por nombrar algunas. Visto estratégicamente, el outsourcing reta al ejecutivo de hoy en favor de una mejor organización flexible, basada en competencias internas y mutuamente benéficas a largo plazo en el exterior.

Lo que ahora diferencia a las empresas es su capital intelectual, su conocimiento y su experiencia, no el tamaño de los recursos materiales que tienen y manejan.

Como resultado, el outsourcing está siendo adoptado por firmas a través del espectro corporativo. Ninguna empresa es demasiado grande o demasiado pequeña para considerar el outsourcing. Las organizaciones preeminentes están adoptando el outsourcing como piedra angular de sus esfuerzos, y con ello capitalizar oportunidades globales y energizar operaciones.

3.8.2. Autopreservación con objetividad

El reto de los administradores a través del outsourcing es mantener su objetividad mientras se desempeñan con creatividad. El aspecto positivo de esto es que el outsourcing propagará la efectividad del administrador. Las organizaciones que tienen que separarse de cualquier operación, presentan una necesidad real de un administrador principal, el cual deberá conocer el funcionamiento de dicha operación. En la actualidad, el administrador principal necesita reconocer el hecho y educar a sus empleados.

3.8.3. Recursos humanos

Outsourcing es en esencia un proceso que involucra a diferentes personas. La comunicación es indispensable para el éxito del outsourcing. Mucha comunicación conduce a mayor aceptación por los empleados, quienes comúnmente se resisten al cambio cuando desconocen qué es lo que ocurre. Las instituciones necesitan realizar un mejor trabajo de información acerca del proceso de cambio a un anuncio de outsourcing, éste generalmente debe ser precedido con frecuentes boletines.

Un problema en la consideración para adoptar outsourcing es la repercusión que tiene en la cultura organizacional de la empresa, ya que a veces el criterio utilizado no incluye una manera adecuada para medir la eficacia que cada una de las personas aporta a la organización, por lo que la empresa corre el riesgo de deshacerse de personal valioso y crear resentimiento en el personal que se queda.

El outsourcing también puede tener un efecto positivo en las expectativas de los empleados, porque esto les permite más adelante, ajustar sus objetivos con los de la organización. La mayoría de las empresas transnacionales ocupan servicios de outsourcing en recursos humanos o nómina. Son empresas que requieren de un esquema de solución que cumpla con los requerimientos del momento, pero que pueda también soportar las posibles exigencias de un futuro no muy lejano. La tendencia a contratar este tipo de solución en las empresas mexicanas es cada día mayor, ya que además permite no rebasar los presupuestos asignados a sueldos y salarios y obtener óptimos resultados.

CAPÍTULO

IV

AUDITORÍA A LA CALIDAD DEL SOFTWARE

CAPÍTULO IV

AUDITORÍA A LA CALIDAD DEL SOFTWARE

4.1. Introducción a los conceptos de calidad del software

4.1.1. DEFINICIONES DE CALIDAD DEL SOFTWARE:

Según el IEEE:

- ◆ “Grado en el que el software posee una combinación deseada de atributos (nos refiere a las cualidades del software).”
- ◆ “Grado en el que un cliente o usuario percibe que el software satisface sus expectativas (incorpora el aspecto subjetivo de la calidad).”

De manera concreta se sugiere la siguiente:

“Concordancia con los requisitos funcionales y de rendimiento explícitamente establecidos con los estándares de desarrollo documentados y con las características implícitas que se espera de todo software desarrollado profesionalmente.”

4.1.2. DEFINICIÓN DEL ASEGURAMIENTO DE CALIDAD DEL SOFTWARE (SOFTWARE QUALITY ASSURANCE):

“Es el conjunto de actividades planificadas y sistemáticas necesarias para aportar la confianza en que el producto (software) satisfará los requisitos dados de calidad.”

El aseguramiento de calidad del software está presente en:

- ◆ Métodos y herramientas de análisis, diseño, programación y prueba.
- ◆ Inspecciones técnicas formales en todos los pasos del proceso de desarrollo del software.
- ◆ Estrategias de prueba multiescala.
- ◆ Control de la documentación del software y de los cambios realizados.
- ◆ Procedimientos para ajustarse a los estándares (y dejar claro cuando se está fuera de ellos).
- ◆ Mecanismos de medida (métricas).
- ◆ Registro de auditorías y realización de informes.

4.1.3. DEFINICIÓN DEL CONTROL DE LA CALIDAD DEL SOFTWARE (SOFTWARE QUALITY CONTROL):

Son las técnicas y actividades de carácter operativo, utilizadas para satisfacer los requisitos relativos a la calidad, centradas en dos objetivos fundamentales:

- ◆ Mantener bajo control un proceso.
- ◆ Eliminar las causas de los defectos en las diferentes fases del ciclo de vida.

En general son las actividades para evaluar la calidad de los productos desarrollados.

4.1.4. DEFINICIÓN DE GESTIÓN DE LA CALIDAD DEL SOFTWARE (SOFTWARE QUALITY MANAGEMENT):

La gestión de la calidad se aplica normalmente a nivel de empresa, pero puede haber una gestión de calidad dentro de la gestión de cada proyecto.

Según la ISO 9000 la gestión de la calidad del software es:

“Conjunto de actividades de la función general de la dirección que determina la calidad, los objetivos y las responsabilidades y se implanta por medios tales como la planificación de la calidad, el control de la calidad, el aseguramiento (garantía) de la calidad y la mejora de la calidad, en el marco del sistema de calidad.”

4.1.5. DEFINICIÓN DE SISTEMA DE CALIDAD:

El sistema de calidad está compuesto de una estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de calidad.

Un sistema de calidad consta de varias partes:

- 1) Documentación
- 2) Parte física: locales, herramientas, computadoras, etc.
- 3) Aspectos humanos:
 - ◆ Formación de personal
 - ◆ Creación y coordinación de equipos de trabajo

4.2. Estándares y modelos de evaluación y mejora de los procesos de software

4.2.1. CERTIFICACIÓN DE LA CALIDAD (QUALITY CERTIFICATION)

Un sistema de certificación de calidad permite una valoración independiente que debe demostrar que la organización es capaz de desarrollar productos y servicios de calidad.

Los pilares básicos de la certificación de calidad son tres:

- ◆ Una metodología adecuada.
- ◆ Un medio de valoración de la metodología.

- ◆ La metodología utilizada y el medio de valoración de la metodología deben estar reconocidos ampliamente por la industria.

Normativas relacionadas a la certificación de la calidad:

- ◆ ISO 9000: Gestión y aseguramiento de calidad (conceptos y directrices generales).
- ◆ Recomendaciones externas para aseguramiento de la calidad (ISO 9001, ISO 9002, ISO 9003).
- ◆ Recomendaciones internas para aseguramiento de la calidad (ISO 9004).
- ◆ Software Engineering Institute (SEI) Capability Maturity Model (CMM) for software.

4.3. Factores que determinan la calidad del software

- ◆ Recursos humanos con una especialización concreta.
- ◆ Infraestructuras: equipamiento e instalaciones.
- ◆ Formación: conocimiento de nuevas tecnologías.
- ◆ Metodología: organización y secuenciación de los trabajos.
- ◆ Arquitectura: plataforma y lenguaje que se utilizará para el software.
- ◆ Gestión: planificación y seguimiento del negocio.

La calidad del software se clasifica en tres grupos:

1) Operaciones del producto (Características operativas)

- ◆ Corrección
- ◆ Fiabilidad
- ◆ Eficiencia
- ◆ Integridad
- ◆ Facilidad de uso

2) Revisión del producto (Capacidad para soportar cambios)

- ◆ Facilidad de mantenimiento
- ◆ Flexibilidad
- ◆ Facilidad de prueba

3) Transición del producto (Adaptabilidad a nuevos entornos)

- ◆ Portabilidad
- ◆ Reusabilidad
- ◆ Interoperabilidad

4.3.1. MÉTRICAS DE LA CALIDAD DEL SOFTWARE

Desarrollar medidas directas de los factores de calidad del software es difícil y en algunos casos imposible.

Cada factor de calidad F_c se puede obtener como combinación de una o varias métricas:

$$F_c = c_1 * m_1 + c_2 * m_2 + \dots + c_n * m_n$$

c_i Factor de ponderación de la métrica i , que dependerá de cada aplicación específica

m_i Métrica i

Habitualmente se califica de 0 a 10 en las métricas y en los factores de calidad.

Métricas para determinar los factores de calidad:

- ◆ Facilidad de auditoría
- ◆ Exactitud
- ◆ Normalización de las comunicaciones
- ◆ Completitud
- ◆ Concisión
- ◆ Consistencia
- ◆ Estandarización de los datos
- ◆ Tolerancia de errores
- ◆ Eficiencia de la ejecución
- ◆ Facilidad de expansión
- ◆ Generalidad
- ◆ Independencia del hardware
- ◆ Instrumentación
- ◆ Modularidad
- ◆ Facilidad de operación
- ◆ Seguridad
- ◆ Autodocumentación
- ◆ Simplicidad
- ◆ Independencia del sistema software
- ◆ Facilidad de traza
- ◆ Formación

4.4. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

- 4.4.PAA-001.** Pedir las especificaciones que el cliente solicitó para el desarrollo del software y el plan de proyecto en respuesta a las especificaciones.
¿Existen inconsistencias entre los requisitos, el plan de proyectos y los elementos de trabajo?

4.4.GSA-001.

- ◆ Verificar la existencia de políticas de calidad, como directrices y objetivos generales de la organización, relativos a la calidad.
- ◆ Verificar la existencia del manual de calidad, un documento que establece e implementa el sistema de calidad.
- ◆ Verificar que el plan de proyecto sea conforme a las especificaciones que el cliente solicitó y a las políticas de calidad.

4.4.RC-001.

- ◆ Que las soluciones sean mantenibles, adaptables a problemas similares y evolucionales.
- ◆ Que tengan un plazo y costo limitado.
- ◆ Que esté certificado.
- ◆ Que se presente un proceso definido y una mejora continua.
- ◆ Que aumente el rendimiento y la capacidad de negocio.

4.4.PAA-002.

¿Cómo se asegura la calidad del software? ¿Existe algún plan para el proyecto de software?

4.4.GSA-002.

- ◆ Verificar la existencia de actividades de verificación y validación del software a lo largo del ciclo de vida.
- ◆ Verificar la existencia de métricas de software para el control del proyecto.

4.4.RC-002.

- ◆ El documento del plan de proyecto es la base para monitorizar las actividades, comunicar el estado y tomar acciones correctivas. El progreso se determina comparando los actuales elementos de trabajo: tareas, horas realizadas, costo y calendario actual, con los estimados en el plan de proyecto. Una apropiada visibilidad nos permitirá tomar acciones correctivas antes de que el trabajo real se desvíe mucho del plan.
- ◆ Para lograr la calidad de un producto hay que combinar la calidad de los recursos con la calidad del proceso.
- ◆ El aseguramiento de calidad del software se diseña para cada aplicación antes de comenzar a desarrollarla y no después. Se deberán realizar pruebas que incluyen los procesos de revisión e inspección, como la gestión de la configuración del software.

- ◆ La norma ISO/IEC9126-1 (2001) ofrece una clasificación de las características de calidad del producto en externas, internas y de uso.

4.4.PAA-003. ¿Se está cumpliendo el plan? ¿Se están haciendo las actividades tal y como se especificaron?

4.4.GSA-003. Revisar el plan de proyecto y los informes de seguimiento, los informes de pruebas, los productos de las revisiones y las auditorías, cómo son los informes de no conformidades o el proceso seguido para las auditorías.

También deberá existir un comunicado que indique que se tienen que seguir los procesos que se van a detallar en el plan de proyecto, firmado por un responsable de alto nivel o, si se tienen los procesos organizativos definidos, en ellos ya figurará la política correspondiente.

En relación con la revisión del estado del proyecto deberán estar incluidas todas las actividades desarrolladas, por lo tanto se estarán revisando actividades de varias áreas a la vez.

4.4.RC-003. Es fundamental para conseguir la implantación de las prácticas, una planificación cuidadosa, un seguimiento continuo para evitar desviaciones respecto a los procesos establecidos y la existencia de una persona o grupo que ayude a resolver dudas sobre los procesos.

4.4.PAA-004. ¿La gente que desarrolla el software conoce su rol y sus responsabilidades?

4.4.GSA-004.

- ◆ Analice la competencia de cada integrante del personal de desarrollo de software.
- ◆ Verifique que cada integrante del equipo de desarrollo cuente con un manual de las funciones que componen el personal.
- ◆ Verifique si existen programas de capacitación para el personal.

4.4.RC-004. Cada rol deberá estar definido por un manual en el que se especifica el objetivo, responsabilidad en todo el ciclo de desarrollo y la forma en que se puede evaluar su trabajo.

Los roles que se proponen son: líder del equipo, gestor de desarrollo, gestor de planificación, gestor de calidad y proceso, y gestor de apoyo.

El equipo que desempeña el desarrollo de su software, deberá tener las siguientes características:

- ◆ *Competente*: La persona debe tener los estudios adecuados para desempeñar el rol que le fue asignado en el equipo de desarrollo.
- ◆ *Capacitado*: La persona debe tener el entrenamiento en el uso de cierta metodología, proceso, herramienta, lenguaje, etc., necesario para el desarrollo del proyecto en el cual trabaja.
- ◆ *Con experiencia*: La persona debe tener el conocimiento práctico acumulado por su desempeño.
- ◆ *Colaborador*: La persona debe tener la disposición para compartir y cooperar conocimiento en función de un objetivo común del equipo. Realizar las tareas en tiempo y forma.

4.4.PAA-005. ¿Existe alguna metodología para el desarrollo del software?

4.4.GSA-005. Analizar si las actividades que realiza el personal siguen la misma práctica para otros productos.

4.4.RC-005. Para controlar las variables de alcance y de calidad del producto, se propone la revisión de las siguientes 5 áreas e implementar acciones correctivas:

- ◆ **Gestión de requisitos y documentación** es el área en donde las actividades están relacionadas con la recaudación, documentación, validación y control de cambios de los requisitos expresados por el cliente o usuario con respecto a lo que se espera del producto de software.
- ◆ **Diseño y documentación** es el área que provee medios para la verificación del diseño con respecto a los requisitos especificados y realiza las modificaciones.
- ◆ **Planificación y realización de actividades de verificación y validación** es el área que realiza las revisiones, inspecciones y pruebas (test) en función de los objetivos de calidad especificados para el proyecto.
- ◆ **Gestión de configuración de software** es el área que identifica los elementos que conforman el producto, lleva el control de sus versiones y cambios, así como responsabilizarse por su disponibilidad y resguardo.

4.4.PAA-006. ¿Cada nuevo proyecto cuenta con una planificación?

4.4.GSA-006. Determinar la forma en que se realizó la planificación: basada en medidas o basada en opiniones.

4.4.RC-006. Para desarrollar un proceso definido se considera la previsión de tiempo, de costos y de la calidad adecuada, por lo que se necesitan las siguientes medidas de un repositorio de experiencias por cada proyecto anterior:

- ◆ El tamaño funcional resultado de la fase de análisis o la medida del tamaño del código fuente.
- ◆ El número de defectos detectados durante la fase de pruebas.
- ◆ El esfuerzo realizado para desarrollar los requisitos medidos.

Con estas medidas se obtienen las métricas de productividad y tasa de defectos, por lo tanto se estima la cantidad de recursos necesarios.

4.4.PAA-007. ¿El producto cuenta con las cualidades para lograr una certificación de calidad?

4.4.GSA-007. Analizar las materias primas y la forma de elaborar el producto con respecto al nivel de calidad demandado, de acuerdo con su **funcionamiento** (que lo haga siempre, no aleatoriamente o bajo ciertas condiciones difíciles de cumplir y no prefijadas), **funcionalidad** (funcionalidades que dice tener, por las que lo hemos adquirido) y **usabilidad** (el uso de las funcionalidades que permita hacerlos de una forma natural o que se puedan aprender de una forma reglada).

4.4.RC-007.

- ◆ Ver las exigencias de los modelos de calidad de procesos y determine cual satisface los objetivos de la empresa. Los modelos de calidad más conocidos son:
 - ◆ Capability Maturity Model Integration (CMMI)
 - ◆ Capability Maturity Model (SW-CMM)
 - ◆ ISO-15504 (SPICE Software Process Improvement and Capability Determination)
- ◆ La calidad debe estar presente en todo el proceso de desarrollo.
- ◆ No debe de haber demasiados roles para una organización pequeña ni demasiados cambios para una organización grande.

4.4.PAA-008. ¿Cuenta con una forma para determinar la calidad del software?

4.4.GSA-008. Verifique que los parámetros, indicadores o criterios de medición estén definidos.

4.4.RC-008. El software debe poseer determinados índices medibles que son las bases para la calidad, el control y el perfeccionamiento de la productividad.
Una vez seleccionados los índices de calidad, se debe establecer el proceso de control que requiere los siguientes pasos:

- ◆ Definir el software que va a ser controlado: clasificación por tipo, esfera de aplicación, complejidad, etc., de acuerdo con los estándares establecidos para el desarrollo del software.
- ◆ Seleccionar una medida que pueda ser aplicada al objeto de control. Para cada clase de software es necesario definir los indicadores y sus magnitudes.
- ◆ Crear o determinar los métodos de valoración de los indicadores: métodos manuales como cuestionarios o encuestas estándares para la medición de criterios periciales y herramientas automatizadas para medir los criterios de cálculo.
- ◆ Definir las regulaciones organizativas para realizar el control: quiénes participan en el control de la calidad, cuándo se realiza, qué documentos deben ser revisados y elaborados, etc.

4.4.PAA-009. ¿Los objetivos de calidad de la empresa concuerdan con su sistema de calidad?

4.4.GSA-009.

- ◆ Analizar la concordancia entre el software diseñado y los requisitos.
- ◆ Verificar el seguimiento de un estándar o metodología en el proceso de desarrollo de software.
- ◆ Detectar si se tienen en cuenta los requisitos implícitos (no expresados por los usuarios).

4.4.RC-009. La dirección de la empresa es la responsable de fijar la política de calidad y las decisiones relativas a iniciar, desarrollar, implantar y actualizar el sistema de calidad, por lo que debe estar sustentada sobre tres principios básicos: tecnológico, administrativo y ergonómico.

El principio tecnológico define las técnicas a utilizar en el proceso de desarrollo del *software*.

El principio administrativo contempla las funciones de planificación y control del desarrollo del *software*, así como la organización del ambiente o centro de ingeniería de *software*.

El principio ergonómico define la interfaz entre el usuario y el ambiente automatizado.

La adopción de una buena política contribuye en gran medida a lograr la calidad del *software*, pero no la asegura y para el aseguramiento de la calidad es necesario su control o evaluación.

- 4.4.PAA-010.** ¿En el desarrollo del sistema de calidad se tienen contempladas las áreas a las que se les debe dar mayor enfoque?
- 4.4.GSA-010.** Verifique que se haya hecho un análisis de costos, que la información de los procesos que planeó la organización sea en tiempo real y flexible, que la información sea centralizada y que los resultados sean visibles de acuerdo con el objetivo, por ejemplo que las transacciones sean rápidas.
- 4.4.RC-010.** La comunicación, el acuerdo y el compromiso entre los diferentes departamentos relacionados, son de suma importancia para tener bien establecido el proceso, las entradas y salidas. Para evitar conflictos y lograr la colaboración en la integración de las partes del software.

OPERACIONES DEL PRODUCTO (CARACTERÍSTICAS OPERATIVAS)

- 4.4.PAA-011.** ¿El software hace lo que se le pide?
- 4.4.GSA-011.** Analice el grado en que la aplicación satisface sus especificaciones y consigue los objetivos encomendados por el cliente.
- 4.4.RC-011.** Los requisitos del software son susceptibles de cambios, no sólo después de la entrega del producto sino también durante el proceso de desarrollo, por lo que es necesario que los requisitos y especificaciones elaborados durante el proyecto estén adecuadamente definidos.
- 4.4.PAA-012.** ¿Lo que hace el software es de forma fiable todo el tiempo?
- 4.4.GSA-012.** Evalúe el grado que se puede esperar de una aplicación para que lleve a cabo las operaciones especificadas y con la precisión requerida.
- 4.4.RC-012.** Siempre ocurrirán casos que no se contemplen en las especificaciones, sin embargo es necesario asegurar que si tal caso surgiese, el sistema no causará eventos catastróficos; deberá producir mensajes de error apropiados, terminar su ejecución limpiamente en lo posible.

- 4.4.PAA-013.** ¿Son adecuados los recursos de hardware y software para que la aplicación funcione?
- 4.4.GSA-013.** Evalúe la cantidad de recursos hardware y software que necesita una aplicación para realizar las operaciones con los tiempos de respuesta adecuados.
- 4.4.RC-013.** La preocupación por la eficiencia (capacidad de un sistema software para exigir la menor cantidad posible de recursos) debe considerarse con otros objetivos tales como la extensibilidad (facilidad de adaptar los productos de software a los cambios) y la reutilización (capacidad de los elementos de software para la construcción de aplicaciones diferentes), debido a la potencia creciente del hardware de las computadoras que nos permite tener una actitud más relajada.
- 4.4.PAA-014.** ¿La aplicación tiene controles y restricciones en su uso?
- 4.4.GSA-014.** Evalúe el grado con que puede controlarse el acceso al software o a los datos por el personal no autorizado.
- 4.4.RC-014.** Los sistemas de software deben tener la capacidad de proteger sus diversos componentes (programas, datos, etc.) contra modificaciones y accesos no autorizados. Son cualidades que los usuarios buscan en los sistemas de software y encargan para su desarrollo.
- 4.4.PAA-015.** ¿La aplicación se maneja de manera sencilla?
- 4.4.GSA-015.** Evalúe el esfuerzo requerido para aprender el manejo de una aplicación, trabajar con ella, introducir datos y conseguir resultados.
- 4.4.RC-015.** Este requisito plantea uno de los mayores retos de los diseñadores de software preocupados por la facilidad de uso; cómo proporcionar explicaciones y guías detalladas a los usuarios novatos sin fastidiar a los usuarios expertos que quieren ir directo al grano.
- Una de las claves de la facilidad de uso es la simplicidad estructural. Un sistema bien diseñado, construido de acuerdo con una estructura clara y bien pensada, tiende a ser más fácil de aprender y usar que uno confuso.
- Los buenos diseñadores de interfaces siguen una política prudente.
- Hacen las menos suposiciones posibles sobre los usuarios.

REVISIÓN DEL PRODUCTO (CAPACIDAD PARA SOPORTAR CAMBIOS)

- 4.4.PAA-016.** ¿Está el software suficientemente documentado para que una persona ajena al desarrollo pero calificada y autorizada sepa lo que tiene que modificar?
- 4.4.GSA-016.** Evalúe el esfuerzo requerido para realizar cambios en la aplicación y conseguir resultados.
- 4.4.RC-016.** La reducción del tiempo de desarrollo se produce porque es mucho más fácil construir software sobre software estable que sobre software que no es estable. Hoy en día todos los procesos de desarrollo de software son en mayor o menor medida iterativos e incrementables.
- 4.4.PAA-017.** ¿Existe alguna base de datos, como una bitácora sobre las pruebas en la aplicación? ¿Se tienen herramientas para controlar y documentar cada una de las incidencias encontradas para reportarlas a programación?
- 4.4.GSA-017.** Verifique que haya un registro de pruebas y cambios hechos en la aplicación, así como el responsable de ellos.
- 4.4.RC-017.** La detección de errores procura una reducción de costos, producido por un adecuado proceso de desarrollo. Los errores, de cualquier índole, son más costosos cuanto más tarde se descubren, además estos costos se incrementan siguiendo una función exponencial.
- 4.4.PAA-018.** ¿La aplicación puede detectar fallas y excepciones? ¿Es sencilla la forma de localizar las fallas?
- 4.4.GSA-018.**
- ◆ Analizar el diseño de arquitectura del programa.
 - ◆ Verificar la existencia de herramientas instaladas para el seguimiento y control de errores.
 - ◆ Realice pruebas de que los errores detectados realmente se hayan corregido.
- 4.4.RC-018.** Se recomienda tener el control del software mediante la disminución del nivel de fragilidad. Es decir, el programa debe funcionar correctamente después de haber corregido el error y no descomponerse en alguna parte de manera inesperada.
- La fragilidad es la tendencia que tiene el software a romperse por muchos sitios cada vez que se cambia algo. Muchas de las rupturas ocurren en sitios que no están relacionados conceptualmente con el área que se está cambiando.

- 4.4.PAA-019.** ¿La aplicación presenta opciones para modificarla, mejorarla o ampliarla?
- 4.4.GSA-019.** Verificar que los cambios o mejoras que se realicen en un módulo de código no sea dependiente a la modificación de otros módulos.
- 4.4.RC-019.** Cada cambio que se produzca no debe ser una cascada de cambios en otros módulos, debido a que incrementa el tiempo para terminar el cambio. Como consecuencia de lo anterior el gestor se negará a realizar modificaciones en la aplicación. Lo que representa un diseño ineficiente y acaba siendo una mala política de gestión.
- 4.4.PAA-020.** ¿La aplicación permite la prueba de las opciones?
- 4.4.GSA-020.** Evalúe el esfuerzo requerido para probar una aplicación de forma que cumpla con lo especificado en los requisitos.
- 4.4.RC-020.** Durante las fases de validación y operación deben existir procedimientos de aceptación, especialmente datos de prueba y procedimientos para detectar fallos y localizar errores.

TRANSICIÓN DEL PRODUCTO (ADAPTABILIDAD A NUEVOS ENTORNOS)

- 4.4.PAA-021.** ¿La aplicación puede usarse en otro equipo o sistema operativo?
- 4.4.GSA-021.** Realice pruebas de la aplicación en otros sistemas operativos y equipos y determine el esfuerzo requerido para utilizarlo.
- 4.4.RC-021.** La portabilidad es un asunto primordial para los que usan el software, debido a que muchas de las incompatibilidades existentes entre las plataformas son injustificadas.
- 4.4.PAA-022.** ¿La aplicación puede comunicarse con otras aplicaciones o sistemas informáticos?
- 4.4.GSA-022.** Analizar los objetivos iniciales del proyecto y determinar si el diseño es el adecuado.
- 4.4.RC-022.** Los requisitos del programa van cambiando, por lo que se debe realizar un diseño que soporte modificaciones sin que éste pierda su consistencia.

PRÁCTICAS HABITUALES

- 4.4.PAA-023.** ¿Cuál es el criterio que se toma para decidir el cambio de la versión de la aplicación?

- 4.4.GSA-023.** Con base en las especificaciones del cliente, el estudio de caso y el análisis de beneficios, se establecen las especificaciones para la nueva versión, creando un conjunto detallado de requisitos funcionales y de negocios.
- 4.4.RC-023.** Mediante un sistema de control de versiones se mantiene la historia de los cambios y modificaciones que se han realizado sobre ellos a lo largo del tiempo, por lo tanto permite examinar el histórico de cambios o recuperar versiones anteriores de la aplicación, incluso aunque haya sido borrado.
- 4.4.PAA-024.** ¿A qué tipos de pruebas fue sometida la aplicación antes de liberarlo al mercado?
- 4.4.GSA-024.** Verifique los tipos de pruebas que fueron usados:
- ◆ Pruebas unitarias
 - ◆ Pruebas funcionales
 - ◆ Pruebas de Integración
 - ◆ Pruebas de validación
 - ◆ Pruebas de sistema
 - ◆ Caja blanca (sistemas)
 - ◆ Caja negra (sistemas)
 - ◆ Pruebas de aceptación
 - ◆ Pruebas de regresión
 - ◆ Pruebas de carga
 - ◆ Pruebas de prestaciones
 - ◆ Pruebas de recorrido
 - ◆ Pruebas de mutación
- 4.4.RC-024.** El proceso de prueba es clave a la hora de detectar errores o fallas. Conceptos como estabilidad, escalabilidad, eficiencia y seguridad se relacionan con la calidad de un producto bien desarrollado.

CAPÍTULO

V

AUDITORÍA A CONTRATOS DE OUTSOURCING

CAPÍTULO V

AUDITORÍA A CONTRATOS DE OUTSOURCING

5.1. Introducción

La traducción al español del neologismo inglés *outsourcing* viene a ser “la externalización de determinadas áreas funcionales (no sólo las informáticas)”. Por tanto, aplicado con carácter general, no es un concepto nuevo, puesto que responde al acto mediante el cual una organización contrata a un tercero para que realice un trabajo en el que está especializado, con el objeto de reducir costos y evitar a la organización la adquisición de una infraestructura propia que le permita la correcta ejecución del trabajo.

El *outsourcing* o “tercerización” en el caso de Tecnologías de Información (TI) se entiende como la cesión, a una empresa externa, de la gestión de los *sistemas de información* (SI) de una organización. Por las especiales características de este tipo de servicios, su contratación dentro de la administración pública reviste una doble dificultad:

1. La complejidad de definir claramente el objeto, plazo y precio del contrato.
2. Adaptar las peculiaridades del outsourcing al marco legal de los contratos del Estado.

5.2. Tipos de outsourcing en TI⁵

Por el grado de compromiso que existe entre el cliente y el proveedor de outsourcing, se pueden establecer seis tipos de outsourcing de TI.

5.2.1. TIPO 1:

Se refiere a la contratación del outsourcer para que éste se encargue de la selección e implementación de la tecnología que se va a utilizar, al concluir esta etapa el área interna de la empresa continuará operando la tecnología.

Una de las ventajas al contratarlo es su conocimiento de los productos existentes, así como la experiencia en la implementación de la nueva tecnología.

Los supuestos en que se basa este tipo de servicio son:

- ◆ Se considera la implementación de un proceso, para una razón social. No se consideran adecuaciones a módulos de factor humano o desarrollo de otros módulos.

⁵ **OLGUÍN** Romo Heriberto. Tomado de Outsourcing en Tecnologías de Información. México. Facultad de ingeniería. UNAM. 1.ª ed. 2007, P.63.

- ◆ La implementación de aplicaciones se llevará a cabo con soporte del propietario del software.
- ◆ Las modificaciones a los programas fuente serán responsabilidad del propietario del software.

Los recursos típicos que involucran un proyecto de esta naturaleza son:

- ◆ Líder de proyecto
- ◆ Ingeniero de sistemas
- ◆ Administrador de base de datos
- ◆ Especialista en infraestructura

Las actividades típicas del outsourcing tipo 1 que se realizan son las siguientes:

- ◆ Entendimiento del proceso
- ◆ Definir y evaluar objetivos del proyecto
- ◆ Identificar la lista de software a evaluar
- ◆ Conducir demos de productos
- ◆ Diseño de solución
- ◆ Diseño de infraestructura
- ◆ Recomendar productos
- ◆ Apoyo en la adquisición de la tecnología
- ◆ Capacitación de personal
- ◆ Instalación de la tecnología
- ◆ Etapa de análisis
- ◆ Mapeo de procesos
- ◆ Adecuación de ambiente de desarrollo
- ◆ Parametrización
- ◆ Migración
- ◆ Pruebas integrales
- ◆ Capacitación de usuarios
- ◆ Ajustes
- ◆ Liberación a producción
- ◆ Inicio de operaciones

5.2.2. TIPO 2:

El *outsourcing tipo 2* incluye las características del tipo 1; es decir, la empresa de outsourcing contratada además de apoyar en la implementación de la nueva tecnología, continuará realizando soporte técnico y mantenimiento a las aplicaciones y asegurará el funcionamiento del proceso.

Una de las ventajas de este tipo de outsourcing, es que el manejo de la tecnología estará asegurado, ya que se deposita la responsabilidad de ésta a un proveedor.

Los supuestos en que se basa este servicio son los siguientes:

- ◆ Los procesos siguen siendo responsabilidad de la empresa.
- ◆ El proveedor garantiza la funcionalidad del sistema.
- ◆ La operación se da con el equipo y en las instalaciones de la empresa.
- ◆ El servidor donde radica la aplicación y las bases de datos estarán en las instalaciones del cliente.
- ◆ El proveedor tiene la responsabilidad de administrar el hardware y el software.
- ◆ El proveedor será responsable de la conectividad de usuarios al servidor de producción utilizando la red interna de la empresa. Los gastos de conectividad correrán por cuenta del cliente.

Los recursos típicos que involucran un proyecto de esta naturaleza son:

- ◆ Líder de proyecto
- ◆ Ingeniero de sistemas
- ◆ Administrador de base de datos
- ◆ Especialista en infraestructura
- ◆ Operador

Las actividades típicas del outsourcing tipo 2 que se realizan son las siguientes:

- ◆ Garantizar la funcionalidad y desempeño de las aplicaciones y del equipo por utilizar.
- ◆ Recibir requerimientos para nuevos desarrollos, parametrización o actualización de conceptos, definición de reportes y desarrollo de interfaces.
- ◆ Otorgar permisos a usuarios y capacitarlos.

5.2.3. TIPO 3:

El *outsourcing tipo 3* incluye las características del tipo 2; es decir, la empresa de outsourcing contratada además de apoyar en la implementación de la nueva tecnología, provee soporte técnico, mantenimiento a las aplicaciones, asegura su funcionamiento y proporciona especialistas para que operen la tecnología utilizada.

Una de las ventajas del tipo 3 es que, además de asegurar el manejo de las TI, se tendrá un operador/analista especializado, de manera centralizada, que asegure el buen uso de las TI.

Los supuestos en que se basa este tipo de servicio son:

- ◆ Los procesos siguen siendo responsabilidad del cliente.
- ◆ El proveedor garantiza la funcionalidad del sistema.
- ◆ La operación es responsabilidad del cliente. A petición del cliente, el proveedor podría suministrar los equipos.

- ◆ El servidor donde radica la aplicación y las bases de datos estará en las instalaciones del proveedor.
- ◆ El proveedor tiene la responsabilidad de administrar el hardware y el software.
- ◆ El proveedor será responsable de la operación de las TI y de la capacitación de los usuarios. Los gastos de capacitación correrán por cuenta del cliente.

Las actividades típicas del outsourcing tipo 3 que se pueden efectuar son las siguientes:

- ◆ Garantizar la funcionalidad y desempeño de las aplicaciones y del equipo por utilizar.
- ◆ Recibir requerimientos para nuevos desarrollos, parametrización o actualización de conceptos, definición de reportes y desarrollo de interfaces.
- ◆ Otorgar permisos a usuarios, vigilar el desempeño de las aplicaciones, capacitar a usuarios, administrar y dar soporte a los procesos.

Los recursos típicos que involucran un proyecto de esta naturaleza son:

- ◆ Líder de proyecto
- ◆ Analista de proyecto
- ◆ Ingeniero de sistemas
- ◆ Administrador de base de datos
- ◆ Especialista en infraestructura
- ◆ Operador
- ◆ Mensajero

5.2.4. TIPO 4:

En el *outsourcing tipo 4*, la empresa de outsourcing contratada implementa el sistema, da soporte técnico y mantenimiento a la aplicación y asegura el funcionamiento del proceso.

La principal ventaja del tipo 4 es que el outsourcer, al realizar las funciones en sus instalaciones, podrá aprovechar los recursos que ya se tengan para atender a otros clientes, lo cual da como resultado mayor competitividad que si el cliente realiza estos procesos por sí mismo.

Los supuestos en que se basan este tipo de servicio se enlistan a continuación:

- ◆ El proceso de captura es responsabilidad del cliente. El proveedor recibe información y genera el servicio por el cual fue contratado.
- ◆ El servicio será validado por el cliente. El cliente revisa, modifica y entera las obligaciones.
- ◆ El proveedor garantiza la funcionalidad del sistema.
- ◆ El equipo para el proceso estará en las instalaciones del proveedor.

- ◆ El proveedor tiene la responsabilidad de administrar el hardware y el software.
- ◆ El proveedor será responsable del uso que se le dé a los datos.

Las actividades típicas del outsourcing tipo 4 que se pueden ejecutar son las siguientes:

- ◆ Garantizar la funcionalidad y desempeño de las aplicaciones y del equipo por utilizar.
- ◆ Recibir requerimientos para nuevos desarrollos, parametrización o actualización de conceptos, definición de reportes y desarrollo de interfaces.
- ◆ Operar los procesos necesarios en sus propias instalaciones.
- ◆ Responsabilidad y manejo de datos confidenciales.

Los recursos humanos típicos que involucran este tipo de outsourcing son los siguientes:

- ◆ Gerente de proyecto
- ◆ Líder de proyecto
- ◆ Supervisor
- ◆ Analista
- ◆ Ingeniero de sistemas
- ◆ Administrador de base de datos
- ◆ Especialista en infraestructura
- ◆ Operador
- ◆ Mensajero

5.2.5. TIPO 5:

En el *outsourcing tipo 5*, la empresa de outsourcing contratada implementa, da soporte técnico y mantenimiento a las aplicaciones, asegura el funcionamiento de las TI y realiza el manejo de información de gran importancia para el cliente.

La principal ventaja del tipo 5 es que se incrementa el grado de responsabilidad para la empresa de outsourcing debido al tipo de información que maneja, puesto que él es responsable de generar la información que va a ser procesada, de igual manera se encarga de la validación de su propio trabajo, entregando al cliente únicamente resultados.

Los supuestos son los siguientes:

- ◆ El proveedor recibe y maneja información del cliente.
- ◆ El proveedor genera el proceso de obligaciones que serán validadas por el cliente. El cliente revisa, modifica y entera las obligaciones.
- ◆ El proveedor garantiza la funcionalidad de las TI.

- ◆ El proceso se lleva a cabo en las instalaciones del proveedor.
- ◆ El proveedor tiene la responsabilidad de administrar el software y el hardware.
- ◆ El proveedor será responsable del mal uso que se le dé a la información.

Las actividades típicas del outsourcing tipo 5 que se realizan son las siguientes:

- ◆ Garantizar la funcionalidad y desempeño de las aplicaciones de TI.
- ◆ Recibir requerimientos para nuevos desarrollos, parametrización o actualización de conceptos, definición de reportes y desarrollo de interfaces.
- ◆ Operar las TI en sus propias instalaciones.
- ◆ Manejo de información de gran importancia para el cliente, lo cual da como resultado una gran responsabilidad.

Algunos de los recursos humanos típicos que involucran un proyecto de esta naturaleza son:

- ◆ Gerente de proyecto
- ◆ Líder de proyecto
- ◆ Supervisor
- ◆ Analista
- ◆ Ingeniero de sistemas
- ◆ Administrador de base de datos
- ◆ Especialista en infraestructura
- ◆ Operador
- ◆ Mensajero

5.2.6. TIPO 6:

En el *outsourcing tipo 6*, el proveedor implementa, da soporte técnico y mantenimiento a la aplicación de TI y asegura su funcionamiento, realiza la recepción física de incidencias y se responsabiliza de los procesos que se lleven a cabo en las instalaciones de la empresa.

Por último, el tipo 6, además de presentar las ventajas de los tipos anteriores, también incluye personal que dará la cara en las instalaciones del cliente.

Los supuestos son:

- ◆ Los procesos que se realicen son responsabilidad del proveedor.
- ◆ Las incidencias podrán ser en papel o medio magnético entregadas en un solo sitio.
- ◆ El proveedor genera el proceso de obligaciones, las valida y las entrega al cliente para su autorización.
- ◆ El proveedor tiene la responsabilidad de la administración del hardware y del software y de garantizar la funcionalidad de las TI.

- ◆ La operación de las aplicaciones se puede dar en las instalaciones del cliente o en las instalaciones del proveedor.
- ◆ El servidor donde radica la aplicación y las bases de datos estará en las instalaciones del proveedor.
- ◆ El proveedor será responsable del enlace y conexión para la transferencia de datos.

Las actividades típicas del outsourcing tipo 6 que se efectuarán serán las siguientes:

- ◆ Garantizar la funcionalidad y desempeño de las aplicaciones de TI.
- ◆ Recibir requerimientos para nuevos desarrollos, parametrización o actualización de conceptos, definición de reportes y desarrollo de interfaces.
- ◆ Operar las TI en sus propias instalaciones o en las del cliente.
- ◆ Manejo total de la información que se necesita para la aplicación del outsourcing de TI en el área requerida, lo cual implica una gran responsabilidad.

Los recursos humanos típicos que involucran un proyecto de esta naturaleza son:

- ◆ Gerente de proyecto
- ◆ Líder de proyecto
- ◆ Supervisor
- ◆ Analista
- ◆ Capturista de datos
- ◆ Ingeniero de sistemas
- ◆ Administrador de base de datos
- ◆ Especialista en infraestructura
- ◆ Operador
- ◆ Mensajero

5.3 Tomar la decisión del outsourcing en tecnologías de información⁶

La disyuntiva entre adquirir, desarrollar o dar en outsourcing las TI depende, en gran medida, de una serie de consideraciones que rodean el ámbito de la informática y que ayudan a la formación de criterios para la toma de decisiones al momento de seleccionar una alternativa, por lo que no existe una respuesta única y se pueden combinar entre ellas de acuerdo con las necesidades del cliente.

La solución debe basarse en varios factores como la madurez de la organización, estabilidad o flexibilidad del problema de negocios, las demandas del mercado incluyendo sus ventajas competitivas, el conocimiento de las TI que la empresa pueda tener y el factor económico.

⁶ **OLGUÍN** Romo Heriberto. Tomado de Outsourcing en Tecnologías de Información. México. Facultad de ingeniería. UNAM. 1.ª ed. 2007, P.70.

La madurez de la organización se refiere a conocer el nivel de estructura y estandarización de la empresa, uso de mejores prácticas en los diferentes procesos y la disposición a tomar riesgos, ya que cualquier decisión adoptada impactará en las distintas áreas del negocio.

La flexibilidad del problema se entiende como la variación de los requerimientos, la volatilidad de la plataforma tecnológica y sistemas operativos bajo los que opera la empresa (esto se refiere a cómo se logrará la integración de las aplicaciones con las que ya se cuenta y la adaptación con las unidades de negocio).

Otra consideración importante es el tiempo de entrega del producto, ya que durante el proceso de desarrollo del mercado se pueden dar cambios en los requerimientos, los cuales deberán adaptarse para que el producto sea competitivo. La organización también deberá contar con el conocimiento necesario sobre las TI requeridas, así como entender el negocio y las necesidades de los usuarios a fin de poder evaluar a los posibles proveedores.

Por otro lado, la empresa debe encomendar la decisión a un equipo que cuente con los conocimientos técnicos de TI, para determinar cuál es el producto más adecuado para su negocio, que conozca la oferta de los proveedores y que haga un análisis detallado de los costos, comparando los de compra contra los de desarrollo a mediano y largo plazo y la aplicación del outsourcing, tomando en cuenta para todos ellos costos ocultos que un proyecto de esta naturaleza conlleva y, por último, el costo total de propiedad.

5.4. Aspectos por considerar en el proceso de contratación del servicio ⁷ de outsourcing

En primer lugar, se realiza un análisis de las necesidades del comprador, a continuación se recogen los factores relevantes a tener en cuenta en el proceso de contratación y, finalmente, se describe cómo deben ser planteadas las especificaciones técnico-funcionales para la elaboración del pliego de prescripciones técnicas, qué normas, estándares y cláusulas tipo pueden ser de aplicación, y cuál es el cuestionario técnico diseñado para normalizar las ofertas y facilitar su evaluación.

5.4.1. Análisis de las necesidades del comprador

Es sumamente importante, en cualquier contrato de outsourcing, examinar los objetivos pretendidos. Se pueden considerar cuatro aspectos dentro de los cuales el outsourcing tendría un papel estratégico para la organización y por ello se explican a continuación:

⁷ **OLGUÍN** Romo Heriberto. Tomado de Outsourcing en Tecnologías de Información. México. Facultad de ingeniería. UNAM. 1.ª ed. 2007, P.101.

5.4.1.1. Racionalización financiera

Reducción de costos en la liberalización de capital para su reinversión en áreas críticas para el negocio. Considerando este factor, el outsourcing puede ser incorporado a áreas que tengan altos costos y funciones o procesos que puedan considerarse auxiliares o secundarios. La externalización de estas funciones supondrá una ventaja económica para la organización.

5.4.1.2. Fortalecimiento de competencias

Responder rápidamente a las cambiantes condiciones del mercado actual. Impulsar la transformación organizativa de forma controlada. El outsourcing permite dirigir los cambios que se deban a la necesidad de desarrollar nuevas funciones dentro de la organización, para de esta manera fortalecer sus procesos más débiles.

5.4.1.3. Captura de valor agregado

Mover el enfoque estratégico hacia la satisfacción del cliente. Dirigir su capital y su organización hacia la satisfacción del cliente. Según este factor, el outsourcing puede aplicarse a áreas con procesos sin contacto directo con los clientes, por su carácter secundario respecto a los objetivos estratégicos de la organización.

5.4.1.4. Diseño de la estrategia de la organización

Concreción de una arquitectura de actividad que implemente todas las funciones y procesos mediante el outsourcing, con especial atención a las funciones de producción y distribución. El outsourcing, desde este punto de vista, se convierte en la herramienta de ejecución de la actividad que permite tener una arquitectura organizativa virtual.

El outsourcing es un medio para alcanzar los objetivos estratégicos de la organización. Los factores más importantes para lograr el éxito del outsourcing son los siguientes:

Tener objetivos claros. El cliente debe tener bien definidos los objetivos que se pretenden alcanzar con el outsourcing y las funciones que desea externalizar.

Compromiso del cliente. El outsourcing requiere que el cliente suministre recursos altamente cualificados, que pueden explotar sus beneficios.

Definición detallada de los servicios incluidos. Los servicios incluidos deben definirse de forma clara y precisa.

Flexibilidad financiera. La solución de outsourcing debe ser flexible, desde el punto de vista financiero, para adaptarse a las condiciones cambiantes del gasto.

Flexibilidad tecnológica. Se deben incorporar procedimientos de actualización tecnológica, así como criterios de evaluación e incorporación de nuevas tecnologías a los servicios prestados.

Flexibilidad operativa. Es muy importante que el outsourcing incorpore elementos de flexibilidad que puedan ser utilizados para cambiar los términos operativos.

5.5. Objetivo de la auditoría a contratos de outsourcing

Los principales objetivos que pueden lograrse con la auditoría a contratos de un servicio de outsourcing son los siguientes:

- ◆ *Optimización y adecuación de los costos* relacionados con la gestión de los SI, en función de las necesidades reales.
- ◆ *Eliminación de riesgos* por tecnología obsoleta.

5.6. Servicios del Outsourcing

El servicio de outsourcing puede aplicarse típicamente en los siguientes supuestos:

- ◆ Gestión y operación de los SI de una organización:
 - ◆ Procesos en línea (*on-line*).
 - ◆ Procesos por lotes (*batch*).
 - ◆ Redes de comunicaciones.
 - ◆ Procedimientos de seguridad de los datos.
- ◆ Control y supervisión de sistemas:
 - ◆ Actualización y mantenimiento del sistema operativo y software de base.
 - ◆ Diseño y administración de las bases de datos.
 - ◆ Diseño de redes de comunicaciones.
 - ◆ Consultoría.
 - ◆ Mantenimiento de equipos físicos y lógicos.
 - ◆ Soporte técnico:
 - ◆ Usuarios.
 - ◆ Relación con vendedores y fabricantes.
- ◆ Desarrollo y mantenimiento de aplicaciones:
 - ◆ Planificación conceptual.
 - ◆ Especificación funcional.
 - ◆ Plan de aplicación.
 - ◆ Diseño.
 - ◆ Implementación.

- ◆ Pruebas de módulos y del sistema.

5.7. Características de un contrato de Outsourcing

Características relativas al *contrato* entre las partes:

- ◆ Su elaboración es compleja, puesto que debe establecer claramente las responsabilidades de ambas partes en cualquier aspecto, no sólo del servicio actual sino también del nivel de servicio futuro.
- ◆ Suele tener una duración de varios años. En el sector privado tiene una duración no menor a 7 ó 7 años, siendo habitual un período de 10 años.
- ◆ Uno de los aspectos más importantes del contrato es la definición de su resolución (finalización), el establecimiento de salidas programadas antes de cumplirse el plazo acordado, así como los períodos de preaviso en caso de reversión del servicio.
- ◆ Junto con los conceptos financieros, a lo largo de todo el proceso de evaluación se deben establecer criterios de *transferencia de personal* (para el caso de que existan).
- ◆ El alcance del contrato es *a la medida*; es decir, podrá ser tan amplio como lo deseen las partes contratantes.
- ◆ El contrato debe ser *flexible* para que la administración pueda cambiar los requisitos del servicio y el proveedor pueda cambiar los medios con los que lo da. Mientras que un contrato de outsourcing se firma para que sea válido durante años, los requisitos de tecnología están en constante evolución.

5.8. Aspectos clave para tomarse en cuenta en los contratos de outsourcing

No se trata sólo de elegir el proveedor de outsourcing adecuado para un contrato de externalización, a continuación se mencionan los diez aspectos más relevantes en el momento de elaborar un contrato de outsourcing:

5.8.1. Precio. Especificar el costo de todos los posibles servicios, inclusive los que en un principio no se requieran utilizar.

5.8.2. Seguridad de la información. Se establecerá en el contrato que el cliente es el dueño de los datos y que el proveedor de outsourcing es únicamente guardián de los mismos.

5.8.3. Nivel de servicio. Los principales puntos por cubrir en un SLA(Acuerdo de Nivel de servicio) son:

- ◆ Tipo de servicio
- ◆ Soporte a clientes y asistencia
- ◆ Provisiones para seguridad y datos
- ◆ Garantías del sistema y tiempos de respuesta
- ◆ Disponibilidad del sistema
- ◆ Conectividad
- ◆ Penalizaciones por incumplimientos

5.8.4. Planes de contingencia. Determinar las responsabilidades de cada una de las partes en caso de ocurrir posibles situaciones que provoquen incidentes.

5.8.5. Disposición. Incluir aspectos como la duración de la prestación de los servicios, así como cláusulas para determinar la recontractación por parte del cliente.

5.8.6. Plan de pagos. En el plan de pagos se establece la forma en que se cubrirá el costo del servicio, teniendo en cuenta que cada pago podrá tener un componente de costo de carácter fijo y otro variable, en función del nivel de servicio. *En los contratos se pueden establecer los siguientes tipos de pagos:*

- ◆ Precio fijo
- ◆ Precio variable, por unidad de uso
- ◆ Precio mixto (parte fija y parte variable)

5.8.7. Otros elementos por considerar:

- ◆ La preparación y administración de posibles casos de conflicto entre las partes.
- ◆ Determinar claramente los criterios de medida del rendimiento del SLA para su aplicación y revisión periódica.
- ◆ Documentar detalladamente todas las actividades.
- ◆ Establecer la infraestructura adecuada de seguimiento, comunicación y responsabilidades, que asegure el acuerdo mutuo a lo largo del proyecto.
- ◆ Actualizar constantemente la calidad y costo del servicio según las exigencias del mercado.
- ◆ Acordar las condiciones de la cesión de los activos. Entiéndase a los activos como el conjunto de recursos informáticos que son propiedad de la organización contratante y que son susceptibles de ser traspasados a la

empresa que proporciona el servicio de outsourcing e incluso posteriormente ser recuperados.

- ◆ Estipular las condiciones del control de los SI (Sistemas de información) a llevar a cabo durante el contrato.
- ◆ Convenir las condiciones en las cuales se obtendrá el control de los SI una vez finalizado el contrato.
- ◆ acordar la propiedad intelectual, especialmente en el traspaso al proveedor de la responsabilidad del desarrollo de aplicaciones.

5.8.8. Terminación del contrato. El contrato de outsourcing debe disponer los mecanismos necesarios para que a la finalización del mismo sea posible la transferencia de activos y del servicio. Este concepto se relaciona con la terminación del contrato, puesto que especifica:

- ◆ El tiempo (a un año de la firma, a dos, etc.) en el que se podrá dar éste por finalizado.
- ◆ La posibilidad de cancelación anticipada del contrato con su correspondiente compensación económica.
- ◆ Los plazos de preaviso de finalización anticipada del servicio.

5.8.9. Confidencialidad. Una cláusula fuerte de confidencialidad es importante para protegerse del daño de la información, y también de las demandas por parte del proveedor de outsourcing.

5.8.10. Rescisión del contrato por incumplimiento del SLA (Acuerdo de Nivel de Servicio).

Uno de los principales objetivos al realizar un contrato de outsourcing de cualquier empresa es tener siempre el control sobre la calidad y disponibilidad de los servicios proporcionados por el proveedor de outsourcing.

5.9. Factores relevantes en el proceso de contratación⁸

En la definición del objeto del contrato y los términos de referencia, así como en la valoración y comparación de ofertas de los oferentes pueden intervenir muchos factores y de diversa índole. Por esas razones es recomendable el planteamiento de comenzar cualquier proceso de outsourcing de forma escalonada y en fases independientes para poder ir midiendo el impacto y corregir cualquier desviación. Teniendo en cuenta este planteamiento a la hora de emprender la contratación de un servicio de "externalización", los factores que intervienen deberán estar recogidos dentro de las especificaciones del conjunto de cuestionarios disponibles a tal efecto:

⁸ **OLGUÍN** Romo Heriberto. Adaptado de Outsourcing en Tecnologías de Información. México. Facultad de ingeniería. UNAM. 1.ª ed. 2007, P.104.

- ◆ De empresa.
- ◆ Económicos.
- ◆ Técnicos particulares.

Estos son los factores que pueden intervenir en mayor medida en el proceso de contratación de un servicio de outsourcing cuyo seguimiento debe efectuarse exhaustivamente:

- ◆ Transferencia de activos o recursos.
- ◆ Flexibilidad.
- ◆ Reversibilidad.
- ◆ Experiencia en el entorno público.
- ◆ Seguridad.
- ◆ Continua inversión en tecnología.
- ◆ Coincidencia en estrategia tecnológica con la organización.

A continuación se describen cada uno de estos factores.

5.9.1. Transferencia de activos o recursos

Dentro del ambiente del outsourcing los recursos utilizados pueden ser de dos tipos:

- ◆ Equipamiento con el cual se lleva a cabo la administración de los sistemas de información.
- ◆ Personal que se dedica a la administración de los sistemas de información.

En la transferencia de equipamiento se valorará positivamente, que la empresa de outsourcing acepte los activos de la empresa y el valor económico que ésta propone en cuanto a:

- ◆ Equipos físicos.
- ◆ Equipos lógicos (no aplicativos)
- ◆ Instalaciones.

5.9.2. Flexibilidad

Será un punto a favor que la empresa de outsourcing se comprometa a adaptarse en la mayor medida posible a cambios respecto del nivel de servicio acordado, en cuanto a:

- ◆ Aumento del horario de utilización de los sistemas de información.
- ◆ Variación de los periodos de tiempo que requieran una capacidad de proceso masivo (24 horas al día).
- ◆ Aumento y mejora del lote de equipos, respecto de lo acordado en el mantenimiento.

- ◆ Actualización tecnológica de los equipos lógicos (versiones, nuevos productos, etc.).
- ◆ Variación de las especificaciones en el desarrollo o el mantenimiento de aplicaciones.

5.9.3. Reversibilidad

Este concepto se refiere a la posibilidad de recuperación de los activos y servicios cedidos a la empresa de outsourcing. Este concepto tiene aplicación tanto en la terminación del periodo de vigencia del contrato como en las salidas programadas que se establezcan.

Se valorará que la empresa de outsourcing considere esta posibilidad de recuperar los activos, y además que:

- ◆ Planifique la opción de recompra de equipos.
- ◆ Proponga un método de valoración de activos que estipule el incremento en el valor de los activos mientras dura la prestación del servicio. Estos activos pueden ser de tres tipos:
 - Activos mejorados (aplicaciones, nuevos desarrollos, etc.).
 - Activos actualizados (equipos físicos y mantenimiento de aplicaciones).
 - Activos formados (formación de personal en las nuevas herramientas).

5.9.4. Experiencia en el entorno

La experiencia del personal de la empresa de outsourcing en otros trabajos con la administración pública será calificada positivamente. Es conveniente que dichos trabajos tengan relación directa con los servicios por contratar.

5.9.5. Seguridad

Se valorarán todas las medidas (procedimientos, recursos físicos y humanos, etc.) de los cuales disponga la empresa de outsourcing para asegurar la confidencialidad, integridad y disponibilidad de la información. Por ejemplo se puede mencionar:

- ◆ Procedimientos de seguridad.
- ◆ Procedimientos relacionados con las instalaciones donde residen los equipos físicos (de acceso, protección contra el fuego, etc.).
- ◆ Procedimientos de respaldos periódicos de información.
- ◆ Procedimientos de contingencia (ante desastres).
- ◆ Dispositivos de seguridad específicos: control de accesos a los sistemas de información, centros de respaldo, etc.

5.9.6. Inversión continua en tecnología

La empresa de outsourcing deberá estar con tecnología actualizada y con los mejores profesionales (formados en esas tecnologías). Con esto, se valorarán factores que demuestren esa inversión continua en tecnología, tales como los siguientes:

- ◆ Tener las últimas versiones de equipos físicos y lógicos.
- ◆ Certificaciones de calidad y seguridad de organizaciones reconocidas.
- ◆ Número de cursos realizados al año para el reciclaje y formación del personal.

5.9.7. Coincidencia en estrategia tecnológica con la organización

Es conveniente que las estrategias tecnológicas de la organización y de la empresa de outsourcing sean coincidentes; es decir, que el entorno y tipo de equipos físicos, lógicos y de comunicaciones sean equivalentes o vayan en la misma línea, en especial en lo relativo a la orientación estratégica de sistemas abiertos.

5.10. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

EL MODELO DEL NEGOCIO

- 5.10.PAA-001.** ¿Cuál es el objetivo del contrato de outsourcing?
- 5.10.GSA-001.** Examinar los requerimientos pretendidos en el objeto del contrato.
- 5.10.RC-001.** Se debe redactar lo más claro posible y se deben analizar todas las posibles matizaciones aunque parezcan intrascendentes. Deberá considerar cuatro aspectos:
1. La racionalización financiera.
 2. El fortalecimiento de competencias
 3. La captura del valor agregado
 4. El diseño de la estrategia de la organización.
- 5.10.PAA-002.** ¿Se hace mención de cuál es el ámbito de aplicación del objetivo del contrato?
- 5.10.GSA-002.** Revisar que se encuentre especificado en qué áreas de la empresa se va efectuar esta operación.
- 5.10.RC-002.** Se debe tener un control adecuado de cada una de las áreas de la empresa y determinar a cuales de ellas se les aplicará el contrato.
- Determinar correctamente el nivel de servicio que se requiere.

- 5.10.PAA-003.** ¿Cuenta con cláusulas identificativas y de reconocimiento de capacidad?
- 5.10.GSA-003.** Revisar que cuente con datos que identifiquen a ambas partes, así como el reconocimiento de capacidad legal necesaria al no cumplirse con lo que se especifique.
- 5.10.RC-003.** La ayuda de una firma legal especializada en contratos de outsourcing puede ser de mucho beneficio.
- 5.10.PAA-004.** ¿Cuenta con cláusula de manifestación de voluntad?
- 5.10.GSA-004.** Revisar que cada una de las partes manifieste su voluntad para cumplir el contrato.
- 5.10.RC-004.** En el momento de seleccionar un proveedor de outsourcing es necesario saber claramente la diferencia entre proveedor de servicio de outsourcing, y de un consultor informático. Tomar en cuenta también que la elección de proveedores tendrá que hacerse con base en el que se acerque más a la solución de las necesidades, evaluando sus capacidades y características y no sólo en el precio.

PRECIOS

- 5.10.PAA-005.** ¿Se especifican las tarifas de todos los servicios disponibles?
- 5.10.GSA-005.** Verificar que estén descritos todos los precios de los servicios, inclusive para los que inicialmente no se vayan a utilizar.
- 5.10.RC-005.** Es recomendable que el cliente realice el contrato para que éste sea utilizado como una base que le permita tener el control del mismo; si el proveedor no es capaz de aceptar la propuesta el cliente tenga la opción de elegir a otro proveedor.
- 5.10.PAA-006.** ¿Los planes de pago para la remuneración del servicio están establecidos?
- 5.10.GSA-006.** Revisar que dentro del contrato se describa la forma en que dichos pagos serán efectuados.
- 5.10.RC-006.** Tomar en cuenta que existen varias formas de establecer el plan de pagos.

ALCANCE DE LOS SERVICIOS

- 5.10.PAA-007.** ¿Está especificado en el contrato de outsourcing el nivel de servicio que es requerido?

5.10.GSA-007. El auditor revisará que dentro del contrato exista una cláusula en la que se estipulen los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes (cliente y proveedor de servicio).

5.10.RC-007.

Se recomienda que para implementar con éxito un nivel de servicio, se deben tomar en cuenta los siguientes puntos: definir los objetivos que pretende solucionar el nivel de servicio, identificar expectativas, adecuada planificación temporal, optimización y/o rediseño de procesos, errores más frecuentes de un nivel de servicio, definir niveles de servicio inalcanzables, regulación excesiva, error en la definición de prioridades, complejidad técnica, irrelevancia. Se recomienda también disponer de la información lo más completa posible y tomar en cuenta las necesidades presentes y futuras de su empresa.

5.10.PAA-008. ¿Se describen los plazos de ejecución de cada una de las fases o módulos?

5.10.GSA-008. Se deberá ver que estén descritos los plazos de finalización y entrega de cada una de las fases o módulos.

5.10.RC-008. Describir los plazos de ejecución en el nivel de servicio.

MEDIOS TÉCNICOS

5.10.PAA-009. ¿Existe alguna cláusula en donde se asume que el proveedor facilitará la integración de nuevas tecnologías?

5.10.GSA-009. Percatarse que exista el clausulado correspondiente en donde se señale que el proveedor es capaz de tener los últimos avances en tecnología o de al menos obtenerla si es que es requerida por el cliente.

5.10.RC-009. Se debe estar seguro sobre lo que se quiere, sobre la tecnología que se requiera, así como también de tener bien calculada la inversión que se pretende realizar. Asesorarse con un experto que lo oriente en materia de tecnologías de información.

5.10.PAA-010. ¿Se delimitan las responsabilidades del cliente y del proveedor en el contrato de outsourcing en caso de tener incidentes?

5.10.GSA-010. Revisar que se tengan determinadas las responsabilidades tanto del cliente como del prestador del outsourcing, en caso de situaciones que provoquen incidentes.

5.10.RC-010. Se recomienda identificar todas las posibles situaciones que provoquen conflictos e incidentes para cada caso.

- 5.10.PAA-011.** ¿Se mencionan aspectos relacionados con la seguridad de la información?
- 5.10.GSA-011.** Se verificará que en el contrato se reconozca al cliente como el dueño de los datos y que el proveedor de outsourcing sea únicamente guardián de los mismos
- 5.10.RC-011.** Primeramente el cliente deberá contar con respaldos de la información y así como también que se escoja adecuadamente a la empresa que le proporcionará el servicio de outsourcing, tomando en cuenta los procedimientos, recursos físicos, humanos, etc., de los cuales disponga la empresa que le proporcionará dicho servicio, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información.
- El cliente también podrá, si es necesario, ordenar una vez al año, la realización de una auditoría de los sistemas de seguridad del centro informático del proveedor.
- 5.10.PAA-012.** ¿Cuenta con el apartado correspondiente en donde se considera la propiedad intelectual?
- 5.10.GSA-012.** Revisar que exista dicho apartado y que mencione las situaciones por las cuales la empresa que contrata el servicio de outsourcing cede o no los derechos de propiedad intelectual a la empresa de outsourcing.
- 5.10.RC-012.** Considerar la contratación del arbitraje para la solución de posibles conflictos.
- 5.10.PAA-013.** ¿Cuenta con cláusulas de confidencialidad?
- 5.10.GSA-013.** Analizar que cuente con cláusulas que den protección en caso de daños de la información, así como de posibles demandas del proveedor de outsourcing.
- 5.10.RC-013.** Es recomendable tener clasificada claramente la información en confidencial y no confidencial, así como también tener algún tipo de documento independiente al contrato de outsourcing que garantice dicha confidencialidad en caso de terminarse el primero. Se recomienda también contar con las licencias de uso, al igual que el registro de patentes si es que se ha desarrollado software u otros sistemas de uso exclusivo.
- 5.10.PAA-014.** ¿Cuenta con cláusulas de rescisión del contrato en caso del incumplimiento en el nivel de servicio?

- 5.10.GSA-014.** Verificar que cuente con cláusulas que permitan rescindir el contrato en caso de no cumplir con un adecuado nivel de servicio.
- 5.10.RC-014.** Establecer claramente cuál es el nivel de servicio que se requiere para evitar problemas con el outsourcer, tomando en cuenta también proyectos que hay que afrontar, sus prioridades y los recursos con los que se cuenta.
- 5.10.PAA-015.** ¿Se tiene asegurada la confidencialidad, integridad y disponibilidad de la información?
- 5.10.GSA-015.** Verificar la existencia de procedimientos de seguridad relativos a las instalaciones donde residen los equipos físicos y del respaldo periódico, de recursos físicos y humanos para el control de accesos a los sistemas de información y de procedimientos ante desastres.
- 5.10.RC-015.** Serán valoradas positivamente todas las medidas que pueda disponer la empresa de outsourcing para reducir los riesgos posibles ante los cambios extremadamente rápidos de las tecnologías, la competencia, las regulaciones de gobierno y las condiciones financieras.

VIGENCIA DEL CONTRATO

- 5.10.PAA-016.** ¿Se describe claramente la duración de la prestación de los servicios?
- 5.10.GSA-016.** Verificar que se especifique la fecha en que entrará en vigor el contrato, el tiempo de su duración, así como también la fecha en que terminará.
- 5.10.RC-016.** Tener en cuenta que existen estados cuyas legislaciones internas no prevén la posibilidad de suscribir contratos con una duración mayor a un año. Se recomienda también no dejar a un lado autoridades importantes en tema del outsourcing, como lo son: la Secretaría de Hacienda y Crédito Público (SHCP) y la Secretaría de la Función Pública (SFP).

TRANSFERENCIA DE RECURSOS

- 5.10.PAA-017.** ¿Están acordadas las condiciones de la cesión de los activos referidos al momento en que se inicia el acuerdo entre el cliente y el proveedor de outsourcing?
- 5.10.GSA-017.** Observar que se mencionen dichas causas dentro del contrato.
- 5.10.RC-017.** Llevar el registro adecuado de todos los activos con los cuales cuenta la empresa.

- 5.10.PAA-018.** ¿La transferencia de programas de parte del proveedor (en caso de haberla) está descrita en las cláusulas?
- 5.10.GSA-018.** Corroborar la descripción de la transferencia de los programas, así como también de la indemnización por el incumplimiento de lo dispuesto, del proveedor hacia el cliente.
- 5.10.RC-018.** Se debe tener presente que para la adquisición de software se tendrán que obtener junto con éste, licencias, derechos, etc., que faciliten su uso ante la ley. Se debe tomar en cuenta la contratación de peritos que establezcan el precio que se tendrá que pagar por los derechos de uso de los programas que serán usados por el cliente.
- 5.10.PAA-019.** ¿Contiene un apartado para los retrasos imputables al cliente?
- 5.10.GSA-019.** Localizar dentro del contrato un apartado que describa la situación que se tomará en caso de tener retrasos debido a razones del cliente.
- 5.10.RC-019.** Proporcionar la información que sea requerida y necesaria para el desarrollo del trabajo.
- 5.10. PAA-020.** ¿Dentro del contrato se establece una comisión de seguimiento y control?
- 5.10.GSA-020.** Revisar que estén los nombres y sus respectivas funciones a realizar, así como también, estar fija la fecha de las reuniones entre miembros de la comisión y representantes del proveedor.
- 5.10.RC-020.** Revisar constantemente que se cumplan adecuadamente los servicios informáticos realizados.

FLEXIBILIDAD DEL SERVICIO

- 5.10.PAA-021.** ¿Se menciona la ubicación donde realizará el trabajo el proveedor?
- 5.10.GSA-021.** Verificar que se describa la ubicación del lugar donde el outsourcer realizará el trabajo del cliente.
- 5.10.RC-021.** Informarse sobre el proveedor de outsourcing, especialmente en la experiencia que pueda tener en el mercado. Verificar que el domicilio sea verdadero.
- 5.10.PAA-022.** ¿Se tiene la posibilidad de cancelación anticipada del contrato?
- 5.10.GSA-022.** El auditor revisará que se tenga contemplada esta posibilidad dentro del contrato, así como también que cuente con la compensación económica correspondiente.

- 5.10.RC-022.** Cualquiera de las partes, bajo su propio criterio, podrá rescindir el presente contrato mediante notificación escrita. Se deberá indicar el día de finalización con un mínimo de un mes de anticipación.
- 5.10.PAA-023.** Analizar la capacidad que tiene la empresa de outsourcing para dar servicio con el mismo equipamiento de forma simultánea
- 5.10.GSA-023.** Verificar el número de organizaciones a las que se da servicio en la actualidad, el número máximo de usuarios y el número de transacciones ejecutadas.
- 5.10.RC-023.** Será valorada positivamente a la empresa de outsourcing que se comprometa a adaptarse en la mayor medida posible a cambios respecto del nivel del servicio pactado, en cuanto al incremento del horario de utilización de los Sistemas de Información y en la actualización tecnológica de los equipos lógicos.

GARANTÍA DE CALIDAD

- 5.10.PAA-024.** ¿Se mencionan garantías de parte del proveedor para el cliente?
- 5.10.GSA-024.** Verificar que se describan garantías ofrecidas por el proveedor de servicio de outsourcing.
- 5.10.RC-024.** Se recomienda contar con seguro por algún tipo de incidente.
- 5.10.PAA-025.** ¿Se mencionan responsabilidades dentro del contrato?
- 5.10.GSA-025.** Revisar que esté claro quien asume el riesgo y las responsabilidades del mismo.
- 5.10.RC-025.** Se recomienda que el cliente esté al tanto de las responsabilidades que pueden ser asignadas a cada una de las partes. Se recomienda también la contratación de un experto que le asesore en los últimos avances en tecnologías de información.
- También es indispensable conocer si el proveedor cuenta con seguro de responsabilidad civil.
- 5.10.PAA-026.** ¿Se incluyen limitaciones de responsabilidad?
- 5.10.GSA-026.** Se revisará que cuente con las opciones por las cuales la responsabilidad sea limitada.
- 5.10.RC-026.** No obstaculizar el trabajo del proveedor y verificar cuando hay incumplimiento debido a casos de fuerza mayor.
- 5.10.PAA-027.** ¿Se realizan pruebas para la verificación y el control de la calidad?

- 5.10.GSA-027.** Determinar qué aspectos se cubren en la planificación y supervisión de la calidad en el servicio de outsourcing.
- 5.10.RC-027.** El control de calidad debe estar basado en la definición de responsables y compromisos por parte de la organización y de la empresa de outsourcing, en el establecimiento de reuniones periódicas de seguimiento donde se expongan los problemas encontrados, en la definición de acciones correctoras y en la utilización de herramientas informáticas de planificación y control.
- 5.10.PAA-028.** ¿Se dispone de programas de capacitación para la formación del personal?
- 5.10.GSA-028.** Determinar el número de cursos realizados al año para el reciclaje y formación de los recursos humanos.
- 5.10.RC-028.** La empresa de outsourcing deberá estar con tecnología de punta y con los mejores profesionales, para ello se valorarán factores que demuestren esa continua inversión en tecnología.

REVERSIBILIDAD

- 5.10.PAA-029.** ¿Existe alguna cláusula para determinar la recontractación por parte del cliente?
- 5.10.GSA-029.** Analizar la conveniencia de la recontractación, considerando la posibilidad de recuperación de los activos y del servicio cedido a la empresa de outsourcing.
- 5.10.RC-029.** Realizar la planificación de la recuperación de los activos, como las aplicaciones, nuevos desarrollos, equipos físicos y la formación de personal en las nuevas herramientas, con el fin de incrementar el valor de sus activos mientras dura la prestación del servicio.
- 5.10.PAA-030.** ¿Existe documentación detallada de los planes de transición para aplicar el servicio de outsourcing en la estructura actual de la empresa?
- 5.10.GSA-030.** Verificar la existencia de reportes de todas las actividades de la preparación y gestión de posibles casos de conflicto entre ambos.
- 5.10.RC-030.** Al establecer la infraestructura adecuada de seguimiento, comunicación y responsabilidades en el periodo de transición se asegura el acuerdo mutuo a lo largo del proyecto, reflejando claramente los diferentes criterios de medida del rendimiento para su aplicación y revisión periódica. Por lo anterior, es necesario dar importancia prioritaria al factor humano.

CAPÍTULO

VI

AUDITORÍA A PROCEDIMIENTOS DE CONTINGENCIA

CAPÍTULO VI

AUDITORÍA A PROCEDIMIENTOS DE CONTINGENCIA

6.1. Introducción

Los procedimientos de contingencia implican un análisis de los posibles riesgos a los cuales pueden estar expuestos el personal, los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en dichos planes se considera un estudio de los riesgos, la forma de reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que los Procedimientos o Planes de Contingencia incluyan un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

6.2. Auditoría a Procedimientos de Contingencia.

El objetivo de la auditoría a procedimientos de contingencia es verificar si en el Centro de Tecnología de Información (CTI) se cuenta con las políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos e información, mantener la seguridad e integridad de las personas así como de los equipos debido a contingencias como incendios, inundaciones, sismos, huelgas, disturbios, sabotajes, robos, etc., y continuar en medio de la emergencia hasta que sea restaurado el servicio por completo.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Dentro de este tipo de auditoría hay dos ámbitos que vamos a analizar. El primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas.

El segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está operativo y actualizado y es donde recae precisamente la auditoría.

6.3. Requerimientos de un Plan de Contingencias.

Haciendo un esquema muy general, un plan de contingencias que sea aprobado debe abarcar en su mayoría los siguientes aspectos:

- ◆ Plan de Reducción de Riesgos (Plan de Seguridad).
- ◆ Plan de Recuperación de Desastres.
- ◆ Actividades Previas al Desastre.
- ◆ Establecimiento del Plan de Acción.
- ◆ Formación de Equipos Operativos.

- ◆ Formación de Equipos de Evaluación (auditoría de cumplimiento de procedimientos de Seguridad).
- ◆ Actividades durante el Desastre.
- ◆ Plan de Emergencias.
- ◆ Formación de Equipos.
- ◆ Entrenamiento.
- ◆ Actividades después del Desastre.
- ◆ Evaluación de Daños.
- ◆ Priorización de Actividades del Plan de Acción.
- ◆ Ejecución de Actividades
- ◆ Evaluación de Resultados.
- ◆ Realimentación del Plan de Acción.

6.3.1. Plan de Reducción de Riesgos (Plan de Seguridad).

Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

Análisis de riesgos:

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección de la Información en análisis, versus el costo de volverla a producir (reproducir).

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su costo potencial desarrollando un plan de acción adecuado. Sin embargo la vida de los seres humanos siempre debe estar por delante de cualquier precaución.

6.3.2. Plan de Recuperación de Desastres.

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el CTI.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

- ◆ Actividades previas al desastre.
- ◆ Actividades durante el desastre.
- ◆ Actividades después del desastre.

6.3.3. Actividades previas al desastre.

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades antes de que ocurra un desastre, éstas son las más importantes pues con ellas se puede evitar un daño mayor inclusive evitar los desastres mismos, esto nos asegura un proceso de recuperación con el menor costo posible a nuestra Institución.

Podemos detallar las siguientes Actividades Generales:

- ◆ Establecimiento del Plan de Acción.
- ◆ Formación de Equipos Operativos.
- ◆ Formación de Equipos de Evaluación (auditoría interna de los procedimientos sobre Seguridad).

6.3.4. Establecimiento del Plan de Acción.

En esta fase de planeamiento se deben establecer los procedimientos relativos a:

- ◆ Sistemas e Información.
- ◆ Equipos de Cómputo.
- ◆ Personal.

6.3.4.1. Sistemas de Información. La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el área de informática como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha institucional.

Con toda esta información se deberá realizar una lista priorizada (un ranking) de los sistemas de información necesarios para que la institución pueda recuperar su operatividad perdida en el desastre (contingencia) y que estén respaldados para trabajar en otro sitio o en su defecto la información vital trasladarla.

6.3.4.2. Equipos de Cómputo. Aparte de las Normas de Seguridad hay que tener en cuenta:

Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene) su ubicación y nivel de uso institucional y en caso de pérdida se pueda saber exactamente de que se trata.

6.3.4.3. Personal. El establecimiento del plan de acción no funcionaría si el personal no lo conoce o simplemente no le importa. Es de vital importancia comunicarle a toda el área

informática de los planes de acción y sus metas para un mejor desenvolvimiento en caso de siniestro.

Igualmente es necesario que existan actividades previas a un desastre que motiven a los empleados a estar cerca de los planes de contingencia, esto por medio de simulacros cada mes, regalándoles tarjetas y carteles sobre la importancia de la seguridad en el trabajo.

6.3.5. Formación de Equipos Operativos.

Para cada unidad operativa de la institución, se deberá designar un responsable, pudiendo ser el jefe de dicha unidad o un Responsable de Seguridad para el caso de las instalaciones.

6.3.6. Formación de Equipos de Evaluación (auditoría interna de los procedimientos sobre seguridad).

Esta función debe ser realizada de preferencia por personal de inspección, de no ser posible, la realizará el personal del área de informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos. Finalmente se desea conocer como marchan los procedimientos de contingencia en la institución.

6.3.7. Actividades durante el desastre.

Una vez presentada la contingencia o siniestro, se deberán ejecutar las siguientes actividades, planificadas previamente:

- ◆ Plan de Emergencias.
- ◆ Formación de Equipos.
- ◆ Entrenamiento.

6.3.8. Plan de Emergencias.

En este plan se establecen las acciones que se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del siniestro:

- ◆ Durante el día.
- ◆ Durante la noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

- ◆ Vías de salida o escape.
- ◆ Plan de Evacuación del Personal.

- ◆ Plan de puesta a buen recaudo de los activos (incluyendo los activos de información) de la institución (si las circunstancias del siniestro lo posibilitan).

- ◆ Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
- ◆ Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas) lista de teléfonos de Bomberos, Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

6.3.9. Formación de Equipos.

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones específicas definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en un área cercana, etc.) deberán existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo con los lineamientos o clasificación de prioridades, para salvar los equipos señalados dentro de los mismos planes de contingencia.

6.3.10. Entrenamiento.

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo con los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se pueden aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

6.3.11. Actividades después del desastre.

Después de ocurrido el siniestro o desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción:

- ◆ Evaluación de Daños.
- ◆ Priorización de Actividades del Plan de Acción.
- ◆ Ejecución de Actividades.
- ◆ Evaluación de Resultados.
- ◆ Realimentación del Plan de Acción.

6.3.12. Evaluación de Daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, qué sistemas se están afectando, qué equipos han quedado no operativos, cuáles se pueden recuperar, y en cuánto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha institución. En el caso de las instalaciones deben acudir especialistas a

evaluar las condiciones del edificio y no entrar hasta que se tenga plena seguridad del centro de cómputo.

6.3.13. Priorización de actividades del Plan de Acción.

Toda vez que el Plan de Acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

6.3.14. Ejecución de Actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador y reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

6.3.15. Evaluación de Resultados.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos evaluar objetivamente, todas las actividades realizadas, qué tan bien se hicieron, qué tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, cómo se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían salir dos tipos de recomendaciones, una la realimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

6.3.16. Realimentación del Plan de Acción.

Con la evaluación de resultados, debemos optimar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra institución el plan de contingencias llevado a cabo.

6.4. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

- 6.4.PAA-001.** ¿Se cuentan con planes de contingencia?
- 6.4.GSA-001.** Pedir al responsable los planes que se tienen implementados, verificar si se tienen por escrito y si cumplen las nuevas normas de protección civil.
- 6.4.RC-001.** En caso de no contar con uno, invitar a que los responsables implementen uno, ya que les proporcionará grandes beneficios y prevendrá cualquier tipo de percance.
- 6.4.PAA-002.** ¿El plan de contingencia cubre todos los aspectos?
- 6.4.GSA-002.**
- ◆ Verificar que sean tanto de protección del personal, como del equipo y de la información, mediante la lectura de los manuales de planes de contingencia.
 - ◆ Revisar los procedimientos de contingencia elaborados y al final de la auditoría hacer una evaluación de la realidad contra lo especificado en dichos planes.
- 6.4.RC-002.** Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.
- 6.4.PAA-003.** ¿Sabe qué hacer en caso de siniestro dentro del CTI?
- 6.4.GSA-003.** Verificar si el personal conoce los planes de contingencia mediante preguntas sencillas de qué hacer en caso de un siniestro en el CTI.
- 6.4.RC-003.** Es importante que todo el personal conozca todas las medidas de seguridad, así que se deben dar a conocer por medio de carteles, trípticos, o cualquier tipo de comunicación, además de ponerlas en práctica de vez en cuando.
- 6.4.PAA-004.** ¿Se puede localizar al responsable del CTI fácilmente?
- 6.4.GSA-004.**
- ◆ Averiguar si existe un responsable de establecer y vigilar que se cumplan estas medidas y si el personal conoce a dicho responsable. Revisar si existen equipos capacitados para afrontar cualquier eventualidad.
 - ◆ Anotar la forma de localizar al responsable y su horario de trabajo.

- 6.4.RC-004.** Debe existir personal responsable y capacitado, al cual se pueda consultar y pueda dar indicaciones a todo el personal en caso de cualquier duda o eventualidad. Es conveniente que tenga un lugar establecido, como un cubículo, y que siempre esté alguien que pueda proporcionar ayuda.
- 6.4.PAA-005.** ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
- 6.4.GSA-005.** Revisar si hay un responsable inmediato que se encuentre en el CTI siempre y esté en contacto con los equipos y el personal.
- 6.4.RC-005.** Resulta eficiente tener dos grupos, uno encargado de la seguridad del personal y si el siniestro lo permite salvar los recursos informáticos y otro para combatir el siniestro.
- 6.4.PAA-006.** ¿Qué medidas de seguridad se utilizan en el CTI?
- 6.4.GSA-006.** Verificar con el personal si hay algún tipo de entrenamiento para salvar la vida, los equipos y la información y cada cuando se realizan los simulacros.
- 6.4.RC-006.** Realizar los simulacros de acuerdo con un procedimiento bien establecido ayudaría al personal a conocer las medidas de seguridad, a estar listos y tal vez menos nerviosos al momento de cualquier eventualidad o siniestro.
- 6.4.PAA-007.** ¿En caso de desastre se cuenta con un seguro que proteja tanto al personal como al equipo?
- 6.4.GSA-007.** Verificar que existan las pólizas de seguro y el alcance de las mismas.
- 6.4.RC-007.** Normalmente una póliza de seguros de equipo de cómputo cubre:
1. Daños materiales al equipo.
- Ampara cualquier pérdida o daño físico, súbito e imprevisto, que requiera de reparación o reemplazo. Excluye:
- ◆ Pérdidas o daños causados por terremoto, temblor, maremoto, erupción volcánica, ciclón, tifón o huracán.
 - ◆ Pérdidas o daños causados por hurto o robo sin violencia.
 - ◆ Pérdidas o daños causados por fallo e interrupción en el suministro de corriente eléctrica, de gas o de agua.
 - ◆ Pérdidas o daños que sean consecuencia del uso continuo o deterioro gradual debido a condiciones atmosféricas.

Sin embargo este tipo de exclusiones se pueden prever mediante la contratación expresa de otra póliza.

2. Portadores externos de datos.

Cubre la indemnización sobre daños causados a dispositivos de almacenamiento de datos así como la información contenida en éstos.

Excluye, cualquier gasto resultante de la incorrecta programación, perforación, clasificación, inserción, anulación accidental de informaciones, pérdidas de información causadas por campos magnéticos y virus informáticos.

3. Incremento en el costo de operación.

Esta cobertura se aplica si un daño material indemnizable diera lugar a una interrupción parcial o total de la operación, lo que causara un desembolso adicional al usar un CTI ajeno y/o suplente.

Los seguros a los equipos de cómputo se aplican a los bienes que se estén operando o que se encuentren en reposo, desmontados para propósitos de limpieza o reparación o durante su traslado dentro del periodo establecido en la póliza.

Generalmente excluyen los daños causados por:

- ◆ Guerra, invasión, actividades de enemigos extranjeros, hostilidades (con o sin declaración de guerra, guerra civil, rebelión, revolución, insurrección, motín, tumulto, huelga, paro decretado por el patrón, conmoción civil, poder militar o usurpado, conspiración, etc).
- ◆ Reacciones nucleares, radiación nuclear o contaminación radiactiva.
- ◆ Acto internacional o negligencia manifiesta del seguro o de sus representantes.

Sin embargo existen algunas pólizas adicionales que pueden contratarse y que cubren lo siguiente:

- ◆ Huelgas, alborotos populares y conmoción civil.
- ◆ Gastos extraordinarios y fletes expresos.
- ◆ Gastos por flete aéreo.
- ◆ Daños por fallo de la instalación de climatización.
- ◆ Robo sin violencia (hurto).
- ◆ Equipos móviles y portátiles fuera de los predios señalados.

- ◆ Cláusula de huracán, ciclón, tifón.
- ◆ Daños mecánicos y eléctricos internos.
- ◆ Equipos de climatización.

Se deben revisar y evaluar las diferentes alternativas de seguro que ofrecen las compañías dedicadas a este rubro.

- 6.4.PAA-008.** ¿Quién realiza la evaluación de los daños después de un desastre?
- 6.4.GSA-008.** Verificar si existen responsables que estén calificados para presentar informes detallados en caso de daños.
- 6.4.RC-008.** Lo ideal es que la aseguradora evalúe los daños y dé un reporte al personal encargado.
- 6.4.PAA-009.** ¿Existe personal de vigilancia en la institución?
- 6.4.GSA-009.** Verificar si hay seguridad dentro y fuera de la institución, el número de personas asignadas y cómo son identificadas por todo el personal.
- La contratación de vigilancia puede realizarse directamente o por medio de empresas que venden este servicio y en caso de que así sea anotar que empresa de seguridad privada está proporcionando este servicio.
- Verificar que existan documentos sobre el personal de seguridad, como el de un certificado sobre sus antecedentes penales y una carta del motivo de separación de sus anteriores empleos, esto para evitar sabotajes.
- 6.4.RC-009.** La contratación de personal de vigilancia es benéfica, y resulta más cómodo obtenerlo por medio de outsourcing. Éstos pueden estar ubicados en lugares estratégicos donde exista más vulnerabilidad. Se recomienda que al momento de reclutar al personal, se le realice exámenes psicológicos y médicos y tener muy en cuenta sus antecedentes de trabajo, ya que un CTI depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- 6.4.PAA-010.** ¿Cómo es la forma de acceder al CTI?
- 6.4.GSA-010.**
- ◆ Determinar si las medidas de seguridad implementadas para regular el acceso a las instalaciones son adecuadas.
 - ◆ Verificar que existan procedimientos, tales como los que describen a continuación, para regular el acceso a las instalaciones:

- ◆ Eliminar puertas no esenciales al CTI, ubicando una sola puerta de acceso con control continuo.
 - ◆ Colocar, donde sea necesario, un guardia o recepcionista, en el punto de entrada durante todo el tiempo que el CTI esté trabajando.
 - ◆ De ser posible, utilizar una sola ruta de evacuación en caso de emergencia.
 - ◆ Equipar todos los puntos de entrada y salida con mecanismos de control de acceso.
 - ◆ Restringir el acceso al área de computadoras sólo al personal autorizado.
 - ◆ Requerir que todas las personas autorizadas a efectuar operaciones dentro del área de computadoras se registren en una bitácora, en donde indiquen su nombre, firma, propósito y hora de entrada y de salida.
 - ◆ Identificar al personal autorizado a través de una credencial con fotografía.
 - ◆ No permitir el acceso al área de cómputo a los programadores o analistas, excepto bajo condiciones estrictas de control.
- ◆ Determinar si los procedimientos para prevenir el acceso de personal no autorizado, son adecuados y si se aplican en todos los accesos posibles.

6.4.RC-010.

Dependiendo del tipo de información que se maneje en el CTI se podría tener la propiedad vigilada las 24 horas del día y los siete días de la semana, por guardias entrenados específicamente para este tipo de instalaciones que son comúnmente visitadas por los clientes.

Además, dichos accesos se deberían encontrar monitoreados por el sistema de Circuito Cerrado de Televisión y contar con un sistema de accesos biométricos (lectura de huella digital) y de tarjetas de proximidad tanto en el edificio de operaciones como en la puerta de acceso al piso falso.

- ◆ Obtener una lista del personal autorizado para acceder a las instalaciones y determinar si su acceso es necesario, verificar si esta lista es regularmente revisada para decidir si el acceso de este personal sigue siendo válido.
- ◆ Observar el funcionamiento de las instalaciones en diferentes oportunidades y a diversos horarios para verificar que únicamente se permite el acceso a personal autorizado.
- ◆ Asegurarse de que cuando la sala de cómputo se encuentre vacía exista una vigilancia permanente, ya sea a través de observación

directa o por la existencia de alarmas o monitores que prevengan el acceso no autorizado.

- ◆ Realizar visitas no anunciadas al CTI, para comprobar la efectividad de las medidas de seguridad para el control de acceso.
- ◆ Verificar que el acceso al equipo del CTI sólo lo realice el personal autorizado.

6.4.PAA-011. ¿Cuenta con encargado de seguridad el acceso al CTI?

6.4.GSA-011. Verificar que tenga algún encargado, puede ser vigilante, recepcionista, tarjeta de control de acceso o circuito cerrado de televisión.

- 6.4.RC-011.**
- ◆ Asegurar que cualquier persona con acceso temporal, porte su identificación y se encuentre debidamente acompañada por un miembro del personal autorizado.
 - ◆ Verificar que existan procedimientos para identificar y acompañar a los visitantes durante el tiempo que permanezcan en las instalaciones.
 - ◆ Verificar que se supervisan estrechamente las visitas autorizadas, mediante mecanismos de control tales como:
 - ◆ Todos los visitantes a los cuales se les otorgó permiso para realizar una visita por el CTI, deben ser acompañados por personal autorizado.
 - ◆ No permitir visitas en grupos difíciles de controlar.
 - ◆ Recuperar todas las tarjetas de identificación dadas a los visitantes.

6.4.PAA-012. ¿Se cuenta con la información de las características físicas del CTI?

- 6.4.GSA-012.**
- ◆ Pedir una descripción breve de la construcción del CTI, de preferencia pedir los planos y lista de materiales con que fue construido.
 - ◆ Pedir una breve descripción de los materiales con que fueron construidos los muebles y de preferencia que sean de materiales no flamables.

6.4.RC-012. Los factores a considerar en la selección del lugar en el cual se colocará el CTI son:

- ◆ Ruido.
- ◆ Espacio requerido.
- ◆ Condiciones ambientales.
- ◆ Acceso al CTI.

El CTI se ubicará en un edificio que se encontrará en un sitio específico dentro de un área general, en cada uno de los puntos anteriores es importante considerar los siguientes criterios:

Selección del Área General:

- ◆ Cercanía a usuarios potenciales.
- ◆ Servicios de seguridad.
- ◆ Buenas vías de comunicación.
- ◆ Suministro de energía confiable.
- ◆ Buenos servicios de comunicación.
- ◆ Rentas e impuestos atractivos.

Selección de un sitio específico:

- ◆ Localización en partes elevadas como protección contra inundaciones.
- ◆ Proximidad a servicios de transporte urbano o comercial.
- ◆ Facilidad de acceso a los bancos de datos.
- ◆ Proximidad a aeropuertos.

Selección de un local o edificio específico:

- ◆ Espacio adecuado para el equipo y personal (tomando en cuenta una expansión).
- ◆ Ausencia de dificultades para la preparación del sitio.
- ◆ Espacio adecuado para los equipos de aire acondicionado y de suministro de energía.
- ◆ Posibilidad de colocar el centro de datos lejos de áreas que contengan materiales peligrosos.
- ◆ Posibilidad de colocar un área o sala de espera para los visitantes del CTI.
- ◆ Posibilidad de controlar el acceso.
- ◆ Instalación de misceláneas adecuadas.

Para controlar los niveles de ruido es necesario considerar la cercanía de algún tipo de taller o equipo de cómputo ruidoso, cuando esto sucede, estos equipos se colocan por separado.

Preparación del plano de distribución consideraciones generales:

- ◆ Flujo eficiente de trabajo.
- ◆ Cercanía de áreas interactuantes.
- ◆ Flujo de trabajo sin retrocesos.
- ◆ No interferencia del tránsito de personas con el procesamiento.
- ◆ Cercanía del personal a recursos (consumibles, archivos, equipo,...) de uso frecuente.
- ◆ Áreas de almacenamiento/recepción adecuadas.
- ◆ De consumibles (papel, cintas, disquetes).
- ◆ De equipo.
- ◆ De material de desecho.
- ◆ Puertas y corredores amplios.
- ◆ Minimizar las puertas, ventanas y obstrucciones.
- ◆ Dos salidas en cada área que contenga personal.
- ◆ Tomas de corriente suficiente y convenientemente localizadas.
- ◆ Espacio adecuado para mobiliario, equipo y material.
- ◆ Distribución adecuada de teléfonos.
- ◆ Áreas que faciliten la observación.
- ◆ Área para alimentos.
- ◆ Sanitarios suficientes.
- ◆ Facilidad de guardarropa.
- ◆ Espacio para unidad de aire acondicionado y equipo eléctrico.
- ◆ Posibilidad de modificación y expansión.
- ◆ Apariencia atractiva.

Requerimientos ambientales:

- ◆ Piso falso.
- ◆ Conducción de cables (eléctricos y de datos).
- ◆ Inyección de aire acondicionado.
- ◆ Resguardo de inundaciones.

Características:

- ◆ Resistente a electricidad estática.
- ◆ Facilidad de mantenimiento.
- ◆ Durabilidad.
- ◆ Apariencia.
- ◆ Costo.
- ◆ 40 cm de elevación.
- ◆ Soportar carga (piso falso y piso firme).
- ◆ Falso plafón.
- ◆ Cableado aéreo.
- ◆ Extracción de aire (flujo).

- ◆ Conductos (canaletas) externos para cableado.
- ◆ Flujo de aire 15 ft³/min. por persona en ocupación constante.
- ◆ Temperatura: rango ideal 18 °C --> 22 °C. No es recomendable operar abajo de 10 °C ni arriba de 30 °C.
- ◆ Humedad relativa: 50 +- 10 % para evitar tanto condensación como electricidad estática. No es recomendable operar arriba de 80% ni abajo de 20%.

Consideraciones específicas para el cuarto de computadoras:

Espacio adecuado para:

- ◆ Operación y mantenimiento de Equipo.
- ◆ Mesas de trabajo y/o de transporte.
- ◆ Gabinetes de almacenamiento.
- ◆ Almacenamiento/Colocación temporal de discos, cintas y material impreso.
- ◆ Equipo de pruebas y personal de mantenimiento.
- ◆ Cables dentro de especificaciones (eléctricos y de datos).
- ◆ Panel de control eléctrico accesible y seguro.
- ◆ Alternar equipo ruidoso con silencioso.

6.4.PAA-013. ¿Existen salidas de emergencia?

- 6.4.GSA-013.**
- ◆ Realizar una inspección visual de todas las salidas de emergencia, su distribución, sus respectivos señalamientos para una rápida ubicación y que no se encuentren obstruidas.
 - ◆ Verificar si los cerrojos están en el interior o exterior y si se cuenta con las llaves para abrir o si hay personal que la abra oportunamente por ambos lados.

- 6.4.RC-013.**
- ◆ Las puertas de acceso a las salas de cómputo deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.
 - ◆ Las puertas del local serán de doble hoja y con una anchura total de 1.40 cm a 1.60 cm.
 - ◆ Es necesario una salida de emergencia.
 - ◆ Tener en cuenta las dimensiones máximas de los equipos si hay que atravesar puertas y ventanas de otras dependencias.

6.4.PAA-014. ¿Existen alarmas para detectar condiciones anormales del ambiente?

6.4.GSA-014. Enlistar todos los tipos y verificar si existen los siguientes mediante una inspección visual:

- ◆ Detectores de fuego (calor o humo) en forma automática o manuales.
- ◆ Detectores de fugas de agua.
- ◆ Detectores magnéticos.

Hacer un pequeño simulacro para verificar su potencia audible y en caso de las visibles si están a la vista de todos, sobre todo para el caso de personas con problemas auditivos y de visión.

Verificar si están conectadas a la estación de bomberos, al puesto de guardia o sólo dentro del CTI.

6.4.RC-014. Todas las áreas deben estar protegidas contra la introducción física.

Las alarmas contra robos, las armaduras y el blindaje se deben usar hasta donde sea posible, en forma discreta, de manera que no se atraiga la atención sobre el hecho de que existe un dispositivo de alta seguridad. La construcción de puertas y ventanas deben recibir especial atención para garantizar su seguridad.

Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente al departamento de bomberos.

6.4.PAA-015. ¿Saben qué hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionada por fuego?

6.4.GSA-015. Preguntar directamente con los operadores del equipo de cómputo el funcionamiento del equipo contra incendio, los tiempos de evacuación en caso de un siniestro por fuego. Se sugiere que realicen un simulacro en la presencia del auditor y registrar los tiempos y acciones de evacuación del local.

Enlistar todas las actividades a realizar después del siniestro, es posible que los especialistas sean los que evalúen los daños y comiencen con la recuperación sobre todo de la información y de los equipos.

6.4.RC-015. Determinar si las previsiones contra incendio del CTI están acordes con los estándares generalmente aceptados para tales medidas de protección, por ejemplo:

- ◆ Que no exista material combustible en las instalaciones de la sala de cómputo.
- ◆ Que los cableados eléctrico y de comunicaciones se encuentren protegidos con material aislante y bajo el piso falso.

- ◆ Que la parte inferior del piso falso se encuentre en buen estado y libre de polvo.
- ◆ Que exista un sistema contra incendio o que al menos haya extintores, así como verificar su vigencia.
- ◆ Que dentro de la sala de cómputo exista señalización de evacuación de emergencia y que se realicen simulacros de evacuación periódicamente.

Determinar a través de entrevistas con el administrador del CTI y sus colaboradores, qué tanto conocen y piensan que son adecuadas las medidas contra incendio del centro, comparadas contra los estándares generalmente aceptados.

Revisar ocasionalmente el seguro contra incendio de la organización, para verificar su vigencia.

6.4.PAA-016. ¿Existen extintores de fuego?

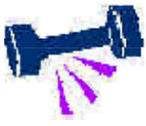
- 6.4.GSA-016.**
- ◆ Anotar la cantidad de estos equipos y verificar si son suficientes para cubrir toda el área del CTI.
 - ◆ Pedir las notas de mantenimiento de los equipos.

- 6.4.RC-016.**
- ◆ Verifique sus extintores.
 - ◆ Instale detectores de humo en áreas de alto riesgo o muy cerradas.
 - ◆ Coloque sistemas automáticos de rocío en áreas con mucho personal.
 - ◆ Revise las baterías de sus detectores de humo una vez al año.

Clasificación de los fuegos:

Se clasifican en función de su velocidad de ignición y según el combustible que los produce. Por su velocidad de ignición los fuegos pueden ser de:

- A: Ignición lenta.
- B: Ignición rápida.
- C, D: Ignición violenta.

Clasificación	Materiales involucrados en el fuego		Elementos para combatir el fuego
Clase A		Los ocasionados por combustibles sólidos ordinarios que producen brasas en su combustión, como la madera, papel, textiles, cartón, etc.	Agua presurizada. Espuma. Extintores de químico seco de uso múltiple.
Clase B		Los originados por combustibles líquidos como gasolina, aceites, petróleo, disolventes, derivados del petróleo, etc.	Dióxido de Carbono. Químico seco común. Extintores de uso múltiple de químico seco. Halón
Clase C		Son los fuegos de instalaciones y equipos eléctricos cuando están bajo tensión.	Dióxido de Carbono Químico seco común Extintores de fuego de halón Químico seco de uso múltiple
Clase D		Fuegos de metales químicamente muy activos (sodio, magnesio, potasio, etcétera), capaces de desplazar el hidrógeno del agua u otros componentes, originando explosiones por la combustión de éste.	Agentes extintores de polvo seco. Extintores de dióxido de Carbono y de halón.

La protección contra fuego es lograda de una mejor manera a través de una correcta construcción del edificio (el cual debe procurarse que sea resistente al fuego). Sin embargo, siempre habrá materiales combustibles y equipo dentro del edificio así que es necesario asegurar que el equipo contra incendio esté disponible de forma inmediata y que se pueda controlar el fuego con relativa facilidad.

Elementos necesarios que se consideran sobresalientes:

- ◆ Las paredes del área del equipo de cómputo deben de ser de material incombustible. Si el área del equipo de cómputo tiene una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles mejorará la seguridad.
- ◆ El techo falso debe ser de material incombustible o resistente al fuego.
- ◆ Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.
- ◆ El piso falso instalado sobre el piso real debe ser incombustible.
- ◆ El techo de la sala y el área de almacenamiento de discos y cintas magnéticas deben ser impermeables.
- ◆ Debe preverse un sistema de drenaje en el piso firme.
- ◆ Los detectores de fuego y humo se deben colocar cuidadosamente en relación con los aparatos de aire

- acondicionado, ya que los conductores de éste pueden difundir el calor o el humo y no permitir que se active el detector.
- ◆ El detector de humo que se elija debe ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y, en consecuencia, los incendios producidos por un circuito corto tal vez no se detecten.
 - ◆ Los detectores de humo y el calor se deben instalar en la sala de cómputo, junto a las áreas de oficina y dentro del perímetro físico de las instalaciones. Es necesario colocar detectores de humo y calor bajo el piso y en los ductos del aire acondicionado.
 - ◆ Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente al departamento de bomberos. Es importante que estos requerimientos no sólo se apliquen en la construcción de la sala de cómputo, sino también en las áreas adyacentes.
 - ◆ La documentación de los sistemas, la programación y las operaciones también necesitan protección contra incendios. La destrucción de esta documentación puede imposibilitar el uso de programas o archivos de respaldo. Se deben establecer procedimientos que garanticen la actualización de toda la documentación como rutina y que las copias de seguridad se almacenen en un lugar lejano, así como las copias de seguridad de los programas y los archivos.

6.4.PAA-017. ¿Sabe el personal del CTI qué hacer en caso de que ocurra un sismo?

6.4.GSA-017. Preguntar al personal qué hacer en caso de sismo y si las acciones coinciden con los estándares generalmente aceptados para tales medidas de protección. Realizar el simulacro de los operadores de cómputo y personal ajeno en la presencia del auditor y registrar los tiempos y acciones de evacuación del local.

- 6.4.RC-017.**
- ◆ Adquiera una póliza contra sismos.
 - ◆ Si es posible trate de tener un equipo de generación eléctrica, capaz de soportar sus necesidades básicas de cómputo, en un terremoto o temblor es de las primeras carencias.
 - ◆ Identifique tuberías de gas y agua que puedan pasar cerca de sus equipos, para evitar riegos por rupturas.
 - ◆ Instale sistemas de corte automático de energía en caso de sismo.
 - ◆ Asegure sus equipos para evitar movimientos o caídas durante el evento.
 - ◆ Mueva equipos pesados a ubicaciones bajas, para evitar incidentes en el evento.

- 6.4.PAA-018.** ¿Sabe el personal del CTI qué hacer en caso de una inundación?
- 6.4.GSA-018.** Preguntar al personal qué hacer en caso de una inundación. Realizar el simulacro de los operadores de cómputo y personal ajeno en la presencia del auditor y registrar los tiempos y acciones de evacuación del local. Cuidar los daños que pueden producir la energía eléctrica y el agua.
- 6.4.RC-018.** Las computadoras, máquinas y equipo en general no se deben colocar en sótano o en las áreas de planta baja sino, de preferencia, en las partes altas de una estructura de varios pisos.
- La ubicación de las tuberías en la construcción de las instalaciones de cómputo y equipo es una decisión importante no debe ponerse por encima de las áreas donde se colocan los equipos. Deben instalarse detectores de agua o de inundación, así como también bombas de emergencia para resolver inundaciones inesperadas.
- Puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente, se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso del agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.
- 6.4.PAA-019.** ¿Sabe el personal del CTI qué hacer en caso de huelgas, paros de actividades o toma de las instalaciones del edificio?
- 6.4.GSA-019.** Verificar si existe una lista de todas las actividades de resguardo inmediato de información vital, corte de suministro de energía de los equipos y comunicación a todo el personal para informar de centros alternos para seguir laborando.
- 6.4.RC-019.** El resguardo de los equipos será en la ubicación física de uso.
- Los equipos de misión crítica deberán contar con vigilancia y algún tipo de sistema que ayude a recabar evidencia de accesos físicos a las instalaciones.
- 6.4.PAA-020.** ¿En caso de interrupción de la energía eléctrica por parte de la suministradora de electricidad se cuenta con sistema de fuerza ininterrumpible?
- 6.4.GSA-020.** Si el CTI cuenta con un sistema de electricidad ininterrumpible, acudir a donde se encuentre y verificar su funcionamiento y que cumpla con las normas de energía necesarias para el equipo de cómputo e iluminación.

Revisar el tablero de interruptores y que cada uno de ellos tenga una leyenda de su función además de un cartel que explique todo el manejo del tablero de control.

6.4.RC-020.

Los interruptores de energía deben estar debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos.

Es uno de los aspectos fundamentales que deben cuidarse cuando se va a diseñar el CTI ya que, si no se efectúa un buen cálculo sobre la carga que se va a utilizar, esto nos ocasionaría serios problemas al utilizar el equipo. Por esto se requiere hacer un análisis sobre todos los equipos y dispositivos que se vayan a utilizar en el CTI como si fuesen a trabajar todos al mismo tiempo, así podremos obtener la carga máxima que se pudiera llegar a utilizar. Los equipos de cómputo son unos de los más sensibles a las variaciones de corriente eléctrica por lo tanto es necesario instalar equipos de protección.

Los requerimientos para el suministro eléctrico:

- ◆ Reguladores.
- ◆ Planta Eléctrica.
- ◆ Tierra Física. Instalación eléctrica que permite absorber descargar eléctricas, conformada por 1 varilla de cobre de 3 metros enterrados bajo el nivel del suelo y de preferencia en un lugar con humedad, complementados con sales y carbón para mejorar asimilación de descargas. No es conveniente usar castillos del edificio, ni tuberías.

Otros requerimientos:

- ◆ Minimizar vibraciones, disturbios electromagnéticos y ruido.
- ◆ Procurar iluminación y atmósfera adecuada para el personal.
- ◆ Recubrimientos acústicos.
- ◆ Interruptores seccionales de luz.
- ◆ Evitar luz solar directa.

6.4.PAA-021.

¿Qué medidas se toman en caso de que alguien pretenda entrar a alguna área sin autorización?

6.4.GSA-021.

Preguntar al personal si conocen a los vigilantes responsables de cada área o sabe a dónde acudir si existe alguna intromisión en el área no autorizada.

6.4.RC-021.

Se deberá tener un tipo de sanción dependiendo del tipo de falta que se realice, y deberá dirigirse al encargado del CTI.

- ◆ El personal que prepara los datos no debe tener acceso a las actividades de operación.

- ◆ Los analistas de sistemas y los programadores no deben tener acceso a las actividades de operación y viceversa.
- ◆ Los operadores no deben tener acceso irrestricto a las funciones de protección de información o departamentos donde se localicen los archivos maestros.
- ◆ Los operadores no deben tener los controles únicos del procesamiento del trabajo y se les debe prohibir que inicien las correcciones de los errores.

Lo ideal es tener un estricto control del acceso y préstamo, el control de los medios magnéticos debe ser llevado mediante inventarios periódicos.

Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.

6.4.PAA-022. Explique la forma como se ha clasificado la información vital, esencial, no esencial, etc.

6.4.GSA-022. Pedir un pequeño informe de la clasificación y la cantidad de dicha información.

6.4.RC-022. Toda la información almacenada deberá estar etiquetada y ordenada según su importancia.

Para mayor seguridad de que la información estará guardada bajo óptimas condiciones, deberá existir un lugar donde se almacenen las copias de la información.

El lugar de almacenamiento puede tener las siguientes características:

- ◆ Bóveda climatizada (temperatura y humedad).
- ◆ Capacidad de almacenamiento de todo tipo de dispositivos de almacenamientos, por ejemplo CDs y DVDs.
- ◆ Servicio los 365 días del año, 7x24.
- ◆ Sistema independiente automatizado de detección y extinción de incendios.

6.4.PAA-023. ¿Existen controles y medidas de seguridad sobre las operaciones de manejo de información? ¿Cuáles son?

6.4.GSA-023.

- ◆ Verificar si todos conocen al responsable de seguridad en caso de que alguien pretenda obtener información confidencial para reportarlo.
- ◆ Pedir una breve descripción de los controles y medidas de seguridad sobre cada uno de los siguientes puntos:
 - ◆ Recepción de documentos.
 - ◆ Información confidencial.

- ◆ Captación de documentos.
- ◆ Documentos de salida.
- ◆ Respaldo de la información.

- 6.4.RC-023.**
- ◆ Asegurar que el acceso a la información está restringido con la adecuada estratificación de niveles de acceso.
 - ◆ Determinar si los procedimientos prevén que las claves asignadas a los usuarios consideren el nivel de acceso para:
 - ◆ Equipos
 - ◆ Archivos
 - ◆ Programas de las aplicaciones
 - ◆ Comandos del sistema operativo, etc.
 - ◆ Verificar la existencia de la documentación mediante la cual se justificaron las asignaciones de claves de acceso a los equipos e información.
 - ◆ Verificar que existan procedimientos para la asignación de claves de acceso temporal o de emergencia. Determinar si es necesario obtener una autorización especial para este tipo de accesos y si este tipo de autorizaciones se limitan a un periodo dado y si se informa de ello a la administración.
 - ◆ Verificar que estos accesos temporales se concedan con poca frecuencia.

6.4.PAA-024. ¿Qué medidas se toman para las modificaciones de un programa?

- 6.4.GSA-024.**
- ◆ Si es necesaria una modificación mayor, verificar si es aprobada por el director del área o se sigue el mismo procedimiento a modificaciones menores.
 - ◆ Preguntar a algunas personas del área de informática si antes de que se les entregue el programa modificado se les envía una lista con dichas modificaciones y los nuevos requerimientos
 - ◆ Verificar fechas de la realización de las modificaciones.

6.4.RC-024. Con un formato es lo más ideal, para hacer cualquier tipo de petición para modificaciones, altas, cambios, etc., y se debe presentar al encargado del área.

Cada uno de estos formatos debe contener el tipo de modificación o requerimiento, la fecha y hora en que se creó y se modificó, además del nombre de las personas que lo solicitaron y de quien lo autorizó y aprobó.

6.4.PAA-025. ¿Cómo se da el acceso a las terminales o computadoras?

6.4.GSA-025. Verificar si es mediante identificación de nodos o terminales, usuario o no se pide identificación.

- 6.4.RC-025.** En caso de que los usuarios lleven su laptop, se les puede proporcionar un nodo en caso de que lo soliciten, con sólo presentar una identificación.
- 6.4.PAA-026.** ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
- 6.4.GSA-026.** Realizar una inspección visual al personal si alguien ingiere alimentos o bebidas y la existencia de anuncios que prohíban el consumo de alimentos o bebidas.
- 6.4.RC-026.** Contar con un área de consumo de alimentos que permita a los operadores consumir sus alimentos en un horario determinado.
- 6.4.PAA-027.** ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso y de los ductos de aire acondicionado (si existe)?
- 6.4.GSA-027.** Pedir notas de mantenimiento del aire acondicionado y verificar el piso falso visualmente.
- 6.4.RC-027.** Verificar el piso y los ductos del aire acondicionado. Tener programado cada cuanto tiempo es necesario limpiar los ductos, en todo caso recibir limpieza al menos una vez por semana, para que permita mantenerse libre de polvo.
- Se requiere el suministro de elementos indispensables para conformar un Sistema de Aire acondicionado de precisión ambiental, que cumpla con los estándares y normas internacionales ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers).

CAPÍTULO

VII

AUDITORÍA AL COMERCIO ELECTRÓNICO

CAPÍTULO VII

AUDITORÍA AL COMERCIO ELECTRÓNICO

7.1. Introducción al comercio electrónico

Las redes mundiales de información están transformando al mundo y acercando más a la gente a través de la innovación en las comunicaciones, lo cual posibilita cambios en todos los ámbitos de la actividad humana; por ejemplo, la competitividad, el empleo y la calidad de vida de las naciones. Con las nuevas tecnologías, el tiempo y la distancia dejan de ser obstáculos, los contenidos pueden dirigirse a una audiencia masiva o a un pequeño grupo de expertos y buscar un alcance mundial o meramente local.

Internet es un medio de comunicación global, que permite el intercambio de información entre los usuarios conectados a la red y que conecta a unos 8 millones de servidores encargados de servicios de información y de todas las operaciones de comunicación y de retransmisión; llega hasta unos 250 millones de usuarios en más de 100 países.

Internet ofrece un nuevo mercado que define la "economía digital". Los productores, proveedores de bienes/servicios y usuarios logran tener acceso y transmisión mundial de la información y esparcimiento en forma sencilla y económica, sea con fines comerciales o sociales.

En la práctica, las empresas están comenzando a usar Internet como un nuevo canal de ventas, sustituyendo las visitas personales, correo y teléfono por pedidos electrónicos, ya que gestionar un pedido por Internet cuesta menos que hacerlo por vías tradicionales.

Nace entonces el comercio electrónico, como una alternativa de reducción de costos y una herramienta fundamental en el desempeño empresarial.

La aparición del comercio electrónico obliga claramente a replantearse muchas de las cuestiones del comercio tradicional, surgiendo nuevos problemas, e incluso agudizando algunos de los ya existentes. Se plantean cuestiones que van, desde la validez legal de las transacciones y contratos sin papel, la necesidad de acuerdos internacionales que armonicen las legislaciones sobre comercio, el control de las transacciones internacionales, incluido el cobro de impuestos, la protección de los derechos de propiedad intelectual, la protección de los consumidores en cuanto a publicidad engañosa o no deseada, fraude, contenidos ilegales y uso abusivo de datos personales, hasta otros provocados por la dificultad de encontrar información en Internet, comparar ofertas y evaluar la fiabilidad del vendedor y del comprador en una relación electrónica, la falta de

seguridad de las transacciones y medios de pago electrónicos, la falta de estándares consolidados, la proliferación de aplicaciones y protocolos de comercio electrónico incompatibles y la congestión de Internet.

Nuestro país carece en el presente, de una normativa jurídica en relación con el comercio electrónico y el formato digital para la celebración de actos jurídicos. En el contexto mundial, nuestro país se encuentra desactualizado.

La observación de la tendencia mundial permite considerar oportuno el tratamiento normativo, siendo también necesario el dominio de los aspectos técnicos que permitan brindar una regulación que viabilice una solución para una problemática concreta y contemporánea, conforme a los estándares internacionales.

7.2. Concepto de uso frecuente del comercio electrónico

El comercio electrónico es una metodología moderna para hacer negocios que detecta la necesidad de las empresas, comerciantes y consumidores para reducir costos, así como mejorar la calidad de los bienes y servicios, además de mejorar el tiempo de entrega de los mismos. No debe seguirse contemplando el comercio electrónico como una tecnología, sino que es el uso de la tecnología para mejorar la forma de llevar a cabo las actividades empresariales.

El comercio electrónico se puede entender como cualquier forma de transacción comercial en la cual las partes involucradas interactúan de manera electrónica en lugar de hacerlo de la manera tradicional con intercambios físicos o trato físico directo.

En la actualidad la manera de comerciar se caracteriza por el mejoramiento constante en los procesos de abastecimiento, y como respuesta a ello los negocios a nivel mundial están cambiando tanto su organización como sus operaciones. El comercio electrónico es el medio de llevar a cabo dichos cambios dentro de una escala global, permitiendo a las compañías ser más eficientes y flexibles en sus operaciones internas, para así trabajar de una manera más cercana con sus proveedores y estar más pendiente de las necesidades y expectativas de sus clientes.

7.3. Obligaciones de información

Los proveedores que trabajen con comercio electrónico deberán proveer a los consumidores de información clara, correcta y de fácil acceso sobre sí mismos, suficiente para permitir, como mínimo:

- 1) **La identificación del proveedor** - incluyendo el nombre legal del proveedor y el nombre bajo el cual desarrolla sus actividades comerciales; el domicilio principal del proveedor; la dirección de correo electrónico u otra forma electrónica de contacto, o un número telefónico.
- 2) **Una comunicación del consumidor con el proveedor** que sea rápida, sencilla y efectiva.

- 3) **Un sistema de solución de conflictos** que sea apropiado y efectivo
- 4) **El procedimiento legal**
- 5) **La ubicación del proveedor y sus funcionarios** para conocimiento de los funcionarios reguladores y los encargados de control.

7.4. Contenidos

Dentro de la empresa se debe contar con un formulario de comunicación de contenidos ilícitos con objeto de:

- 1) Ofrecer al cliente la posibilidad de informar sobre contenidos ilícitos, perjudiciales, ofensivos, etc.
- 2) Crear pruebas de que la empresa ha puesto todo su empeño en evitar la difusión de contenidos ilícitos.

7.5. Comunicaciones comerciales

Para evitar la ambigüedad relacionada con el intento de parte del consumidor de realizar una transacción, se deberá poder, antes de finalizar la transacción, identificar en forma precisa los bienes y/o servicios que se deseen comprar; identificar y corregir cualquier error o modificar la orden de compra, expresar un consentimiento informado y concreto de la compra, y mantener exacto y completo un archivo de la transacción.

El consumidor deberá poder cancelar la transacción antes de finalizar la compra.

El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo por la autorización del propio consumidor o por requerimiento de una autoridad judicial.

El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales (si es el caso), y formas de pago de los bienes y servicios ofrecidos por el proveedor.

7.6. Contratación electrónica

En mayo de 2000 entraron en vigor reformas al hoy Código Civil Federal (CC), Código de Comercio (CCom), Código Federal de Procedimientos Civiles (CFPC) y Ley Federal de Protección al Consumidor (LFPC). Su finalidad es habilitar la contratación electrónica, de manera que los acuerdos celebrados por medios electrónicos ópticos o cualquier otra

tecnología pudieran considerarse legalmente válidos, plenamente obligatorios y exigibles entre las partes que concurrieron a su celebración.

La adopción de un lenguaje universal y uniforme en nuestra legislación fue un acierto del legislador mexicano, pues sentó las bases para lanzar una plataforma sostenible de negocios electrónicos mexicanos en un aspecto global. La red de redes no toma muy en cuenta las divisiones geopolíticas y que por consecuencia cualquier jurisdicción que decida separarse de los estándares y reglas uniformes aceptadas internacionalmente está condenada a la disminución de su comercio, con las consecuencias que ello implica para su economía local.

Con el objeto de mantener nuestras leyes en armonía con el resto del mundo, los términos de la reforma necesitan ser lo suficientemente generales y amplios como para mantener uniformidad con legislaciones de otros países. Sin embargo, también son necesarios lineamientos y reglas que permiten aplicar e interpretar esta legislación.

La contratación electrónica presenta varias fases que comprenden, el consentimiento en la red y el lugar de celebración.

Los efectos jurídicos son distintos si la contratación es entre empresas o entre éstas y los consumidores.

Se puede decir que la modalidad de la contratación electrónica se da en dos formas:

- 1) Con el proveedor de acceso a Internet.
- 2) Con el proveedor de bienes y servicios a través de la red.

En el primero, el consumidor celebra un contrato con el proveedor que le da acceso a Internet, quien por un pago mensual, le asigna una dirección (dominio) y que es individual a través de un signo o palabras suministradas por el usuario. Con esto se tiene derecho a recibir y enviar información por correo electrónico con carácter de exclusiva. Asimismo tiene acceso a una página de presentación donde suministra información en forma pública y sin restricciones, recibiendo también comunicaciones electrónicas.

En el segundo, el usuario ingresa a Internet libremente visitando distintos sitios, recabando información y pudiendo contratar, configurándose de esta forma el contrato electrónico.

En el contrato electrónico se da el intercambio de información entre personas que da como resultado una relación comercial, con la finalidad de la entrega de bienes intangibles o tangibles.

La contratación electrónica por medios digitales es la que se lleva a cabo desde la formación del consentimiento hasta la ejecución del contrato, mediante dispositivos de enlaces electrónicos que se comunican interactuando canales de red basados en el procesamiento y transmisión de datos digitalizados, con el fin de crear, modificar, transferir, conservar o aniquilar derechos.

El contrato electrónico es un contrato a distancia. Por ello es necesario definir si se trata de un contrato celebrado entre personas físicamente presentes o entre ausentes.

En las contrataciones por teléfono, la doctrina ha considerado separadamente el momento y el lugar de celebración. Con el uso del teléfono la comunicación es instantánea, por lo que se considera que es entre presentes. En cambio, con relación al lugar, como las personas están físicamente distantes, el contrato es regido por las normas relativas a la contratación entre ausentes.

En este caso hay una distancia geográfica que se traduce en un tiempo de comunicación jurídicamente relevante, pero el medio utilizado neutraliza la geografía, ya que la comunicación es instantánea.

El lugar de celebración del contrato tiene efectos importantes para fijar la competencia; la ley que se le aplica; el carácter nacional o internacional del contrato y para interpretarlo conforme los usos y costumbres. En la mayoría de los casos que presentan conflictos se tiene un lugar de celebración y cumplimiento fijados, pero las relaciones virtuales tienden a ser autónomas por su configuración de sistema, lo que hace que en algunos sectores, el lugar sea virtual.

El lugar de los contratos en las relaciones globales es una cuestión de atribución de efectos jurídicos y no de determinar quien vive en ese lugar o si estuvo presente o no en la celebración o ejecución del contrato.

Un lugar jurídico puede ser un nombre de dominio, que no coincida con el lugar real donde efectivamente esté el sujeto. La noción de lugar es un concepto normativo.

7.7. Responsabilidad civil

Los proveedores que utilicen el comercio electrónico deberán prestar atención a los intereses de los consumidores y actuar de acuerdo con un comercio, una publicidad y prácticas de marketing honestas.

Los proveedores no realizarán manifestación alguna u omisión, o realizarán ninguna práctica que pueda ser falsa, engañosa, fraudulenta o abusiva.

La publicidad y el marketing deberán ser claramente identificados como tales.

La publicidad y el marketing identificarán al proveedor para el cual tales actividades se realizan, y la falta de tal identificación se considerará como engañosa.

Los proveedores que vendan, promuevan o realicen marketing de bienes o servicios a los consumidores no efectuarán prácticas que puedan causar riesgo o daño a los consumidores.

Cuando los proveedores entreguen información sobre ellos mismos, o los bienes o servicios que proveen, deben presentar esa información de manera que sea clara, certera y fácilmente accesible.

Los proveedores deberán observar, en cada manifestación que hagan, las políticas o prácticas relacionadas con sus transacciones con los consumidores.

Los proveedores deben tener en cuenta la naturaleza global del comercio electrónico y, siempre que sea posible, deberán considerar las variadas características que regulan los mercados a que ellos apuntan.

Los proveedores no explotarán las características especiales del comercio electrónico para ocultar su identidad o ubicación real, o para evitar cumplir con los estándares de protección del consumidor y los mecanismos de aplicación.

Los proveedores no usarán términos contractuales abusivos.

Los proveedores desarrollarán e implementarán procedimientos efectivos y fáciles de utilizar que permitan a los consumidores elegir si desean o no recibir mensajes comerciales a través del correo electrónico.

El robo o "fraude de identidad" es un delito por medio del cual alguien obtiene y utiliza datos e información personal de un tercero de manera fraudulenta. Se recomienda tener cuidado con la información bancaria y de cuentas de tarjetas de crédito, débito y departamentales, reforzando contraseñas, cambiándolas regularmente, así como revisar constantemente las cuentas bancarias.

Se debe tener responsabilidad por información falsa o perjudicial que se mencione o publique en Internet sobre personas o compañías, ya que podrían emprender alguna acción legal.

En cuestión de la responsabilidad de los intermediarios, en particular de los proveedores de alojamiento, es una de las más delicadas. De lo que se trata es determinar en qué medida pueden ser responsables los intermediarios técnicos de contenidos ilegales y nocivos publicados en su red o en su servidor.

Para poner fin a la incertidumbre jurídica existente, se excluye de toda responsabilidad a los intermediarios que desempeñan un papel pasivo encargándose del simple "transporte" de información procedente de terceros.

Del mismo modo, limita la responsabilidad de los prestadores de servicios por otras actividades intermedias, tales como el almacenamiento de información.

En otras palabras, los proveedores de infraestructura o de acceso no podrán ser considerados responsables de la información transmitida, siempre que no sean ellos los originarios de la misma y no seleccionen el destinatario de la transmisión o de la información seleccionada.

7.8. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

- 7.8.PAA-001.** ¿La empresa que proporciona el servicio cuenta con información clara y suficiente sobre ellos mismos en su página de Internet?
- 7.8.GSA-001.** Verificar que en la página de Internet se encuentre la información sobre el nombre de la empresa así como también de su ubicación.
- 7.8.RC-001.** En el caso de que la empresa proporcione los datos anteriormente señalados deberá indicar un número telefónico real y no proporcionar un buzón de correo postal.
- 7.8.PAA-002.** ¿La empresa cuenta con sistema de devolución en caso de proporcionar algún producto defectuoso?
- 7.8.GSA-002.** Revisar que la empresa cuente con la opción para que el cliente pueda devolver el o los productos en caso de que presenten fallas o defectos, o si el cliente manifestó un tipo de desconfianza o inconformidad en los productos.
- 7.8.RC-002.** Es necesario proporcionar la dirección del lugar para poder llevar el producto defectuoso, así como también que pueda ponerse en contacto con una persona para hacer las aclaraciones posibles respecto a la inconformidad del producto, no sólo con una computadora.
- 7.8.PAA-003.** ¿Se proporciona una garantía en el momento de adquirir un producto o servicio?
- 7.8.GSA-003.** El auditor revisará que se estipule alguna garantía y bajo qué condiciones es válida.
- 7.8.RC-003.** La garantía que ofrecen realmente la puedan hacer efectiva, y que no tenga que cruzar el cliente el mundo entero para que la reconozcan.
- 7.8.PAA-004.** ¿Se presenta la opción de un “almacén virtual”?
- 7.8.GSA-004.** Se verificará que dentro del portal exista la opción para ingresar en un almacén virtual, así como también para poder localizar el área en donde se escriben las preguntas más frecuentes. FAQ (Frequently Asked Questions)
- 7.8.RC-004.** La empresa deberá satisfacer al cliente, mediante las preguntas más frecuentes, la curiosidad sobre términos comerciales, garantías,

procedimiento para entrega, y procedimiento para devolución, así como también facilidad en el proceso de compra.

- 7.8.PAA-005.** ¿La empresa maneja confidencialidad en el momento de recibir preguntas extras del cliente?
- 7.8.GSA-005.** Revisar que cuando se envíe una pregunta a la dirección de correo electrónico no sea necesario proveer información personal sobre el cliente.
- 7.8.RC-005.** Se le pide a la empresa que para poder enviar preguntas adicionales no sea obligación que el cliente proporcione datos de su persona.
- 7.8.PAA-006.** ¿Se cuenta con la opción para llenar un formulario de contenidos ilícitos?
- 7.8.GSA-006.** Se revisará si existe un apartado para denunciar la posible existencia de contenido ilícito que perjudique física o moralmente al cliente que visite el sitio.
- 7.8.RC-006.** Si se desea obtener buena reputación se debe contar con un apartado ya que así no se fomenta la difusión de contenidos ilícitos.
- 7.8.PAA-007.** ¿El proveedor de acceso es responsable de la información transmitida?
- 7.8.GSA-007.** El auditor confirmará que el proveedor de infraestructura o de acceso no sea responsable de la información transmitida, siempre que no sean ellos los originarios de la misma y no seleccionen el destinatario de la transmisión o de la información considerada.
- 7.8.RC-007.** Los proveedores de alojamiento deberán comunicar a las autoridades competentes información que permita identificar a los propietarios de las páginas alojadas.
- 7.8.PAA-008.** ¿El consumidor tiene la posibilidad de conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, (en su caso), y formas de pago de los bienes y servicios ofrecidos por el proveedor?
- 7.8.GSA-008.** Verificar que los bienes y servicios ofrecidos por el proveedor cuenten con toda la información sobre términos, condiciones, costos, cargos adicionales y formas de pago de bienes y servicios.
- 7.8.RC-008.** La información presentada tiene que estar en un formato entendible y que proporcione todas las condiciones para que sea una transacción lo más transparente posible.

- 7.8.PAA-009.** ¿Los contratos informáticos cuentan con los elementos llamados complementarios?
- 7.8.GSA-009.** Se deberá comprobar que en dichos contratos se mencione el contratante, parte expositiva, cláusulas o pactos y anexos
- 7.8.RC-009.** Es de vital importancia que los elementos complementarios que conforman el contrato sean claros, bien definidos, para que no existan problemas de confusión entre la parte contratante y la que provee el servicio.
- 7.8.PAA-010.** ¿Se descubren fraudes en el comercio electrónico y van más allá de los niveles fronterizos a los cuales está afectando?
- 7.8.GSA-010.** Notificar a las agencias encargadas de vigilar el cumplimiento de las leyes de protección al consumidor, correspondientes a los territorios afectados, tomen las acciones que correspondan en contra de las prácticas fraudulentas.
- 7.8.RC-010.** Los países miembros trabajarán con la finalidad de permitir que sus agencias encargadas de vigilar el cumplimiento de las leyes de protección al consumidor emprendan acciones en contra de proveedores nacionales que se dediquen a las prácticas fraudulentas y engañosas en contra de los consumidores extranjeros; así como también proveedores extranjeros con el mismo tipo de prácticas en contra de sus propios consumidores. De igual manera los países miembros buscarán promover la cooperación de terceras partes tales como instituciones financieras y órganos encargados del registro del nombre del dominio con la finalidad de detener las prácticas comerciales transfronterizas fraudulentas y engañosas.
- 7.8.PAA-011.** ¿El proveedor pertenece a un esquema de autorregulación, una asociación de proveedores, una organización de resolución de conflictos u otro órgano de certificación?
- 7.8.GSA-011.** Revisar que el proveedor pertenezca a un tipo de esquema
- 7.8.RC-011.** El proveedor deberá informar a los consumidores los detalles apropiados y un método sencillo para verificar tal pertenencia, y contar con un fácil acceso a las reglas y las prácticas de esos organismos.
- 7.8.PAA-012.** Al manejar publicidad, ¿se maneja de forma adecuada?
- 7.8.GSA-012.** Verificará el auditor que la publicidad y el marketing estén claramente identificados.

La publicidad y el marketing identificarán al proveedor para el cual tales actividades se realizan, y la falta de tal identificación se considerará como engañosa.

- 7.8.RC-012.** Los proveedores desarrollarán e implementarán procedimientos efectivos y fáciles de utilizar que permitan a los consumidores elegir si desean o no recibir mensajes comerciales (publicidad) a través del correo electrónico.
- Cuando los consumidores indiquen que no desean recibir mensajes comerciales a través del correo electrónico, esa elección debe ser respetada.
- Los proveedores deberán tener especial cuidado en la publicidad y el marketing que está destinado a los menores, la tercera edad, los enfermos graves, y otros que no tengan la capacidad de entender plenamente la información que les es mostrada.
- 7.8.PAA-013.** ¿El proceso de confirmación en una transacción evita ambigüedades?
- 7.8.GSA-013.** Para evitar ambigüedades se revisará que el proveedor liste de forma precisa los bienes y servicios que el cliente desee adquirir; que se pueda identificar y corregir cualquier error o la posible modificación en la orden de compra.
- 7.8.RC-013.** Se debe poder expresar un consentimiento informado y concreto de la compra, y mantener un completo y exacto archivo de la transacción.
- Es recomendable se pueda cancelar la transacción, al no estar seguro de ella antes de concluir la compra.
- 7.8.PAA-014.** ¿Su sistema de resolución alternativa de conflictos funciona?
- 7.8.GSA-014.** Se revisará que el acceso real a mecanismos alternativos de resolución de conflictos no sea tardado, además que no implique algún costo indebido o una carga.
- 7.8.RC-014.** Los proveedores, los consumidores y los gobiernos deben trabajar en forma conjunta para continuar desarrollando y utilizando políticas, procedimientos y autorregulaciones que sean justas, efectivas y transparentes, incluyendo mecanismos alternativos para la resolución de conflictos, asumir los reclamos de los consumidores y resolver las disputas que surjan en las transacciones de comercio electrónico entre

consumidores y proveedores, con especial atención de las transacciones transfronterizas.

- 7.8.PAA-015.** ¿Se proporciona el servicio de talleres de reparación?
- 7.8.GSA-015.** Se revisará que el servicio a los talleres de reparación sea de fácil acceso al consumidor.
- 7.8.RC-015.** Los talleres de reparación deben proporcionar de manera clara las políticas de su servicio y también que su mecanismo de acceso no sea complicado.
- 7.8.PAA-016.** ¿El proceso de contratación electrónica es completo?
- 7.8.GSA-016.** Verificar que el proceso consista de: oferta, aceptación y acuse de recibo, sin embargo en los contratos celebrados por correo electrónico el acuse de recibo también será por la misma vía.
- 7.8.RC-016.** En este tipo de contratos es recomendable que exista un tiempo relevante entre la oferta y la aceptación, porque hay posibilidad de que ocurran riesgos, y que pueden ser, la muerte, la incapacidad o la quiebra, del oferente o del aceptante, o la retractación.
- 7.8.PAA-017.** En el caso de que el cliente confirme la celebración del contrato electrónico ¿el oferente confirma la recepción de la aceptación?
- 7.8.GSA-017.** Verificar que la empresa tenga la capacidad de confirmar la aceptación de su cliente, pidiéndole algún tipo de documento, ya sea bitácora o registro que lo compruebe.
- 7.8.RC-017.** El oferente se obliga a confirmar la recepción de la aceptación al que la hizo. El envío del acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente, debe ser a la dirección que el aceptante haya señalado.
- 7.8.PAA-018.** ¿El objeto que se pretende comercializar se encuentra dentro del mercado?
- 7.8.GSA-018.** Checar que dentro del amplio mercado de productos, se encuentre en existencia y que sea posible comercializarlo.

- 7.8.RC-018.** El objeto dentro del comercio debe ser susceptible de apropiación por permitirlo la naturaleza o la ley.
- 7.8.PAA-019.** ¿Se encuentra dentro de la posibilidad jurídica el objeto?
- 7.8.GSA-019.** Revisar si es posible la comercialización del producto de acuerdo con la disposición expresada en la ley, dentro del territorio al cual corresponda.
- 7.8.RC-019.** Sería recomendable que cada oferente diera la indicación que posiblemente en otro territorio los actos conjurados entre las dos partes (oferente y contratante) no serían bien vistas por la ley.
- 7.8.PAA-020.** ¿Se menciona la hora y el lugar de la contratación en el contrato electrónico?
- 7.8.GSA-020.** Se verificará que en el contrato electrónico aparezcan tanto la hora como el lugar de la contratación.
- 7.8.RC-020.** Es vital dentro de un contrato electrónico aparezcan la hora y lugar de contratación, ya que identifica, entre otras cosas, el momento de la transferencia de propiedad en el caso de venta, así como la ley aplicable al contrato y la jurisdicción competente para atender las controversias que surgieran.
- 7.8.PAA-021.** ¿Cuénta con sellos temporales?
- 7.8.GSA-021.** Solicitar al proveedor indique quién es el tercero que proporciona un sello temporal.
- 7.8.RC-021.** Para que la validez y la confiabilidad de un contrato sean mayores es necesario que cuente con la garantía de un sello temporal.
- 7.8.PAA-022.** ¿Es segura la utilización de la firma electrónica?
- 7.8.GSA-022.** Verificar que la firma electrónica esté avalada por una empresa de certificación.
- 7.8.RC-022.** Los certificados deberán contener una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad que certifica, el número de serie del certificado y la firma digital del que otorga.
- 7.8.PAA-023.** ¿El proceso para la resolución de conflictos comerciales es el indicado?

- 7.8.GSA-023.** Revisar que en la resolución de conflictos se maneje el proceso de arbitraje.
- 7.8.RC-023.** En el proceso de arbitraje las partes deben someterse a él mediante una cláusula o convenio arbitral que esté contenido en un contrato. El arbitraje debe proporcionar agilidad, eficacia y especialización en la materia.
- 7.8.PAA-024.** ¿Las ventas no han resultado como se esperaba?
- 7.8.GSA-024.** Revisar que la empresa cuente con un buen historial de reputación de clientes que anteriormente hicieron una compra, y también que se tenga en constante innovación su mercado de productos.
- 7.8.RC-024.** Los proveedores deben competir por innovar y mantener cautivo a su nicho de mercado, las ventas crecerán de manera sólida.
- 7.8.PAA-025.** Si se utiliza algún tipo de estrategia de ventas, ¿ésta funciona adecuadamente?
- 7.8.GSA-025.** Se analizará que la estrategia de venta empleada proporcione información clara y suficiente sobre los servicios ofrecidos.
- 7.8.RC-025.** Se recomienda que la mercadotecnia dirigida a la población vulnerable, como los niños, ancianos y enfermos incorpore mecanismos que adviertan cuando la información no sea apta para ese tipo de población.
- 7.8.PAA-026.** ¿Se tiene la posibilidad de realizar la transacción en más de un idioma?
- 7.8.GSA-026.** El auditor verificará que el proveedor presente la información sobre las transacciones en los idiomas disponibles.
- 7.8.RC-026.** Los proveedores deberán proveer a los consumidores el texto completo y claro de las condiciones y términos de la transacción, de forma que haga posible a los consumidores acceder y mantener un registro de tal información.
- 7.8.PAA-027.** ¿La información de la transacción contiene todo lo necesario?
- 7.8.GSA-027.** Verificar que dentro de la transacción se establezcan los siguientes puntos:

Los costos totales e impuestos cobrados por el proveedor.

Información sobre la existencia de otros costos de rutina que no sean los cobrados o los impuestos recolectados por el proveedor.

Los plazos de entrega o cumplimiento del servicio, términos, condiciones y métodos de pago, restricciones, limitaciones o condiciones de la compra, tales como el requisito de aprobación de la misma por parte de los padres o tutores, restricciones geográficas o de tiempo, Instrucciones de uso, incluyendo alertas de seguridad y cuidado de la salud, información sobre la existencia de servicios después de la venta, los detalles y las condiciones referidas a la información sobre política de retracto, cancelación, retorno, cambio, terminación y reembolso, y finalmente las garantías disponibles.

- 7.8.RC-027.** Toda la información sobre costos deberá indicar la moneda aplicable a la transacción.
- 7.8.PAA-028.** ¿Los mecanismos de pago con los que se cuenta son adecuados?
- 7.8.GSA-028.** Analizar que los mecanismos de pago sean fáciles de utilizar y sean seguros, así como también se indique la información del grado de seguridad de tales mecanismos.
- 7.8.RC-028.** Los mecanismos de reembolso ofrecen una herramienta poderosa para aumentar la confianza del consumidor, su desarrollo y uso debe ser apoyado para el comercio electrónico.
- 7.8.PAA-029.** ¿El portal de comercio electrónico cuenta con derechos de autor?
- 7.8.GSA-029.** Se debe verificar que cuente con los permisos o licencias correspondientes para no vulnerar derechos de terceros.
- 7.8.RC-029.** La legislación que se aplicará será la ley federal de derechos de autor, y se deberá cuidar que el material mostrado en el sitio sea original.
- 7.8.PAA-030.** ¿Proporciona la opción de comprobantes fiscales?
- 7.8.GSA-030.** Revisar que sea posible la obtención de un comprobante fiscal como lo es la factura electrónica.
- 7.8.RC-030.** Se recomienda se encuentre disponible el uso de estos procedimientos, porque puede llegar a representar una reducción del 50% de los costos en la administración.
- Incrementa las ventas debido a que se le proporciona una factura electrónica al cliente.

CAPÍTULO

VIII

AUDITORÍA AL DATA WAREHOUSE (DW)

CAPÍTULO VIII

AUDITORÍA AL DATA WAREHOUSE (DW)

8.1. Introducción

En la actualidad, los sistemas se han concentrado en lo transaccional, generando una mayor eficiencia en los procesos y la posibilidad de un mayor control a nivel operativo.

La optimización de los flujos de trabajo a través de la implementación de sistemas ERP (*Enterprise Resource Planning*) así como el aumento del número de transacciones por las posibilidades del comercio electrónico, continuamente generan enormes volúmenes de datos internos y externos a la organización, cuyo almacenamiento y análisis representa nuevos desafíos tecnológicos.

Por otro parte, existen nuevas ideas en la forma de hacer negocios, como resultado de cambios en la conducta de los consumidores, la dinámica de los mercados y la alta competitividad a nivel global. El marketing ya no puede orientarse a los productos y menos a los mercados, y debe adaptarse a las necesidades de cada cliente. La creciente globalización implica que el mercado ya no es el sencillo entorno local, sino la complejidad del planeta entero, con sus diferencias culturales y sociales.

Este gran volumen de datos, así como las nuevas reglas de negocios, implican nuevos desafíos, pero a la vez importantes oportunidades. Para aprovecharlas, las empresas han concentrado grandes recursos en un nuevo concepto tecnológico: *data warehousing*.

Data warehousing es el proceso mediante el cual las empresas extraen sentido y significado a sus datos a través del uso de un almacén de datos, o *data warehouse*.

El término *data warehouse* es usado con frecuencia para designar a cualquier sistema nuevo que sirve para almacenar información, un *data warehouse* es un conjunto de datos integrados, no transaccionales, no volátiles, orientados a un tema específico, variables en el tiempo y que se utiliza para el apoyo al proceso de toma de decisiones.

El proceso de *data warehousing* debe orientarse a proveer la información correcta, a la persona indicada, en el formato adecuado, y en el tiempo preciso.

Alrededor de este almacén de datos se localizan las funciones que permiten el procesamiento analítico de la información, convirtiéndola en conocimiento con el cual se pueden hacer cosas, o sea, conocimiento útil. Entre ellas están las posibilidades de generar reportes no estructurados, la visualización de los datos, el reconocimiento de patrones, el resumen de datos y su rotación de acuerdo con las variables de interés, el análisis de hipótesis, etc.

8.2. Concepto de Data Warehouse

Un Data Warehouse o **Almacén de Datos** es una colección de datos orientado a temas, integrado, no volátil, de tiempo variante, que se utiliza para el soporte del proceso de toma de decisiones gerenciales

No obstante si el Data Warehouse fuese exclusivamente un almacén de datos, los problemas seguirían siendo los mismos que en los Centros de Información.

La ventaja principal de este tipo de sistemas se basa en su concepto fundamental, la estructura de la información. Este concepto significa el almacenamiento de información homogénea y fiable, en una estructura basada en la consulta y el tratamiento jerarquizado de la misma, y en un entorno diferenciado de los sistemas operacionales.

Base de Datos Operacional	Data Warehouse
Datos Operacionales	Datos del negocio para Información
Orientado a la aplicación	Orientado al sujeto
Actual	Actual + histórico
Detallada	Detallada + más resumida
Cambia continuamente	Estable

El data warehouse es siempre un almacén de datos transformados y separados físicamente de la aplicación donde se encontraron los datos en el ambiente operacional.

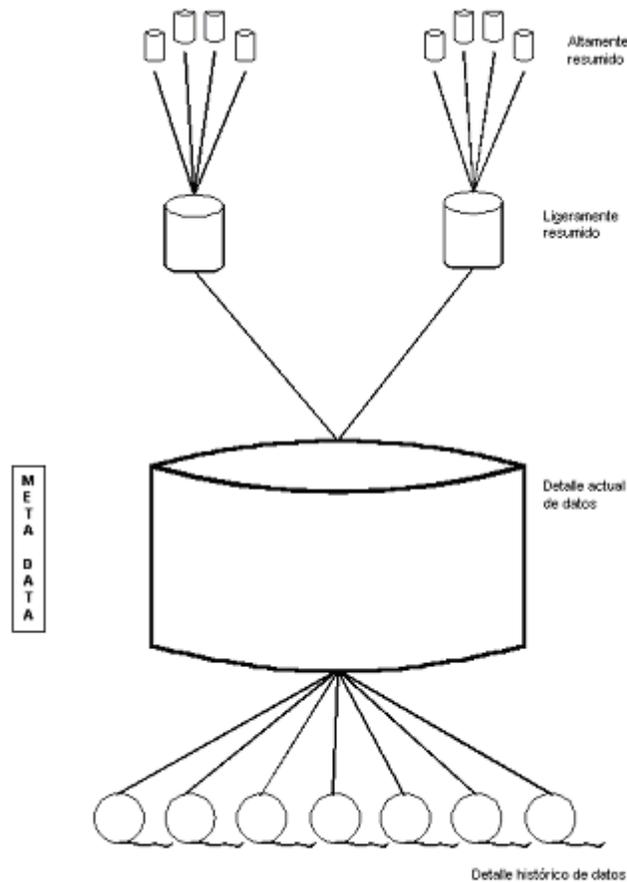


Fig. 8.1. Estructura de los datos en un Data Warehouse

La figura 8.1. Representa la estructura de los datos dentro de un Data Warehouse y así obtener el grado de detalle que deseemos al realizar una consulta

8.3. Características de un Data Warehouse

Entre las principales características de un Data Warehouse se tienen:

- ◆ Orientado al tema
- ◆ Integrado
- ◆ De tiempo variante
- ◆ No volátil

Orientado al tema

La información se clasifica con base en los aspectos que son de interés para la empresa.

Integración

La integración de datos se muestra de diversas maneras: en convenciones de nombres consistentes, en la medida uniforme de variables, en la codificación de estructuras consistentes, en atributos físicos de los datos consistentes, fuentes múltiples y otros.

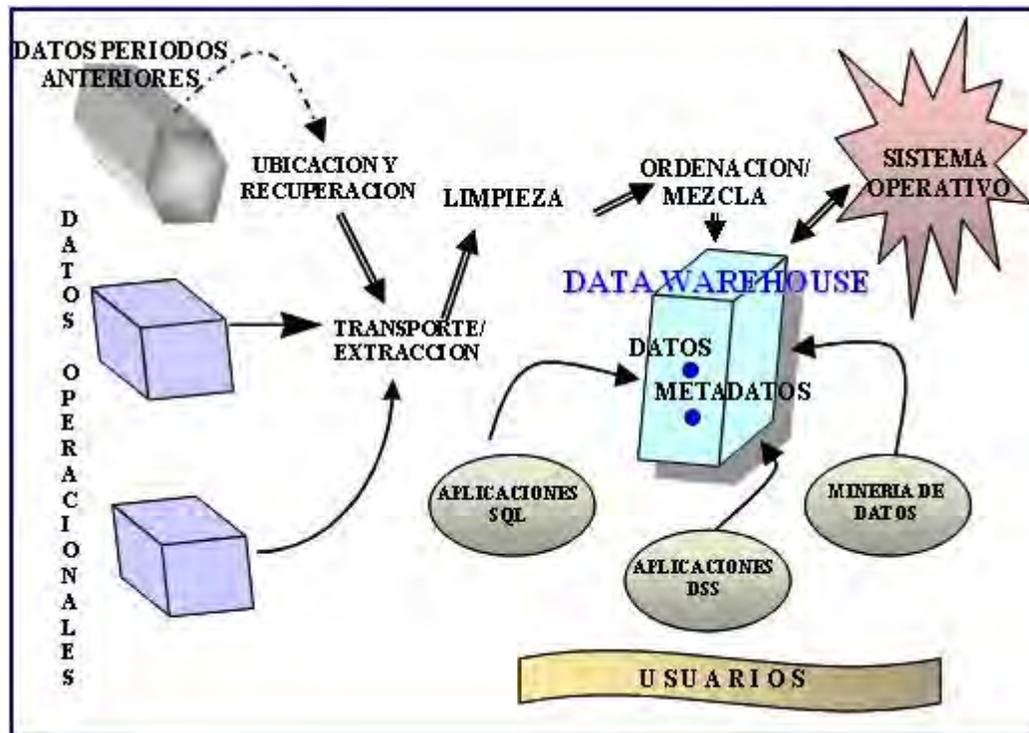


Fig 8.2. Ambiente de Data Warehousing.

En la figura 8.2. los datos provenientes de bases de datos operacionales y otros datos, son pasados a través de un proceso de transporte y extracción, para de esta forma, obtenerlos “limpios”. Posteriormente son sometidos a un proceso de ordenación y mezcla para enviarlos dentro del Data Warehouse. Los usuarios finales utilizan diferentes tipos de aplicaciones y herramientas dependiendo del tipo de datos que requieran.

De tiempo variante

Toda la información del data warehouse es requerida en algún momento. Esta característica básica de los datos en un almacén, es muy diferente de la información encontrada en el ambiente operacional. En éstos, la información se requiere al momento de acceder. En otras palabras, en el ambiente operacional, cuando se accede a una unidad de información, se espera que los valores requeridos se obtengan a partir del momento de acceso.

No volátil

La información es útil sólo cuando es estable. Los datos operacionales cambian sobre una base momento a momento. La perspectiva más grande, esencial para el análisis y la toma de decisiones, requiere una base de datos estable.

8.4. Elaboración de un Data Warehouse.

No existe una fórmula que garantice el éxito de la construcción de un data warehouse, pero hay muchos puntos que contribuyen con dicho objetivo.

A continuación, se indican algunos puntos claves que deben considerarse en la planificación de un data warehouse:

1. Establecer una asociación de usuarios, gestión y grupos

Involucrar tanto a los usuarios como a la gestión para asegurar que el data warehouse contenga información que satisfaga los requerimientos de la empresa.

2. Seleccionar una aplicación piloto con una alta probabilidad de éxito

Una aplicación piloto de alcance limitado, con un reembolso medible para los usuarios y la gestión, establecerá el data warehouse como una tecnología clave para la empresa.

3. Construir prototipos rápida y frecuentemente

La única manera para asegurar que el data warehouse reúna las necesidades de los usuarios, es hacer el prototipo a lo largo del proceso de implementación y aún más allá, así como agregar los nuevos datos y/o los modelos en forma permanente.

4. Implementación incremental

La implementación incremental disminuye riesgos y asegura que el tamaño del proyecto permanezca manejable en cada fase.

5. Reportar activamente y publicar los casos exitosos

La realimentación de los usuarios ofrece una excelente oportunidad para publicar los hechos exitosos dentro de una organización. La publicidad interna sobre cómo el data warehouse ha ayudado a los usuarios a operar más efectivamente puede apoyar la construcción del data warehouse a lo largo de una empresa.

Antes de desarrollar un data warehouse es crítico el desarrollo de una estrategia equilibrada que sea apropiada para sus necesidades y sus usuarios.

Las preguntas que deben tenerse en cuenta son:

- ◆ ¿Quién es el auditorio?
- ◆ ¿Cuál es el alcance?
- ◆ ¿Qué tipo de data warehouse debería construirse?

El diseño de los data warehouses es muy diferente al diseño de los sistemas operacionales tradicionales. Se pueden considerar los siguientes puntos:

1. Los usuarios de los data warehouses usualmente no conocen mucho sobre sus requerimientos y necesidades como los usuarios operacionales.
2. El diseño de un data warehouse involucra con frecuencia lo que se piensa en términos más amplios y con conceptos del negocio más difíciles de definir que en el diseño de un sistema operacional.
3. Finalmente, la estrategia de diseño ideal para un data warehouse es generalmente de afuera hacia adentro (outside-in) a diferencia de arriba hacia abajo (top-down).

8.5. Software en un Data Warehouse

Existe una gran cantidad de poderosas herramientas de consulta y reporte en el mercado. Las más simples de estas herramientas son productos de reporte y consultas básicas. Ellos proporcionan desde pantallas gráficas a generadores SQL (Structured Query Language), o más preciso, generadores de acceso-llamada a base de datos. Más que aprender SQL o escribir un programa para acceder a la información de una base de datos, las herramientas de consulta le permiten apuntar y dar un click a los menús y botones para especificar los elementos de datos, condiciones, criterios de agrupación y otros atributos de una solicitud de información.

La herramienta de consulta genera un llamado a una base de datos, extrae los datos pertinentes, efectúa cálculos adicionales, manipula los datos si es necesario y presenta los resultados en un formato claro. Las herramientas de consulta y reporte son más apropiadas cuando se necesita responder a la pregunta ¿"Qué sucedió"? (Ejemplo: ¿"Cómo comparar las ventas de los productos X, Y, Z del mes pasado con las ventas del presente mes y las ventas del mismo mes del año pasado?").

Los generadores de reporte tienen sus limitaciones cuando los usuarios finales necesitan más que una sola vista estática de los datos, que no sean sujeto de otras manipulaciones. Para estos usuarios, las herramientas del procesamiento analítico en línea (OLAP - On Line Analytical Processing) proveen capacidades "Slide y Dice" que contestaría "¿qué sucedió?" al analizar por qué los resultados están como están.

Algunos proveedores ofrecen ahora la técnica OLAP relacional (Relational On Line Analytical Processing - ROLAP) que explora y opera en el data warehouse directamente usando llamadas SQL estándares.

Los retos administrativos y de desarrollo de OLAP, a diferencia de las encontradas con las herramientas de consulta y reporte, son generalmente más complejos. Definiendo el OLAP y el

software de acceso a los datos, se requiere un claro entendimiento de los modelos de datos de la corporación y las funciones analíticas requeridas por ejecutivos, gerentes y otros analistas de datos.

Las herramientas de sistemas de información ejecutivos (Executive Information Systems, SIE), proporcionan medios sumamente fáciles de usar para consulta y análisis de la información confiable. Generalmente se diseñan para el usuario que necesita conseguir los datos rápidamente, pero quiere utilizar el menor tiempo posible para comprender el uso de la herramienta.

También, permiten a los desarrolladores de sistemas colocar el contexto del negocio alrededor de información diversa. Un uso típico de un SIE (Executive Information Systems) es facilitar al usuario la recuperación y análisis de la medida de performance (Desempeño con respecto al rendimiento) de la organización.

El concepto de sistema de información ejecutivo es simple: los ejecutivos no tienen mucho tiempo, ni la habilidad en muchos casos, para efectuar el análisis de grandes volúmenes de datos. El SIE presenta vistas de los datos simplificados, altamente consolidados y mayormente estáticas.

Data mining es una categoría de herramientas de análisis open-end. En lugar de hacer preguntas, se toma estas herramientas y se pregunta algo "interesante", una tendencia o una agrupación peculiar, por ejemplo. El proceso de data mining extrae los conocimientos guardados o información predictiva desde el data warehouse sin requerir pedidos o preguntas específicas.

Las herramientas Mining usan algunas de las técnicas de computación más avanzadas como:

- ◆ redes neuronales
- ◆ detección de desviación
- ◆ modelamiento predictivo y
- ◆ programación genética

8.6. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

CARACTERÍSTICAS

- 8.6.PAA-001.** ¿El data warehouse se encuentra orientado al tema?
- 8.6.GSA-001** Revisar que la información se encuentre clasificada de acuerdo con los aspectos de interés para la empresa.
- 8.6.RC-001.** La empresa debe tener claros cuales son sus datos e información de interés, así como también el registro de clientes, proveedores, productos, actividades, etc., identificar la información adecuada y necesaria para cada área de interés de la organización.

- 8.6.PAA-002.** ¿La información en el DW se encuentra integrada y estandarizada?
- 8.6.GSA-002.** Con respecto al tipo de información requerida realizar pruebas en todas las áreas de la empresa para verificar si la información solicitada es entendible y puede ser útil para cada una de las áreas de la misma.
- 8.6.RC-002.** La calidad en la integración y estandarización depende de la información histórica y que a su vez esté bien estructurada
- Es aconsejable el manejo de estructuras de datos multidimensionales.
- 8.6.PAA-003.** ¿El DW es de tiempo variante?
- 8.6.GSA-003.** Pedir información al DW no únicamente actual, sino que también, de varios periodos de tiempo (varios años atrás).
- Pedir que se dé de alta información y verificar que no pueda ser modificada.
- 8.6.RC-003.** La información almacenada deberá contener datos de periodos de tiempo largo desde cinco a diez años.
- 8.6.PAA-004.** ¿Cumple con la no volatilidad?
- 8.6.GSA-004.** Pedir se muestre la carga de información.
- Verificar se muestre la información anteriormente cargada.
- 8.6.RC-004.** Seleccionar, mediante una etapa de filtrado, los datos que realmente se necesitan ingresar al DW.

ESTRUCTURA DEL DATA WAREHOUSE

- 8.6.PAA-005.** ¿Permite el manejo de diferentes niveles de detalle en la información?
- 8.6.GSA-005.** Hacer consultas sobre información de datos actuales.
- Realizar consultas sobre información de datos antiguos.
- Pedir datos ligeramente resumidos y altamente resumidos sobre la información.
- 8.6.RC-005.** Planear cuidadosamente, junto con el diseñador, la forma de la estructura en el DW.

- 8.6.PAA-006.** ¿Los datos que se presentan altamente resumidos en el DW aportan información valiosa para la organización?
- 8.6.GSA-006.** Elaborar encuestas encaminadas a conocer si dicha información es fundamental y valiosa para el cumplimiento de los objetivos en la empresa.
- 8.6.RC-006.** Considerar los datos altamente resumidos como parte del DW sin tomar en cuenta en donde se alojen físicamente.
- 8.6.PAA-007.** ¿La metadata cumple su función dentro del DW?
- 8.6.GSA-007.** Preguntar al analista si es de utilidad la metadata para ubicar los contenidos dentro del DW.
- 8.6.RC-007.** La metadata debe estar bien elaborada porque es la guía de los algoritmos usados para la esquematización entre el detalle de datos actual, con los datos ligeramente resumidos y éstos, con los datos completamente resumidos, etc.
- Es necesario tener una variedad de metadata disponibles, información sobre las vistas de datos de los usuarios finales e información sobre las bases de datos operacionales.

ARQUITECTURA DE UN DW (Data Warehouse Architecture - DWA)

- 8.6.PAA-008.** ¿La arquitectura de un DW cuenta con todos sus elementos?
- 8.6.GSA-008.** La DWA debe constar de las siguientes partes:
- ◆ Base de datos operacional / Nivel de base de datos externo.
 - ◆ Nivel de acceso a la información.
 - ◆ Nivel de acceso a los datos.
 - ◆ Nivel de directorio de datos (Metadata).
 - ◆ Nivel de gestión de proceso.
 - ◆ Nivel de mensaje de la aplicación
 - ◆ Nivel de data warehouse.
 - ◆ Nivel de organización de datos.
- 8.6.RC-008.** Con la finalidad de comprender cómo se relacionan todos los componentes involucrados en una estrategia data warehousing, es fundamental tener una Arquitectura Data Warehouse.

- 8.6.PAA-009.** ¿El nivel de acceso a la información, en la DWA, proporciona los medios necesarios para los usuarios encargados en dicho nivel?
- 8.6.GSA-009.** Verificar que el nivel de acceso a la información cuente con las herramientas necesarias que debe utilizar el usuario en dicho nivel.
- 8.6.RC-009.** Compatibilidad entre hardware y software
- Encontrar un lenguaje de datos común que puede usarse a través toda la empresa.
- Integración entre varias herramientas
- 8.6.PAA-010.** ¿Las interfaces, entre las herramientas de acceso a la información y las bases de datos operacionales, funcionan adecuadamente?
- 8.6.GSA-010.** Verificar que la interfaz, entre las herramientas para acceder a la información y las bases de datos operacionales, sea eficiente.
- 8.6.RC-010.** Una de las claves de una estrategia data warehousing es abastecer a los usuarios finales con "acceso a datos universales".
- 8.6.PAA-011.** ¿El nivel de gestión de procesos incluye todos los procedimientos requeridos por el DW y la información del directorio de datos (metadata)?
- 8.6.GSA-011.** Revisar las tareas asignadas para la construcción y mantenimiento al DW y la metadata.
- 8.6.RC-011.** Este nivel puede depender de un alto nivel de control de trabajo para muchos procesos (procedimientos).
- 8.6.PAA-012.** ¿El nivel de Mensaje de la aplicación cumple con su objetivo?
- 8.6.GSA-012.** Verificar que la información sea suministrada alrededor de la red de la empresa.
- 8.6.RC-012.** Verificar protocolos de comunicación.
- Garantizar el suministro de la información de forma segura y en el menor tiempo posible.
- 8.6.PAA-013.** ¿El DW se encuentra en un lugar físicamente separado de otra aplicación?

- 8.6.GSA-013.** Que el almacén de datos se encuentre en un lugar distinto a donde están los datos en el ambiente operacional.
- 8.6.RC-013.** Los data DW se localizan sobre plataformas cliente/servidor, pero por lo general se almacenan sobre mainframes.
- En un DW físico, muchas copias de datos operacionales y/o externos son almacenados en una forma que es fácil de acceder y es altamente flexible.
- 8.6.PAA-014.** ¿El nivel de organización de datos realiza los procesos necesarios a la información?
- 8.6.GSA-014.** Se deben realizar todos los procesos necesarios como: seleccionar, editar, resumir, combinar y cargar datos en el depósito y acceder a la información desde bases de datos operacionales y externas.
- 8.6.RC-014.** Involucrar programas de análisis de calidad de datos y filtros que identifican modelos y estructura de datos dentro de la data operacional existente.
- 8.6.PAA-015.** ¿Se involucran todos los procesos necesarios en el tratamiento a los datos?
- 8.6.GSA-015.** Verificar la extracción de datos desde bases de datos operacionales.
- Comprobar el funcionamiento de la transformación y carga de datos, (integración de datos) en el depósito de datos.
- 8.6.RC-015.** Resolver las inconsistencias en los datos, antes que los mismos sean almacenados en el data warehouse.
- 8.6.PAA-016.** ¿La metadata se encuentra relacionada con el DW?
- 8.6.GSA-016.** Corroborar que se describan los contenidos del DW dentro de la metadata.
- 8.6.RC-016.** Integrar y transformar los contenidos de la metada.
- 8.6.PAA-017.** Solicitar el acceso a la plataforma del DW.
- 8.6.GSA-017.** Verificar que funcione correctamente dicha plataforma.

- 8.6.RC-017.** Seleccionar la plataforma acorde con los requerimientos de la empresa y pensando a tiempo futuro.
- 8.6.PAA-018.** ¿Se contempla la evolución del DW?
- 8.6.GSA-018.** Visualizar que pueden añadirse nuevos elementos sobre una base regular para que el contenido siga la evolución de los datos en la base de datos fuente, tanto en los contenidos como en el tiempo.
- 8.6.RC-018.** Es recomendable que los requerimientos de una serie de fases se desarrollen e implementen en modelos consecutivos que permitan un proceso de implementación más gradual e iterativo.
- Idear métodos para identificar datos nuevos o modificados en las bases de datos operacionales.
- VARIAS
- 8.6.PAA-019.** ¿El flujo de datos en el DW funciona correctamente?
- 8.6.GSA-019.** Comprobar que se tengan 3 eventos posibles cuando la información va al nivel de detalle actual:
- ◆ Que la información sea eliminada.
 - ◆ Que la información sea resumida.
 - ◆ Que la información se archive.
- 8.6.RC-019.** Contemplar las excepciones de algún tipo de información en el procedimiento de flujo de datos.
- 8.6.PAA-020.** ¿Se tienen considerados diversos medios de almacenamiento para guardar datos más antiguos?
- 8.6.GSA-020.** Verificar que se cuente con la opción de almacenamiento en medios como la cinta magnética, almacenamiento foto óptico, Raid, etc.
- 8.6.RC-020.** Dependiendo del volumen de información, la frecuencia de acceso, el costo de los medios y el tipo de acceso, seleccionar aquel o aquellos medios de almacenamiento que satisfagan las necesidades del nivel de detalle más antiguo en el DW.
- 8.6.PAA-021.** ¿Se contemplan diferentes tipos de niveles de reestructuramiento en los datos, dependiendo del nivel de detalle solicitado?

- 8.6.GSA-021.** Verificar que a diferentes tipos de niveles de detalle en los datos, la información se presente de diferente forma.
- 8.6.RC-021.** La información de los niveles de esquematización más altos puede ser libremente indexada, mientras que la de los niveles más bajos de detalle, por ser tan voluminosa, puede ser indexada moderadamente.
- 8.6.PAA-022.** ¿Se considera la partición de la información en el DW?
- 8.6.GSA-022.** Preguntar al administrador y programadores sobre dicha partición de la información.
- 8.6.RC-022.** Contar con programadores calificados, debido a que, en el caso de las particiones de las aplicaciones del data warehouse, la mayor parte del trabajo recae sobre el programador.
- 8.6.PAA-023.** ¿Cuenta con controles de calidad el DW?
- 8.6.GSA-023.** Verificar que el DW cuente con certificados de control de calidad en la carga de datos.
- 8.6.RC-023.** A veces es aconsejable seguir el camino inverso de carga. Por ejemplo, pueden alimentarse los sistemas con información depurada del DW o almacenar en el mismo alguna consulta generada por el usuario que sea de interés, por eso se realiza la realimentación de datos o feedback.
- 8.6.PAA-024.** ¿Se tiene establecida una asociación entre usuarios, gestión y grupos?
- 8.6.GSA-024.** Preguntar si se tiene establecida tal asociación.
- 8.6.RC-024.** Involucrar tanto a los usuarios como a la gestión para asegurar que el data warehouse contenga información que satisfaga los requerimientos de la empresa.
- 8.6.PAA-025.** ¿Se llevan registros sobre reportes y publicaciones de casos exitosos?
- 8.6.GSA-025.** Pedir que se muestren dichos reportes y publicaciones.

- 8.6.RC-025.** Tener realimentación con el usuario para comprender cómo evoluciona la implementación del data warehouse a través del tiempo y así poder reunir requerimientos de usuario nuevamente identificados.
- 8.6.PAA-026.** ¿Se tienen estrategias para el desarrollo de un DW?
- 8.6.GSA-026.** Preguntar si se tienen identificados los siguientes puntos:
- ◆ ¿Quién es el auditorio?
 - ◆ ¿Cuál es el alcance?
 - ◆ ¿Qué tipo de DW debería construirse?
- 8.6.RC-026.** Existen diversas estrategias mediante las cuales las organizaciones pueden conseguir sus data warehouses. Se recomienda contemplar las siguientes:
- ◆ Establecer un ambiente "data warehouse virtual".
 - ◆ Construir una copia de los datos operacionales desde un sistema operacional único y posibilitar al data warehouse de una serie de herramientas de acceso a la información.
 - ◆ Seleccionar el número de usuarios basados en el valor de la empresa y hacer un análisis de sus puntos, preguntas y necesidades de acceso a datos.
- 8.6. PAA-027.** ¿Se tienen estrategias para el diseño de un DW?
- 8.6.GSA-027.** Pedir se muestren las estrategias que se implementan en caso de diseñar un DW.
- 8.6.RC-027.** Tomar en cuenta los siguientes puntos:
- ◆ Saber los requerimientos y necesidades de usuarios operacionales y de DW.
 - ◆ Estar en contacto con la Reingeniería de los Procesos del Negocio (Business Process Reengineering).
 - ◆ Considerar el diseño de afuera hacia adentro (outside-in) a diferencia de arriba hacia abajo (top-down).
- 8.6.PAA-028.** ¿Se manejan estrategias para la gestión del DW?
- 8.6.GSA-028.** Pedir se muestren las estrategias que se implementan en caso de la gestión del DW.

8.6.RC-028.

Tomar en cuenta los siguientes puntos:

- ◆ Que el DW permita obtener información realmente vital, más rápida y barata.
- ◆ Tener en cuenta que el mantenimiento de la estructura del data warehouse es tan crítico como el mantenimiento de cualquier otra aplicación de misión crítica.
- ◆ Demandas para mejorar diferentes tipos de datos, para un DW consistente.

CAPÍTULO

IX

AUDITORÍA A BUSINESS INTELLIGENCE (BI)

CAPÍTULO IX

AUDITORÍA A BUSINESS INTELLIGENCE (BI)

9.1. ¿Qué es la inteligencia del negocio?

Uno de los recursos más importantes de cualquier organización es la información, gracias a ella se pueden tomar decisiones que permiten mejorar el rumbo de las empresas e instituciones. Hay que saber “escuchar” lo que nos dicen los datos que día con día genera una organización, si estamos interesados en descubrir las nuevas necesidades de los usuarios, o bien, deseamos mejorar los procesos.

El término Business Intelligence (BI) se refiere al uso de estrategias y tecnología para la recolección, integración, análisis y presentación de los datos de la empresa, con el fin de facilitar la toma de decisiones a las personas que deciden; es decir, permiten la comprensión del funcionamiento actual de la empresa y la anticipación de acciones para dar una buena operación al negocio, representando una ventaja competitiva.

En la figura 9.1. podemos apreciar que las decisiones se realizan a nivel operativo, táctico y estratégico. De lado izquierdo de la pirámide encontramos el tipo de personas que se encuentran por cada nivel. De lado derecho se presentan las herramientas que se utilizan dependiendo del nivel del cual se trate.



FIG. 9.1. NIVELES DENTRO DEL NEGOCIO

9.2. Características de las herramientas de la inteligencia del negocio

Las herramientas de BI posibilitan el modelado de las representaciones con base en consultas para crear informes que tienen las siguientes características:

- ♦ *Accesibilidad a la información, usar datos de diversas fuentes.* Los datos son la fuente principal de este concepto, lo primero que deben garantizar este tipo de herramientas y técnicas será el acceso de los usuarios a los datos con independencia de la procedencia de éstos.

- ♦ *Apoyo en la toma de decisiones.* Se busca ir más allá en la presentación de la información, de manera que los usuarios tengan acceso a herramientas de análisis que les permitan seleccionar y manipular sólo aquellos datos que les interesen.
- ♦ *Orientación al usuario final.* Se busca independencia entre los conocimientos técnicos de los usuarios y su capacidad para utilizar estas herramientas.

9.3. Herramientas de Business Intelligence

Las herramientas de inteligencia se basan en la utilización de un sistema de información de inteligencia que se forma con distintos datos extraídos de los datos de producción, con información relacionada con la empresa o sus ámbitos y con datos económicos.

Mediante las herramientas y técnicas ETL (extraer, transformar y cargar) se extraen los datos de distintas fuentes, se depuran y preparan (homogeneización de los datos) y se cargan en un almacén de datos.

Por último, las herramientas de inteligencia analítica posibilitan el modelado de las representaciones con base en consultas para crear tablas de bordes; lo cual se conoce como presentación de informes.

Los tipos de herramientas de Business Intelligence se pueden clasificar, de acuerdo con su nivel de complejidad. Cada producto de mercado integra, combina, potencia, adapta y personaliza dichas funciones.

9.3.1. Query & reporting. Son herramientas para la elaboración de informes y listados, tanto en detalle como sobre información agregada, a partir de la información de los datawarehouses y datamarts. Son desarrollos a medida y/o herramientas para una explotación libre.

9.3.2. Cuadro de mando analítico. Es una herramienta de query orientada a la obtención y presentación de indicadores para la dirección (frente a la obtención de informes y listados).

9.3.3. Cuadro de mando integral o estratégico (*Balanced Scorecard*). Este modelo parte de que la estrategia de la empresa es el punto de referencia para todo proceso de gestión interno.

Los objetivos estratégicos se asocian mediante relaciones causa-efecto y se organizan en cuatro áreas o perspectivas: financiera, cliente, procesos y formación o desarrollo. El cuadro de mando integral es una herramienta que permite alinear los objetivos de las diferentes áreas o unidades con la estrategia de la empresa y seguir su evolución.

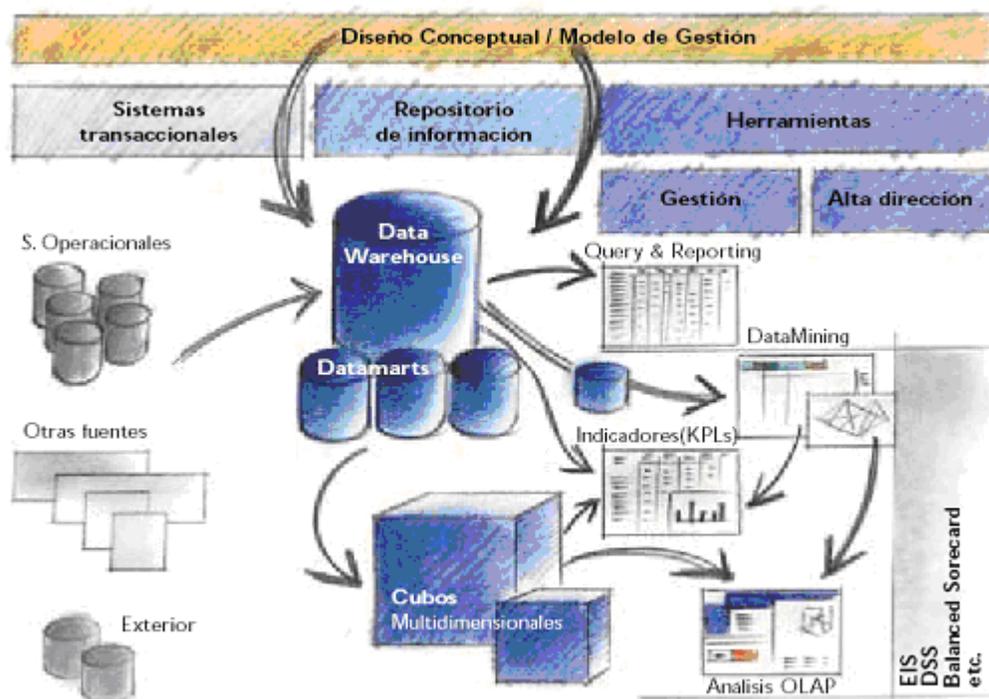
9.3.4. OLAP (*on-line analytical processing*). Son herramientas que manejan interrogaciones complejas de bases de datos relacionales, proporcionando un acceso

multidimensional a los datos, capacidades intensivas de cálculo y técnicas de indexación especializadas.

Utilizan un servidor intermedio para almacenar los datos multidimensionales precalculados de forma que la explotación sea rápida.

9.3.5. Datamining (minería de datos). Son auténticas herramientas de extracción de conocimiento útil, a partir de la información contenida en las bases de datos de cualquier empresa. El objetivo que se persigue es descubrir patrones ocultos, tendencias y correlaciones, y presentar esta información de forma sencilla y accesible a los usuarios finales, para solucionar, prever y simular problemas del negocio. El datamining incorpora la utilización de tecnologías basadas en redes neuronales, árboles de decisión, reglas de inducción, análisis de series temporales y visualización de datos.

Fig. 9.2. Modelo integral de una solución BI



De manera integral, Business intelligence, se puede definir como el conjunto de metodologías, aplicaciones y tecnologías, que permite reunir, depurar y transformar datos de los sistemas transaccionales e información que se encuentra desestructurada (interna y externa) en información estructurada, para su explotación directa (reporting, análisis OLAP, Data Mining, etc.) o para su análisis y transformación en conocimiento para el soporte a la toma de decisiones sobre el negocio. Dicha definición trata de describir el ámbito integral del entorno BI mostrado en la figura 9.2.

9.4. Algunas soluciones de BI

Algunas de las soluciones de BI más reconocidas en el mercado son:

- ◆ *Cubeware, Sagent solution platform*. Sistema integrado que extrae, transforma, distribuye y presenta la información clave para la toma de decisiones en la empresa.
- ◆ *Microstrategy*. Ayuda en el conocimiento de la información manejada en una empresa.
- ◆ *MIS Decisionware, Cognos*. Software que contiene una herramienta para modelación, pronóstico y simulación del negocio.
- ◆ *Bissantz, Bitam/artus business intelligence suite*. Herramienta capaz de agrupar la información y utilizarla como un activo que ayudará a la empresa a identificar las oportunidades de negocio, optimar las áreas de finanzas, clientes, procesos internos de aprendizaje e innovación.
- ◆ *Applix TM1*: Es una herramienta orientada a las necesidades de planeamiento, presupuesto, pronóstico, consolidaciones financieras, reportes y análisis. Permite acceder, analizar y visualizar información corporativa que permite medir la gestión del negocio en cualquier momento en cualquier lugar.

9.5. Elementos que intervienen en la toma de decisiones

Se distinguen tres elementos tomadores de decisiones:

- ◆ Los ejecutivos, quienes toman decisiones de forma analítica e intuitiva, y necesitan mucha información debido a que sus decisiones son de tipo estratégico.
- ◆ Los administradores y analistas, responsables de decisiones de tipo táctico, quienes lo hacen de manera analítica y también demandan información considerable.
- ◆ Los empleados, que toman decisiones rutinarias y cuentan con datos limitados a su dominio.

De acuerdo con cada tipo tomador de decisión, los administradores de información deben ofrecer diferentes herramientas de software, así como distintas formas de presentar la información para facilitar la tarea de análisis.

Las herramientas dinámicas para toma de decisiones (como las simulaciones, el análisis de escenarios y las representaciones en gráficas) son adecuadas para los ejecutivos y los administradores.

9.6. Sistema analítico

Los sistemas analíticos o de toma de decisiones recuperan los datos de las operaciones diarias de la organización, generados por los sistemas transaccionales, y los procesan, con objeto de tenerlos disponibles para los tomadores de decisiones.

El desarrollo de sistemas analíticos es un tema complejo, con algunas décadas de evolución, y con aportaciones de áreas como la inteligencia artificial, que ha incorporado técnicas como la minería de datos (descubrimiento de patrones) el data warehousing (análisis multidimensional de información) y el OLAP (Procesamiento Analítico en Línea, por sus siglas en inglés “On-line Analytical Processing”).

Los sistemas analíticos operan con aplicaciones ya existentes como SAP (Systems, Applications and Products in Data Processing), además, cuentan con interfaces para hacer consultas desde la Web.

9.7. Funcionalidad de los sistemas analíticos

Las principales funciones que los sistemas analíticos incluyen, son:

- ◆ Con ayuda de los metadatos, el informático hace “la traducción” entre los campos de la base de datos para formar los conceptos de negocios, que maneja el experto tomador de decisiones.
- ◆ Sistema de semáforos, mediante éste se puede visualizar el nivel de los indicadores claves del negocio para alertar sobre los problemas que puedan ocurrir en los procesos.
- ◆ Cruces de información.
- ◆ Ordenamientos y agrupamientos de información por región, producto y usuario, entre otros conceptos.
- ◆ Sumarización.
- ◆ Comparación de conceptos de negocio en diferentes periodos.
- ◆ Generación de gráficos para visualizar de forma sencilla la información.

9.8. Aplicaciones de los sistemas analíticos

La nueva generación de servicios financieros puede ofrecer escenarios y recomendaciones de inversión a sus usuarios, de acuerdo con el monto disponible y el nivel de riesgo y utilidad deseados. A continuación se mencionan algunos ejemplos:

Amazon®. Utiliza los sistemas analíticos para conocer la experiencia de cada comprador y perfeccionar tanto su estrategia de mercadotecnia, como las referencias cruzadas de productos de manera individual.

Six Flags®. Esta organización ha logrado economía en los costos de compras compartidas y administración de inventarios, debido a la capacidad que tiene para realizar rápidamente, análisis de datos financieros globales, lo que lleva al mejoramiento en procesos de negocio.

Xerox®. Ha utilizado las herramientas analíticas en su Sistema de Gestión de Cuentas por Cobrar con la finalidad de hacer el análisis de deuda por cliente y cobrador, focalizando el uso de recursos en la cobranza de las facturas.

Con este sistema, Xerox ha logrado cambiar su recaudación mensual de un seguimiento aleatorio de las deudas, a un control semanal sistemático.

Las soluciones de inteligencia de negocios proporcionan grandes ventajas al facilitar el análisis de información de las organizaciones. El reto para que estas herramientas de software funcionen de manera adecuada, implica el convencimiento de los directivos en apoyar la adopción de una cultura de democracia en la información, de tal manera que los problemas y la información asociada no se vean de forma aislada por una unidad funcional, sino que se consideren como problemas e información sustantivos relacionados con otras áreas de la organización

9.9. ¿Cómo elegir una aplicación BI?

Lo primero que hay que decir es que se tiene que identificar cuáles son las necesidades y el tipo de herramienta que se busca: análisis, reporte, base de datos, OLAP (“On-line Analytical Processing”) etc.

Los principales factores (sin orden de importancia) a tomar en cuenta cuando se elige una herramienta de Business Intelligence:

- ◆ La Plataforma. No es lo mismo estar atados a Microsoft, o poder trabajar en Unix, o tener una estrategia Open Source Linux.
Lo mismo aplica al hardware. Algunos fabricantes son restrictivos.
- ◆ El Curriculum del vendedor. Es muy útil conocer el tipo de implementaciones que se han hecho, si se han realizado en tiempo, si se utilizan, la satisfacción de usuarios, etc.
- ◆ El tamaño del cubo. Es imprescindible hacer un análisis previo de la amplitud de la información a almacenar. Algunas aplicaciones pueden “explotar” llegado cierto nivel.
- ◆ La velocidad de consulta. Los usuarios siempre quieren velocidad en sus consultas y si 20 segundos de espera es mucho, quizás haya que buscar otra herramienta.
- ◆ Servicios de soporte y ayuda a nivel mundial. Tenemos que tener la seguridad de que si algo falla en la aplicación, se pueda resolver en el menor tiempo posible.
- ◆ Evaluaciones de analistas.
- ◆ El ecosistema del vendedor (consultores, acuerdos, comunidad de desarrolladores).
- ◆ Base instalada de usuarios. Si hay de mismo sector mucho mejor.
- ◆ Graphical User Interface (GUI). Se habla de una herramienta para usuarios finales y si a éstos no les gusta, no la utilizarán y será dinero tirado.
- ◆ Precio.
- ◆ Integración con otras herramientas. Ninguna herramienta funciona como una isla aislada del resto. Lo mismo que una empresa, si creas islas, crearás incomunicación.

9.10. ¿Por qué fallan muchos proyectos Business Intelligence?

A veces es sorprendente, que con el desarrollo al que han llegado muchas herramientas, el uso de metodologías contrastadas y el mayor nivel de conocimiento de técnicos y usuarios, se produzcan tantos desastres en la implementación de soluciones Business Intelligence, en términos de exceso de costo sobre el previsto, no utilización por parte de los usuarios, no cumplir con las expectativas, información errónea, etc.

Algunos de los principales fallos:

- ◆ Muchos Data Warehouses crecen en tamaño de forma desproporcionada porque los técnicos no consiguen decir no a las “excesivas” demandas de los usuarios.
- ◆ Se prefiere realizar el proyecto con gente de la propia empresa, cuando éstos no tienen ni tiempo, ni conocimientos.
- ◆ Se fijan unas fechas de entrada en producción del sistema poco realistas, que provoca nuevas fechas y más retrasos.
- ◆ El presupuesto destinado para el proyecto es escaso en comparación con el grado de complejidad que se quiere desarrollar.
- ◆ La selección del software y hardware a veces se realiza siguiendo criterios de acuerdos generales o compromisos, antes que puramente técnicos.
- ◆ Antes del proyecto, no se realizan benchmarks o “pruebas de concepto” para determinar la viabilidad.
- ◆ Los datos de origen no están limpios. Duplicidades, errores, caracteres erróneos, implican un proceso ETL (Extracción, Transformación y Carga) más costoso, mayor tamaño de la Base de datos y peor rendimiento.
- ◆ El patrocinador del proyecto no ejerce como tal durante el mismo. No “baja a la tierra”.
- ◆ Mala elección de los consultores y excesiva rotación entre ellos.
- ◆ Escasa involucración de los usuarios finales que les lleva a sentir cierta frustración con los resultados obtenidos.
- ◆ Caer en el error de “en informática todo se puede hacer” y empezar con personalizaciones, escribir código fuera de las funcionalidades estándar.
- ◆ No alinear el proyecto dentro de una estrategia de negocio.

Existen muchos más factores que pueden hacer fallar un proyecto Business Intelligence, pero éstos pueden hacer literalmente “tumbarlo”, no conseguir más proyectos para los consultores, mala imagen del producto y riesgos internos para el director de informática y otros patrocinadores.

9.11. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

- 9.11.PAA-001.** Identifique los objetivos de instalar una herramienta BI en la empresa. ¿Cuál es la información requerida para gestionar y tomar decisiones?
- 9.11.GSA-001.** El análisis de criterios directivos (misión, objetivos estratégicos, factores de seguimiento, indicadores clave de gestión o KPIs, modelos de gestión, etc.) deben estar presentes en algún documento como antecedente para la iniciativa de utilización de alguna herramienta BI.
- 9.11.RC-001.** Bajo el concepto general “soporte a la toma de decisiones” se esconden múltiples necesidades particulares: contrastar que todo va bien, analizar diferentes aspectos de la evolución de la empresa, presentar información de forma más intuitiva, comparar información en diferentes periodos de tiempo, comparar resultados con previsiones, identificar comportamientos y evoluciones excepcionales, confirmar o descubrir tendencias e interrelaciones, necesidad de realizar análisis predictivos, etc. son todas ellas necesidades parciales dentro del concepto general.
- 9.11.PAA-002.** Identifique la herramienta BI con las características que se mencionen. ¿Cuál debe ser el formato y composición de los datos a utilizar?
- 9.11.GSA-002.** El método de almacenamiento de los datos repercute en la rapidez y exactitud de recuperación de los datos, por lo que es necesario conocer los requerimientos de presentación de la información al usuario final.
- 9.11.RC-002.** La información requerida para la toma de decisiones deberá estar depurada y estructurada.
- 9.11.PAA-003.** Identifique las características de los datos a utilizar. ¿De dónde proceden los datos para la toma de decisiones?
- 9.11.GSA-003.** Si los datos de origen no están limpios, presentan duplicidades, errores, caracteres erróneos, etc., implican un proceso de extracción más costoso, con un mayor tamaño de la base de datos y menor rendimiento.
- 9.11.RC-003.** Se requerirá de un proceso ETL (Extracción, Transformación y Carga) previo en el caso de que los datos sean inadecuados para la herramienta de BI.

- 9.11.PAA-004.** ¿Se sabe cuál es la disponibilidad y periodicidad requerida de los datos?
- 9.11.GSA-004.** Realice una prueba de petición de información, observe y determine el tiempo requerido para obtener la respuesta.
- 9.11.RC-004.** No debe transcurrir mucho tiempo entre la necesidad de información y el resultado. Es importante que los indicadores y modelos sean selectivos, sencillos y admitidos por todos los usuarios.
- 9.11.PAA-005.** Pida los documentos que acrediten la elección de la aplicación de BI.
- 9.11.GSA-005.** Verifique que en los documentos se haya hecho el análisis de las herramientas que se buscan.
- 9.11.RC-005.** En los documentos deben haberse considerado:
- ◆ Los recursos de hardware y software disponibles para decidir si la aplicación de BI es el adecuado.
 - ◆ La forma y el tipo de implementación del vendedor (metodología y tiempo).
 - ◆ La cantidad de personas que harán la instalación y la capacitación al usuario final.
 - ◆ El precio de la aplicación y las licencias por usuario, para considerarlo en el presupuesto.
 - ◆ La capacidad de integrarse con otras herramientas, para no causar incomunicación entre áreas.
- 9.11.PAA-006.** Identifique la herramienta de BI instalada.
- 9.11.GSA-006.** Verifique que la aplicación funciona con los requerimientos necesarios. Considere lo siguiente:
- ◆ El tamaño de la información a almacenar.
 - ◆ La velocidad de consulta de la información.
 - ◆ La existencia de servicios de soporte y ayuda.
- 9.11.RC-006.** Algunas características básicas que debería tener una herramienta de BI:
- ◆ Tener potentes posibilidades gráficas.
 - ◆ Posibilidad de almacenar y compartir los informes y cálculos creados por los usuarios.

- ◆ Ser rápida. No debe transcurrir mucho tiempo entre la necesidad de información y el resultado.
- ◆ Tener un lenguaje funcional y de negocio.
- ◆ Ser de manejo sencillo.
- ◆ La administración la deben llevar a cabo los usuarios y no el personal técnico.

- 9.11.PAA-007.** Identifica alguna mejora antes y después de utilizar la aplicación de BI.
- 9.11.GSA-007.** A partir de la utilización de alguna herramienta de BI al cuestionarse sobre políticas de calidad de un proceso, como “¿dónde está...?”, “¿cuánto falta...?”, “¿cuánto tiempo estamos tardando en...?”, “¿dónde están los cuellos de botella?”, “¿dónde estamos siendo más/menos productivos?”, “¿dónde faltan/sobran recursos?”, etc. debe obtener respuestas con una base sólida.
- 9.11.RC-007.** Cualitativamente, los beneficios surgen del incremento de la eficiencia en el proceso de toma de decisiones: mayor información, de mejor calidad, más fiable, compartida por toda la organización, menores tiempos de respuesta en su obtención, mejora de la comunicación en la empresa y creación de un lenguaje homogéneo.
- 9.11.PAA-008.** Verificar que el usuario final de la aplicación BI, se le haya solicitado información de sus necesidades sobre el contenido de datos extraíbles del sistema BI.
- 9.11.GSA-008.** Corroborar la existencia de minutas o bitácora de juntas para el consenso de requerimientos de los usuarios finales para el proyecto de elección de la aplicación de BI.
- 9.11.RC-008.** Es importante tener la alineación de los objetivos del departamento de sistemas de información y los usuarios. Sobre todo contar con apoyo e impulso desde la dirección general.
- 9.11.PAA-009.** ¿La forma y el tiempo de implementación afectan en el proceso cotidiano de la empresa?
- 9.11.GSA-009.** Corrobore con el documento de planeación de la instalación de las herramientas BI.
- 9.11.RC-009.** Determinar la cantidad de tiempo y el horario para realizar los cambios en la empresa, permite determinar prioridades en la fase de implementación del sistema BI.

- 9.11.PAA-010.** ¿Se cuenta con el personal calificado (consultores, desarrolladores, programadores y capacitadores) para las fases de diseño, implementación, prueba y capacitación de la aplicación BI?
- 9.11.GSA-010.** Consultar el curriculum del vendedor de la aplicación y determinar si éste ha trabajado anteriormente con la empresa u otras empresas en otros proyectos.
- 9.11.RC-010.** Contar con el personal adecuado es un factor crítico de éxito para una estrategia de BI.
- 9.11.PAA-011.** ¿Usuarios de diferentes áreas utilizan la aplicación? ¿Se cuenta con la disponibilidad de los datos al nivel de detalle que lo necesitan? ¿La información presentada en cada área es consistente con las demás áreas?
- 9.11.GSA-011.** El uso de la herramienta en diferentes áreas nos permite corroborar la utilidad de la información para la comunicación entre los procesos.
- 9.11.RC-011.** Se recomienda que la presentación de los datos con la herramienta de BI cuente con las características de integridad de la información.
- 9.11.PAA-012.** ¿Se cuenta con algún control de permisos para la visualización de los datos?
- 9.11.GSA-012.** La visualización de ciertos datos debe ser restringida para ciertas áreas, por lo que corrobore la existencia de una jerarquía de accesos a los datos.
- 9.11.RC-012.** Se recomienda que el manejo de claves y contraseñas de la aplicación de BI sean igual al que se utiliza para acceder al sistema de la empresa para evitar una mayor frecuencia de olvido de éstas y una menor necesidad de administrar el control de permisos.
- 9.11.PAA-013.** ¿El usuario final conoce la forma de reportar alguna incidencia con la aplicación BI?
- 9.11.GSA-013.** Ver si el usuario conoce la forma de reportar algún incidente en la aplicación BI.
- Para una adecuada toma de decisiones el usuario de la aplicación debe tener resultados de la información solicitada de forma consistente y rápida, por lo que en caso de presentarse alguna incidencia ésta debe de resolverse en el menor tiempo posible.

- 9.11.RC-013.** La existencia de una mesa de ayuda para la aplicación es necesaria para mantener la aplicación de BI disponible y sin errores.
- 9.11.PAA-014.** ¿El usuario final conoce alguna otra forma de validación de la información generada por la aplicación de BI?
- 9.11.GSA-014.** El soporte para la toma de decisiones es fundamental para fortalecer la confianza de la persona que consulta la información y ésta puede utilizar otros criterios de solicitud de información que le proporcionen un resultado común.
- 9.11.RC-014.** El usuario final debe conocer la forma de gestión de la información, las áreas involucradas para ello y los diferentes reportes posibles que pueden ser generados.
- 9.11.PAA-015.** ¿El usuario de gestión de información tiene la forma de administrar los reportes que se generan?
- 9.11.GSA-015.** Preguntar si se cuenta con la forma de administrar los reportes. El mantenimiento del contenido y la estructura de información por un usuario que gestiona información podrá modificar los reportes que se generen en la aplicación de acuerdo con las necesidades del negocio.
- 9.11.RC-015.** El manejo de reportes debe ser sencillo para el usuario final (sólo consulta información) y la gestión, debido a que de esta forma la frecuencia de uso de la aplicación será mayor.
- 9.11.PAA-016.** ¿El sistema de Gestión del conocimiento cumple con su objetivo?
- 9.11.GSA-016.** Verificar que la organización disponga de la información que necesita en el momento preciso y bajo el contexto indicado.
- 9.11.RC-016.** Utilizar tecnologías web y complementarlas con “portales de información”.
- 9.11.PAA-017.** ¿El sistema, para la toma de decisiones, satisface las necesidades críticas de la empresa, en cuestión de información?
- 9.11.GSA-017.** Investigar sobre el nivel de satisfacción en la información que se maneja en la empresa, la cual sea un medio, para llevar a cabo estudios sobre el negocio de forma sencilla y eficaz.
- 9.11.RC-017.** Implementar los datos mediante DW.

Analizar la información del negocio mediante CRM (Customer Relationship Management).

- 9.11.PAA-018.** ¿La BI, a nivel operativo, permite que los empleados, que trabajan con información operativa, puedan recibirla de manera oportuna, exacta y adecuada?
- 9.11.GSA-018.** Preguntar a la población de empleados del nivel operativo sobre la eficiencia en la información obtenida.
- 9.11.RC-018.** Suministrar herramientas de reportes u hojas de cálculo.
- 9.11.PAA-019.** ¿El nivel táctico de BI comunica la información a los analistas y gerencia media de la empresa?
- 9.11.GSA-019.** Verificar el uso de herramientas de análisis y consulta.
- 9.11.RC-019.** Buscar herramientas que satisfagan las necesidades de analistas y gerencia media, y que permitan anticipar soluciones que aporten mayor impacto positivo a la empresa.
- 9.11.PAA-020.** ¿La BI, a nivel estratégico, proporciona lo necesario a la alta dirección de la empresa, para analizar y monitorear tendencias, patrones metas y objetivos de la organización?
- 9.11.GSA-020.** Preguntar a la alta dirección si está satisfecha con las herramientas proporcionadas de nivel estratégico.
- 9.11.RC-020.** Considerar el uso de un Cuadro de mando integral o Balanced Scorecard. El Cuadro de mando integral reconoce que la finalidad de conseguir beneficios, en una actividad empresarial, es el resultado de una cadena de causas y efectos que suceden en cuatro ámbitos: el financiero, el cliente, los procesos internos, así como la preparación y desarrollo del personal.

<u>Objetivos estratégicos</u>	<u>Indicadores estratégicos</u>	
	<u>Indicadores de causa</u>	<u>Indicadores de efecto</u>
Financieros		
Clientes		
Interno		
Formación(desarrollo)		

CAPÍTULO

X

AUDITORÍA AL SISTEMA HELP DESK

CAPÍTULO X

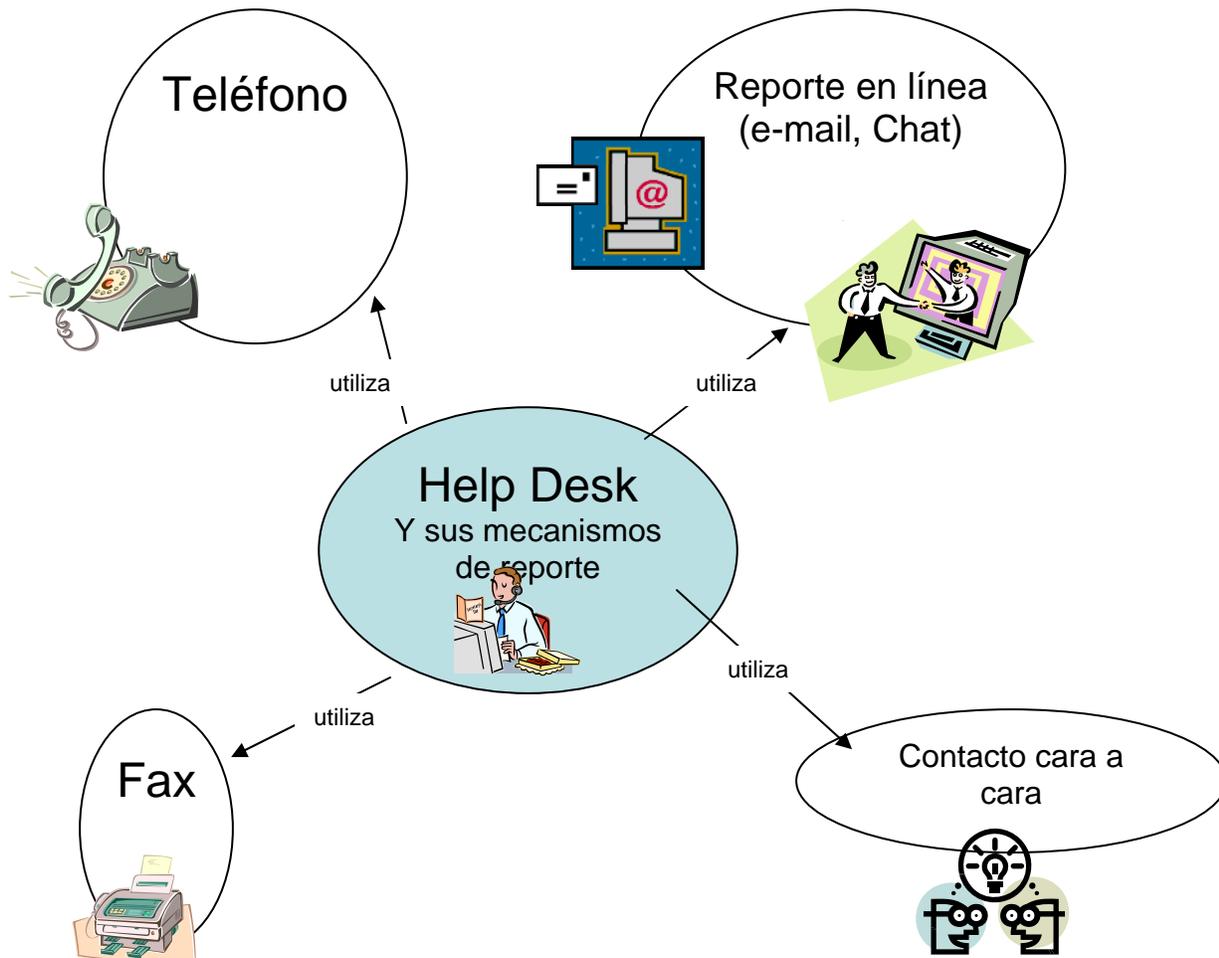
AUDITORÍA AL SISTEMA HELP DESK O MESA DE AYUDA

10.1. Introducción

El Help Desk (escritorio de ayuda) es un área táctica especializada en el soporte de Tecnologías de Información (TI) que tiene como tarea principal la de administrar, coordinar y resolver los incidentes de la manera más rápida posible, así como asegurar que los problemas se resuelven y no sean ignorados.

Los servicios de Help Desk incrementan la productividad de los usuarios y reducen considerablemente los costos de manutención.

La siguiente figura ilustra los mecanismos de reporte más comunes que se utilizan:



10.2. Mecanismos de reporte

Mecanismo	Teléfono	Fax	En línea	Contacto cara a cara
Ventaja	La atención es inmediata y puede ser automatizada. Para resolver el problema se utilizan soluciones verbales, cualquier duda es aclarada en el momento.	La respuesta es casi inmediata y el experto puede responder por la misma vía.	En caso de chat es ventaja ya que la atención es inmediata y las dudas pueden ser aclaradas en el momento.	La atención y la respuesta es inmediata.
Desventaja	Los usuarios deberían tener ciertos conocimientos para poder explicarle al Help Desk su problema y no que se estuviera adivinando únicamente.	La legibilidad de la información depende de la calidad del fax.	En el caso del mail es desventaja ya que ésta puede tardar en responderse porque no sabemos el flujo de correos que reciba el Help Desk.	Puede ser que el problema correspondía a otro tipo de experto y esto sería pérdida de tiempo.

10.3. Participantes en un Help Desk

Analista. Representante del Área de Soporte a través del Help Desk que es responsable de recibir, documentar, analizar, diagnosticar, escalar o corregir y verificar la resolución de reportes abiertos por usuarios y/o clientes.

Cliente. Cliente externo que generalmente accede al Help Desk para solicitar asistencia técnica o soporte técnico especializado dependiendo del tipo de acuerdo post-venta que tenga contratado. Los servicios que les proporciona un Help Desk son:

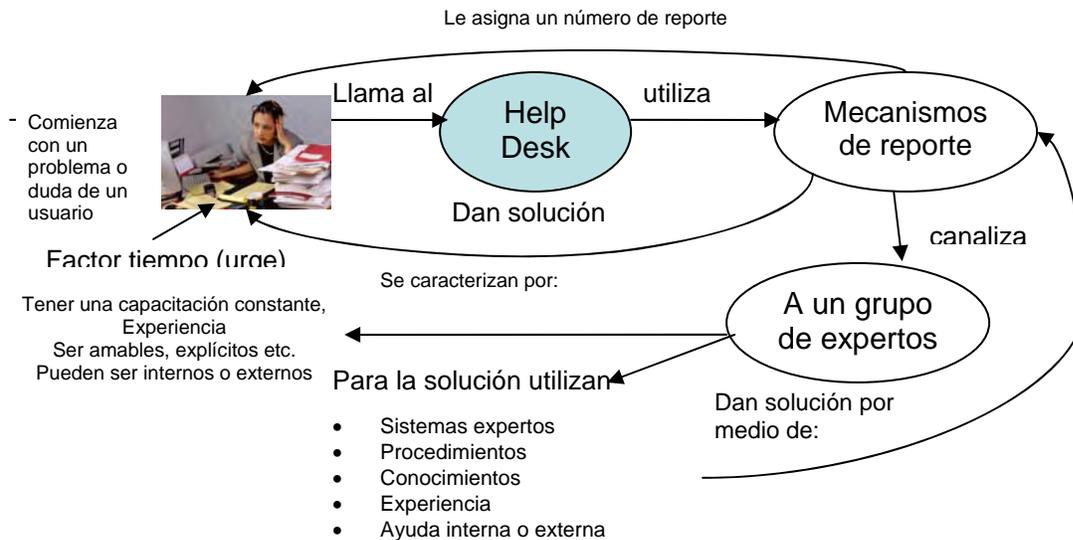
- ◆ Servicios en línea
- ◆ Soporte Técnico
- ◆ Información de productos.

Usuario. Representantes del servicio de Help Desk, trabajan en:

- ◆ Ayuda en línea
- ◆ Atención de fallas
- ◆ Asistencia técnica

10.4. Funcionamiento ideal de un Help Desk

El sistema Help Desk utiliza mecanismos de reporte, los cuales son canalizados a un grupo de expertos, y estos a su vez, utilizan procedimientos, conocimientos, experiencia, entre otros, para poder dar solución al cliente mediante el mecanismo de reporte.



En la figura anterior el cliente, que presenta un problema o duda, solicita atención al Help Desk.

10.5. Características del Help Desk

Características externas:

- ◆ Disponibilidad. Horario y procedimiento de respaldo adecuados para cubrir necesidades de usuarios y clientes.
- ◆ Accesibilidad. Asertividad y disposición suficientes de analistas para atender las necesidades de usuarios y clientes.
- ◆ Flexibilidad. Capacidad de adaptación para satisfacer las demandas y las solicitudes de clientes y usuarios, respectivamente.

Características internas:

- ◆ Medible. Definición de métricas para evaluar la calidad del servicio que se ofrece a clientes y/o usuarios.
- ◆ Autodidacta. Orientación a la innovación y el aprendizaje de nuevas soluciones y sistemas con el objeto de asistir mejor a usuarios y/o clientes.

10.6. Criterios de dimensión de un Help Desk

Se deben tomar en cuenta los siguientes puntos para establecer las dimensiones físicas y lógicas del Help Desk.

Criterios dependientes de la competencia de los analistas y del tipo de tecnología a soportar:

- ◆ Cantidad de llamadas contestadas. Volumen de llamadas procesadas en un cierto parámetro de tiempo. Aquí no podemos ingresar el número de llamadas resueltas ya que en varios métodos (teléfono, fax, e-mail) no sabemos si quedó resuelto el problema a menos que el usuario se vuelva a comunicar para informarnos que ya quedó arreglado su problema.
- ◆ Duración promedio de llamada contestada. Tiempo promedio por un analista para procesar una llamada.

Criterios dependientes de la cantidad de analistas y de la tecnología utilizada:

- ◆ Dilación a la contestación. Tiempo promedio que se mantiene en espera un usuario o cliente antes de ser conectado con un analista.
- ◆ Cantidad de llamadas no completadas. Número de llamadas desconectadas antes de llegar a ser transferidas con un analista.

10.7. Tecnologías aplicadas en un Help Desk

Herramientas:

- ◆ Herramientas para la comunicación
 - ◆ Foros de discusión
 - ◆ Correo de voz
 - ◆ Correo electrónico
- ◆ Sistemas para la administración de Help Desk
 - ◆ Captura y registro de llamadas
 - ◆ Manejo de llamadas
 - ◆ Reportes y consultas
- ◆ Tecnologías relacionadas con el teléfono
 - ◆ Integración del cómputo con la telefonía
 - ◆ Distribuidor automático de llamadas
 - ◆ Respuesta interactiva de voz
- ◆ Herramientas para resolver problemas
 - ◆ Bases de conocimiento y sistemas expertos
 - ◆ Software para el diagnóstico remoto

10.8. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

ADMINISTRACIÓN DEL HELP DESK

- 10.8.PAA-001.** ¿Se cuenta con un objetivo claro para implementar un Help Desk?
- 10.8.GSA-001.** Determinar si la administración ha identificado/definido claramente los siguientes elementos críticos:
- ◆ La definición completa de la misión.
 - ◆ Los servicios que deben ser ofrecidos por el Help Desk y una clara delimitación de las responsabilidades y los diferentes servicios que se presten aparte de las funciones de soporte.
 - ◆ Las metas primarias de servicio.
- 10.8.RC-001.** No es conveniente que las áreas de responsabilidad se encuentren dispersas en el Help Desk, por lo que es necesario:
- ◆ Identificar las áreas de responsabilidad de soporte.
 - ◆ Evaluar que tan apropiadas son las responsabilidades.
 - ◆ Determinar si se requieren áreas de responsabilidad adicionales.
- 10.8.PAA-002.** ¿La empresa cuenta con el control de la cobertura de su servicio de Help Desk?
- 10.8.GSA-002.** Determine aproximadamente cuántos usuarios utilizan el Help Desk, en qué horario se da el servicio y con qué tecnologías cuentan.
- 10.8.RC-002.** El conocimiento sobre los clientes nos proporciona mayor porcentaje de éxito en el servicio. Nos da la noción de la cantidad de recursos que se necesitan emplear y los tipos de servicios que se ofrecerían.
- 10.8.PAA-003.** ¿En el funcionamiento del Help Desk se identifican las partes que son más conflictivas dentro del proceso de solución?
- 10.8.GSA-003.** Verifique:
- ◆ Si existe un proceso para la captura de problemas dentro del ambiente.

- ◆ Si los clientes son notificados del tiempo de la acción correctiva.
- ◆ Si se ha establecido una jerarquía para escalar los problemas.
- ◆ Que los elementos fuera de lo normal sean revisados en el momento de su manifestación.

10.8.RC-003. En el funcionamiento del Help Desk, el cliente espera que de manera inmediata le sea solucionado el problema. El analista debe estar capacitado y dar soluciones, pero puede que alguna cosa o tema esté fuera de su conocimiento por lo que se debe canalizar el problema a un grupo de expertos.

10.8.PAA-004. En caso de que exista más de un Help Desk: ¿se mantiene comunicación constante entre los help desk?

10.8.GSA-004. Verificar que los procedimientos para la solución de problemas y nuevos desarrollos entre los help desk sean similares.

Verificar la existencia de minutas sobre las reuniones entre los help desk.

10.8.RC-004. Para mejorar el desempeño de comunicación del negocio con los clientes, es necesario que los help desk mantengan la mutua responsabilidad de mantenerse informados en la solución de problemas y nuevas herramientas, el uso del mismo software de sistema y la capacitación compartida.

10.8.PAA-005. Revisar las formas de evaluación que utiliza la empresa para medir la eficiencia de su Help Desk.

10.8.GSA-005. Comprobar si la administración realiza encuestas periódicamente para obtener realimentación sobre la imagen que los consumidores tienen del servicio.

Determinar si los métodos de administración para evaluar el nivel de servicio son congruentes con las metas que se establecieron anteriormente.

Corroborar que el área de administración del Help Desk recibe la documentación adecuada para la revisión y el análisis estadístico de sus recursos.

10.8.RC-005. La administración debe recibir la documentación adecuada para la revisión y el análisis estadístico de los recursos, satisfacción del cliente, tiempo de respuesta e identificación del tipo de problema.

Para ello existen herramientas de análisis, como algunas de las siguientes:

- ◆ Histogramas (Diagrama de Pareto).
- ◆ Gráficas lineales.
- ◆ Gráficas de dispersión.
- ◆ Gráficas de control.

Estas herramientas nos sirven principalmente para:

- ◆ Determinar factores que tienen impacto en la satisfacción del cliente.
- ◆ Evaluar el desempeño de los empleados, en lo referente a la calidad de atención.
- ◆ Mostrar la relación de las variables en los procedimientos del Help Desk, como las siguientes:
 - ◆ Cantidad de llamadas procesadas o casos resueltos con respecto al total de llamadas recibidas en una semana o mes.
 - ◆ Tiempo de resolución de llamadas o casos con respecto a la asignación de prioridades.
 - ◆ Cantidad de llamadas por tipo de servicio ofrecido en forma semanal o mensual.

Estas mediciones están orientadas a ayudar a definir las mejoras estratégicas o cambios al diseño para mantener competitivo al servicio en el mercado.

10.8.PAA-006. Observe las operaciones que se realizan en el Help Desk.

10.8.GSA-006. Revise y evalúe los procesos que en general se ejecutan en el Help Desk.

Se deben tomar en cuenta los siguientes puntos:

- ◆ El direccionamiento y manejo de las llamadas entrantes.
- ◆ El registro, acceso, rastreo, y línea de tiempo que siguen las llamadas para asegurar una respuesta completa y a tiempo.
- ◆ La clasificación y prioridad de las solicitudes.
- ◆ Validación de los usuarios para cambios de contraseñas.
- ◆ La rapidez para contestar las llamadas.
- ◆ La cortesía y paciencia con las que se trata al usuario.
- ◆ Identifique si la base de conocimiento es adecuada para resolver problemas rápidamente.

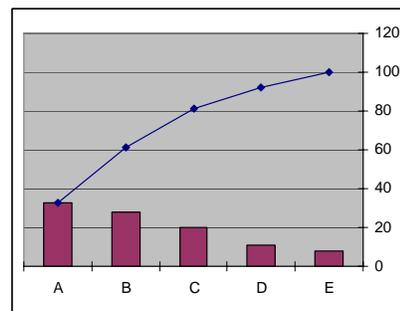
- 10.8.RC-006.** Se deben realizar pruebas de trabajo para determinar si la respuesta se adapta a los controles y procedimientos que tiene la empresa como meta. También para que los elementos no sobresalgan del tiempo o del status normal y para asegurar que todas las peticiones de los usuarios acceden al sistema.
- 10.8.PAA-007.** ¿Existe algún plan para el mejoramiento de los sistemas y de las operaciones?
- 10.8.GSA-007.** Determinar si se ha desarrollado alguna documentación para ayudar a establecer prioridades, definir fechas límite y definir responsabilidades sobre tareas o proyectos.
- 10.8.RC-007.** Con el fin de prever la extensión de operaciones en el Help Desk, se recomienda comprar o construir herramientas que corran en un ambiente multiplataforma, ya que así se adaptarán de mejor forma al hardware y software de la organización. Además de que permitirán una mejor interacción entre las distintas unidades del negocio.
- Establecer si la administración del Help Desk y los empleados tienen el entrenamiento adecuado y si se establecen redes de oportunidades en los campos de productos, servicios, habilidades en comunicación, habilidades técnicas y demás campos pertinentes.
- 10.8.PAA-008.** ¿La empresa realiza algún tipo de evaluación de la información en las llamadas?
- 10.8.GSA-008.** Determinar si se han establecido Indicadores Clave de Desempeño (Key Performance Indicator, KPI) y si los hay, revisar si se están cumpliendo.
- Realizar una prueba real para determinar o validar los KPI.
- Realizar una comparación con los promedios de otros Help Desk en situaciones similares.
- Evaluar el tamaño del staff (número de empleados) en función de la demanda.
- 10.8.RC-008.** Las distribuciones de las llamadas deben estar monitoreadas y programadas apropiadamente para atender los picos y valles en la demanda del consumidor.

Algunos KPI (Key Performance Indicator) típicos son:

- ◆ Número de llamadas por mes; tiempo promedio por llamada; número de llamadas por analista.
- ◆ Porcentaje de nuevas llamadas.
- ◆ Reincidencia en llamadas o eventos.
- ◆ Número de llamadas recibidas al día comparando el número de casos resueltos. Este rastreo identificará si el Help Desk tiene pocos recursos humanos hasta el punto de que no tienen el tiempo suficiente de trabajar en los problemas que reciben.
- ◆ Tiempo promedio requerido para cerrar los casos (incluyendo llamada inicial, seguimiento y consultas subsecuentes).
- ◆ Porcentaje y tipo de llamadas que requieren consulta posterior.

Investigar estas llamadas puede servir como una oportunidad de crear una nueva herramienta para el HD (Help Desk) que permita solucionar el problema en una sola llamada, sin necesidad de seguimiento o consultas subsecuentes.

- ◆ Porcentaje de problemas que se solucionan con la primer llamada comparado con el porcentaje de problemas que requieren un mayor análisis.
- ◆ Clasificación de problemas y Diagrama de Pareto para los diferentes tipos de problemas, ejemplo: problemas de hardware, de software, tipos de aplicaciones, etc.



A= hardware , B= Software, C= aplicaciones, D= Red, E= otros.

- ◆ Porcentaje de llamadas inconclusas o abandonadas.

FUNCIONAMIENTO DE LOS SISTEMAS

- 10.8.PAA-009.** Identifique la forma de uso de los sistemas de cómputo por cada tipo de empleado.
- 10.8.GSA-009.** Revise y evalúe los sistemas de cómputo a los cuales los empleados del Help Desk tienen acceso.

Revisar la documentación del sistema para identificar las capacidades del sistema.

10.8.RC-009. Mediante la evaluación del uso del sistema se podrá identificar si se está utilizando a su mayor capacidad y si los niveles de acceso a estos sistemas son los apropiados.

10.8.PAA-010. ¿Son apropiados o consistentes los cambios y ajustes en los archivos de control con respecto a las políticas de la empresa? (Los archivos de control son utilizados en la mayoría de los sistemas y contienen parámetros críticos que conducen el procesamiento en los sistemas.)

10.8.GSA-010. Revise y evalúe los procedimientos para ingresar cambios en los archivos de control e identifique los parámetros críticos.

10.8.RC-010. Al revisar y evaluar los controles sobre entradas críticas y su salida asociada, se asegura que se captura la información sobre las llamadas, que todas las transacciones tienen un reporte completo y que los archivos se encuentran a salvo de modificaciones sin autorización.

10.8.PAA-011. ¿El personal identifica las rutinas críticas para el funcionamiento del Help Desk?

10.8.GSA-011. Determinar si la edición y evaluación de rutinas se encuentran en campos o funciones que son críticas para el Help Desk.

10.8.RC-011. Se recomienda trabajar con la administración de los clientes para determinar si los reportes producidos por el sistema son los adecuados y clasificar los correspondientes como críticos, de esta manera se garantiza la satisfacción del cliente a corto plazo.

SEGURIDAD EN LOS SISTEMAS

10.8.PAA-012. ¿Se garantiza que los empleados de la empresa de Help Desk sólo tengan acceso a las áreas de los sistemas que les son asignadas?

10.8.GSA-012. Identificar, evaluar y probar todo el entorno de seguridad para el sistema, esto incluye:

- ◆ Verificar si la seguridad física es la adecuada, por ejemplo la vigilancia de las instalaciones, de los equipos y del personal de Help Desk.
- ◆ Métodos y procesos para acceder al sistema.
- ◆ Controles para la identificación y contraseñas de los usuarios.

- ◆ La habilidad para acceder directamente al programa y a los archivos de datos.
- ◆ Los archivos de respaldo, revisar su integridad física tanto como su integridad lógica.

10.8.RC-012. Los usuarios y sus niveles de acceso deben ser apropiados y basados en las responsabilidades de su trabajo.

Las contraseñas deben ser cambiadas periódicamente y las contraseñas anteriores no deben ser permitidas.

Las identificaciones deben caducar después de cierto periodo de tiempo de inactividad. Las identificaciones deben de ser suspendidas si después de varios intentos la contraseña no corresponde.

10.8.PAA-013. ¿Existe algún plan o procedimiento para recuperar los datos del sistema en caso de un evento de problema de hardware, pérdida de archivos o desastre?

10.8.GSA-013. Revisar y evaluar los controles para la verificación de los archivos de respaldo, niveles de retención, procedimientos de almacén y la documentación de los procedimientos anteriores.

Realizar una prueba en tiempo real para validar los archivos de respaldo, su retención y su almacenamiento seguro.

Determinar si existe un Plan de Recuperación Total de Equipo y si se siguen adecuadamente los procesos documentados en este plan.

Determinar si estos planes se han probado recientemente.

10.8.RC-013. El Plan de Recuperación Total de Equipo debe incluir repuestos, formas, terminales, PC, teléfonos y otro equipo necesario. Los procedimientos de restauración y de operación con equipo de cómputo limitado también se deben incluir en forma de un Plan de Funcionamiento Emergente.

Si existieron problemas durante las pruebas, se deben comprobar que se han aplicado acciones correctivas al respecto y que los planes se han actualizado de acuerdo con las necesidades actuales del Help Desk.

Las políticas de retención deben proteger la integridad de la compañía, en caso de que se necesite una restauración total y además debe cumplir con los requerimientos de las regulaciones vigentes en ese aspecto.

REPORTES INFORMATIVOS

- 10.8.PAA-014.** ¿Hay algún encargado o existe alguna forma de verificar que la información en los reportes sea veraz y adecuada a la actividad que realizan los empleados del Help Desk?
- 10.8.GSA-014.** Verificar la veracidad de los reportes, corroborando los totales, rastreando la información hasta la parte de producción de la misma, recalculando operaciones críticas, etcétera.
- 10.8.RC-014.** Se deben diferenciar los reportes importantes de los reportes que son generados constantemente por los analistas y debe existir la separación en las actividades de escribir los reportes y en revisarlos, para asegurarse de que no existen omisiones o errores de cálculo o captura.
- 10.8.PAA-015.** ¿El personal conoce la forma de realizar cambios o modificaciones a los reportes generados?
- 10.8.GSA-015.** Verificar que los códigos de programa están protegidos de cambios sin autorización.

Verificar que existe la documentación adecuada para los programas de soporte.
- 10.8.RC-015.** Los códigos de programa deben estar protegidos de cambios sin autorización, esto garantizará que los reportes no contendrán errores al menos en su generación. También debe existir la documentación adecuada para los programas de soporte y es necesario que se conozca perfectamente el software para realizar los reportes para evitar errores y confusiones en su generación.
- 10.8.PAA-016.** Pida los reportes que se generan y evalúan.
- 10.8.GSA-016.** Evaluar que se generan al menos los siguientes tipos de reporte:

Nivel de la Organización	Periodicidad	Información Requerida
Alta Gerencia	Mensual	Reporte de mediciones financieras. Reporte de satisfacción del cliente. Reporte de eficiencia y efectividad del servicio. Actividades para la estabilización del servicio. Reporte de conflictos no resueltos y preocupaciones.
Equipo administrador	Mensual	Reporte de mediciones financieras. Reporte de satisfacción del cliente.

del servicio		Reporte de eficiencia y efectividad del servicio. Reporte de conflictos no resueltos y preocupaciones. Análisis de causa raíz de las discrepancias del desempeño. Actividades para la estabilización del servicio.
Equipo operador del servicio	Mensual	Reporte de satisfacción del cliente. Reporte de desempeño del servicio. Resolución de las quejas del cliente. Reporte de conflictos no resueltos y preocupaciones. Análisis de causa raíz de las discrepancias del desempeño. Actividades para la estabilización del servicio. Lista de defectos del servicio y su resolución. Lista de empleados ausentes por: enfermedad, entrenamiento, etc.

10.8.RC-016. Los reportes señalados deben desarrollar al menos lo siguiente:

- ◆ Los controles para escalar adecuadamente los problemas.
- ◆ Los controles para rastrear y limitar el acceso a personas autorizadas a los datos de los clientes.
- ◆ Los integrantes de cada departamento tienen los parámetros correctos de autorización y solamente se utilizan en sus respectivas áreas.
- ◆ Si el conocimiento que se ha adquirido está bajo constante mantenimiento para futuras referencias o para imprimirlo en los manuales de usuario.
- ◆ Existen procesos para recolectar información y para evaluar las áreas, para mejorar los beneficios a la comunidad.
- ◆ Los procesos para el monitoreo de las solicitudes de los clientes.
- ◆ Los controles suficientes para asegurar que la administración y los usuarios están al tanto de problemas dentro del ambiente.

10.8.PAA-017. ¿Se cuenta con la información necesaria para identificar a un cliente y que ésta es correcta?

10.8.GSA-017. Verificar qué datos se le piden a los clientes.

Verificar si los datos de los clientes se actualizan.

Verificar que es posible contactar al cliente para garantizar que está satisfecho.

- 10.8.RC-017.** Mantener una fuente de información detallada de clientes y proveedores es una práctica muy importante, ya que de ella se desprenden muchas oportunidades de negocio y pueden garantizar que sus requerimientos sean satisfechos. Los datos que frecuentemente se piden son:
- ◆ Nombre
 - ◆ Clave con la que se identifica en el servicio Help Desk
 - ◆ Correo electrónico
 - ◆ Número de teléfono
 - ◆ Domicilio
- 10.8.PAA-018.** ¿Existe algún procedimiento de revisión de reportes?
- 10.8.GSA-018.** Verificar que la organización establezca los periodos de revisión.
- Analizar que la revisión de los reportes se realicen dependiendo de la importancia que ameriten.
- 10.8.RC-018.** El presentar los resultados en forma gráfica permitirá visualizar la información de interés de forma más general, resaltando los puntos importantes, para las áreas involucradas.
- 10.8.PAA-019.** ¿Se genera un nuevo reporte para el seguimiento de un problema no resuelto?
- 10.8.GSA-019.** Corrobore si es el caso de que el nuevo reporte tenga el número de reporte anterior mientras no se cierre el problema y si se sigue utilizando el mismo número de reporte, el archivo cuente con un tipo de bitácora de los operadores que dieron el seguimiento del problema.
- 10.8.RC-019.** El cierre de los problemas resueltos debe contar con la autorización correspondiente del usuario para cerrar el problema.
- 10.8.PAA-020.** ¿Cuál es el seguimiento que se le da a un reporte con una terminación anormal?
- 10.8.GSA-020.** Verifique la existencia de este tipo de reportes y de un reporte adicional automatizado que identifica el reinicio del trabajo anterior.
- Corrobore que incluye una explicación general o una indicación de las condiciones asociadas con la terminación anormal.

- 10.8.RC-020.** El exceso de terminaciones anormales puede indicar:
- ◆ Instrucciones de operación inadecuadas.
 - ◆ Soporte inadecuado de operaciones.
 - ◆ Entrenamiento o monitoreo de desempeño del operador inadecuados.

DOCUMENTACIÓN

- 10.8.PAA-021.** ¿Los empleados del Help Desk cuentan con los manuales (el manual de atención al cliente, manual de uso de las herramientas del Help Desk, etc.) actualizados?

- 10.8.GSA-021.** Verificar que existe la documentación necesaria para los participantes del Help Desk.

Evaluar que los procedimientos de funcionamiento del Help Desk sean de acuerdo con lo especificado en los manuales.

- 10.8.RC-021.** La documentación debe ser revisada (instructivos, procedimientos, manuales) para determinar si ésta describe adecuadamente los flujos de intercambio de información, las pantallas, ediciones, mensajes de error, operaciones en los procedimientos, procesamiento especial y los reportes. Es importante el entendimiento de que la documentación está redactada para que se realice exactamente lo que se describe en ella, de otra manera es importante corregir las faltas o las omisiones y tener una documentación constantemente actualizada.

- 10.8.PAA-022.** ¿Cuál es la forma de registro de los errores de sistema, programa, operador, telecomunicación y del hardware? ¿Qué documentación se genera al presentarse un problema?

- 10.8.GSA-022.** Verifique la existencia de alguna documentación de control y de los reportes de condiciones anormales.

Verifique que en el registro aparezcan los siguientes datos:

- ◆ Fecha del error.
- ◆ Descripción de la resolución del error.
- ◆ Código del error.
- ◆ Descripción del error.
- ◆ Fuente del error.
- ◆ Fecha y hora de la intensificación del error.
- ◆ Iniciales de la persona responsable de mantener el registro.
- ◆ Iniciales de la persona responsable del cierre del registro.

- ◆ Nombre del responsable de la resolución de errores.
- ◆ Código de situación para la resolución del problema (por ejemplo, no tiene solución en el ambiente actual, problema en espera de una fecha específica, etc.).

- 10.8.RC-022.** No hay razón para que un problema permanezca pendiente por un largo periodo de tiempo, no se debe aceptar que un problema permanezca sin ser resuelto. El riesgo primario que resulta de la falta de atención a los problemas no resueltos es la interrupción de las operaciones del negocio. La resolución de problemas debe ser comunicada a los propietarios de los sistemas, a programación, a operaciones y al personal de usuarios para asegurarse de que los problemas serán resueltos a su debido tiempo.
- 10.8.PAA-023.** Si la empresa cuenta con sitio web, ¿ésta cuenta con documentación detallada de la resolución de los problemas, como herramienta complementaria?
- 10.8.GSA-023.** Analice y evalúe si esta opción resulta beneficiosa para remover cuellos de botella en el servicio.
- 10.8.RC-023.** Un mismo problema puede presentarse repetidas veces, por lo que una documentación detallada puede enseñar al usuario a solucionar sus problemas y contar con su disponibilidad cuando la requiera, es importante que mantenga la documentación actualizada o con un control de las versiones.
- 10.8.PAA-024.** ¿Existe alguna base de conocimientos en donde se guarde la forma de resolución de incidentes?
- 10.8.GSA-024.** Si existe verifique que los operadores tengan permitido agregar o modificar alguna resolución a la base de conocimientos, con el fin de ser reutilizadas en situaciones posteriores.
- 10.8.RC-024.** Se recomienda contar con una base de datos con las resoluciones de incidentes categorizados porque permite a los operadores consultarlo y reducir el tiempo de solución a los problemas del cliente.

CAPÍTULO

XI

AUDITORÍA A MINERÍA DE DATOS

CAPÍTULO XI

AUDITORÍA A MINERÍA DE DATOS

11.1. Introducción a la minería de datos

La minería de datos es un mecanismo de explotación consistente en la búsqueda de información valiosa en grandes volúmenes de datos; es decir, es el análisis de archivos y bitácoras de transacciones, trabaja a nivel del conocimiento con el fin de descubrir patrones, relaciones, reglas, asociaciones o incluso excepciones útiles para la toma de decisiones.

La minería de datos puede ser dividida en:

MINERÍA DE DATOS PREDICTIVA (MDP): usa primordialmente técnicas estadísticas.

MINERÍA DE DATOS PARA EL DESCUBRIMIENTO DE CONOCIMIENTO (MDDC): usa principalmente técnicas de inteligencia artificial.

11.2. Aplicaciones de minería de datos

Actualmente se aplica en áreas tales como:

Aspectos climatológicos: predicción de tormentas, etc.

Medicina: encontrar la probabilidad de una respuesta satisfactoria a un tratamiento médico.

Mercadotecnia: identificar clientes susceptibles de responder a ofertas de productos y servicios por correo, fidelidad de clientes, afinidad de productos, etc.

Inversión en casas de bolsa y banca: análisis de clientes, aprobación de préstamos, determinación de montos de crédito, etc.

Detección de fraudes y comportamientos inusuales: telefónicos, seguros, en tarjetas de crédito, de evasión fiscal, electricidad, etc.

Análisis de canastas de mercado para mejorar la organización de tiendas, segmentación de mercado (clustering).

Determinación de niveles de audiencia de programas televisivos.

Industria y manufactura: diagnóstico de fallas.

11.3. Técnicas de minería de datos

Análisis preliminar de datos usando:

Query tools

Es el primer paso de un proyecto de Minería de datos, se aplica una consulta SQL al conjunto de datos para rescatar algunos aspectos visibles antes de aplicar las técnicas.

Técnicas de Visualización

Son aptas para ubicar patrones en un conjunto de datos, puede usarse al comienzo de un proceso de Minería de datos para determinar la calidad de los datos.

Redes neuronales artificiales

Son modelos predecibles no lineales que aprenden a través del entrenamiento.

Reglas de Asociación

Establecen asociaciones con base en los perfiles de los clientes sobre los cuales se realiza la Minería de datos.

Algoritmos Genéticos

Son técnicas de optimización que usan procesos tales como combinaciones genéticas y mutaciones, etc.

Redes Bayesianas

Buscan determinar relaciones causales que expliquen un fenómeno según los datos contenidos en una base de datos. Se han usado principalmente para realizar predicciones.

Árbol de Decisión

Son estructuras que representan conjuntos de decisiones, y estas decisiones generan reglas para la clasificación de un conjunto de datos.

11.4. Algoritmos de Minería de datos

Supervisados o predictivos

Predicen el valor de un atributo en un conjunto de datos conociendo otros atributos.

A partir de datos cuya etiqueta se conoce se induce una relación entre dicha etiqueta y otra serie de atributos. Esas relaciones sirven para realizar la predicción de datos cuya etiqueta es desconocida.

No supervisados o del descubrimiento del conocimiento

Con estos algoritmos se descubren patrones y tendencias en los datos actuales. El descubrimiento de esa información sirve para llevar a cabo acciones y obtener un beneficio de ellas.

11.5. Etapas principales del proceso de Minería de datos

1. **Determinación de los objetivos.** Delimitar los objetivos que el cliente desea bajo la orientación del especialista en Minería de datos.

2. **Selección y procesado de los datos.** Se refiere a la selección, limpieza, enriquecimiento, reducción y la transformación de las bases de datos.

2.1. Selección de características. Reduce el tamaño de los datos eligiendo las variables más influyentes en el problema.

3. **Extracción de conocimiento** (determinación del modelo). Comienza con un análisis estadístico de los datos, y luego se lleva a cabo una visualización gráfica de los mismos para tener una primera aproximación.

4. **Análisis de los resultados** (interpretación y evaluación). Verifica si los resultados obtenidos son coherentes y los compara con los obtenidos por el análisis estadístico y de visualización gráfica.

Los pasos anteriores se ilustran en la figura 11.1.

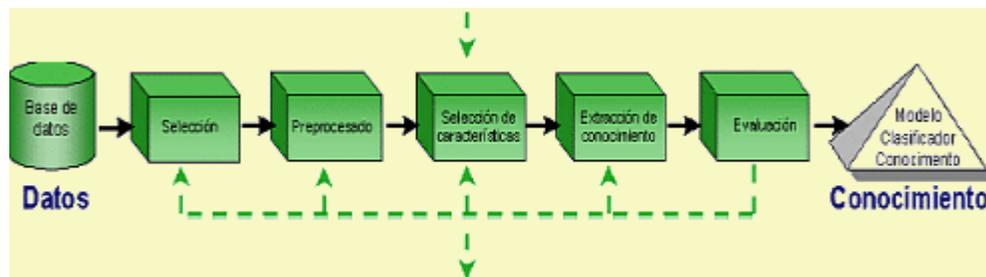


fig. 11.1.

11.6. Extensiones del data mining

Web Mining

Consiste en aplicar las técnicas de Minería de datos a documentos y servicios de la Web.

Las herramientas de Web Mining analizan y procesan los logs para producir información significativa.

Text Mining

Se refiere a examinar una colección de documentos y descubrir información no contenida en ningún documento individual de la colección. Dado que el 80 % de la información de una compañía se almacena en forma de documentos, existen técnicas que apoyan al Text Mining.

11.6.1. Algunos Software

Clementine de SPSS (proveedor líder a nivel mundial de software y soluciones para análisis predictivo)

Las organizaciones utilizan el conocimiento extraído con Clementine para:

- ◆ Retener a los clientes rentables.
- ◆ Identificar oportunidades de venta cruzada.
- ◆ Detectar fraudes.
- ◆ Reducir riesgos y mejorar la prestación de servicios a la administración.
- ◆ Alcanzar un mayor nivel de conocimiento de sus clientes on line, y por lo tanto, mejorar el diseño de sus sitios web.

PolyAnalyst 4.5 de Megaputer

Megaputer es líder en negocios y software inteligentes para Web. Ofrece las mejores herramientas para Data Mining, Text Mining y Web Mining.

- ◆ Plataformas compatibles: Microsoft Windows XP/NT/2000, UNIX y Linux 200
- ◆ Requiere de Microsoft Excel.

11.7. ¿POR QUÉ USAR LA MINERÍA DE DATOS?

- ◆ Ahorra grandes cantidades de dinero a una empresa y abre nuevas oportunidades de negocios.
- ◆ Contribuye a la toma de decisiones tácticas y estratégicas.
- ◆ Proporciona poder de decisión a los usuarios del negocio, y es capaz de medir las acciones y resultados de la mejor forma.
- ◆ Genera modelos descriptivos: permite a empresas, explorar y comprender los datos e identificar patrones, relaciones y dependencias que impactan en los resultados finales.
- ◆ Genera modelos predictivos: permite que relaciones no descubiertas través del proceso del Minería de datos sean expresadas como reglas de negocio.

11.8. Conclusiones

El desarrollo de la tecnología de Minería de datos está en un momento crítico.

Existen elementos que la hacen operable, pero hay factores que pueden crear un desprestigio a esta tecnología como son:

- ◆ Los productos son actualmente costosos, y los consumidores pueden hallar una relación costo/beneficio improductiva.
- ◆ Se requiere de mucha experiencia para utilizar herramientas de la tecnología, para identificar patrones equívocos, triviales o no interesantes.
- ◆ La posibilidad de resolver los aspectos técnicos para hallar patrones en el tiempo o espacio establecido.
- ◆ Manejo de datos del cliente que les puede representar un peligro o riesgo para su privacidad.

11.9. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

11.9.PAA-001. ¿Se tienen bitácoras con el registro de las transacciones?

11.9.GSA-001. Pedir al encargado nos muestre las bitácoras de las transacciones que se efectúan.

11.9.RC-001. Una sesión en las bitácoras de las solicitudes de los servidores web incluirá los recursos que un visitante solicitó durante su estancia en el sitio Web.

11.9.PAA-002. ¿Se cuenta con mecanismos para identificar usuarios y sesiones?

11.9.GSA-002. Revisar que tenga al menos 3 mecanismos para identificar a los usuarios y las sesiones. El primer mecanismo tiene que identificar usuarios y sus sesiones las cuales tengan un tiempo de duración determinado; es decir, la sesión inicia cuando el usuario ingresa en la página web y termina cuando su tiempo de estancia expira o también si se dejan de registrar peticiones.

El segundo consiste en definir los recursos máximos que pueden estar siendo utilizados dentro de una sesión. El tercer método se basa en un algoritmo heurístico basado en el problema de que un visitante no siempre está un tiempo determinado en un sitio y que el número de recursos web solicitados nunca está bien definido.

- 11.9.RC-002.** El análisis del tráfico de acceso a un determinado servidor web es fundamental para entender el comportamiento y hábitos de los clientes/usuarios del sitio, y por otra parte, ayudan a mejorar su diseño.
- 11.9.PAA-003.** ¿El proceso para extraer conocimiento consta de todas las etapas?
- 11.9.GSA-003.** Se revisará que dentro de las etapas se encuentren las siguientes: Limpieza de datos, integración de los datos, selección de datos, transformación de datos, minería de datos, evaluación de patrones, representación del conocimiento.
- 11.9.RC-003.** Se recomienda no pasar a la siguiente etapa hasta que se concluya con la anterior, para así asegurar que la información que se obtenga sea de utilidad.
- 11.9.PAA-004.** ¿La limpieza en los datos se hace de manera correcta?
- 11.9.GSA-004.** Verificar que no se presente ruido ni inconsistencia en los datos
- 11.9.RC-004.** Se recomienda crear programas de limpieza o utilizar algunos que existan comercialmente en caso de las bases de datos que cuenten con gran cantidad de registros.
- 11.9.PAA-005.** ¿Permite la integración de los datos?
- 11.9.GSA-005.** Verificar que puedan combinarse datos que provengan de diferentes fuentes.
- 11.9.RC-005.** La mayoría de las veces es necesario que las empresas que comparten datos tengan las aplicaciones compatibles, con base en un estándar, para poder trabajar con la información.
- 11.9.PAA-006.** ¿Se efectúa la selección de datos?
- 11.9.GSA-006.** Se revisará que se cuente con la capacidad para seleccionar los datos de mayor relevancia.
- 11.9.RC-006.** Para poder extraer datos que sean útiles es necesario que se disponga de ellos. Se debe tomar en cuenta que para extraer conocimiento, se requiere decidir de qué fuentes externas e internas

se van a obtener los datos, así como también la manera de organizarlos y finalmente de que forma serán extraídos.

- 11.9.PAA-007.** ¿Los datos son adecuados para cumplir un propósito en concreto y también aptos para las técnicas que se pretenden emplear?
- 11.9.GSA-007.** Revisar que los datos pasen por un proceso de transformación.
- 11.9.RC-007.** Los datos después de la transformación deben continuar completos y consistentes.
- 11.9.PAA-008.** ¿Los algoritmos de minería de datos trabajan de manera correcta?
- 11.9.GSA-008.** Se verificará que los algoritmos analicen el conjunto de datos, buscando en ellos patrones y tendencias que sean específicos.
- 11.9.RC-008.** Se recomienda que los resultados obtenidos a partir de los algoritmos sean correctos ya que son base fundamental para definir los parámetros de un modelo de minería de datos.
- 11.9.PAA-009.** ¿El procedimiento en la minería de datos dirigida es el indicado?
- 11.9.GSA-009.** Se preguntará qué variable se pretende representar al construir un modelo en específico y verificar si existen posibles relaciones entre las demás variables para poder lograrlo.
- 11.9.RC-009.** Siempre se debe tener muy claro el motivo por el cual se desea representar una variable y no otra.
- 11.9.PAA-010.** ¿La minería de datos clasifica correctamente?
- 11.9.GSA-010.** Verificar que los objetos se agrupen en una clase predefinida dependiendo de las características que tenga.
- 11.9.RC-010.** Cada registro ocupado por un objeto debe estar marcado para identificar el espacio que está cubriendo.
- Las clases deberán estar muy bien definidas.
- 11.9.PAA-011.** ¿La minería de datos permite calcular valores aproximados de variables continuas y discretas?

- 11.9.GSA-011.** Verificar la posibilidad, de que a partir de datos de entrada, pudiéramos hacer estimaciones para alcanzar una variable de interés que en el momento sea desconocida.
- 11.9.RC-011.** Es frecuente que la clasificación y la estimación se usen de manera complementaria para obtener una mejor información de conocimiento.
- 11.9.PAA-012.** ¿Los objetivos en cuanto a la predicción en la minería de datos se cumplen?
- 11.9.GSA-012.** Verificar que los registros estén clasificados conforme a un comportamiento que pensamos obtener a futuro o de algún valor estimado.
- 11.9.RC-012.** Es recomendable tener paciencia porque para verificar la predicción es necesario esperar y después observar. Es también benéfico tener datos históricos para poder construir un modelo y en base a él poder predecir posibles comportamientos a futuro.
- 11.9.PAA-013.** ¿Las reglas de asociación cumplen su objetivo?
- 11.9.GSA-013.** Revisar que los objetos que compartan características en común estén juntos.
- 11.9.RC-013.** Es bastante atractivo desarrollar reglas de asociación si se quieren identificar las oportunidades de venta, pudiendo incrementar las utilidades en productos y servicios.
- 11.9.PAA-014.** ¿Se lleva a cabo el clustering?
- 11.9.GSA-014.** Revisar la realización de segmentación en un grupo diverso de datos y que a partir de ellos sean creados grupos similares.
- 11.9.RC-014.** Algunas veces el clustering se utiliza como paso previo para una forma alternativa de minería de datos o modelado.
- 11.9.PAA-015.** ¿El aprendizaje supervisado se desarrolla de manera completa?
- 11.9.GSA-015.** Verificar que conste de dos etapas:
- Entrenamiento-** Construcción de un modelo a partir de la utilización de un subconjunto de datos con atributos conocidos.

Prueba- Usar el modelo en los demás datos

- 11.9.RC-015.** Si un modelo resulta carente en cuanto a la obtención de una solución predictiva (aprendizaje supervisado) tendremos que recurrir a los métodos no supervisados a través del descubrimiento de patrones y de tendencias en los datos actuales.
- 11.9.PAA-016.** ¿El algoritmo de árbol de decisión permite determinar una solución final?
- 11.9.GSA-016.** Verificar que la muestra de los datos esté disponible, y que el conjunto de condiciones se pueda relacionar desde un nodo raíz hasta las posibles hojas.
- 11.9.RC-016.** Se recomienda utilizar diferentes tipos de algoritmos para la construcción de árboles de decisión, y así poder comparar los datos obtenidos en cada uno de ellos.
- 11.9.PAA-017.** ¿El árbol de decisión creado mediante un algoritmo CART (Classification And Regreition Trees) se realizó conforme a dicho algoritmo?
- 11.9.GSA-017.** Verificar que se construyó con base en los siguientes pasos:
- ◆ Que se hayan tenido un conjunto de datos llamados de entrenamiento, la cual tenga registros preclasificados. Además, datos independientes del registro que determinan el valor del atributo dependiente.
 - ◆ Se particionaron los registros en cada nodo, con base en el atributo que analiza el registro de entrada.
- 11.9.RC-017.** La mejor forma de poder elegir el nodo principal de partición es hacer una consideración inicial de todos los campos independientes (posibles nodos raíz) se lleva a cabo un ordenamiento y se miden los índices de diversidad; el que tenga el mayor índice de diversidad será comparado con otros valores y si no reducen sus índices, deberá ser elegido como nodo raíz de la partición del árbol de decisión.
- 11.9.PAA-018.** ¿Se realizan evaluaciones sobre los árboles de decisiones que se construyen?
- 11.9.GSA-018.** Pedir que sean proporcionados los porcentajes de acierto y de error de cada nodo de particionamiento.

11.9.RC-018. Se debe considerar un posible cambio en los nodos de particionamiento, así como también una modificación al conjunto de entrenamiento, si éstos presentan un porcentaje de error alto. Si la tasa de aciertos es de 100%, se está efectuando una clasificación específica para los registros de entrenamiento y no así, por características que puedan ser extraídas del conjunto. Si existen ramas que proporcionan tasas de acierto bajas se deberán eliminarlas mediante la técnica de poda de ramas débiles.

11.9.PAA-019. ¿El Algoritmo utilizado es el CHAID (CHI squared Automatic Interaction Detection) se aplica correctamente?

11.9.GSA-019. Se revisará que el algoritmo se apege al test de chi cuadrada

$$P(X_0)_D = \int p(x)_D dx$$

En donde:

- $P(X_0)_D$ es la distribución chi cuadrada con D grados de libertad y
- X_0 es el valor de la estadística para un atributo dado.

11.9.RC-019. Siempre es recomendable tener buenos recursos de cómputo sobre todo si el algoritmo que interviene en la elaboración de árboles de decisión hace que se obtengan muchos nodos hijos.

11.9.PAA-020. ¿Los modelos obtenidos son válidos?

11.9.GSA-020. El auditor revisará que el modelo obtenga conclusiones válidas y satisfactorias, de acuerdo con la realidad la cual se pretende representar.

11.9.RC-020. Hacer comparaciones entre diferentes modelos obtenidos para buscar el que mejor se ajuste al problema, y en caso de que ninguno cubra dicha necesidad, se procederá a crear otro modelo.

11.9.PAA-021. ¿Se usan algoritmos genéticos para el análisis de los datos?

11.9.GSA-021. Verificar que dentro de las variables estén las que se desean optimar así como también las de estudio.

- 11.9.RC-021.** Se pretende que los segmentos de información tiendan a reproducirse y a perdurar generación tras generación. Se deben introducir elementos aleatorios (mutaciones) para que las variables tengan modificaciones, para así poder contar con varias soluciones a un problema.
- 11.9.PAA-022.** ¿Se cuenta con el hardware necesario para aplicaciones de minería de datos?
- 11.9.GSA-022.** Se verificará que el hardware tenga la capacidad en velocidad para realizar muchos procesos (en paralelo).
- 11.9.RC-022.** El hardware debe consistir de potentes equipos de cómputo con funcionalidad de multiprocesadores.
- 11.9.PAA-023.** ¿Las técnicas de minería de datos empleadas se encuentran integradas con un data warehouse?
- 11.9.GSA-023.** Revisar que las técnicas trabajen en conjunto con un data warehouse así como también con las herramientas flexibles e interactivas para analizar el negocio.
- 11.9.RC-023.** Se pretende obtener mayor velocidad en cuanto a la extracción, importación y análisis de los datos.
- 11.9.PAA-024.** ¿El almacén de datos se encuentra justificado para realizar la minería de datos?
- 11.9.GSA-024.** Verificar que en caso de tener un almacén de datos se cuente con un volumen considerable de datos o se tenga la posibilidad de que aumenten con el tiempo; además que se puedan combinar de manera no establecida y arbitraria y los mismos provengan de fuentes heterogéneas.
- 11.9.RC-024.** Las ventajas de usar data warehouse siempre se verán a mediano y largo plazo, además de que gracias a un almacén de datos podemos recoger información que también puede ser histórica y que sería de nuestro interés.
- 11.9.PAA-025.** ¿Se presentan acciones cuando se encuentran datos faltantes?
- 11.9.GSA-025.** Se revisará que se puedan tomar acciones como las siguientes:
- ◆ ignorar, ya que el algoritmo presenta robustez a datos que falten.

- ◆ eliminar o reemplazar la columna.
- ◆ eliminar o reemplazar la fila.
- ◆ reemplazar el valor.
- ◆ segmentación, obteniendo modelos diferentes para cada segmento.
- ◆ esperar a que los datos faltantes sean ingresados.

- 11.9.RC-025.** Se recomienda tener un amplio criterio y considerar las razones por las cuales puedan existir datos faltantes y tomar las respectivas acciones.
- 11.9.PAA-026.** ¿Se cuenta con registro de monitoreo para los modelos implementados?
- 11.9.GSA-026.** Pedir un registro de evaluación con datos para detectar si el modelo requiere de actualización.
- 11.9.RC-026.** El registro debe contar con la evaluación de datos nuevos con cierta frecuencia, ya que un modelo que es válido por un tiempo puede no serlo para otro.
- 11.9.PAA-027.** ¿El modelo requiere ser difundido?
- 11.9.GSA-027.** Verificar que el modelo esté expresado de manera comprensible para que pueda ser distribuido en la organización.
- 11.9.RC-027.** Siempre que un modelo involucre a muchos usuarios necesita ser difundido.
- 11.9.PAA-028.** ¿Es posible la visualización de los datos?
- 11.9.GSA-028.** Verificar que cuente con las técnicas necesarias para poder visualizar los datos mediante el uso de gráficos e imágenes.
- 11.9.RC-028.** Con la utilización de imágenes para obtener patrones se aprovecha la capacidad humana, además se puede ayudar al usuario a comprender los patrones descubiertos con mayor rapidez.
- 11.9.PAA-029.** ¿Se cuenta con los dos tipos de visualización en el proceso de minería de datos?
- 11.9.GSA-029.** Se debe contar con visualización previa para entender de una mejor manera los datos, sugerir patrones, así como las herramientas a utilizar.

También se debe contar con la posibilidad de una visualización posterior, ya que mediante esta se pueden mostrar los patrones y tener mejor entendimiento.

11.9.RC-029. Los dos tipos de visualizaciones son necesarias para tener a los dos diferentes tipos de usuarios (los encargados de investigar las relaciones en los patrones y tendencias, y los expertos a los que se les van a mostrar los resultados).

Se requiere de mayor experiencia para poder seleccionar un gráfico dentro de un conjunto de gráficas que proporciona un sistema.

11.9.PAA-030. ¿Se encuentra la información de la web suficientemente estructurada para facilitar la minería de datos de manera efectiva?

11.9.GSA-030. Verificar que el web mining esté estructurado en fases:

- ◆ Debe ser posible localizar documentos relevantes y también no usuales en la red.
- ◆ Debe ser posible extraer la información a partir de un documento, ya sea HTML, XML, texto, PDF, etc.
- ◆ Debe ser posible descubrir patrones generales a partir de sitios web individuales.
- ◆ Se analizarán, validarán e interpretarán los patrones obtenidos.

11.9.RC-030. No solamente la información debe ser relevante también de calidad y autorizada.

CAPÍTULO

XII

AUDITORÍA A SITIOS WEB

CAPÍTULO XII

AUDITORÍA A SITIOS WEB

12.1. Introducción

Un sitio Web es un conjunto de páginas Web relacionadas entre sí.

Una página Web o página de Internet es un documento que contiene información específica de un tema en particular y que es almacenado en algún sistema de cómputo que se encuentre conectado a la red mundial de información denominada Internet, de tal forma que este documento pueda ser consultado por cualquier persona.

La mayoría de las empresas tienen la visión de que el usuario obtenga en un solo sitio todas las posibilidades de información y conocimientos que necesite. Generalmente no funciona ya que conlleva un trabajo inmenso, un número muy elevado de empleados y de inversiones; es decir, unos costos desmesurados.

12.2. Objetivo de una auditoría a sitios web

El objetivo de una auditoría a sitios Web es ofrecer una perspectiva concreta sobre las características que este recurso proporciona, de tal manera que la organización de la cantidad de contenidos y la estructura de información del sitio sea acorde con lo que la empresa requiere.

Esta guía recoge una serie de factores que deben ser considerados a la hora de realizar el análisis de un sitio Web. Sirve tanto para analizar un sitio antes de hacer una propuesta, como para evaluar y auditar secciones ya terminadas en la fase de producción.

Para ello es necesario reunir en un mismo espacio a todos los responsables directos del proyecto: encargados o gerentes, diseñadores de la Web, personas relacionadas con la gestión de clientes, responsables de marketing y comunicación, etc. Es importante la presencia de personas con alto grado de poder de decisión dentro de la empresa, para obtener los resultados deseados en la auditoría.

12.3. Planificación del sitio

El primer paso a la hora de crear un sitio consiste en planificarlo cuidadosamente.

Deberemos tomarnos tiempo para pensar la estructura que va a tener el sitio. No debe creerse que sea un tiempo perdido, ya que tener en la cabeza de antemano la estructura de un sitio nos va a ahorrar después mucho tiempo y problemas.

12.4. Tipos de promoción

Una vez que ha sido diseñado el sitio Web y está en el servidor de nuestro proveedor de Internet. El siguiente punto que tenemos que seguir para que la presencia en Internet pueda ser rentable para la empresa, es el de realizar algún tipo de promoción de acuerdo con los objetivos o políticas de la empresa.

Las diferentes formas de promoción están ordenadas en función de su origen:

- ◆ Promoción on-line se refiere a que engloba todas aquellas opciones por desarrollar dentro de Internet.
- ◆ Promoción interna, se entiende que es todo aquello que se puede realizar dentro del propio sitio Web.
- ◆ Promoción externa es todo aquello que puede realizarse fuera del sitio Web.

12.5. Formas de publicación de sitios web

Una vez que usted haya decidido establecer un sitio Web en la red mundial, necesitará decidir dónde albergarlo. Sus archivos de la página Web serán albergados en una computadora anfitriona (servidor Web) conectada a Internet las 24 horas del día. Este servidor puede ser una computadora ubicada en su casa, en su oficina, o puede usar uno de los crecientes proveedores de servicios de albergue de sitios Web, en donde ellos se encargan de los detalles técnicos, lo que le permite concentrarse en el desarrollo del contenido. De cualquier modo, hay que tomar en cuenta los pros y los contras.

12.6. PREGUNTAS O ACCIONES PARA EL AUDITOR (CI-PAA-XXX); GUÍA O SUGERENCIAS PARA EL AUDITOR (CI-GSA-XXX) Y RECOMENDACIONES PARA EL CLIENTE (CI-RC-XXX). (C=CAPÍTULO, I=INCISO)

EL MODELO DEL NEGOCIO

12.6.PAA-001. ¿El sitio Web cumple con las expectativas de la empresa? ¿Cuáles son los objetivos de la empresa al crear el sitio Web?

12.6.GSA-001. Analice la meta del sitio y determine si el sitio Web quiere entretener, enseñar, informar, persuadir, compartir o vender.

Las respuestas le ayudarán a determinar los contenidos y el diseño indicados para el sitio Web.

12.6.RC-001. La mayoría de los sitios Web son una extensión de los objetivos del negocio, para que el sitio logre los objetivos de la empresa, el diseño Web debe considerar la perspectiva de los consumidores o usuarios desde el principio hasta el final.

La arquitectura de hardware, el software, las comunicaciones, el contenido y el diseño visual deben mezclarse para hacer que la experiencia del usuario sea eficaz y permitir que los objetivos del negocio sean satisfechos.

Sitios Web lentos y poco útiles significan oportunidades y negocios perdidos, ya que los clientes demandan permanentemente respuestas

rápidas y cuando ellos no las obtienen entonces se van a los sitios de nuestros competidores con un sólo click.

- 12.6.PAA-002.** ¿Qué enfoque ha dado la empresa a su situación en Internet?
- 12.6.GSA-002.** Analice si el sitio Web es coherente con los temas que trata y la audiencia que quiere cautivar.
- Corrobore si la empresa trata de satisfacer al espectro más amplio de usuarios dando una información general o si los usuarios tienen la necesidad de perspectivas más o menos detalladas de la información.
- 12.6.RC-002.** Los sitios Web deben ofrecer una perspectiva concreta y un volumen limitado de información, de tal manera que no sea problema organizar la cantidad de contenidos y sea manejable la estructura de información del sitio.
- 12.6.PAA-003.** ¿Quiénes son los usuarios del sitio Web? ¿Ha analizado el tipo de personas que visitan el sitio Web, con sus edades, sexo y nivel de educación?
- 12.6.GSA-003.** Ponerse en el lugar del usuario y descubrir por qué entran allí, nos da información sobre el nivel de interés en el producto y lo que se ofrece.
- Determine si es el público al que se quiere llegar.
- 12.6.RC-003.** El sitio Web debe hablar el mismo lenguaje que el usuario, con palabras, frases y conceptos que le sean familiares. Tiene que seguir las convenciones "del mundo real", para que la información aparezca natural y lógica.
- Determine la mejor forma para llamar la atención de sus visitantes. Por ejemplo, una apariencia sobria y seria le ayudará a ganar credibilidad entre usuarios adultos, mientras que un diseño atrevido (o incluso una buena animación) podría "enganchar" fácilmente a los jóvenes.
- 12.6.PAA-004.** ¿Están las herramientas que facilitan que el usuario se sienta con el control del sitio?
- 12.6.GSA-004.** Observe cautelosamente la funcionalidad del sitio, verificando por ejemplo:
- ◆ Si al abrir alguna ventana éste cubre el navegador.
 - ◆ Si hay animaciones que requieran plug-ins especiales.

- ◆ Si existe alguna forma de "saltar" (skip) las animaciones.
- ◆ Si hay manera de bloquear los pop-ups, para evitar la proliferación de ventanas en la pantalla del usuario.
- ◆ Si cuentan con una "salida de emergencia" en caso de elegir erróneamente, para dejar las cosas tal como estaban.
- ◆ Si existe algún enlace para volver al inicio en cada página.

12.6.RC-004. Se espera que los desarrolladores del sitio Web hayan considerado el uso de ciertas técnicas de codificación y permitan que el usuario tenga una experiencia satisfactoria al navegar por las páginas.

PLANIFICACIÓN Y ANATOMÍA DEL SITIO

12.6.PAA-005. ¿Se realizó la planificación de su sitio Web? ¿Cómo está estructurado su sitio Web?

12.6.GSA-005. Verifique el tipo de información o productos que encuentra en las páginas.

Analice la forma de exploración del sitio. Determine que tipo de jerarquía utiliza.

12.6.RC-005. La estructura es el esqueleto que se utiliza para enlazar y "colgar" los contenidos que lo componen.

La página principal es el primer lugar que consultan los usuarios, por lo que no debe haber información irrelevante o que raramente se necesita, éstas deben estar en las páginas de contenido.

Las secciones son las partes en que se divide el sitio, deben conservar las características y lineamientos generales de diseño, contienen el desarrollo de la información que el usuario está buscando por medio de los vínculos de la página principal.

Para estructurar un sitio Web se debe usar una jerarquía que permita tener una navegación lógica por él.

Las jerarquías más comunes son:

Árboles estrechos. Una página principal tiene vínculos a las secciones del sitio Web, que a su vez se dividen en subsecciones. La información permanece bien organizada, pero en ocasiones el usuario debe hacer varios clicks para llegar a lo que busca.

Árboles anchos. Los usuarios acceden directamente a las páginas de contenido desde la página de inicio. No tiene secciones. Es una jerarquía indicada para secciones o proyectos muy pequeños, pues a

medida que crece el sitio Web se torna confuso y se pierde el orden jerárquico de la información.

Malla completa. Todas las páginas del sitio Web están enlazadas entre sí. Se usa en proyectos especiales que no tengan muchas páginas, pues el número de vínculos o enlaces de cada página será igual al número de páginas menos una. Es decir, en un sitio Web con 20 páginas, cada página deberá tener espacio para 19 vínculos y el vínculo de la página de inicio.

Jerarquía mixta. Es la estructura más común en Internet. Aunque los datos se organizan en una estructura de árbol, brinda la posibilidad de dar saltos entre páginas o secciones, sin necesidad de un orden lógico.

Sirve para explorar las partes más profundas del sitio Web, incluso desde la primera página (por ejemplo, cuando hay servicios para descargar archivos).

12.6.PAA-006. ¿Qué ofrece su sitio Web? ¿Qué más puede ofrecer?

12.6.GSA-006. Analice el tipo de valor que dan los usuarios por el contenido de su sitio Web. Determine si es debido a que se le da personalización, síntesis, belleza, comodidad, esquemas, gráficos y/o información detallada.

Determine si el contenido se asocia con la imagen de la marca o de la fuente de origen.

12.6.RC-006. El sitio Web debe ser fácil de indexar en una lista de favoritos. Esto se logra evitando el uso intensivo de frames y utilizando nombres de archivos que no caduquen. Por ejemplo, para los artículos que son noticias o textos circunstanciales, lo recomendable es nombrar las páginas con la fecha, de manera que al publicar una nueva noticia no se sobrescriba la antigua anulando la URL que algún usuario puede haber marcado como favorita.

12.6.PAA-007. ¿Se siguen pautas de diseño acordes a los conocimientos de la interacción persona-PC (IPO /HCI)?

12.6.GSA-007. Verificar que las pestañas o etiquetas de los vínculos o enlaces tengan los mismos nombres que los títulos de las páginas o secciones a las que se dirigen.

Verificar que las mismas acciones (botones, links) lleven a los mismos sitios.

Verificar que los mismos elementos sean iguales en todo el sitio Web.

12.6.RC-007. Es recomendable que se sigan ciertas pautas de diseño debido a que los clientes están acostumbrados a una serie de convencionalismos que no es aconsejable modificar ya que los han ido aprendiendo y adquiriendo tras cierto tiempo.

12.6.PAA-008. ¿Necesita que el sitio Web siempre esté disponible en Internet?

12.6.GSA-008. Evalúe el nivel de demanda del sitio Web, identificando las necesidades del cliente en este ámbito.

Verifique el espacio que ocupa el sitio Web en el host.

Identifique si el servidor de hosting es dedicado o es compartido.

12.6.RC-008. El servicio de hosting es un servicio que permite que el sitio Web sea consultado y publicado desde la red. Si el sitio Web es de alta demanda es conveniente que el servidor de hosting sea dedicado porque tiene una máquina entera a su disposición, mientras que si utiliza el servidor de hosting compartido o no dedicado, éste comparte los recursos de la máquina con otros clientes de la empresa que da hosting. Por lo tanto, no se cuenta con todos los recursos de la máquina y esto hace que a veces un cliente demande muchos recursos y haga que su vecino baje el rendimiento de su sitio Web.

12.6.PAA-009. ¿Cuánto tiempo tarda en cargarse cada una de sus páginas Web con un módem de 56K?

12.6.GSA-009. Pruebe cada una de las páginas del sitio Web en una computadora con conexión vía telefónica, para verificar el tamaño de cada página.

12.6.RC-009. Una página estándar no debería sobrepasar los 60K, lo que conlleva una carga de unos 30 segundos con un módem de 56K.

12.6.PAA-010. ¿Su sitio Web tiene un dominio que tiene relación con el contenido o finalidad de la página? ¿Es fácil de deletrear y recordar?

12.6.GSA-010. Verificar si el nombre del dominio tiene la extensión más adecuada (.com, .gov, .edu, .org, .mil, .net o la extensión del país de origen).

12.6.RC-010. Es importante tener el nombre del sitio Web ya registrado porque es el nombre con el que se identifica el sitio Web de la empresa. Además, porque cualquier persona ajena a la empresa puede inscribir dicho

dominio con el nombre de la empresa que desee, con el riesgo que esto significa para una marca.

12.6.PAA-011. ¿Cada cuándo realiza el servicio de mantenimiento de su sitio Web?

12.6.GSA-011. Verifique la fecha de la última modificación de las páginas del sitio Web.

Vea si tiene avisos recientes.

12.6.RC-011. La información y eventos publicados deben ser vigentes, impidiendo mantener publicaciones cuya vigencia haya concluido, pues esto provoca que el sitio Web se perciba como poco confiable. Así también, si existen contenidos nuevos, es bueno que se destaquen, para que se vea que se renueva constantemente.

PROMOCIÓN

12.6.PAA-012. ¿Muestra la página de inicio la naturaleza del negocio y se identifica el logotipo o marca?

12.6.GSA-012. Verifique que al navegar en las páginas del sitio Web, sea notorio la procedencia del contenido.

Analice si la primera página que ve el usuario se identifique y sea claro lo que ofrece la empresa.

12.6.RC-012. El usuario se encuentra ante decisiones que concluirán en una posible compra, por lo que es esencial crear una sensación de seguridad que permita al cliente olvidarse de la navegación y centrarse en la información ofrecida.

Existen diversas formas de lograr esa sensación de comodidad:

- ◆ Logotipos de la empresa siempre presentes.
- ◆ Títulos de página claros.

12.6.PAA-013. ¿Aparece la marca en un lugar importante dentro de la página?

12.6.GSA-013. Localice la posición del logotipo en las páginas.

12.6.RC-013. Recuerde que la marca (logotipo) puede servir como un vínculo o enlace a la página de inicio del sitio Web.

12.6.PAA-014. ¿Tiene banners su sitio Web? ¿Tienen un tamaño y lugar fijo?

12.6.GSA-014. Verifique la cantidad de banners que contiene cada página del sitio Web.

Verifique la posibilidad de cerrar banners y el tiempo que aparecen en la página.

Analice si la existencia de banners dificulta la visibilidad del contenido de la página.

12.6.RC-014. Si el sitio contiene banners, trate de optimar el tamaño al mínimo.

Si el sitio "vive" de la publicidad considere la posibilidad de ubicarlos en la parte superior de la página o en el margen derecho (según estudios, funcionan mejor los que se encuentran a la derecha, cerca de la barra de scroll).

NAVEGACIÓN

12.6.PAA-015. ¿Aparece la navegación en un lugar prominente, donde se vea fácilmente? ¿Tiene el sitio Web un site map o un buscador para quienes quieren acceder directamente a los contenidos sin tener que navegar?

12.6.GSA-015. Analizar si hay patrones coherentes en la jerarquización, agrupación y presentación de contenidos.

Verificar si es necesario realizar la misma petición por el usuario para acceder a determinado sitio, es decir existe otra forma más rápida de acceder a una página que ya ha sido consultada.

12.6.RC-015. Si su navegación está hecha con imágenes, considere también tener una navegación en texto plano (puede ser al final de la página), con el fin de tener textos alternos cuando no se encuentre disponible o no se logre cargar la imagen o información solicitada.

El sitio debe tener los objetos, acciones y opciones a la vista. El usuario no tiene que recordar dónde estaban las cosas que buscaba.

Si bien es imposible tener todas las opciones a la vista en sitios demasiado extensos, al menos debería haber una categorización clara de los contenidos que indique el camino a seguir. Una buena redacción de los enlaces, las cabeceras de contenidos y en los menús, ayuda a que el usuario no se pierda.

El sitio Web debe contar con una distribución clara y consistente que permita al usuario identificar las áreas que la componen (navegación, menús, despliegue de información, entre otros).

La estructura del sitio debe minimizar su nivel de profundidad, con la finalidad de no complicar la navegación en el mismo. La profundidad recomendada es de tres a cinco niveles.

- 12.6.PAA-016.** ¿Existen enlaces rotos o que no conducen a algún sitio?
- 12.6.GSA-016.** Corrobore la existencia de enlaces rotos.
- 12.6.RC-016.** Elimine los enlaces rotos mientras corrige los errores, cualquier obstáculo o barrera, por pequeña que sea, será suficiente para que el cliente abandone nuestra Web para irse a la competencia. Facilitar la navegación y mejorar su experiencia de uso es la mejor manera de garantizar el éxito de nuestro negocio.
- Los enlaces deben ser descriptivos, de modo que simplifiquen la búsqueda de información.
- Debe mantenerse consistencia en el formato de los enlaces con la finalidad de que sean fácilmente distinguibles.
- 12.6.PAA-017.** ¿Sabe dónde se encuentra exactamente, cuando está navegando en el sitio Web?
- 12.6.GSA-017.** Verificar la existencia de elementos que permitan al usuario saber exactamente dónde se encuentra dentro del sitio Web y cómo volver atrás.
- 12.6.RC-017.** Es deseable contar con "breadcrumbs" que orienten al usuario y le permitan saber dónde está. Cuando existan procesos que impliquen varios pasos a seguir, es conveniente informarle al usuario de en qué etapa se encuentra y cuántas le faltan para acabar la tarea. Esto se puede lograr usando enumeración de pasos, con navegación contextual. Asimismo, lo ideal es que cada paso sea sólo una acción y que reciba confirmación de que se ha ejecutado satisfactoriamente.
- 12.6.PAA-018.** ¿Aparecen mensajes de error en su página?
- 12.6.GSA-018.** Asegúrese de que el motor de búsqueda acepta errores ortográficos y que se actualiza periódicamente.

Corrobore que los mensajes inesperados de error proporcionen información de cómo solventar el error.

12.6.RC-018. Lo ideal es que un sitio Web pueda ser navegado sin necesidad de ayuda, pero existen aplicaciones complejas que deben contar con asistencia, como en el caso de un sitio Web con herramientas novedosas, el uso de éstas pueden inducir a confusión. Es importante tener la ayuda integrada en el contenido mismo. Es decir, la ayuda puede ser mediante la presentación de un texto breve descriptivo, en relación con el contenido que se está viendo, que al dar click lo llevarán a una sección de ayuda completa, donde se pueda ver todo el contenido de la misma.

Los clientes sólo usan el 5% de su tiempo de navegación para realizar transacciones, el 95% restante lo dedican a buscar productos, comparar y otra serie de tareas no transaccionales. De ahí la importancia de que esta fase del proceso de compra esté tan estructurada y de que no lleve al usuario a cometer errores que agoten el tiempo que está dispuesto a dedicarle a esta tarea en esfuerzos inútiles.

CONTENIDOS

12.6.PAA-019. ¿Es coherente el contenido con el contexto de la página o sitio Web?

12.6.GSA-019. Analizar si existe congruencia en el diseño con el contenido, al igual que las imágenes que se muestren.

Verificar la jerarquía de la información en mayor a menor importancia.

Corroborar la existencia de ruido visual que es generado por la acumulación de elementos.

12.6.RC-019. Hay que evitar la información irrelevante y ceñirse a lo necesario. Una buena idea es dosificar la información y no ofrecer todos los detalles de una vez. Debemos ajustarnos al nivel de información demandado por el usuario.

12.6.PAA-020. ¿La redacción es corta y precisa?

12.6.GSA-020. Verificar que la información sea clara y concisa.

- 12.6.RC-020.** Evite los textos demasiado extensos. Lo deseable sería que cada párrafo transmita una idea. El uso de palabras apropiadas al contexto del contenido y al perfil de la comunidad a la que está enfocado el contenido, permite a los lectores concentrarse en el mensaje y comprenderlo de manera fácil y sencilla. También asegúrese de que la estructura gramatical, ortografía y redacción sean correctas.
- Con la finalidad de preservar la imagen deseada originalmente debe utilizarse fuentes tipográficas estándar en los navegadores (arial, verdana, times new roman, Georgia).
- La presentación de la información en cada página debe respetar la forma de lectura jerárquica de arriba hacia abajo y de izquierda a derecha.
- El contraste entre letra (color/tamaño) y fondo debe permitir la lectura de manera sencilla, aún en los letreros más pequeños y además debe eliminar los problemas de impresión.
- 12.6.PAA-021.** ¿Existen referencias cruzadas entre textos que están relacionados?
- 12.6.GSA-021.** Corrobore si existe manera de acceder a la misma información usando referencias diferentes.
- 12.6.RC-021.** Evite usar líneas horizontales para hacer separaciones en los textos, pueden ser interpretadas como el fin de la información.
- Lo mismo sucede con informaciones que aparecen duplicadas en el sitio, bajo distintos nombres. Por ejemplo, un enlace a "ayuda" debe llevar a una página que se llame así y no "preguntas frecuentes".
- Igualmente, si existen preguntas frecuentes, deben estar en una página llamada así y no duplicarse para aparecer también en "ayuda".
- 12.6.PAA-022.** ¿Las imágenes que se muestran tienen la resolución correcta?
- 12.6.GSA-022.** Corrobore que las imágenes sean de una resolución mínima de 800 x 600 píxeles siendo la recomendable de 1024 x 768.
- 12.6.RC-022.** Las imágenes demasiado grandes pueden cortarse en "trocitos" y unirlos mediante tablas para acelerar la descarga. Considere este recurso, si la velocidad en su sitio Web es un factor importante.
- No deben utilizarse las mismas imágenes para un botón que para algo que claramente es un elemento decorativo.

Debe evitarse el uso de páginas con leyendas como “Página en construcción” o “Próximamente podrá consultar la información en este sitio Web” o cualquier leyenda similar, ya que dan la imagen de un sitio Web poco serio y profesional.

12.6.PAA-023. ¿En alguna de sus páginas tiene una animación cíclica?

12.6.GSA-023. Analice la importancia de la existencia de cada una de las animaciones en el sitio Web.

Verifique si existe alguna forma de la animación que utilice menos recursos.

12.6.RC-023. Evite las animaciones cíclicas (ej. gifs animados que se repiten), a menos que cumplan con un propósito claro.

Use animaciones Flash sólo si es absolutamente necesario. Si es posible hacer lo mismo utilizando DHTML, hágalo.

TECNOLOGÍA

12.6.PAA-024. ¿La tecnología utilizada en el sitio Web es compatible con el software y hardware de los usuarios objetivos?

12.6.GSA-024. Corroborar si es necesario descargar elementos como plug-ins para poder usar el sitio Web.

Corroborar si se le informa al usuario de la necesidad de descargar plug-ins y si se le explica la importancia de hacerlo.

Verificar que la Web este sustentada al menos por los siguientes protocolos o acuerdos tecnológicos HTTP y CGI.

12.6.RC-024. Los estándares de la Web son un término general para referirse a los estándares y especificaciones que describen aspectos generales de la World Wide Web. De manera reciente estos términos se han asociado a dos objetivos; primero, para el correcto desarrollo de un sitio Web y segundo para el desarrollo y filosofía del diseño del sitio Web.

También están los estándares que se relacionan con aspectos de Internet y se enfocan directamente o indirectamente en el desarrollo y administración de los servicios del sitio Web.

Algunas organizaciones que puede consultar para la recomendación y uso de los estándares son las siguientes:

- ◆ World Wide Web Consortium (W3C)

- ◆ Internet Engineering Task Force (IETF) con las siguientes publicaciones:
 - ◆ Internet Standard (STD)
 - ◆ Request for Comments (RFC)
- ◆ International Organization for Standardization (ISO)
- ◆ ECMA International
- ◆ Unicode Consortium
- ◆ Internet Assigned Numbers Authority (IANA)

La implementación de un sitio Web debe ser independiente del navegador; por lo tanto deberá contemplarse por lo menos una versión anterior de cada navegador y no usar leyendas del tipo: “Esta página se ve mejor en el navegador X ”.

En caso de utilizar tecnología no estándar que requiera que los usuarios instalen librerías (plug-ins) adicionales, debe incluirse el enlace a los sitios de los cuales pueden obtenerse, así como instructivos claros sobre cómo realizar su instalación.

- 12.6.PAA-025.** ¿Requiere de intercambio de información con el usuario? ¿La información que envía es confidencial?
- 12.6.GSA-025.** Verificar si utiliza algún protocolo de seguridad, como SSH, SSL, TSL o HTTPS.
- 12.6.RC-025.** Los protocolos son utilizados para intercambiar información con el fin de que ésta no sea interceptada por terceros. Contar con protocolos seguros es importante tanto por las preocupaciones relacionadas con la privacidad como para permitir el comercio electrónico.

INTERFAZ

- 12.6.PAA-026.** ¿El sitio Web es fácil de usar para nuestros usuarios objetivo?
- 12.6.GSA-026.** Comprobar si se realizan mejoras prácticas de “usabilidad” en el sitio Web o si éstas son adecuadas para el usuario.
- 12.6.RC-026.** Puede usar diferentes técnicas para determinar la “usabilidad” del sitio Web, como las siguientes:

Benchmark que consiste en determinar los sitios competidores directos y analizarlos. También se analizan aquellos sitios que aunque no son competidores, pueden servir como referencia para llevar a cabo acciones parecidas a sus sitios.

Análisis heurístico es una de las técnicas más utilizadas y conocidas, consiste en contrastar las páginas del sitio con una serie de criterios que se denominan “principios heurísticos”.

Se pueden dar varios tipos de análisis heurísticos atendiendo a su alcance:

- ◆ Análisis del sitio Web completo
- ◆ Análisis de secciones concretas, dentro del sitio Web, definidas previamente por quien encargue el estudio.

Normalmente el reporte se ordena según las mismas secciones del sitio Web y por la severidad o grado de prioridad de los problemas detectados.

El estándar relativo a la “usabilidad” en aplicaciones web será la ISO/AWI 23973 (Software ergonomics for World Wide Web User Interfaces)

La norma hace referencia a cuatro grandes áreas:

- ◆ propósito y estrategia
- ◆ contenido y funcionalidad
- ◆ navegación e interacción
- ◆ presentación y diseño de elementos multimedia

Determina un modelo y un escenario de trabajo para la aplicación de la normativa; es decir, determinará cómo, cuándo y dónde llevar a cabo las prácticas de “usabilidad” para interfaces Web.

Algunos estándares que también pueden ser útiles son:

- ◆ ISO/IEC 11581: Símbolos y funciones icónicas.
- ◆ IEC TR 61997: Guías para interfaces de usuario en sistemas multimedia de propósito general.
- ◆ ISO/IEC 18021: Tecnologías de la Información - Interfaz de usuario para dispositivos móviles.
- ◆ ISO 13407: Diseño centrado en el usuario para sistemas interactivos.

12.6.PAA-027. ¿Se ve el sitio Web exactamente igual tanto en Mac como en PC?

12.6.GSA-027. Corrobore que el sitio Web se visualice igual en diferentes sistemas operativos.

- 12.6.RC-027.** El sitio debe ser compatible con distintas versiones de sistemas operativos.
- Muchas veces hay scripts que no se ven cuando se usa Macintosh o PC. Hay que tener cuidado con las fuentes, los colores y los scripts usados en el sitio Web.
- 12.6.PAA-028.** ¿Se ve el sitio exactamente igual tanto en Internet Explorer como en Netscape u otros navegadores?
- 12.6.GSA-028.** Corrobore que el sitio Web pueda ser visualizado y navegado igual en diferentes navegadores.
- 12.6.RC-028.** Recorra a código específico para que se muestre igual (simplifique a versiones anteriores de HTML o utilice JavaScript).
- 12.6.PAA-029.** ¿Se han previsto respuestas del sistema frente a interacciones del usuario?
- 12.6.GSA-029.** Verificar que el sitio Web al realizar alguna operación muestre un mensaje indicándole qué está ocurriendo y el tiempo estimado que tendrá que esperar.
- Verificar que cuando se presente un error se le informe al usuario.
- Verificar cuánto tarda el servidor en finalizar una tarea y responder al usuario. (El tiempo máximo que esperará un usuario es de 10 segundos).
- 12.6.RC-029.** El sitio Web siempre debe mantener al usuario informado sobre lo que está sucediendo, a través de un feedback apropiado en un tiempo razonable. Por ejemplo, presentar mensajes de espera cuando se está efectuando una transacción (Ej., un banco) o bien de confirmación cuando se ha efectuado una operación solicitada por el usuario (Ej., "su pedido ha sido aceptado").
- Se debe tener un diseño cuidadoso que prevenga la ocurrencia de errores. La mayoría de los errores cometidos por los usuarios se dan al rellenar formularios. Es prudente usar sistemas de validación antes de que el usuario envíe su información y deba volver atrás para corregir.
- 12.6.PAA-030.** ¿Puede el usuario ponerse en contacto para hacer sugerencias o comentarios?

12.6.GSA-030. Verificar si los usuarios requieren registrarse.

Verificar si se muestra la política de privacidad para el usuario.

Verificar que la liga de enlace al correo electrónico funcione correctamente.

12.6.RC-030. La finalidad es mostrar al usuario toda la información necesaria para ponerse en contacto con la empresa. Sería conveniente colocar todos los datos de la empresa, como dirección postal, ubicación en la ciudad, teléfonos, correo electrónico, etc.

Mediante estos datos surgen estadísticas que le indican al personal del sitio Web las preferencias, nivel social, pasatiempos y demás información incluso geográfica de los navegantes.

Los sitios Web deben mostrar las políticas de uso del mismo y/o confidencialidad de la información en él publicada, los términos y condiciones bajo los cuales se preste algún servicio, así como las exclusiones aplicables.

EN CASOS APLICABLES

Si se contempla el uso de un buscador en el sitio Web:

12.6.PAA-031. ¿El sitio Web cuenta con un buscador?

12.6.GSA-031. Asegurar que los resultados provean información precisa respecto a la página que contiene las palabras clave.

Asegurar que se resaltan las palabras clave en la lista de resultados y se proporcionen las listas de resultados junto con una liga a la información de interés.

12.6.RC-031. El buscador debe realizar las consultas en todo el sitio Web. En caso que las búsquedas sean limitadas debe de indicarse las restricciones, con la finalidad de que él seleccione el que mejor sirva a sus necesidades. También debe tratar las mayúsculas, minúsculas y los acentos como caracteres equivalentes.

Si se usan versiones en otros idiomas:

12.6.PAA-032. ¿El sitio Web cuenta con una versión en otro idioma?

12.6.GSA-032. Asegurarse que sea visible el enlace de cambio de idioma.

12.6.RC-032. En las traducciones a otros idiomas deben cuidarse el contexto, la redacción y la ortografía.

Si el sitio se planea para ser consultado en dispositivos de acceso móvil:

12.6.PAA-033. ¿La entidad tiene planeado el despliegue de su sitio Web en un dispositivo móvil?

12.6.GSA-033. Analice los objetivos de la empresa y los usuarios del sitio Web.

Verificar que el contenido es adecuado para el contexto de dispositivos móviles.

Verificar que no se utilicen elementos no soportados por la generalidad de estos dispositivos.

Verificar que se consideran las limitaciones de recursos y características de los diferentes tipos de dispositivos.

12.6.RC-033. Debido a la existencia de una gran variedad de dispositivos de acceso móvil que cuentan con diferentes características y limitantes, es recomendable tomar en cuenta las siguientes pautas para conservar la consistencia y uniformidad del contenido:

- ◆ Evitar el uso de páginas que se actualicen automáticamente, si se requiere hacer uso de ellas, informar al usuario y proporcionar los medios para detener la actualización.
- ◆ Utilizar un conjunto de caracteres que sea soportado por una gran variedad de dispositivos.
- ◆ Incluir mecanismos de acceso rápido al menú de navegación y las funcionalidades usadas frecuentemente.
- ◆ Mantener el número de pulsaciones de teclas al mínimo, cinco como máximo por página.
- ◆ Evitar la saturación visual del sitio Web al mantener un diseño simple y ligero.
- ◆ Mantener el tamaño de la página en porciones acordes con los mecanismos de despliegue de los dispositivos.
- ◆ Limitar el uso de las barras de desplazamiento sólo a una dirección.

CONCLUSIONES

CONCLUSIONES

La auditoría a tecnologías de información deberá ser considerada como pilar indispensable para el adecuado funcionamiento de una empresa.

Debido a que las Tecnologías de Información (TI) cada vez se presentan con mayor diversidad en las organizaciones, se debe buscar el mejor desempeño, si se desea permanecer en un buen mercado de negocios.

Como resultado a las presiones competitivas y económicas en el ambiente actual del negocio, es necesario disminuir costos por medio de mejores prácticas para asegurar que los riesgos se manejan en conformidad con los objetivos del negocio.

El auditor en TI, para evaluar los sistemas y procesos del negocio, deberá conocer las necesidades prioritarias para la organización, los conocimientos y experiencias disponibles del personal, los medios para reforzar el uso de estándares, el estado de los proyectos en la empresa y establecer una metodología que guíe, de manera ordenada, las relaciones y conductas de los grupos e individuos, para asegurar que los riesgos identificados sean mitigados y controlados hasta alcanzar un nivel aceptable.

Otro punto importante al cual llegamos, es que las auditorías a TI son una actividad que requiere que el auditor tenga un amplio conocimiento en la TI que audite, así como las características de un líder para dirigir al grupo de personas que colaborarán con él para realizar las auditorías que se les asignen.

Como una ayuda para auditores y profesionales en TI, la serie de preguntas, actividades, guías, sugerencias y recomendaciones, plasmadas en este trabajo de tesis, esperamos que contribuya como una ayuda para poder consultar lo que debería auditarse para cada una de ellas. Seguramente para fines aun más precisos y profesionales, deberá ser detallada a un nivel mayor y adentrarse con más profundidad en cada tema.

La elaboración de éste amplio documento nos ha proporcionado una gran cantidad de experiencias que han servido para reflexionar en varios puntos, de las cosas más importantes consideramos que el trabajo en equipo fue un verdadero reto y algo muy alentador, ya que nos fue difícil coordinarnos en las actividades, puesto que al tener un atraso, provocamos un atraso a todos y por lo tanto al proyecto. Después de varios intentos logramos llegar al término de éste trabajo.

GLOSARIO

GLOSARIO

Almacén virtual	Equivalente de un local físico en donde podemos comprar o vender bienes y servicios. El almacén virtual está constituido por un conjunto de páginas web mostradas al “cliente” desde un servidor.
Breadcrumbs	Navegación basada en el “paso a paso”.
Call center	Centro de atención de llamadas entrantes (Inbound) o salientes (outbound) es una herramienta de comunicación y relación con los clientes que utiliza el teléfono como medio de comunicación básico gestionado por “personas humanas” en conjunto con los recursos humanos, físicos y tecnológicos necesarios y disponibles, basados en metodologías de trabajo y procesos determinados y adecuados, para atender las necesidades y dar servicio a cada “cliente único” con el objeto de atraerlos y fidelizarlos con la organización y permitir su viabilidad.
CGI	(Common Gateway Interface) Es la utilización de un pequeño programa que permite comunicarse con un servidor web.
CMM	(Capability Maturity Module) Modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI.
Complejidad	Debe contener todos aquellos hechos que pudieran ser importantes.
Concisión	Brevidad y economía de medios en el modo de expresar un concepto con exactitud.
Concreción	Reducción a lo esencial o a lo preciso de un asunto o materia.
Conectividad	Capacidad de un dispositivo (una PC, periférico, PDA, móvil, robot, electrodoméstico, coche, etc.) de poder ser conectado (generalmente a una PC u otro dispositivo) sin la necesidad de una computadora, es decir en forma autónoma.
Consistencia	Ausencia de contradicciones.
Core business	Corazón del negocio. Es el conjunto de actividades que realiza una empresa y que la caracterizan definen y diferencian en el mercado.
Core processes	Procesos clave que son fundamentales en una empresa para garantizar la continuación de la competitividad.

CRM	(Customer Relationship Management) Administración de la relación con el cliente. Estrategia de negocio orientada a la satisfacción del cliente.
Directrices	Guías de acción. Instrucciones o normas generales para la ejecución de algo.
Eficiencia	Es la óptima utilización de los recursos disponibles para la obtención de resultados deseados.
Ergonómico	Cuando está echo para la comodidad o seguridad del usuario.
ERP	(Enterprise Resource Planning) Planificación de recursos empresariales. Son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía comprometida en la producción de bienes o servicios.
Escalabilidad	Propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para, o bien manejar el crecimiento continuo de trabajo de manera fluida, o bien para estar preparado para hacerse más grande sin perder calidad en los servicios ofrecidos.
Exactitud	Capacidad de un instrumento de medir un valor cercano al valor de la magnitud real.
Extensibilidad	Facultad de adaptar software a los cambios que se especifiquen.
Fiabilidad	Probabilidad de que el dispositivo desarrolle una determinada función bajo ciertas condiciones y durante un período de tiempo determinado.
Flexibilidad	Capacidad de adaptarse rápidamente a las circunstancias.
GUI	(Graphic User Interface) Interfaz gráfica de usuario. Es el conjunto de métodos y formas que permiten la interacción de un sistema con el usuario utilizando gráficos e imágenes.
Hardware	Corresponde a todas las partes físicas y tangibles de una computadora.
Help desk	Mesa de Ayuda donde se ofrecen servicios acerca de soporte técnico (bugs, consultas, etc.)
Heurístico	(Del griego heurisko, hallar) Ayuda en el aprendizaje, para descubrir o resolver problemas utilizando la experimentación y los métodos de ensayo y error.

HTTP	(HyperText Transfer Protocol) Protocolo de Transferencia de hipertexto. Protocolo de comunicación para peticiones de acceso a páginas web y respuesta de la misma.
HTTPS	Versión segura del protocolo http.
IEEE	(The Institute of Electrical and Electronics Engineers) El Instituto de Ingenieros Eléctricos y Electrónicos. Es una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas.
Ignición	Ocurre cuando el calor que emite una reacción llega a ser suficiente como para sostener la reacción química.
Integridad	Se refiere a las medidas de salvaguarda que se incluyen en un sistema de información para evitar la pérdida accidental de los datos.
Interoperabilidad	Habilidad que tiene un sistema o producto para trabajar con otros sistemas o productos sin un esfuerzo especial por parte del cliente.
ISACA	(Information Systems Audit and Control Association) Asociación de Auditoría y Control de Sistemas de la Información. Asociación internacional de profesionales que se dedica a la auditoría, control y seguridad de los sistemas de información.
KPI	(Key Performance Indicators) Indicadores clave de desempeño. Miden el nivel de desempeño de un proceso, e indican que tan buenos son los procesos, de manera que se pueda alcanzar el objetivo propuesto.
Mainframe	Computadora central (macrocomputadora). Computadora grande poderosa y costosa utilizada principalmente en empresas que necesitan procesar gran cantidad de datos o soportar gran cantidad de usuarios.
Metadata	Datos que describen otros datos.
Migración	Proceso consistente en hacer que los datos y las aplicaciones existentes funcionen en una computadora, software o sistema operativo distinto.
OLAP	(On-Line Analytical Processing) Procesamiento analítico en línea. Es una solución utilizada en el campo de la llamada Inteligencia empresarial (o Business Intelligence) cuyo objetivo es agilizar la consulta de grandes cantidades de datos.
Out soucer	Proveedor externo. Aquel que hace provisión de servicios externos.
Parametrizacion	Establecer un conjunto de valores normalizados para trabajar con la información y registros con los que se alimenta un sistema.

Plugins	Módulo de software o hardware que adiciona una característica o un servicio a un sistema más grande.
Portabilidad	Característica que posee un software para ejecutarse en diferentes plataformas, el código fuente del software es capaz de reutilizarse en vez de crearse un nuevo código cuando el software pasa de una plataforma a otra. A mayor portabilidad menor es la dependencia del software con respecto a la plataforma.
Procesos en línea	Varios procesos, ejecutándose uno tras de otro.
Procesos por lote (Modo batch)	Ejecución de un programa sin el control o supervisión directa del usuario.
Reingeniería	Revisión fundamental y el rediseño radical de los procesos de negocios para lograr mejoras dramáticas en medidas de desempeño tales como en costos, calidad, servicio y rapidez.
Repositorio	(Depósito) Es un sitio donde se almacena y mantiene información digital, generalmente bases de datos o archivos informáticos.
Reusabilidad	La noción de objeto permite que programas que traten las mismas estructuras de información reutilicen las definiciones de objetos empleadas en otros programas e incluso los procedimientos que los manipulan. De esta forma, el desarrollo de un programa puede llegar a ser una simple combinación de objetos ya definidos donde éstos están relacionados de una manera particular.
Reutilización	Acción de volver a utilizar los bienes o productos.
SEI	(Software Engineering Institute) Instituto federal estadounidense de investigación y desarrollo, fundado por el Congreso de los Estados Unidos en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software, que dieran respuesta a los problemas que generaba al ejército estadounidense a la programación e integración de los subsistemas de software en la construcción de complejos sistemas militares.
Sello temporal	(timestamp) Registro de fecha.
Service bureau	Empresa que proporciona servicios.
SIE	(Sistemas de Información Empresarial) Especialistas en el desarrollo de software de administración y gestión para empresas.
SLA	(Service Level Agreement) Acuerdo de Nivel de Servicio. Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad del servicio.

Software	Se refiere al equipamiento lógico o soporte lógico de una computadora digital, y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica.
SSH	(Secure SHell) Protocolo para facilitar la comunicación segura entre dos sistemas usando una arquitectura cliente/servidor y permite a los usuarios conectarse a un host remotamente.
SSL	(Secure Socket Layer) Protocolo de capa de conexión segura. Proporciona autenticación (identidad) y privacidad de la información mediante el uso de criptografía .
Stake holder	Persona, grupo de personas o institución que se interesa por el buen funcionamiento de una empresa.
Transaccional	Una transacción es un evento o proceso que genera o modifica la información que se encuentran eventualmente almacenados en un sistema de información.
TSL	(Transport Layer Security) Seguridad de la capa de transporte. Evolución del protocolo SSL.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Manzano Villalón, José Antonio Calvo. et al. *Introducción a la auditoría informática*. España, Fundación General de la Universidad Politécnica de Madrid, 2002.

Solís Montes, Gustavo Adolfo. *Reingeniería de la auditoría informática*. México, Trillas, 2002.

Olgún Romo, Heriberto. Dirección, Organización y Administración de Centros de Tecnología de Información. México, UNAM, Facultad de Ingeniería, 2005.

Olgún Romo, Heriberto, et al. *Outsourcing en tecnologías de información*. México, UNAM, Facultad de Ingeniería, 2007.

<http://www.gestiopolis.com/delta/term/TER214.html> (8/04/2007 19:26)

<http://msdn2.microsoft.com/es-es/library/ms174861.aspx> (8/04/2007 19:30)

<http://www.answermath.com/data-mining/mineria-de-datos-6-herramientas.htm>
(8/04/2007 19:33)

<http://www.daedalus.es/AreasMD-E.php> (8/04/2007 20:22)

http://www.profeco.gob.mx/ecomercio/ecomercio_anexo.asp (21/04/2007 16:01)

<http://www.hipermarketing.com/nuevo%204/contenido/e-business/comercio%20electronico/nivel3todo.html> (21/04/2007 17:32)

<http://www.tecnicaspostales.com/ilicitos.asp> (23/04/2007 13:46)

<http://www.vlex.com/vid/167120> (19/05/2007 22:40)

<http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/outsourcingantonio.htm>
(26/05/2007 17:00)

http://www.microsoft.com/spain/empresas/legal/tipos_e-contratos.mspx
(26/05/2007 17:30)

<http://www.isaca-bogota.net/docs/pdfs/boletines/2004/Isaca-Bogota%20News%202004-09.pdf> (26/05/2007 17:00)

<http://www.ieid.org/congreso/ponencias/Viega,%20Maria%20Jose.pdf>
(26/05/2007 19:10)

<http://www.previsora.gov.co/pdfs/CONTRATO%20CON%20MARION%20S.A.pdf>
(26/05/2007 21:00)

http://www.earcon.com/outsourcing/contrato_outs_empresa_sa.pdf (26/05/2007 22:00)

<http://www.pwc.com/uy/spa/pdf/Outsourcing.pdf> (26/05/2007 22:20)

<http://www.programacion.com/bbdd/tutorial/warehouse/> (3/12/2008 15:19)

<http://www.datawarehouse.com.mx/> (3/12/2008 19:44)

<http://www.idensa.com/> (10/12/2008 20:23)

<http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-ssh.html> (17/04/2008 19:55)

<http://www.uv.es/~sto/cursos/seguridad.java/html/sjava-25.html> (17/04/2008 20:10)

<http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5084/INDEX.HTM>
(18/04/2008 21:05)

<http://www.agendaempresa.com/firmas/febrero/2005/193/8216/core/business/8217/casero>
(14/04/2009 11:35)

http://es.wikipedia.org/wiki/Reingenier%C3%ADa_de_Procesos (14/04/2009 11:50)

http://es.wikipedia.org/wiki/Help_desk (14/04/2009 12:00)

<http://www.deguate.com/infocentros/gerencia/glosario/o.htm> (14/04/2009 12:15)

<http://www.promonegocios.net/administracion/definicion-eficiencia.html>
(14/04/2009 13:34)

<http://www.monografias.com/trabajos14/progorie/progorie.shtml> (15/04/2009 9:00)

<http://www.sedic.es/autoformacion/metadatos/tema2.htm> (15/04/2009 9:19)

<http://www.alegsa.com.ar/Dic/sistema%20transaccional.php> (15/04/2009 11:20)

<http://www.mujeresdeempresa.com/tecnologia/tecnologia001003.shtml>
(16/04/2009 19:57)

http://www.microsoft.com/spain/empresas/internet/tipos_breadcrumbs.mspx
(16/04/2009 20:05)

<http://www.alegsa.com.ar/Dic/gui.php> (16/04/2009 20:12)

<http://www.organizateya.com/consistencia.htm> (16/04/2009 20:19)

http://www.elguille.info/colabora/NET2005/Percynet_ConstruyendoSoftCalidad.htm
(16/04/2009 20:52)

<http://www.mastermagazine.info/termino/5288.php> (16/04/2009 22:28)