ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

AUDITORÍA Y CONTROL DE GESTIÓN

“EL AUDITOR DE SISTEMAS Y SU PARTICIPACIÓN EN EL OUTSOURCING DE PROCESOS INFORMÁTICOS"

TESIS DE GRADO

Previa la obtención del título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentada por:

Jimmy Jefferson Andrade Mejía

GUAYAQUIL- ECUADOR

AÑO 2009

DEDICATORIA

Dedico este trabajo a mi adorable familia, mis padres, hermanos y por supuesto mi esposa e hijo, ya que es por ellos que hoy me encuentro donde estoy.

AGRADECIMIENTO

Agradezco a Dios por guiarme en este camino y ayudarme a realizar mis elecciones.

A mis padres por la formación que de ellos recibí y su constante apoyo.

A mi esposa y mi hijo por ser mi razón de querer ser mejor día a día.

A la Directora de tesis por su apoyo para la culminación de la misma.

A todos los profesores del ICM por impartir sus conocimientos sin egoísmos, por guiarnos por este camino académico y disipar las dudas que en el trayecto se presentan.

TRIBUNAL DE GRADUACIÓN

Ing. Pablo Álvarez **COORDINADOR DE AUDITORIA** **PRESIDENTE**	**Ms. Alice Naranjo** **DIRECTORA DE TESIS**
Ing. Dalton Noboa **VOCAL PRINCIPAL**	**Ing. Soraya Solis** **VOCAL SUPLENTE**

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

Jimmy J. Andrade Mejía

RESUMEN

En muchos países del mundo el outsourcing ha experimentado un gran crecimiento. Sin embargo existen muy pocos libros que abordan el tema del outsourcing informático.

El outsourcing informático se impone en la mayoría de las empresas como una forma de mejorar la eficiencia de las operaciones, es una decisión estratégica que se toma a nivel directivo con la finalidad de contar con profesionales de experiencia en el desarrollo de soluciones informáticas

Esta tesis aporta una visión completa de los aspectos del outsourcing, su problemática, la participación del auditor de sistemas en el outsourcing informático y entrega un manual con controles que incluye aspectos jurídicos a tener en cuenta en el outsourcing, esquemas de seguridad contractuales, controles específicos acorde al tipo de outsourcing que toda persona debe tener en cuenta en el outsourcing para garantizar acuerdos exitosos.

El tema de tesis “EL AUDITOR DE SISTEMAS Y SU PARTIPACIÓN EN EL OUTSOURCING DE PROCESOS INFORMÁTICOS”, aporta con el establecimiento de los controles que se requieren en el proceso de

administración del outsourcing informático, los cuales se recogen en una manual que se describe en el capítulo IV de esta tesis.

Este manual aporta información para auditores, usuarios de sistemas, profesionales informáticos, personal de seguridad Informática, abogados y en general aquellos profesionales que estén directa o indirectamente vinculados al outsourcing informático.

La idea de escribir un manual fue de la Directora de tesis quien como auditora de sistemas profesional, después de la observación de muchos casos fallidos de outsourcing en empresas nacionales me indicó consideró necesario aportar con un proceso investigativo y generar como producto resultante un documento con controles para poder guiar a las empresas en la administración adecuada del outsourcing informático. Esa ardua tarea es la que me he propuesto y espero que este manual cumpla ese fin y sea un parte tangible para los empresarios en virtud de que podrán administrar mejor esos contratos de outsourcing informático y podrán disminuir los típicos problemas que se presentan por inexistencia de controles ya que el manual propone muchos controles preventivos, detectivos, correctivos, administrativos para garantizar un manejo adecuado del outsourcing de procesos informáticos.

ÍNDICE GENERAL

DEDICATORIA.....I

AGRADECIMIENTOS.....II

RESUMEN.....III

ÍNDICE GENERAL.....IV

ÍNDICE DE FIGURAS.....V

ÍNDICE DE TABLAS.....VI

ABREVIATURAS.....VII

INTRODUCCIÓN.....1

1. ANTECEDENTES.....1

1.1. Contratación externa.....2

1.1.1. Historia.....4

1.1.2. Tipos de contratación externa.....7

1.1.2.1. Contratación externa a corto plazo.....8

1.1.2.2. Contratación externa a largo plazo.....12

1.1.3. Litigios.....16

1.1.4. El recurso humano y la contratación externa.....17

1.1.5. Privatización……22

1.1.6. Factores de éxito en la contratación externa…….....26

1.2. Outsourcing……....31

1.2.1. Definición……..32

1.2.2. Orígenes……..34

1.2.3. Desarrollo en aéreas no informáticas……...….35

1.2.4. El outsourcing en las administraciones publicas……..39

1.3. Pasos del outsourcing……..42

1.3.1. identificar áreas/procesos claves del negocio……43

1.3.2. Evaluar las oportunidades……44

1.3.3. Seleccionar al proveedor del outsourcing……...45

1.3.4. Proceso de transición……..…46

1.3.5. Monitorear y evaluar el desempeño……...…47

1.4. El auditor de sistemas……..48

1.4.1. Concepto……..48

1.5. La auditoria de sistemas informáticos……49

1.5.1. Concepto……..49

1.5.2. Fases de la auditoria informática……..50

1.5.2.1. Fase contractual……..51

1.5.2.2. Fase preliminar……52

1.5.2.3. Fase final……..54

2. MARCO TEÓRICO……55

2.1. Outsuorcing informático……55

2.1.1. Definición……55

2.1.2. Concepto……..56

2.1.3. Ventajas y riesgos del outsourcing informático……57

2.1.3.1. Ventajas……57

2.1.3.2. Desventajas……59

2.1.3.3. Riesgos……61

2.1.3.3.1. Riesgo programático……..61

2.1.3.3.2. Riesgo contractual……62

2.1.3.3.3. Riesgos en la seguridad de datos……..63

2.1.3.3.4. Otros riesgos……..64

2.2. Razones para adoptar outsourcing……..66

2.3. Modelos de outsourcing informático…….....70

2.3.1. Outsourcing informático total……71

2.3.2. Outsourcing informático parcial…….....71

2.3.2.1. Out-tasking……..72

2.3.2.2. Las 7 tendencias del outsourcing informático……73

2.3.3. El pseudo-outsourcing……75

2.3.4. El e-sourcing……75

2.3.5. Facilities management……76

2.4. Aspectos contractuales a tener en cuenta en el outsourcing……78

2.4.1. Los acuerdos de niveles de servicios……...78

2.4.2. Tipos de servicios que debe incluir un contrato de outsourcing informático……..…82

2.4.3. Contrato de mantenimiento de software…….83

2.4.4. Prevención frente al outsourcing…….84

3. FUNDAMENTACIÓN NORMATIVA Y/O ESTÁNDARES INTERNACIONALES……..86

3.1. Mandato numero 8 de la asamblea constituyente…….....87

3.1.1. Disposiciones generales……87

3.1.2. Artículo 16 de la contratación civil de servicios técnicos especializados……89
3.2. Normas de control interno……...89
3.2.1. Normas de control interno coso……...90
3.2.1.1. Definición y objetivos……94
3.2.1.2. Componentes……95
3.2.1.2.1. Evaluación de riesgos……96
3.2.1.2.2. Actividades de control……99
3.2.1.2.3. Supervisión……...101
3.3. Estándares internacionales……...103
3.3.1. Estándar de control de sistemas COBIT……..103
3.3.1.1. COBIT (objetivos de control para tecnología de información y tecnologías relacionadas)……...104
3.3.1.2. Características……..105
3.3.1.3. Principios……...106
3.3.1.4. Requerimientos de la información del negocio……106
3.3.1.5. Dominios de relevancia de COBIT……107
3.3.2. Estándar ISO 17799……115
3.3.3. ITIL (information technology infrastructure library)……149
3.3.3.1. Objetivo……150

3.3.3.2. Forma de uso de ITIL en managed services……..151

3.3.3.3. Proceso de manejo de incidentes……..152

3.3.3.4. Proceso de manejo de problemas……154

3.3.3.5. Proceso de manejo de configuraciones……157

3.3.3.6. Proceso de control de cambios……..158

3.3.3.7. Proceso de manejo de entregas……160

4. MANUAL DE CONTROLES DEL OUTSOURCING INFORMÁTICO……..162

4.1. Información preliminar……162

4.1.1. Introducción……..162

4.1.2. Objetivos……...164

4.1.3. Alcance……..167

4.1.4. Responsables……..167

4.2. Análisis de riesgos……168

4.2.1. Clasificación de los riesgos……..……174

4.2.1.1. Riesgos sin intención (RS)……...……..174

4.2.1.2. Riesgos Dolosos (RD).……176

4.2.1.3. Riesgos de orden natural (RN)……..177

4.3. Cuadro de riesgos según su clasificación……178

4.4. Políticas de control……183

4.4.1. Política de seguridad…….……..183

4.4.2. Revisión y evaluación……..……...……...185

4.4.3. Seguridad organizacional……187

4.4.4. Seguridad de acceso a terceros…….……192

4.4.5. Abastecimiento externo…….……..195

4.4.6. Clasificación y control de activos…….……..197

4.4.7. Clasificación de la información……..199

4.4.8. Seguridad personal……..201

4.4.9. Seguridad física y ambiental……...205

4.4.10. Seguridad de equipos……..207

4.4.11. Comunicación y operaciones……..209

4.4.12. Control de acceso……212

4.4.13. Desarrollo y mantenimiento de sistemas……..215

4.4.14. Conformidad……..218

4.4.15. Controles de contrato……...220

4.4.16. Controles de auditoría……..223

4.4.17. Seguimiento y control……...227

4.4.18. Estandarización……230

CONCLUSIONES……...231

RECOMENDACIONES…….234

BIBLIOGRAFÍA…….235

ÍNDICE DE FIGURAS

Figura 1.1. Evolución del enfoque de auditoría……..7

Figura 1.2. Evolución del outsourcing……38

Figura 1.3. Pasos del outsourcing……..42

Figura 1.4. Identificar áreas/procesos claves del negocio……43

Figura 1.5. Evaluar oportunidades……44

Figura 1.6. Seleccionar al proveedor outsourcing……...45

Figura 1.7. Proceso de transición……..46

Figura 1.8. Monitorear y evaluar desempeño……..47

Figura 3.1. Las tres dimensiones conceptuales del COBIT……107

Figura 3.2. Propiedad, monitoreo, evaluación y comunicación……...154

Figura 3.3. Control de problemas y errores……156

Figura 3.4. Niveles de Control……..158

Figura 3.5. Monitoreo de cambios……159

Figura 3.6. Entrega del servicio……161

INDICE DE TABLAS

Tabla 2.1. Ejemplos de IT riesgos e impactos de la externalización……65

Tabla 3.1. Dominios del COBIT……108

Tabla 3.2. Objetivos de alto nivel (planeación y organización P05)……109

Tabla 3.3. Objetivos de alto nivel (planeación y organización po9)……110

Tabla 3.4. Objetivos de alto nivel (adquisición e implementación A11)…….111

Tabla 3.5. Objetivos de alto nivel (entrega de servicio y soporte DS2)……..112

Tabla 3.6. Objetivos de alto nivel (entrega de servicio y soporte DS5)……..113

Tabla 3.7. Objetivos de alto nivel (monitoreo M3)……..114

Tabla 4.1 Riesgos sin intención (RS)……....179

Tabla 4.2 Riesgos dolosos (RD)……..180

Tabla 4.3 Riesgos de orden natural (RN)……181

ABREVIATURAS

COSO Comité de Organizaciones Patrocinadoras de la Comisión Treadway.

ISO Organización Internacional de Normalización.

TI Tecnología de Información

AICPA Instituto Americano de Contadores Públicos Certificado. (American Institute of Certified Public

Accountants)

CISA Auditor Certificado de Sistemas de Información. (Certified Information Systems Auditor)

IFAC Federación Internacional de Contadores. (International Federation of Accountants)

IIA Instituto de Auditores Internos. (Institute of Internal Auditors)

ISACA Asociación para la Auditoría y Control de Sistemas de Información. (Information Systems Audit and Control Foundation)

ISACF Fundación para la Auditoría y Control de Sistemas de Información. (Information Systems Audit.and Control Foundation)

ISO Organización de Estándares Internacionales. (International Standards Organisation) (Con oficinas en Génova, Suiza)

ITIL Biblioteca de Infraestructura de Tecnología de Información. (Information Technology Infrastructure Library)

INTRODUCCIÓN

Este siglo es el de la “era de la información” y está bien complementado con la existencia en el mundo de los contratos de outsourcing de procesos informáticos que surgen como resultado de una necesidad empresarial en muchos casos en PYMES que ven en el outsourcing informático una opción para poder desarrollar sus operaciones concentrándose en sus procesos principales y estratégicos.

Existen los más variados tipos de contratos de outsourcing de procesos informáticos que se desarrollaron por las necesidades tecnológicas actuales, tales como los contratos sobre bases de datos, los contratos de procesamiento de datos, los contratos de desarrollo de sistemas de información, de seguridad, de restablecimiento de operaciones, entre otros.

Es importante tratar la problemática de los contratos de outsourcing y establecer controles a tener en cuenta para una mejor coexistencia del outsourcing informático.

La tesis propone controles en el ámbito de los contratos de outsourcing de procesos informáticos.

La tesis comienza con una breve introducción en la que se señalan los conceptos del outsourcing, tipos, sus elementos, y los principios generales más importantes.

En el capitulo I se describen los antecedentes, la contratación externa, una breve historia del outsourcing, los tipos de contratación externa, los litigios, el outsourcing, sus definiciones y orígenes, el outsourcing informático, sus ventajas y riesgos, beneficios, características y por último trataremos del auditor de sistemas y la metodología para realizar auditorias de sistemas.

En el Capítulo II se profundiza en el outsourcing informático, los modelos de outsourcing informático, los aspectos contractuales a tener en cuenta en el outsourcing, los acuerdos de niveles de servicios, los tipos de servicios que debe incluir un contrato de outsourcing informático, las ventajas e inconvenientes en este tipo de contratación, entre los principales aspectos

En el Capítulo III se enfoca la fundamentación normativa y/o estándares internacionales, ente ellos se revisan aspectos legales como el mandato numero 8 de la asamblea constituyente, el ISO, COBIT e ITIL que son estándares internacionales que aportan con controles para el manual del Outsuorcing de

procesos informáticos. La norma ISO 17.799 de tecnología de la información es de gran utilidad en este tipo de contratos para brindar seguridad a quien transfiere datos o delega servicios informatizados.

En el Capítulo IV se desarrolla el manual que detalla algunos temas entre ellos: introducción, objetivos, alcance, responsables, análisis de riesgos, políticas y controles que abarcan diversas temáticas para proteger el éxito de los contratos de outosurcing de proceso informáticos.

CAPITULO 1

1. ANTECEDENTES.-

Este capítulo tiene como finalidad dar a entender en qué consiste la contratación externa desde sus inicios hasta la actualidad, de qué manera ha ido evolucionando y en qué forma afecta la misma a las organizaciones que la emplean, sus ventajas y desventajas, veremos también la similitud que guarda con respecto al outsourcing y comprender el significado del outsourcing informático que es el tema central de este trabajo, incluyendo algo tan importante como es su vulnerabilidad y las seguridades que se deben tomar al respecto y por supuesto entender la participación que tiene el Auditor de Sistemas en dichos procesos empezando por comprender el significado del mismo junto con la actividad denominada Auditoría de Sistemas.

1.1 CONTRATACIÓN EXTERNA.-

[1]La contratación externa se la puede considerar como un sinónimo del outsourcing ya que básicamente hablan de lo mismo, el Outsourcing puede definirse según Dorban Chacón (1999), como la acción de recurrir a una agencia externa para operar una función que anteriormente se realizaba dentro de la compañía.

El valor de la contratación externa radica en que ofrece una alternativa para lograr economías y otras mejoras importantes en la ejecución de las actividades y la prestación de servicios en una organización. El hecho de que determinadas actividades o servicios se asignen a contratación externa hace que sea muy importante la existencia de normas y procedimientos convenidos para que se tengan en cuenta, cuando corresponda, además de las opciones internas para realizar esas actividades o prestar esos servicios, las opciones disponibles fuera de la organización son una alternativa.

Esta decisión de utilizar o no servicios externos para el desarrollo de determinada función pasa por la pregunta de qué es más conveniente, ¿Fabricar o comprar?, además de determinar la fijación correcta del

[1] Del Peso Navarro Emilio, Manual del Outsourcing Informático Análisis y Contratación, 2003, 2ª Ed., Ed. Díaz de Santos.

tamaño, es decir, encontrar el tamaño idóneo, o la cantidad necesaria de personal para una organización. Estos dos cuestionamientos definen la aplicación estratégica del outsourcing.

El contratar servicios externos supera la conocida y ya clásica subcontratación de actividades, puesto que, en este caso, no sólo se pone en manos de un tercero un proceso o parte de la actividad empresarial sino que se comparte los riesgos del éxito o del fracaso del propio negocio.

La contratación externa es una forma de separación entre proveedor y comprador en la que el contratante mantiene la gestión directa de algunos servicios y contrata otros servicios específicos. En realidad, cualquier transacción o intercambio contractual implica unos costos que van más allá del propio precio de la transacción. Desde este punto de vista, lo primero que debe ser considerado es el hecho de que la contratación ocasiona lo que en la teoría económica se conoce como costos de transacción. Éstos se pueden identificar con los costos que corresponden a la especificación y redacción de contratos, la evaluación de ofertas, la negociación del contrato con el proveedor elegido y el seguimiento y evaluación de los resultados del contrato.

La decisión de comprar o producir un determinado servicio en una organización es el resultado de la comparación de costos y beneficios asociados a la misma, así como de factores institucionales y de la propia historia de la organización. Esta valoración debería tener en cuenta al menos la respuesta a tres preguntas; ¿hay proveedores identificables que puedan proveer los servicios requeridos de forma efectiva y eficiente?, ¿es factible la competencia potencial entre los proveedores? y ¿es posible que los costos de la contratación puedan superar los ahorros potenciales?

1.1.1 HISTORIA.-

Si revisamos a través de la historia descubriremos que la contratación externa se venía presentando desde los tiempos medievales, un claro ejemplo de contratación de terceros que se remonta a la antigüedad es el servicio de mensajería o correo. Los reyes se comunicaban mediante el intercambio de mensajes (principalmente escritos) que eran llevados de un lugar a otro por mensajeros a su servicio. Evidentemente, sólo aquellos con suficientes recursos económicos tenían mensajeros que transportaban sus mensajes.

Con el paso del tiempo más personas necesitaban enviar mensajes y para reducir los costos utilizaban mensajeros comunes que entonces llevaban varios mensajes a la vez. Finalmente, estos mensajeros comunes se convirtieron en lo que hoy en día conocemos como el servicio de correo. Jamás pasó por la mente de aquellos gobernantes que en el futuro sus mensajes serían llevados por personas que no estaban directamente bajo sus órdenes y mucho menos que compartirían el mensajero con un pobre campesino. Hoy en día los pocos reyes que subsisten e, incluso, los grandes mandatarios, no dudan en enviar una carta por correo.

Otro servicio que fue contratado externamente hace más de cien años es el de la producción de la energía eléctrica. Con la invención del motor eléctrico en 1821, Michael Faraday inicia el uso de la energía eléctrica en las empresas de producción. Ahora bien, cada empresa necesitaba tener su propio generador y era inaudito pensar en darle a un tercero el control de algo tan clave como la generación de energía. Es en 1879 cuando en San Francisco se crea la primera empresa de producción de electricidad. A partir de esa fecha las empresas comienzan a contratar externamente la actividad de producir electricidad para concentrarse en las actividades que sí le eran propias.

Actualmente, nadie piensa que la adquisición de electricidad es una contratación externa y sólo algunas empresas tienen su propia planta de producción eléctrica y únicamente para usos de emergencia.

El servicio telefónico, en cambio, adoptó esta modalidad de contratación rápidamente.

En sus inicios, los teléfonos sólo servían para hablar de un punto predeterminado a otro punto también predeterminado. Hoy en día al haber sido contratado externamente ese servicio, un teléfono dado es capaz de comunicarse con cualquier otro teléfono en el mundo.

En fin podemos notar que la contratación externa no es algo nuevo, muy al contrario lo vivimos a diario desde hace mucho tiempo ya, comenzando con una necesidad, como todo lo importante que hoy en día tenemos.

FIGURA 1.1. Evolución del enfoque de auditoria

1.1.2 TIPOS DE CONTRATACIÓN EXTERNA.-

En forma general existen dos tipos de contratación externa: de corto plazo y de largo plazo. Cada una tiene sus propias características y normalmente no es que la primera (de corto plazo) se prolongue y luego se convierta en largo plazo, sino que desde un inicio se contrata a un tercero de corto o de largo plazo.

1.1.2.1 CONTRATACIÓN EXTERNA A CORTO PLAZO.-

La contratación externa de corto plazo se adopta para actividades puntuales para las que la organización no tiene los recursos humanos o técnicos necesarios. Los proyectos de construcción o desarrollo en empresas que no se dedican a la construcción o al desarrollo son actividades idóneas para la contratación externa de corto plazo.

Dichos proyectos requieren de recursos que normalmente la empresa no tiene, tales como obreros, carpinteros, plomeros, analistas o programadores. También requiere de equipos especializados que tendrían que alquilarse, ya que su utilización sería únicamente para dicho proyecto y perderían su utilidad, una vez finalizada la actividad.

La contratación externa de corto plazo no conlleva el traspaso de activos o recursos humanos de la empresa contratante al contratado. En lugar de contratar a terceros, la empresa puede contratar personal especializado pero la contratación es temporal y, por lo tanto, la oferta de trabajo no es muy interesante o el salario tiene que ser más alto de lo normal para compensar el aspecto temporal de la contratación.

El proceso de contratación de personal normalmente toma tiempo y consume recursos, además de requerir de conocimientos especializados que nuevamente pueden no existir dentro de la empresa. Dependiendo de la duración del proyecto, es posible que la legislación laboral vigente le otorgue carácter permanente o indefinido a la relación laboral a pesar de que la intención de las partes haya sido diferente. La terminación de una relación laboral considerada como indefinida tiene bajo ciertas legislaciones costos adicionales y en algunos casos no es viable. Los equipos y conocimientos requeridos para realizar el proyecto pueden ser muy especializados. Los mismos pueden estar disponibles en el mercado, pero también es posible que no lo estén. Su adquisición puede ser costosa y el valor residual bastante pequeño. Los mismos pueden ser útiles para llevar a cabo otros proyectos similares, pero dado que la empresa no se dedica a esa actividad dichos activos no tienen ninguna utilidad para la empresa, una vez terminado el proyecto. Estas condiciones aumentan considerablemente el costo de realizar el proyecto internamente en vez de entregárselo a un tercero que se dedica normalmente a esa actividad y que puede hacer un mejor uso de los equipos y conocimientos.

Otra razón para la contratación externa de corto plazo obedece a que la gerencia de la empresa contratante no quiere distraer su atención de las actividades normales.

El control de proyectos especiales tiende a requerir atención gerencial y puede causar traumas en las actividades normales. El contrato de terceros en el corto plazo normalmente estipula un costo total, sin embargo, aunque en algunos casos se realiza al costo más un porcentaje de ganancia; esta modalidad no es recomendada, ya que no estimula el control de costos, el cual es una de las razones para la contratación externa y además requiere de conocimientos de los que normalmente carece la empresa contratante.

También estipula un cronograma de entregas y una descripción más o menos detallada del producto final. Dicha descripción puede en algunos casos ser parte del producto en sí, como en el caso de levantamiento de requerimientos más desarrollo del producto. Aún en estos casos es muy importante que el contrato inicial sea lo más detallado posible en cuanto a plazos, costos y resultados esperados.

La contratación externa de corto plazo no debe verse como símil de una relación laboral con una persona jurídica, sino como una relación de corto plazo para llevar a cabo un objetivo muy bien definido.

El producto o resultado final de la contratación externa de corto plazo puede en ocasiones proveer una ventaja competitiva a la empresa contratante. Dicho producto tiende a ser único y especializado, por lo que puede proveer dicha diferencia competitiva. Por otro lado, cualquier competidor puede, a su vez, adquirir un producto o servicio semejante mediante su contratación a la empresa que ejecutó el servicio o producto. En algunos casos es posible incluir en el contrato cláusulas que prohíban a la empresa el trabajar con competidores durante un determinado período, pero eso normalmente aumenta el costo total.

En el caso de proyectos de desarrollo de activos informáticos o intangibles, es importante determinar la propiedad del producto final y sus derivados, es posible que el tercero contratado espere hacer uso de copias del producto en otros contratos. La propiedad del código ejecutable de un sistema es diferente y separada a la propiedad de su código fuente y especificaciones. En estos casos se debe determinar si el código fuente y sus especificaciones forman parte del producto que

recibe la empresa o no y también incluir procesos mediante los cuales dichos activos son pasados a la empresa apropiadamente. Un disco magnético y un manual rara vez son suficientes para lograr una efectiva transferencia del producto contratado externamente.

1.1.2.2 CONTRATACIÓN EXTERNA A LARGO PLAZO.-

La contratación externa de largo plazo sí puede verse hasta cierto punto como una relación laboral con una persona jurídica. Este contrato externo de largo plazo describe el resultado esperado de la actividad o actividades a realizar, así como su costo; también puede incluir ciertas condiciones sobre la forma en que se realizan las actividades pero el énfasis no es en la forma sino en el resultado.

La idea básica detrás de este tipo de contratación es el traspasar la operación a un tercero que sabe cómo realizarla mejor y más económicamente. Las estipulaciones sobre cómo se debe realizar la operación tienden a reducir la eficiencia y eficacia que el tercero trae consigo, pero en ocasiones son necesarias. Las estipulaciones sobre el costo y los resultados deben ser muy específicas.

La contratación externa de largo plazo se aplica a actividades que la empresa realiza internamente de forma rutinaria pero que no las realiza bien, le salen muy costosas o la distraen de otras actividades de mayor relevancia estratégica. La informática es una actividad que muchas empresas han decidido contratar a terceros por diversas razones.

En algunos casos los presupuestos de informática se incrementan anualmente y la gerencia no sabe cómo detenerlos, en otros los resultados obtenidos son inferiores a los que obtienen los competidores. Además, la informática es una actividad indispensable en la mayor parte de las empresas, pero es muy diferente al resto de las actividades de la empresa, convirtiéndola en una caja negra que sólo crea dolores de cabeza. En cualquiera de estos casos la contratación externa es una solución idónea al problema.

Al inicio de esta modalidad de contratación de largo plazo, el contratado adquiere equipos y personal de la empresa contratante a cambio de un pago inicial único. A partir de ese momento el contratado reestructura dichos activos y recursos humanos para obtener el mayor beneficio posible. En ocasiones, todas las operaciones son llevadas a cabo en los mismos equipos y con el mismo personal, pero generalmente la

reestructuración elimina algunos de ellos y agrega otros que el tercero contratado considera más efectivos.

La contratación externa de largo plazo tiende a ser muy bien vista por la función financiera de la empresa, ya que liquida activos fijos proveyendo flujo de caja y permite una mejor planificación financiera, porque los costos de operación de la actividad contratada pasan a ser limitados y predeterminados.

En ocasiones se ha visto que la decisión de contratar externamente se da exclusivamente para obtener dicho flujo de caja. A nivel estratégico, el flujo de caja debe ser un beneficio colateral de la contratación externa y no una razón para efectuarla.

Dado que el tercero contratado adquiere los activos y recursos humanos, generalmente exige que el contrato sea de largo plazo para poder amortizar los costos iníciales. Por su parte, la empresa exige que los costos anuales, así como la calidad y niveles de servicio, queden claros y estrictamente estipulados durante todo el período.

Dada la naturaleza de la modalidad mencionada, es muy importante que la relación sea beneficiosa para ambas partes. Los contratos leoninos

que llevan a la quiebra a una de las dos partes terminan siendo negativos aún para la parte que aparentemente se beneficia al inicio. Otro aspecto de suma importancia es la confianza que exista entre las partes. Es muy difícil lograr una efectiva contratación externa si existe desconfianza.

Es importante notar que el servicio que se recibe en la contratación de terceros en el largo plazo es un servicio estándar, un servicio que no provee ningún tipo de ventaja competitiva y que cualquier competidor también puede obtener, incluso a partir del mismo tercero contratado.

Al contratar externamente, la empresa incrementa el control de los costos de la actividad y aumenta su eficiencia, pero al mismo tiempo renuncia al control operacional de la actividad contratada. Perder el control operacional de la actividad resulta beneficioso, ya que permite que la gerencia de la empresa dedique su atención a actividades más importantes y estratégicas.

Por otro lado, algunos gerentes ven esa pérdida de control operacional como algo negativo. Intentar mantener el control operacional de la actividad es un error frecuente y generalmente va unido a una falta de confianza para con la empresa que ofrece el servicio contratado.

La estrategia de contratar a terceros no implica perder el control estratégico de la actividad requerida. Por el contrario, es vital que la empresa mantenga dicho control para asegurar que la actividad se lleve a cabo de una forma alineada con el resto de la estrategia de la empresa. También es común encontrar empresas, que al contratar a terceros para una función, intentan olvidarse de la misma y no mantienen ningún tipo de personal interno que controle, supervise y dirija al tercero contratado. Con el tiempo, estos errores resultan costosos y difíciles de corregir.

1.1.3 LITIGIOS.-

La contratación externa, al igual que cualquier otro tipo de contratación laboral o comercial, puede llevar a un desacuerdo entre las partes. Es posible que la empresa contratante no esté satisfecha con el nivel de calidad o servicio o que quiera rescindir el contrato antes de la fecha establecida. El contratado también puede estar insatisfecho con la relación y querer aumentar los costos, acelerar los pagos, redistribuir los activos de una forma diferente a la inicialmente acordada o, incluso,

terminar el contrato anticipadamente. Nada de esto es diferente al resto de las relaciones que la empresa mantiene con otros terceros.

En algunos casos se teme que el tercero tiene una ventaja en caso de desacuerdo, ya que el mismo tiene el control operacional de una actividad importante de la empresa, la cual no puede prescindir de la misma. Eso es similar a la relación laboral en la cual el patrono no puede prescindir de un día a otro de los servicios de todos o algunos de sus empleados. También es similar a la relación con un proveedor único o importante o, incluso, con un cliente importante.

En todos estos casos la solución depende de la calidad de los contratos utilizados, del sistema legal vigente y del sistema jurídico. Ni el mejor contrato resultara útil si no hay forma alguna de hacerlo cumplir. Es necesario que las leyes faciliten un proceso rápido y eficiente, pero cabe recordar que si ello no es posible el problema no radica en el concepto de contratación externa ni en que problemas similares se encontrarán, ya que esto sería un problema para la organización aun cuando no sea esta la modalidad de contratación a utilizar.

1.1.4 EL RECURSO HUMANO Y LA CONTRATACIÓN EXTERNA.-

En este tipo de contratación de largo plazo, además de los activos, la empresa traspasa el recurso humano que anteriormente realizaba la actividad contratada.

Desde el punto de vista de la empresa y del recurso humano, este traspaso tiene sus ventajas y desventajas. La principal ventaja para la empresa es que reduce su personal, lo cual también puede verse como una desventaja. La empresa pierde personal con experiencia en la empresa. La mayor parte de ese personal seguirá laborando para el tercero contratado en tareas propias de la empresa, pero por otra parte también puede pasar a trabajar en otras tareas, incluyendo actividades de un competidor.

El recurso humano que labora en una empresa necesita tener dos tipos de conocimientos importantes: el conocimiento técnico propio de la tarea o actividad que realiza y el conocimiento técnico y sociológico de las actividades de la empresa, y de la forma en que ésta opera (cultura empresarial). Los conocimientos técnicos son a menudo adquiridos con antelación a la relación laboral, pero el conocimiento de la cultura propia de la empresa sólo se adquiere con el tiempo durante la interacción

laboral. Aunque algunos autores descuentan la importancia de este conocimiento, la mayoría de las investigaciones han demostrado que es de gran importancia para el buen desarrollo de la actividad laboral.

Cada vez que la empresa pierde personal con antigüedad en la empresa está perdiendo ese conocimiento.

Cada vez que se agrega personal a la empresa, el nuevo personal necesita aprender la cultura para poder hacer el mejor uso de sus conocimientos técnicos.

También es posible que parte del personal contratado por terceros no acepte el cambio y decida renunciar. Eso implica la pérdida completa de dicha experiencia para la empresa, experiencia que podría ser utilizada por competidores que decidan contratar a ese mismo personal. Cabe destacar que aunque estas personas llevan consigo experiencia y conocimiento propio de las operaciones de la empresa, no debe ser de las operaciones clave o estratégicas de la empresa, sino de las conexas o de soporte, ya que, como mencionamos anteriormente, y desarrollaremos en detalle más adelante, las actividades a ser contratadas externamente no deben ser actividades clave o estratégicas.

La cultura y ambiente laboral de la empresa también tienden a ser afectadas por los procesos de contratación externa. A diferencia de la contratación de servicios, el cambio de la relación laboral en estos procesos tiende a causar malestar en el resto del recurso humano que permanece en la empresa. Aunque en la mayor parte de los países la relación laboral no es considerada de por vida, la mayor parte de los empleados no ven bien el cambio forzado.

De forma similar, a los demás procesos de reducción de personal, muchos empleados empiezan a temer que ellos serán los próximos en ser contratados por terceros. Para los empleados contratados por terceros, el cambio de patrono no tiene que ser estrictamente negativo. De hecho, generalmente resulta positivo para su carrera profesional en el aspecto técnico. En muchas empresas el personal técnico encuentra un techo muy bajo en cuanto a su posición jerárquica (y, por tanto, a su salario). Es lamentable que las posiciones gerenciales tiendan a ser las mejor remuneradas. También es lamentable que la mayor parte de las rutas de ascenso profesional dentro de una empresa pasen rápidamente del área técnica al área gerencial. De hecho, es curioso observar que la recompensa por una labor técnica bien realizada es sacar a la persona de dicha área y convertirla en un gerente, actividad para la cual es

altamente probable que no haya recibido ningún tipo de instrucción académica

Generalmente, la carrera profesional técnica es mejor reconocida y remunerada dentro de empresas especializadas en dicha área técnica.

Por ejemplo, un tercero contratado por servicios de informática tiene mucho más personal especializado en informática que cualquier otro tipo de empresa, entiende mejor a dicho personal y le ofrece retos profesionales mucho más interesantes y relacionados propiamente con la carrera informática. Los escalafones como analista I, analista II, analista IV son corrientes dentro de empresas especializadas. De esa forma el analista puede ascender en rango y salario sin tener que salir de su especialidad profesional.

Como contrapartida a la anterior ventaja se encuentra el hecho de que cambiar de un patrono a otro devuelve el reloj de la antigüedad con respecto a ascensos (aún cuando es posible que dicho reloj siga su curso en cuanto a las obligaciones laborales contractuales). El empleado también tiene que acostumbrarse a la nueva cultura empresarial que puede ser o no de su agrado personal.

Otro cambio que puede ser positivo o negativo se encuentra en los beneficios laborales (incluyendo la jubilación) que el nuevo patrono ofrece en comparación con los que ofrece el patrono anterior. Para compensar dichas pérdidas es posible que el nuevo patrono deba pagar salarios más altos, pero eso dependerá de la influencia que tenga el sindicato u otros representantes de los empleados en el desarrollo del contrato.

1.1.5 PRIVATIZACIÓN.-

[2]Es común que la contratación externa se interprete como un proceso de privatización cuando la empresa que contrata es una institución pública (Bingman y Pitsvada, 1997; Brayton, 2002; Chi, Arnold y Perkins, 2003; Elam, 1997; Johnsen, 2002; Kakabadse y Kakabadse, 2001; Lugar y Goldstein, 1989; Miranda y Lerner, 1995; Prager, 1997).

[2] Carvallo Alman Amelia, Outsourcing La Subcontratación, Ed. LIMUSA, 2002, 169 pp

Pero contratación externa no tiene que ser siempre privatización, aun cuando la empresa que contrata sea pública.

El término privatización arrastra consigo innumerables connotaciones negativas que, lamentablemente, llevan a muchos a ver negativamente cualquier proceso que lleve dicho nombre. La privatización en sí no tiene nada de malo, tampoco lo tiene la nacionalización (aunque esta última sí conlleva el lamentable hecho de que el mercado no funcionó bien en dicha actividad).

El Estado tiene actividades que le son propias y a las cuales no debe renunciar. Es difícil determinar objetivamente cuáles son dichas actividades y el tamaño de la lista dependerá de la corriente filosófica del autor.

El objetivo del presente texto no es el de defender una de dichas filosofías por lo que no enunciaremos cuáles actividades deben ser realizadas por el Estado y cuáles por el sector privado, aunque sí reconocemos la existencia de actividades que son realizadas mejor por el sector privado que por el sector público, y viceversa.

También es posible que una institución pública traslade parte de sus actividades a un tercero contratado y que éste también sea una institución pública.

A nivel mundial existe una tendencia a contratar a terceros para cierto tipo de actividades (siempre y cuando no sean claves o estratégicas para la empresa).

La informática o computación es la primera actividad que viene a la mente cuando se menciona contratación externa. La informática es una actividad que puede distraer muchos recursos humanos financieros; puede duplicar o triplicar sus costos de forma anual sin que se vean resultados directos ni se sepa cuándo se detendrá (si es que se llega a detener) dicho proceso de encarecimiento.

La informática también es una actividad complicada de entender por aquellos que no son especializados en el área y también es una tarea para la que ya se han desarrollado muchos métodos eficientes de contratación externa. Otras tareas comúnmente contratadas externamente son la administración del recurso humano, la contabilidad y/o el proceso administrativo contable, mercadeo, distribución,

almacenamiento, logística y todas aquellas actividades que hacen uso intensivo de tecnología informática de telecomunicaciones.

Es común encontrar empresas que se dedican a la búsqueda de recursos humanos para sus clientes. La búsqueda en sí no es una actividad clave para la mayor parte de las empresas y la utilización de una base de información suficientemente amplia de donde escoger es siempre beneficioso. Hace 20 años todas las empresas realizaban todas sus búsquedas con personal y recursos propios.

Es difícil que una empresa pueda ser especialmente efectiva en mercadeo, ventas, manufactura, almacenamiento, logística y distribución al mismo tiempo (en otras palabras, cubrir la totalidad de la cadena de valor de forma efectiva es bastante complicado y, en ocasiones, contraproducente). Es preferible que la empresa seleccione en cuáles actividades puede efectivamente agregar valor y en cuáles es mejor que la realice un tercero. Empresas como Nike han contratado a terceros para la manufactura, almacenamiento y distribución de sus productos y se han concentrado en el diseño y mercadeo de los mismos. Empresas como Federal Express han pasado de ser simples empresas de mensajería a ofrecer servicios de almacenamiento y logística a sus

clientes. Son muchas las tiendas (por correo o Internet) que han entregado sus almacenes a Federal Express, para que los administre, ofreciendo de esta manera a sus clientes no sólo menores precios, sino la capacidad de entregar mercancía ordenada por el cliente tan sólo horas antes.

Las actividades de soporte que utilizan tecnología de comunicaciones tales como help-desks (puestos de ayuda), tele mercadeo, transcripción y proceso de transacciones financieras son normalmente contratadas externamente. En estos casos es común encontrar contrataciones de larga distancia. Cuando el servicio es prestado por medios electrónicos, el usuario final no sabe (ni necesita saber) si el operador que le presta el servicio se encuentra en el mismo edificio o en el otro lado del globo terráqueo.

El problema principal que se observa en contrataciones externas de largo plazo tiende a estar relacionado con el buen manejo del idioma (es posible que se hable un idioma diferente en el país donde se encuentra el tercero) y los conocimientos de la cultura corporativa o general del país. Por otro lado, dichas contrataciones externas permiten llevar la especialización a extremos nunca antes pensados.

Las pequeñas y medianas empresas pueden contar con personal de apoyo especializado al que sólo recurren ocasionalmente sin tener que contratar dicho personal a tiempo completo.

Otro problema en la contratación externa a larga distancia es el relacionado con las leyes, ya que puede ser difícil, o hasta imposible, asegurar que los contratos se respeten e, inclusive, puede ocurrir que las leyes locales no permitan la “exportación” de datos necesaria en un servicio de contratación externa a larga distancia.

1.1.6 FACTORES DE ÉXITO EN LA CONTRATACIÓN EXTERNA.-

✓ Siempre hay riesgos cuando se recurre a la contratación externa. Para evitar posibles problemas y aumentar las perspectivas de un proyecto satisfactorio de contratación externa deben considerarse algunos temas importantes, entre otros los siguientes:

✓ *Seleccionar los servicios que se subcontratarán* - Defina, establezca y observe un proceso de planificación para el proyecto de contratación externa. Considere el tiempo para la diligencia debida y

seleccione un grupo diversificado de profesionales de la organización para preparar un informe de evaluación sobre los requisitos de SyTI de la institución, que especifique las áreas que serán objeto de la contratación externa en sintonía con los planes y las prioridades de la institución.

- ✓ *Seleccionar el proveedor de servicios* - La selección de un proveedor de servicios para la contratación externa es crucial. Los términos y las condiciones del contrato deben considerarse cuidadosamente con anterioridad a la firma de cualquier convenio. La organización que contrata externamente SyTI debe estar preparada para supervisar, ponderar, y administrar los resultados de la contratación externa. La meta principal de la mayoría de los proveedores de servicios es aumentar sus ingresos, y la manera para alcanzar esta meta es vender sistemas nuevos grandes o servicios ampliados a los clientes, en lugar de ampliar aplicaciones existentes. Los proveedores también ofrecen servicios mediante alianzas con otros distribuidores, lo cual puede no constituir la opción más interesante para los clientes. El tratamiento con los proveedores es tan importante para la contratación externa que en el presente manual se dedica una sección completa para

ayudar a los administradores a tomar decisiones apropiadas en este ámbito.

✓ *Liderazgo en SyTI* - El liderazgo en SyTI es un tema importante para la prestación satisfactoria de SyTI y se recomienda en gran medida la existencia de un líder en la organización contratante con experiencia en SyTI a cargo del proceso de contratación. La continuidad de la competencia ("expertise") interna puede ser un problema: aunque existen excepciones, el cargo de jefe de información o director de SyTI en los Estados Unidos tiene una vigencia de alrededor de tres a cuatro años, un tiempo mucho más breve que el necesario para implantar proyectos complejos.

✓ *Elegir un equipo comprometido y competente para la implantación* - Se debe formar un equipo para supervisar el proyecto de contratación externa al comienzo del proceso con la combinación correcta de usuarios y profesionales técnicos. Es también importante obtener la promesa de los gerentes para que se asignen estas personas, algunas veces de tiempo completo, al equipo del proyecto.

✓ *Establecer reuniones para informes de progreso y análisis de los puntos críticos del proyecto* - Son imprescindibles las revisiones frecuentes al plan del proyecto por medio de entrevistas y participación del equipo de implementación durante el proceso de selección. Los canales de comunicación entre el equipo de implementación y la administración siempre deben estar *Parte C - Adquisición y contratación de servicios y productos de SyTI* abiertos para el análisis de problemas imprevisibles durante el período de implementación. Los gerentes necesitan supervisar las actividades, comprobar que están aplicándose los convenios y el cronograma de implementación y proporcionar los recursos necesarios al equipo para llevar adelante su tarea de la manera más dinámica.

✓ *Instrucción del equipo de gestión de proyectos y los usuarios* - Reconocer las inquietudes y las dudas que trae la contratación externa y disponer de una estrategia para tratar los complejos temas relativos al personal, que característicamente ocurren en toda implementación. La comunicación interpersonal deficiente y la falta de educación de los usuarios en cuanto a los temas relacionados con SyTI pueden imponer, y en efecto lo harán, una carga en la contratación externa. Es importante

que el equipo del proyecto consiga apoyo de todos los usuarios o clientes del sistema.

✓ *Respaldar la gestión para los proyectos de SyTI* - El apoyo de la gestión es vital para el éxito de los proyectos de SyTI. El personal directivo superior debe considerar la implementación de SyTI como un proceso institucional esencial para la institución asistencial, el cual integra requisitos de información diferentes y modifica las tareas y las funciones de gestión y cotidianas con el objetivo de mejorar el desempeño operativo.

✓ *Establecer metas realistas para los proveedores* - Deben evitarse proveedores que ofrecen soluciones rápidas a problemas de largo plazo. Establezca plazos realistas para la finalización de tareas complejas. Se requiere tiempo para que una entidad externa comprenda íntegramente las características empresariales de una institución, establezca operaciones e introduzca procesos. Los proyectos complejos necesitan tiempo.

✓ *Realizar pruebas frecuentes durante el desarrollo o el mantenimiento de una aplicación* – Las instituciones deben garantizar que un equipo interno realice una prueba meticulosa de las aplicaciones contratadas externamente. El proyecto para el desarrollo o el mantenimiento de sistemas a través de contratación externa debe estar libre de errores y ser funcionalmente completo. Deben observarse los parámetros definidos durante la fase de implementación y el sistema debe integrarse eficazmente con otros sistemas en la institución y desempeñarse a niveles satisfactorios.

Los proveedores subcontratados afrontan muchos de los mismos problemas experimentados por sus clientes. La escasez de trabajadores capacitados para SyTI y un mercado sumamente competitivo han ocasionado que algunos proveedores exijan demasiado del personal en relación con el número y la complejidad de los proyectos asignados. En consecuencia, algunos clientes potenciales, especialmente aquellos con recursos adecuados, con capacidad para concentrarse tanto en SyTI como en operaciones empresariales, pueden elegir la seguridad relativa del desarrollo o el control interno de las operaciones. Algunos clientes también pueden vacilar en hacer contratación externa porque han oído

casos des proveedores de servicios de contratación externa que toman demasiadas atribuciones que requieren el control total de los departamentos de SyTI y ello genera problemas de comunicación que obstaculizan las operaciones de la empresa. A pesar de ello, un mercado en maduración significa que más clientes saben lo que desean y necesitan, y más proveedores están decididos a contribuir al logro de sus metas.

1.2 OUTSOURCING.-

Para poder comprender lo que es un outsourcing informático, debemos saber lo que es el outsourcing o tercerización como tal, este tiene mucha similitud con la contratación externa, tanto así que podríamos decir que uno es sinónimo del otro. A continuación estudiaremos con detalle al outsourcing.

1.2.1 DEFINICIÓN.-

[3]Outsourcing es una mega-tendencia que se está imponiendo en la comunidad empresarial de todo el mundo y consiste básicamente en la contratación externa de recursos anexos, mientras la organización se dedica exclusivamente a la razón de su negocio.

El Outsourcing hasta hace tiempo era considerado simplemente como un medio para reducir significativamente los costos; sin embargo en los últimos años ha demostrado ser una herramienta útil para el crecimiento de las empresas.

Outsourcing es el uso estratégico de recursos externos para realizar tareas que tradicionalmente se manejan con recursos propios. Cuando el conocimiento y las habilidades requeridas para llevar a cabo algunas actividades propias del funcionamiento de una empresa o institución, pública o privada, no están en la nómina y sería muy caro o desventajoso incorporarlas, estamos en presencia de una oportunidad de outsourcing.

Este tema ha evolucionado desde el manejo de aspectos físicos del negocio hacia aspectos intelectuales; ahora las compañías asumen

---

[3] Barry James; White, Robert. “Manual del Outsourcing”. Ed. Gestión2000.com

asociaciones estratégicas de riesgo compartido. Dichas alianzas, en realidad no son sociedades formales, porque los capitales y patrimonios son independientes, pero en algunos casos la simbiosis es tal que no hace falta la relación patrimonial para ser considerados socios de negocios.

Otros definen el Outsourcing como una tendencia que se está imponiendo en la comunidad empresarial de todo el mundo y consiste básicamente en la contratación externa de recursos anexos, mientras la organización se dedica exclusivamente a la razón de su negocio. El Outsourcing hasta hace tiempo era considerado simplemente como un medio para reducir significativamente los costos; sin embargo en los últimos años ha demostrado ser una herramienta útil para el crecimiento de las empresas.

1.2.2 ORÍGENES

El outsourcing es una actividad que para muchos se viene realizando desde hace muchos años atrás pero con otro nombre, ***Facilities Management,*** aunque sean cosas diferentes como podremos ver más adelante. La diferencia entre ambos radica básicamente en que antes

solo se veía como una forma de ahorrar dinero ahora, en cambio, se busca mucho más.

Desde sus inicios el outsourcing ha ido evolucionando con el pasar del tiempo y así distintas áreas de las organizaciones se han ido externalizando.

De esta forma es sencillo el comprobar que funciones que hace no muchos años ninguna organización se hubiese atrevido a poner en manos de terceros hoy en día vemos, como lo más natural, que sean compañías externas las que realicen estas labores.

A través del tiempo la evolución del outsourcing ha sido:

- Limpieza;
- Seguridad;
- Catering;
- Biblioteca;
- Sistemas informáticos;
- Producción;
- Diseño/desarrollo de producto;
- Funciones administrativo-financieras.

Todo esto hará que en un futuro no muy lejano aparezcan lo que se viene denominando empresas virtuales, dedicadas únicamente al core business y que tienen externalizadas todas sus funciones.

Cada vez más empresas están considerando las políticas de empleo y se están planteando hasta que punto les interesa mantener grandes departamentos legales, financieros, contables o informáticos durante todo el año cuando la carga de trabajo de esos departamentos es necesaria únicamente durante una parte de él.

1.2.3 DESARROLLO EN AÉREAS NO INFORMÁTICAS.-

Las empresas americanas del automóvil hace veinte años emplearon el outsourcing subcontratando a terceros parte de su producción con lo que obtuvieron grandes beneficios por reducción de costes, mejora, calidad y tecnología y flexibilidad en la producción y en las plantillas de personal.

El outsourcing es un proceso que no termina en el área informática, cada vez son más las áreas que las utilizan, entre esas están:

Outsourcing financiero

- Contabilidad
- Nóminas
- Finanzas.

Atención a clientes

- Atención telefónica
- Soporte telefónico
- Sistemas de información al cliente
- Idealización de clientes (tarjetas).

Recursos humanos

- Selección de personal
- Prevención de riesgos
- Servicios médicos
- Asesoría laboral.

Administración

- Servicio de archivo
- Intranet corporativa
- Formación.

Servicios generales

- Limpieza
- Seguridad
- Servicio de comedor
- Mantenimiento
- Gestión inmobiliaria.

Marketing

- Campañas publicitarias
- Tele-marketing
- Promociones
- Mailing.

Logística

- Distribución
- Almacenamiento
- Stocks
- Gestión de vehículos.

En el siguiente grafico podremos apreciar el crecimiento y evolución que el outsourcing viene teniendo en los diferentes negocios

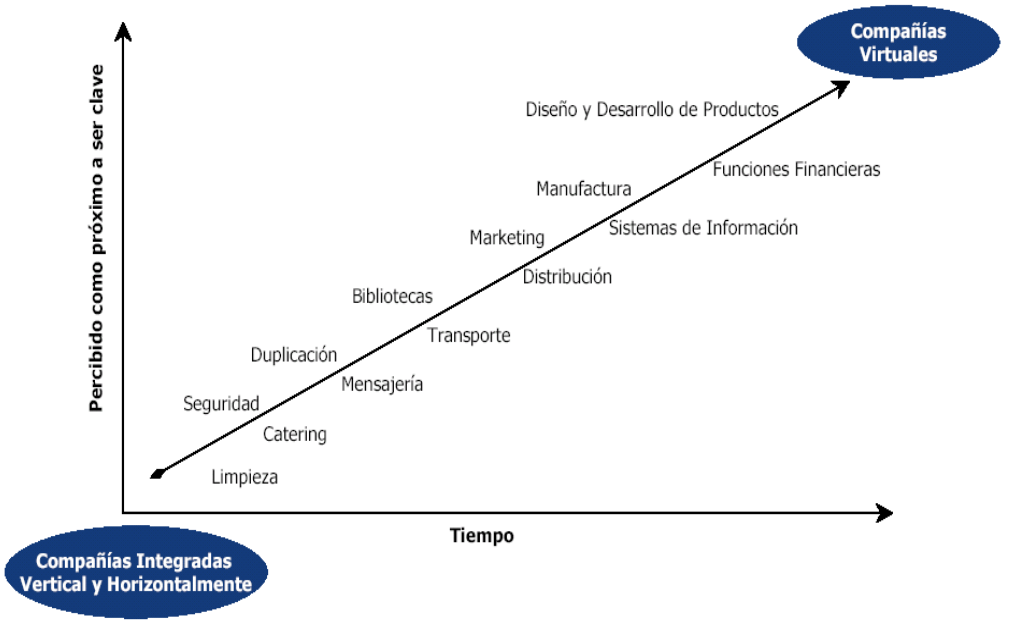


FIGURA 1.2. Evolución del outsourcing

Sin embargo, aún siendo algunos muy importantes indudablemente da el paso de sacar el Departamento de Informática de la empresa y subcontratar la ejecución de todos o de parte de los trabajos informáticos es una operación que tiene una gran trascendencia y más aún si recordamos como ha ido evolucionando aquel en la propia empresa.

Se obtienen grandes ventajas como veremos más adelante, pero ello conlleva también enormes riesgos si no se toman las medidas oportunas y adoptan una serie de precauciones.

En principio se precisa una buena planificación, un contrato que contemple todos los aspectos tan complejos que se dan en esta operación y una buena elección de la empresa que ejecute el trabajo.

1.2.4 EL OUTSOURCING EN LAS ADMINISTRACIONES PÚBLICAS.-

En las administraciones publicas la aplicación del outsourcing no resulta muy corriente y ello es debido principalmente a que las especiales características propias de estas así como a la especificad del contrato.

Por las especiales características de esta clase de servicio, su contratación dentro de las Administraciones Publicas presenta una doble dificultad:

- Una primera, que viene propiciada por la complejidad de definir claramente el objeto, precio y plazo del contrato.
- Una segunda, que surge de la necesidad de adaptar las peculiaridades de este tipo de contratación al marco legal de los contratos del Estado.

A continuación se detallan algunas de estas características, que suelen tener reflejo en los pliegos de prescripciones técnicas y que las diferencian, en cierto modo, de los contratos privados:

- **Complejidad de la Administración**

El sistema de contratación de las Administraciones es muy complejo. La obligación de convocar concurso público es una limitación a la hora de seleccionar un suministrador.

- **La competencia y responsabilidad jurídica**

Las administraciones tienen fijados unos programas que deben dar resultados ya fijados y es responsable jurídicamente de prestar una serie de servicios a los ciudadanos.

- **Repercusión pública de los fallos**

Los fallos en un servicio público son más llamativos que los producidos en una actividad privada.

- **La sensibilidad de la Administración frente a la divulgación de datos**

Datos que, considerados en su contexto general, son totalmente irrisorios y no importa que se publiquen, dejan de serlo cuando son desplazados de su conjunto, existiendo una especial sensibilidad a ello.

- **Pérdida del conocimiento**

La cesión del servicio informático, si no se hace bien, lleva consigo perdida del conocimiento sobre las aplicaciones y operaciones informáticas.

- **Preparación de la continuidad**

Es muy importante la preparación de un buen Plan de Retorno. Es necesario disponer de todos los derechos de uso y derechos patrimoniales al trabajo al objeto de poder continuarlos una vez finalizado el contrato.

- **Facilitar las mejoras en las ofertas**

La rigidez del concurso público respecto a la valoración de los demás aspectos que aparecen en las ofertas es una dificultad a la hora de efectuar mejoras en las ofertas.

- **La forma de pago**

La duración del proyecto durante varios periodos presupuestarios a modular los pagos e indicar que se van a realizar pagos parciales la contratación del número de años es un nuevo obstáculo.

- **Negociación de las diferencias**

Las diferencias de criterio que surjan respecto a la interpretación del contrato o los nuevos problemas que se presenten deberán resueltos por pequeños grupos de trabajo que sirvan de árbitro.

- **Contratación de terceros**

La subcontratación de trabajos por el suministrador de outsourcing es un tema a tener en cuenta y siempre deberán contar con el consentimiento de las Administraciones Públicas.

Este tipo de contratación presenta muchos problemas por las Administraciones Públicas que solo se aminoran, en cierto grado, cuando se trata de trabajos nuevos y, en cierto modo, autónomos.

1.3 PASOS DEL OUTSOURCING

[4]Podemos decir que los pasos más importantes para un outsourcing son 5, como veremos brevemente en los cuadros siguientes.

FIGURA 1.3. Pasos del outsourcing

Estos serian entonces los 5 pasos para un outsourcing, a continuación veremos uno por uno mediante el mismo formato.

1.3.1 IDENTIFICAR AÉREAS/PROCESOS CLAVES DEL NEGOCIO

[4] ERNST & YOUNG

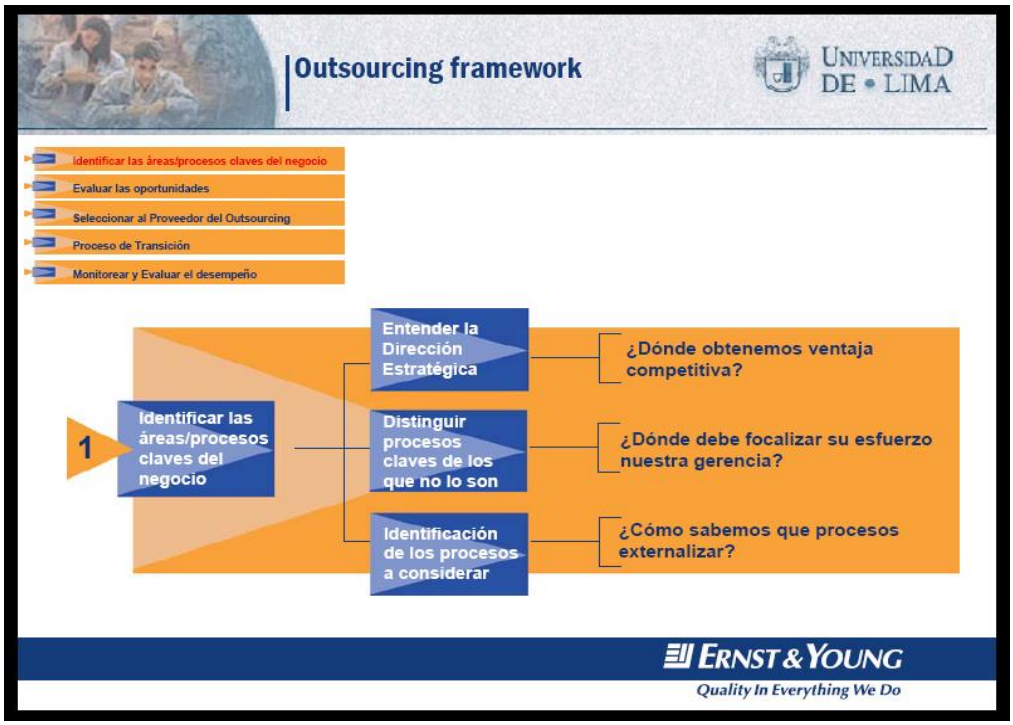


FIGURA 1.4. Identificar áreas/procesos claves del negocio

Como podemos apreciar en el cuadro, este paso consta de una clasificación que incluye:

- Entender la dirección estratégica
- Distinguir procesos claves
- Identificar los procesos a considerar

Mediante este proceso lograremos encontrar la pauta correcta para entender que necesita la organización basándonos en sus áreas claves.

1.3.2 EVALUAR LAS OPORTUNIDADES

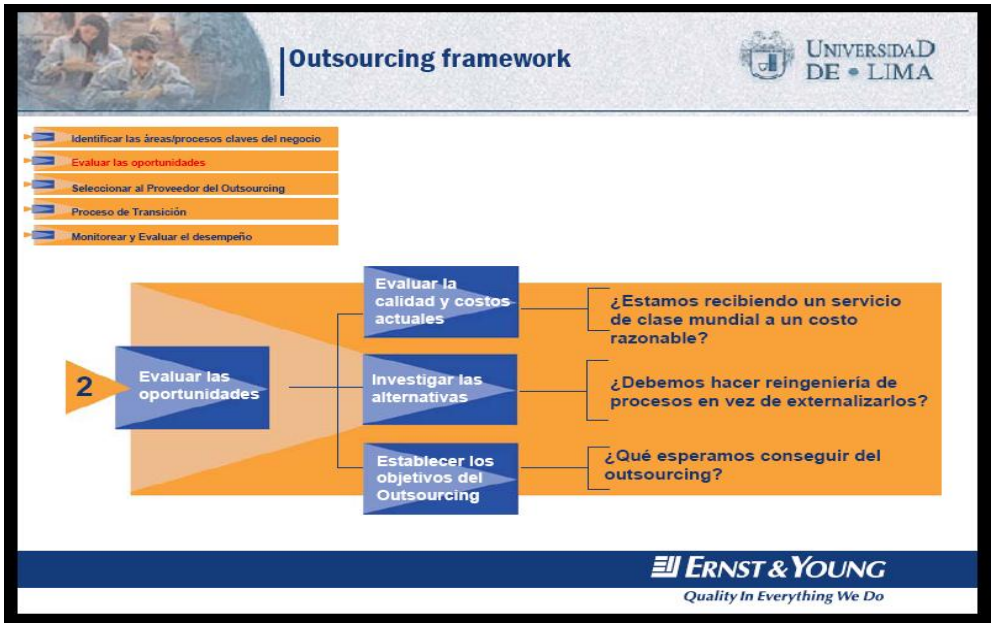


FIGURA 1.5. Evaluar oportunidades

Este paso tiene como finalidad determinar que oportunidades reales y potenciales tiene la organización para obtener el resultado deseado, también tiene una subdivisión que es:

- Evaluar calidad y costos actuales
- Investigar alternativas
- Establecer objetivos del outsourcing

1.3.3 SELECCIONAR AL PROVEEDOR DEL OUTSOURCING

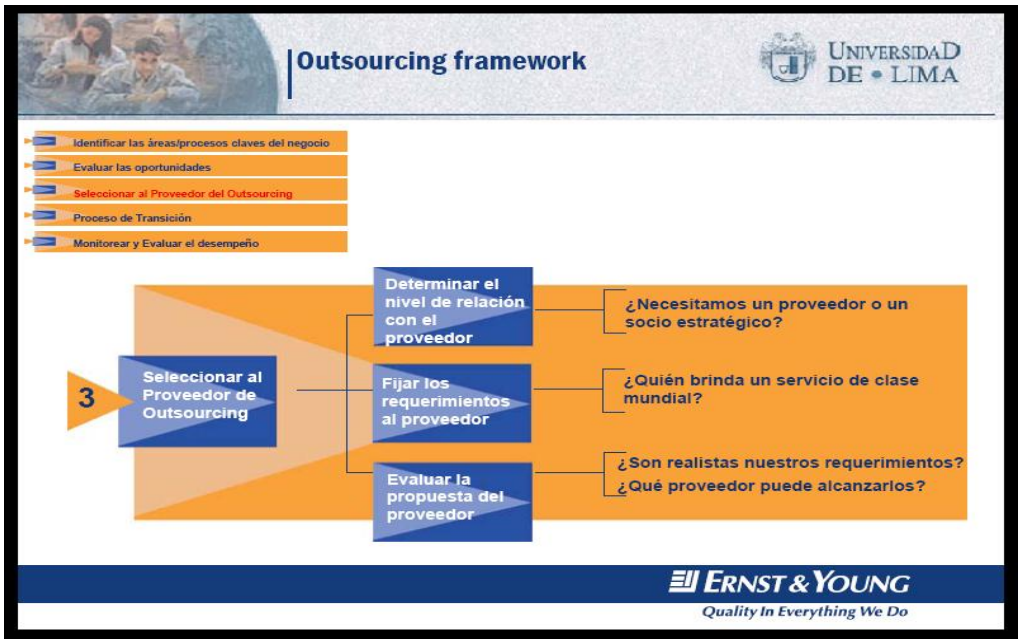


FIGURA 1.6. Seleccionar al proveedor de outsourcing

Aquí el objetivo es fijar al proveedor más idóneo que tendrá la tarea de prestar el servicio de outsourcing a la organización, como es de esperase este proceso también contiene 3 pasos adicionales para lograr el resultado deseado, esos pasos son:

- Determinar nivel de relación con proveedor
- Fijar requerimientos a proveedor
- Evaluar propuesta del proveedor

1.3.4 PROCESO DE TRANSICIÓN

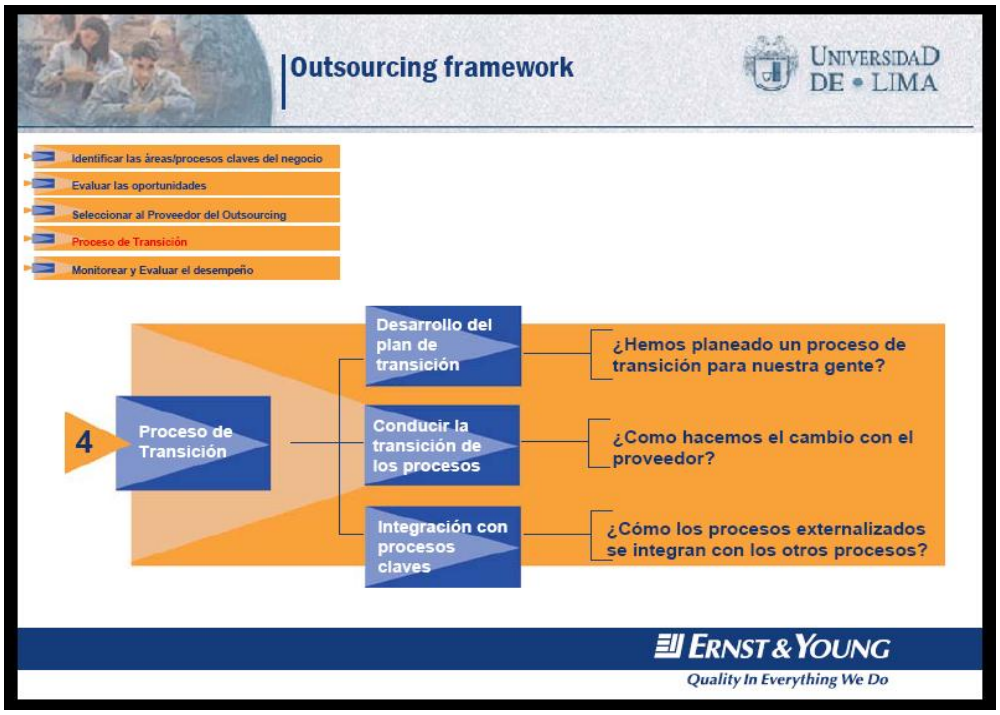


FIGURA 1.7. Proceso de transición

En esta fase conseguiremos integrar de manera satisfactoria todos los procesos que pasarán a ser manejados por la contratista, esto mediante un proceso de transición que contiene:

- Desarrollo de plan de transición
- Conducir la transición de los procesos
- Integración con procesos claves

1.3.5 MONITOREAR Y EVALUAR EL DESEMPEÑO

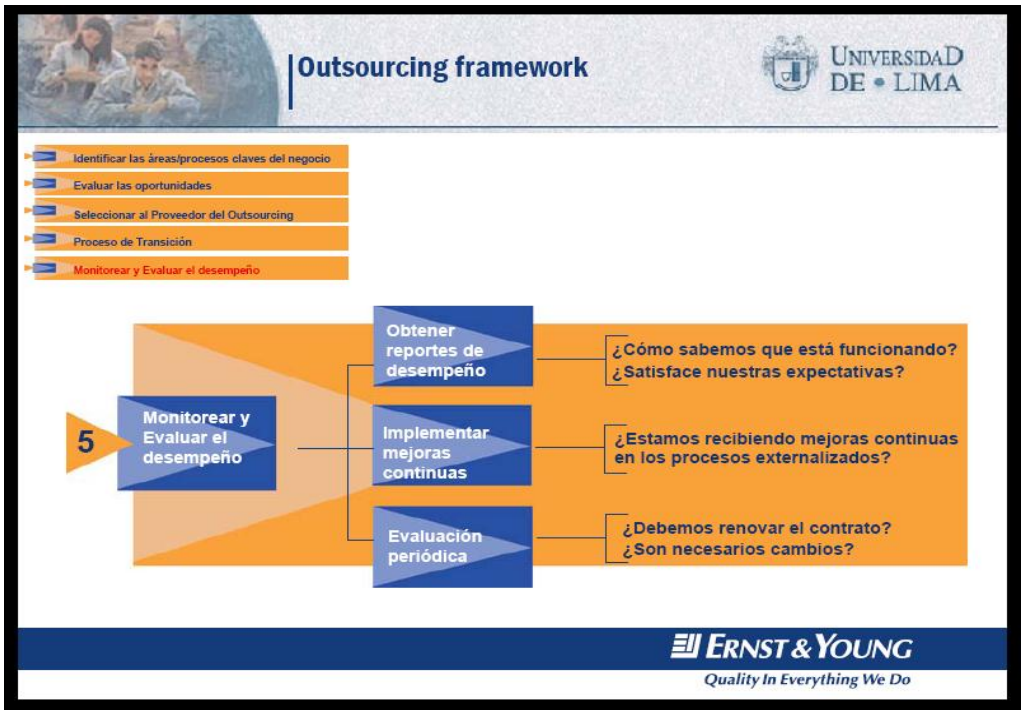


FIGURA 1.8. Monitorear y evaluar desempeño

Y finalmente hacer un seguimiento y una evaluación de los resultados para saber a ciencia cierta si lo obtenido es exactamente lo deseado, y de esta forma tomar correctivos en caso de ser necesarios, como subpasos tiene:

- Obtener reportes de desempeño
- Implementar mejoras continuas
- Evaluación periódica

1.4 EL AUDITOR DE SISTEMAS.-

1.4.1 CONCEPTO.-

La auditoria tradicionalmente financiera hasta encontrar hoy en día un tipo nuevo conocido como auditoria de sistemas.

[5]Conociendo la importancia y el valor que se le da a toda la información que de forma sistematizada se maneja en la compañías actuales y que más aun se ven obligadas a mantenerse a la vanguardia, nace también la necesidad de controlar el correcto funcionamiento y utilización no solo de la información sino además de los sistemas que procesan dicha información, en todos los aspectos asegurándose de que estos cumplan todas las normativas que la rigen obteniendo como resultado un proceso de calidad y acorde a las exigencias, debido a estas necesidades se dio cabida a lo que ahora conocemos como Auditoria de Sistemas, la cual da como resultado la formación de profesionales que tengan la capacidad de desarrollarlas.

[5] http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas

La naturaleza especializada de la auditoria de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la auditoria de los Sistemas de Información.

Entonces podemos decir que el Auditor de Sistemas será el encargado de revisar, controlar, evaluar y recomendar con respecto a los sistemas de información que en las empresas, instituciones o compañías se encargan de abarcar todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Para poder desarrollar las actividades que anteriormente mencionamos el Auditor de Sistemas necesitará de una adecuada planeación de la auditoría en informática, incluyendo de ser necesario un llamado equipo de auditoría, deberá también seguir una serie de pasos previos que permitirán dimensionar el tamaño y características de área dentro del organismo a auditar, sus sistemas, organización y equipo.

1.5 LA AUDITORIA DE SISTEMAS INFORMÁTICOS.-

1.5.1 CONCEPTO.-

La auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

1.5.2 FASES DE LA AUDITORÍA INFORMÁTICA

La elaboración de un plan para acometer una Auditoría Informática requiere de acciones muy similares a las que se realizan cuando nos enfrentamos a una auditoría financiera o de balances por lo que a continuación se relacionan los pasos que de forma general deben tenerse en cuenta para iniciar una certificación del grado de utilización y protección de la información automatizada en una entidad.

Una versión preliminar de los pasos que se deben dar para acometer la evaluación de la organización interna de una empresa cuando ésta tiene componentes de su control interno automatizados y enfocada desde el punto de vista de las sociedades de servicios, pudiera ser:

1.5.2.1 FASE CONTRACTUAL

Denominada así debido a que en este período se establecen los primeros vínculos con el cliente potencial encaminados a conocer de forma abreviada los principales rasgos mediante los cuales se puedan determinar

la magnitud del riesgo al que se encuentra sometido el cliente y por ende el estimado de tiempo que se requiere para elaborar un dictamen de la situación informática.

1. Contacto inicial con el cliente.
2. Investigación preliminar.
3. Cálculo del riesgo de Auditoría.
4. Determinar:

    - Tipo y alcance del trabajo a realizar.
    - Fecha de realización del trabajo.
    - Fijación de honorarios.

5. Envío de propuesta inicial y firma del contrato.

1.5.2.2 FASE PRELIMINAR

6. Confección preliminar del calendario de trabajo.
7. Conocimiento del Cliente.

    - Organigrama.
    - Planes de contingencia.
    - Normas y procedimientos.

- Bases jurídicas.
- Suministradores del hardware (incluye alternativas energéticas).
- Suministradores del software.
- Características, si existe del centro de diseño propio.
- Sistemas operativos en funcionamiento.
- Niveles de seguridad.

8. Revisión analítica preliminar (RAP)

- Sistemas operativos instalados
- Control del software
- Inventario detallado de equipos vs. software control de antivirus
- Acceso a las computadoras
- Acceso a locales donde se encuentran los equipos

9. Descripción del control interno administrativo.

- Organigrama de la actividad
- Esquema computacional
- Cruce de los puntos anteriores
- Balance de carga y capacidad
- Alcance de los sistemas implantados

- Determinar suficiencia del equipa miento
- Necesidad de automatización

10. Evaluación del control interno

- Sistemas instalados
- Actividades y funciones
- Procedimientos organizativos y/o manuales del sistema informativo computacional
- Uso de cuestionarios
- Ficheros traza con cruzamiento de puestos de trabajo y claves de acceso.
- Uso flujo gramas
- Chequeo de salvaguardas
- Chequeo de claves de acceso y accesos remotos (teniendo en cuenta que para algunos sistemas operativos no tienen diferencias)
- Evaluación de la confiabilidad de la información
- Destacar puntos débiles y fuertes (incluir apuntes para el Memorándum de revisión interna.

1.5.2.3 FASE FINAL

11. Preparación del informe y Memorándum de revisión interna

12. Discusión con el cliente de ambos documentos

13. Entrega informe final (dictamen) y Memorándum de revisión interna.

Destacar iguales términos que para los informes de Auditoría de Balances:

- Confiable
- Con salvedades
- No confiable

CAPITULO 2

2. MARCO TEÓRICO

En este capítulo se dará a conocer de una forma más detallada en qué consiste el outsourcing informático y todos sus componentes, esto en conjunto con temas y subtemas relacionados al mismo, cual son los principales motivos por el cual se lo utiliza, sus ventajas y desventajas, además de como se dan este tipo de contrataciones y las medidas que se deben tomar con la finalidad de que todo se desarrolle de la forma más normal, legal y beneficiosa posible tanto para contratante como para el contratado.

2.1 OUTSUORCING INFORMÁTICO

2.1.1 DEFINICIÓN.-.

[6]Un outsourcing informático no es más que la misma definición que ya conocemos del outsourcing pero esta vez de una forma más especifica dirigida a los servicios informáticos. Es decir cuando hablamos del outsourcing del área de sistemas informáticos estamos pensando en la cesión total de la gestión a un tercero incluyendo; activos, recursos humanos, hardware, software, mantenimiento, etc., en definitiva, todo.

2.1.2 CONCEPTO.-

[7]Por el año 1970, fue común para las empresas de computación exportar sus entradas de datos al exterior. Esto continuó en 1980, cuando contabilidades, facturación y proceso de palabras se convirtieron en trabajos outsourcing.

Entonces podremos decir que el servicio de outsourcing informático es aquel que ofrece a las empresas la posibilidad de optimizar sus proyectos, por

---

[6] Del Peso Navarro Emilio, Manual del Outsourcing Informático Análisis y Contratación, 2003, 2ª Ed., Ed. Díaz de Santos.

[7] Del Peso Navarro Emilio, Manual del Outsourcing Informático Análisis y Contratación, 2003, 2ª Ed., Ed. Díaz de Santos.

medio de la gestión externa de todos o parte de sus procesos informáticos. Este tipo de servicio resulta beneficioso para empresas para las cuales los servicios informáticos son una herramienta y no una finalidad. La empresa prestataria del servicio es la que tiene personal especializado y altamente calificado en el área de sistemas.

El outsourcing informático permite satisfacer necesidades informáticas de carácter temporal, permitiendo disponer de personal calificado por períodos definidos. Esto es mientras dure el proyecto de desarrollo, sin tener que crear un departamento con personal propio.

2.1.3 VENTAJAS Y RIESGOS DEL OUTSOURCING INFORMÁTICO

2.1.3.1 VENTAJAS

La verdad es que existen muy pocas estrategias de negocios que puedan aportar tantas ventajas como las que aporta un outsourcing, claro que estas van a depender del tipo de objetivos que se hayan podido fijar en la fase contractual.

La principal como ya hemos mencionado es la posibilidad de podernos despreocupar, hasta cierto punto, de esta área subcontratada para concentrar más esfuerzos en alguna otra en la cual seamos débiles.

También nos ayuda a reforzar la posición de las organizaciones ante sus competidores más directos, además que nos permite reducir costos de manera significativa.

Entre otros beneficios a los cuales accedemos a través del outsourcing tenemos:

- A través del Outsourcing se consigue contratar servicios eficientes, altamente calificados
- El outsourcing ofrece la actualización tecnológica que es difícil de conseguir internamente
- Adquirir lo más avanzado de la tecnología sin contratar y capacitar personal interno
- Disponer de servicios informáticos en forma instantánea
- Enfocar a los ejecutivos y a la empresa en su función principal
- Dedicar los recursos a funciones que están fuera de control

- Reducir y controlar gastos de operación. *(En un estudio realizado por el Outsourcing Institute se encontró que las compañías usando outsourcing reducen sus costos en forma notable.*
- Tener acceso a capacidades de clase mundial
- Una sola cuenta total por el servicio recibido
- Mejora en la calidad del servicio obtenido, comparado con el que existía

Además de las ventajas ya mencionadas el outsourcing presenta otros beneficios como los que mencionaremos a continuación:

- La empresa se preocupa exclusivamente por definir la funcionalidad de las diferentes áreas de su organización, dejando que la empresa de Outsourcing se ocupe de decisiones de tipo tecnológicos, manejo de proyecto, implantación, administración y operación de la infraestructura.
- Poseer lo mejor de la tecnología sin enganchar y entrenar personal de la organización para manejarla.
- Disponer de servicios de información en forma rápida considerando las presiones competitivas.
- A través de soluciones de Outsourcing se logra la contratación de servicios con idéntica funcionalidad y disminución de costos.

- Aplicar el talento y los recursos de la organización a las áreas claves.
- Ayuda a enfrentar cambios en las condiciones de los negocios.

2.1.3.2 DESVENTAJAS

Aun siendo el outsourcing una de las estrategias más exitosas de los últimos tiempos, sabemos también que nada es perfecto y este método no es la excepción, por esa razón podemos decir que entre las desventajas más relevantes podemos nombrar las siguientes:

- El costo puede que sea superior al esperado.
- En caso de que el proveedor no resulte satisfactorio, el cambio de proveedor genera gasto financiero y te tiempo.
- Pérdida de control directo sobre esa área.
- Como se tiene una empresa ajena, las actualizaciones e innovaciones de esa área las obtiene la empresa mientras la compañía que contrata no las adquiere.
- El proveedor externo podría utilizar la información que obtenga en beneficio personal, incluso se puede convertir en competencia.

Entonces dentro de estas desventajas podemos sumar áreas que se recomiendan no deben aplicárseles outsourcing, estas son:

- La tesorería
- El control a proveedores
- El servicio al cliente
- Distribución y ventas
- La administración de la calidad.
- La administración estratégica.

2.1.3.3 RIESGOS

Pese a los beneficios comentados anteriormente, el outsourcing también puede entrañar una serie de riesgos ya que como toda implementación también mantiene sus riesgos, de los cuales podemos mencionar como los más relevantes, los siguientes:

2.1.3.3.1 RIESGO PROGRAMÁTICO

El riesgo programático se refiere al riesgo relacionado con la actividad subcontratada propiamente, con el contexto de negocio que rodea a la actividad, con su complejidad… Este riesgo puede venir determinado por el gran tamaño del contrato de outsourcing. Su gran escala suele determinar una mayor complejidad, incertidumbre y riesgo así como una mayor dificultad de medir los resultados.

Este tipo de riesgo también se puede manifestar cuando el servicio contratado al proveedor externo está relacionado con una tecnología novedosa, no testeada suficientemente con anterioridad lo que aumenta el riesgo de aparición de problemas no predecibles con anterioridad.

La implementación práctica del servicio o actividad subcontratada también puede constituir un factor de riesgo cuando es necesaria la colaboración de distintos departamentos, reestructuraciones en la organización.

2.1.3.3.2 RIESGO CONTRACTUAL.-

Se trata de riesgos relativos al precontrato y contrato que ligan a proveedor de servicios y cliente. En este sentido se pueden dar riesgos de renegociación oportunista, falta de representación de las capacidades reales del proveedor, etc.

El riesgo pre-contractual suele comprender la posible representación incorrecta de sus aptitudes por parte del proveedor de servicios cuando el cliente no está capacitado para detectar dicha incapacidad del proveedor para llevar a cabo la prestación con los niveles de calidad exigidos.

Tras la firma del contrato existe el riesgo de verse inevitablemente vinculado al proveedor (lock-in) con unos altos costes de sustitución que hacen imposible el cambio a otro proveedor. Estos costes de sustitución pueden adoptar la forma de costes hundidos en inversiones específicas, personalización de equipos para el proveedor, etc. El proveedor los puede utilizar para deliberadamente rebajar la calidad de los servicios / productos prestados y obtiene un mayor poder negociador cuando esto ocurre.

2.1.3.3.3 RIESGOS EN LA SEGURIDAD DE DATOS

Varios casos de fraude o robo de identidad por parte de empleados de empresas contratadas contra clientes de las empresas contratantes (Intel y

Citibank en 2005) vienen a dar apoyo al primer punto. Esto está afianzado en el hecho que no hay un motivo real, más allá de la ética empresarial, por el cual una misma empresa no pueda prestar servicios a dos empresas contratantes, rivales entre sí, a la vez. Esto se da especialmente en el caso de empresas que operan en un marco legal privilegiado o en un monopolio natural (por ejemplo, el tratamiento de basuras).

Cada vez más las empresas y los clientes de ellas se preocupan por las debilidades en materia de seguridad que se presentan en el outsourcing ya que sus proveedores llegan a manejar datos confidenciales.

Para fortalecer la seguridad y la privacidad, se tienen que exigir el cumplimiento de reglas y requisitos. Aunque en esta área las empresas han tomado muchísimas medidas para reducir los riesgos, los clientes siguen pensando en los posibles fraudes o daños que puede causar.

Eso sí, los clientes nunca están muy satisfechos con los servicios ni mucho menos con un servicio externalizado. En cierto modo, el ISO e ITIL puede garantizar la seguridad. Por lo menos son reglas rigurosas y que han sido probados por muchas empresas. Y es mejor tener controles que no tenerlos.

Otro elemento importante es la formación en materia de seguridad que se le debe proporcionar al personal que interviene en el manejo de los datos y se debe aplicar seguridad en la infraestructura. Los riesgos se pueden reducir pero son inevitables, ya que no hay nada 100% seguro.

En nuestro país muchos clientes de la banca se quejan porque sus datos personales llegan a manos de las empresas comerciales que les brindan muchas ofertas indicando que tienen buenos saldos o son buenos clientes y esa información de saldos la pudo haber proporcionado únicamente la banca. Aún en nuestro país hay mucho por hacer en materia de protección de datos personales.

2.1.3.3.4 OTROS RIESGOS.-

El outsourcing puede tener otra serie de consecuencias potencialmente adversas para la empresa. Puede suponer una pérdida de conocimientos y capacidades internas y una dilución de la ventaja competitiva de la empresa a largo plazo. Al mismo tiempo puede llevar a un coste total mayor y a una reducción de la calidad.

En relación con los recursos humanos de la empresa puede determinar una desmoralización de los mismos, si la política de externalización no se lleva a

cabo de forma inteligente, informando a los empleados sobre dicha política, etc.

De una forma un poco más específica podemos mencionar entre los riesgos más importantes que se corren con una implementación de outsourcing los que a continuación mencionamos:

- No negociar el contrato adecuado.
- Elección del contratista.
- Puede quedar la empresa en mitad de camino si falla el contratista.
- Incrementa el nivel de dependencia de entes externos.
- Incrementa en el costo de la negociación y monitoreo del contrato.
- Existente control sobre el personal del contratista.

A continuación presento una tabla que puede mostrar de una forma clara el riesgo y su respectivo impacto en la externalización.

RIESGOS	IMPACTO
Estrategia: La estrategia de la externalización no se alinea con objetivos corporativos.	• La decisión de externalizar no es la correcta. • El contrato no se fija y no se maneja conforme a objetivos corporativos
Viabilidad: Las asunciones, suposiciones (e.g., reembolso, período, cliente y suministro - impactos de cadena, y ahorro en costes) son incorrectos	• El potencial para la externalización no se explora detalladamente, dando por resultado la falta de beneficios completamente derivados.

como resultado de una inadecuada y lenta diligencia de los proveedores y del fracaso de la organización en determinar riesgos relevantes.	• El contrato se concede a un proveedor inapropiado. • Los productos del proveedor no se manejan con eficiencia ni eficacia porque no fueron anticipados correctamente.
Transacción: Las políticas no se aplican: los acuerdos del servicio-nivel apropiado no se ejecutan: los recursos operacionales, humanos (HR) y las implicaciones reguladoras no se consideran: y los arreglos de contingencia no se planean.	• La ausencia de un acuerdo bien-elaborado podría llevar a una situación en la cual el cliente podría apoyarse en un documento legal para asegurar la el acuerdo con el vendedor en los términos contractuales previstos. • Las aperturas potenciales de la conformidad reguladora existen para conducir a penas financieras y a repercusiones negativas sobre el buen nombre de la compañía.
Transición: Se carece de una transición formal, planeando fracasar el plan para la retención de habilidades apropiadas, y una poco efectiva escalada y resolución de disputas operacionales IT.	• Hay una pérdida de recursos dominantes durante el período de transición. • Las dificultades operacionales se presentan. • Disminuye la confianza del cliente en el servicio de la externalización
Optimización y Transformación: El contrato de la externalización no es manejado eficazmente. Por lo tanto los beneficios y la eficiencia de la externalización no se comprenden.	• El retorno de la inversión no fue lo que se esperaba o es mínimo comparada con los costos de la externalización. • La organización proporciona servicios inferiores a los niveles establecidos y esperados. • Hay una elevación en los costos imprevistos.
Terminación y Renegociación: Hay una terminación inadecuada de los procesos de la externalización.	• La compañía no puede asumir el control la actividad externalizada en una fecha posterior ni terminar o renegociar el contrato.

TABLA 2.1: Ejemplos de IT riesgos e impacto de la externalización

2.2 RAZONES PARA ADOPTAR OUTSOURCING

Podemos decir que existen muchas razones para utilizar este sistema de contratación entre las más relevantes tenemos:

- Reducir o controlar el gasto de operación. En un estudio realizado por el Outsourcing Institute se encontró que las compañías redujeron costos en un 90 %.
- Disponer de los fondos de capital. El Outsourcing reduce la necesidad de tener que incluir fondos de capital de funciones que no tienen que ver con la razón de ser de la compañía.
- Tener acceso al dinero efectivo. Se puede incluir la transferencia de los activos del cliente al proveedor.
- Manejar más fácilmente las funciones difíciles o que están fuera de control. El Outsourcing es definitivamente una excelente herramienta para tratar esta clase de problema.

Dentro de este sistema podemos enunciar razones de tipo estratégicas, estas pueden ser:

- Enfocar mejor la empresa. Permite a la compañía enfocarse en asuntos empresariales más ampliamente.

- Tener acceso a las capacidades de clase mundial. La misma naturaleza de sus especializaciones, los proveedores ofrecen una amplia gama de recursos de la clase mundial para satisfacer las necesidades de sus clientes.
- Acelerar los beneficios de reingeniería.
- Compartir riesgos.
- Destinar recursos para otros propósitos.

Otros motivos más por los cuales se considera como una excelente opción la utilización de la externalización pueden ser:

- Alcanzar la máxima efectividad enfocándose en lo que la empresa hace mejor.
- Aumentar la flexibilidad para alcanzar el cambio según las condiciones de negocio, la demanda de los productos y/o servicios y la tecnología.
- Mejorar el rendimiento de la organización, aumentando la productividad, la calidad, mejorando la fiabilidad y el tiempo en las entregas, en general, ciclos de tiempo más rápidos, optimización de la utilización de los recursos, mayor disponibilidad y mayor rendimiento.

- Transferencia de costos de personal (incluso los derechos adquiridos por ley) y gastos de gestión a la empresa proveedora.
- Convertir los costos fijos en costos variables.
- Reducir inversiones en equipo, inventarios, personal, entre otros, para utilizar esos recursos para otras utilidades.
- Ganar acceso al mercado y oportunidades de negocio, a través de la red de proveedores.
- Expandir las operaciones en períodos en que tal expansión no podría ser financiada.
- Recibir ideas innovadoras para mejorar el negocio, los productos o los servicios.

Ante todos los puntos expuestos podemos resumir que el outsourcing es *u*na gran oportunidad de conseguir cuatro factores clave de negocio: especialización, escalabilidad, eficiencia de costes y velocidad de respuesta ante el mercado.

Una vez empezado un negocio, la compañía no necesita especializarse en atención al cliente o soporte en línea, entre otras muchas. Es por ello que muchas compañías han optado por el outsourcing. El servicio al es

desarrollado mejor por una empresa especializada, con experiencia, y costes mucho más bajos. De modo, además de ahorro que se produce, los creadores del negocio puede concentrase en hacer crecer la compañía y mejorar su rendimiento.

A continuación aquí presento algunas de las principales razones para subcontratar una empresa de outsourcing, estas son:

- La actividad a subcontratar no es vital, no genera benéficios o no contribuye a ser más competitivo.
- La actividad a subcontratar es un proceso rutinario que malgasta tiempo y energía de personas.
- La actividad a subcontratar es una necesidad temporal o bien que aparece de forma cíclica.
- Es más barato subcontratar la actividad que hacerla desde la propia empresa, pero afecta a personas o recursos que serían rentables y necesarios usados en otra actividad.
- Las habilidades requeridas para desarrollar la actividad son tan especializadas es poco práctico y rentable tener a alguien empleado de manera regular en ello.

2.3 MODELOS DE OUTSOURCING INFORMÁTICO

Anteriormente y a través de la historia conocíamos al modelo de outsourcing denominado tradicional, mediante este modelo los activos, los recursos y las responsabilidades operativas del proyecto son transferidos por completo a una entidad externa, mejorando así la competitividad de la empresa que lo pone en práctica.

Pero en la actualidad sabemos claramente que es precisamente el hecho de determinar si la participación del subcontratado será total o parcial, la que determine ante qué tipo de outsourcing nos encontramos. Por esta razón encuentro necesario tratar el outsourcing desde ambos puntos de vista.

2.3.1 OUTSOURCING INFORMÁTICO TOTAL

Entendemos claramente que el outsourcing, en principio, sólo significa la subcontratación con un suministrador externo de un servicio o parte del mismo, es entonces cuando al referirnos a este pensamos en el todo o nada.

Es decir cuando hablamos de un outsourcing informático pensamos en la cesión total de la gestión a un tercero, los activos, recursos humanos, hardware, software, mantenimiento, etc., en fin de absolutamente todo. Una de las formas del outsourcing total es el llamado **COSOURCING**, el cual consiste en la integración total del suministrador del outsourcing informático en el tejido de la empresa a la que presta o prestara el servicio.

2.3.2 OUTSOURCING INFORMÁTICO PARCIAL

SI NOS REFERIMOS A UN OUTSOURCING PARCIAL PODREMOS ENCONTRAR RAMIFICACIONES QUE SE PRESENTAN EN FORMA DE ABANICO DE SERVICIOS OFRECIDOS POR EL SUMINISTRADOR EN ESTE CASO, ESTOS PUEDEN SER:

- **SISTEMAS CENTRALIZADOS.**
- **SISTEMAS DISTRIBUIDOS.**
- **GESTIÓN DE APLICACIONES.**
- **REDES Y COMUNICACIONES.**
- **MANTENIMIENTO DE SOFTWARE Y HARDWARE**
- **DESARROLLO DE APLICACIONES.**

AHORA ANALIZAREMOS LA VARIEDAD QUE NOS PUEDE PRESENTAR EL OUTSOURCING PARCIAL.

2.3.2.1 OUT-TASKING

ESTA SE TRATA DE UNA DE LAS FORMULAS QUE EN LA ACTUALIDAD ESTÁ SUSTITUYENDO A LAS TRADICIONALES FORMAS DE OUTSOURCING. MEDIANTE ESTE TÉRMINO SE DESIGNA A UN MODELO DE CONTRATACIÓN DE SERVICIOS EN EL CUAL LAS EMPRESAS USUARIAS FIJAN ACUERDOS CON OTRAS EMPRESAS PARA LA GESTIÓN DE DETERMINADAS TAREAS, ES DECIR QUE LAS FIRMAS DE OUT-TASKING NO SE HACEN CARGO DE TODAS LAS TECNOLOGÍAS DE LA INFORMACIÓN DEL USUARIO SINO TAN SOLO DE CUESTIONES MUY ESPECIFICAS YA SEÑALADAS Y ACORDADAS CON EL CONTRATANTE.

A ESTE MÉTODO SE LO CONSIDERA COMO UNO MUY PRÁCTICO CUANDO SE TRATA DE CONTRATAR SERVICIOS EXTERNOS YA QUE PERMITE A LAS ORGANIZACIONES CONTRATAR DETERMINADAS PERSONAS O COMPAÑÍAS PARA QUE SE ENCARGUEN DE ASUNTOS ESPECÍFICOS EN LA GESTIÓN DE SUS SISTEMAS DE INFORMACIÓN.

ESTO HACE QUE EN MUCHAS OCASIONES EL OUT-TASKING SEA RECONOCIDO COMO EL PRIMER PASO PARA REALIZAR CONTRATOS DE OUTSOURCING A GRAN ESCALA.

2.3.2.2 LAS 7 TENDENCIAS DEL OUTSOURCING INFORMÁTICO

[8]**PARA TRATAR OTROS TIPOS DE OUTSOURCING PARCIALES TOMAREMOS LAS 7 GRANDES TENDENCIAS DEL OUTSOURCING INFORMÁTICO SEGÚN LESLIE P. WILCOCKS, ESTAS SON:**

1. OUTSOURCING EXTRATERRITORIAL, ESTE TIPO DE OUTSOURCING ES PROPICIADO POR LAS GRANDES DIFERENCIAS DE SALARIOS Y EL AVANCE Y REDUCCIÓN DE COSTES EN LAS COMUNICACIONES, HOY EN DÍA PODEMOS ENCONTRAR MUY BUENOS PROFESIONALES EN PAÍSES CON MENOR DESARROLLO QUE LOS LLAMADOS PAÍSES INDUSTRIALIZADOS, LOS MISMOS QUE PUEDEN REALIZAR LOS TRABAJOS CON UN COSTE MUY INFERIOR.

2. OUTSOURCING DE VALOR AÑADIDO, SON AQUELLOS EN EL CUAL LOS CONTRATANTES SE IMPLICAN A LA VEZ EN EL DESARROLLO DE ALGÚN PRODUCTO DEMANDADO POR EL MERCADO QUE INCORPORA VALOR AÑADIDO A LA OPERACIÓN.

3. PARTICIPACIÓN DE CAPITAL, SE TRATA DE ACUERDOS DE ASOCIACIÓN O CREACIÓN DE NUEVAS ENTIDADES.

4. MULTIPROVISIONAMIENTO, ESTE ES PARA EVITAR EL RIESGO DE UN SOLO SUMINISTRADOR, POR ESO CONTRATA CADA ÁREA CON UNO DISTINTO. TIENE EL INCONVENIENTE DE QUE SE PRECISA CONTROLAR LA GESTIÓN CON VARIOS ADMINISTRADORES.

[8] 1Leslie P. Wilcocks “Reducir los riesgos de la subcontratación Informática” Expansión Febrero de 1999

5. COAPROVISIONAMIENTO, ES CUANDO EL SUMINISTRADOR SE COMPROMETE EN EL PROCESO DEL CLIENTE, PROCURANDO REDUCIR EL PROCESO DE DESARROLLO Y TERMINACIÓN DE LOS PRODUCTOS DEPENDIENTES DE SU REMUNERACIÓN DEL ÉXITO OBTENIDO.

6. SEGREGACIONES, ES AQUEL QUE TAMBIÉN SE CONOCE COMO PSEUDO-OUTSOURCING. SE AGREGA EL ÁREA INFORMÁTICA DE UNA ORGANIZACIÓN CONVIRTIÉNDOLA EN UNA EMPRESA QUE DA SERVICIO A ESA ORGANIZACIÓN INTEGRÁNDOSE COMO UNA MÁS EN EL GRUPO DE EMPRESAS Y A VECES HASTA ENTREGANDO EL SERVICIO A OTRAS EMPRESAS QUE NO SON DEL GRUPO.

7. OUTSOURCING DE TRANSICIÓN, ESTA ES UNA DE LAS QUE MÁS ÉXITO HA TENIDO ÚLTIMAMENTE. SIRVE PARA SOLUCIONAR UN PROBLEMA TEMPORAL, COMO ES LA TRANSICIÓN A UN NUEVO SISTEMA.

8. OTROS TIPOS DE OUTSOURCING PUEDEN SER:

2.3.3 EL PSEUDO-OUTSOURCING

CUANDO LAS OPERACIONES LAS VIENEN REALIZANDO ALGUNOS GRUPOS EMPRESARIALES CREANDO NUEVAS EMPRESAS DEDICADAS ESPECÍFICAMENTE A GESTIONAR LA INFORMÁTICA DE TODAS LAS EMPRESAS DEL GRUPO, PUES EN ESE

MOMENTO PODEMOS DECIR QUE NOS ENCONTRAMOS ANTE UN PSEUDO-OUTSOURCING.

PODEMOS DECIR QUE ESTE SERÍA COMO UN OUTSOURCING CON PARACAÍDAS, YA QUE LA NUEVA EMPRESA DEPENDERÁ TOTALMENTE DEL GRUPO; CON LO CUAL, LO QUE SE HA HECHO EN REALIDAD ES SIMPLEMENTE UN TRASLADO DE FUNCIONES DENTRO DE LA OPERATORIA DE LA ORGANIZACIÓN DE GRUPO EMPRESARIAL.

CON ESTE PROCEDIMIENTO LO QUE SE PRETENDE ES DESHACERSE DEL PERSONAL INFORMÁTICO TRASLADÁNDOLO DESDE GRANDES EMPRESAS, CON UN ALTO PRESTIGIO, A OTRAS EN LAS QUE ES MÁS FÁCIL FLEXIBILIZAR LA PLANTILLA SIN GRANDES ESCÁNDALOS NI PERJUICIOS DE IMAGEN.

2.3.4 EL E-SOURCING

ESTE SE BASA EN EL MERCADO DE INTERNET INCLUYENDO VARIAS TECNOLOGÍAS EN EL MISMO, ESPECIALMENTE EN LA WEB, ESTAS FACILITAN DESDE SOLUCIONES PURAS DE E-SOURCING HASTA SISTEMAS DINÁMICOS DE TRANSACCIÓN Y SUBASTA.

PARA PODER EFECTUAR LA ELECCIÓN MÁS APROPIADA EN FUNCIÓN A SUS NECESIDADES, LAS EMPRESAS DEBERÁN TENER EN CUENTA SU TAMAÑO Y LOS

RECURSOS PROPIOS, TANTO FINANCIEROS COMO TECNOLÓGICOS, CON LOS QUE CUENTA.

EL E-SOURCING ES UN SISTEMA DISEÑADO PARA SOPORTAR PROCESOS DE COMPRA COMPLEJOS SIENDO EL VOLUMEN DE TRANSACCIONES ALGO DEFICIENTE. ESTÁN DIRIGIDOS A EMPRESAS GRANDES Y EL PROCESO ES EL SIGUIENTE:

- EL COMPRADOR PIDE A LOS PROVEEDORES OFERTAS SOBRE UN PRODUCTO O SERVICIO DETALLANDO LOS REQUISITOS QUE DEBEN TENER AQUELLAS.
- EL SISTEMA RECOPILA LAS OFERTAS QUE REÚNAN TODOS LOS REQUISITOS EXIGIDOS.
- FACILITA DICHA INFORMACIÓN AL CLIENTE PARA QUE EL PUEDA VALORARLAS Y ASÍ PODER ELEGIR LA QUE LE RESULTE LA MÁS CONVENIENTE.

2.3.5 FACILITIES MANAGEMENT

FACILITIES MANAGEMENT ES UN SISTEMA QUE CONSTANTEMENTE ES CONFUNDIDO CON EL OUTSOURCING YA QUE DIFERENCIARLAS RESULTA MUY COMPLEJO EN

OCASIONES, POR ESTA RAZÓN DECIDÍ CITARLA PARA ENTENDER LA RELACIÓN ENTRE SÍ.

HAY QUE ENTENDER QUE SON COSAS DIFERENTES, AUNQUE COMO OCURRE EN OTROS CASOS EXISTE UNA SERIE DE PUNTOS DE FRICCIÓN EN QUE PUEDE SER DIFÍCIL DISTINGUIR SI SE TRATA DE UN OUTSOURCING O UN FACILITIES MANAGEMENT, TAMBIÉN CONOCIDA COMO GESTIÓN DE ACTIVOS.

VOY A CITAR DOS EJEMPLOS PARA TRATAR DE COMPRENDERLO MEJOR.

LA EMPRESA X ES PROPIETARIA DE UN INMUEBLE QUE PIENSA ALQUILAR POR OFICINAS Y CONTRATA CON LA EMPRESA Y QUE ESTA SEA QUIEN LE GESTIONE LA ADMINISTRACIÓN DEL EDIFICIO: LIMPIEZA, SEGURIDAD, COBRO DE ALQUILERES, ETC. ESTAMOS ANTE UN CASO DE FACILITIES MANAGEMENT.

1. LA EMPRESA X CONTRATA CON LA EMPRESA Y PARA QUE REALICE TODAS LAS OPERACIONES DE SU CENTRO DE PROCESO DE DATOS, PARA LO CUAL LE TRANSFIERE: EQUIPOS, PERSONAL Y APLICACIONES. ESTO ES UN CLARO CASO DE OUTSOURCING.

COMO PODEMOS VER EN LOS EJEMPLOS CITADOS LA DIFERENCIA CLAVE ES QUE LOS FACILITIES MANAGEMENT SE ALEJAN CADA VEZ MÁS DE LOS ENTORNOS TECNOLÓGICOS Y SE ACERCAN A OTRO TIPO DE GESTIÓN DE ACTIVOS COMO EL DEL

CASO EXPUESTO, MIENTRAS QUE EL OUTSOURCING SE MANTIENE DENTRO DEL MARCO DE LA TECNOLOGÍA.

2.4 ASPECTOS CONTRACTUALES A TENER EN CUENTA EN EL OUTSOURCING.-

Esta es talvez la parte más importante del capítulo ya que aquí veremos los aspectos que debemos tener en cuenta como auditores de Sistemas al momento de establecer un contrato de outsourcing Informático, todos los requisitos y cumplimiento de los mismos como tal.

Entre los más relevantes tenemos:

2.4.1 LOS ACUERDOS DE NIVELES DE SERVICIOS.

Los Acuerdos de Niveles de Servicios (ANS), parte vital en un contrato de Outsourcing, tratan de aquellos compromisos que deben determinar la calidad del servicio, por lo tanto deben ser medibles, viables y responder a las necesidades y expectativas del cliente.

Uno de los aspectos fundamentales cuando se adelanta cualquier negociación de Outsourcing es el tema relacionado con los Acuerdos de Niveles de Servicios, ANS, o SLAs (Service Level Agreements) que hacen

referencia al consenso sobre el alcance y requerimientos de servicios entre el cliente y el proveedor conocido en esta práctica como outsourcer.

Cuando se decide contratar externamente servicios de Informática y Telecomunicaciones o de Procesos de Negocios es muy importante poder medir la calidad de los servicios prestados por el Outsourcer en función de su disponibilidad, seguridad, atención oportuna, tiempo de respuesta a incidentes, etc.

“Los SLAs lo que hacen es estructurar herramientas de medición alrededor de poder determinar objetivamente si un proceso de Outsourcing está andando o no. Es una métrica de servicio, acuerdos contractuales entre el proveedor y el cliente que especifican en términos mesurables la cantidad y calidad y oportunidad de servicios a prestar” afirma Francisco Daza, Gerente de Operaciones de Atos Origin.

Adicionalmente es fundamental medir la satisfacción de los usuarios internos y externos de los clientes. “Un proyecto de Outsourcing puede ser financieramente productivo, haber reducido una serie de costos, puede haber una propuesta de creación de valor muy importante, pero si el usuario no estuvo satisfecho el procesos se va abajo, es un desastre por demanda popular” explica Daza.

Los ANS establecen compromisos sobre la oportunidad en la atención, la disponibilidad, el desempeño, las tareas entregables establecidas mediante un cronograma donde se debe dimensionar la complejidad de las labores, los problemas de seguridad y eventos asociados al control de acceso y detección de Intrusos para ver que tan vulnerable o efectivo es el sistema de seguridad de la empresa. En los procesos de Outsourcing de Negocios se miden también las transacciones a procesar por unidad de tiempo.

En Outsourcing de servicios informáticos “Un aspecto importante con respecto a la medición y disponibilidad de los servicios es cómo se mide la disponibilidad: En ocasiones se mide la disponibilidad del servidor, de la red, pero realmente los servicios que el usuario ve al frente van incorporando una serie de elementos alrededor de esto. Es importante tener en cuenta que cuando se quiera medir disponibilidad de servicio debe hacerse de manera homogénea teniendo en cuenta cada uno de los elementos, lo que al usuario le importa es que todos los elementos están interactuando.”, explica Daza. Yo puedo medir la disponibilidad de un servidor y determinar que se “cayo” media hora en el mes y cuando se levantó el servidor se “cayó” la red, otra media hora, después se “cayó” una información que estaba en el servidor UNIX una hora, luego hubo problema en el PC otra hora, si uno mira los componentes individualmente, cada uno tuvo una caída

de media hora o una hora y cumplió los niveles de servicio, pero el usuario no tuvo servicio casi durante medio día. No es fácil, pero es un reto en que se le debería trabajar porque realmente eso es lo que determina la satisfacción del usuario."

Es conveniente establecer un formato que refleje lo que estipula el acuerdo, donde se aclare la gerencia o unidad para la cual se está prestando el servicio, el tipo de servicio, cuándo empieza y termina, el objetivo de servicio, la forma de acceder al mismo (mediante una llamada, enviando un correo electrónico, etc.), los horarios del servicio donde se aclare el tiempo requerido para atender el inconveniente y para solucionarlo dependiendo del tipo de aplicaciones o complejidad y cómo se miden los servicios que se van a prestar.

Después de establecerse las ANS, deben complementarse con el establecimiento de sistemas de medición objetiva de servicios que califica el nivel de desempeño frente a un desempeño mínimo y a uno deseado. Se establecen entonces esquemas de multas y recompensas. Adicionalmente, hay que medir la satisfacción del cliente, lo cual se puede hacer mediante encuestas realizadas por un tercero de manera periódica o cuando lo consideren las partes dependiendo del nivel de control que se quiera. Sin

embargo, es aconsejable hacer encuestas en “caliente” en el momento en que un usuario solicita un servicio, para medir el día a día, puesto que permite tener información específica, tener un control y tomar acciones de mejora. De esta manera, se puede observar si se está cumpliendo o no con las expectativas del cliente.

Finalmente, es primordial establecer reuniones periódicas donde se presente un reporte con esos indicadores para revisar los resultados y aplicar los premios o los descuentos o multas pertinentes

2.4.2 TIPOS DE SERVICIOS QUE DEBE INCLUIR UN CONTRATO DE OUTSOURCING INFORMÁTICO

Como todos sabemos el servicio de OUTSOURCING en Informática consiste en externalizar todos los trabajos necesarios para garantizar el correcto funcionamiento diario de su red, mediante el pago de una tarifa plana. Siendo así estamos obligados a tener muy en cuenta los tipos de servicios que el contrato debe incluir, básicamente incluye tres tipos de servicios:

Mantenimiento preventivo

- Acciones a realizar para evitar futuros problemas: copias de seguridad, antivirus, espacio en disco, control de accesos, passwords etc.

Mantenimiento correctivo

- Intervenciones para la resolución de problemas puntuales. Trabajo con acceso remoto y desplazamiento in situ si el problema lo requiere. Atención inmediata.

Asesoría IT

- Soporte a la empresa en decisiones relacionadas con su infraestructura informática y de comunicaciones

2.4.3 CONTRATO DE MANTENIMIENTO DE SOFTWARE

La importancia del contrato de mantenimiento sobre un software radica en el hecho de que cualquier aplicación informática, por más que se intente depurar al máximo por su desarrollador o fabricante, contiene o puede

contener errores o defectos implícitos desconocidos en el momento de la adquisición del software.

A esto hay que añadir los continuos avances que tienen lugar en el sector tecnológico, que hacen que lo que hoy es actualidad, mañana ha podido quedar obsoleto, por lo que se requiere una permanente actualización de nuestros sistemas.

Vemos así como el software, lejos de ser un producto estático, es un producto dinámico que, necesaria y constantemente, requiere ser modificado, adaptado, corregido y mejorado. Por ello, es indudable la necesidad de los usuarios de adaptar el software a los cambios, tanto internos como externos que pueda sufrir su empresa, cambios legales, sectoriales, etc.

2.4.4 PREVENCIÓN FRENTE AL OUTSOURCING

Es muy importante tener en cuenta que desde el mismo momento en que una organización empieza a hablar de subcontratación, ya sea de todo o parte de sus tareas informáticas, se empieza a generar una serie de temores, miedos y prevenciones.

Estos temores y preocupaciones se centran mayormente en áreas como la Dirección General y la Dirección General de Sistemas de Información y dentro de esta especialmente en el área o Departamento de Informática, planteándose desde ahí las siguientes preguntas:

- ¿Perderemos el control de una parte importante de la Organización?
- ¿Pondremos en manos de un tercero que dentro de un tiempo podría desaparecer?
- ¿Cómo pueden desde afuera estar al tanto de nuestras necesidades y de que sería lo más conveniente para nosotros?
- ¿Qué sucedería si dentro de un tiempo decidimos volver a gestionar los recursos informáticos de la organización?

Por todas estas interrogantes que se dan a raíz de una subcontratación es que resulta necesario que tomemos todas las cautelas que nos permitan tener la certeza de que ante la firma de un contrato de outsourcing no nos exponemos a la posible pérdida del control sobre la información de la empresa, sino más bien a todo lo contrario.

Debemos asegurar que en el caso de un outsourcing parcial, nóminas, explotación, mantenimiento, no existirá problema alguno en la continuidad de la

Dirección de Sistemas de Información, es más, ni aun siendo un outsourcing total las garantías deberán ser las mismas, ya que no solo deberán continuar con su responsabilidad anterior sino que además participara en el Comité de Seguimiento y Control para mejor desarrollo del proyecto

CAPITULO 3

2. FUNDAMENTACIÓN NORMATIVA Y/O ESTÁNDARES INTERNACIONALES

Mediante este capítulo pretendo difundir y entregar un breve análisis de aquellas normativas y estándares internacionales que se vienen desarrollando y actualizando a través del tiempo con la finalidad de entregar al profesional en auditoria el marco normativo necesario en el cual basarse para realizar su trabajo de manera totalmente profesional cumpliendo de esta forma con todas las leyes y disposiciones que le rigen, específicamente en el área de contratación externa

También mencionaremos las nuevas disposiciones que se crearon en la Asamblea Nacional Constituyente, nos referimos al mandato 8, el cual elimina la tercerización, pero deja en claro ciertas clausulas para actividades especiales no especificas de la organización.

Cabe recalcar que las normativas analizadas en este capítulo hacen referencia justamente a las Normas de Control Interno, ya que son estas las que rigen en el tipo de auditoría que hemos estado tratando, pero nos centraremos en la base

de este trabajo que es lo que nos interesa, por esta razón consideraremos de dichas normas únicamente las partes que traten sobre el outsourcing, más específicamente el Informático. Solo aquellas normas o estándares que lo requieran serán transcritas tal como se presentan.

3.1 MANDATO NÚMERO 8 DE LA ASAMBLEA CONSTITUYENTE

En este caso específico trataremos únicamente las disposiciones generales que dentro de este mandato se encuentran y el artículo 16 de la contratación civil de servicios técnicos especializados, por ser estas nuestro punto de interés, a continuación transcribiré las mismas

.

3.1.1 DISPOSICIONES GENERALES.-

PRIMERA.- Para el caso de las empresas del sector estratégico público., los servicios técnicos especializados que requieran dichas empresas, podrían ser contratados civilmente. Los trabajadores de las empresas de servicios técnicos especializados, tendrán relación directa y bilateral con estas y se sujetaran a las disposiciones del Código de Trabajo.

SEGUNDA.- Se podrá contratar civilmente servicios técnicos especializados ajenos a las actividades propias y habituales de la usuaria, tales como los de contabilidad, publicidad, consultoría, auditoria, jurídicos y de sistemas, entre otros, que serán prestados por personas naturales o jurídicas con su propio personal y que contaran con la adecuada infraestructura física y estructura organizacional, administrativa y financiera. La relación laboral será directa y bilateral entre los prestadores de servicios técnicos especializados y sus trabajadores.

TERCERA.- Los profesores de establecimientos particulares de niveles pre-primario, primario, medio y superior, que no laboren jornadas completas diarias o semanales de trabajo, serán contratados mediante la modalidad de jornada parcial. El Ministerio de Trabajo y Empleo establecerá la respectiva Comisión Sectorial para la fijación del sueldo o salario básico unificado de los trabajadores de este sector. Además tendrá derecho a la protección integral del Código del Trabajo y percibirán sus remuneraciones aun en los periodos vacacionales.

CUARTA.- Se garantiza la contratación colectiva de trabajo en las instituciones de sector público, empresas públicas estatales, de organismos sectoriales y por las entidades de derecho privado en las que, bajo cualquier denominación,

naturaleza o estructura jurídica , el Estado o sus instituciones tienen participación accionara mayoritaria y/o aportes directos o indirectos de recursos públicos, que se ajuste a los términos establecidos en los mandatos constituyente y en las regulaciones del Ministerio de Trabajo y Empleo.

3.1.2 ARTICULO 16 DE LA CONTRATACIÓN CIVIL DE SERVICIOS TÉCNICOS ESPECIALIZADOS

Se podrá contratar civilmente servicios técnicos especializados ajenos a las actividades propias y habituales de la empresa usuaria, tales como los de contabilidad, publicidad, consultoría, auditoría, jurídicos y de sistemas, entre otros, que serán prestados por personas naturales o jurídicas en sus particulares instalaciones, con su propio personal, las que contarán con la adecuada infraestructura física y estructura organizacional, administrativa y financiera. La relación laboral será directa y bilateral entre los contratistas prestadores de servicios técnicos especializados y sus trabajadores, sin que haya responsabilidad solidaria por parte de la usuaria, salvo el caso de que exista vinculación en los términos señalados en el artículo 13 del Reglamento.

Entonces analizando las disposiciones generales que se desarrollaron dentro de este mandato podremos ver que exactamente la segunda disposición general es

la que nos da carta abierta al desarrollo de este proyecto ya que mantiene la contratación de personal externo, en actividades como son auditoria y sistemas también, siendo estas dos vitales para el desarrollo de un outsourcing informático, siempre y cuando se conozca a ciencia cierta que estas no forman parte de las actividades usuales de la usuaria.

3.2 NORMAS DE CONTROL INTERNO

A continuación veremos aquellas normas que rigen las contrataciones de servicios de outsourcing, considerare únicamente aquellos puntos que sean de interés para este proyecto, es decir los que hagan referencia a la contratación externa.

3.2.1 NORMAS DE CONTROL INTERNO COSO

Como se dijo anteriormente solo mencionaremos lo que haga referencia al outsourcing, considero que el COSO está muy generalizado, pero aun así tomare en cuenta su desarrollo ya que estos puntos que se tratan aquí son de utilidad a la hora de determinar y fijar controles en las políticas que se incluirá en el manual resultante de toda la investigación previa.

Debido al mundo económico integrado que existe hoy en día se ha creado la necesidad de integrar metodologías y conceptos en todos los niveles de las diversas áreas administrativas y operativas con el fin de ser competitivos y responder a las nuevas exigencias empresariales, surge así un concepto que se creó hace más de una década y ha venido siendo utilizado eficazmente en las tareas de control interno donde se brinda una estructura común el cual es documentado en el denominado informe COSO.

La definición de control interno se entiende como el proceso que ejecuta la administración con el fin de evaluar operaciones especificas con seguridad razonable en tres principales categorías: Efectividad y eficiencia operacional, confiabilidad de la información financiera y cumplimiento de políticas, leyes y normas, en este caso del personal contratado mediante el método de contratación externa, también conocida como outsourcing.

El control interno posee cinco componentes que pueden ser implementados en todas las compañías de acuerdo a las características administrativas, operacionales y de tamaño; los componentes son: un ambiente de control, una valoración de riesgos, las actividades de control (políticas y procedimientos), información y comunicación y finalmente el monitoreo o supervisión.

La implementación del control interno implica que cada uno de sus componentes estén aplicados a cada categoría esencial de la empresa convirtiéndose en un

proceso integrado y dinámico permanentemente, como paso previo cada entidad debe establecer los objetivos, políticas y estrategias relacionadas entre sí con el fin de garantizar el desarrollo organizacional y el cumplimiento de las metas corporativas; aunque el sistema de control interno debe ser intrínseco a la administración de la entidad y busca que esta sea más flexible y competitiva en el mercado se producen ciertas limitaciones inherentes que impiden que el sistema como tal sea 100% confiable y donde cabe un pequeño porcentaje de incertidumbre, por esta razón se hace necesario un estudio adecuado de los riesgos internos y externos con el fin de que el control provea una seguridad razonable para la categoría a la cual fue diseñado, estos riesgos pueden ser atribuidos a fallas humanas como la toma de decisiones erróneas, simples equivocaciones o confabulaciones de varias personas, es por ello que es muy importante la contratación de personal con gran capacidad profesional, integridad y valores éticos así como la correcta asignación de responsabilidades bien delimitadas donde se interrelacionan unas con otras con el fin de que no se rompa la cadena de control fortaleciendo el ambiente de aplicación del mismo, cada persona es un eslabón que garantiza hasta cierto punto la eficiencia y efectividad de la cadena, cabe destacar que la responsabilidad principal en la aplicación del control interno en la organización debe estar siempre en cabeza de la administración o alta gerencia con el fin de que exista un compromiso real

a todos los niveles de la empresa, siendo función del departamento de auditoría interna o quien haga sus veces, la adecuada evaluación o supervisión independiente del sistema con el fin de garantizar la actualización, eficiencia y existencia a través del tiempo, estas evaluaciones pueden ser continuas o puntuales sin tener una frecuencia predeterminada o fija, así mismo es conveniente mantener una correcta documentación con el fin de analizar los alcances de la evaluación, niveles de autorización, indicadores de desempeño e impactos de las deficiencias encontradas, estos análisis deben detectar en un momento oportuno como los cambios internos o externos del contexto empresarial pueden afectar el desarrollo o aplicación de las políticas en función de la consecución de los objetivos para su correcta evaluación.

La comprensión del control interno puede así ayudar a cualquier entidad pública o privada a obtener logros significativos en su desempeño con eficiencia, eficacia y economía, indicadores indispensables para el análisis, toma de decisiones y cumplimiento de metas.

Aunque la tecnología y la información representan un gran factor para el desarrollo empresarial existen muchas compañías en las cuales estos nuevos enfoques de control y administración son desconocidos totalmente, ya sea por motivos de cultura gerencial y contable o por falta de formación técnica

profesional de sus dueños o administradores lo que deja al país rezagado frente a la competitividad mundial que se exige permanentemente.

Siendo el contador público un gran participe en la administración de las compañías como asesor o consultor, es este profesional que debe adquirir el compromiso de propender el desarrollo empresarial con la implementación de nuevos conceptos, concepto como el de control interno moderno que sería de gran utilidad en la consecución de objetivos y metas institucionales sobretodo de las pequeñas y medianas empresas que son las más urgidas de una adecuada asesoría operativa, financiera y normativa, categorías que reúne en su estructura conceptual y aplicativa el control interno.

3.2.1.1 DEFINICIÓN Y OBJETIVOS

El Control Interno es un proceso integrado a los procesos, y no un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y políticas.

Al hablarse del control interno como un proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, inherentes a la gestión e integrados a los demás procesos básicos de la misma: planificación, ejecución y supervisión. Tales acciones se hallan incorporadas (no añadidas) a la infraestructura de la entidad, para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad.

Según la Comisión de Normas de Control Interno de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), el control interno puede ser definido como el plan de organización, y el conjunto de planes, métodos, procedimientos y otras medidas de una institución, tendientes a ofrecer una garantía razonable de que se cumplan los siguientes objetivos principales:

- Promover operaciones metódicas, económicas, eficientes y eficaces, así como productos y servicios de la calidad esperada.
- Preservar al patrimonio de pérdidas por despilfarro, abuso, mala gestión, errores, fraudes o irregularidades.
- Respetar las leyes y reglamentaciones, como también las directivas y estimular al mismo tiempo la adhesión de los integrantes de la organización a las políticas y objetivos de la misma.

- Obtener datos financieros y de gestión completos y confiables y presentados a través de informes oportunos.

En cuanto a los objetivos anteriores podemos decir que solo nos competen dos de ellos, aquellos resaltados con negritas, por tratarse de puntos necesarios de considerar al momento de la implementación de un outsourcing, más aun si se trata de uno realizado a la gestión de las bases de datos del usuario.

3.2.1.2 COMPONENTES

El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión

Todos los puntos mencionados anteriormente son de vital importancia para llevar de manera eficiente el control interno dentro de una organización, pero

básicamente dentro de un outsourcing informático podemos resumir que los más relevantes son tres de aquellos, que son:

3.2.1.2.1 EVALUACIÓN DE RIESGOS

El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza se evalúa la vulnerabilidad del sistema. Para ello debe adquirirse un conocimiento práctico de la entidad y sus componentes de manera de identificar los puntos débiles, enfocando los riesgos tanto al nivel de la organización (interno y externo) como de la actividad.

El establecimiento de objetivos es anterior a la evaluación de riesgos. Si bien aquéllos no son un componente del control interno, constituyen un requisito previo para el funcionamiento del mismo.

Los objetivos (relacionados con las operaciones, con la información financiera y con el cumplimiento), pueden ser explícitos o implícitos, generales o particulares. Estableciendo objetivos globales y por actividad, una entidad puede identificar los factores críticos del éxito y determinar los criterios para medir el rendimiento.

A este respecto cabe recordar que los objetivos de control deben ser específicos, así como adecuados, completos, razonables e integrados a los globales de la institución.

Una vez identificados, el análisis de los riesgos incluirá:

- Una estimación de su importancia / trascendencia.
- Una evaluación de la probabilidad / frecuencia.
- Una definición del modo en que habrán de manejarse.

Dado que las condiciones en que las entidades se desenvuelven suelen sufrir variaciones, se necesitan mecanismos para detectar y encarar el tratamiento de los riesgos asociados con el cambio. Aunque el proceso de evaluación es similar al de los otros riesgos, la gestión de los cambios merece efectuarse independientemente, dada su gran importancia y las posibilidades de que los mismos pasen inadvertidos para quienes están inmersos en las rutinas de los procesos.

Existen circunstancias que pueden merecer una atención especial en función del impacto potencial que plantean:

- Cambios en el entorno.
- Redefinición de la política institucional.

- Reorganizaciones o reestructuraciones internas.
- Ingreso de empleados nuevos, o rotación de los existentes.
- Nuevos sistemas, procedimientos y tecnologías.
- Aceleración del crecimiento.
- Nuevos productos, actividades o funciones.

Los mecanismos para prever, identificar y administrar los cambios deben estar orientados hacia el futuro, de manera de anticipar los más significativos a través de sistemas de alarma complementados con planes para un abordaje adecuado de las variaciones.

En conclusión considero este punto como importante dentro de un outsourcing informático, aunque aquí se encuentre más generalizado a toda la organización, por el echo de que la evaluación de riesgos es la que nos permitirá determinar aquellos puntos que debemos fortalecer y prestar mayor atención al momento de otorgar permisos y accesos a terceros dentro de una contratación externa.

3.2.1.2.2 ACTIVIDADES DE CONTROL

Están constituidas por los procedimientos específicos establecidos como un reaseguro para el cumplimiento de los objetivos, orientados primordialmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos según lo expresado en el punto anterior: conociendo los riesgos, se disponen los controles destinados a evitarlos o minimizarlos, los cuales pueden agruparse en tres categorías, según el objetivo de la entidad con el que estén relacionados:

- Las operaciones
- La confiabilidad de la información financiera
- El cumplimiento de leyes y reglamentos

En muchos casos, las actividades de control pensadas para un objetivo suelen ayudar también a otros: los operacionales pueden contribuir a los relacionados con la confiabilidad de la información financiera, éstas al cumplimiento normativo, y así sucesivamente.

A su vez en cada categoría existen diversos tipos de control:

- Preventivo / Correctivos

- Manuales / Automatizados o informáticos
- Gerenciales o directivos

En todos los niveles de la organización existen responsabilidades de control, y es preciso que los agentes conozcan individualmente cuales son las que les competen, debiéndose para ello explicitar claramente tales funciones.

La gama que se expone a continuación muestra la amplitud abarcativa de las actividades de control, pero no constituye la totalidad de las mismas:

- Análisis efectuados por la dirección.
- Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades.
- Comprobación de las transacciones en cuanto a su exactitud, totalidad, y autorización pertinente: aprobaciones, revisiones, cotejos, recálculos, análisis de consistencia, pre numeraciones.
- Controles físicos patrimoniales: arqueos, conciliaciones, recuentos.
- Dispositivos de seguridad para restringir el acceso a los activos y registros.
- Segregación de funciones.
- Aplicación de indicadores de rendimiento.

Es necesario remarcar la importancia de contar con buenos controles de las tecnologías de información, pues éstas desempeñan un papel fundamental en la gestión, destacándose al respecto el centro de procesamiento de datos, la adquisición, implantación y mantenimiento del software, la seguridad en el acceso a los sistemas, los proyectos de desarrollo y mantenimiento de las aplicaciones.

A su vez los avances tecnológicos requieren una respuesta profesional calificada y anticipativa desde el control.

Este punto centra su importancia en el outsourcing por encontrase plenamente relacionado con los riesgos que se encuentren, ya que aquí podremos determinar los controles que utilizaremos para la prevención de dichos riesgos.

3.2.1.2.3 SUPERVISIÓN

Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado. Procede la evaluación de las actividades de control de los sistemas a través del tiempo, pues toda organización tiene áreas donde los mismos están en desarrollo, necesitan ser reforzados o se impone directamente su reemplazo debido a que perdieron su eficacia o resultaron inaplicables. Las causas pueden encontrarse en los cambios internos y externos a la gestión que, al variar las circunstancias, generan nuevos riesgos a afrontar.

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias sobrevinientes.

En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

- Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.

- Son ejecutados por los propios responsables de las áreas de gestión (auto evaluación), la auditoría interna (incluidas en el planeamiento o solicitadas especialmente por la dirección), y los auditores externos.

- Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios insoslayables.

- La tarea del evaluador es averiguar el funcionamiento real del sistema: que los controles existan y estén formalizados, que se apliquen cotidianamente

como una rutina incorporada a los hábitos, y que resulten aptos para los fines perseguidos.

- Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.

- El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.

Existen controles informales que, aunque no estén documentados, se aplican correctamente y son eficaces, si bien un nivel adecuado de documentación suele aumentar la eficiencia de la evaluación, y resulta más útil al favorecer la comprensión del sistema por parte de los empleados. La naturaleza y el nivel de la documentación requieren mayor rigor cuando se necesite demostrar la fortaleza del sistema ante terceros.

Este punto es tan necesario que sin él los demás no tendrían sentido de ser, ya que de nada servirá obtener un buen contrato inicial, establecer políticas de control y todo lo demás sino no supervisamos periódicamente que estos se estén llevando a cabalidad.

3.3 ESTÁNDARES INTERNACIONALES

3.3.1 ESTÁNDAR DE CONTROL DE SISTEMAS COBIT

La siguiente parte de esta unidad tiene la finalidad de exponer las Normas COBIT de la forma más simple y sencilla posible. Por esta razón la analizaremos de una forma detallada.

Empezaremos diciendo que el cuerpo del trabajo está dividido en dos partes principales las cuales reflejan las Características y Estructura de COBIT y el Relevamiento y Aplicación de las Normas COBIT.

3.3.1.1 COBIT (OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS)

Como sabemos COBIT se basa en controles para la gestión de IT, por esa razón tratare de ampliar este tema lo mayor posible.

COBIT fue lanzado lanzado en 1996, esta es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, de escritorio, portátiles, etc., y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Los usuarios de dicho sistema pueden ser:

- La Gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Los Usuarios Finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- Los Auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.
- Los Responsables de TI: para identificar los controles que requieren en sus áreas.

3.3.1.2 CARACTERÍSTICAS

Entre las características principales de este sistema tenemos:

- Orientado al negocio
- Alineado con estándares y regulaciones "de facto"
- Basado en una revisión crítica y analítica de las tareas y actividades en TI
- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA)

3.3.1.3 PRINCIPIOS

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

3.3.1.4 REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO

Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios que son:

- **Efectividad:** La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
- **Eficiencia:** Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
- **Confiabilidad:** proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
- **Cumplimiento:** de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
- **Confidencialidad:** Protección de la información sensible contra divulgación no autorizada
- **Integridad:** Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
- **Disponibilidad:** accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

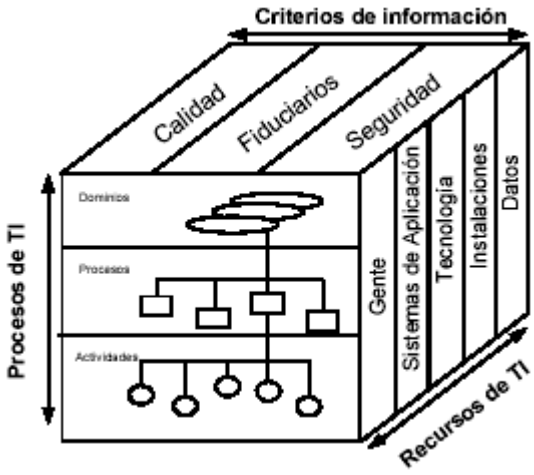


FIGURA 3.1. Las tres dimensiones conceptuales de COBIT

3.3.1.5 DOMINIOS DE RELEVANCIA DE COBIT

A continuación veremos de manera resumida y mediante el uso de cuadros, los dominios que nos resultan interesantes, los de alto impacto, de este estándar llamado COBIT.

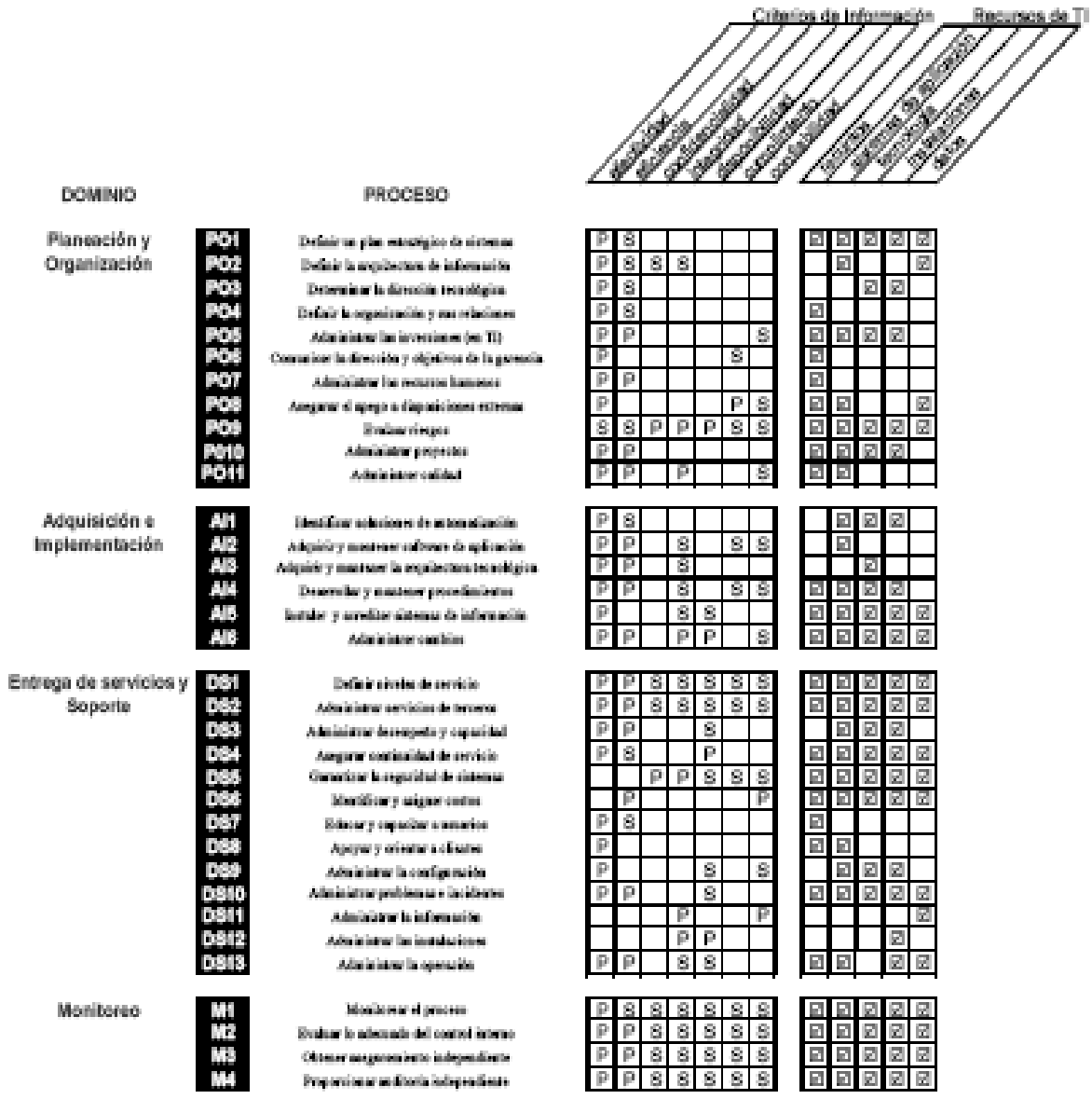


TABLA 3.1. Dominios del COBIT

En el cuadro anterior podemos apreciar la clasificación de los dominios considerados como de alto nivel.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

PLANEACION Y ORGANIZACION

PO8

Control sobre el proceso de TI de:

aseguramiento del cumplimiento de requerimientos externos

que satisface los requerimientos de negocio de:

cumplir con obligaciones legales, regulatorias y contractuales

se hace posible a través de:

la identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, y llevando a cabo las medidas apropiadas para cumplir con ellos

y toma en consideración:

- leyes, regulaciones, contratos
- monitoreo de evoluciones legales y regulatorios
- revisiones regulares en cuanto a cambios
- búsqueda de asistencia legal y modificaciones
- seguridad y ergonomía
- privacidad
- propiedad intelectual
- flujo de datos

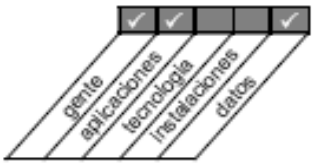


TABLA 3.2. Objetivos de alto nivel (planeación y organización P08)

Aquí el primero de los dominios, de suma importancia ya que nos fija cual será el proceder y los pasos a tomar para obtener un proceso que vaya acorde con las necesidades de la organización y las normativas.

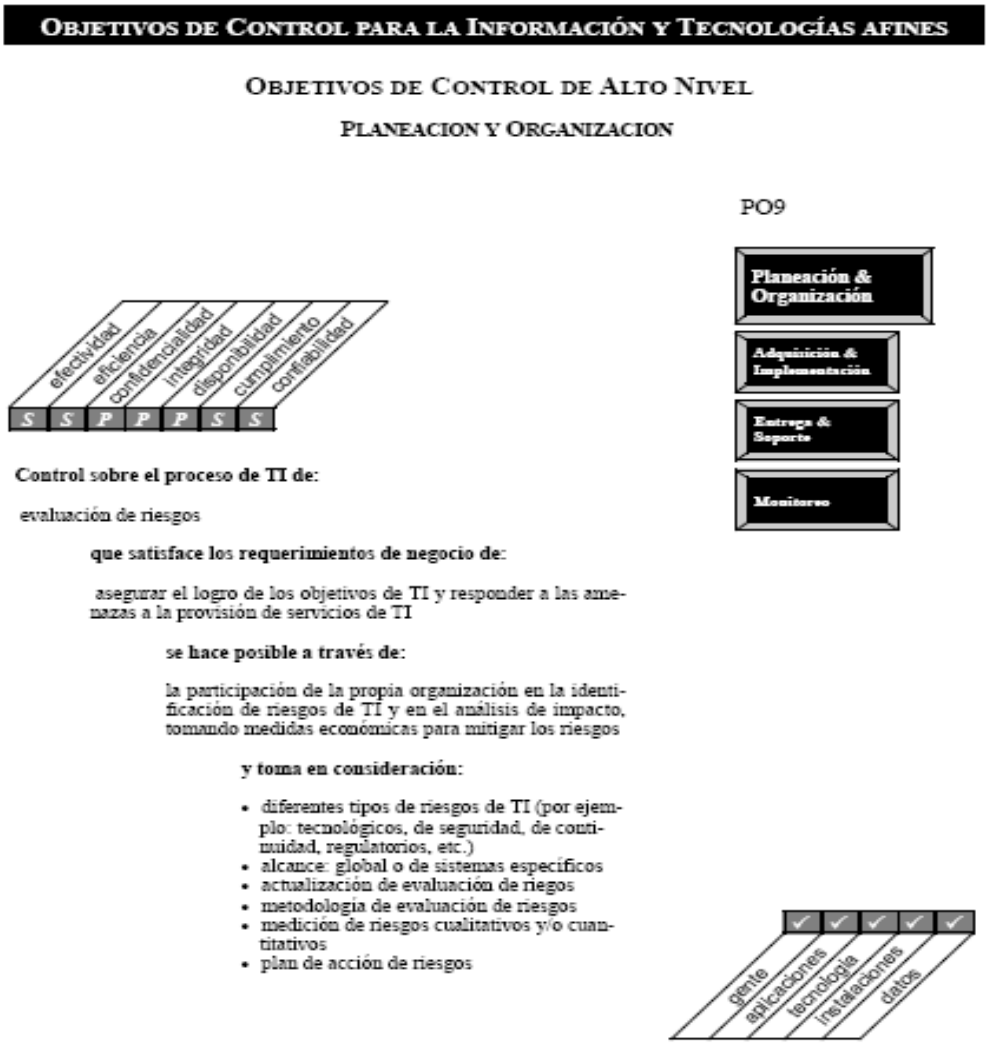


TABLA 3.3. Objetivos de alto nivel (planeación y organización P09)

Mediante este proceso buscamos obtener una plena identificación de todos los riesgos, o al menos los más relevantes, y conocer a su vez el impacto del mismo.

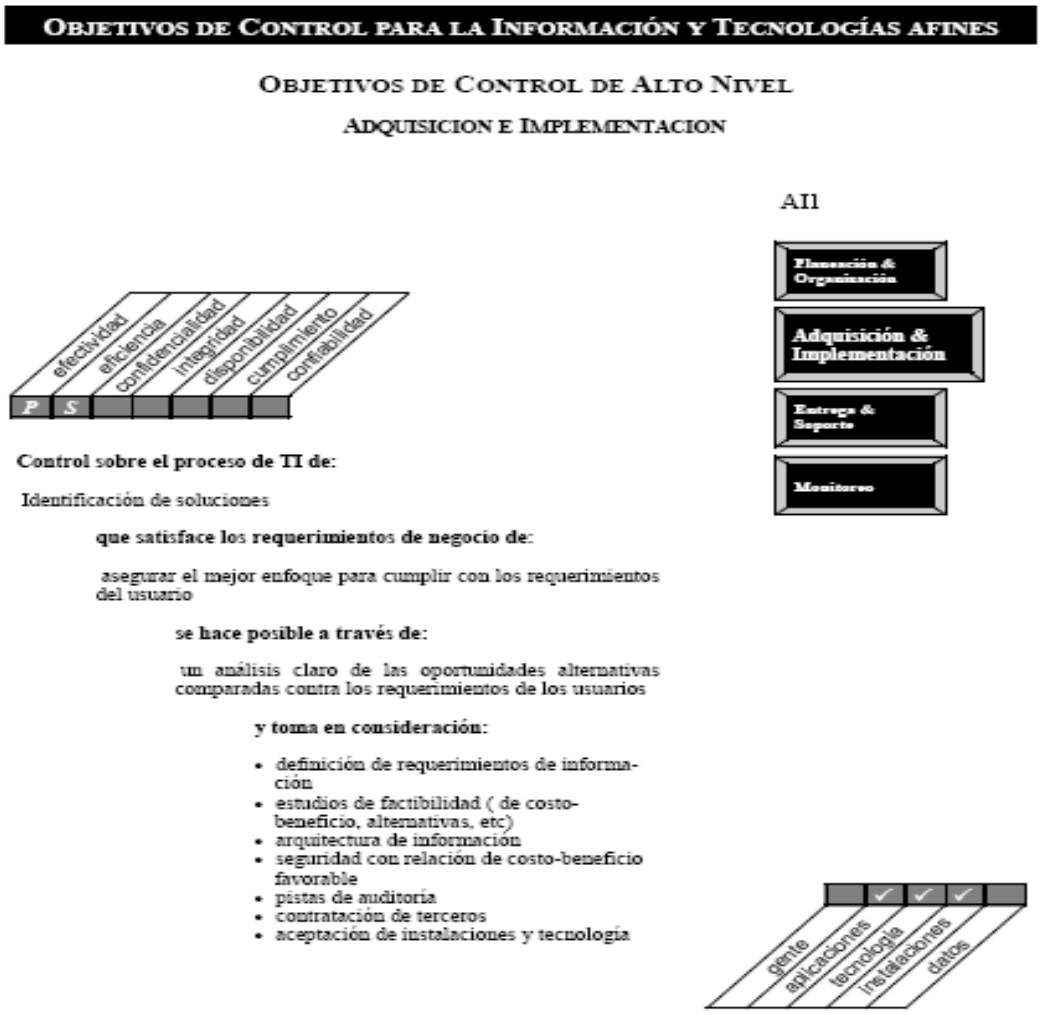


TABLA 3.4. Objetivos de alto nivel (adquisición e implementación A11)

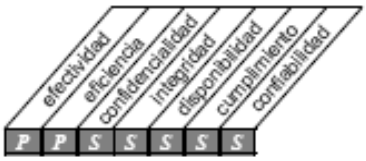
Este va ligado al anterior ya que tiene como objetivo el proponer la identificación de soluciones posibles, a los eventuales riesgos que puedan presentarse,

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS2



Control sobre el proceso de TI de:

administración de servicios prestados por terceros

que satisface los requerimientos de negocio de:

asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos

se hace posible a través de:

medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización

y toma en consideración:

- acuerdos de servicio con terceras partes
- acuerdos de confidencialidad
- requerimientos legales regulatorios
- monitoreo de la entrega de servicio

TABLA 3.5. Objetivos de alto nivel (Entrega

de servicios y soporte DS2) Este es definitivamente uno de los más importantes en lo que a nuestro tema respecta, ya que trata de la administración de servicios prestados por terceros con la única finalidad de regular la misma y obtener los resultados deseados.

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍAS AFINES

OBJETIVOS DE CONTROL DE ALTO NIVEL

ENTREGA DE SERVICIOS Y SOPORTE

DS5

TABLA 3.6. Objetivos de alto nivel (Entrega de servicios y soporte DS5)

Con este simplemente de busca el poder garantizar en el límite de lo posible la seguridad del uso y manipulación de los sistemas.

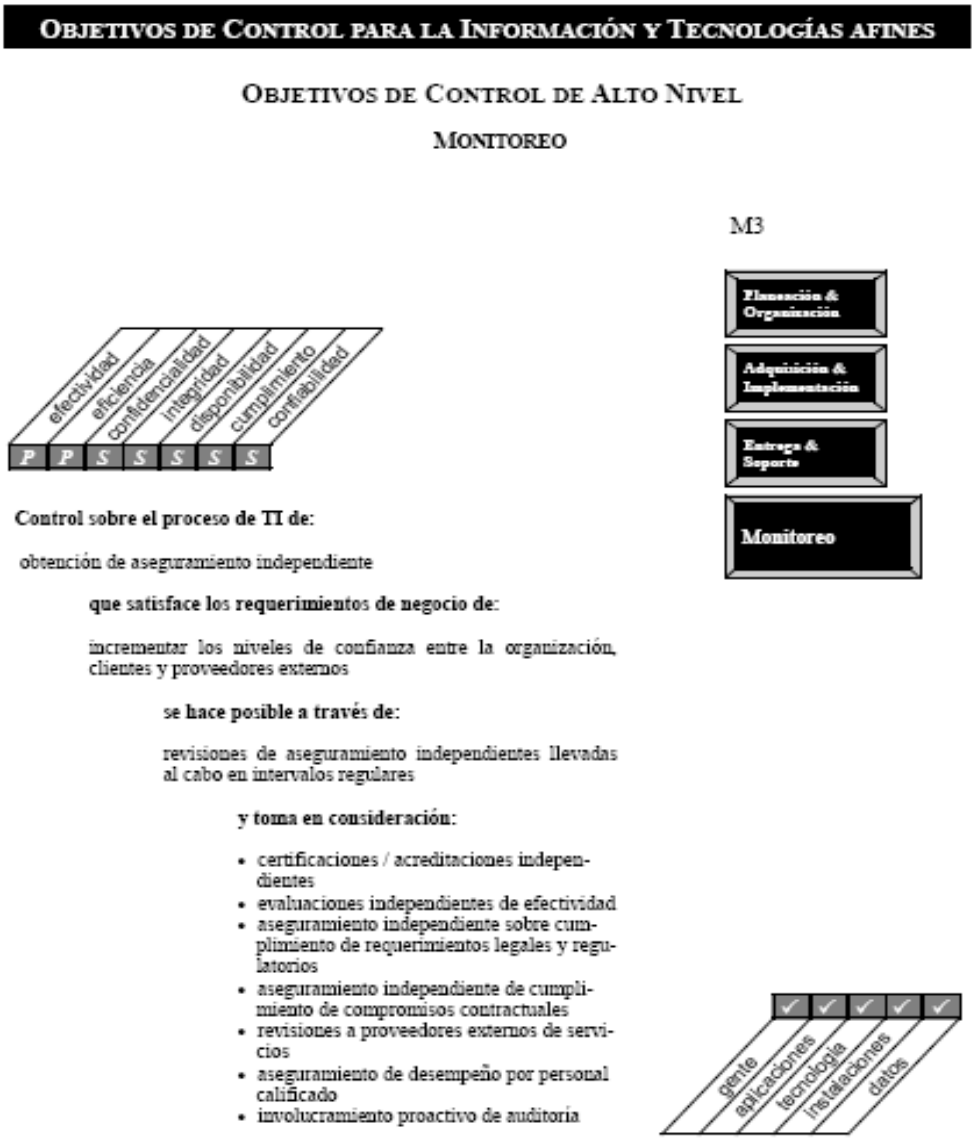


TABLA 3.7. Objetivos de alto nivel (Monitoreo M3)

Y finalmente el que busca establecer un alto grado de confianza entre organizaciones, clientes y proveedores externos para que funcionen entre sí con mayor eficiencia.

3.3.2 ESTÁNDAR ISO 17799

De igual forma la Norma ISO 17799 trata de protección y control de la información manejada sistemáticamente con el uso de medios informático, por esa razón veremos todos los dominios que a eso respectan, trascribiéndolos tal como van, y resaltando con negritas aquellas partes que mencionen el outsourcing, nuestro tema de interés.

Para establecer la seguridad de la información, dentro de una organización ISO dice que se deben considerar los siguientes aspectos:

a) política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa;

b) una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional;

c) apoyo y compromiso manifiestos por parte de la gerencia;

d) un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos;

e) comunicación eficaz de los temas de seguridad a todos los gerentes y empleados;

f) distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas;

g) instrucción y entrenamiento adecuados;

h) un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

ISO destaca bajo los siguientes numerales, aspectos importantes relacionados con el outsourcing:

4.2 SEGURIDAD FRENTE AL ACCESO POR PARTE
DE TERCEROS

4.2.1 Identificación de riesgos del acceso de terceras partes

4.2.2 Requerimientos de seguridad en contratos con terceros

4.3 TERCERIZACIÓN

4.3.1 Requerimientos de seguridad en contratos de tercerización

4.2 Seguridad frente al acceso por parte de terceros

Objetivo: Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

El acceso a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado.

Cuando existe una necesidad de la empresa para permitir dicho acceso, debe llevarse a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control. Los controles deben ser acordados y definidos en un contrato con la tercera parte.

El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso.

Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información.

4.2.1 Identificación de riesgos del acceso de terceras partes

4.2.1.1 Tipos de acceso

El tipo de acceso otorgado a terceras partes es de especial importancia. Por ejemplo, los riesgos de acceso a través de una conexión de red son diferentes de los riesgos relativos al acceso físico. Los tipos de acceso que deben tenerse en cuenta son:

a) acceso físico, por ej., a oficinas, salas de cómputos, armarios ;

b) acceso lógico, por ej. a las bases de datos y sistemas de información de la organización.

4.2.1.2 Razones para el acceso

Puede otorgarse acceso a terceros por diversas razones. Por ejemplo, existen terceros que proveen servicios a una organización y no están ubicados dentro de la misma pero se les puede otorgar acceso físico y lógico, tales como:

a) personal de soporte de hardware y software, quienes necesitan acceso a nivel de sistema o a funciones de las aplicaciones;

b) socios comerciales o socios con riesgos compartidos ("joint ventures"), quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos.

La información puede ponerse en riesgo si el acceso de terceros se produce en el marco de una inadecuada administración de la seguridad. Cuando existe una necesidad de negocios que involucran una conexión con un sitio externo, debe llevarse a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos. Ésta debe tener en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y la incidencia de este acceso en la seguridad de la información de la organización.

4.2.1.3 Contratistas in situ

Las terceras partes que sean ubicadas in situ por un período de tiempo determinado según contrato, también pueden originar debilidades en materia de seguridad. Entre los ejemplos de terceras partes in situ se enumeran los siguientes:

a) personal de mantenimiento y soporte de hardware y software;

b) limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados;

c) pasantías de estudiantes y otras designaciones contingentes de corto plazo;

d) consultores.

Es esencial determinar qué controles son necesarios para administrar el acceso de terceras partes a las instalaciones de procesamiento de información. En general, todos los requerimientos de seguridad que resultan de los controles internos o del acceso de terceros, deben estar reflejados en los contratos celebrados con los mismos (ver también 4.2.2). Por ejemplo, si existe una necesidad específica de confidencialidad de la información, podrían implementarse acuerdos de no-divulgación (ver 6.1.3).

No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o el acceso.

4.2.2 Requerimientos de seguridad en contratos con terceros

Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización. El contrato debe garantizar que no surjan malentendidos entre la organización y el proveedor.

Las organizaciones deben estar satisfechas con las garantías de su proveedor. Se deben considerar las siguientes cláusulas para su inclusión en el contrato:

a) la política general de seguridad de la información;

b) la protección de activos, con inclusión de:

1) procedimientos de protección de los activos de la organización, incluyendo información y software;

2) procedimientos para determinar si se han comprometido los activos, por ej., debido a pérdida o modificación de datos;

3) controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato, o en un momento convenido durante la vigencia del mismo;

4) integridad y disponibilidad;

5) restricciones a la copia y divulgación de información;

c) una descripción de cada servicio del que podrá disponerse;

d) el nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables;

e) disposición que contemple la transferencia de personal cuando corresponda;

f) las respectivas obligaciones de las partes con relación al acuerdo;

g) responsabilidades con respecto a asuntos legales, por ej., legislación referida a protección de datos, especialmente teniendo en cuenta diferentes sistemas legales nacionales si el contrato contempla la cooperación con organizaciones de otros países (ver también 12.1);

h) derechos de propiedad intelectual y asignación de derecho de propiedad intelectual (ver 12.1.2), y protección de trabajos realizados en colaboración (ver también 6.1.3) ;

i) acuerdos de control de accesos que contemplen:

1) los métodos de acceso permitidos, y el control y uso de identificadores únicos como IDs y contraseñas de usuarios;

2) un proceso de autorización de acceso y privilegios de usuarios;

3) un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso;

j) la definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos;

k) el derecho a monitorear, y revocar (impedir), la actividad del usuario;

l) el derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditorías;

m) el establecimiento de un proceso gradual para la resolución de problemas; también deben considerarse, si corresponde, disposiciones con relación a situaciones de contingencia;

n) responsabilidades relativas a la instalación y el mantenimiento de hardware y software;

o) una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos;

p) un proceso claro y detallado de administración de cambios;

q) los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos;

r) los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad;

s) los controles que garanticen la protección contra software malicioso (ver 8.3);

t) las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad;

u) la relación entre proveedores y subcontratistas.

4.3 Tercerización

Objetivo: Mantener la seguridad de la información cuando la responsabilidad por el procesamiento de la misma fue delegada a otra organización.

Los acuerdos de tercerización deben contemplar los riesgos, los controles de seguridad y los procedimientos para sistemas de información, redes y/o ambientes de PC (desk top environments) en el contrato entre las partes.

4.3.1 Requerimientos de seguridad en contratos de tercerización

Los requerimientos de seguridad de una organización que terceriza la administración y el control de todos sus sistemas de información, redes y/o ambientes de PC, o de parte de los mismos, deben ser contemplados en un contrato celebrado entre las partes.

Entre otros ítems, el contrato debe contemplar:

a) cómo se cumplirán los requisitos legales, por ej., la legislación sobre protección de datos;

b) qué disposiciones se implementarán para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, estarán al corriente de sus responsabilidades en materia de seguridad;

c) cómo se mantendrá y comprobará la integridad y confidencialidad de los .activos de negocio de la organización ;

d) qué controles físicos y lógicos se utilizarán para restringir y delimitar el acceso de los usuarios autorizados a la información sensible de la organización;

e) cómo se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres;

f) qué niveles de seguridad física se asignarán al equipamiento tercerizado;

g) el derecho a la auditoría.

Asimismo, se deben tener en cuenta las cláusulas enumeradas en el punto 4.2.2 como parte de este contrato. El mismo debe permitir la ampliación de los requerimientos y procedimientos de seguridad en un plan de administración de la seguridad a ser acordado entre las partes.

Si bien los contratos de tercerización pueden plantear algunas cuestiones complejas en materia de seguridad, los controles incluidos en este código de práctica pueden servir como punto de partida para acordar la estructura y el contenido del plan de gestión de la seguridad.

Otros numerales que indirectamente se vinculan con el outsourcing, contratos con terceros, son los siguientes:

6.1 Seguridad en la definición de puestos de trabajo y la asignación de recursos

Objetivo: Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.

Las responsabilidades en materia de seguridad deben ser explicitadas en la etapa de reclutamiento, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado.

Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados (ver 6.1.2), especialmente si se trata de tareas críticas. **Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no revelación).**

6.1.2 Selección y política de personal

Se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto. Éstos deben incluir los siguientes:

a) disponibilidad de certificados de buena conducta satisfactorios, por ej. Uno laboral y uno personal

b) una comprobación (de integridad y veracidad) del curriculum vitae del aspirante

c) constatación de las aptitudes académicas y profesionales alegadas

d) verificación de la identidad (pasaporte o documento similar).

Cuando un puesto, por asignación inicial o por promoción, involucra a una persona que tiene acceso a las instalaciones de procesamiento de información, y en particular si éstas manejan información sensible, por ej. Información financiera o altamente confidencial, la organización también debe llevar a cabo una verificación de crédito. En el caso del personal con posiciones de jerarquía considerable, esta verificación debe repetirse periódicamente.

Un proceso de selección similar debe llevarse a cabo con contratistas y personal temporario. Cuando éste es provisto a través de una agencia, el contrato celebrado con la misma debe especificar claramente las responsabilidades de la agencia por la selección y los procedimientos de notificación que ésta debe seguir si la selección no ha sido efectuada o si los resultados originan dudas o inquietudes.

La gerencia debe evaluar la supervisión requerida para personal nuevo e inexperto con autorización para acceder a sistemas sensibles. El trabajo de todo el personal debe estar sujeto a revisión periódica y a procedimientos de aprobación por parte de un miembro del personal con mayor jerarquía.

Los gerentes deben estar al corriente de que las circunstancias personales de sus empleados pueden afectar su trabajo. Los problemas personales o financieros, los cambios en su conducta o estilo de vida, las ausencias recurrentes y la evidencia de stress o depresión pueden conducir a fraudes, robos, errores u otras implicaciones que afecten la seguridad. Esta información debe manejarse de acuerdo con la legislación pertinente que rija en la jurisdicción del caso.

6.1.3 Acuerdos de confidencialidad

Los acuerdos de confidencialidad o no divulgación se utilizan para reseñar que la información es confidencial o secreta. Los empleados deben firmar habitualmente un acuerdo de esta índole como parte de sus términos y condiciones iníciales de empleo.

El personal ocasional y los usuarios externos aún no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el acuerdo mencionado antes de que se les otorgue acceso a las instalaciones de procesamiento de información.

Los acuerdos de confidencialidad deben ser revisados cuando se producen cambios en los términos y condiciones de empleo o del contrato, en particular

cuando el empleado está próximo a desvincularse de la organización o el plazo del contrato está por finalizar.

6.1.4 Términos y condiciones de empleo

Los términos y condiciones de empleo deben establecer la responsabilidad del empleado por la seguridad de la información. Cuando corresponda, estas responsabilidades deben continuar por un período definido una vez finalizada la relación laboral. Se deben especificar las acciones que se emprenderán si el empleado hace caso omiso de los requerimientos de seguridad.

Las responsabilidades y derechos legales del empleado, por ej. En relación con las leyes de derecho de propiedad intelectual o la legislación de protección de datos, deben ser clarificados e incluidos en los términos y condiciones de empleo.

También se debe incluir la responsabilidad por la clasificación y administración de los datos del empleador. Cuando corresponda, los términos y condiciones de empleo deben establecer que estas responsabilidades se extienden más allá de los límites de la sede de la organización y del horario normal de trabajo, por ej. Cuando el empleado desempeña tareas en su domicilio (ver también 7.2.5 y 9.8.1).

6.3 Respuesta a incidentes y anomalías en materia de seguridad

Objetivo: Minimizar el daño producido por incidentes y anomalías en materia de seguridad, y monitorear dichos incidentes y aprender de los mismos.

Los incidentes que afectan la seguridad deben ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible.

Se debe concientizar a todos los empleados y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la organización. Se debe requerir que los mismos comuniquen cualquier incidente advertido o supuesto al punto de contacto designado tan pronto como sea posible. La organización debe establecer un proceso disciplinario formal para ocuparse de los empleados que perpetren violaciones de la seguridad. Para lograr abordar debidamente los incidentes podría ser necesario recolectar evidencia tan pronto como sea posible una vez ocurrido el hecho (ver 12.1.7).

6.3.1 Comunicación de incidentes relativos a la seguridad

Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible.

Se debe establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta a incidentes, que establezca la acción que ha de emprenderse al recibir un informe sobre incidentes. Todos los empleados y **contratistas** deben estar al corriente del procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto como sea posible.

Deberán implementarse adecuados procesos de "feedback" para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados y resueltos los mismos.

Estos incidentes pueden ser utilizados durante la capacitación a fin de crear conciencia de seguridad en el usuario (ver 6.2) como ejemplos de lo que puede ocurrir, de cómo responder a dichos incidentes y de cómo evitarlos en el futuro (ver también 12.1.7).

6.3.2 Comunicación de debilidades en materia de seguridad

Los usuarios de servicios de información deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios.

Deberán comunicar estos asuntos a su gerencia, o directamente a su proveedor de servicios, tan pronto como sea posible. Se debe informar a los usuarios que ellos no deben, bajo ninguna circunstancia, intentar probar una supuesta debilidad. Esto se lleva a cabo para su propia protección, debido a que el intentar probar debilidades puede ser interpretado como un potencial mal manejo del sistema.

8.1.3 Procedimientos de manejo de incidentes

Se deben establecer responsabilidades y procedimientos de manejo de incidentes para garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad (ver también 6.3. l).

Se deben considerar los siguientes controles.

a) Se deben establecer procedimientos que contemplen todos los tipos probables de incidentes relativos a seguridad, incluyendo

1) fallas en los sistemas de información y pérdida del servicio;

2) negación del servicio;

3) errores ocasionados por datos comerciales incompletos o inexactos;

4) violaciones de la confidencialidad;

b) Además de los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible), los procedimientos también deben contemplar (ver también 6.3.4):

1) análisis e identificación de la causa del incidente;

2) planificación e implementación de soluciones para evitar la repetición del mismo, si resulta necesario;

3) recolección de pistas de auditoría y evidencia similar;

4) comunicación con las personas afectadas o involucradas con la recuperación, del incidente;

5) notificación de la acción a la autoridad pertinente;

c) Se deben recolectar (ver 12.1.7) y proteger pistas de auditoría y evidencia similar, según corresponda, para:

1) análisis de problemas internos:

2) uso como evidencia en relación con una probable violación de contrato, de requisito normativo, o en el caso de un proceso judicial civil o criminal, por ej. Por aplicación de legislación sobre protección de datos o fraude informático;

3) negociación de compensaciones por parte de los proveedores de software y de servicios;

d) Se deben implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema. Los procedimientos deben garantizar que:

1) sólo se otorga acceso a los sistemas y datos existentes al personal claramente identificado y autorizado **(ver también 4.2.2 en relación con el acceso de terceros);**

2) todas las acciones de emergencia emprendidas son documentadas en forma detallada

3) las acciones de emergencia se comunican a la gerencia y se revisan sistemáticamente;

4) la integridad de los controles y sistemas de la empresa se constata en un plazo mínimo.

8.1.6 Administración de instalaciones externas

El empleo de un contratista externo para la administración de las instalaciones de procesamiento de información puede introducir potenciales exposiciones al riesgo en materia de seguridad, como la posibilidad de compromiso, daño o pérdida de datos en la sede del contratista. Estos riesgos deben ser

identificados con anticipación, y deben acordarse controles adecuados con el contratista e incluirse en el contrato **(ver también 4.2.2 y 4.3 para orientación con respecto a contratos con terceros que contemplan el acceso a instalaciones de la organización y contratos de tercerización)**

Se deben abordar, entre otras, las siguientes cuestiones específicas:

a) identificar las aplicaciones sensibles o críticas que convienen retener en la organización;

b) obtener la aprobación de los propietarios de aplicaciones comerciales;

c) implicancias para la continuidad de los planes comerciales;

d) estándares de seguridad a especificar, y el proceso de medición del cumplimiento;

e) asignación de responsabilidades específicas y procedimientos para monitorear con eficacia todas las actividades de seguridad pertinentes

f) responsabilidades y procedimientos de comunicación y manejo de incidentes relativos a la seguridad (ver 8.1.3).

8.6.2 Eliminación de medios informáticos

Cuando ya no son requeridos, los medios informáticos deben eliminarse de manera segura. Si los mismos no se eliminan cuidadosamente, la información sensible puede filtrarse a personas ajenas a la organización. Se deben

establecer procedimientos formales para la eliminación segura de los medios informáticos, a fin de minimizar este riesgo. Deben considerarse los siguientes controles.

a) Los medios que contienen información sensible deben ser almacenados y eliminados de manera segura, por ej. Incinerándolos o haciéndolos trizas, o eliminando los datos y utilizando los medios en otra aplicación dentro de la organización.

b) El siguiente listado identifica ítems que podrían requerir una eliminación segura:

1) documentos en papel,

2) voces u otras grabaciones;

3) papel carbónico;

4) informes de salida,

5) cintas de impresora de un solo uso;

6) cintas magnéticas;

7) discos o casetes removibles;

8) medios de almacenamiento óptico **(todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor);**

9) listados de programas;

10) datos de prueba;

11) documentación del sistema,

c) Puede resultar más fácil disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

d) **Muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipos y medios. Se debe seleccionar cuidadosamente a un contratista apto con adecuados controles y experiencia.**

e) Cuando sea posible, se debe registrar la eliminación de los ítems sensibles, a fin de mantener una pista de auditoría.

Al acumular medios para su eliminación, se debe considerar el efecto de acumulación, que puede ocasionar que una gran cantidad de información no clasificada se torne más sensible que una pequeña cantidad de información clasificada.

8.7.3 Seguridad del comercio electrónico

El comercio electrónico puede comprender el uso de intercambio electrónico de datos (EDI), correo electrónico y transacciones en línea a través de redes

públicas como Internet. El comercio electrónico es vulnerable a diversas amenazas relativas a redes, que pueden tener como resultado actividades fraudulentas, **disputas contractuales** y divulgación o modificación de información. Se deben aplicar controles para proteger al comercio electrónico de dichas amenazas. Las consideraciones en materia de seguridad con respecto al comercio electrónico deben incluir las siguientes:

a) Autenticación. Qué nivel de confianza recíproca deben requerir el cliente y comerciante con respecto a la identidad alegada por cada uno de ellos?

b) Autorización. Quién está autorizado a fijar precios, emitir o firmar los documentos comerciales clave? Cómo conoce este punto el otro participante de la transacción.

c) Procesos de oferta y contratación. Cuáles son los requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos?

d) Información sobre fijación de precios. Qué nivel de confianza puede depositarse en la integridad del listado de precios publicado y en la confidencialidad de los acuerdos relativos a descuentos?

e) Transacciones de compra. Cómo es la confidencialidad e integridad de los datos suministrados con respecto a órdenes, pagos y direcciones de entrega, y confirmación de recepción?

c) Verificación. Qué grado de verificación es apropiado para constatar la información de pago suministrada por el cliente?

d) Cierre de la transacción. Cuál es forma de pago más adecuada para evitar fraudes?

e) Ordenes. Qué protección se requiere para mantener la confidencialidad e integridad de la información sobre órdenes de compra y para evitar la pérdida o duplicación de transacciones.

f) Responsabilidad. Quién asume el riesgo de eventuales transacciones fraudulenta

Gran parte de las consideraciones mencionadas pueden resolverse mediante la aplicación de las técnicas criptográficas enumeradas en el punto 10.3, tomando en cuenta el cumplimiento de los requisitos legales (ver 12.1, en particular los puntos 12.1.6 para legislación sobre criptografía).

Los acuerdos de comercio electrónico entre partes, deben ser respaldados por un acuerdo documentado que comprometa a las mismas a respetar los términos y condiciones acordados, incluyendo los detalles de autorización [ver el punto b), más arriba]. Pueden requerirse otros acuerdos con proveedores de servicios de información y de redes que aporten beneficios adicionales.

Los sistemas públicos de transacciones deben dar a conocer a sus clientes sus términos y condiciones comerciales.

Se debe tomar en cuenta la resistencia a ataques con que cuenta el "host" utilizado para el comercio electrónico, y las implicancias de seguridad de las interconexiones de red que se requieren para su implementación (ver 9.4.7).

8.7.5 Seguridad de los sistemas electrónicos de oficina

Se deben preparar e implementar políticas y lineamientos para controlar las actividades de la empresa y riesgos de seguridad relacionados con los sistemas electrónicos de oficina. Éstos propician la difusión y distribución más rápidas de la información de la empresa mediante una combinación de documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales y máquinas de fax.

Las consideraciones respecto de las implicancias de seguridad y comerciales al interconectar tales servicios, deben incluir:

a) vulnerabilidades de la información en los sistemas de oficina, por ej. La grabación de llamadas telefónicas o tele conferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo;

b) política y controles apropiados para administrar la distribución de información, por ej. El uso de boletines electrónicos corporativos (ver 9.1)

c) exclusión de categorías de información sensible de la empresa, si el sistema no brinda un adecuado nivel de protección (ver 5.2)

d) limitación del acceso a la información de agenda de personas determinadas, por ej. El personal que trabaja en proyectos sensibles;

e) la aptitud del sistema para dar soporte a las aplicaciones de la empresa, como la comunicación de órdenes o autorizaciones

f) categorías de personal, contratistas o socios a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo (ver 4.2);

g) restricción de determinadas instalaciones a específicas categorías de usuarios;

h) identificación de la posición o categoría de los usuarios, por ej. Empleados de la organización o contratistas en directorios a beneficio de otros usuarios;

i) retención y resguardo de la información almacenada en el sistema (ver 12.1.3 y 8.4.1)

j) requerimientos y disposiciones relativos a sistemas de soporte UPC de reposición de información perdida (ver 1 1.1).

9.2.1 Registración de usuarios

Debe existir un procedimiento formal de registración y des registración de usuarios para otorgar acceso a todos los sistemas y servicios de información multi-usuario. El acceso a servicios de información multi-usuario debe ser controlado a través de un proceso formal de registración de usuarios, el cual debe incluir los siguientes puntos:

a) utilizar IDs de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de IDs grupales solo debe ser permitido cuando son convenientes para el trabajo a desarrollar ;

b) verificar que el usuario tiene autorización del propietario del sistema para el uso del sistema o servicio de información. También puede resultar apropiada una aprobación adicional de derechos de acceso por parte de la gerencia;

c) verificar que el nivel de acceso otorgado es adecuado para el propósito del negocio y es coherente con la política de seguridad de la organización, por ej. que no compromete la separación de tareas (ver 8.1.4) ;

d) entregar a los usuarios un detalle escrito de sus derechos de acceso;

e) requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso ;

f) garantizar que los proveedores de servicios no otorgan acceso hasta que se hayan completado los procedimientos de autorización ;

g) mantener un registro formal de todas las personas registradas para utilizar el servicio ;

h) cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la organización ;

i) verificar periódicamente, y cancelar IDs y cuentas de usuarios redundantes;

j) garantizar que los IDs de usuario redundantes no se asignen a otros usuarios;

Se debe considerar la inclusión de cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados (ver también 6.1.4. y 6.3.5.)

9.3.2 Equipos desatendidos en áreas de usuarios

Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ej. Estaciones de trabajo o servidores de archivos, pueden requerir una protección específica contra accesos no autorizados, cuando se encuentran desatendidos durante un periodo extenso. Se debe concientizar a todos los usuarios y **contratistas**, acerca de los requerimientos y procedimientos de seguridad, para

la protección de equipos desatendidos, así como de sus responsabilidades por la implementación de dicha protección.

Se debe notificar a los usuarios que deben cumplir con los siguientes puntos:

a) concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ej. un preservador de pantallas protegido por contraseña ;

b) llevar a cabo el procedimiento de salida de los procesadores centrales cuando finaliza la sesión (no solo apagar la PC o terminal) ;

c) proteger las PCs o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ej. contraseña de acceso, cuando no se utilizan.

10.3.5.2 Normas, procedimientos y métodos

Un sistema de administración de claves debe estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) generar y obtener certificados de clave pública;

c) distribuir claves a los usuarios que corresponda, incluyendo como deben activarse las claves cuando se reciben;

d) almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados;

e) cambiar o actualizar claves incluyendo reglas sobre cuando y como deben cambiarse las claves;

f) ocuparse de las claves comprometidas;

g) revocar claves incluyendo como deben retirarse o desactivarse las mismas, por ej. cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deben archivarse);

h) recuperar claves perdidas o alteradas como parte de la administración de la continuidad del negocio, por ej. la recuperación de la información cifrada;

i) archivar claves, por ej. , para la información archivada o resguardada;

j) destruir claves;

k) registrar (logging) y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves deben tener fechas de entrada en vigencia y de fin de vigencia, definidas de manera que solo puedan ser utilizadas por un periodo limitado de tiempo. Este periodo debe definirse según el riesgo percibido y las circunstancias bajo las cuales se aplica el control criptográfico.

Podría resultar necesario considerar procedimientos para administrar requerimientos legales de acceso a claves criptográficas, por ej. Puede resultar necesario poner a disposición la información cifrada en una forma clara, como evidencia en un caso judicial.

Además de la administración segura de las claves secretas y privadas, también debe tenerse en cuenta la protección de las claves públicas. Existe la amenaza de que una persona falsifique una firma digital reemplazando la clave pública de un usuario con su propia clave. Este problema es abordado mediante el uso de un certificado de clave pública. Estos certificados deben generarse en una forma que vincule de manera única la información relativa al propietario del par de claves publica/privada con la clave pública. En consecuencia es importante que el proceso de administración que genera estos certificados sea confiable. Normalmente, este proceso es llevado a cabo por una autoridad de certificación, la cual debe residir en una organización reconocida, con adecuados controles y procedimientos implementados, para ofrecer el nivel de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicios o contratos con proveedores externos de servicios criptográficos, por ej. Con una autoridad de certificación, deben comprender los tópicos de responsabilidad legal, confiabilidad del servicio y tiempos de respuesta para la prestación de los mismos (ver 4.2.2).

10.5.5 Desarrollo externo de software

Cuando se terceriza el desarrollo de software, se deben considerar los siguientes puntos:

a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual (ver 12.1.2);

b) certificación de la calidad y precisión del trabajo llevado a cabo;

c) acuerdos de custodia en caso de quiebra de la tercera parte;

d) derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado;

e) requerimientos contractuales con respecto a la calidad del código;

f) realización de pruebas previas a la instalación para detectar códigos troyanos.

11.1.3 Elaboración e implementación de planes de continuidad de los negocios

Los planes deben ser desarrollados para mantener o restablecer las operaciones de los negocios en los plazos requeridos una vez ocurrida una interrupción o falla en los procesos críticos de los negocios. El proceso de

planificación de la continuidad de los negocios debe considerar los siguientes puntos:

a) identificación y acuerdo con respecto a todas la responsabilidades y procedimientos de emergencia;

b) **implementación de procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de la dependencias de negocios externos y a los contratos vigentes;**

c) documentación de los procedimientos y procesos acordados;

d) instrucción adecuada del personal en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis;

e) prueba y actualización de los planes.

El proceso de planificación debe concentrarse en los objetivos de negocio requeridos, por ej. Restablecimiento de los servicios a clientes en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia (“fallback”) en sitios alternativos de procesamiento de la información.

12.1 Cumplimiento de requisitos legales

Objetivo: Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o **contratos**; y de los requisitos de seguridad.

El diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual.

Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados. Los requisitos legales varían según el país y en relación con la información que se genera en un país y se transmite a otro (por ej. flujo de datos a través de fronteras).

12.1.1 Identificación de la legislación aplicable

Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información. Del mismo modo deben definirse y documentarse los controles específicos y las responsabilidades individuales para cumplir con dichos requisitos.

12.1.2 Derechos de propiedad intelectual (DPI)

12.1.2.1 Derecho de propiedad intelectual

Se deben implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, como derecho de propiedad intelectual, derechos de diseño o marcas registradas. La infracción de derechos de autor (derecho de propiedad intelectual) puede tener como resultado acciones legales que podrían derivar en demandas penales.

Los requisitos legales, normativos y contractuales pueden poner restricciones a la copia de material que constituya propiedad de una empresa. En particular, pueden requerir que sólo pueda utilizarse material desarrollado por la organización, o material autorizado o suministrado a la misma por la empresa que lo ha desarrollado.

12.1.2.2 Derecho de propiedad intelectual del software

Los productos de software que constituyan propiedad de una empresa se suministran normalmente bajo un acuerdo de licencia que limita el uso de los productos a máquinas específicas y puede limitar la copia a la creación de copias de resguardo solamente. Se deben considerar los siguientes controles:

a) publicación de una política de cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software;

b) emisión de estándares para los procedimientos de adquisición de productos de software;

c) mantenimiento de la concientización respecto de las políticas de adquisición y derecho de propiedad intelectual de software, y notificación de la determinación de tomar acciones disciplinarias contra el personal que incurra en el cumplimiento de las mismas;

d) mantenimiento adecuados de registros de activos;

e) mantenimiento de pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

f) implementación de controles para garantizar que no se exceda el número máximo permitido de usuarios;

g) comprobaciones para verificar que sólo se instalan productos con licencia y software autorizado;

h) emisión de una política para el mantenimiento de condiciones adecuadas con respecto a las licencias;

i) emisión de una política con respecto a la eliminación o transferencia de software a terceros;

j) utilización de herramientas de auditoría adecuadas;

cumplimiento de términos y condiciones con respecto a la obtención de software e información en redes públicas (ver también el punto 8.7.6).

3.3.3 ITIL (Information Technology Infrastructure Library)

Mediante esta metodología podremos conocer una manera de gestionar los servicios de tecnologías y recursos informáticos mediante estándares internacionales, lo incluimos por considerarlo de mucha importancia para entender y así poder exigir una correcta administración de nuestro IT al momento de aplicar un outsourcing informático.

ITIL son las siglas de una metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gubernativa de Comercio Británica (Office of Goverment Comerce). Las siglas de ITIL significan (Información Technology Infrastructure Library) o Librería de Infraestructura de Tecnologías de Información.

Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado. Estas mejores prácticas de dan en base a toda la experiencia adquirida con el tiempo en determinada actividad, y son soportadas bajo esquemas

organizacionales complejos, pero a su vez bien definidos, y que se apoyan en herramientas de evaluación e implementación.

3.3.3.1 OBJETIVO

ITIL como metodología propone el establecimiento de estándares que nos ayuden en el control, operación y administración de los recursos (ya sean propios o de los clientes). Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesiten (si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas), lo que nos lleva a una mejora continua.

Otra de las cosas que propone es que para cada actividad que se realice se debe de hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda la gente esté al tanto de los cambios y no se tome a nadie por sorpresa.

En la documentación se pone la fecha en la que se hace el cambio, una breve descripción de los cambios que se hicieron, quien fue la persona que hizo el cambio, así como quien es el que autorizo el cambio, para que así se lleve todo un seguimiento de lo que pasa en el entorno. Esto es más que nada como

método con el que se puede establecer cierto control en el sistema de cambios, y así siempre va a haber un responsable y se van a decir los procedimientos y cambios efectuados.

3.3.3.2 FORMA DE USO DE ITIL EN MANAGED SERVICES

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos:

1. Manejo de Incidentes
2. Manejo de problemas
3. Manejo de configuraciones
4. Manejo de cambios y
5. Manejo de entregas

3.3.3.3 PROCESO DE MANEJO DE INCIDENTES

Su objetivo primordial es restablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, esto se hace con la finalidad de que se minimicen

los efectos de la operación. Se dice que el proveedor de debe de encargar de que el cliente no debe percibir todas aquellas pequeñas o grandes fallas que llegue a presentar el sistema. A este concepto se le llama disponibilidad (que el usuario pueda tener acceso al servicio y que nunca se vea interrumpido).

Para este proceso se tiene un diagrama que en cada una de sus fases maneja cuatro pasos básicos que son: propiedad, monitoreo, manejo de secuencias y comunicación.

En el proceso de manejo de incidentes vemos que se da como primera etapa la detección del incidente (es cuando el sistema presenta alguna anomalía o falla, y que esto se puede traducir en un error en el sistema o que el usuario no puede hacer algo y recurre a pedir ayuda); ya que lo tenemos identificado se hace una clasificación del incidente (vemos si el error que se presenta es conocido o si nunca se ha presentado) y de la mano va el soporte inicial (es el punto en el que el cliente llega a la mesa de servicio a solicitar ayuda, porque no sabe o no puede hacer algo); en caso de que el incidente sea conocido se hace el procedimiento de solicitud de servicio (se ejecutan los pasos a seguir según el manual de procedimientos para poder llegar a la solución de una forma viable y eficiente); una vez que ya que se la dio una solución al incidente por medio del manual de procedimientos se recurre a la documentación y contabilización del incidente, para ver que tanta incidencia tiene este caso; finalmente se hace una

evaluación para ver si efectivamente se resolvió el incidente de forma satisfactoria y en supuesto de ser afirmativa se cierra el incidente y el otro supuesto seria que de la solución que se planteo no es lo suficientemente eficiente o acertada para que resuelva el problema y se recurre a hacer una investigación y un diagnostico de la situación para ver cómo es que se puede atacar el problema de frente y resolverlo; una vez que se tiene todo un contexto analizado se recurre a la ejecución de la propuesta de solución del incidente y se hace un estudio para ver si el incidente es recuperable o si es caso perdido (la mayoría de los casos son recuperables, peo cuando el nivel de daño es muy fuerte, se da el caso de que se dé por perdido); y finamente se cierra el incidente y esta solución se documenta en una base de datos a la que se le llama base del conocimiento o Knowledge Data Base (aquí vienen documentadas todas las soluciones, y se establecen los pasos a seguir para que se hagan de forma eficiente) para que al momento de volverse a presentar el incidente ya va a estar documentado y esto hace que sea más fácil, rápida y eficiente su resolución.

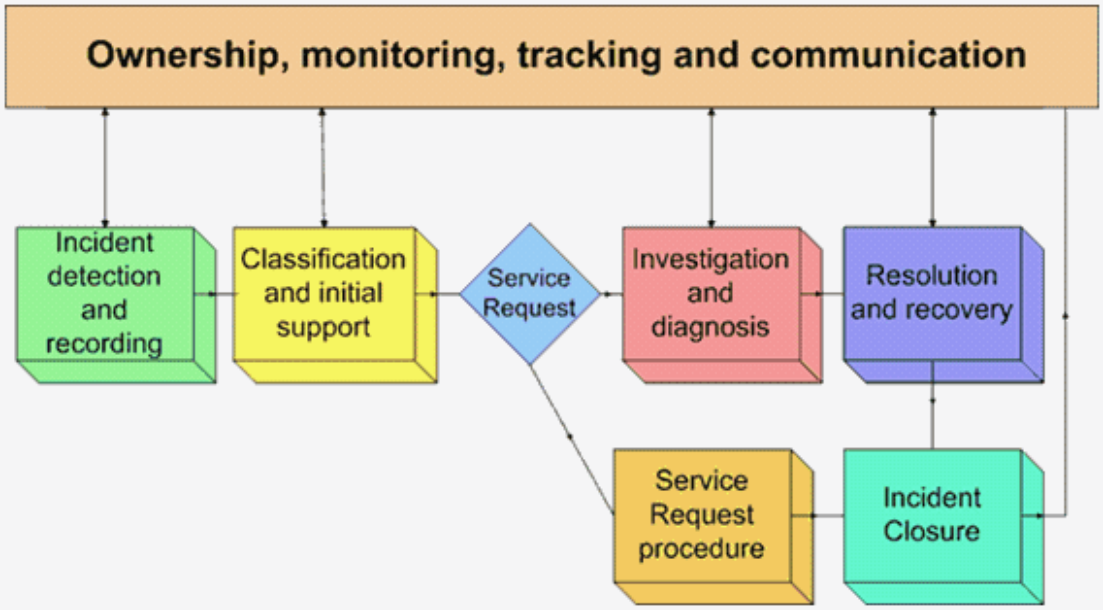


FIGURA 3.2. Propiedad, monitoreo, evaluación y comunicación

3.3.3.4 PROCESO DE MANEJO DE PROBLEMAS

El Objetivo de este proceso es prevenir y reducir al máximo los incidentes, y esto nos lleva a una reducción en el nivel de incidencia. Por otro lado nos ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

En este proceso lo que se busca es que se pueda tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo al problema.

El diagrama de este proceso es muy particular, ya que se maneja en dos fases: la primera está relacionada con lo que es el control del problema y la segunda es con el control del error.

En lo que respecta a la fase de control del problema: primero se tiene que identificar el problema en base a alguna sintomatología; ya que tenemos este antecedente, pasamos a la clasificación de los problemas (en este proceso al igual que en el proceso de manejo de incidentes tenemos que ver si es un problema conocido), en caso de ser conocido, se recurre al procedimiento de solicitud de servicio, donde se van a aplicar las soluciones de acuerdo a como están en el manual de procedimientos; y en caso de no ser conocido se tendría que hacer una fase de investigación para ver qué es lo que genera el problema y más tarde hacer un diagnostico; ya que tenemos un diagnóstico tenemos que hacer un RFC (Request For Change o Solicitud de Cambio),

Esta solicitud de cambio implica que se va a tener que implementar la solución y finalmente se va a hacer una evaluación para ver si se resolvió el problema de raíz. En caso de que si se funcione esta solución se pasa a la documentación.

Con lo que respecta a la segunda fase del modelo, el control del error se hace por medio de una identificación del error en general, posteriormente se hace una especie de registro, y este va a servir para clasificar el error; ya que se tiene una clasificación y se recurre a una evaluación de que tanto daño genero o puede

llegar a generar el error, esto con la finalidad de cuantificar los desperfectos que podría llegar a causar en caso de que el error prevalezca y no se solucione; posteriormente se hace la resolución o corrección del error (este puede deberse a varios aspectos: configuraciones, falta de seguridad, inconsistencia de datos, etc.); y este modelo tiene una fase muy difícil, que es determinar que problemas están asociados o como es que al momento de cambiar algo el sistema, se va a cambiar de forma uniforme y no se va a alterar, y que presente inconsistencias. Por ejemplo que es lo que pasaría si cambio algunos de los datos en la configuración del sistema, se tendría que afectar el sistema de manera uniforme para que siga en equilibrio y no esté cambiado en algunas partes y en otras que se quede como estaba antes.

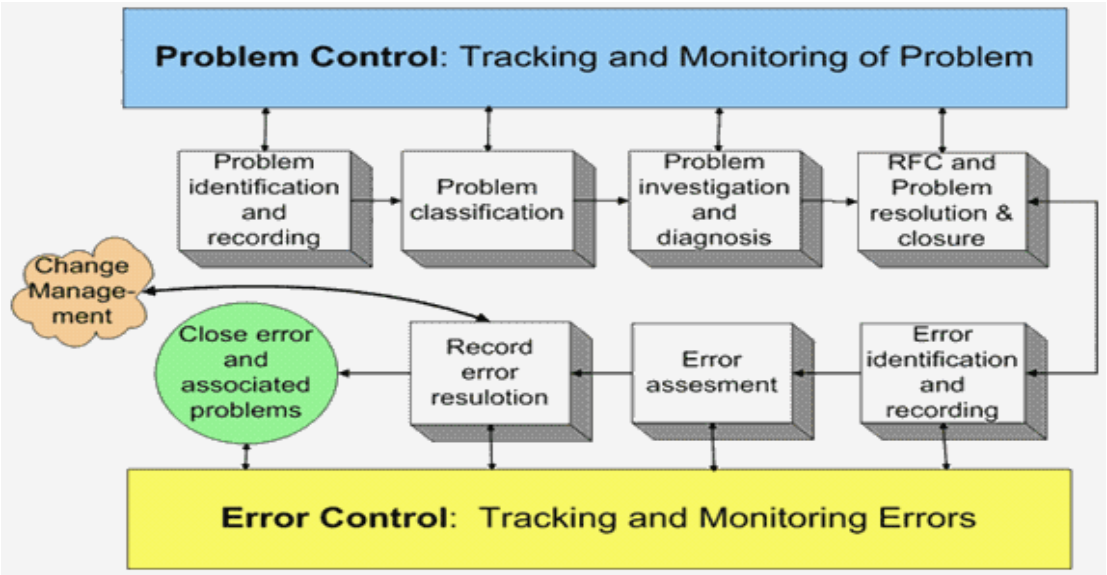


FIGURA 3.3. Problemas y errores de control

3.3.3.5 PROCESO DE MANEJO DE CONFIGURACIONES

Su objetivo es proveer con información real y actualizada de lo que se tiene configurado e instalado en cada sistema del cliente.

Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, entonces al cambiar una o varias de ellas se afecta el sistema en general, lo que hace que sea muy difícil de manipular. Aunque es lo más parecido a la realidad, porque nuestro entorno es dinámico y las decisiones de unos afectan a otros.

Por ejemplo en lo que respecta a la administración de cambios vemos que se relaciona directamente con la administración de incidentes y de problemas, lo que conlleva una planeación, identificación, control, seguimiento del status, verificación y auditoria de configuraciones, lo que hace que haya muchas variables.

En otro ejemplo la implementación de cambios implica que se tiene que hacer la liberación y distribución de nuevas versiones, esto de da por una fase de planeación, identificación, control, revisión del status, verificación y auditoria, y

puede depender de la administración de las capacidades, ya que si no se cuenta con el software o con el hardware esta fase no se podría llevar a cabo; y así se haría con todos los niveles hasta llegar al cierre del control de cambios.

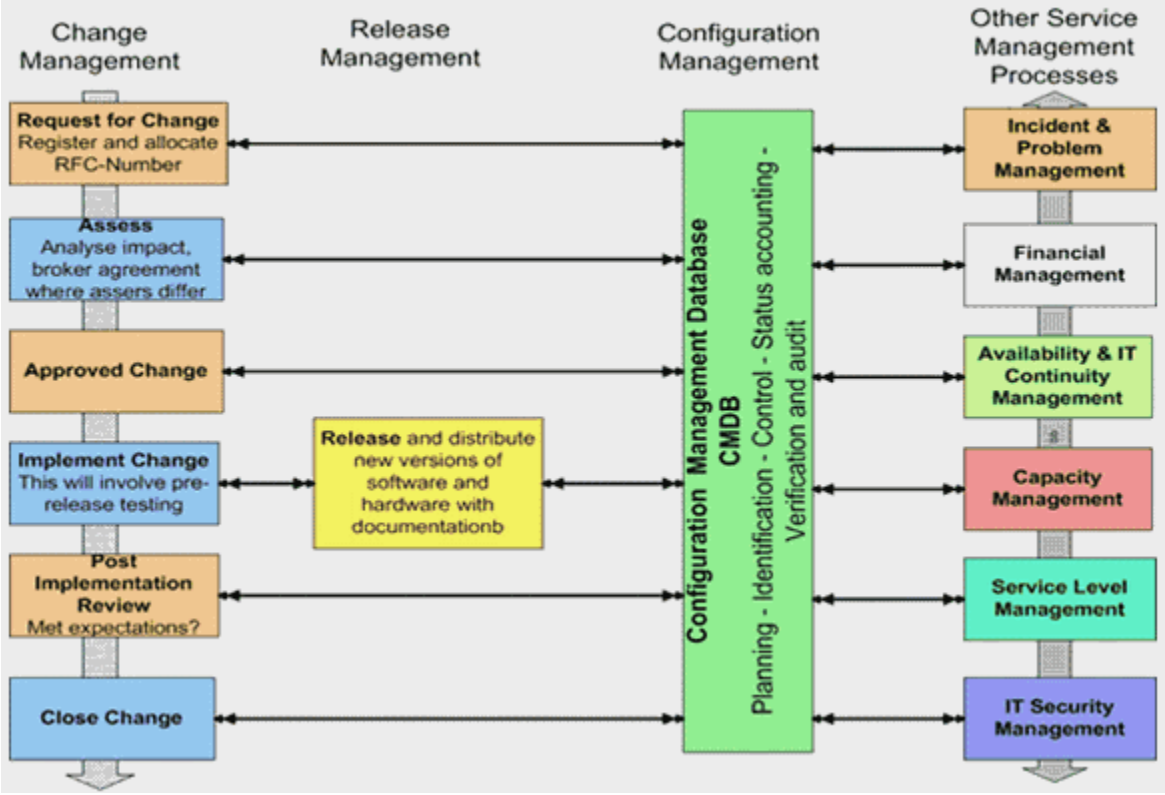


FIGURA 3.4. Niveles de control

3.3.3.6 PROCESO DE CONTROL DE CAMBIOS

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de los cambios.

Este diagrama al parecer es muy fácil de seguir, pero en realidad no lo es, ya que entre etapa y etapa se da una fase de monitoreo para ver que no se han sufrido desviaciones de los objetivos.

Primero vemos que tenemos un registro y clasificación del cambio que se tiene que hacer, se pasa a la fase de monitoreo y planeación, si el rendimiento es satisfactorio se da la aprobación del cambio, y en caso de que el rendimiento sea malo se pasa a la fase de reingeniería hasta que el proceso funcione adecuadamente, ya que se aprueban los cambio, se construyen prototipos o modelos en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las capacidades del sistema, ya que el proceso está probado se da la autorización e implementación; ya implementado se ve que no se hayan tenido desviaciones y se ajusta a las necesidades actuales que también se le considera como revisión post-implementación

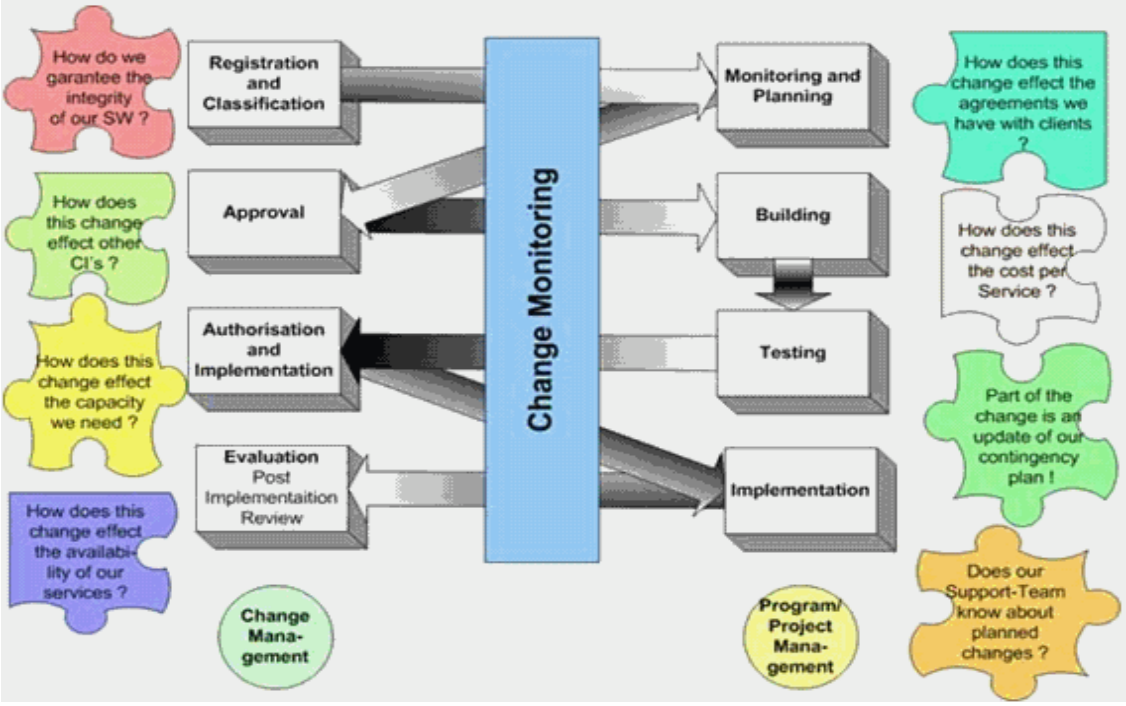


FIGURA 3.5. Monitoreo de cambios

3.3.3.7 PROCESO DE MANEJO DE ENTREGAS

Su objetivo es planear y controlar exitosamente la instalación de Software y Hardware bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real.

Este proceso tiene un diagrama que marca la transición que se da de acuerdo a los ambientes por los que se va dando la evolución del proyecto.

En lo que respecta al ambiente de desarrollo vemos que se tiene que hacer la liberación de las políticas, la liberación de la planeación, el diseño lógico de la infraestructura que se va a implementar y la adquisición de software y hardware

están entre los ambientes de desarrollo y de pruebas controladas; ya que se requiere que ambos hagan pruebas sobre ellos; en el ambiente de pruebas controladas vemos que se hace la construcción y liberación de las configuraciones (nivel lógico), se hacen las pruebas para establecer los acuerdos de aceptación; se da la aceptación total de versiones y de modelos, se arranca la planeación y finalmente las pruebas y comunicaciones; y en lo que es el ambiente real vemos que se da la distribución e instalación.

En la etapa del ambiente real es la que se ve de forma más concreta, ya que muchas veces no tenemos idea de todo lo que pasa hasta antes de la instalación.

En el proceso de entrega del servicio el usuario hace uno del servicio y no sabe que detrás del servicio que está recibiendo hay un sin fin de actividades y de decisiones que se tuvieron que tomar para que llegar a este punto.

Este proceso es en el que más cuidado debemos de poner, ya que en caso de haber fallas, el primero en detectarlas o en percibirlas es el usuario, y eso nos genera que el cliente este insatisfecho o molesto. Por lo general los usuarios no saben que para que puedan hacer uso de los servicios, se paso por una fase de planeación, monitoreo, análisis y por un sin fin de pruebas, con la intención de que en caso de que algo no funcione, se dé en la fase de pruebas controladas y

no en la fase de pruebas en ambiente real, donde el mayor afectado es el cliente.

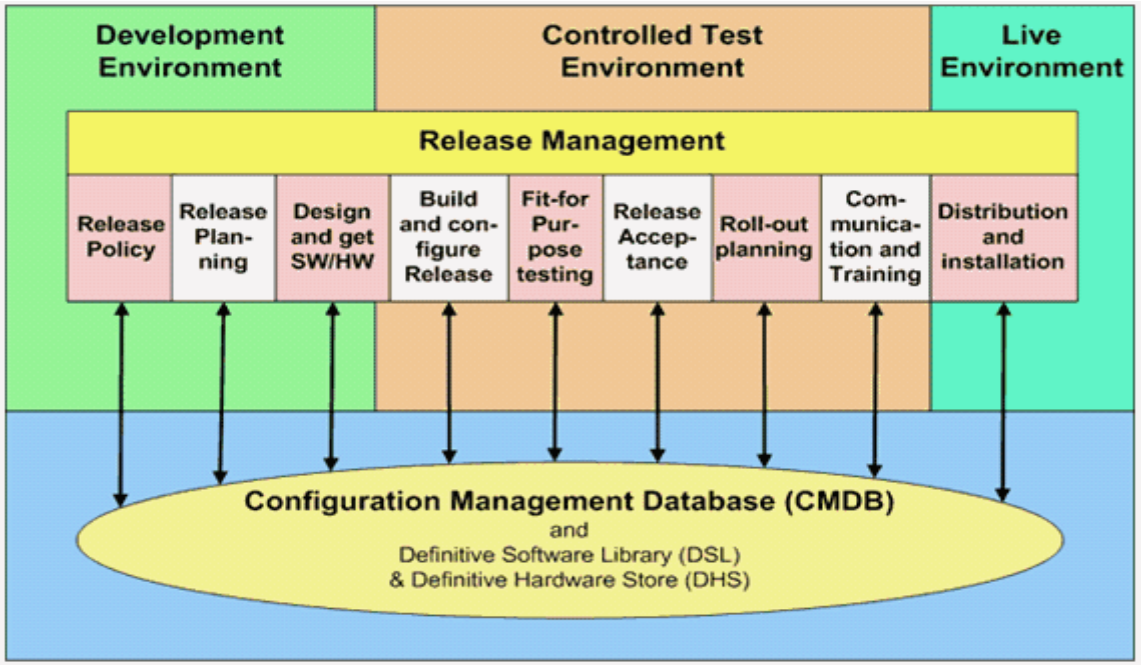


FIGURA 3.6. Entrega del servicio

CAPITULO 4

4.0 MANUAL DE CONTROLES DEL OUTSOURCING INFORMÁTICO

4.1 INFORMACIÓN PRELIMINAR

En el presente capitulo tendremos como finalidad desarrollar un manual de controles de outsourcing, específicamente el informático, que nos permita delinear de una manera general la forma correcta en la que se debe desarrollar un proceso de contratación externa, permitiendo así la satisfacción de todos los participantes del outsourcing, resguardando la integridad de la organización contratante mediante el uso de políticas y controles.

4.1.1 INTRODUCCIÓN

Como hemos podido analizar a lo largo del trabajo no hay duda que el outsourcing informático constituye una herramienta de suma importancia en el desarrollo de las actividades para las organizaciones que buscan cumplir sus objetivos, pero también comprobamos que dicho proceso debe ser realizado de

una manera concienzuda y con la supervisión del caso, la misma que permitirá una contratación externa correcta, en función de las necesidades y requerimientos de la empresa.

Sabemos también el papel fundamental que juega el auditor de sistemas en dichos contratos, ya que como tal debe verificar que la contratación con terceros se dé en conformidad con la ley y con las políticas de la empresa, las cuales deben estar claramente difundidas, en caso de no existir estas deberán ser creadas y recomendadas por el auditor.

El Auditor de Sistemas debe verificar también el buen uso de la información de la organización ya que será esta la que manipularán el personal externo, por tanto es necesario dejar en claro las responsabilidades de los mismos en caso de darse un mal uso de los datos y las bases de la organización.

Por ello considero necesario el desarrollo de un manual que:

1. Permita dar a conocer de forma general en el cómo proceder al momento de contratar los servicios de terceros en el área informática.
2. Indicar las medidas que debemos tomar para precautelar los intereses de la organización, los puntos fuertes y débiles de la misma, analizando riesgos del

uso de personal externo y por supuesto recomendando posibles soluciones y correctos controles para evitar que estos ocurran.

Este manual pretende entregar una herramienta clave para conseguir una adecuada administración del outsourcing informático, valiéndonos de todos los conceptos aquí analizados.

4.1.2 OBJETIVOS

Es una herramienta valiosa para cualquier tipo de organización que desee implementar el uso de servicios informáticos de terceros, por tanto podemos decir que los objetivos de este manual son:

1. Establecer controles básicos para la administración del outsourcing de procesos informáticos.
2. Implementar mecanismos de seguridad en una aplicación de outsourcing de procesos informáticos.
3. Establecer compromisos de seguridad por parte de los proveedores de servicios de procesos informáticos.
4. Fijar responsables en el uso de los sistemas de la organización en el outsourcing de procesos informáticos.

5. Ver que el contrato de outsourcing de procesos informáticos debe incluir todos los requerimientos.

6. Considerar todos los posibles riesgos generales, contractuales, de accesos, etc., que pueda contener un outsourcing de procesos informáticos.

7. Dar a conocer lineamientos para el correcto uso de los activos físicos y lógicos, dentro del proceso de tercerización, antes, durante y después del tiempo que esta tome.

8. Establecer controles para el correcto desarrollo del outsourcing de procesos informáticos basándose en la elaboración del contrato y el seguimiento de la correcta realización del mismo, preservando siempre los intereses de la organización contratante mediante el análisis de riesgos posibles y controles respectivos a dichos riesgos.

Con este manual el usuario podrá asegurarse que la contratación será realizada sobre la base de los requerimientos legales del caso además de los requerimientos y necesidades propios de la empresa ya que aquí analizamos no solo los riesgos y zonas vulnerables de la contratación externa, sino que además entregamos los controles respectivos para evitar que estos se susciten.

Para el correcto control y cumplimiento de lo que aquí expongo, este manual se ha realizado basado en herramientas de control como son las normas Iso 17799, las COBIT además de lo que pudiera aportar las ITIL, todas estas por ser las más apegadas al tema de servicios informáticos, enfocándonos por supuesto en los controles a las actividades de terceros para controlar las mismas de una forma correcta y eficiente.

Decimos que podemos obtener una contratación de servicios informáticos externos satisfactoria porque entre los controles más relevantes tenemos aquellos que tratan la delineación correcta del contrato previo a su realización, esta delineación deberá estar en concordancia con lo que sea desea obtener del proveedor externo sin dejar de lado todos los aspectos legales que lo norman, este manual recomienda que esto se haga de manera minuciosa y mediante el uso de una comité de expertos que lleve a cargo el tema.

También podremos ver que el manual no limita su campo de acción únicamente en la elaboración del contrato, sino que también plantea controles dentro del proceso y plan de funcionamiento que vaya a elaborar el proveedor externo asegurándonos de esta forma que el cumplimiento del contrato se dé a

cabalidad, previniendo y cuidando el activo más importante dentro de este proceso, la información.

4.1.3 ALCANCE

Este manual debe ser utilizado como herramienta de ayuda en la implementación de controles del outsourcing de procesos informáticos, ya sea que los servicios tercerizados sean para mantenimientos de sistemas, administración de bases de datos, y cualquier operación informática que la empresa requiera, es decir que su alcance está limitado únicamente a controles antes, durante y después de la prestación del servicio que se refieran a procesos informáticos contratados con terceros.

4.1.4 RESPONSABLES

Los responsables tanto de la correcta realización como del cumplimiento de este manual son:

- **Gerente general.-** En el establecimiento de políticas y controles, como los que se encuentran incluidos en este manual, que permitan el correcto funcionamiento de la organización en base a sus necesidades y requerimientos dentro del outsourcing de procesos informáticos.

- **Asesoría legal / representante del Dpto. Legal.-** En el establecimiento de aspectos legales contractuales básicos incluyendo elementos descritos en este manual en los controles de outsourcing informático.
- **Auditor de sistemas.-** En el asesoramiento de controles, como los que se encuentran incluidos en este manual, que permitan la correcta ejecución del outsourcing de procesos informáticos.
- **Personal de seguridad/Administradores de sistemas.**- En la implementación y aplicación de los controles previamente establecidos por el personal especializado en los contratos de outsourcing informático.

4.2 ANÁLISIS DE RIESGOS

Con los resultados proporcionados por el modelo de madurez a continuación se realizará el Análisis de Riesgo, tomando en cuenta todos los dominios con sus respectivos objetivos de control, luego se procede a identificar los riesgos para cada uno de ellos con la ayuda de los miembros de directivas de los altos niveles, y para finalizar se realiza su respectiva evaluación.

Con la ayuda de esta metodología, nosotros tendremos una visión mucho más clara sobre la situación actual en la que se encuentra la institución, y así podremos identificar los dominios de nivel de riesgo más severos.

Cabe indicar que estos riesgos que a continuación mencionaremos dentro de nuestro análisis fueron consideradas por el hecho de ser las de más alto nivel en base a datos obtenidos de una organización que por razones obvias no mencionaremos su nombre pero que para el desarrollo de este manual llamaremos XY, estos datos servirán únicamente para explicar la metodología que el manual propone.

También vale mencionar que estos fueron evaluados en base a cuestionarios de los cuales fueron participes, el Auditor Interno, personal de sistemas, y expertos del tema de dicha institución, esta documentación es de exclusividad de la empresa que hemos denominado XY.

A continuación podremos observar el cuadro del análisis de riesgo no sin antes aclarar que el nivel de riesgo está representado por los colores del semáforo, cuyos parámetros de evaluación son los siguientes:

Equivalencias nivel de riesgo según su ocurrencia (N.O.)		
8 a 10	Alto	
4 a 7	Medio	
1 a 3	Bajo	

Equivalencias nivel de riesgo según su impacto (N.I.)		
8 a 10	Alto	
4 a 7	Medio	
1 a 3	Bajo	

Niveles de ponderación Del riesgo (NOxNI)		
80 a 100	Muy alto	
60 a 79	Alto	
40 a 59	Medio	
20 a 39	Bajo	
1 a 19	Muy bajo	

Dominio	Riesgos	Evaluación del riesgo			
		Ponderación			Nivel de riesgo
		N.O.	N.I.	NOxNI	
4.4.1 Política de Seguridad	• Desorientación por desconocimiento • Desinformación que ponga en riesgo los sistemas	6 6	8 8	48 48	
4.4.2 Revisión y evaluación	• Utilización de procedimientos no autorizados • Desconocimiento por parte de altos mandos de procesos	7 6	6 6	42 36	
4.4.3 Seguridad Organizacional	• Sistemas e información importante vulnerables • Mala organización de procesos de seguridad • Roturas y no cumplimiento de controles establecidos • No restricción de accesos lógicos a sistemas e información importante	7 6 6 5	7 8 8 7	49 48 48 35	
4.4.4 Seguridad de acceso a terceros	• Ingresos no autorizados de personas ajenas a la institución • Perdidas o robos de equipos de la institución • Acciones dolosas, de terceras personas, en áreas no restringidas	5 3 3	8 8 7	40 24 21	
4.4.5 Abastecimiento externo	• No contar con abastecimiento adecuado • No verificar la procedencia y legalidad del proveedor abastecedor y sus productos	3 5	6 6	18 30	
4.4.6 Clasificación y control de activos	• Mal uso de los activos de la institución • No conocer responsables del buen o mal uso de los activos • Perdida de activos de la empresa o institución	6 5 3	7 7 7	42 35 21	
4.4.7 Clasificación de la información	• Desconocimiento de ubicación de la información • Perdida de información de importancia para la institución o empresa	6 5	6 8	36 40	

4.4.8 Seguridad personal	• Desconocimiento de casos anteriores de inseguridad personal	8	7	56	
	• Peligro de la integridad física del personal	5	7	35	
	• Uso inadecuado de activos que provoquen peligro	5	7	35	
4.4.9 Seguridad física y ambiental	• Pérdidas humanas en caso de siniestro	2	6	12	
	• Daños causados por personas ajenas a la institución	5	9	45	
4.4.10 Seguridad de equipos	• Robo o hurto de equipos de la institución	3	8	24	
	• Avería y desperfectos de equipos por falta de mantenimiento	7	7	49	
4.4.11 Comunicación y Operaciones	• Congestionamiento de procesos por no planeación	7	8	56	
	• Desconocimiento de uso de sistemas de información	7	8	56	
	• Desconocimiento de uso de sistemas de información realizada por terceros	8	7	56	
4.4.12 Control de Acceso	• Desorientación sobre permisos para accesos lógicos	6	8	48	
	• Ingreso a los sistemas e información importante de personas ajenas a la institución	5	8	40	
	• Perdida de información importante	5	9	45	
	• Mal uso y manipulación dolosa de la información por terceras personas y/o empleados	4	8	32	
4.4.13 Desarrollo y mantenimiento de sistemas	• Caída de los sistemas	8	7	56	
	• Paralización de los procesos de la empresa o institución	7	8	56	
	• Perdidas de bases con datos y registros importantes	5	8	40	
4.4.14 Conformidad	• Problemas legales con terceros o autoridades locales por desconocimientos	3	8	24	
	• Trampas legales dolosas, realizadas por terceros	4	7	28	
4.4.15 Controles de contrato	• Insatisfacción del servicio recibido	7	6	42	

	• Malentendidos sobre valores y plazos del servicio • Que el servicio prestado no sea el requerido	5 5	8 9	40 45	
4.4.16 Controles de Auditoria	• No tener bases reales para la realización de exámenes de auditoria • No tener reacción ante anomalías o novedades presentadas en el servicio • No poder estableces alternativas de solución ni acciones de contingencia ante novedades	7 8 8	7 8 8	49 64 64	
4.4.17 Seguimiento y control	• Perdida del objetivo del servicio en medio de su desarrollo • Incumplimiento por parte del proveedor del servicio en cuanto a lo establecido • Desconocimiento de calidad de servicios externos anteriores	7 7 7	7 8 8	49 56 56	
4.4.18 Estandarización	• Elaboración de controles sin su debido soporte ni guía • Uso de controles inservibles para la organización	7 6	6 7	42 42	

4.2.1 CLASIFICACIÓN DE LOS RIESGOS

Para un mejor análisis de los riesgos propuestos voy a clasificarlos en tres tipos que son:

- Riesgos sin intención
- Riesgos dolosos
- Riesgos de orden natural

4.2.1.1 RIESGOS SIN INTENCIÓN (RS)

Son aquellos de los cuales podemos decir que se dan por desconocimiento, negligencia, desorganización y cualquier motivo que no pueda ser enmarcado como doloso o premeditado.

Dentro de estos he considerado los siguientes:

- RS1: Desorientación por desconocimiento
- RS2: Desinformación que ponga en riesgo los sistemas
- RS3: Utilización de procedimientos no autorizados
- RS4: Desconocimiento por parte de altos mandos de procesos
- RS5: Sistemas e información importante vulnerables
- RS6: Mala organización de procesos de seguridad
- RS7: Roturas y no cumplimiento de controles establecidos
- RS8: No restricción de accesos lógicos a sistemas e información importante
- RS9: Ingresos no autorizados de personas ajenas a la institución

- RS10: No contar con abastecimiento adecuado
- RS11: No verificar la procedencia y legalidad del proveedor abastecedor y sus productos
- RS12: Mal uso de los activos de la institución
- RS13: No conocer responsables del buen o mal uso de los activos
- RS14: Desconocimiento de ubicación de la información
- RS15: Perdida de información de importancia para la institución o empresa
- RS16: Desconocimiento de casos anteriores de inseguridad personal
- RS17: Uso inadecuado de activos que provoquen peligro
- RS18: Avería y desperfectos de equipos por falta de mantenimiento
- RS19: Congestionamiento de procesos por no planeación
- RS20: Desconocimiento de uso de sistemas de información
- RS21: Desconocimiento de uso de sistemas de información realizada por terceros
- RS22:Desorientación sobre permisos para accesos lógicos
- RS23 Ingreso a los sistemas e información importante de personas ajenas a la institución
- RS234: Perdida de información importante
- RS25: Caída de los sistemas
- RS26: Paralización de los procesos de la empresa o institución
- RS27: Perdidas de bases con datos y registros importantes

- RS28: Problemas legales con terceros o autoridades locales por desconocimientos
- RS29: Insatisfacción del servicio recibido
- RS30: Malentendidos sobre valores y plazos del servicio
- RS31: Que el servicio prestado no sea el requerido
- RS32: No tener bases reales para la realización de exámenes de auditoria
- RS33: No tener reacción ante anomalías o novedades presentadas en el servicio
- RS34: No poder estableces alternativas de solución ni acciones de contingencia ante novedades
- RS35: Perdida del objetivo del servicio en medio de su desarrollo
- RS36: Incumplimiento por parte del proveedor del servicio en cuanto a lo establecido
- RS37: Desconocimiento de calidad de servicios externos anteriores
- RS38: Elaboración de controles sin su debido soporte ni guía
- RS39: Uso de controles inservibles para la organización

4.2.1.2 RIESGOS DOLOSOS (RD)

Estos son aquellos que se producen de manera intencional, con previo deseo de perjudicar a la institución como tal o alguna persona de la misma, también con la finalidad de beneficio propio del doloso.

Estos generalmente son penados por la ley cuando se ponen al descubierto, aquí nombraremos los que considere como tales, son:

- RD1: Perdidas o robos de equipos de la institución
- RD2: Acciones dolosas, de terceras personas, en áreas no restringidas
- RD3: Perdida de activos de la empresa o institución
- RD4: Daños causados por personas ajenas a la institución
- RD5: Robo o hurto de equipos de la institución
- RD6: Mal uso y manipulación dolosa de la información por terceras personas y/o empleados
- RD7: Trampas legales dolosas, realizadas por terceros

4.2.1.3 RIESGOS DE ORDEN NATURAL (RN)

En este grupo vamos a encontrar como su nombre lo indica riesgos que existen por motivos naturales, tales como los que pueden causar un terremoto, maremoto, tormentas eléctricas, huracanes, en fin todos los considerados desastres naturales.

Estos riesgos pueden ser considerados como riesgos de alto impacto, pero no gozan de alta ponderación por el hecho de que su nivel de ocurrencia que aunque es incierta pues sabemos también que es baja, aquí los que hemos considerado para este proyecto.

- RN1: Peligro de la integridad física del personal
- RN2: Pérdidas humanas en caso de siniestro

4.3 CUADRO DE RIESGOS SEGÚN SU CLASIFICACION

A continuación presento los gráficos de los cuadros de los riesgos según su clasificación, estos nos ayudaran a tener una idea mas clara de cuales son los de más alto riesgo y de esta manera poder tener en cuenta dichos riesgos a la hora de contratar servicios de outsourcing informático.

Para entender la simbología de los colores recordaremos el cuadro de los colores en base a la ponderación.

Niveles de ponderación Del riesgo (NOxNI)		
80 a 100	Muy alto	
60 a 79	Alto	
40 a 59	Medio	
20 a 39	Bajo	
1 a 19	Muy bajo	

- **RIESGOS SIN INTENCIÓN (RS)**

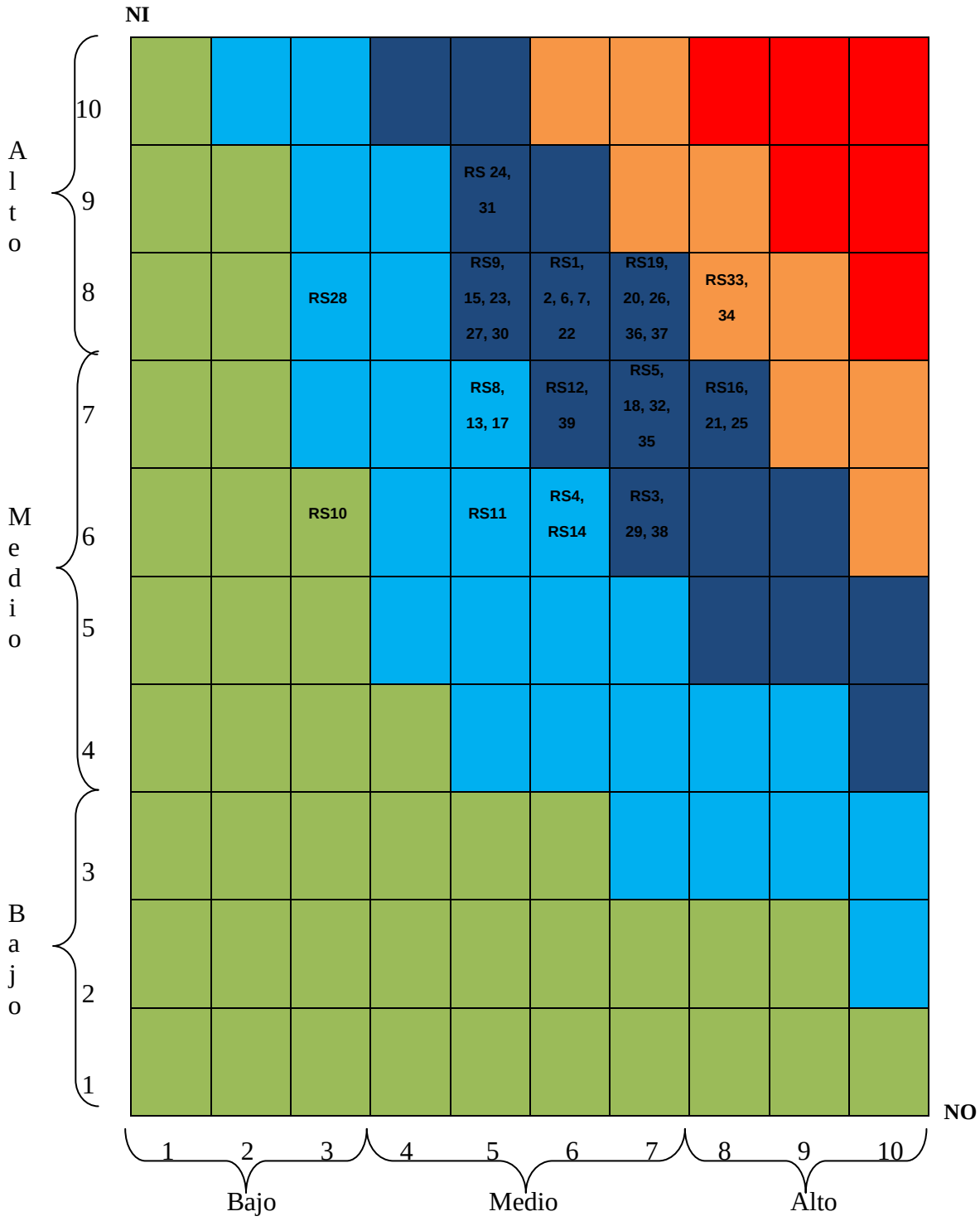


TABLA 4.1 Riesgos sin intención

- **RIESGOS DOLOSOS (RD)**

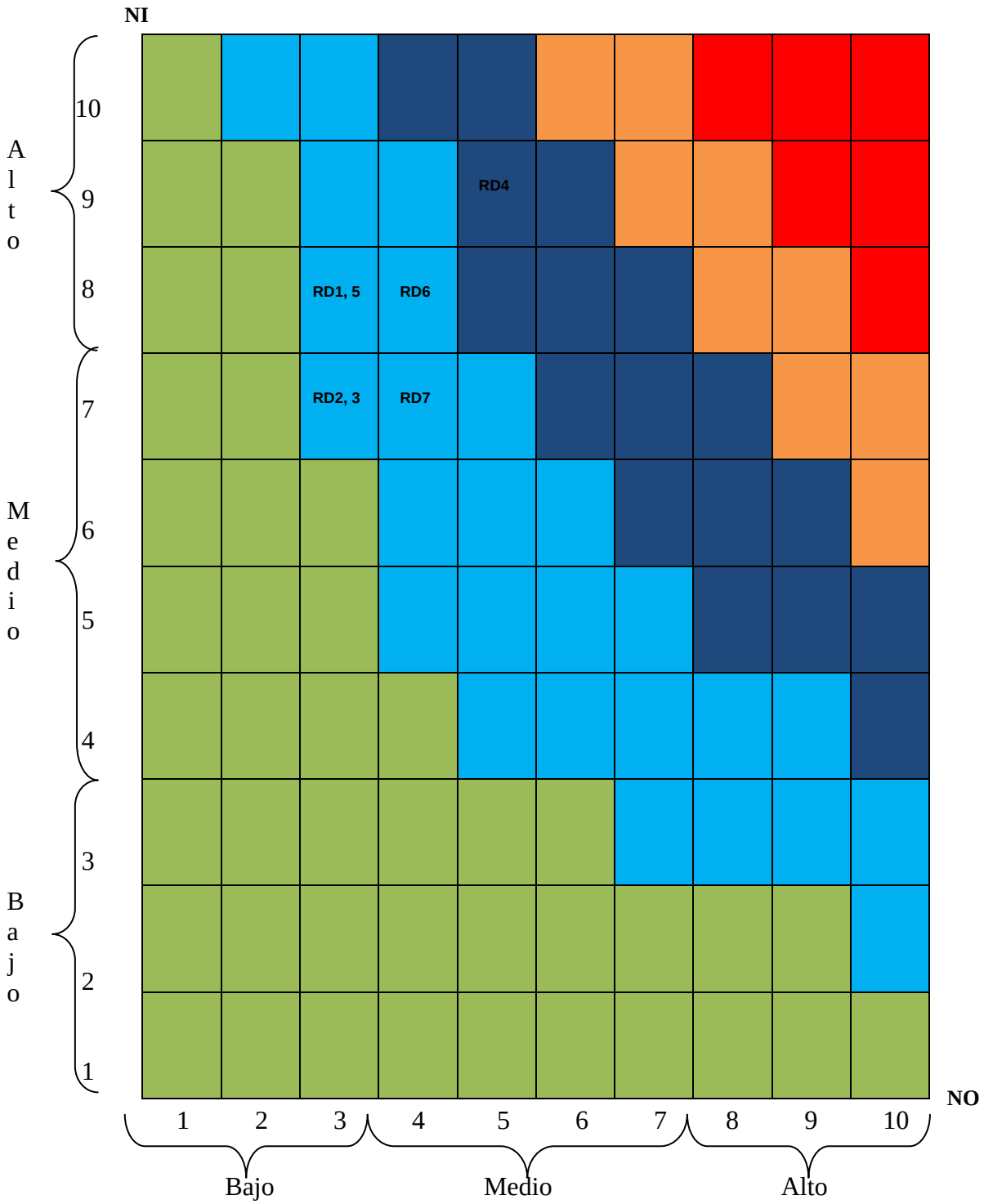


TABLA 4.2 Riesgos dolosos

- **RIESGOS DE ORDEN NATURAL (RN)**

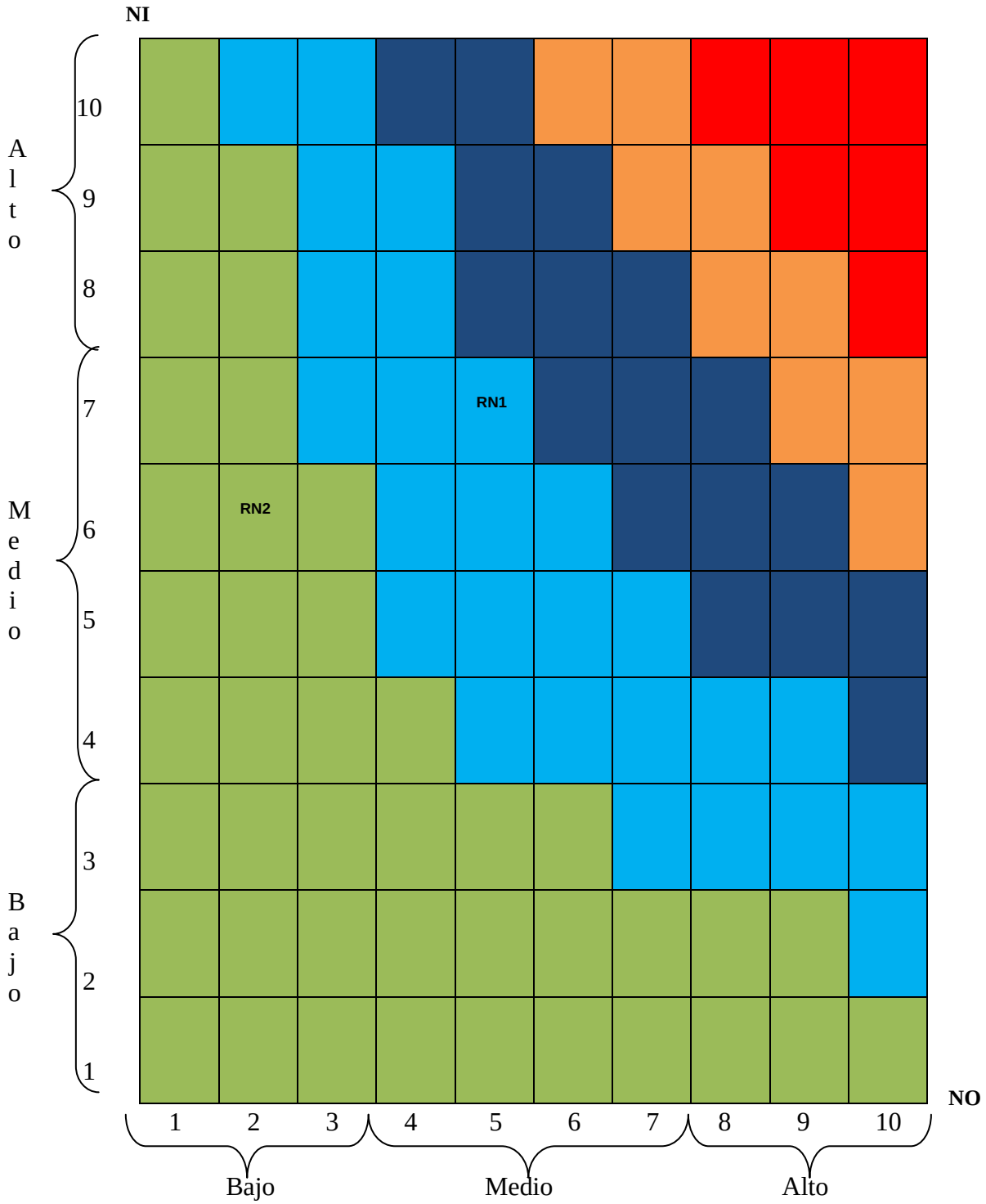


TABLA 4.3 Riesgos de orden natural

Luego de analizar estos cuadros podemos descubrir que los riegos sin intención son aquellos que pueden representar mayor riesgo mientras que los de orden natural contienen a los de mas bajo riesgo, esto por su poco nivel de ocurrencia.

4.4 POLÍTICAS DE CONTROL

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.1 Política de Seguridad	**Objetivo de Control:**	4.4.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
	Control:	Deben existir políticas de seguridad relacionadas con el tratamiento con terceros, las cuales deben estar establecidas, aprobadas por la máxima autoridad y difundidas a todos los miembros de la organización
	Procedimiento a cumplir:	Establecer las políticas Aprobación de las políticas por la máxima autoridad Difusión de las políticas a todo el personal dentro de la Organización.
	Evidencias:	Política de seguridad con políticas definidas acerca del tratamiento con terceros. Publicación, comunicados sobre la política a los miembros de la Organización. Política publicada en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.1 Política de Seguridad	**Objetivo de Control:**	4.4.1.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN TRATADA POR TERCEROS
	Control:	Las políticas en cuanto a tratamiento con terceros deben ser parte del documento de Política de Seguridad de la Organización
	Procedimiento	Establecer las políticas

	a cumplir:	Incluir dentro de las políticas de información, el tratamiento a terceros Difusión de las políticas a todo el personal externo que vaya a participar en el outsourcing.
	Evidencias:	Política de seguridad con políticas definidas acerca del tratamiento con terceros. Publicación, comunicados sobre la política a los miembros externos o terceras personas Política impresa y distribuida a los interesados.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.2 Revisión y evaluación.	**Objetivo de Control:**	4.4.2.1 REVISIÓN Y EVALUACIÓN DE LA POLÍTICA DE SEGURIDAD
	Control:	Se debe establecer un responsable encargado del mantenimiento y de la revisión de las políticas de seguridad de tratamiento a terceros.
	Procedimiento a cumplir:	Establecer y asignar un responsable del mantenimiento de las políticas. Fijar revisiones periódicas a las políticas de seguridad para terceros.
	Evidencias:	Documento impreso de la asignación del responsable.

		Autorizaciones y firmas de los altos directivos aprobando la designación. Consentimiento por escrito del responsable aceptando su designación.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.2 Revisión y evaluación	**Objetivo de Control:**	4.4.2.2 REVISIONES PERIÓDICAS DE LAS POLÍTICAS DE SEGURIDAD
	Control:	El responsable designado para el mantenimiento de las políticas de seguridad deberá establecer revisiones periódicas de la misma.
	Procedimiento a cumplir:	Establecer cronograma de revisiones junto con los puntos a revisar Aprobación de cronograma por altos mandos Cumplimiento a cabalidad del cronograma establecido
	Evidencias:	Sello o firma de verificación para constancia de revisión efectuada Informe en físico de resultados obtenidos en base a la revisión

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.3 Seguridad Organizacional	**Objetivo de Control:**	4.4.3.1 MANEJAR LA SEGURIDAD DE LA ORGANIZACIÓN
	Control:	Se deberán establecer programas de concienciación y concientizacion de seguridad para el tratamiento de terceros a todos los miembros de la Organización
	Procedimiento a cumplir:	Establecer los programas de concienciacion y respectivas metodologías Aprobación de programas de concienciacion de seguridad Implementar dichos programas a todo el personal de la organización, incluidos terceros y altos mandos,
	Evidencias:	Registro de programas de concienciacion realizados dentro de la organización Cuestionarios de utilidad del programa, desarrollado por participantes Publicación de resultados obtenidos del programa

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.3 Seguridad Organizacional	**Objetivo de Control:**	4.4.3.2 CORRECTA IMPLEMENTACIÓN DE SEGURIDAD EN LA ORGANIZACIÓN
	Control:	Se deberá establecer un foro gerencial de seguridad de información que controle la implementación de la seguridad, realizada por terceros, de la información dentro de la organización
	Procedimiento a cumplir:	Iniciar proceso de elección de participantes del foro gerencial

		Elección de integrantes del foro en base a conocimientos y experiencia Poner en acción el foro paralelamente con el servicio externo
	Evidencias:	Archivos de todo el proceso de elección de integrantes del foro. Pruebas y evaluaciones realizadas a postulantes del mismo Nombramiento escrito de los integrantes junto con sus funciones.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.3 Seguridad Organizacional	**Objetivo de Control:**	4.4.3.3 COORDINAR Y CONTROLAR SEGURIDAD DE LA ORGANIZACIÓN
	Control:	El foro gerencial para la seguridad de la información deberá coordinar las actividades de control con especialistas cuando el caso lo amerite.
	Procedimiento a cumplir:	Establecer que puntos pueden o deben ser estudiadas por especialistas. Aprobación de altos mandos de la aplicación de especialistas Elección de especialistas a participar dentro del proceso de consulta
	Evidencias:	Informe que determina cuales son los puntos que necesitan la intervención adicional de especialistas y el por que

		Designación, en forma escrita, de especialistas a participar Informe del resultado obtenido de la coordinación con especialistas

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.3 Seguridad Organizacional	**Objetivo de Control:**	4.4.3.4 MANTENER UN CONTROL RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN
	Control:	Se deberá establecer responsable de la seguridad de información conforme a la política de seguridad de tratamiento a terceros.
	Procedimiento a cumplir:	Establecer las políticas y procedimientos de seguridad de la información. Aprobación de las políticas y procedimientos por la máxima autoridad Difusión de las políticas y procedimientos a todo el personal dentro de la Organización.
	Evidencias:	Política y procedimientos de seguridad con políticas definidas acerca del tratamiento con terceros. Publicación, comunicados sobre la política a los miembros de la Organización. Política publicada en la intranet. Registros de seguridad implementada.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL

4.4.3 Seguridad Organizacional	**Objetivo de Control:**	4.4.3.5 CONTROLAR EL ACCESO LÓGICO A LA INFORMACIÓN DE LA ORGANIZACIÓN
	Control:	Se deberán definir autorizaciones a todo el personal externo para los medios de procesamiento de la información y darlas a conocer de manera clara a los interesados.
	Procedimiento a cumplir:	Creación un manual que identifique función junto con autorización de acceso Aprobación de manual por la máxima autoridad Difusión de manual a todo el personal interno y externo de la Organización.
	Evidencias:	El manual de funciones-autorizaciones en físico. Publicación, comunicados sobre el manual a los miembros internos y externos de la Organización. Manual publicado en la intranet. Registro de seguridad implementada.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.4 Seguridad de acceso a terceros	**Objetivo de Control:**	4.4.4.1 CONTROLAR RIESGOS DEL ACCESO DE TERCERAS PERSONAS
	Control:	Se debe establecer y definir los posibles riesgos que existen en relación al acceso a terceras personas, determinándolos independientemente entre físicos y lógicos.
	Procedimiento a cumplir:	Establecer los posibles riesgos que contenga el acceso a terceros

		Clasificarlos entre físicos y lógicos Informar sobre estos riesgos a los altos mandos.
	Evidencias:	Informe entregado a altos mandos identificando los posibles riesgos Cuadro clasificatorio de los riesgos físicos y lógicos Registros de accesos.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.4 Seguridad de acceso a terceros	**Objetivo de Control:**	4.4.4.2 CONTROLAR EL ACCESO A TERCERAS PERSONAS SEGÚN FUNCIÓN
	Control:	Se debe definir claramente los tipos de accesos a personas que se encuentran en la organización como contratistas in-situ o como terceros
	Procedimiento a cumplir:	Definición de los tipos accesos, según funciones, a personal in-situ o terceros Aprobación por jefes de áreas y altos mandos de accesos Difusión de los tipos de acceso a todo el personal interno y externo de la Organización.
	Evidencias:	Informe de los tipos de accesos según funciones Publicación, comunicados sobre los tipos de acceso a los miembros in-situ y terceros de la Organización.

		Accesos publicados en la intranet. Registros de accesos.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.4 Seguridad de acceso a terceros	**Objetivo de Control:**	4.4.4.3 ASEGURAR EL CORRECTO ACCESO A TERCERAS PERSONAS
	Control:	Deben existir requerimientos de seguridad establecidos dentro de los contratos con terceras personas.
	Procedimiento a cumplir:	Establecer requerimientos de seguridad para considerarlos dentro de los contratos con terceros Aprobación de los requerimientos por los altos mandos altos de la organización Incluir en los contratos con terceros requerimientos de seguridad
	Evidencias:	Informe de los requerimientos de seguridad a incluirse en los contratos con terceros Contratos realizados con los requerimientos de seguridad incluidos

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL

4.4.5 Abastecimiento externo	**Objetivo de Control:**	4.4.5.1 CONTROLAR CONTRATOS DE ABASTECIMIENTO EXTERNO
	Control:	Deberán existir mecanismos de seguridad para los contratos de abastecimiento externo
	Procedimiento a cumplir:	Establecer mecanismos de seguridad para contratos de abastecimiento externo Aprobación de los mecanismos por los altos mandos de la organización Incluir los mecanismos de seguridad dentro de los contratos de abastecimiento externo
	Evidencias:	Informe de los mecanismos de seguridad para contratos de abastecimiento externo Contratos realizados de abastecimiento externo incluyendo mecanismos de seguridad

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.5 Abastecimiento externo	**Objetivo de Control:**	4.4.5.2 CONTROLAR LEGALIDAD DE CONTRATOS DE ABASTECIMIENTO EXTERNO
	Control:	Deben existir requerimientos legales, en torno a la normativa legal del caso, para los contratos de abastecimiento externo
	Procedimiento a cumplir:	Utilización de Normativa legal para la elaboración de requerimientos legales Elaboración de requerimientos legales en contratos de abastecimiento externo

		Comparación de contenido legal en contrato con la normativa legal utilizada
	Evidencias:	Normativa Legal utilizada Contratos realizados de abastecimiento externo Informe Normativa vs. Requerimientos

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.6 Clasificación y control de activos	**Objetivo de Control:**	4.4.6.1 CONTROLAR ASIGNACIÓN Y USO DE ACTIVOS
	Control:	Se debe definir con claridad a los responsables de los activos de información y su alcance en cuanto a manipulación de los mismos cuando estos son asignados a tercera personas
	Procedimiento a cumplir:	Registrar asignación de activos de información a terceras personas Definir alcance en el uso de los activos de información por terceras personas Definir responsables de los activos de información cuando se asignan a terceros
	Evidencias:	Registros de activos con personal externo responsable Informe del alcance en cuanto al uso de los activos de información

		Publicación de modo de uso de los activos de información

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.6 Clasificación y control de activos	**Objetivo de Control:**	4.4.6.2 ACTUALIZACIÓN DE ASIGNACIÓN Y USO DE ACTIVOS
	Control:	Se deberá realizar la respectiva actualización en la clasificación de activos, designados a terceros, cuando este sea devuelto o reasignado
	Procedimiento a cumplir:	Definir modo de actualización para reasignación de activos usados por terceros Verificaron de estado de activo al momento de devolución Actualización de clasificación de activos al momento de reasignación del mismo
	Evidencias:	Método de actualización para reasignación de activos Informe del estado del activo devuelto Reasignación del activo con respectivo responsable

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.7 Clasificación de la información	**Objetivo de Control:**	4.4.7.1 CORRECTA CLASIFICACIÓN DE LA INFORMACIÓN

	Control:	Deberá establecerse niveles de protección de la información y distribuirse según función y grado de responsabilidad que el personal externo tenga.
	Procedimiento a cumplir:	Establecer Los posibles niveles de acceso a la información Crear usuarios con respectivas claves que definan el acceso a la información Difusión de usuarios y claves a cada uno de los integrantes del personal externo, según su función y responsabilidades.
	Evidencias:	Pruebas de acceso, según usuario, en el sistema. Registro de actividades en el sistema. Recibidos de la entrega de usuarios con respectivas claves.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.7 Clasificación de la información	**Objetivo de Control:**	4.4.7.2 CORRECTO MANEJO DE LA INFORMACIÓN
	Control:	La información deberá ser manejada de una forma responsable por terceros y según la necesidad del proceso
	Procedimiento a cumplir:	Crear manual de manejo de la información Definir responsabilidades en el manejo de la información Establecer sanciones por mal manejo de la información

		Aprobación de sanciones por altos directivos de la organización
	Evidencias:	Físico del manual del manejo de la información Físico de establecimiento de responsabilidades y Sanciones por mal manejo de la información Publicación de sanciones por mal manejo de la información

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.8 Seguridad personal	**Objetivo de Control:**	4.4.8.1 CONTROL DE LA SEGURIDAD PERSONAL MEDIANTE ASIGNACIÓN DE PUESTOS
	Control:	Deberá determinarse requerimientos de seguridad para definir responsabilidades de puesto asignados a terceros.
	Procedimiento a cumplir:	Establecer requerimientos de seguridad Definir responsabilidades de puestos en base a requerimientos de seguridad Aprobación de requerimientos de seguridad por parte de altos directivos de la organización
	Evidencias:	Físico de los requerimientos de seguridad con respectiva aprobación Publicación, comunicados sobre los requerimientos a los miembros de la Organización. Requerimientos publicados en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.8 Seguridad personal	**Objetivo de Control:**	4.4.8.2 CONTROL DE LA SEGURIDAD PERSONAL MEDIANTE EL USO DE LA INFORMACIÓN
	Control:	Debe establecerse al inicio de la contratación de terceros un compromiso de confidencialidad sobre e uso de la información de la organización, responsabilizándolos de esta forma por algún mal uso de la misma.
	Procedimiento a cumplir:	Establecer compromisos de confidencialidad sobre el uso de la información de la organización Aprobación de los compromisos de confidencialidad por altos directivos de la empresa Inclusión de los compromisos de confidencialidad dentro de los contratos con terceras personas.
	Evidencias:	Físico de los compromisos de confidencialidad con su respectiva aprobación Contratos realizados a terceros.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.8 Seguridad personal	**Objetivo de Control:**	4.4.8.3 CONTROL DE LA SEGURIDAD PERSONAL MEDIANTE REPORTES DE NOVEDADES

	Control:	Todo el personal externo responsable de su puesto y función deberá emitir reportes de incidentes, debilidades o mal funcionamiento de cualquier activo de información que bajo su potestad se encuentre
	Procedimiento a cumplir:	Establecer formatos de informes de incidentes, debilidades o mal funcionamiento de activos de información. Aprobación de formatos por altos directivos de la organización Distribución de dichos formatos a todo el personal externo
	Evidencias:	Formatos de informes de incidentes, debilidades o mal funcionamiento, en físico Archivo de informes de incidentes ya entregados. Formatos publicados en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.8 Seguridad personal	**Objetivo de Control:**	4.4.8.4 CONTROL DE LA SEGURIDAD PERSONAL MEDIANTE EL USO DE ACTIVOS
	Control:	Todos los empleados usuarios, contratistas y terceras personas, deberán devolver todos los activos de la organización que se encuentren en su posesión a la terminación de su empleo, contrato o puesto.
	Procedimiento a cumplir:	Definir método de devolución de activos a cargo de terceros Crear formatos para la devolución de activos donde también se especifique la condición del activo al momento de su devolución

		Difundir el método de devolución a todo el personal externo en la organización.
	Evidencias:	Formatos de devolución de activos en físico Archivos de devoluciones de activos realizadas. Formatos publicados en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.9 Seguridad física y ambiental	**Objetivo de Control:**	4.4.9.1 CONTROLAR LA SEGURIDAD FÍSICA MEDIANTE LA CLASIFICACIÓN DE ESPACIOS DE TRABAJO
	Control:	Deberán establecerse los perímetros físicos de trabajo de tal manera que brinden las seguridades del caso para el personal externo y activos de información ya sean estos de la organización o de la prestadora del servicio.
	Procedimiento a cumplir:	Establecer los perímetros de acceso por persona/función Aprobación de los perímetros por la máxima autoridad Comunicación de perímetros de acceso según función.
	Evidencias:	Perímetros de acceso en físico con la respectiva aprobación. Publicación, comunicación de los accesos permitidos sobre la política a los miembros de la Organización. Letreros y/o señales de prohibido el paso sin previa identificación.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.9 Seguridad física y ambiental	**Objetivo de Control:**	4.4.9.2 CONTROLES DE ACCESOS FÍSICOS NO AUTORIZADOS A TERCEROS
	Control:	Se debe establecer controles de ingreso para toda persona propia, externa y/o extraña a dichos perímetros.
	Procedimiento a cumplir:	Establecer los controles necesarios para el ingreso o salida de la organización de propios o extraños. Aprobación de los controles por la máxima autoridad Difusión de los controles a todo el personal dentro de la Organización y a las personas ajenas que deseen ingresar a la misma.
	Evidencias:	Controles establecidos y aprobados para el ingreso o salida de personal externo o extraños. Publicación, comunicados sobre los controles a los miembros de la Organización. Controles publicados en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.10 Seguridad de equipos	**Objetivo de Control:**	4.4.10.1 PREVENIR DAÑO, ROBO O MAL USO DE EQUIPOS

	Control:	Se debe establecer la correcta ubicación de los equipos de información ya sean de la organización o de la externa para que puedan contar con la seguridad necesaria.
	Procedimiento a cumplir:	Determinar lugares estratégicos para la ubicación de los equipos Aprobación de la ubicaron de equipos por personal encargado, seguridad industrial y altos directivos
	Evidencias:	Documento aprobado para la ubicación de equipos. Constatación visual de la correcta ubicación de los equipos

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.10 Seguridad de equipos	**Objetivo de Control:**	4.4.10.2 CONTROLAR EL CORRECTO FUNCIONAMIENTO DE EQUIPOS
	Control:	Se deberá establecer un equipo de especialistas externos que se encargue del correcto mantenimiento de los equipos de información
	Procedimiento a cumplir:	Establecer grupo de trabajo conformado por especialistas para el mantenimiento de equipos de la organización Evaluación de las capacidades de especialistas que conformaran el grupo de trabajo Selección de los candidatos a formar parte del equipo de especialistas.

		Aprobación de grupo de trabajo por altos mandos
	Evidencias:	Proceso de evaluación y selección de especialistas Documento de aprobación y designación de integrantes del equipo de especialistas

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.11 Comunicación y Operaciones	**Objetivo de Control:**	4.4.11.1 ASEGURAR LA CORRECTA Y SEGURA OPERACIÓN DE LOS MEDIOS DE INFORMACIÓN
	Control:	Se debe definir responsabilidades a todo el personal externo dentro de los procedimientos de operaciones de información.
	Procedimiento a cumplir:	Establecer responsabilidades a personal externo en el uso de la información Aprobación por altos mandos de las responsabilidades según función Difusión de las responsabilidades a todo el personal dentro de la Organización.
	Evidencias:	Documento aprobado con asignación de responsabilidades apara el personal externo Publicación, comunicados sobre las responsabilidades a los miembros de la Organización. Responsabilidades publicadas en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.11 Comunicación y Operaciones	**Objetivo de Control:**	4.4.11.2 CONTROLAR EL USO DE LOS MEDIOS DE INFORMACIÓN MEDIANTE REGISTROS
	Control:	Se deberá documentar todos los procedimientos de operación de información, realizado por terceros, dejando un registro claro con todos los detalles.
	Procedimiento a cumplir:	Establecer formatos para documentar el registro de los procedimientos de operación. Aprobación de los formatos por la máxima autoridad Difusión de los formatos a todo el personal dentro de la Organización.
	Evidencias:	Formatos para documentación de procedimientos Publicación de los formatos establecidos Archivos de procedimientos ya documentados en el formato establecido.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.11 Comunicación y	**Objetivo de Control:**	4.4.11.3 CONTROLAR EL CUMPLIMIENTO DE ACTIVIDADES DE TERCEROS

Operaciones	**Control:**	La organización deberá gestionar la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.
	Procedimiento a cumplir:	Establecer parámetros de control y gestión que permitan monitorear el desempeño de los terceros Aprobación de los parámetros de control, para monitoreo, por la máxima autoridad
	Evidencias:	Parámetros de control para monitoreo previamente aprobados Exámenes de evaluación de desempeño

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.12 Control de Acceso	**Objetivo de Control:**	4.4.12.1 POLÍTICA PARA EL CONTROL DEL ACCESO A LA INFORMACIÓN
	Control:	Debe definirse claramente una política de control de acceso que defina los derechos de usuario o grupos de usuarios en cuanto al ingreso de terceras personas y a la manipulación de la información
	Procedimiento a cumplir:	Establecer las políticas Aprobación de las políticas por la máxima autoridad Difusión de las políticas a todo el personal dentro de la Organización.

	Evidencias:	Política de seguridad con políticas definidas acerca del acceso de terceros a la información. Publicación, comunicados sobre la política a los miembros de la Organización. Política publicada en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.12 Control de Acceso	**Objetivo de Control:**	4.4.12.2 CONTROLAR EL ACCESO A LA INFORMACIÓN MEDIANTE USO DE IDENTIFICACIONES
	Control:	Cada empleado, contratista o tercera persona deberán portar identificaciones, otorgadas por la organización, que detallen sus nombres y función en la organización aclarando así las áreas a las cuales tienen acceso.
	Procedimiento a cumplir:	Crear identificaciones que identifique datos personales básicos y función de cada persona externa que labore dentro de la organización Exigir el uso de identificaciones mientras se encuentren dentro de la organización y antes de ingresar a cualquier área de la organización Establecer penalidades a quien no porte su identificaron mientras se encuentre laborando
	Evidencias:	Constatación visual de las identificaciones. Difusión de penalidades en caso de no portar las identificaciones. Penalidades publicadas en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.12 Control de Acceso	**Objetivo de Control:**	4.4.12.3 CONTROLAR EL ACCESO A LA INFORMACIÓN MEDIANTE LA ASIGNACIÓN DE USUARIOS Y CLAVES
	Control:	Cada empleado usuario, contratista o tercera persona deberá contar con un usuario y contraseña que le permita tener acceso a la información de la organización, dicho usuario deberá contar con niveles de acceso y privilegios según el grado de responsabilidad de su función.
	Procedimiento a cumplir:	Establecer usuarios y contraseñas, con sus respectivos grados de acceso según función, para el acceso de terceros a la información Determinar grados y/o niveles de privilegios y accesos según función y responsabilidades del usuario Crear registros cada vez que algún usuario ingrese con su password y usuario.
	Evidencias:	Registro de actividades según usuarios Entrega de contraseñas y usuarios terceros

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.13 Desarrollo y mantenimiento de sistemas	**Objetivo de Control:**	4.4.13.1 PREVER ERRORES, CONFLICTOS Y MAL USO DE LOS SISTEMAS DE INFORMACIÓN DEJANDO CLARO LOS REQUERIMIENTOS RESPECTIVOS
	Control:	Se debe identificar todos los requerimientos de seguridad en la fase de requerimientos de un proyecto desarrollado por terceros, estos deben ser justificados, acordados y documentados

	Procedimiento a cumplir:	Establecer requerimientos de seguridad para proyectos desarrollado por terceros Verificar la estipulación de dichos requerimientos dentro del plan de desarrollo de los proyectos Documentar los requerimientos de seguridad acordados Aprobación de los requerimientos por la máxima autoridad
	Evidencias:	Requerimientos de seguridad en papel Plan de desarrollo de los proyectos Archivo de documentación de requerimientos acordados

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.13 Desarrollo y mantenimiento de sistemas	**Objetivo de Control:**	4.4.13.2 PREVER ERRORES, CONFLICTOS Y MAL USO DE LOS SISTEMAS DE INFORMACIÓN DEFINIENDO CONTROLES PARA EL DESARROLLO DE APLICACIONES
	Control:	Se deberá establecer controles apropiados en las aplicaciones desarrolladas por el usuario externo para asegurar un procesamiento correcto.
	Procedimiento a cumplir:	Establecer controles en el desarrollo de aplicaciones realizadas por personal externo Aprobación de los controles por la máxima autoridad Difusión de los controles a todo el personal interesado dentro de la Organización.

	Evidencias:	Controles de seguridad para el desarrollo de aplicaciones Publicación, comunicados de los controles a los miembros de la Organización. Controles publicados en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.13 Desarrollo y mantenimiento de sistemas	**Objetivo de Control:**	4.4.13.3 PREVER ERRORES, CONFLICTOS Y MAL USO DE LOS SISTEMAS DE INFORMACIÓN MEDIANTE CONTROLES CRIPTOGRÁFICOS
	Control:	Se deberán establecer controles criptográficos y de gestión de claves para todos los usuarios externos que deban tener acceso a los sistemas de información de la organización
	Procedimiento a cumplir:	Establecer controles criptográficos para el acceso a la información Aprobación de dichos controles por la máxima autoridad
	Evidencias:	Controles criptográficos para acceso a información con su respectiva aprobación Difusión y comunicación de controles al personal interesado Publicación de controles en intranet

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.14 Conformidad	**Objetivo de Control:**	4.4.14.1 VERIFICAR QUE LOS CONTRATOS CON TERCEROS ESTÉN REALIZADOS EN CONFORMIDAD CON LA LEY **(ver Anexo 1, LISTADO DE ELEMENTOS BÁSICOS QUE SE DEBEN INCLUIR EN TODO CONTRATO DE OUTSOURCING)**
	Control:	Deberá existir claramente dentro de las políticas de contratación con terceros los requerimientos legales que sean necesarios
	Procedimiento a cumplir:	Establecer requerimientos legales necesarios dentro de los contratos con terceros Aprobación de requerimientos legales por conocedores y máximas autoridades Inclusión de requerimientos legales dentro del contrato con terceros
	Evidencias:	Los requerimientos legales previamente aprobados Contratos realizados con requerimientos incluidos

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.14 Conformidad	**Objetivo de Control:**	4.4.14.2 INFORMAR SOBRE LOS PARÁMETROS LEGALES DE CADA FUNCIÓN
	Control:	Deberán darse a conocer a todo el personal externo la legislación aplicable existente dentro de sus funciones
	Procedimiento a cumplir:	Informar y comunicar sobre la legislación existente aplicable dentro de la organización

		Actualizar continuamente según las disposiciones legales al momento Difusión de cambios en la misma en caso de que los haya
	Evidencias:	Publicación, comunicados sobre la legislación a los miembros de la Organización. Legislación publicada en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.15 Controles de contrato **(ver anexo 2, DERECHOS Y OBLIGACIONES DE LAS PARTES)**	**Objetivo de Control:**	4.4.15.1 DEJAR EN CLARO TIEMPO DE SERVICIO, REMUNERACIÓN Y FORMA DE PAGO A TERCEROS
	Control:	Se deberá establecer dentro de los contratos con terceros, el tiempo que prestaran sus servicios, este deberá estar detallado claramente junto con la remuneración y sistema de pago
	Procedimiento a cumplir:	Aprobación de las políticas por la máxima autoridad Difusión de las políticas a todo el personal dentro de la Organización.
	Evidencias:	Política de seguridad con políticas definidas acerca del tratamiento con terceros.

		Publicación, comunicados sobre la política a los miembros de la Organización. Política publicada en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.15 Controles de contrato	**Objetivo de Control:**	4.4.15.2 DEJAR ESTABLECIDOS PERSONAL PARTICIPANTE CON SUS RESPECTIVAS FUNCIONES
	Control:	Se establecerá con claridad en los contratos con terceros, a los participantes del mismo, esto junto con el detalle del personal que participara en la realización del servicio.
	Procedimiento a cumplir:	Establecer personal externo participante en el contrato Inclusión detallada de estos dentro del contrato
	Evidencias:	Contratos realizados con detalle de personal externo participante

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL

4.4.15 Controles de contrato	**Objetivo de Control:**	4.4.15.3 ESTABLECER QUE LOS CONTRATOS CON TERCEROS SE CUMPLAN SEGÚN REQUERIMIENTOS **(ver anexo 3, CLAUSULAS CONTRACTUALES DE TERCERIZACIÓN)**
	Control:	Se definirá detalladamente dentro del contrato con terceros, todas las cláusulas posibles y sus multas en caso de incumplimiento o ruptura del mismo, estas pueden darse por cualquiera de las dos partes.
	Procedimiento a cumplir:	Establecer cláusulas y/o multas Aprobación de las cláusulas y/o multas posibles por la máxima autoridad Inclusión de las multas y/o cláusulas posibles dentro del contrato
	Evidencias:	Escrito de multas y cláusulas, aprobadas por directorio, por incumplimiento de contrato Contratos realizados con clausulas y/o multas incluidas en el mismo

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.16 Controles de Auditoria **(ver anexo 4, AUDITORIA AL OUTSOURCING INFORMÁTICO)**	**Objetivo de Control:**	4.4.16.1 DEFINIR BASES PARA LA REALIZACIÓN DE EXÁMENES DE AUDITORIA **(ver anexo 5, PROGRAMA GENERAL DE TRABAJO)**
	Control:	Se deberá establecer las bases o funciones de la administración de seguridad con terceros para la realización correcta de exámenes a las mismas.
	Procedimiento a cumplir:	Establecer bases para las funciones de la administración de seguridad con terceros para realización de exámenes de forma correcta

		Aprobación de las bases por la máxima autoridad Difusión de las bases a todo el personal dentro de la Organización.
	Evidencias:	Bases de la administración de seguridad con terceros aprobadas Publicación, comunicados sobre las bases a los miembros de la Organización. Exámenes de auditoría realizados.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.16 Controles de Auditoria	**Objetivo de Control:**	4.4.16.2 ESTABLECER RIESGOS DE LA PRESTACIÓN DE SERVICIOS EXTERNOS
	Control:	En las bases deberá establecerse los posibles riesgos que conlleve la utilización de servicios externos en la organización
	Procedimiento a cumplir:	Realizar el respectivo análisis de riesgos Establecer posibles riesgos del uso de servicios externos Incluir los riesgos en las bases de control de la administración con terceros Comunicar de los posibles riesgos a los interesados
	Evidencias:	Documentación del análisis de riesgos Riesgos posibles del uso de servicios externos

		Publicación, comunicados sobre los riesgos posibles a todos los interesados

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.16 Controles de Auditoria	**Objetivo de Control:**	4.4.16.3 ESTABLECER SOLUCIONES A POSIBLES RIESGOS AL CONTRATAR SERVICIOS EXTERNOS
	Control:	Se establecerá posibles soluciones a los riesgos comunes que resulten de la contratación con terceros.
	Procedimiento a cumplir:	Realizar el respectivo análisis de riesgos Establecer soluciones posibles a riesgos comunes determinados por la contratación de terceros Aprobación de las soluciones posibles por los altos mandos Incluir las soluciones dentro de las bases de administración de terceros
	Evidencias:	Soluciones posibles a riesgos comunes previamente aprobada Publicación, comunicados sobre las posibles soluciones, a los miembros de la Organización. Bases en físico con la inclusión de las soluciones posibles a riesgos comunes

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.16 Controles de Auditoria	**Objetivo de Control:**	4.4.16.4 ESTABLECER ALTERNATIVAS DE ACCIÓN EN CASO DE CONTINGENCIAS
	Control:	El personal externo deberá definir y establecer la metodología de restauración de los sistemas de información luego de una contingencia.
	Procedimiento a cumplir:	Aprobación de las políticas por la máxima autoridad Definir actividades sistemáticas para contingencias Difusión de las políticas a todo el personal dentro de la Organización.
	Evidencias:	Política de seguridad con políticas definidas acerca del tratamiento con terceros. Publicación, comunicados sobre la política a los miembros de la Organización. Política publicada en la intranet.

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.17 Seguimiento y control	**Objetivo de Control:**	4.4.17.1 COORDINAR CORRECTAMENTE LAS FUNCIONES ENTRE TERCEROS Y ORGANIZACIÓN
	Control:	Se deberá formar una comisión que se encargue de coordinar las funciones entre ambas partes, organización con terceros.

	Procedimiento a cumplir:	Selección de personal que conformara comisión de coordinación entre terceros y la organización Aprobación de comisión por altos mandos de la organización Formación de comisión de coordinación
	Evidencias:	Proceso de selección de miembros de la comisión Aprobación escrita de la comisión Comisión de coordinación

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.17 Seguimiento y control	**Objetivo de Control:**	4.4.17.2 ASEGURAR EL CORRECTO DESARROLLO Y CUMPLIMIENTO DE ACTIVIDADES FIJADAS
	Control:	La comisión deberá velar por el cumplimento del plan acordado y que es compromiso del servidor externo
	Procedimiento a cumplir:	Establecer funciones de la comisión y sus áreas de análisis Incluir en las funciones el velar por el cumplimiento de los compromisos contraídos por el servidor externo Establecer revisiones periódicas del desarrollo y cumplimiento de las funciones de los terceros

	Evidencias:	Funciones de la comisión en papel con su respectiva autorización Comunicado de funciones a todos los miembros de la comisión Plan de revisiones periódicas establecidas por la comisión

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.17 Seguimiento y control	**Objetivo de Control:**	4.4.17.3 EVALUAR EL DESARROLLO Y CUMPLIMIENTO DE LAS FUNCIONES DE TERCEROS
	Control:	Esta comisión deberá realizar informes sobre los resultados obtenidos por el personal externo, con la finalidad de evaluar si su trabajo es el deseado por la organización
	Procedimiento a cumplir:	Establecer parámetros de evaluación al personal externo Aprobación de los parámetros por los altos mandos de la organización Evaluar al personal externo para medir la satisfacción de su trabajo realizado Presentar informes a los altos mandos con resultados de la evaluación
	Evidencias:	Parámetros de evaluación con su respectiva aprobación Evaluaciones realizadas al personal externo Informes entregados a los altos mandos de la organización

Dominio/Proceso	**Norma:**	ISO/COBIT/ITIL
4.4.18 Estandarización	**Objetivo de Control:**	4.4.18.1 MANTENER CONFORMIDAD DE LAS FUNCIONES DE TERCEROS CON ESTÁNDARES RECONOCIDOS
	Control:	Se deberán fijar las funciones del personal externo basándose en estándares reconocidos y aplicables según la función de la tercera persona
	Procedimiento a cumplir:	Definir funciones de terceros basados en estándares reconocidos y aplicables según el caso Aprobación de las funciones por altos mandos Realizar comparativos de funciones vs. estándares
	Evidencias:	Funciones de terceros establecidas y aprobadas Estándares reconocidos y aplicables a las funciones de terceros Cuadros comparativos de funciones vs. estándares

ANEXO 1

LISTADO DE ELEMENTOS BÁSICOS QUE SE DEBEN INCLUIR EN TODO CONTRATO DE OUTSOURCING

De este listado el auditor/abogado/asesor deberá seleccionar los elementos que se ajustan al contrato que van a establecer en la empresa contratante

Acceso para auditoria
Administración del contrato
Ajuste de cargos por cambios en el proyecto
Almacenamiento de información
Ámbito de aplicación del contrato
Aplicación del contrato
Aprobación por fases
Arbitraje
Calidad del servicio
Cambios en la legislación
Cargos
Cesión de datos
Cesión de derechos de uso
Cargos fijos
Cargos variables
Cifrado de datos
Condiciones de aceptación final
Condiciones de terminación parcial
Condiciones por terminación total
Confidencialidad
Conversión de programas
Corrección de errores
Criterios de valoración
Cumplimiento
Definiciones
Derecho de propiedad de programas, equipos, materia del contrato
Disponibilidad de servicio
Disponibilidad de información
Entrega de aplicaciones
Estándares de uso
Exclusiones
Expectativas de rendimiento

Fecha de pago
Modalidad de pago
Garantías
Indemnizaciones
Incumplimientos del contrato
Incumplimientos de pago
Incumplimiento de entregas
Integridad de datos
Licencias de uso
Limitaciones de responsabilidad
Mantenimiento de aplicaciones
Métodos de evaluación de rendimiento
Migraciones
Modificaciones del contrato, adéndums
Modificaciones de tarifas
Modificaciones de software
Módulos contratados
Niveles de servicio
Obsolescencia
Opciones de renovación
Pacto de propiedad intelectual
Pacto de confidencialidad
Penalización por terminación parcial
Penalizaciones varias
Plazos de entrega
Procedimientos de seguridad, de operación, de respaldos, de continuidad, de pruebas de aceptación
Propiedad de datos, de equipos, intelectual, de programas
Prórroga
Previsiones de seguridad
Quiebra
Recuperación ante desastres
Recursos
Resolución de disputas
Representantes de la empresa contratante
Representantes de la empresa contratada
Relación entre las partes
Responsabilidad civil

Responsabilidad de la calidad del servicio
Responsabilidad contractual
Revisión de precios
Revisiones de seguridad
Riesgos físicos, lógicos, laborales
Satisfacción del usuario
Servicios de respaldo
Solución de conflictos
Suministros
Supervisión del progreso del contrato
Supresión del servicio
Terminación de contrato
Tiempo de respuesta
Transferencia de equipos, datos, programas, licencias de uso, de personal
Ubicación física en que se desarrolla el contrato
Unidades de medida del servicio
Volúmenes a procesar

Estos elementos son los que a mi criterio deben prevalecer, pero pueden añadirse muchos más de acuerdo al tipo de contrato de servicios informáticos.

ANEXO 2

DERECHOS Y OBLIGACIONES DE LAS PARTES

A continuación nos referiremos a los más importantes derechos y obligaciones tanto de la empresa cliente como del outsourcer.

Los principales derechos de la empresa cliente son:

a) Definir el objeto del outsourcing
b) Supervisar al outsourcer
c) Ejercer sus derechos de propiedad intelectual
d) Exigir la exclusividad del outsourcer
e) Mantener la propiedad de los bienes trasladados al outsourcer
f) Exigir la confidencialidad de la información proporcionada al outsourcer
g) Coordinar la estrategia del negocio sin que esto cree una relación de subordinación del outsourcer respecto a la empresa cliente
h) Obtener los resultados a los términos pactados

Asimismo, las principales obligaciones de la empresa cliente son:

a) Determinar los alcances de la delegación de la actividad que realizara el outsourcer
b) Proporcionar la información necesaria al outsourcer para el cumplimiento de su prestación
c) Supervisar el cumplimiento de la actividad en los plazos pactados
d) Retribuir al outsourcer
e) Cumplir con las demás clausulas pactadas en el contrato de outsourcing

Por otro lado, los principales derechos del outsourcer son:

a) Gozar de autonomía jurídica, económica y administrativa
b) No subordinarse a la dirección de la empresa cliente
c) Realizar negocios con otras empresas en tanto no viole el pacto de exclusividad
d) Recibir la información necesaria de la empresa cliente para el cumplimiento de su prestación
e) Ser retribuido

Finalmente, las principales obligaciones del outsourcer son:

a) Contratar personal capacitado para la realización del outsourcing
b) Respetar los derechos de propiedad intelectual de la empresa cliente
c) Mantener la exclusividad y la confidencialidad a favor de la empresa cliente

d) Responsabilizarse por la pérdida de bienes o documentos de la empresa cliente
e) Presentar informes periódicos a la empresa cliente
f) Lograr los resultados en los términos pactados, asumiendo el riesgo de dichos resultados
g) Cumplir con las demás clausulas pactadas en el contrato de outsourcing

Cláusulas contractuales

DE LOS CONTRATOS DE DESARROLLO DE SOFTWARE

Lineamientos para realizar contratos de servicios de desarrollo o construcción de Software
Para la contratación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente:
Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.
Todo proyecto deberá ser aprobado por el Comité en base a un informe técnico que contenga lo siguiente:

- Bases del concurso (Requerimientos claramente especificados)
- Análisis de ofertas (Tres oferentes como mínimo) y Selección de oferta ganadora

Bases del Concurso
Las bases del concurso especifican claramente los objetivos del trabajo, delimita las responsabilidades de la empresa oferente y la contratante.
De las empresas oferentes:
Los requisitos que se deben solicitar a las empresas oferentes son:

a. Copia de la Cédula de Identidad del o los representantes de la compañía
b. Copia de los nombramientos actualizados de los representantes legales de la compañía
c. Copia de los Estatutos de la empresa, en que aparezca claramente definido el objeto de la compañía, esto es para determinar si está o no facultada para realizar la obra
d. Copia del RUC de la compañía
e. Referencias de clientes (Mínimo 3)
f. La carta con la oferta definitiva del contratista debe estar firmada por el representante legal de la compañía oferente.

De la contratante
Las responsabilidades de la contratante son:

a. Delinear adecuadamente los objetivos y alcance del aplicativo.
b. Establecer los requerimientos del aplicativo
c. Definir responsabilidades de la contratista y contratante
d. Establecer campos de acción

Análisis de ofertas y Selección de oferta ganadora:
Para definir la empresa oferente ganadora del concurso, el Comité establecerá una reunión en la que se debe considerar los siguientes factores:

a. Costo
b. Calidad
c. Tiempo de permanencia en el mercado de la empresa oferente
d. Experiencia en el desarrollo de aplicativos
e. Referencias comprobadas de Clientes
f. Cumplimiento en la entrega de los requisitos

Aprobada la oferta se debe considerar los siguientes lineamientos en la elaboración de contratos:
Todo contrato debe incluir lo siguiente:
Antecedentes, objeto del contrato, precio, forma de pago, plazo, obligaciones del contratista, responsabilidades, fiscalizador de la obra, garantías, entrega recepción de obra provisional y definitiva, sanciones por incumplimientos, rescisión del contrato, disposiciones supletorias, documentos incorporados, solución de controversias, entre otros aspectos.
Las garantías necesarias para cada contrato deben ser incluídas en forma conjunta con el Departamento Legal, quienes deben asesorar el tipo de garantía necesaria en la elaboración de cada contrato.

Las garantías que se deben aplicar de acuerdo al tipo de contrato son:

a. Una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato por el 5% del monto total del contrato para asegurar su fiel cumplimiento, la cual se mantendrá vigente durante todo el tiempo que subsista la obligación motivo de la garantía.
b. Una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato equivalente al 100 % (ciento por ciento) del anticipo. Esta garantía se devolverá en su integridad una vez que el anticipo se haya amortizado en la forma de pago estipulada en el contrato.
c. Un fondo de garantía que será retenido de cada planilla en un porcentaje del 5 %.

Junto al contrato se deberá mantener la historia respectiva del mismo que se compone de la siguiente documentación soporte:

- Estudio de factibilidad
- Bases del concurso
- Ofertas presentadas
- Acta de aceptación de oferta firmada por los integrantes del Comité
- Informes de fiscalización
- Acta de entrega provisional y definitiva

DE LOS CONTRATOS DE MANTENIMIENTO DE EQUIPOS DE COMPUTO

Lineamientos para realizar contratos de mantenimiento

Todo contrato de mantenimiento debe tener como mínimo lo siguiente:

1. Antecedentes del contrato
2. Objeto del contrato
3. Productos cubiertos en el contrato
4. Vigencia del contrato
5. Forma de pago
6. Horario de atención
7. Especificaciones del tipo de servicio esperado
8. Esquema para notificación de fallas
9. Penalidades
10. Condiciones y excepciones
11. Confidencialidad
12. Garantía de fiel cumplimiento

Entre otros requerimientos que surjan producto de la experiencia en contratos anteriores

Garantía de fiel cumplimiento

El PROVEEDOR de acuerdo con la política vigente, para proveer servicio de mantenimiento a la empresa, a la suscripción del contrato deberá entregar una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato por el 5% del monto total del contrato para asegurar su fiel cumplimiento, la cual se mantendrá vigente durante todo el tiempo que subsista la obligación motivo de la garantía. Esta garantía será de realización automática con un plazo de vencimiento por treinta (30) días después de concluido el contrato a favor de la empresa, en caso de que no se haya tenido el nivel de cumplimiento en este contrato establecido.

Verificación de cumplimiento y normativas vigentes

Se efectuarán tareas periódicas de control sobre el cumplimiento satisfactorio del servicio brindado por el proveedor para comprobar el cumplimiento del contrato y de las políticas y procedimientos vigentes

DE LA ADMINISTRACION DE PROBLEMAS

Análisis de problemas
Todo problema debe ser analizado en sus causas reales y efectos.

Registro de problemas
Toda actividad de recuperación del problema debe quedar registrada.
Se deberá efectuar el registro de los problemas presentados hasta la solución identificada

Asesoría especializada en resolución de problemas
Si un problema no ha sido resuelto, éste deberá ser registrado y se debe encontrar la solución y en casos que se requiera con autorización de la Dirección se contratará la asesoría respectiva de personal externo capacitado.

Prioridad de problemas
Todo problema debe tener un nivel de prioridad, el mismo que será asignado por el Jefe del departamento que recibe dicho problema.

Notificación de problemas a la dirección
Se utilizarán informes gerenciales para notificar al Director de Sistemas el registro completo del problema hasta su solución.

CLÁUSULAS CONTRACTUALES DE TERCERIZACIÓN

Si la empresa ha tercerizado el servicio de mantenimiento preventivo y correctivo de equipos e impresoras, éste contrato debe contemplar las condiciones básicas establecidas en las políticas de la empresa.

MODELO

CONTRATO DE MANTENIMIENTO DE EQUIPOS DE COMPUTO

CLAUSULA PRIMERA.- ANTECEDENTES DEL CONTRATO

Comparecen a la celebración de este contrato de Mantenimiento de Equipos de Procesamiento Automático de Datos por una parte, la Corporación Naranjo Arrobo, con RUC 09123804741, con domicilio en la ciudad de Guayaquil en Colón 103 y Malecón, a quien se llamará el "CLIENTE" , y, por otra parte RELECSA, Reparaciones Electrónicas del Ecuador, S. A. , con el número de RUC 1234567890, con domicilio en la ciudad de Guayaquil en Colón 405 y Luis Urdaneta, a quien se denominará "PROVEEDOR".

CLAUSULA SEGUNDA.- OBJETO DEL CONTRATO

El cliente contrata al PROVEEDOR a fin de que le preste servicios de mantenimiento preventivo y correctivo a los Equipos de Procesamiento de Datos de su propiedad, en los lugares determinados y detallados en los Anexo 1 " Ubicación física de los equipos", de acuerdo a las especificaciones técnicas solicitadas por el cliente y que forman parte del presente contrato, en el Anexo 2 " Normas técnicas para el mantenimiento".

CLAUSULA TERCERA.- PRODUCTOS CUBIERTOS EN EL CONTRATO

Con tales antecedentes, el Cliente garantiza la propiedad de los Equipos de Procesamiento de Datos que son objeto del presente contrato.

Sólo son cubiertos por este contrato los Equipos de Procesamiento de Datos descritos e identificados según Anexo N° 1 adjunto al presente contrato.

El PROVEEDOR efectuará una revisión preventiva a los Equipos de Procesamiento de Datos de propiedad del cliente , a fin de determinar los servicios a prestar, incluyendo los repuestos y accesorios necesarios para que los Equipos se encuentren operativos.

El cliente y RELECSA, Reparaciones Electrónicas del Ecuador, S. A. acuerdan establecer una orden de servicio técnico. A este servicio técnico se le asignará un numero de identificación, en el lugar previsto para el efecto.

CLAUSULA CUARTA.- DE LA VIGENCIA DEL CONTRATO

El presente contrato entra en vigencia a partir del 15 de Noviembre de 2002 y rige por un periodo de dos años.

CLAUSULA QUINTA.- PAGOS

Los pagos se efectuarán de acuerdo a lo convenido con el PROVEEDOR. Estos pagos pueden ser reajustados por el PROVEEDOR previo aviso escrito con sesenta (60) días de anticipación, a la facturación con la nueva tarifa y debidamente aceptados por el cliente. Estos reajustes podrán realizarse únicamente a partir del segundo año de la vigencia del contrato.

Las tarifas se encuentran descritas en la sección de anexos, en el Anexo 3 " Equipos y tarifas contractuales de mantenimiento".

Los gastos de transporte así como todo los gastos ocasionados por desplazamiento excepcionales y que no están incluidos en los servicios del presente contrato, serán facturados al cliente separadamente.

CLAUSULA SEXTA.- DEL MANTENIMIENTO

El PROVEEDOR conviene en suministrar el servicio de mantenimiento que incluye :

a).Mantenimiento preventivo programado: Este servicio esta basado en las necesidades específicas de cada máquina, equipo y dispositivo en particular, según lo determinen las normas técnicas señaladas en el Anexo 2. El mantenimiento incluye entre otros : lubricación, ajustes, así como otros servicios descritos en el anexo 4 "Programa se servicio preventivo y correctivo", y pruebas de los equipos objeto del contrato, a ser ejecutado durante lo periodos seleccionados de común acuerdo entre las partes.

b).Mantenimiento no programado "correctivo": Hecho sobre la base de llamadas, incluye: ajustes, reparación, reemplazo de partes, piezas y partes inservibles y/o deterioradas; salvo los casos de excepción previstos en la cláusula Décima quinta y en el Anexo 4 de este contrato. Los repuestos serán sustituidos con otros nuevos, de acuerdo a lo establecido en la cláusula Décima tercera.

CLAUSULA SEPTIMA.- SERVICIO FUERA DEL HORARIO NORMAL

El PROVEEDOR se obliga a realizar el mantenimiento y a efectuar las reparaciones necesarias de los Equipos Informáticos objeto del contrato cuando fuere ello necesario por el CLIENTE aun fuera del "Horario Normal", es decir las 24 horas del día, los 365 días del año. Además se contará con servicio telefónico hotline disponible las 24 horas del día, los 365 días del año, el cual ofrece las siguientes funcionalidades:

- Recepción y registro de todas las incidencias de hardware.
- Soporte telefónico de primeros niveles.
- Distribución de incidencias de soporte presencial a técnicos
- Mantener informado al usuario sobre el estado y circunstancias de sus solicitudes de servicio pendientes de cumplimentar.

CLAUSULA OCTAVA.-SERVICIOS DE MANTENIMIENTO REALIZADO POR EL CLIENTE

El cliente se compromete en principio a no efectuar ningún tipo de operaciones de mantenimiento o reparación de los Equipos Informáticos objetos del contrato. Si contraviniese esta obligación, serán de su cuenta y riesgo las consecuencias resultantes. Sin embargo, el CLIENTE podrá realizar por su propia cuenta y cargo, cuando fuere necesario, sujeto a la autorización, entrenamiento, instrucciones y directrices del PROVEEDOR, los servicios de

mantenimiento indicados en el Anexo 5, o cualquier otro que las partes así decidan de mutuo acuerdo y por escrito.

Las reparaciones o mantenimiento realizadas por funcionarios del CLIENTE entrenados y autorizados por el PROVEEDOR causarán un crédito a favor del CLIENTE para cada equipo, máquina y/o dispositivo objeto de la reparación o del mantenimiento según lo estipulado en el Anexo 5.

CLAUSULA NOVENA.- MODIFICACIONES O ALTERACIONES A LOS EQUIPOS DEL CLIENTE

El CLIENTE puede realizar modificaciones o alteraciones a los equipos que a bien tenga y que estimare conveniente, lo cual no afectará al proveedor pues se entregará una descripción del equipo junto con la entrega del equipo al proveedor cuando sea necesario su mantenimiento.

CLAUSULA DECIMA.- SERVICIO

El CLIENTE puede solicitar la prestación de servicios previstas en el presente contrato desde la firma del mismo. Así mismo puede hacer un pedido de prestación de servicios complementarios, agregar o suprimir los productos que son el objeto del presente contrato.

Las solicitudes para realizar el mantenimiento correctivo a los equipos informáticos se llevarán a cabo una vez que el CLIENTE reporte una falla al PROVEEDOR, usando un código de llamada, que lo identifique y registre el día y la hora. El tiempo de respuesta máximo de atención ser estipulado para cada caso de servicio, en el siguiente detalle.

NIVEL DE CALIDAD DE LA ATENCION Y TIEMPOS DE RESPUESTA

El tiempo máximo transcurrido entre la notificación de cualquier incidencia al PROVEEDOR y la puesta en contacto del técnico con el usuario será siempre menor de 4 horas laborables. Para ello se toma como referencia una jornada laboral partida de 9 a 14 horas y de 16 a 18:30 Caso de que el usuario no este localizable la empresa contratada siempre debe dejar constancia del intento de dicho contacto a través de auxiliares de departamento, servicio, conserjerías o cualquier otro medio indicado por el CLIENTE.
Se definen como puestos de máxima disponibilidad a:

- Ordenadores personales con conexión a red.
- Impresoras láser de red.

Se define como puesto operativo a la capacidad de dicho puesto para arrancar, funcionando el sistema operativo, operar sus aplicaciones básicas y/o disponer de conexión a red.

Para los puestos de máxima disponibilidad se define un tiempo máximo de puesto operativo de 4 horas laborables, tanto por reparación como por sustitución, de forma que si no se puede lograr la reparación en dicho plazo la empresa contratada sustituirá el equipo averiado por otro de similares características que ofrezca al usuario la misma funcionalidad que el estropeado hasta la resolución completa de la avería. Esta cláusula se exige tanto para los equipos que estén en garantía como para los que no lo están.

En cualquier caso la resolución definitiva de cualquier incidencia tendrá un plazo máximo de 24 horas laborables, no siendo computables en este plazo los retrasos ocasionados por la compra de piezas o repuestos.

CLAUSULA DECIMA PRIMERA.- NOTIFICACION DE LAS FALLAS

Al ocurrir un desperfecto en los equipos objeto del contrato, el CLIENTE lo debe comunicar de inmediato al PROVEEDOR y facilitará acceso pleno y libre a los Equipos Informáticos bajo las condiciones de seguridad establecidos por el CLIENTE. El PROVEEDOR deber acatar y cumplir en su desempeño las normas de seguridad establecido por el CLIENTE.

El registro y control de todas las fases concernientes al proceso de reparación de fallas o desperfectos de los Equipos Informáticos, desde su concurrencia y notificación a el PROVEEDOR hasta su efectiva solución por ella, se debe llevar mediante el Reporte de fallas por el Anexo 6. Su contenido será de obligatoria aceptación para las partes.

CLAUSULA DECIMA SEGUNDA.- PENALIDADES

El retraso por parte del PROVEEDOR en el cumplimiento de lo convenido en el presente contrato dar lugar a ser sancionado con multa equivalente al cinco (5) por mil del monto total del presente contrato, por cada día de retraso en la entrega, deducible del pago de la respectiva factura, independientemente de las responsabilidades civiles y penales que se pudiera generar como consecuencia del incumplimiento del presente contrato.

CLAUSULA DECIMA TERCERA.- REPUESTOS

El PROVEEDOR, durante un periodo de 15 días contados a partir de la entrada en vigencia del presente contrato, se obliga a asegurar y proveer con la prontitud requerida, los repuestos, equipos, dispositivos, componentes y/o piezas necesarios para garantizar un máximo nivel de mantenimiento y operatividad de los Equipos de Procesamiento de Datos, y restaurar a éstos su funcionamiento óptimo cuando una falla o irregularidad se produzca. Los repuestos, equipos, dispositivos, componentes y/o piezas serán incorporados a los equipos objeto del contrato a perpetuidad hasta que culmine su vida útil o por cualquier otra causa que conlleve a su reemplazo.

CLAUSULA DECIMA CUARTA.- PROPIEDAD Y GARANTIA DE LOS REPUESTOS

Pasarán a ser propiedad del CLIENTE las piezas o repuestos que se instalarán en los Equipos Informáticos en cumplimiento de este contrato. A tal efecto el PROVEEDOR garantiza la utilización de partes nuevas o equivalentes en capacidad de aportar un buen rendimiento a los Equipos de Procesamiento de Datos, los repuestos tendrán la garantía establecida por el fabricante, siempre y cuando el CLIENTE no cuente con los repuestos requeridos.(Ver notas adicionales).

CLAUSULA DECIMA QUINTA.- CONDICIONES Y EXCEPCIONES

Excepciones.- El servicio de mantenimiento no incluye:

a) Trabajo eléctrico externo a las máquinas o mantenimiento de accesorios, dispositivos u otros no suministrado por el PROVEEDOR.

b) Reparación de daños o incremento de tiempo de servicio causado por : accidente, transporte, negligencia o mal uso, alteraciones, incluyendo entre otras : desviaciones del diseño estructural o de circuitos de la máquina suministrada por el PROVEEDOR, instalación o remoción de dispositivos o cualquier otra modificación siempre que la realice alguien no autorizado por el PROVEEDOR.

c) Reparación de daños o incremento de tiempo de servicio causado por fallas del ambiente, incluyendo entre otras: Fallas en el suministro de la energía eléctrica, aire acondicionado o control de humedad. Así mismo, por el uso de suministro o materiales que no cumplan las especificaciones de el PROVEEDOR parar dicha reparación.

d) Cualquier servicio donde los técnicos del PROVEEDOR se encuentran imposibilitados de realizar, por causa de alteraciones en las máquinas o su conexión por medios eléctricos o mecánicos a otra máquina.

CLAUSULA DECIMA SEXTA.- ACCESO A LAS MAQUINAS

El personal técnico del PROVEEDOR tendrá libre y completo acceso a los lugares donde se encuentren ubicadas las máquinas y dispositivos de acuerdo a las normas de seguridad establecidas por el CLIENTE, para proveer los servicios contemplados en este contrato. En caso de que la reparación de una máquina o el mantenimiento de la misma sea efectuado por un técnico no autorizado por el PROVEEDOR y como resultado de ello se requieran reparaciones posteriores por parte del PROVEEDOR para restaurar la máquina a una buena condición de operación, dichas reparaciones serán efectuadas sobre la base de tiempo y materiales a las tarifas vigentes de el PROVEEDOR.

CLAUSULA DECIMA SEPTIMA.- LOCAL (ES) PARA EL MANTENIMIENTO, REPARACION Y DEPOSITO

El CLIENTE facilitará sin costo alguno el espacio o local(es) necesario(s) para el depósito de las piezas y/o dispositivos de repuestos de los Equipos Informáticos y para la ejecución de los trabajos que deba efectuar el PROVEEDOR según este contrato, todo dentro de las normas de seguridad establecidas por el CLIENTE.
La provisión de servicios a dichos espacios o locales, tales como aire acondicionado general, energía eléctrica, teléfonos, estarán a cargo del CLIENTE. También es responsable por las piezas de repuestos almacenados que le hayan sido formalmente consignados por el PROVEEDOR, las cuales permanecerán a disposición del personal de mantenimiento de la misma, debiendo ésta acatar las normas y disposiciones que establezca el CLIENTE en materia de control y registro de las existencias de depósito.

CLAUSULA DECIMA OCTAVA.- DE LA CONFIDENCIALIDAD

El PROVEEDOR se compromete a guardar la más absoluta reserva, seguridad e integridad de los procesos, programas, datos e información pertenecientes al CLIENTE o instalados en los locales de ésta última. Así como también, a no violar la confidencialidad, seguridad y propiedad de los archivos, programas y sistemas de aplicación, absteniéndose, sin la respectiva autorización por escrito del CLIENTE, a efectuar cualquier tipo de cambio, transacción, modificación y adición de información a los archivos, programas y sistemas de aplicación, no pudiendo facilitar a terceros bajo ningún concepto, información alguna, así como se compromete a no revelar información de la arquitectura tecnológica con la que cuenta la empresa.
La propiedad de la información es del CLIENTE, y no será bajo ningún concepto divulgada, comunicada, suministrada o puesta a disposición de terceros.
EL PROVEEDOR debe conseguir de sus empleados, agentes o contratados el mismo grado de reserva y cuidado con la información del CLIENTE.

CLAUSULA DECIMA NOVENA.- TRASLADO DE LOS EQUIPOS INFORMATICOS

En caso de que fuese necesario trasladar o movilizar los Equipos de Procesamiento de Datos objeto del contrato desde el lugar en que encuentren instalados, de conformidad a lo establecido en el Anexo 1, ambas partes deberán acordar previamente en cuanto a las condiciones en que tales acciones deberán ser efectuadas y acerca de sus implicaciones técnicas y consecuencias resultantes para las obligaciones que las partes asumen por este contrato. En tales casos, el PROVEEDOR supervisará la movilización de los Equipos Informáticos y procederá a su reinstalación sobre la base de tiempo y materiales a su tarifa vigente.

CLAUSULA VIGESIMA.- CAMBIOS O MODIFICACIONES EN LOS EQUIPOS INFORMATICOS PARA MEJORAR EL FUNCIONAMIENTO

Si el PROVEEDOR desarrollare cambios mandatorios de ingeniería y mejoras en los programas de mantenimiento a fin de incrementar la calidad, confiabilidad, mantenimiento y / o funcionamiento de los Equipos Informáticos lo suministrará e instalará sin costo adicional para el CLIENTE.

El CLIENTE facilitará el tiempo requerido para realizar en los Equipos Informáticos las instalaciones de los cambios de ingeniería y mejoras en los programas básicos, dentro del horario de trabajo establecido en el Anexo 6.

CLAUSULA VIGESIMA PRIMERA.- FACTURA

Las facturas de pago serán presentadas, una vez efectuados los servicios de mantenimiento.

Salvo acuerdo particular del PROVEEDOR con el CLIENTE, las facturas relativas al presente contrato son pagables cada treinta (30) días, a fin de mes de la fecha de facturación.

CLAUSULA VIGESIMA SEGUNDA.- GARANTIA DEL FIEL CUMPLIMIENTO

El PROVEEDOR de acuerdo con la política vigente, para proveer servicio de mantenimiento al CLIENTE, a la suscripción del contrato deberá entregar una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato por el 5% del monto total del contrato para asegurar su fiel cumplimiento, la cual se mantendrá vigente durante todo el tiempo que subsista la obligación motivo de la garantía. Esta garantía será de realización automática con un plazo de vencimiento por treinta (30) días después de concluido el contrato a favor del CLIENTE, en caso de que no se haya tenido el nivel de cumplimiento en este contrato establecido.

CLAUSULA VIGESIMA TERCERA.- RESPONSABILIDAD LABORAL

El presente Contrato no crea ni genera relación jurídica laboral alguna entre el CLIENTE y el personal que contrate el PROVEEDOR. El CLIENTE no asumirá ninguna responsabilidad por las obligaciones que contraiga el PROVEEDOR para la ejecución del servicio.

CLAUSULA VIGESIMA CUARTA.- ANEXOS

Forman parte integrante del presente contrato, los Anexos debidamente autorizados por las partes, que se menciona a continuación:

1. Ubicación física de los equipos
2. Normas técnicas para el mantenimiento
3. Equipos y tarifas contractuales de mantenimiento
4. Programa de servicio preventivo y correctivo
5. Servicio de mantenimiento que puede realizar el CLIENTE
6. Modelo de reporte de Fallas

CLAUSULA VIGESIMA QUINTA.- MODIFICACION

Ninguna cláusula del presente contrato podrá ser modificada, suprimida o agregada por una de las partes unilateralmente. Toda proposición de cambio deber ser comunicada y aceptada por escrito un mes antes de la fecha de realización.

CLAUSULA VIGESIMA SEXTA.- RESOLUCION

En caso de incumplimiento por causa injustificada, de alguna cláusula del presente contrato, este podrá ser resuelto por cualquiera de las partes previo aviso por escrito con treinta (30) días de anticipación. Cualquier pago que quedar, pendiente será cancelado en un plazo máximo de cinco (5) días hábiles, contados a partir de la más próxima fecha de pago.

CLAUSULA VIGESIMA SEPTIMA.- ARBITRAJE

Las partes se someten al conocimiento y decisión de uno o mas árbitros para la solución de las controversias que en el futuro puedan surgir entre ellas como consecuencia del presente contrato. De acuerdo a la Ley de Arbitraje los Árbitros resolverán las controversias que se originen con arreglo al derecho aplicable.

CLAUSULA VIGESIMA OCTAVA.- COMPETENCIA

Las partes renuncian expresamente al fuero de sus domicilios y se someten a la competencia de los Jueces y Tribunales de Justicia, así mismo, declaran expresamente que en todo lo no previsto en el presente contrato se rigen por lo dispuesto en el Código Civil en lo que fuera pertinente.

En señal de conformidad e invocando a la buena Fe, las partes firman el presente contrato, en dos ejemplares del mismo tenor y efecto legal, en la ciudad de Guayaquil, a los quince días del mes de Noviembre de 2002.

CLIENTE
(sello y firma)

PROVEEDOR
(sello y firma)

AUDITORÍA AL OUTSOURCING INFORMÁTICO.

La auditoría al outsourcing informático es una herramienta de apoyo administrativo que sirve de mediadora entre la organización y el proveedor, en aras de obtener proyectos exitosos, evaluando la calidad, eficiencia y eficacia de los Sistemas de Información, con base en los parámetros de Auditoría de Sistemas generalmente aceptados y comprobando la completitud, integridad, y confiabilidad en el manejo de los datos, seguridad en los equipos y telecomunicaciones, la producción óptima y oportuna de la información y el cumplimiento de las normas administrativas y fiscales vigentes.

La auditoría no puede ordenarle al contratista la forma como debe realizar su trabajo, mas bien le asesora y hace sugerencias para que resulte mejor elaborado; de ésta manera vigila la ejecución del contrato desde un comienzo y cuando aquel concluye, se puede tener la convicción que el contratista ha realizado su labor conforme a las especificaciones convenidas con la administración y sin reparos que ameriten su rechazo, garantizando así los criterios de calidad y eficiencia de la organización.
Como se puede apreciar, la auditoría no da lugar para que las tareas que realiza la administración dejen de efectuarse o se ejecuten mediocremente; la calidad de dichos contratos prácticamente se garantiza cuando la labor que cumplen las auditorías es bien ejercida.

Objetivos de la Auditoría.

A continuación se relacionan los objetivos más relevantes de la auditoría al outsourcing informático:

- Verificar que el proveedor esté realizando o implementando el outsourcing informático conforme al cronograma y especificaciones contratadas.
- Encaminar la acción administrativa hacia el logro de los objetivos planeados.
- Señalar desviaciones y errores a fin de lograr su corrección.
- Comprobar las condiciones de seguridad en el manejo de datos, equipos y telecomunicaciones; la producción óptima y oportuna de la información y el cumplimiento de las normas administrativas y fiscales vigentes.
- Asesorar y colaborar con el contratista en aspectos técnicos y administrativos.

- Revisar los grupos de trabajo responsables de la sistematización de cada proceso.
- Evaluar la eficiencia, economía y eficacia de los sistemas con base en los parámetros de Auditoría de Sistemas generalmente aceptados.
- Evaluar e informar sobre el desarrollo, implementación y mantenimiento de los sistemas de información, para que la organización continúe con los controles que han tenido un desempeño efectivo y para que se modifiquen o desarrollen aquellos que sean necesarios.
- Ejercer control sobre el software y hardware, buscando su adecuada administración ante los potenciales riesgos que los puedan afectar.
- Verificar la existencia de normas, procesos, procedimientos y recursos humanos, físicos y logísticos que deban interactuar ante la presencia de un siniestro o emergencia, garantizando la continuidad de las operaciones automatizadas o reduciendo su impacto.
- Verificar la protección de los recursos computacionales y el acceso a los equipos, a los programas y a la información, de manera que se busque una adecuada administración ante posibles riesgos que los afecten y que aseguren la oportunidad y confiabilidad de la información y sus registros.

AUDITORIA DE SISTEMAS DE INFORMACION
CONTROL DEL OUTSOURCING INFORMÁTICO

PROGRAMA GENERAL DE TRABAJO

	PROCEDIMIENTOS	OBJETIVO
A	**Familiarización y Documentación del OUTSOURCING**	Conocer la Situación actual del outsourcing
B	**Revisar los procedimientos y los Controles de Acceso.**	Evaluar la administración de las claves de acceso
C	**Revisar los planes de Contingencia**	Evaluar los planes de Contingencia para el outsourcing
D	**Evaluar los Controles Físicos**	Evaluar las medidas de seguridad física conservando los aspectos de confiabilidad, integridad, disponibilidad de la información.
E	**Determinación de áreas críticas**	Determinar el área de mayor riesgo dentro del outsourcing.

Programa de Auditoria

Entidad:
Fecha:
Tiempo de Inicio:
Tiempo Previsto:
Auditores Responsables:

A: **Familiarización y Documentación del OUTSOURCING**		Conocer la Situación actual del outsourcing		
PASOS		**Referencia a papeles de trabajo**	**Preparado por:**	**Tiempo de Duración**
1	Conducir una entrevista con personal apropiado vinculado al outsourcing, para realizar relevantamiento de información.			
2	Obtener el organigrama actual, así como también una breve descripción de cada uno de los cargos vinculados en el outsourcing.			
3	Obtener documentación legal.			
4	Obtener el manual de políticas y manual técnico vinculados al outsourcing			
5	Obtener el manual y los flujos de los diferentes procedimientos relacionados.			

Programa de Auditoria

Entidad:
Fecha:
Tiempo de Inicio:
Tiempo Previsto:
Auditores Responsables:

B: Revisar los procedimientos y los Controles de Acceso.		Evaluar la administración de las claves de acceso		
PASOS		**Referencia a papeles de trabajo**	**Preparado por:**	**Tiempo de Duración**
1	Conducir una entrevista con personal apropiado para obtener información acerca de los procedimientos para crear y quitar claves de acceso al personal del outsourcing			
2	Obtener una lista del personal de outsourcing con su respectivo perfil.			
3	Conocer el procedimiento para evaluar, asignar y entregar claves de acceso al personal de outsourcing			
4	Revisar las políticas de las aplicaciones de contraseñas. Todo lo que respecta a longitud, composición, encriptación, periodicidad.			
5	Verificar que se cumplan las políticas acerca de las claves de acceso			
6	Examinar los procedimientos para quitar el acceso a empleados de outsourcing cuando dejan de laborar.			
7	Determinar si las cuentas se suprimen.			

Programa de Auditoria

Entidad:
Fecha:
Tiempo de Inicio:
Tiempo Previsto:
Auditores Responsables:

C: Revisar los planes de Contingencia		Evaluar los planes de Contingencia para el outsourcing		
PASOS		**Referencia a papeles de trabajo**	**Preparado por:**	**Tiempo de Duración**
1	Verificar la existencia de políticas o planes de contingencias, con los servidores de aplicaciones y datos.			
2	Verificar políticas de respaldo de información			
3	Verificar los procedimientos de respaldo de información.			
4	Determinar que los archivos de respaldo se guardan en un lugar seguro.			
5	Revisar los siguientes planes y procedimientos de recuperación en caso de desastres: Almacenamiento y custodia de datos en lugar seguro, Lugar temperado, respaldo de información, Revisiones periódicas.			

Programa de Auditoria

Entidad:
Fecha:
Tiempo de Inicio:
Tiempo Previsto:
Auditores Responsables:

D: Evaluar los Controles Físicos		Evaluar las medidas de seguridad física conservando los aspectos de confiabilidad, integridad, y disponibilidad de la información.		
PASOS		**Referencia a papeles de trabajo**	**Preparado por:**	**Tiempo de Duración**
1	Verificar la existencia de políticas de seguridad física.			
2	Determinar si todo el hardware está ubicado en áreas físicamente seguras			
3	Revisar la seguridad de la sala de ordenadores y los controles de acceso físico			
4	Determinar si los equipos están protegidos contra factores ambientales, tales como: apagones, inundaciones, calor, humedad.			
5	Realizar las inspecciones en el sitio para verificar controles.			

Programa de Auditoria

Entidad:
Fecha:
Tiempo de Inicio:
Tiempo Previsto:
Auditores Responsables:

E: Determinación de áreas críticas		Determinar el área de mayor riesgo dentro del outsourcing.		
PASOS		**Referencia a papeles de trabajo**	**Preparado por:**	**Tiempo de Duración**
1	Seleccionar una muestra del personal de outsourcing para efectuar seguimiento.			
2	Elaborar y aplicar los cuestionarios necesarios para verificación de controles.			
3	Aplicar la técnica scoring para evaluar la importancia de cada uno de los módulos o secciones del contrato del outsourcing organizado por temáticas.			
3	Clasificar la información obtenida			
4	Realizar el análisis en base a los cuestionarios aplicados al personal.			
5	Determinar el área (temática) de mayor riesgo según resultado de los cuestionarios, matiz scoring y criterio del auditor.			

CONCLUSIONES

Del outsourcing

1. Estar al día con los avances tecnológicos bien sea por cuenta propia o a través de terceros es una oportunidad de negocios que los ejecutivos deben tomar previo un adecuado análisis costo beneficio de las opciones.

2. Muchas empresas con contratos de outsourcing exitosos, que asumían por su propia cuenta el rol informático como un área interna, sin ser su negocio la informática, se han dado cuenta que es mucho más rentable contratar estos servicios con empresas especialistas, que definitivamente reducen los costos en forma asombrosa y alcanzan en la mayoría de las veces excelentes resultados, los cuales difícilmente lograrían ellos mismos por no ser expertos en el tema.

3. El outsourcing informático está contribuyendo a crear nuevas fuentes de empleo, en lugar de sustituirlos ha generado gran cantidad de empresas cuya razón de ser es la información y todo lo relacionado a ella. En estos tiempos modernos se habla hasta del teletrabajo.

4. Una adecuada modernización de los recursos informáticos propios o contratados a través de terceros permitirá canalizar los esfuerzos aumentando la

productividad, factor indispensable para que nuestras empresas puedan satisfacer las necesidades del país y esté en capacidad de competir con éxito en los mercados internacionales.

5. Con un outsourcing bien administrado, las empresas contarían con el apoyo de personal experimentado que aporte conocimiento de la industria, tecnología y una metodología probada para agregar valor

6. Uno de los objetivos más buscados por todas las empresas es la mayor eficiencia al menor costo, sin dejar por un lado los estándares de calidad y servicio al cliente. Considero que el outsourcing informático es una opción que debe ser correctamente evaluada para sacar de ella el máximo beneficio.

7. También puedo concluir que debido a los diferentes posibilidades de Outsourcing de servicios o productos, las empresas deben elegir la que más se acomode de acuerdo a sus recursos y necesidades

8. El outsourcing es el proceso planificado mediante el cual se transfiere la responsabilidad de realizar ciertas actividades, que la compañía ha decidido no manejarlas internamente, sino transferirlas a una organización externa para sacar de ella el máximo beneficio siempre y cuando se establezcan adecuados controles y se evalúe el producto o servicios finales obtenidos.

Del Manual

1. Este manual presenta controles para disminuir la incertidumbre en la toma de decisión de un outsourcing y garantizar controles que faciliten la consecución de los objetivos gerenciales luego de haber tomado la decisión estratégica de invertir en outsourcing.
2. Para que un contrato de outsourcing trabaje correctamente deben ser aplicados los controles en este manual propuesto, pues considero son los más básicos para el buen funcionamiento operacional de un contrato de este tipo.
3. En este manual detallé los controles mínimos que deben ejecutarse en el outsourcing informático para poder aminorar los riesgos a los que está expuesto.

RECOMENDACIONES

1. Se recomienda aplicar los controles que se describen en este manual, producto resultante de la investigación del outsourcing informático a todas las empresas que contratan este tipo de servicios

2. Siendo el contador público autorizado un gran partícipe en la administración de las compañías como asesor o consultor; es este profesional quien debe adquirir el compromiso de propender el desarrollo empresarial con la propuesta de controles, sobretodo de las pequeñas y medianas empresas que son las más que más necesitan ayuda en el establecimiento de controles para el outsourcing informático.

3. Todo profesional CPA debe capacitarse conociendo aspectos legales para estar actualizados con estos temas y sugerir el establecimiento de controles contractuales en el outsourcing.

BIBLIOGRAFÍA

1. Enciclopedia Autodidáctica Océano, Volumen II (ISBN 84-7764-011-4, Grupo Editorial Océano, 1988)

2. Muñoz Razo Carlos, Auditoría en Sistemas Computacionales (ISBN: 970-17-0405-3, Pearson Education, México, 2002)

3. Cuervo José; Delitos informáticos: Protección Penal de la Intimidad http://www.informatica-juridica.com/trabajos/delitos.asp

4. Comité Directivo de COBIT y El IT Governance Institute, 2002. COBIT – Objetivos de Control, Tercera Edición (ISBN: 1-893209-17-2)

5. Diccionario Enciclopédico, Tomo IV (ISBN 84-7153-005-8, Bibliograf S.A., 1973.

6. Internacional Organization for Standarization. Recuperado en abril de 2007. http://www.iso.org/iso/home.htm

7. Miguel Angel Caffaro; Informática Profesional, publicación del Consejo Profesional en Ciencias

Informáticas Año 17, Nº 87, Mayo de 2001. http://www.cpci.org.ar/newsletters/87/Pericia.ht- 22k

8. MONOGRAFIAS. (2006), ”Auditoria de Sistemas”, http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas

9. Microsoft Corporation, Biblioteca Premium Microsoft Encarta 2006.

10. Barry James; White, Robert. “Manual del Outsourcing”. Ed. Gestión2000.com

11. Chapman, Jacqueline. “Aprenda a Externalizar (Outsourcing): en una semana”. Ed. Gestión 2000, 2005.

12. Del Peso Navarro Emilio, Manual del Outsourcing Informático Análisis y Contratación, 2003, 2ª Ed., Ed. Díaz de Santos.

13. Schneider Ben, Outsourcing, 2004, Grupo Editorial Norma.

14. Corbett Michael, The Outsourcing Revolution : Why It Makes Sense and How to Do It Right, Ed. Dearborn Trade Publishing, 2004, 256pp

15. Charles L. Gay, James Essinger, Inside Outsourcing, Ed. Nicholas Brealey, 2000, 256 pp

16. Carvallo Alman Amelia, Outsourcing La Subcontratación, Ed. LIMUSA, 2002, 169 pp