

GUÍA DE ACTUACIÓN: LA INVERSIÓN TECNOLÓGICA EN LAS EMPRESAS

– *Manual práctico para acertar con la inversión
tecnológica en las empresas* –



MIGUEL ÁNGEL PESQUERA GONZÁLEZ

Consejero de Industria, Trabajo y Desarrollo Tecnológico
del Gobierno de Cantabria

La modernización tecnológica de nuestras empresas es el camino deseable para mejorar sus niveles de competitividad y de crecimiento, que es tanto como decir de sostenimiento; lo cual es aplicable a todas las escalas de la empresa. Sin embargo, el cúmulo de información y publicidad existente, también en el terreno de las nuevas tecnologías, puede generar dudas entre aquellos que, decididos a modernizar sus procesos, no disponen de los suficientes puntos de referencia para tomar las decisiones apropiadas.

La inversión tecnológica para una empresa no puede limitarse a la adquisición de equipos avanzados cuyas potencialidades se desconocen o no pueden integrarse en un esquema global de gestión empresarial. Es necesario ahondar en la generación de una cultura tecnológica que integre estos avances en los procesos productivos y les dote de contenido práctico y eficaz.

Esta Guía de actuación para la inversión tecnológica en las empresas es, por tanto, una herramienta oportuna y apropiada para navegar en el cada vez más amplio mundo de la tecnología, pues nos ofrece los puntos de referencia precisos para este recorrido hacia la competitividad de nuestro tejido productivo.

Los retos de la economía española en el momento actual requieren hoy más que nunca una adecuada promoción y fomento de la capacidad emprendedora. Sin inversión, la I+D y la innovación no son suficientes, y sin capacidad emprendedora no hay inversión. Es la combinación adecuada y eficiente de estas variables lo que conducirá al éxito de una política económica acorde con los nuevos modelos de crecimiento vigentes. El esfuerzo que se debe realizar es necesario para empresarios, Administraciones, universidades y la sociedad en general, con el objetivo de acercarnos a una senda de crecimiento de la productividad similar a la del resto de países de la Unión Europea con mayor crecimiento, y a la de los Estados Unidos, paradigma actual del crecimiento económico a largo plazo.

Sin embargo la gestión de este esfuerzo inversor en tecnología dentro de las empresas debe producirse de forma que sea realmente eficaz para los fines perseguidos. Este trabajo delimita una Guía de Actuación para el aseguramiento de esa inversión tecnológica. Desde CEOE-CEPYME Cantabria esperamos que nuestra humilde aportación favorezca el éxito dentro de éste tan necesario como a veces difícil empeño.

Índice

1. ¿QUÉ HACER PARA ASEGURARSE QUE LA INVERSIÓN EN TIC SE REALIZA ADECUADAMENTE EN LA EMPRESA?	11
2. ESTÁNDARES EXISTENTES O POR QUÉ INVENTAR DE NUEVO LA RUEDA	13
2.1. Misión del COBIT	13
2.2. Principios del COBIT	14
2.3. El PMBOK	18
3. DOMINIOS DE PROCESOS EN LAS TIC O QUÉ TIPO DE PROCESOS DEBEN TENERSE EN CUENTA	21
3.1. Planificación y organización	21
3.2. Adquisición e implementación	38
3.3. Presentación y soporte	42
3.4. Monitorización	49
4. LA IMPORTANCIA DE LA ASESORÍA EXTERNA	53



¿QUÉ HACER PARA ASEGURARSE QUE LA INVERSIÓN
EN TIC SE REALIZA ADECUADAMENTE EN LA EMPRESA?



1. ¿Qué hacer para asegurarse que la inversión en tic se realiza adecuadamente en la empresa?

Los cambios continuos que se están produciendo en el mundo empresarial traen inevitablemente la necesidad de la implantación de mejores sistemas de información y comunicaciones.

Por una parte, el desarrollo de productos/servicios industriales competitivos no está por lo general al alcance de la mayoría de las empresas españolas: la falta de materias primas y las altas necesidades de capital son fuertes barreras.

Sin embargo, el desarrollo de productos o servicios basados en información es mucho más asequible: el requisito básico es la imaginación.

Adicionalmente, se ha demostrado empíricamente que existe una relación directa entre la inversión en TIC y la mejora de la productividad de la empresa.

La economía española atraviesa un período de crecimiento sostenido por encima de la media europea y, al menos a corto plazo, hay buenas perspectivas para seguir en esta senda. Sin embargo, en términos de crecimiento de la productividad nos encontramos en clara desventaja, peligrando el crecimiento a largo plazo de nuestra economía.

Los datos disponibles para el análisis cada vez cuentan con un mayor respaldo estadístico, y los resultados obtenidos a partir de ellos establecen lo que parecería los hechos estilizados de las causas y factores del crecimiento económico para las economías desarrolladas:

1. La contribución del stock de capital derivado de la inversión de las Tecnologías de la Información y la Comunicación (TIC) es primordial para el crecimiento de cualquier economía. Con independencia de su magnitud, la inversión TIC supone una contribución positiva al crecimiento de la productividad y la renta.

2. El sector TIC es una fuente del crecimiento de la Productividad Total de los Factores (PTF) de cualquier país, que sobrepasa a la contribución de cualquier otro sector.
3. La inversión y la innovación no son suficientes para aumentar la productividad si además no van acompañadas de cambios en ciertos aspectos en la empresa.
4. La educación adecuada de los futuros empresarios, inversores, y empleados, en el ámbito TIC son fundamentales para garantizar el crecimiento de la productividad, fomentando el “emprendizaje” productivo.

Para la economía española estos mismos aspectos deben ser tenidos en cuenta junto con las propias características intrínsecas de nuestra economía, que hacen que las medidas a adoptar deban tener un mayor énfasis. Es por ello que todas estas cuestiones, deben tratarse no sólo desde un punto de vista de política tecnológica, sino que deben abordarse bajo la óptica de la política económica de nuestro país.

Sin inversión, la I+D y la innovación no son suficientes, y sin capacidad emprendedora no hay inversión. Es la combinación adecuada y eficiente de estas variables lo que conduciría al éxito de una política económica acorde con los nuevos modelos de crecimiento vigentes. El esfuerzo que se debe realizar es necesario para empresarios, administraciones, universidades y la sociedad en general, con el objetivo de acercarnos a una senda de crecimiento de la productividad similar a la del resto de países de la Unión Europea con mayor crecimiento, y a la de los Estados Unidos, paradigma actual del crecimiento económico a largo plazo.

Sin embargo este esfuerzo inversor debe producirse de forma que sea realmente eficaz para los fines perseguidos. Este trabajo delimita una Guía de Actuación para el aseguramiento de esa inversión.

ESTÁNDARES EXISTENTES O POR QUÉ INVENTAR DE NUEVO LA RUEDA

- 2.1. Misión del COBIT
- 2.2. Principios del COBIT
- 2.3. El PMBOK



2.

Estándares existentes o por qué inventar de nuevo la rueda

Llegados a este punto quizá estemos un tanto preocupados al pensar cómo podremos abordar todas estas actividades que nos demandan las nuevas condiciones del mercado y el negocio.

Afortunadamente existen varios estándares desarrollados que nos darán las pautas que podemos seguir para cubrir todas estas necesidades.

Hablaremos básicamente de dos de ellos: uno orientado al gobierno de las TIC en general (COBIT) y otro específicamente orientado a la gestión de proyectos (PMBOK).

2.1. MISIÓN DEL COBIT:

Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

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

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los ordenadores personales, servidores y ambientes distribuidos. Esta basado en la filosofía de que los recursos de las TIC 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.

Usuarios:

- La Dirección: para apoyar sus decisiones de inversión en las TIC y control sobre el rendimiento de las mismas, llevando a cabo el análisis coste-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 las TIC, su impacto en la organización y determinar el control mínimo requerido.
- Los Responsables de las TIC: para identificar los controles que requieren en sus áreas.

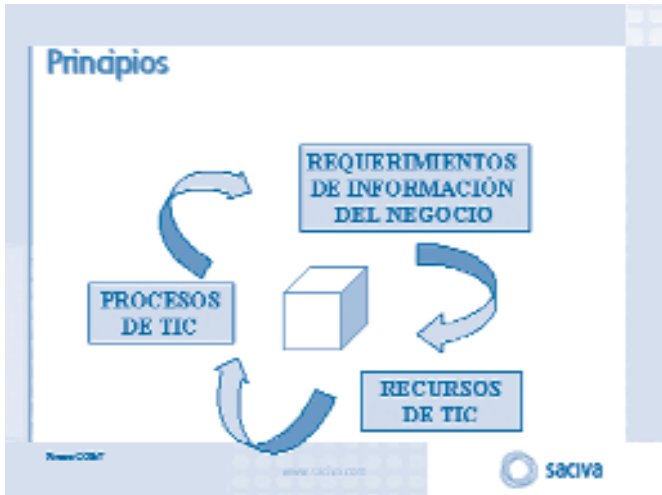
También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de las TIC en las empresas.

Características:

- Orientado al negocio.
- Alineado con estándares y regulaciones “de facto”.
- Basado en una revisión crítica y analítica de las tareas y actividades en las TIC.
- Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA).

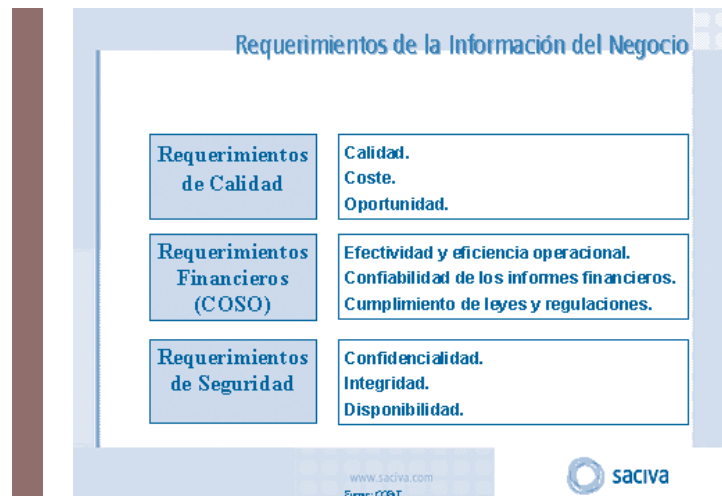
2.2. PRINCIPIOS DEL COBIT:

El enfoque del control en las TIC 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 las TIC.



2.2.1. REQUERIMIENTOS DE LA INFORMACIÓN DEL NEGOCIO

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



Requerimientos de Calidad: Calidad, Coste y Oportunidad.

Requerimientos Financieros: Efectividad y Eficiencia operacional, Confiabilidad de los informes financieros y Cumplimiento de leyes y regulaciones.

- 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.

Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad

- 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.

2.2.2. RECURSOS DE LAS TIC

En COBIT se establecen los siguientes recursos en las TIC necesarios para alcanzar los objetivos de negocio:

- Datos: Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.
- Aplicaciones: entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
- Tecnología: incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

Recursos de TIC

- **Datos:** Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficos, sonidos, etc.
- **Aplicaciones:** entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.
- **Tecnología:** incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.
- **Instalaciones:** Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- **Recursos Humanos:** Por la habilidad, conciencia y productividad del personal para planificar, adquirir, prestar servicios, dar soporte y monitorizar los sistemas de Información.

FUSION:COBIT www.saciva.com

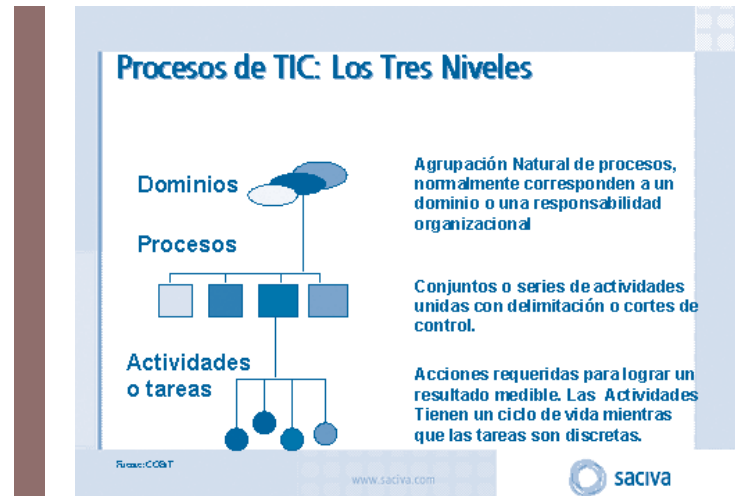
- Instalaciones: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.
- Recursos Humanos: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorizar los Sistemas de Información.

2.2.3. PROCESOS DE LAS TIC

La estructura de los procesos de las TIC se define a partir de una premisa simple y pragmática: “Los recursos de las Tecnologías de la Información y Comunicaciones (TIC) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos”.

Siguiendo este esquema, podemos dividirlos en tres niveles: Dominios, Procesos y Actividades

- Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
- Actividades: Acciones requeridas para lograr un resultado medible.



Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TIC. Estos procesos están agrupados en cuatro grandes dominios que se detallan a continuación junto con sus procesos y una descripción general de las actividades de cada uno.

2.3. EL PMBOK

El PMBOK (Project Management Body of Knowledge) es un estándar desarrollado por el PMI (Project Management Institute) cuya última versión se editó en el año 2000.

Contiene las mejores prácticas consolidadas a lo largo de treinta y cinco años por los directores de proyecto de diferentes negocios entre ellos las TIC.

El PMI (Project Management Institute) define un proyecto como un *“Esfuerzo temporal acometido para crear un único servicio o producto”*. Existen otras definiciones, pero en cualquiera de ellas podemos identificar los siguientes elementos característicos de un proyecto:

- conjunto de actividades
- con un objetivo
- una duración, un inicio y un final
- es único e irrepetible

Hasta hace algún tiempo se identificaba claramente el concepto de *proyecto informático* con tecnología. En la actualidad, cualquier *proyecto de negocio* tiene componentes tecnológicos, al igual que la mayor parte de los proyectos informáticos actuales tiene cada vez más componentes “no tecnológicos”. Esto está llevando a la convergencia entre ambos tipos de proyecto, de forma que cualquier proyecto TIC, hoy por hoy es un proyecto de empresa.

DOMINIOS DE PROCESOS EN LAS TIC O QUÉ TIPO DE PROCESOS DEBEN TENERSE EN CUENTA

- 3.1. Planificación y organización
- 3.2. Adquisición e implementación
- 3.3. Presentación y soporte
- 3.4. Monitorización



3.

Dominios de procesos en las TIC o qué tipo de procesos deben tenerse en cuenta

Para asegurarse el éxito en la gestión de los procesos de Tecnologías de Información y Comunicaciones debe prestarse atención a varios grupos de procesos, tal y como se puede observar en la Fig.

Procesos de TIC: Dominios

- Planificación y Organización (*Planning and Organization*)
- Adquisición e implementación (*Acquisition and Implementation*)
- Prestación de Servicios y Soporte (*Delivery and Support*)
- Seguimiento (*monitoring*)

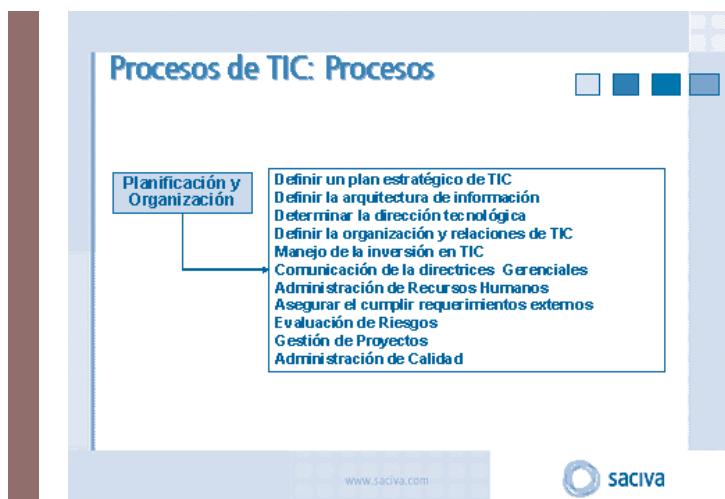
Fuente: CCGT
www.saciva.com
saciva

3.1. PLANIFICACIÓN Y ORGANIZACIÓN

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que las tecnologías de información y las comunicaciones puede contribuir de la mejor manera al logro de los objetivos de negocio.

Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas.

Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.



3.1.1. DEFINIR UN PLAN ESTRATÉGICO

La empresa necesita clarificar qué tipo de información necesita, de forma que se pueda lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de las TIC de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planificación estratégica emprendido a intervalos regulares dando lugar a planes a largo plazo, que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- La definición de objetivos de negocio y necesidades de las TIC; la alta Dirección será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

- El inventario de soluciones tecnológicas e infraestructura actual; se deberán evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, coste y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.
- Los cambios organizacionales; se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de las TIC.
- Estudios de viabilidad oportunos; para que se puedan obtener resultados efectivos.

3.1.2. DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN

Debe llevarse a cabo esta definición para satisfacer los requerimientos de negocio, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información, tomando en consideración:

- La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
- El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.
- La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

3.1.3. DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA

Objetivo: Aprovechar al máximo de la tecnología disponible o tecnología emergente, satisfaciendo los requerimientos de negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica, tomando en consideración:

- La capacidad de adecuación y evolución de la infraestructura actual, que deberá concordar con los planes a largo y corto plazo de tecnología de información y debiendo abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

- La Monitorización de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.
- Las contingencias (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura), con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.
- Planes de adquisición, los cuales deberán reflejar las necesidades identificadas en el plan de infraestructura tecnológica.

3.1.4. DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE LAS TIC

Evidentemente en un momento determinado se produce la prestación de servicios de las TIC internamente en la empresa.

Esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, teniendo en cuenta:

- El Comité de Dirección; el cual se encargará de vigilar la función de servicios de información y sus actividades.
- Propiedad, custodia; la Dirección deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- Supervisión; para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente.
- Segregación de funciones; con la que se evitará la posibilidad de que un solo individuo resuelva un proceso crítico.
- Los roles y responsabilidades; La Dirección deberá asegurarse de que todo el personal deberá conocer y contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas.
- La descripción de puestos; deberá delinear claramente tanto la responsabilidad como la autoridad, incluyendo las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.
- Los niveles de asignación de personal; deberán hacerse evaluaciones de requerimientos regularmente para asegurar una asignación de personal adecuada en el presente y en el futuro.
- El personal clave; La Dirección deberá definir e identificar al personal clave de tecnología de información.

3.1.5. MANEJO DE LA INVERSIÓN EN TIC

Objetivo: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros.

Su realización se concreta a través presupuestos periódicos sobre inversiones y operaciones establecidas y aprobados por el negocio, teniendo en cuenta:

- Las alternativas de financiamiento; se deberán investigar diferentes alternativas de financiamiento.
- El control del gasto real; se deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costes asociados con las actividades de la función de servicios de información.
- La justificación de costes y beneficios; deberá establecerse un control de la Dirección que garantice que la prestación de servicios por parte de la función de servicios de información se justifique en cuanto a costes. Los beneficios derivados de las actividades de las TIC deberán ser analizados en forma similar.

3.1.6. COMUNICACIÓN DE LAS DIRECTRICES Y ASPIRACIONES DE LA DIRECCIÓN

Objetivo: Asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones del alto nivel (Dirección), se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesiéndose para esto estándares para traducir las opciones estratégicas en reglas de usuario prácticas y utilizables. Toma en cuenta:

- Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno deberá ser establecido por la Alta Dirección y promoverse a través del ejemplo.
- Las directrices tecnológicas.
- El cumplimiento, La Dirección deberá también asegurar y monitorear la duración de la implementación de sus políticas.
- El compromiso con la calidad, La Dirección de la función de servicios de información deberá definir, documentar y mantener una filosofía de calidad, debiendo ser comprendidos, implementados y mantenidos por todos los niveles de la función de servicios de información.

- Las políticas de seguridad y control interno, la alta Dirección deberá asegurar que esta política de seguridad y de control interno especifique el propósito y los objetivos, la estructura de la Dirección, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento de estas políticas.

3.1.7. ADMINISTRACIÓN DE RECURSOS HUMANOS

Objetivo: Maximizar las contribuciones del personal a los procesos de las TIC, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal, tomando en consideración:

- El reclutamiento y promoción, deberá tener como base criterios objetivos, considerando factores como la educación, la experiencia y la responsabilidad.
- Los requerimientos de calificaciones, el personal deberá estar calificado, tomando como base una educación, entrenamiento y o experiencia apropiados, según se requiera.
- La capacitación, los programas de educación y entrenamiento estarán dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal.
- La evaluación objetiva y medible del desempeño, se deberá asegurar que dichas evaluaciones sean llevadas a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

3.1.8. ASEGURAR EL CUMPLIMIENTO CON LOS REQUERIMIENTOS EXTERNOS

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales.

Para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en las TIC, llevando a cabo las medidas apropiadas para cumplir con ellos y se toma en consideración:

- Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continuo de los mismos

- Leyes, regulaciones y contratos
- Revisiones regulares en cuanto a cambios
- Búsqueda de asistencia legal y modificaciones
- Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información
- Privacidad
- Propiedad intelectual
- Flujo de datos externos y criptografía

3.1.9. EVALUACIÓN DE RIESGOS

Objetivo: Asegurar el logro de los objetivos de las TIC y responder a las amenazas hacia la provisión de servicios de las TIC.

Para ello se logra la participación de la propia organización en la identificación de riesgos de las TIC y en el análisis de impacto, tomando medidas económicas para mitigar los riesgos y se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de las TIC (por ej.: tecnológicos, de seguridad, etc.) de manera de que se pueda determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable.
- Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos.
- Actualización de evaluación de riesgos.
- Metodología de evaluación de riesgos.
- Medición de riesgos cualitativos y/o cuantitativos.
- Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.
- Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

3.1.10. ADMINISTRACIÓN DE PROYECTOS

Objetivo: Establecer prioridades y entregar servicios oportunamente y de acuerdo al presupuesto de inversión.

Para ello se realiza una identificación y priorización de los proyectos en línea con el plan operacional por parte de la misma organización. Además, la organización deberá adoptar y aplicar sólidas técnicas de administración de proyectos para cada proyecto emprendido y se toma en consideración:

- Definición de un marco de referencia general para la administración de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos del tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.
- La involucración de los usuarios en el desarrollo, implementación o modificación de los proyectos.
- Asignación de responsabilidades y autoridades a los miembros del personal asignados al proyecto.
- Aprobación de fases de proyecto por parte de los usuarios antes de pasar a la siguiente fase.
- Presupuestos de costes y horas hombre.
- Planes y metodologías de aseguramiento de calidad que sean revisados y acordados por las partes interesadas.
- Plan de administración de riesgos para eliminar o minimizar los riesgos.
- Planes de prueba, entrenamiento, revisión post-implementación.

3.1.11. ADMINISTRACIÓN DE CALIDAD

Objetivo: Satisfacer los requerimientos del cliente.

Para ello se realiza una planificación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización y se toma en consideración:

- Definición y mantenimiento regular del plan de calidad, el cual deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

- Responsabilidades de aseguramiento de calidad que determine los tipos de actividades de aseguramiento de calidad tales como revisiones, auditorías, inspecciones, etc. que deben realizarse para alcanzar los objetivos del plan general de calidad.
- Metodologías del ciclo de vida de desarrollo de sistemas que rijan el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información.
- Documentación de pruebas de sistemas y programas.
- Revisiones y reportes de aseguramiento de calidad.

3.1.12. EL PLAN DE SISTEMAS TIC

Una herramienta fundamental para llevar a cabo la Planificación y Organización es el Plan de Sistemas TIC.

3.1.12.1. ¿Qué es el plan de sistemas TIC?

El plan de sistemas TIC es el documento que guía el esfuerzo coordinado de los especialistas en sistemas de información con los usuarios de los mismos sistemas a fin de satisfacer sus necesidades de captación, registro y proceso de datos para que cuenten con la información suficiente, confiable y oportuna para desarrollar sus tareas y tomar las decisiones que les competen.

El plan de sistemas TIC deberá incrementar la eficiencia en las diferentes áreas que integren la empresa o institución, suministrándoles la información de calidad, que requieren para desarrollar las acciones (ejecución) y tomar las decisiones en todas y cada una de las tareas que comprende el proceso administrativo: prever, planear, organizar, integrar, dirigir y controlar.

3.1.12.2. Cinco pasos para desarrollar el plan de sistemas TIC

En el proceso de desarrollo del plan de sistemas TIC intervienen:

- El personal del área de sistemas de información (gerente y analistas) que se encargan de recabar, analizar y diseñar los aspectos técnicos del plan. En el diagrama de flujo, previamente presentado, se denomina al personal del área de sistemas de información encargado del desarrollo del plan: “el informático”.

- Los usuarios, quienes solicitan les sean satisfechas sus necesidades de información para la mejor conducción y operación de aquello que está bajo su responsabilidad.
- Los integrantes del comité de informática, quienes fijan prioridades, normas y toman las decisiones fundamentales con respecto al plan. Suele ser muy recomendable integrar el comité de informática con el fin de que todas las áreas de la organización se vean representadas, y sean tomadas en cuenta en los proyectos de este tipo, lo cual suele evitar que la actividad de este departamento se sesgue a servir sólo, o fundamentalmente, al área del cual depende linealmente.
- Los proveedores de equipo, software y diversos elementos relacionados con la informática, a fin de que nos suministren la información y cotizaciones para efecto de presupuestación.

A continuación se presentan cinco pasos de un proceso estándar, mas no el único, que suelen seguir muchas organizaciones para desarrollar el plan de sistemas TIC.

1. El primer paso consiste en enterarse y tomar en cuenta las directrices que establecen tanto el plan estratégico general de la organización como la normatividad y estrategias a nivel superior.

La consideración de este nivel contesta las siguientes interrogantes:

- ¿Qué es y desea ser la organización (planificación estratégica)?
- ¿Cuáles son los principales retos a los que deberá enfrentarse?
- ¿Cuáles son las estrategias, prioridades y políticas generales de la empresa o institución?
- ¿Cuáles son los recursos que se podrán utilizar para satisfacer las necesidades TIC de toda la organización?

Asimismo, en este paso deberán analizarse los objetivos y requerimientos informáticos para cada una de las áreas funcionales cumpla con los objetivos que se establecieron en el plan estratégico del área, lo cual es útil para orientar la labor del especialista en sistemas de información el estudio correspondiente a cada área, y determinar las prioridades que cada sistema de información deba tener dentro del plan estratégico informática; este análisis provee respuesta a siguientes preguntas:

- ¿Cuáles son las áreas funcionales que integran a la organización?
- ¿Qué debe lograr cada área?

2. El segundo paso corresponde a la investigación de las necesidades específicas que en materia informática tienen todas y cada una de las áreas organizacionales, funciones, procesos y puestos que integran a la empresa o institución, para lo cual se procede a observar, aplicar cuestionario, hacer revisión documental y, en su caso, entrevistar al personal que corresponda, obteniendo la siguiente información:

- ¿Cuál es la situación actual de la organización y de cada área organizacional en lo que se refiere a sistemas de información?
- ¿Cuáles son las necesidades de información actuales y futuras por cada área, función, proceso y puesto?
- ¿Cuántos y cuáles recursos podrá destinar cada área al desarrollo, instalación y operación de las diferentes tareas que pueda comprender la satisfacción de sus necesidades informáticas?

El producto de este paso lo constituyen dos resultados:

- I. El diagnóstico de la situación de cada área y proceso con respecto a las aplicaciones informáticas con las que actualmente cuentan.
- II. Un inventario más o menos detallado de las necesidades de información en toda la organización y en cualquiera de los niveles.

3. El tercer paso corresponde al análisis de toda la información obtenida para determinar la viabilidad técnica, y en su caso económica, para satisfacer cada uno de los requerimientos en cuanto a los sistemas de información, que los diferentes usuarios hubiesen solicitado; además, en este paso deberá presentarse a grosso modo la manera de satisfacerlos, ya sea mediante procesos manuales que impliquen la racionalización de las operaciones, sistemas mecanizados o sistemas informáticos computerizados.

En este paso se desarrolla el análisis de la factibilidad de cada aplicación desde el punto de vista:

- Técnico: Acceso a los datos, las aplicaciones, el hardware y las instalaciones.
- Económico: Evaluando el costo y beneficios de cada aplicación.
- Operacional: Evaluación de si la solución deseada es posible de acuerdo con las condiciones y restricciones que presenta la organización.

4. El cuarto paso consiste en el desarrollo conceptual de las diversas soluciones informáticas, indicando aquellas que puedan ser adquiridas a modo de paquetería y las que necesariamente deban ser desarrolladas, ya sea mediante recursos internos o con la participación de terceros.

Con base en la experiencia y en la investigación que se haga, con respecto a cada solución (aplicación informática), deberá calcularse el monto de la inversión y gasto que cada aplicación informática tendría para, con base en esto, hacer un presupuesto general del plan.

El diseño del sistema incluye:

- El diseño lógico: datos, procesos y resultados (entradas/procesos/ salidas)
- Operación del usuario: simplicidad, eficiencia y detección de errores.
- Diseño de la base de datos: Relación lógica entre los datos, requerimientos de volumen y rapidez, diseño y organización de los archivos y especificaciones de los registros.
- El diseño físico: Equipo y su localización.

5. El quinto y último paso comprende la presentación del proyecto del plan de sistemas TIC al comité de informática, que hace el personal del área de sistemas, con el fin de que dicho comité lo evalúe y, en su caso, determine las modificaciones que convengan y lo apruebe, para que sea considerado como el plan maestro que deberá regir las actividades relacionadas con la informática en la organización durante el periodo que el plan comprende.

Es importante mencionar que un plan no está completo si le falta el programa de actividades y el presupuesto con su flujo de efectivo.

Asimismo, los integrantes del comité deberán conocer y considerar los recursos con que cuente la organización para satisfacer dichas necesidades de información (recursos tecnológicos, humanos y financieros).

Para efecto de cómo deba presentarse el plan de sistemas TIC, posteriormente comentaremos un documento estándar que suele utilizarse con frecuencia.

Debido a que la función de sistemas de información organizacionalmente constituye un departamento de servicio a todas las demás áreas de la empresa o institución, tanto sus alcances como los resultados tienen efecto indirecto en todas las áreas de la organización, mediante el suministro de información que les permita tomar mejores decisiones, planear y coordinar mejor el trabajo, así como tener un óptimo control de las actividades que comprende.

Un buen plan de sistemas TIC deberá dar respuesta a las siguientes preguntas:

- ¿Qué información requieren o es conveniente a cada una de las áreas, funciones, procesos y puestos que integran la organización?
- ¿Cada cuánto requieren esa información?
- ¿En dónde se requiere esa información?
- ¿Con qué presentación la requieren para hacerla más amigable y útil para el usuario?
- ¿En dónde se encuentran los datos relativos a cada tipo de información?
- ¿Cuál es el proceso que deberá hacerse para captar, registrar y obtener los resultados informáticos deseados?
- ¿Cómo pueden satisfacerse las diversas necesidades informáticas de la organización?
- ¿Cuánto tiempo llevaría satisfacer esas necesidades?
- ¿Cuánto costaría satisfacer las necesidades informáticas?
- ¿Cuál debe ser la participación de los usuarios y del personal del área de sistemas de información?

El plan de sistemas TIC tiene por objeto responder a las siguientes preguntas:

- ¿A qué áreas, procesos, funciones y/o puestos deberá darse respaldo en lo que se refiere a la instalación, mantenimiento y operación de sistemas de información?
- ¿Qué tipo de recursos informáticos (computerizados y no computerizados) deberán tenerse?
- ¿Cuál puede ser el costo y el beneficio de cada aplicación informática?
- ¿En cuanto tiempo y cuándo deberán satisfacerse las necesidades de proceso de información de las diferentes áreas, funciones, procesos y puestos (programa de actividades)?
- ¿Cuál será la inversión total y por aplicación que deberá realizarse para contar con las ventajas y funcionalidades que pretende el plan?
- ¿Quiénes tienen algún tipo de responsabilidad en el desarrollo de las acciones previstas por el plan de sistemas TIC?

3.1.12.3. Documento estándar del plan de sistemas TIC

No existe un documento único para presentar el plan de sistemas TIC, esto depende de los propósitos, formación y gusto de quien lo desarrolla; no obstante lo anterior, a continuación presentamos un documento estándar que presenta elementos comunes en muchos de los planes informáticos.

1. Carátula: Identifica el documento como plan de sistemas TIC indicando el nombre de la organización y el periodo que comprende.
2. Índice: Referencia cada elemento del plan de sistemas TIC indicando el número de página que le corresponde.
3. Resumen ejecutivo: Contiene el extracto del plan en un máximo de cuatro hojas, con el fin de reducir el tiempo y esfuerzo requerido para que la dirección general y alta gerencia se enteren fácil y rápidamente del contenido del plan sin necesidad de leer todo el documento. La persona que desee o requiera enterarse con mayor detalle de un determinado aspecto, podrá consultar el índice y dirigirse a la parte del plan que contenga la información en detalle que requiera.
4. Objetivos que se pretenden lograr con el plan de sistemas TIC tanto a nivel general como por cada una de las áreas, funciones o procesos.

Un buen plan debe anticiparse a las demandas del futuro, administrar bien implica prever el futuro y resolver de antemano los problemas y/o escasez que pudiesen presentarse.

5. Estrategias aplicables al esfuerzo informático y, en su caso, la descripción de las políticas informáticas que deberán seguirse en cuanto a equipo, programación y contratación de servicios relacionados.
Identifique las unidades clave del negocio, las cuales deban tener una mayor prioridad y cuidado en la oportuna satisfacción de sus necesidades informáticas.

6. Descripción de la situación actual en la que se encuentran los sistemas de información operados en la organización, mencionando el nivel en que éstos satisfacen las necesidades de los diferentes usuarios, así como los problemas y limitaciones que se presentan.

7. Relación de requerimientos informáticos y descripción de las aplicaciones cuyo objeto sea la satisfacción de cada uno de esos requerimientos.

En requerimientos informáticos deberán describirse tanto los actuales como aquellos previstos por la evolución, modernización y dinámica de crecimiento de la organización.

Es recomendable hacer un análisis de costo/beneficio por cada una de las aplicaciones informáticas a implementar. Este estudio será útil para que el comité determine prioridades y la conveniencia “económica” de desarrollar o no desarrollar una determinada aplicación.

8. Programa general de las actividades que deban ser desarrolladas dentro del plan, indicando su duración, fecha de inicio, revisión y terminación, recursos necesarios y responsables en cada subproyecto.

Dependiendo de la situación de la cual se parta y de los objetivos que se deseen alcanzar, el desarrollo del plan de sistemas TIC puede consistir:

- En una simple automatización donde se transfieren los procesos manuales al ordenador.
- Conversión en donde se pasan y adaptan sistemas computerizados de un equipo a otro o de un sistema computerizado (paquete) a otro.
- Un proceso de racionalización donde se pretende mejorar el desempeño en cada sistema informático, incluyendo los procesos no computerizados.
- En la reingeniería de los sistemas buscando el óptimo desempeño, desarrollando nuevas aplicaciones informáticas.

Cuando el plan comprende el desarrollo de nuevas aplicaciones que deban correr en un equipo de cómputo, en el programa de informática deberán especificarse; en secuencia los tiempos correspondientes al:

- Análisis del sistema.
- Diseño del sistema:
 - o Procesos.
 - o Programas.
 - o Archivos o base de datos.
- Diseño de resultados:
 - o Impresos.
 - o Desplegados por pantalla.
 - o Informes multimedia.
- Programación: traducir las necesidades de tratamiento a los datos en códigos inteligibles para el ordenador.

- Prueba de cada unidad o programa, prueba de cada proceso y prueba general, tanto con datos de prueba como con datos y volúmenes reales de la información que deba ser procesada; paralelo de procesos y prueba piloto.
- Conversión de datos cuando esto es requerido.
- Carga o captura de registros maestros.
- Entrenamiento o capacitación a usuarios.
- Tiempos en paralelo, cuando deba operarse durante algún tiempo, tanto con el nuevo sistema como con el anterior.
- Liberación o puesta en producción de la aplicación, con la revisión constante de que el sistema satisface las necesidades informáticas del usuario.
- Documentación de los sistemas que incluye la formulación de al menos los manuales: técnico y de operación.
- Mantenimiento para resolver cualquier inconsistencia o error oculto en el nuevo sistema, y para mantenerlo actualizado.

Cuando hay alguna adición o cambio de equipo deben considerarse los costos y tiempos relacionados con ello, como son la instalación física y de software básico y aplicativo, puesta a punto, entrenamiento para los nuevos equipos, etcétera.

En el caso de adquirir paquetes de software, el ahorro de tiempo consiste esencialmente en el que se dedicaría al análisis y a la programación, pero es común que sea necesario considerar el esfuerzo relacionado con la adaptación de la paquetería, la capacitación de los usuarios y la instalación del paquete hasta su liberación, que es el momento en que el usuario opera por sí mismo el sistema sin requerir de manera constante del especialista informático.

En el programa de actividades deberán resaltarse las fechas y tiempos de revisión de avance para asegurar que las cosas vayan dándose conforme a lo planeado y requerido.

9. Presupuesto requerido: con indicación pormenorizada por partida y tiempo de los cargos que deberán hacerse para que opere el plan de sistemas TIC, que incluye el hardware local y para telecomunicaciones, software, servicios y al personal (sueldos, salarios, etcétera).

10. Anexos: comprende documentos con diversa información, como la especificación de equipos, proveedores, legislación y normatividad aplicable en aspectos como las telecomunicaciones, disponibilidad de líneas, servicios de Internet, etcétera.

La descripción de los recursos de equipo (hardware) requeridos, incluyendo CPU, capacidad de memoria, velocidad de proceso, espacio para almacenamiento secundario, dispositivos de respaldo, impresoras, equipo de comunicaciones, facilidades de Internet, equipo auxiliar, insumos misceláneas, etcétera.

Es recomendable incluir un esquema resumido de las aplicaciones propuestas, cuando se cuente con algún adelanto respecto al análisis y diseño de las mismas, a fin de brindar a la dirección mayores elementos para evaluar los alcances del plan.

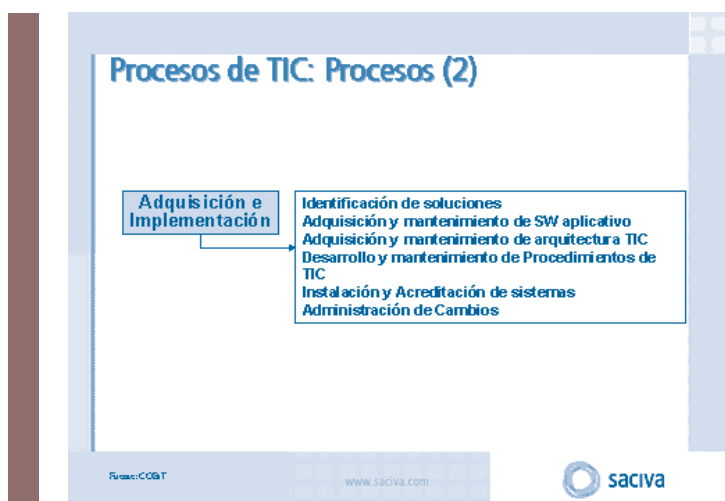
El detalle del diseño de cada aplicación informática aparecerá en la documentación respectiva, la cual deberá tenerse disponible de acuerdo con las fechas establecidas en el calendario correspondiente al programa general de actividades.

Las especificaciones técnicas de, cada diseño de sistema Informático aparecen con todo detalle en la documentación correspondiente a cada sistema informático que se vaya desarrollando. A continuación se enlistan algunos de los elementos que usualmente forman parte de la documentación detallada de los sistemas de información computerizados.

- La descripción de la base de datos, con su tipología, datos, diseño de registros, tipos de datos, longitudes, campos clave, etcétera.
- Flujos para cada proceso y general, instrucciones de operación, parámetros, estándares de programación, diagramas de bloque y de programación estructurada, etcétera.
- Diseño de paneles de control y desplegados visuales, así como fases, pasos y parámetros para procesos interactivos.
- Diseño de informes impresos con sus características, datos que contienen periodicidad y, eventualmente, relación de usuarios.
- Diseños multimedia con imágenes, sonido y video.
- Facilidades adicionales del sistema, como son generador de impresos, gráficas y consultas esporádicas.

3.2. ADQUISICIÓN E IMPLEMENTACIÓN

Para llevar a cabo la estrategia de las TIC, las soluciones de las TIC deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.



3.2.1. IDENTIFICACIÓN DE SOLUCIONES AUTOMATIZADAS

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario.

Para ello se realiza un análisis claro de las oportunidades alternativas comparadas contra los requerimientos de los usuarios y toma en consideración:

- Definición de requerimientos de información para poder aprobar un proyecto de desarrollo.
- Estudios de factibilidad con la finalidad de satisfacer los requerimientos del negocio establecidos para el desarrollo de un proyecto.

- Arquitectura de información para tener en consideración el modelo de datos al definir soluciones y analizar la factibilidad de las mismas.
- Seguridad con relación de coste-beneficio favorable para controlar que los costes no excedan los beneficios.
- Pistas de auditoría para ello deben existir mecanismos adecuados. Dichos mecanismos deben proporcionar la capacidad de proteger datos sensibles (ej. Identificación de usuarios contra divulgación o mal uso).
- Contratación de terceros con el objeto de adquirir productos con buena calidad y excelente estado.
- Aceptación de instalaciones y tecnología a través del contrato con el Proveedor donde se acuerda un plan de aceptación para las instalaciones y tecnología específica a ser proporcionada.

3.2.2. ADQUISICIÓN Y MANTENIMIENTO DEL SOFTWARE APLICATIVO

Objetivo: Proporciona funciones automatizadas que soporten efectivamente al negocio.

Para ello se definen declaraciones específicas sobre requerimientos funcionales y operacionales y una implementación estructurada con entregables claros y se toma en consideración:

- Requerimientos de usuarios, para realizar un correcto análisis y obtener un software claro y fácil de usar.
- Requerimientos de archivo, entrada, proceso y salida.
- Interfase usuario-maquina asegurando que el software sea fácil de utilizar y que sea capaz de auto documentarse.
- Personalización de paquetes.
- Realizar pruebas funcionales (unitarias, de aplicación, de integración y de carga y estrés), de acuerdo con el plan de prueba del proyecto y con los estándares establecidos antes de ser aprobado por los usuarios.
- Controles de aplicación y requerimientos funcionales
- Documentación (materiales de consulta y soporte para usuarios) con el objeto de que los usuarios puedan aprender a utilizar el sistema o puedan sacarse todas aquellas inquietudes que se les puedan presentar.

3.2.3. ADQUISICIÓN Y MANTENIMIENTO DE LA INFRAESTRUCTURA TECNOLÓGICA

Objetivo: Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general.
- Mantenimiento preventivo del hardware con el objeto de reducir la frecuencia y el impacto de fallas de rendimiento.
- Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

3.2.4. DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS

Objetivo: Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.
- Manuales de Operaciones y controles, de manera que estén en permanente actualización.
- Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria.

3.2.5. INSTALACIÓN Y ACEPTACIÓN DE LOS SISTEMAS

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado.

Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas y toma en consideración:

- Capacitación del personal de acuerdo al plan de entrenamiento definido y los materiales relacionados.
- Conversión / carga de datos, de manera que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.
- Pruebas específicas (cambios, desempeño, aceptación final, operacional) con el objeto de obtener un producto satisfactorio.
- Acreditación de manera que La Dirección de operaciones y usuaria acepten los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.
- Revisiones post implementación con el objeto de reportar si el sistema proporciono los beneficios esperados de la manera mas económica.

3.2.6. ADMINISTRACIÓN DE LOS CAMBIOS

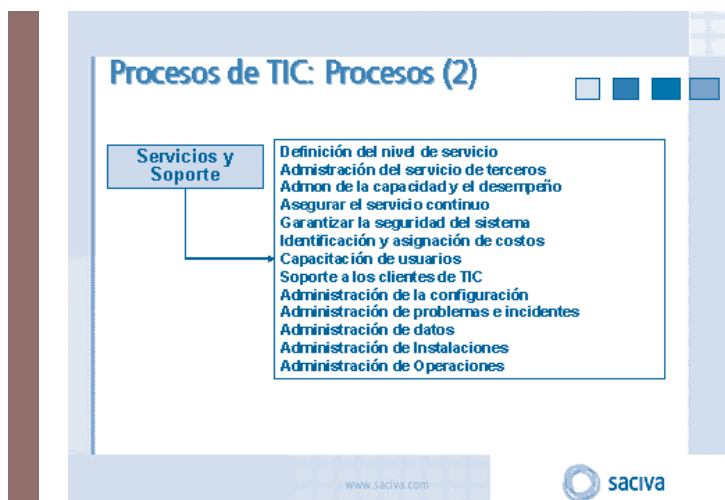
Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores.

Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de las TIC actual y toma en consideración:

- Identificación de cambios tanto internos como por parte de proveedores.
- Procedimientos de categorización, priorización y emergencia de solicitudes de cambios.
- Evaluación del impacto que provocaran los cambios.
- Autorización de cambios.
- Manejo de liberación de manera que la liberación de software este regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega, etc.
- Distribución de software, estableciendo medidas de control específicas para asegurar la distribución de software correcto al lugar correcto, con integridad y de manera oportuna.

3.3. PRESTACIÓN Y SOPORTE

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.



3.3.1. DEFINICIÓN DE NIVELES DE SERVICIO

Objetivo: Establecer una comprensión común del nivel de servicio requerido.

Para ello se establecen convenios de niveles de servicio que formalicen los criterios de desempeño contra los cuales se medirá la cantidad y la calidad del servicio y se toma en consideración:

- Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable

de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.

- Definición de las responsabilidades de los usuarios y de la función de servicios de información.
- Procedimientos de desempeño que aseguren que la manera y las responsabilidades sobre las relaciones que rigen el desempeño entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.
- Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.
- Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicios contra su coste.
- Garantías de integridad.
- Convenios de confidencialidad.
- Implementación de un programa de mejoramiento del servicio.

3.3.2. ADMINISTRACIÓN DE SERVICIOS PRESTADOS POR TERCEROS

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.

Para ello se establecen medidas de control dirigidas a la revisión y Monitorización 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 servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, Monitorización y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.
- Acuerdos de confidencialidad. Además, se deberá calificar a los terceros y el contrato deberá definirse y acordarse para cada relación de servicio con un proveedor.

- Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- Monitorización de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

3.3.3. ADMINISTRACIÓN DEL DESEMPEÑO Y LA CAPACIDAD

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.

Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos y toma en consideración:

- Requerimientos de disponibilidad y desempeño de los servicios de sistemas de información.
- Monitorización y reporte de los recursos de tecnología de información.
- Utilizar herramientas de modelado apropiadas para producir un modelo del sistema actual para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de configuración, desempeño y disponibilidad.
- Administración de capacidad estableciendo un proceso de planificación para la revisión del desempeño y capacidad de hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar cargas de trabajo con cantidad y calidad de desempeño.
- Prevenir que se pierda la disponibilidad de recursos mediante la implementación de mecanismos de tolerancia de fallas, de asignación equitativos de recursos y de prioridad de tareas.

3.3.4. ASEGURAR EL SERVICIO CONTINUO

Objetivo: mantener el servicio disponible de acuerdo con los requerimientos y continuar su provisión en caso de interrupciones.

Para ello se tiene un plan de continuidad probado y funcional, que esté alineado con el plan de continuidad del negocio y relacionado con los requerimientos de negocio y toma en consideración:

- Planificación de Severidad
- Plan Documentado
- Procedimientos Alternativos
- Respaldo y Recuperación
- Pruebas y entrenamiento sistemático y singulares

3.3.5. GARANTIZAR LA SEGURIDAD DE SISTEMAS

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida.

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- El autenticación y Autorización, acceso lógico junto con el uso de los recursos de las TIC deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso.
- Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario.
- Administración de llaves criptográficas definiendo implementando procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas.
- Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos.
- Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.
- Firewalls si existe una conexión con Internet u otras redes públicas en la organización de Utilización.

3.3.6. EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados.

Para ello se realiza un plan completo de entrenamiento y desarrollo y se toma en consideración:

- Currículum de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información.
- Campañas de concienciación, definiendo los grupos objetivos, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento.
- Técnicas de concienciación proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

3.3.7. IDENTIFICACIÓN Y ASIGNACIÓN DE COSTES

Objetivo: Asegurar un conocimiento correcto de los costes atribuibles a los servicios de las TIC.

Para ello se realiza un sistema de contabilidad de costes que asegure que éstos sean registrados, calculados y asignados a los niveles de detalle requeridos y toma en consideración:

- Los elementos sujetos a cargo deben ser recursos identificables, medibles y predecibles para los usuarios.
- Procedimientos y políticas de cargo que fomenten el uso apropiado de los recursos de computo y aseguren el trato justo de los departamentos usuarios y sus necesidades.
- Tarifas definiendo e implementando procedimientos de gestión de costes de prestar servicios, para ser analizados, monitoreados, evaluados asegurando al mismo tiempo la economía.

3.3.8. APOYO Y ASISTENCIA A LOS CLIENTES DE LAS TIC

Objetivo: asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente.

Para ello se realiza un Buró de ayuda que proporcione soporte y asesoría de primera línea y toma en consideración:

- Consultas de usuarios y respuesta a problemas estableciendo un soporte de una función de buró de ayuda.

- Monitorización de consultas y despacho estableciendo procedimientos que aseguren que las preguntas de los clientes que pueden ser resueltas sean reasignadas al nivel adecuado para atenderlas.
- Análisis y reporte de tendencias adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias.

3.3.9. ADMINISTRACIÓN DE LA CONFIGURACIÓN

Objetivo: Dar cuenta de todos los componentes de las TIC, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios.

Para ello se realizan controles que identifiquen y registren todos los activos de las TIC así como su localización física y un programa regular de verificación que confirme su existencia y toma en consideración:

- Registro de activos estableciendo procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de adquisición.
- Administración de cambios en la configuración asegurando que los registros de configuración reflejen el status real de todos los elementos de la configuración.
- Chequeo de software no autorizado revisando periódicamente los ordenadores personales de la organización.
- Controles de almacenamiento de software definiendo un área de almacenamiento de archivos para todos los elementos de software válidos en las fases del ciclo de vida de desarrollo de sistemas.

3.3.10. ADMINISTRACIÓN DE PROBLEMAS

Objetivo: Asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

3.3.11. ADMINISTRACIÓN DE DATOS

Objetivo: Asegurar que los datos permanezcan completos, precisos y válidos durante su entrada, actualización, salida y almacenamiento.

Lo cual se logra a través de una combinación efectiva de controles generales y de aplicación sobre las operaciones de las TIC. Para tal fin, La Dirección deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen los errores y las omisiones durante la creación de los datos.

Este proceso deberá controlar los documentos fuentes (de donde se extraen los datos), de manera que estén completos, sean precisos y se registren apropiadamente. Se deberán crear también procedimientos que validen los datos de entrada y corrijan o detecten los datos erróneos, como así también procedimientos de validación para transacciones erróneas, de manera que éstas no sean procesadas. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.

La Dirección deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

3.3.12. ADMINISTRACIÓN DE INSTALACIONES

Objetivo: Proporcionar un ambiente físico conveniente que proteja al equipo y al personal de las TIC contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

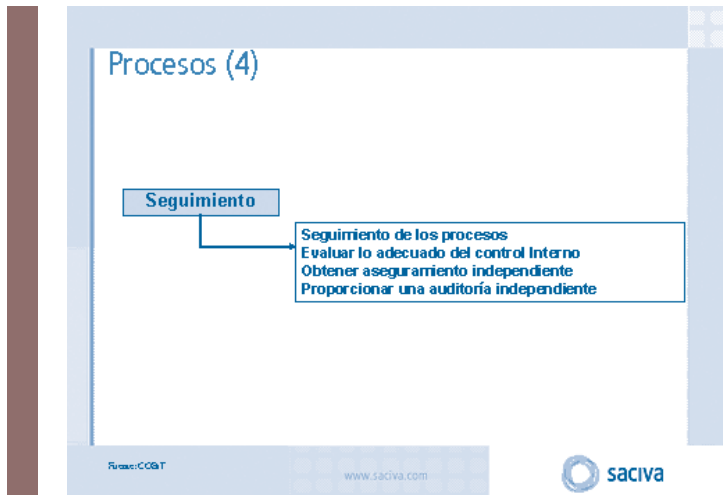
3.3.13. ADMINISTRACIÓN DE LA OPERACIÓN

Objetivo: Asegurar que las funciones importantes de soporte de las TIC estén siendo llevadas a cabo regularmente y de una manera ordenada.

Esto se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, La Dirección deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

3.4. MONITORIZACIÓN

Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad. Este es, precisamente, el ámbito de este dominio.



3.4.1. SEGUIMIENTO DEL PROCESO

Objetivo: Asegurar el logro de los objetivos establecidos para los procesos de las TIC. Lo cual se logra definiendo por parte de La Dirección reportes e indicadores de desempeño y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.

Para ello La Dirección podrá definir indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización. La Dirección deberá también medir el grado de satisfacción de los clientes con respecto a los servicios de información proporcionados para identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento, confeccionando informes que indiquen el avance de la organización hacia los objetivos propuestos.

3.4.2. EVALUAR LO ADECUADO DEL CONTROL INTERNO

Objetivo: Asegurar el logro de los objetivos de control interno establecidos para los procesos de las TIC.

Para ello La Dirección es la encargada de monitorear la efectividad de los controles internos a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias., evaluar su efectividad y emitir reportes sobre ellos en forma regular. Estas actividades de Monitorización continuo por parte de La Dirección deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

3.4.3. OBTENCIÓN DE ASEGURAMIENTO INDEPENDIENTE

Objetivo: Incrementar los niveles de confianza entre la organización, clientes y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

Para ello La Dirección deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos, como así también para trabajar con nuevos proveedores de servicios de tecnología de información. Luego, la Dirección deberá adoptar como trabajo rutinario tanto hacer evaluaciones periódicas sobre la efectividad de los servicios de tecnología de información y de los proveedores de estos servicios como así también asegurarse el cumplimiento de los compromisos contractuales de los servicios de tecnología de información y de los proveedores de estos servicios.

3.4.4. PROVEER AUDITORÍA INDEPENDIENTE

Objetivo: Incrementar los niveles de confianza y beneficiarse de recomendaciones basadas en mejores prácticas de su implementación, lo que se logra con el uso de auditorías independientes desarrolladas a intervalos regulares de tiempo. Para ello La Dirección deberá establecer los estatutos para la función de auditoría, destacando en este documento la responsabilidad, autoridad y obligaciones de la auditoría. El auditor deberá ser independiente del auditado, esto significa que los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado y en lo posible deberá ser independiente de la propia empresa. Esta auditoría deberá respetar la ética y los estándares profesionales, seleccionando para ello auditores que sean técnicamente competentes, es decir que cuenten con habilidades y conocimientos que aseguren tareas efectivas y eficientes de auditoría.

La función de auditoría deberá proporcionar un reporte que muestre los objetivos de la auditoría, período de cobertura, naturaleza y trabajo de auditoría realizado, como así también la organización, conclusión y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo.

Los 34 procesos propuestos se concretan en los 32 objetivos de control detallados anteriormente.

Un Control se define como "las normas, estándares, procedimientos, usos y costumbres y las estructuras organizativas, diseñadas para proporcionar garantía razonable de que los objetivos empresariales se alcancen y que los eventos no deseados se prevengan o se detecten, y corregirán".

Un Objetivo de Control se define como "la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de las TIC".

LA IMPORTANCIA DE LA ASESORÍA EXTERNA



4.

La importancia de la asesoría externa

Resulta evidente a la vista de lo expuesto que un factor crítico para el éxito del aseguramiento de la inversión es preciso contar con el adecuado nivel de asesoría experta.

Esta asesoría puede ubicarse dentro de la propia empresa pero resulta generalmente más recomendable acudir a empresas especializadas en el asesoramiento en TIC. No es función del empresario saber de todo, pero sí es su responsabilidad hacer lo preciso.

ENTIDADES A DISPOSICIÓN DE LOS EMPRESARIOS DE CANTABRIA

SODERCAN, S.L., Sociedad para el Desarrollo Regional de Cantabria, participada por la Consejería de Industria, Trabajo y Desarrollo Tecnológico.
Hernán Cortés, 39. 39003 Santander - Cantabria
Teléf.: +34 942 290 003 - fax: +34 942 219 704
información@sodercan.com

CEOE-CEPYME Cantabria, la Confederación de Empresarios de Cantabria.
C/ Rualasal, 8 - planta 6.^a - 39001 Santander - Cantabria
Teléf.: +34 942 365 305 - fax: +34 942 365 080
ceocant@ceocant.es
www.ceocant.es

Manual promovido por la Consejería de Industria, Trabajo y Desarrollo Tecnológico del Gobierno de Cantabria y CEOE-CEPYME Cantabria en el marco del Acuerdo de Concertación Social.

Elaborado por:

ESPYME INTERNACIONAL S.L. y SACIVA ASESORES S.L.

© CEOE-CEPYME Cantabria 2004

Edita:

CEOE-CEPYME Cantabria

Rualasal 8, Planta 6ª

39001 Santander

Tel.: +34 942 365 365

Fax: + 34 942 365 080

e-mail: ceocant@ceocant.es

www.ceocant.es

Maquetación e impresión: Gráficas Calima, S. A.

D. Legal: SA-15-2005