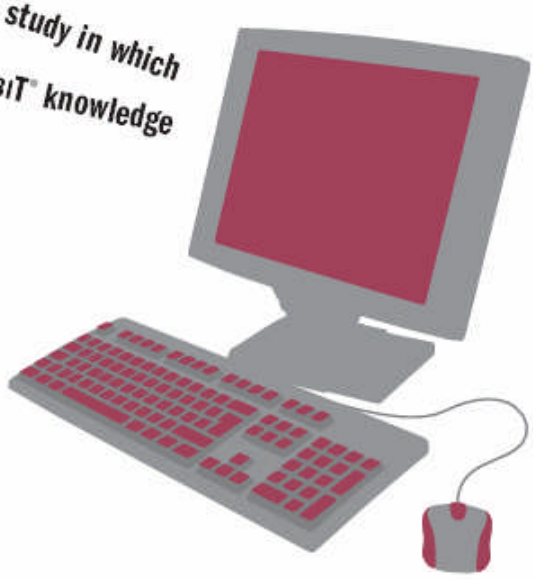
GOBIERNO DE TI UTILIZANDO COBIT® Y VAL IT™:

TIBO CASO DE ESTUDIO,

2DA EDICION

An extended case study in which students can apply their COBIT® knowledge



GOVERNANCE INSTITUTE®
LEADING THE IT GOVERNANCE COMMUNITY

Reconocimientos

IT Governance Institute®
El TI Governance Institute (ITGI™) (*www.itgi.org*) se estableció en 1998 para promover el avance del pensamiento internacional y estándares para dirigir y controlar las tecnologías de la información de las empresas. El gobierno efectivo de las TI ayuda a asegurar que las TI soportan los objetivos del negocio, optimizan las inversiones en TI y gestionan los riesgos y oportunidades relacionados con las TI de manera apropiada. ITGI ofrece investigación original y casos de estudio para ayudar a los líderes y Juntas Directivas de las empresas en sus responsabilidades de gobierno de TI.

Limitación de Responsabilidad
ITGI y los autores de *Gobierno de TI utilizando COBIT® y Val IT™: TIBO – Caso de Estudio, 2da Edición*, han concebido esta publicación primordialmente como un recurso educativo para educadores. ITGI, ISACA® y los autores no declaran que la utilización de este producto asegurará un resultado exitoso. La publicación no debería ser considerada como conteniendo todos los procedimientos y pruebas apropiadas ni omitiendo todos los procedimientos o pruebas apropiadas que están razonablemente orientados a obtener los mismos resultados. Al determinar la conveniencia de un procedimiento o prueba específica, el/la profesional del control debería aplicar su propio juicio profesional a la circunstancia de control específica presentada por un sistema en particular o un entorno de TI. Se hace notar que esa publicación es una actualización de *CobiT® in Academia: TIBO Case Study.*

Revelación

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *research@isaca.org*
Web sites: *www.itgi.org* and *www.isaca.org*

ISBN 978-1-60420-025-6
Gobierno de TI utilizando COBIT® y Val IT™: TIBO – Caso de Estudio, 2da Edición
Printed in the United States of America

Reconocimientos

ITGI Desea Reconocer a:

Researcher
Ed O'Donnell, University of Kansas, USA

Contribuitors
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA
Steven De Haes, University of Antwerp Management School, Belgium
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Robert Parker, CISA, CA, CMC, FCA, Canada
V. Sambamurthy, Ph.D., Michigan State University, USA
Scott Lee Summers, Ph.D., Brigham Young University, USA
John Thorp, The Thorp Network, Canada
Wim Van Grembergen, Ph.D., University of Antwerp (UA) and University of Antwerp Management School (UAMS) and TI Alignment and Governance Research Institute (ITAG), Belgium
Ramesh Venkataraman, Ph.D., Indiana University, USA

ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FH KIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart, IV, CISA, CISM, CIPP/G, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

ITGI Advisory Panel
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

Reconocimientos

Academic Relations Committee
Scott Lee Summers, Ph.D., Brigham Young University, USA, Chair
Casey G. Cegielski, Ph.D., CISA, Auburn University, USA
Patrick Hanrion, CISM, CISSP, CNE, MCSE, Microsoft, USA
Donna Hutcheson, CISA, XR Group Inc., USA
Cejka Jiri Josef, CISA, Dipl. El. -Ing., KPMG Fides Peat, Switzerland
Michael Lambert, CISA, CISM, CARRA, Canada
Ed O'Donnell, University of Kansas, USA
Theodore Tryfonas, Ph.D., CISA, University of Glamorgan, Wales
Ramesh Venkataraman, Ph.D., Indiana University, USA

CobiT Steering Committee
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Steven DeHaes, University of Antwerp Management School, Belgium
Rafael Eduardo Fabius, CISA, Republica AFAP, S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, TI Winners, South Africa
Jimmy Heschl, CISM, CISA, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

Reconocimientos

ITGI Affiliates and Sponsors
ISACA chapters
American Institute for Certified
Public Accountants ASIS
International
The Center for Internet Security
Commonwealth Association of Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of
Management
Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp
Management School
Aldion Consulting
Pte. Ltd.
CA Inc.
Hewlett-Packard
IBM
ITpreneurs Nederlands BV
LogLogic Inc.
Phoenix Business and
Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass TI Solutions

Reconocimientos

Este Trabajo ha sido traducido al español por Ricardo Bría (Ricardo.Bria@gmail.com) de la versión en inglés de '*Gobierno de TI utilizando COBIT® y Val IT™: TIBO – Caso de Estudio, 2da Edición*', con permiso de ITGI. Ricardo Bría asume toda la responsabilidad de la exactitud y fidelidad de la traducción.

This Work is translated by Ricardo Bría (Ricardo.Bria@gmail.com) into Spanish from the English language version of '*IT Governance Using COBIT® and Val IT™: TIBO - Case Study2nd Edition*' with the permission of the IT Governance Institute. Ricardo Bría assumes sole responsibility for the accuracy and faithfulness of the translation.

TABLA DE CONTENIDO

Contenido

1. PROPOSITO DEL DOCUMENTO

El *Caso de Estudio TIBO, 2 da Edición* es un producto desarrollado el ITGI, en colaboración con un grupo de académicos y especialistas internacionales, como parte de *Gobierno de TI utilizando COBIT® y Val IT™*. El objetivo de este documento es presentar un caso de estudio completo (incluyendo la descripción del caso, preguntas a los alumnos y amplias notas para el Profesor) en el cual los alumnos puedan aplicar su conocimiento de COBIT a una situación práctica. Este caso puede ser integrado dentro del Programa de estudios de las carreras en Sistemas de Información, Seguridad de la Información, Auditoría, Auditoría de Sistemas de Información y/o Sistemas de Información Contable.

Este caso ha sido diseñado para ser utilizado primariamente en cursos de Post Grado.

El caso también podría ser utilizado en clases de Grado, siempre que los alumnos hayan estado lo suficientemente expuestos a conceptos de control interno en un entorno de IT, marcos generales de control y COBIT en particular.

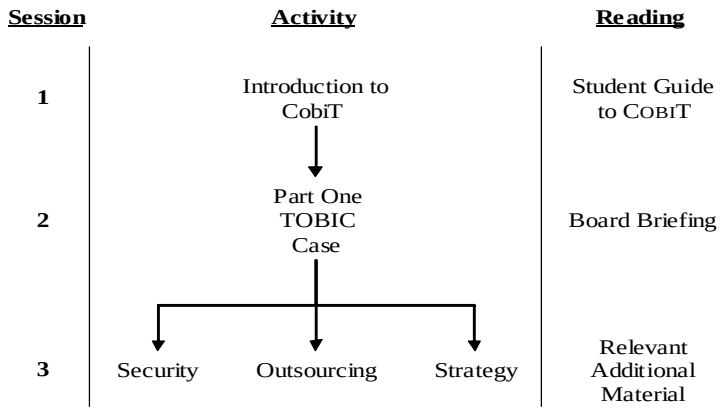
El caso ha sido diseñado para mapear el libro *Gobierno de TI utilizando COBIT® y Val IT™: TIBO–Caso de Estudio, 2 da Edición,* que explica todos los elementos de COBIT y que también ha sido desarrollado por el ITGI. El material de este caso se nutre directamente de los procesos de TI de COBIT.

Se sugiere que el caso se presente en una o posiblemente dos clases (ver **Figura 1-Mapa Sugerido del Caso**), luego de la presentación de COBIT (sesión 0). Se sugiere también que la primera parte del caso sea cubierta en una clase de aproximadamente 1.5 horas. A los alumnos se le deberá entregar previamente, como material de lectura, el caso de estudio y el *Board Briefing on IT Governance 2 Edition*[1], y posteriormente en clase, las preguntas relacionadas con cada uno de los asuntos que trata el Caso: seguridad, servicios a terceros, alineación estratégica (incluidos en la Sección de Material Adicional). Las preguntas podrán ser discutidas de manera interactiva en una segunda sesión o en presentaciones de pequeños grupos. En las Notas para el Profesor se provee material adicional de lectura y soluciones sugeridas para cada una de las partes del Caso.

El ITGI ha desarrollado tres productos adicionales que pueden acompañar a este Caso de estudio en la serie de documentos sobre *Gobierno de TI utilizando COBIT® y Val IT™* para académicos:

- *Libro para el estudiante, 2 da Edición*
- *Presentación,2 da Edición, 35 slides de PowerPointo sobre COBIT*
- *Mini Casos, 2 da Edición, para ejercicios más pequeños de COBIT, o para ser utilizados para alumnos de grado o post grado.*

Figura 1-Mapa Sugerido del Caso



[1] ITGI, Board Briefing on IT Governance, 2nd Edition, USA, 2003

2. Descripciones del Caso de Estudio

UN DIA EN LA VIDA DE LA HISTORIA DE LA SUBCONTRATACION DE TIBO

Era evidente que el Chief Executive Officer (CEO) del Trusted Imperial Banking Organisation (TIBO), John Mitchell, no estaba de humor para charlas cordiales. El Director de IT, Steven De Haes, fue convocado de manera urgente a la oficina del CEO en la Planta 30 del edificio central del Banco en el distrito financiero de Londres por la asistente personal del CEO, Pyms Forsythe. De Haes tenía un presentimiento acerca del motivo cuando Forsythe lo llamó a la reunión minutos antes. Forsythe le dijo, "Mitchell ha recibido la Encuesta de Defensa del Consumidor Financiero (Financial Ombudsman Survey)[2] y ha estado hablando por teléfono con el Vicepresidente Senior (SVP) de Banca Personal (BP) desde entonces. No está muy contento, y tu estrambótico Web-enabled Banking Operations (We-BOP) creo que está más muerto que vivo. De todas manera, quiere verte ya."

De Haes sabía que el SVP de BP, Wim Van Grembergen, no era amigo de IT. El área de TI había estado trabajando en el We-BOP para BP desde hace un año, para enfrentar a una dura competencia por clientes en el Reino Unido. La competencia provenía no solo de las ofertas de Internet de algunos Bancos, sino también de Bancos Online. A De Haes le hubiera gustado que su jefe, el Chief Operating Officer (COO), Erik Guldentops, estuviera con el, pero estaba de viaje fuera del país (otra vez). Bruscamente, Mitchell dijo: "Qué demonios estáis haciendo en TI con We-BOP? Me ha llamado el Defensor del Consumidor para decirme que está trabajando en una Reclamación formal por nuestro servicio de e-banking!. Ha recibido más de 40 reclamaciones en los últimos dos meses solamente. He hablado con Wim Van Grembergen, y me comenta que el no ha estado involucrado con We-BOP en los últimos 6 meses, desde que decidisteis subcontratarlo. Quiero que vuelvas a traer a We-BOP internamente y quiero que lo hagas YA!!".

Al cabo de un rato, De Haes pudo calmar al CEO y brindarle algo más de información sobre el proyecto y su historia. Esto reveló que hay un gran descontento en TI relacionado con la calidad del trabajo del contratista, pero también entre el área de BP e TI ya que TI tomó por su cuenta la decisión de subcontratar el servicio. De Haes manifestó que TI tomó la decisión de buena fe porque el área de BP estaba "furiosa" con su inhabilidad para competir en el mercado de e-banking. La discusión, reveló también que había habido varias señales de advertencia respecto de la calidad del servicio.

"Tienes razón Steven. Hablando con Wim hace un rato, me he enterado que el informe que genera la Mesa de Ayuda del subcontratista es enviado a Joshua Dean, uno de los tuyos de Soporte a Usuarios. Joshua asumía que el contratista estaba gestionando de manera efectiva todas estas incidencias y reclamos. Pero no estaban siendo ingresadas en su sistema de Soporte a usuarios. Joshua había notado que los informes eran cada vez más extensos y se lo había mencionado a Ed O'Donnell. Ed no se sorprendió, ya que había notado que la factura por el servicio de Mesa de Ayuda subcontratada había ido incrementándose en los últimos meses. Además, Katherine, del área de Desarrollo, había escuchado que el proveedor de servicios en Singapur no podía resolver los problemas con transacciones erróneas" dijo Mitchell.

Estaba claro que el CEO de TIBO iba a tener que convocar a todos los involucrados si quería llegar al fondo de este asunto. Le pidió a Forsythe que organizara una reunión para el día siguiente. "Pyms, por favor, cambia también la reunión de Seguridad del Comité de Auditoría del Consejo de Dirección. Sé que todos hemos estado muy seriamente preocupados con el enfoque de "bombero" que le hemos dado a la Seguridad desde el 11 de Septiembre de 2001 y el incidente del virus y el de hacking, pero primero

[2] Una Organización para la defensa del consumidor. Ver Apéndice 1

tenemos que resolver el problema de We-BOP".

"Hey…, Steven, antes que te vayas. Tienes alguna idea de a quién deberíamos llamar como nuestro experto en seguridad para la reunión con el Comité de Auditoría?"

"Si recuerdas, John, nosotros elevamos una solicitud para incorporar un Senior CISO[3] pero la decisión del Comité Ejecutivo fue que estábamos bien así y que podíamos obviarla. Todavía estoy debatiendo con Auditoría Interna porque están tratando de asignarme esa responsabilidad a mí, ya que Eric y Roger no pudieron ponerse de acuerdo en quién debería tenerla. En realidad, solo tenemos a Ida Doano, nuestra administradora de seguridad, pero Ida no tiene el nivel ni el perfil como para estar en esa reunión."

De regreso a su oficina, De Haes no podía dejar de pensar en cómo se había iniciado todo. TI había planificado el We-BOP, pero no poseía las habilidades ni capacidades de desarrollo, ya que la mayoría de la gente de TI era del entorno de mainframe. En un partido de golf, De Haes escuchó a un amigo de otro Banco hablar de una extraordinaria empresa de desarrollo de software de Singapur que genera aplicaciones y brinda el servicio de e-banking.

El contrato fue redactado en base al acuerdo estándar de proveedores, negociado por De Haes y Guldentops y firmado por el CEO de TIBO. El departamento legal del Banco también revisó el contrato y se realizaron algunos cambios en aspectos legales. El acuerdo de nivel de servicio (SLA) del contrato cubría:

- El alcance del trabajo
- Los tiempos para el desarrollo y la implantación
- Desempeño, Seguimiento y Reporting
- Roles y Responsabilidades
- Pagos y Funcionalidades

El objetivo era que el contratista fuera el proveedor de servicios completos de e-banking, —incluyendo funcionalidad de front-office, interfaces con el back office y las funciones de Mesa de Ayuda (Soporte al Cliente)— en dos etapas. En la primera, los clientes tendrían acceso a sus cuentas corrientes y de ahorros. Las próximas funciones a ser integradas en la aplicación Web serían Préstamos y Tarjetas de Crédito. La infraestructura de back-office había sido desarrollada internamente y estaba operativa.

Cuando la aplicación se puso operativa, todo funcionó correctamente para el reducido volumen de usuarios (5% de la base de clientes). Luego de seis meses, cuando el número de usuarios se incrementó, comenzaron los problemas con la calidad del servicio:

- Insatisfactorio tiempo de respuesta
- Clientes podían acceder al sistema solo durante ciertos momentos en el día (disponibilidad del sistema)
- Ocasionalmente, las transacciones no se procesaban o se procesaban de manera errónea.

Como resultado, la Mesa de Ayuda recibió un número creciente de preguntas y reclamaciones. El proveedor informaba estas incidencias mensualmente y generaba facturas adicionales dado el incremento del trabajo en la Mesa de Ayuda. Hasta ahora, estos problemas no habían escalado por encima del nivel operativo, donde eran resueltos por TI y personal del área de BP haciendo horas extras.

Antes de llamar a Guldentops, el COO, en Manila para informarle del estado del problema con el We-BOP, De Haes reflexionó acerca de la pobre Doano, administradora de seguridad, quien estaba totalmente

[3] Chief Information Security Officer

saturada con el desarrollo de procedimientos de seguridad, la familiarización con las herramientas de seguridad, la administración de contraseñas para los usuarios del área de BP que querían acceso a todo y la generación de informes que no proveían la información que se necesitaba y que eran leídos por pocos.

Mientras sonaba el teléfono, De Haes también comenzó cambiar mentalmente la agenda prevista para el día siguiente. Iba a tener que hablar con Dean y su gente acerca de su falta de reacción a las alertas del Cortafuegos y también con O'Donnell, quien aparentemente sabía que las debilidades existían. Y, también estaba la poco deseada reunión para revisar prioridades de proyectos con Van Grembergen. De Haes necesitaba que encontrar la manera de convencerlos de lo poco razonable de sus expectativas. Finalmente, Guldentops contestó el teléfono.

"Hola Erik, sé que es cerca de medianoche en Manila, pero tenemos un problema GORDO..."

EL PERFIL DE TIBO

TIBO es una Institución financiera de tamaño medio con las siguientes características:

- El "corazón" de su negocio incluye la banca de individuos—cuentas de ahorro, cuentas corrientes, préstamos y tarjetas de crédito— así como realizar servicios de compensación y liquidación para otros bancos de la zona. Una de sus fortalezas ha sido la atención personalizada a sus clientes de parte de los gerentes de cuenta de la banca personal.
- Está reduciendo su red de agencias y persiguiendo agresivamente el negocio de e-banking.
- Está comenzando a adquirir servicios de TI de terceros (subcontratos o UTEs).
- Ha pasado por varias fusiones locales y como resultado tiene un entorno complejo con servicios compartidos de IT que son difíciles de integrar.
- Es una organización orientada a los procesos con una cultura emergente de incorporación de "stakeholders", pero sin una estrategia formal y tendencia a cambiar prioridades luego de prolongados debates con dichos stakeholders.
- Está compitiendo en un Mercado que está sufriendo numerosos cambios, incluyendo la creciente presencia de entidades de Ahorro y Préstamo y Bancos Internacionales. Nuevos productos están siendo incorporados por la competencia –incluyendo tasas de interés más elevadas- que son muy atractivas para los clientes. Adicionalmente, se empieza a notar la proliferación de oferta de servicios financieros con acceso 24/7.
- Posee una base de clientes fiel, buenos ingresos y sus adquisiciones hasta ahora han sido exitosas, pero los efectos del incremento de la competencia se están haciendo sentir. Hay preocupación respecto de pérdida de Mercado y disminución de beneficios.
- Es consciente de indicadores que los Reguladores están preocupados por el riesgo sistémico, ya que TIBO provee servicios de compensación y pagos a otras entidades financieras.

2. Descripciones del Caso de Estudio

EL ENTORNO TI DE LA EMPRESA

Proyectos

Los proyectos de TIBO incluyen:

- **We-BOP** En la actualidad (parcialmente implementado y subcontratado), incluye el acceso de clientes a aplicaciones de ahorros y cuentas corrientes; próximamente se implementarán los módulos de préstamos y tarjetas; todos con una única interface para el cliente.
- Customer relationship management **(CRM)**—Tendrá como objetivo disponer de toda la información de clientes en un solo sitio para permitir la venta cruzada de productos, facilitar la gestión de los gerentes de cuenta y empleados de sectores de soporte a clientes.
- Core business applications rebuilding (**CoBAR)** —Incluye primariamente las aplicaciones de Ahorros, Cheques y Préstamos
- **IT_Net**—Expansión de la Red de IT y plataformas de aplicaciones estandarizadas.
- **For_Pay**—Servicios de pagos al Exterior
- **Work_it**—Aplicación Workflow y conectividad remota para Gerentes de Cuenta

Tecnología

El ambiente de TI consiste de tres plataformas distintas. La plataforma mainframe provee las aplicaciones primarias del negocio y financieras del CoBAR; incluyen ahorro, cheques, préstamos, fideicomiso, banca personal e interfacecon tarjetas de crédito (alianza con una de las grandes compañías de tarjetas). Todas son aplicaciones en tiempo real, con procesos nocturnos de actualización. Las aplicaciones de compensación y liquidación así como las contables – balance, cuentas a pagar, activos inmovilizados y conciliaciones bancarias – operan también en el mainframe. Esta plataforma de mainframe también se utiliza para ForPay, como un servicio a otros bancos.

Un nuevo entorno Cliente-Servidor que consiste de 5 servers UNIX, formarán la base para la nueva aplicación CRM, que está en una etapa inicial de desarrollo.

La conectividad al sistema corporativo está provista por IT_Net, que es una red virtual privada (VPN), provista por el proveedor de telecomunicaciones de la empresa. En términos generales, la infraestructura de red está envejeciendo y al límite de su capacidad. Solamente los senior managers tienen portátiles.

La red de PCs, involucra servidores Windows utilizados como servidores de datos, impresión, servicios de comunicación y gateway. Las estaciones de trabajo corren bajo Windows. Esta es la plataforma para la aplicación Work_it. La conectividad remota se introducirá basada en la funcionalidad disponible en IT_Net.

El acceso al mainframe se otorga por un sistema de administración de seguridad. La seguridad UNIX está provista por el sistema operativo del Host; no se utilizan herramientas de seguridad propietarias. Los contrafuegos son instalados y gestionados por el proveedor de IT_Net, como un servicio contratado.

La casa Central tiene aproximadamente 600 empleados. A nivel nacional, la corporación emplea aproximadamente 9,000 personas, de las cuales 450 están en TI. Los servicios de TI son críticos para todos los 600 empleados de la Casa Central.

2. Descripciones del Caso de Estudio

Estándares y Procedimientos

Los procedimientos de TI son desarrollados internamente, y varían en calidad y conformación entre las diferentes áreas de TI. El desarrollo de la estrategia de TI es relativamente informal; está basada en discusiones con la gerencia y documentada a través de minutas de reunión, en lugar de procesos determinados o formatos estándar. TI querría mayores directivas de las áreas de negocio y la Dirección Ejecutiva, pero las decisiones estratégicas se toman a nivel de cada proyecto.
La organización de TI es bastante tradicional, con un grupo de desarrollo de sistemas, un grupo de operaciones y un grupo de sistemas y tecnología. El grupo gerencial consiste de un gerente por cada uno de los tres grupos, más el Director del Área.

Los desarrollos de sistemas son mayoritariamente internos, basados en el mainframe, con una metodología de ciclo de vida de desarrollo de sistemas (SDLC) adquirida varios años atrás y ajustada a la medida del Banco. En los últimos años estos métodos han demostrado estar obsoletos y ser muy laboriosos para llevar a cabo. No obstante, al menos se han asegurado contar con una razonable documentación de los sistemas. Hay muy poca experiencia en adquisición de paquetes. Muy pocas personas tienen alguna experiencia con sistemas Cliente-Servidor y ninguna tiene experiencia en desarrollos web.

Operaciones está bien organizada, con buena disciplina y procedimientos estrictos. Generalmente, todo el trabajo es tratado con alta prioridad. Hay turnos cubriendo operaciones las 24 horas del día, con un pequeño grupo nocturno que gestiona los procesos de batch nocturnos. Los acuerdos de nivel de servicio internos (SLAs) están definidos en términos técnicos y en realidad son declaraciones de nivel de servicio; por ejemplo, disponibilidad objetivo y requerimientos de capacidad de la red. Hay una pequeña Mesa de Ayuda interna, utilizada mayoritariamente para ocasionales consultas de usuarios y restauración de contraseñas.

Seguridad

La seguridad está basada en un procedimiento de larga data, el cual está basado a su vez en el tradicional sistema de administración de seguridad de mainframes. Las estaciones de trabajo no poseen unidades de diskette o CD.La política de seguridad, simple pero no muy actualizada, establece las responsabilidades generales y la importancia de la privacidad y seguridad de los datos del banco. TI tiene servers endurecidos, cortafuegos, encriptación y una VPN. La autenticación de usuarios basada en Tokens está sustentada por una política de seguridad de amplio cumplimiento. Existe un pequeño grupo de soporte administrativo a la seguridad que gestiona los nuevos empleados, las bajas y los cambios de derechos de acceso. No existe un Gerente de Seguridad dedicado, aunque el administrador de seguridad es el responsable de la asignación y gestión de privilegios. Debido a las presiones del negocio y el entorno tecnológico, el personal tiende a ser laxo respecto de las reglas de seguridad. La seguridad aún se gestiona en modo reactivo y el banco ha solicitado ayudas puntuales y asesoramiento a terceros. Previo a esta situación, la opinión generalizada es que ha habido pocos eventos dignos de preocupación.

LA ESTRUCTURA ORGANIZATIVA

Las siguientes secciones describen las entidades encontradas en TIBO.

Consejo de Administración (Board of Directors)

El Consejo de TIBO tiene los siguientes atributos:

- El Consejero Delegado (Chariman of the Board) no está involucrado en la operación del día a día.
- Está compuesto por miembros internos y externos; la mayoría de los miembros del Comité de

Auditoría son externos.
- Los miembros no tienen muchos conocimientos técnicos, pero son conscientes del riesgo y se interesan por lo que hace el resto.

Comité Ejecutivo

Sus miembros tienen los siguientes atributos:
- Tienen gran influencia sobre el Consejo, pero necesitan la cooperación de los miembros externos.
- Sus metas son lograr resultados y son, en cierta manera, proclives a correr riesgos.
- Está compuesto por el Chief Exective Officer (CEO), Chief Financial Officer (CFO), Chief Operating Officer (COO) y un Director del negocio. TI se encuentra dentro de las responsabilidades del COO.
- El Control no está muy alto en su lista de prioridades, pero escuchan a Auditoría y apoyan la implantación de recomendaciones.
- Recientemente, apoyaron el desarrollo del sistema de banca por Internet.

Grupo de Estrategia de Negocio

Tiene los siguientes atributos:
- Reporta al Director de Negocios y no posee inclinación hacia las tecnologías.
- Sus mayores prioridades son el CRM y el proyecto CRM.
- Acaba de finalizar un proceso de redimensionamiento, reduciendo en un 50% el número de Agencias.
- Ha realizado un estudio comparativo (Benchmark) del costo del TI para el área de Negocios y concluido que el sector interno de TI es mas caro que en la competencia.
- Quiere un valor neto presente positivo (NPV) para inversiones significativas en infraestructuras de TI.

Las iniciativas estratégicas en curso son:
- Cierre de Agencias de bajo rendimiento (casi completado).
- Sistema de banca por Internet (We-BOP), para descargar la demanda de servicios en las Agencias (en curso).
- Desarrollar capacidades de CRM para crear oportunidades de venta cruzada de servicios bancarios (proyecto iniciado).

Comité de Coordinación de TI

Este Comité involucra una mezcla de Gerentes de TI y áreas usuarias (ver **figura 2**). Se reúne mensualmente y se ocupa primariamente del control de proyectos actuales y futuros. Reporta trimestralmente al Grupo de Estrategias de Negocio. Ha estado muy poco involucrado con el We-BOP dado a que su desarrollo y operación están subcontratados.

Dirección de TI

El Director de TI y el equipo gerencial:
- Muy técnicos y deseosos de dejar una impronta en el e-business, específicamente a través del We-BOP, al cual soportan enteramente.
- Preocupados por la antigüedad / capacidad de la Red, en vista del proyecto de e-banking
- Apoyan firmemente fuertes controles sobre TI
- Concuerdan en que es necesario mayor cooperación con el Grupo de Estrategias de Negocio, que generalmente apoya las prioridades de proyectos de la Dirección de TI, pero con quien no siempre hay acuerdo respecto de las prioridades.
- Firmes creyentes que los sistemas centrales actuales pueden soportar el negocio por varios años, se ponen molestos cuando se trata el tema de la reconstrucción de dichos sistemas.

2. Descripciones del Caso de Estudio

Equipos de trabajos de TI

Los Equipos de TI de TIBO:

- Profesionales altamente calificados y muy orientados a la calidad; han implantado un sólido proceso de control de proyectos y medición de desempeño. Sin embargo, este es demasiado detallado y se utiliza solamente a nivel local.
- Continuamente dispersos por temas de gestión de cambios, como resultado de los permanentes cambios a las aplicaciones y la infraestructura.
- Preocupados por la velocidad de los cambios, especialmente la contratación externa y proyectos auspiciados por los responsables del Negocio, que no siempre son comercialmente exitosos y utilizan recursos necesarios para inversiones necesarias de infraestructura, tales como la nueva Red para incrementar la conectividad y estandarizar las soluciones.
- Preocupados también por el incremento de los problemas de mantenimiento y la escasez de habilidades disponibles relacionadas con los sistemas centrales; sensación de frustración creciente.

Operación del Negocio

Los Ejecutivos son / están:

- Adquiriendo conocimientos de TI y un poco celosos que TI conserve su presupuesto, mientras que ellos deben redimensionarse.
- Reclamando mayor conectividad remota y flujos de trabajo (Workflow) automatizados para ser más efectivos en una red de Agencias reducida.
- Protestando por el rendimiento y el soporte de los sistemas centrales y promoviendo la celebración de SLAs y la reconstrucción de los mismos por ser prácticamente obsoletos.
- Requiriendo conectar cada vez mas clientes de e-banking aunque no sean rentables en lo inmediato, tensando los sistemas de operación y soporte.

2. Descripciones del Caso de Estudio

Figura 3—Acuerdo de Nivel de Servicio del Contrato de Outsourcing

We-BOP

Revisión	Fecha	Descripción	Páginas afectadas
1.0	Febrero 200x	Primera Edición	Todas

Propósito de este Documento
Este documento constituye un acuerdo entre el contratante y una tercera parte, definidas en la próxima Sección, para el desarrollo de un servicio completo de e-banking denominado aquí como "We-BOP.". Detalla el entorno, las expectativas, los entregables y las responsabilidades asociadas con la implementación de este acuerdo.

Partes del Acuerdo
Este acuerdo, fechado en Febrero de 200x, es entre TIBO© con oficinas situadas en …. (a partir de aquí, denominado "el contratante") y ….., con oficinas ubicadas en ……(a partir de aquí denominado "el proveedor").

Alcance del Trabajo
El alcance de este acuerdo es para que el proveedor desarrolle un servicio complete de e-banking, We-BOP. Este servicio incluye:

- El desarrollo de una aplicación web de cara al cliente (front office) con la siguiente funcionalidad:
  – Acceso a cuentas de ahorro
  – Access a cuentas corrientes
  – Administración de Tarjetas de Crédito
  – Administración de Préstamos
- El desarrollo de interfaces del front office con la retaguardia (back office) del contratante.
- Establecimiento de una Mesa de Ayuda como soporte a clientes (help desk) de la aplicación desarrollada, We-BOP.

Definición de Fechas de entrega para el Desarrollo e Implementación
La aplicación We-BOP y su interface se desarrollarán en dos fases:

- Fase 1: Estará operativo el 30 Abril 200x
  – Aplicación web de cara al cliente que permita:
    Acceso a cuentas de ahorro
    Access a cuentas corrientes
  – La interface entre dicha aplicación y la retaguardia del contratante
  – Mesa de Ayuda operativa para soporte al cliente
- Fase 2: Operativa el 31 Marzo 200x+1

– Funcionalidades extendidas de la aplicación web:
  Tarjetas de Crédito
  Préstamos

Desempeño, Seguimiento y Reporting
We-BOP
El proveedor informará trimestralmente respecto del desempeño del sistema We-BOP .
El informe será enviado al Director de TI del contratante.
Mesa de Ayuda El proveedor informará mensualmente respecto de los pedidos a Mesa de Ayuda y cómo se solucionan. Este informe será enviado al Director de TI del contratante. El proveedor generará un fichero específico de errores para el control y la gestión de errores reportados, que podrá ser accedido directamente por el contratante.

Roles y Responsabilidades
Comunicación Los contactos y comunicaciones entre el contratante y el proveedor se realizan por correo electrónico, teléfono y reuniones regulares. El contratante y el proveedor deben comunicar su estructura organizativa (y sus cambios) mutuamente, a fin de que cada grupo pueda mantener su lista de distribución actualizada. El contratante y el proveedor deben informarse mutuamente las ausencias de personal no planificadas (reuniones, vacaciones, reemplazos, etc.).
Responsabilidades del Contratante El contratante debe proporcionar al proveedor toda la información relacionada con las especificaciones necesarias de su retaguardia (back-office) para establecer las interfaces con la aplicación web (front office). El proveedor debe ser informado de cualquier cambio en la retaguardia que pudiera afectar la interface. El contratante responderá rápidamente –dentro de 5 días laborables- cualquier requerimiento del proveedor respecto de información o decisiones que son razonablemente necesarias para que el proveedor pueda desarrollar el sistema y proveer los servicios.
Responsabilidades del Proveedor El proveedor garantiza que el desarrollo del sistema We-BOP y la función de Mesa de Ayuda serán realizadas de manera humana y profesional, consistentes con los estándares razonablemente aplicables a este tipo de servicios.
El proveedor no divulgará ninguna información confidencial respecto del contratante que pudiera obtener durante el proceso de desarrollo.

Pagos y Penalidades
Para el desarrollo de la aplicación web, el contratante abonará al proveedor como sigue:
25 % al inicio del proyecto
50 % luego de la entrega de la Fase 1
25 % luego de la entrega de la Fase 2
Por la Mesa de Ayuda, el proveedor facturará una suma fija mensual de US $ xxxx.xx.
Si la aplicación web no puede ser entregada en la fecha estipulada, el contratante facturará una penalidad por día de demora de US $ xxxx.xx .
Todos los importes a ser abonados por el contratante, en la moneda de la factura, serán depositados en la cuenta designada por el proveedor. Todas las facturas serán abonadas dentro de los 30 días de la fecha de la misma. En caso contrario, el proveedor podrá agregar un cargo administrativo de 1.5% a la factura correspondiente.

Firmas

CEO del Contratante Fecha
CEO del Proveedor Fecha

3. MATERIALS ADDICIONAL

EL ASUNTO DE LA SEGURIDAD

Preguntas

1. En una llamada anónima al CFO, una persona manifiesta tener acceso a información de clientes proveniente de los sistemas de la empresa y da pruebas de ello mediante un fax conteniendo información sensible (nombres, gerentes de cuenta, etc.)
   - Analizar los riesgos de seguridad.
   - Recomendar algunas buenas prácticas para mitigar los riesgos.
2. Se le informa que la filtración ha ocurrido en la empresa subcontratada y se le hace entrega de una copia del actual (breve e inadecuado) acuerdo de nivel de servicio (SLA). Los datos se filtraron porque el contratista utilizó datos reales y on-line, durante las pruebas de aceptación de la segunda fase de una instalación de un servidor web inseguro.
   - Defina qué debería haber incluido la Gerencia en el SLA en relación a la seguridad.
   - Qué es lo que cree que realmente pasó que permitió que esa información se hiciera pública?

EL ASUNTO DE LA SUBCONTRATACION

Preguntas

1. Se ha presentado aquí un detallado proceso de subcontratación. Evalúe el proceso. Describir los problemas encontrados por TIBO o los riesgos a los que se enfrenta e identifique las mejores prácticas que, de haberse implementado podrían haber prevenido o aliviado dichos problemas y riesgos.
2. Identificar los roles que deberían jugar en el proceso de Subcontratación la Auditoría, la Dirección de TI y el CEO. Comparar estas mejores prácticas con los roles desempeñados.

EL ASUNTO DE LA ALINEACIÓN ESTRATEGICA

Información y Antecedentes Adicionales

La estrategia del negocio está determinada por la estrategia del Grupo de Estrategia de Negocio, que está compuesto por el CEO, los Vice Presidentes de operaciones minoristas y mayoristas y dos miembros externos. Uno de los miembros externos es Charles Penrose, el ex-CEO de Accubank. Accubank se fusionó con TIBO hace 18 meses. El otro miembro externo es Nigel Sorrell. Nigel es también miembro del Consejo de Administración.

El Grupo de Estrategia de Negocio se reúne el primer Martes de cada mes para revisar el progreso de iniciativas estratégicas en marcha y discutir la dirección estratégica del Banco. La información para revisar el grado de avance se obtiene normalmente invitando al Gerente del Proyecto de la iniciativa en cuestión a dar una breve presentación. El grupo trata de mantenerse actualizado y atento a eventos que podrían alterar las prácticas de la industria. En concreto, el grupo ha estado pensando en:

- Estrategias de Canales
- Tendencias actuales
- Retención y relación con Clientes

El Grupo de Estrategia de Negocio tiene excelentes procedimientos de documentación. Mantiene un documento de iniciativas estratégicas que detalla cada una de las iniciativas, incluyendo gráficos de su grado de avance. Este documento se distribuye al Consejo de Administración y al Comité Ejecutivo.

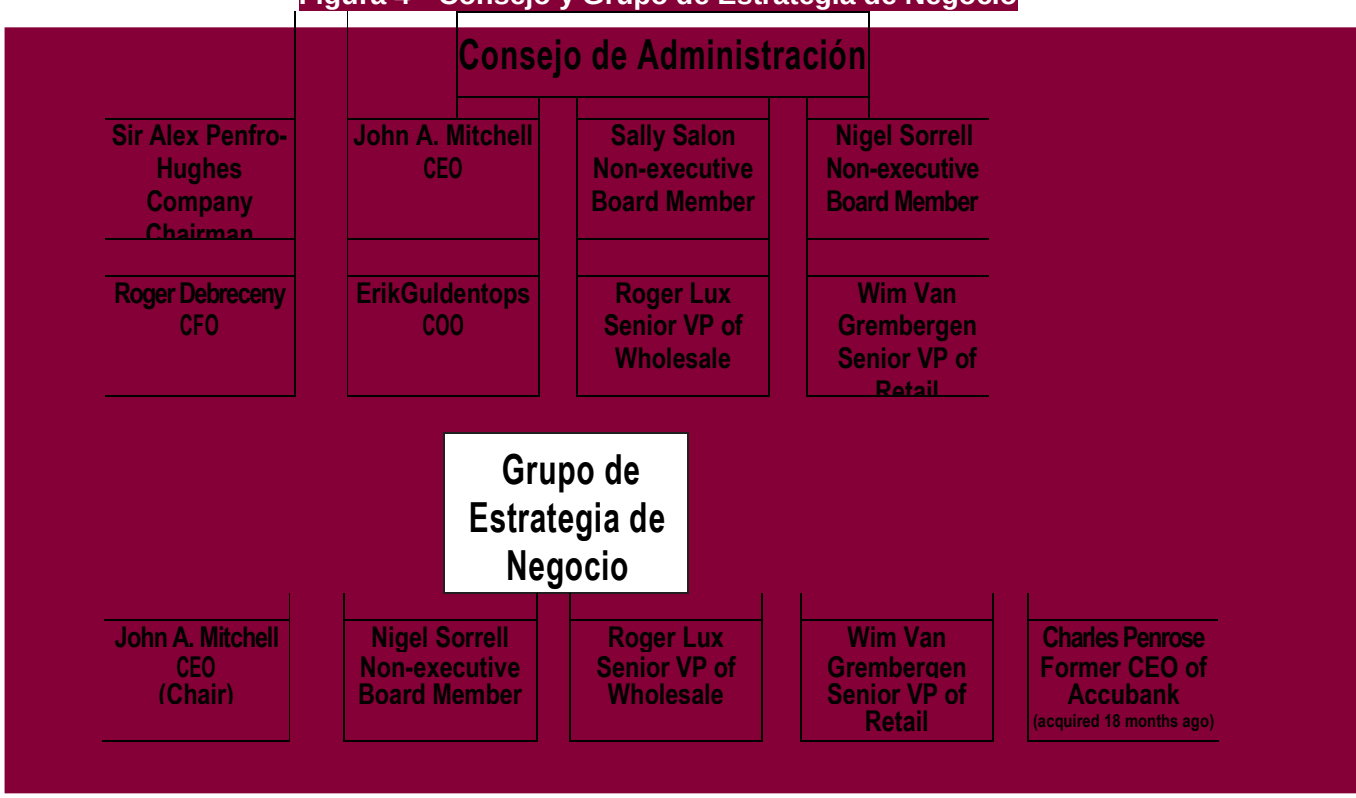
3. Materials Addicional

El Comité Ejecutivo se reúne el primer Jueves de cada mes. La discusión de asuntos estratégicos es un punto permanente de la Agenda del Comité. John Mitchell siempre se asegura que se le dedique la atención adecuada al tema de la dirección estratégica del Banco.

El Consejo de Administración se reúne trimestralmente (ver **figura 4**). Las iniciativas estratégicas están siempre dentro de los múltiples temas que se tratan en dichas reuniones.

Las decisiones estratégicas se delegan hacia niveles más bajos de la organización para su implementación. Por ejemplo, la iniciativa We-BOP se delegó en el Director de TI. El Director de TI le asignó a un Gerente de Proyecto que comenzara a buscar soluciones alternativas y posibles para la iniciativa We-BOP. Este decidió que la manera más segura de ingresar al campo del e-banking era subcontratando esta funcionalidad.

Figura 4—Consejo y Grupo de Estrategia de Negocio



Preguntas

1. Analice las implicancias de gobierno en la forma en que el Consejo, el nivel Ejecutivo y la Dirección de TI gestionaron el proceso de subcontratación. Cuáles serían las mejores prácticas para el gobierno de servicios prestados por terceros?
2. Porqué el CEO no estaba enterado de los reclamos de clientes antes de conocer el Informe del Defensor del Consumidor? Cómo se podría evitar esto en el futuro? Qué cambios en gobierno propone para solucionar este problema?
3. Estando el Consejo a punto de comenzar con la iniciativa CRM, cómo se podría lograr una mayor alineación entre TI y la estrategia del negocio que la que fue evidente en la iniciativa We-BOP?

APPENDIX 1—FINANCIAL OMBUDSMAN SERVICE

El Servicio de Defensa del Consumidor Financiero (Financial Ombudsman Service) es una agencia de regulación muy poderosa de Inglaterra que puede ayudarle si tiene una reclamación financiera que resolver con su:

- Banco
- Sociedad de Construcción
- Asesor Financiero
- Cooperativa de Crédito
- Compañía de Seguros
- Firma de Inversiones
- Agente de Bolsa
- Compañía de Fideicomiso

El Servicio de Defensa del Consumidor fue establecido por ley para proveer a los consumidores un servicio gratuito e independiente para resolver disputas con entidades financieras. Puede brindar ayuda con la mayoría de las reclamaciones relacionadas con::

- Servicios bancarios
- Tarjetas de Crédito
- Políticas de Seguros de Inversión
- Asesoría financiera y de inversión
- Pólizas de Seguro
- Gestión de Fondos e Inversiones
- Seguros de Vida
- Hipotecas
- Planes de Pensión
- Planes y cuentas de ahorro
- Acciones y bonos

Puede imponer multas, pero el mayor impacto de dichos incidentes resulta de la publicación que se realiza de los mismos.

APPENDIX 2—OBJETIVOS DE CONTROL Y MODELOS DE MADUREZ DE COBIT

PO1 DEFINIR UN PLAN ESTRATEGICO PARA TI

Descripción del Proceso

Se requiere una planeación estratégica de TI para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia del negocio y las prioridades. La función de TI y los participantes del negocio son responsables de garantizar que se materialice el valor óptimo de los portafolios de proyectos y servicios. El plan estratégico debe mejorar el entendimiento de los interesados clave respecto a las oportunidades y limitaciones de TI, evaluar el desempeño actual y aclarar el nivel de inversión requerido. La estrategia de negocio y las prioridades se deben reflejar en los portafolios y deben ser ejecutadas por los planes tácticos de TI, los cuales establecen objetivos, planes y tareas específicas, entendidas y aceptadas tanto por el negocio como por TI.

PO1.1 Administración del valor de TI
Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos. Reconocer que existen inversiones obligatorias, de sustento y discrecionales que difieren en complejidad y grado de libertad en cuanto a la asignación de fondos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los componentes TI de los programas y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, calendario o funcionalidad, que pudieran impactar los resultados esperados de los programas. Los servicios de TI se deben ejecutar contra acuerdos de niveles de servicios equitativos y exigibles. La rendición de cuentas del logro de los beneficios y del control de los costos es claramente asignada y monitoreada. Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.

PO1.2 Alineación de TI con el negocio
Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado la TI está bien entendido. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de la TI, y mediar entre los imperativos del negocio y la tecnología, de tal modo que se puedan establecer prioridades concertadas.

PO1.3 Evaluación del desempeño actual
Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

PO1.4 IT Plan estratégico de TI
Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo la TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales. Define cómo se cumplirán y medirán los objetivos y recibirá una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para

permitir la definición de planes tácticos de TI.

PO1.5 IT Planes tácticos de TI
Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes proyectados. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones.

PO1.6 IT Administración del portafolio de TI
Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos y específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas. Esto incluye clarificar los resultados de negocio deseados, garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance completo del esfuerzo requerido para lograr los resultados, definir una rendición de cuentas clara con medidas de soporte, definir proyectos dentro del programa, asignar recursos y financiamiento, delegar autoridad, y licenciar los proyectos requeridos al momento de lanzar el programa.

APENDICE 2

Modelo de Madurez

Administración del proceso de *Definir un plan estratégico* de TI que satisfaga el requisito de negocio de TI de sostener o *extender la estrategia de negocio y los requerimientos de gobierno al mismo tiempo que se mantiene la transparencia sobre los beneficios costos y riesgos es*:

0 **No existente** cuando
no se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.

1 **Inicial/Ad Hoc** cuando
La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requisito de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.

2 **Repetible pero intuitiva** cuando
La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.

3 **Proceso definido** cuando
Una política define cómo y cuándo realizar la planeación estratégica de TI. La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Sin embargo, se otorga discrecionalidad a gerentes individuales específicos con respecto a la implantación del proceso, y no existen procedimientos para analizar el proceso. La estrategia general de TI incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador o como seguidor. Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías. La planeación estratégica de TI se discute en reuniones de la dirección del negocio.

4 **Administrado y medible** cuando
La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La planeación estratégica de TI es una función administrativa definida con responsabilidades de alto nivel. La dirección puede monitorear el proceso estratégico de TI, tomar decisiones informadas con base en el plan y medir su efectividad. La planeación de TI de corto y largo plazo sucede y se distribuye en forma de cascada hacia la organización, y las actualizaciones se realizan según son necesarias. La estrategia de TI y la estrategia organizacional se vuelven cada vez más coordinadas al abordar procesos de negocio y capacidades de valor agregado y al aprovechar el uso de aplicaciones y tecnologías por medio de la re-ingeniería de procesos de negocio. Existen procesos bien definidos para determinar e uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas.

5 **Optimizado** cuando
La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Las consideraciones de riesgo y de valor agregado se actualizan de modo constante en el proceso de planeación estratégica de TI. Se desarrollan planes realistas a largo plazo de TI y se actualizan de manera constante para reflejar los cambiantes avances tecnológicos y el progreso relacionado al negocio. Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia. El plan estratégico incluye cómo los nuevos avances tecnológicos

APENDICE 2

pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.

APENDICE 2

PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

Descripción del Proceso

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los participantes y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia..

PO9.1 Alineación de la administración de riesgos de TI y del negocio
Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización

PO9.2 Establecimiento del contexto del riesgo
Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

PO9.3 Identificación de eventos
Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

PO9.4 IT Evaluación de riesgos
Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

PO9.5 Respuesta a los riesgos
Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar. Al elaborar la respuesta, considerar los costos y beneficios y seleccionar respuestas que limiten los riesgos residuales dentro de los niveles de tolerancia de riesgos definidos.

PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos
Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

APENDICE 2

Modelo de Madurez

La administración del proceso de *Evaluar y administrar los riesgos de TI* que satisfaga el requisito de negocio de TI de *analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y las metas de negocio* es:

0 **No existente** cuando
La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI

1 **Inicial/Ad Hoc** cuando
Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan a gerentes específicos con poca frecuencia. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.

2 **Repetible pero intuitiva** cuando
Existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implantación donde se identifican riesgos.

3 **Proceso definido** cuando
Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.

4 **Administrado y medible** cuando
La evaluación y administración de riesgos son procesos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con la TI. La gerencia puede monitorear la posición de riesgo y tomar decisiones informadas respecto a la exposición que está dispuesta a aceptar. Todos los riesgos identificados tienen un propietario denominado, y la alta dirección, así como la gerencia de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar. La gerencia de TI ha elaborado medidas estándar para evaluar el riesgo y para definir las proporciones riesgo/retorno. La gerencia presupuesta para que un proyecto operativo de administración de riesgos re-evalúe los riesgos de manera regular. Se establece una base de datos administrativa y parte del proceso de administración de riesgos se empieza a automatizar. La gerencia de TI toma en cuenta las estrategias de mitigación de riesgo.

5 **Optimizado** cuando
La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la

APENDICE 2

organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detectará y actuará cuando se realicen decisiones grandes de inversión, operación o de TI, sin tomar en cuenta el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.

APENDICE 2

PO10 ADMINISTRAR ROYECTOS

Descripción del Proceso

Establecer un programa y un marco de control administrativo de proyectos para la administración de todos los proyectos de TI. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. El marco de trabajo debe incluir un plan maestro, asignación de recursos, definición de entregables, aprobación de los usuarios, un enfoque de entrega por fases, aseguramiento de la calidad, un plan formal de pruebas, revisión de pruebas y revisión post-implantación después de la implantación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio. Este enfoque reduce el riesgo de costos inesperados y de cancelación de proyectos, mejora la comunicación y el involucramiento del negocio y de los usuarios finales, asegura el valor y la calidad de los entregables de los proyectos, y maximiza su contribución a los programas de inversión en TI.

P010.1 Marco de trabajo para la administración de programas
Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversión en TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos. Asegurarse de que los proyectos apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos.

P010.2 Marco de trabajo para la administración de proyectos
Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planeación, la ejecución, el control y el cierre de las etapas de los proyectos, así como los puntos de verificación y las aprobaciones. El marco de trabajo y las metodologías de soporte se deben integrar con la administración del portafolio empresarial y con los procesos de administración de programas.

P010.3 Enfoque de administración de proyectos
Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores del proyecto, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.

P010.4 Compromiso de los interesados
Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.

P010.5 Estatuto de alcance del proyecto
Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversión en TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de arrancar el proyecto.

APENDICE 2

P010.6 Inicio de las fases del proyecto
Asegurarse que el arranque de las etapas importantes del proyecto se apruebe de manera formal y se comunique a todos los interesados. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa. La aprobación de las fases subsiguientes se debe basar en la revisión y aceptación de los entregables de la fase previa, y la aprobación de un caso de negocio actualizado en la próxima revisión importante del programa. En el caso de fases traslapadas, se debe establecer un punto de aprobación por parte de los patrocinadores del programa y del proyecto, para autorizar así el avance del proyecto.

P010.7 Plan integrado del proyecto
Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste. Las actividades e interdependencias de múltiples proyectos dentro de un mismo programa se deben entender y documentar. El plan del proyecto se debe mantener a lo largo de la vida del mismo. El plan del proyecto, y las modificaciones a éste, se deben aprobar de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

P010.8 Recursos del proyecto
Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto. La obtención de productos y servicios requeridos para cada proyecto se debe planear y administrar para alcanzar los objetivos del proyecto, usando las prácticas de adquisición de la organización.

P010.9 Administración de riesgos del proyecto
Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central.

PO10.10 Plan de calidad del proyecto
Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado. El plan debe ser revisado y acordado de manera formal por todas las partes interesadas para luego ser incorporado en el plan integrado del proyecto.

PO10.11 Control de cambios del proyecto
Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (ej. costos, cronograma, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto, de acuerdo al marco de trabajo de gobierno del programa y del proyecto.

PO10.12 Planeación del proyecto y métodos de aseguramiento Identificar las tares de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

PO10.13 Medición del desempeño, reportes y monitoreo del proyecto Medir el desempeño del proyecto contra los criterios clave del proyecto (ej. alcance, calendario, calidad, costos y riesgos); identificar las desviaciones con respecto al plan; evaluar su impacto sobre el proyecto y sobre el programa global; reportar los resultados a los interesados clave; y recomendar, implantar y monitorear

las medidas correctivas, según sea requerido, de acuerdo con el marco de trabajo de gobierno del programa y del proyecto.

PO10.14 Cierre del proyecto
Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados. Identificar y comunicar cualquier actividad sobresaliente requerida para alcanzar los resultados planeados del proyecto y los beneficios del programa, e identificar y documentar las lecciones aprendidas a ser usadas en futuros proyectos y programas

APENDICE 2

Modelo de Madurez

La administración del proceso de *Administrar proyectos* que satisfaga el requisito de negocio de TI de *entregar los resultados del proyecto en el tiempo, con el presupuesto y con la calidad acordados* es:

0 **No existente** cuando
Las técnicas de administración de proyectos no se usan y la organización no toma en cuenta los impactos al negocio asociados con la mala administración de los proyectos y con las fallas de desarrollo en el proyecto.

1 **Inicial/Ad Hoc** cuando
El uso de técnicas y enfoques de administración de proyectos dentro de TI es una decisión individual que se deja a los gerentes de TI. Existe una carencia de compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos. Las decisiones críticas sobre administración de proyectos se realizan sin la intervención de la gerencia usuaria ni del cliente. Hay poca o nula participación del cliente y del usuario para definir los proyectos de TI. No hay una organización clara dentro de TI para la administración de proyectos. Los roles y responsabilidades para la administración de proyectos no están definidas. Los proyectos, calendarios y puntos clave están definidos pobremente, si es que lo están. No se hace seguimiento al tiempo y a los gastos del equipo del proyecto y no se comparan con el presupuesto.

2 **Repetible pero intuitiva** cuando
La alta dirección ha obtenido y comunicado la conciencia de la necesidad de una administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos de proyecto a proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción del gerente de proyecto.

3 **Proceso definido** cuando
El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados. Los proyectos de TI se definen con los objetivos técnicos y de negocio adecuados. La alta dirección del negocio y de TI, empiezan a comprometerse y a participar en la administración de los proyectos de TI. Se ha establecido una oficina de administración de proyectos dentro de TI, con roles y responsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, calendarios y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento en administración de proyectos es un resultado principalmente de las iniciativas individuales del equipo. Los procedimientos de aseguramiento de calidad y las actividades de implantación post-sistema han sido definidos, pero no se aplican de manera amplia por parte de los gerentes de TI. Los proyectos se empiezan a administrar como portafolios.

4 **Administrado y medible** cuando
La gerencia requiere que se revisen métricas y lecciones aprendidas estandarizadas y formales después de terminar cada proyecto. La administración de proyectos se mide y evalúa a través de la organización y no solo en TI. Las mejoras al proceso de administración de proyectos se formalizan y comunican y los miembros del equipo reciben entrenamiento sobre estas mejoras. La gerencia de TI ha implantado una estructura organizacional de proyectos con roles, responsabilidades y criterios de desempeño documentados. Los criterios para evaluar el éxito en cada punto clave se han establecido. El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos. Cada vez más, los proyectos abordan las metas organizacionales, en lugar de abordar solamente las específicas a TI. Existe un apoyo fuerte y activo a los proyectos por parte de los patrocinadores de la alta dirección, así como de los interesados. El entrenamiento relevante sobre administración de proyectos se planea para el equipo en la oficina de proyectos y a lo largo de la función de TI.

5 **Optimizado** cuando

APENDICE 2

Se encuentra implantada una metodología comprobada de ciclo de vida de proyectos, la cual se refuerza y se integra en la cultura de la organización completa. Se ha implantado una iniciativa continua para identificar e institucionalizar las mejores prácticas de administración de proyectos. Se ha definido e implantado una estrategia de TI para contratar el desarrollo y los proyectos operativos. La oficina integrada de administración de proyectos es responsable de los proyectos y programas desde su concepción hasta su post-implantación. La planeación de programas y proyectos en toda la organización garantiza que los recursos de TI y del usuario se utilizan de la mejor manera para apoyar las iniciativas estratégicas.

APENDICE 2

AI2 ADQUIRIR Y MANTENER SOFTWARE APLICATIVO

Descripción del Proceso

Las aplicaciones deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.

AI2.1 Diseño de alto nivel
Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, tomando en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.

AI2.2 Diseño detallado
Preparar el diseño detallado y los requerimientos técnicos del software de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Los conceptos a considerar incluyen, pero no se limitan a, definir y documentar los requerimientos de entrada de datos, definir interfaces, la interface de usuario, el diseño para la recopilación de datos fuente, la especificación de programa, definir y documentar los requerimientos de archivo, requerimientos de procesamiento, definir los requerimientos de salida, control y auditabilidad, seguridad y disponibilidad, y pruebas. Realizar una reevaluación para cuando se presenten discrepancias técnicas o lógicas significativas durante el desarrollo o mantenimiento.

AI2.3 Control y auditabilidad de las aplicaciones
Asegurar que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable. Los aspectos que se consideran especialmente son: mecanismos de autorización, integridad de la información, control de acceso, respaldo y diseño de pistas de auditoría.

AI2.4 Seguridad y disponibilidad de las aplicaciones.
Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo. Los asuntos a considerar incluyen derechos de acceso y administración de privilegios, protección de información sensible en todas las etapas, autenticación e integridad de las transacciones y recuperación automática. .

AI2.5 Configuración e implantación de software aplicativo adquirido
Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.

AI2.6 Actualizaciones importantes en sistemas existentes
Seguir un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los

diseños y/o funcionalidad actuales. Los aspectos a considerar incluyen análisis de impacto, justificación costo/beneficio y administración de requerimientos.

AI2.7 Desarrollo de software aplicativo
Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad. Aprobar y autorizar cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad. Los aspectos a considerar incluyen aprobar las especificaciones de diseño que satisfacen los requerimientos de negocio, funcionales y técnicos; aprobar las solicitudes de cambio; y confirmación de que el software aplicativo es compatible con la producción y está listo para su migración. Además, garantizar que se identifican y consideran todos los aspectos legales y contractuales para el software aplicativo que desarrollan terceros.

AI2.8 Aseguramiento de la Calidad del Software
Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. Los asuntos a considerar en el plan de aseguramiento de calidad incluyen especificar el criterio de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas.

AI2.9 Administración de los requerimientos de aplicaciones
Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.

AI2.10 Mantenimiento de software aplicativo
Desarrollar una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software. Los asuntos a considerar incluyen liberación planeada y controlada, planeación de recursos, reparación de defectos de programa y corrección de fallas, pequeñas mejoras, mantenimiento de documentación, cambios de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de actualización, condiciones contractuales tales como aspectos de soporte y actualizaciones, revisión periódica de acuerdo a las necesidades del negocio, riegos y requerimientos de seguridad.

APENDICE 2

Modelo de Madurez

La administración del proceso de *Adquirir y mantener software aplicativo* que satisfaga el requisito de negocio de TI de *hacer disponibles aplicaciones de acuerdo con los requerimientos del negocio, en tiempo y a un costo razonable* es:

0 **No existente** cuando
No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.

1 **Inicial/Ad Hoc** cuando
Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición y mantenimientos de software aplicativo varían de un proyecto a otro. Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.

2 **Repetible pero intuitiva** cuando
Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro de la operación de TI. El mantenimiento es a menudo problemático y se resiente cuando se pierde el conocimiento interno de la organización. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.

3 **Proceso definido** cuando
Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia de TI y del negocio. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que se salten pasos. Las actividades de mantenimiento se planean, programan y coordinan.

4 **Administrado y medible** cuando
Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación. Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones. Han evolucionado prácticas y procedimientos para ajustarlos a la medida de la organización, los utilizan todo el personal y son apropiados para la mayoría de los requerimientos de aplicación.

5 **Optimizado** cuando
Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base en componentes, con aplicaciones predefinidas y estandarizadas que corresponden a las necesidades del negocio. El enfoque se extiende para toda la empresa. La metodología de adquisición y mantenimiento presenta un buen avance y permite un posicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantes del negocio. La metodología de adquisición e implantación de software aplicativo ha sido sujeta a mejora continua y se soporta con bases de datos internas y externas que contienen materiales de referencia y las mejores prácticas. La metodología produce documentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento

APENDICE 2

DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS

Descripción del Proceso

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

DS2.1 Identificación de las relaciones con todos los proveedores
Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores.

DS2.2 Administración de las relaciones con los proveedores
Formalizar el proceso de administración de relaciones con proveedores por cada proveedor. Los responsables de las relaciones deben coordinar a los proveedores y los clientes y asegurar la calidad de las relaciones con base en la confianza y la transparencia (por ejemplo, a través de acuerdos de niveles de servicio).

DS2.3 Administración de riesgos del proveedor
Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.

DS2.4 Monitoreo del desempeño del proveedor
Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado

APENDICE 2

Modelo de Madurez

La administración del proceso de *Administrar los servicios de terceros que satisfagan los requerimientos de TI del negocio de brindar servicios de terceros satisfactorios siendo transparentes respecto a los beneficios, costos y riesgos* es*:*

0 **No existente** cuando
Las responsabilidades y la rendición de cuentas no están definidas. No hay políticas y procedimientos formales respecto a la contratación con terceros. Los servicios de terceros no son ni aprobados ni revisados por la gerencia. No hay actividades de medición y los terceros no reportan. A falta de una obligación contractual de reportar, la alta gerencia no está al tanto de la calidad del servicio prestado.

1 **Inicial/Ad Ho** cuando
La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. No hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva. Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).

2 **Repetible pero intuitiva** cuando
El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.

3 **Proceso definido** cuando
Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operacionales y de control. Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero está valorado y reportado.

4 **Administrado y medible** cuando
Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, calendario, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.

5 **Optimizado** cuando
Los contratos firmados con los terceros son revisados de forma periódica en intervalos predefinidos. La responsabilidad de administrar a los proveedores y la calidad de los servicios prestados está asignada. Se monitorea el cumplimiento de las condiciones operacionales, legales y de control y se implantan acciones correctivas. El tercero está sujeto a revisiones periódicas independientes y se le retroalimenta sobre su desempeño para mejorar la prestación del servicio. Las mediciones varían como respuesta a los cambios en las condiciones del negocio. Las mediciones ayudan a la detección temprana de problemas potenciales con los servicios de terceros. La notificación completa y bien definida del cumplimiento de los niveles de servicio, está asociada con la compensación del tercero. La gerencia ajusta el proceso de adquisición y monitoreo de servicios de terceros con base en los resultados de los KPIs y KGIs.

APENDICE 2

DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

Descripción del Proceso

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye la monitorización de la seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

DS5.1 Administración de la seguridad de TI
Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

DS5.2 Plan de seguridad de TI
Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

DS5.3 Administración de identidad
Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

DS5.4 Administración de cuentas del usuario
Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

APENDICE 2

DS5.6 Definición de incidente de seguridad
Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

DS5.7 Protección de la tecnología de seguridad
Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad.

DS5.8 Administración de llaves criptográficas
Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

DS5.9 Prevención, detección y corrección de software malicioso
Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

DS5.10 Seguridad de la red
Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

DS5.11 Intercambio de datos sensitivos
Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

APENDICE 2

Modelo de Madurez

La administración del proceso de *Garantizar la seguridad de los sistemas* que satisfaga el requerimiento de negocio de TI de *mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad* es:

0 **No-existente** cuando
La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.

1 **Inicial/Ad Hoc** cuando
La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

2 **Repetible pero intuitivo** cuando
Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

3 **Proceso definido** cuando
Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

4 **Administrado y Medible** cuando
Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.

5 **Optimizado** cuando
La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está

integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIs para ajustar el plan de seguridad en un proceso de mejora continua.

APENDICE 2

DS6 IDENTICAR Y ASIGNAR COSTOS

Descripción del Proceso

La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de una sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones más informadas respectos al uso de los servicios de TI.

DS6.1 Definición de servicios
Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente. Los servicios de TI deben vincularse a los procesos del negocio de forma que el negocio pueda identificar los niveles de facturación de los servicios asociados.

DS6.2 Contabilización de TI
Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido. Las variaciones entre los presupuestos y los costos actuales deben analizarse y reportarse de acuerdo con los sistemas de medición financiera de la empresa.

DS6.3 Modelación de costos y cargos
Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa. El modelo de costos de TI debe garantizar que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos. La gerencia del usuario debe poder verificar el uso actual y los cargos de los servicios.

DS6.4 Mantenimiento del modelo de costos
Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

APENDICE 2

Modelo de Madurez

La administración del proceso de *Identificar y asignar costos* que satisfagan los requerimientos del negocio de TI de *transparentar y entender los costos de TI y mejorar la relación costo-eficiencia por medio del uso bien informado de servicios de TI* es:

0 **No-existente** cuando
Hay una completa falta de cualquier proceso reconocible de identificación y distribución de costos en relación a los servicios de información brindados. La organización no reconoce incluso que hay un problema que atender respecto a la contabilización de costos y que no hay comunicación respecto a este asunto.

1 **Inicial/Ad Hoc** cuando
Hay un entendimiento general de los costos globales de los servicios de información, pero no hay una distribución de costos por usuario, cliente, departamento, grupos de usuarios, funciones de servicio, proyectos o entregables. Es casi nulo el monitoreo de los costos, sólo se reportan a la gerencia los costos agregados. La distribución de costos de TI se hace como un costo fijo de operación. Al negocio no se le brinda información sobre el costo o los beneficios de la prestación del servicio.

2 **Repetible pero intuitivo** cuando
Hay conciencia general de la necesidad de identificar y asignar costos. La asignación de costos está basada en suposiciones de costos informales o rudimentarios, por ejemplo, costos de hardware, y prácticamente no hay relación con los generadores de valor. Los procesos de asignación de costos pueden repetirse. No hay capacitación o comunicación formal sobre la identificación de costos estándar y sobre los procedimientos de asignación. No está asignada la responsabilidad sobre la recopilación o la asignación de los costos.

3 **Proceso definido** cuando
Hay un modelo definido y documentado de costos de servicios de información. Se ha definido un proceso para relacionar costos de TI con los servicios prestados a los usuarios. Existe un nivel apropiado de conciencia de los costos atribuibles a los servicios de información. Al negocio se le brinda información muy básica sobre costos.

4 **Administrado y Medible** cuando
Las responsabilidades sobre la administración de costos de los servicios de información están bien definidas y bien entendidas a todos los niveles, y son soportadas con capacitación formal. Los costos directos e indirectos están identificados y se reportan de forma oportuna y automatizada a la gerencia, a los propietarios de los procesos de negocio y a los usuarios. Por lo general, hay monitoreo y evaluación de costos, y se toman acciones cuando se detectan desviaciones de costos. El reporte del costo de los servicios de información está ligado a los objetivos del negocio y los acuerdos de niveles de servicio, y son vigilados por los propietarios de los procesos de negocio. Una función financiera revisa que el proceso de asignación de costos sea razonable. Existe un sistema automatizado de distribución de costos, pero se enfoca principalmente en la función de los servicios de información en vez de hacerlo en los procesos de negocio. Se acordaron los KPIs y KGIs para mediciones de costos, pero son medidos de manera inconsistente.

5 **Optimizado** cuando
Los costos de los servicios prestados se identifican, registran, resumen y reportan a la gerencia, a los propietarios de los procesos de negocio y a los usuarios. Los costos se identifican como productos cobrables y pueden soportar un sistema de cobro que cargue a los usuarios por los servicios prestados, con base en la utilización. Los detalles de costos soportan los acuerdos de niveles de servicio. El monitoreo y la evaluación del costo de los servicios se utilizan para optimizar el costo de los recursos de TI. Las cifras obtenidas de los costos se usan para verificar la obtención de beneficios y para el proceso de presupuesto de la organización. Los reportes sobre el costo de los servicios de información brindan advertencias oportunas de cambios en los requerimientos del negocio, por medio del uso de sistemas de reporte inteligentes. Se utiliza un modelo de costos variables, derivado de los volúmenes de datos procesados de cada servicio prestado. La administración de costos se ha llevado a un nivel de

práctica industrial, basada en el resultado de mejoras continuas y de comparación con otras organizaciones. La optimización de costos es un proceso constante. La gerencia revisa los KPIs y KGIs como parte de un proceso de mejora continua en el rediseño de los sistemas de medición de costos.

APENDICE2

ME1 MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI

Descripción del Proceso

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.

ME1.1 Enfoque del Monitoreo
Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI. El marco de trabajo se debería integrar con el sistema de administración del desempeño corporativo.

ME1.2 Definición y recolección de datos de monitoreo
Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes. Los indicadores de desempeño deberían incluir:

- La contribución al negocio que incluya, pero que no se limite a, la información financiera
- Desempeño contra el plan estratégico del negocio y de TI
- Riesgo y cumplimiento de las regulaciones
- Satisfacción del usuario interno y externo
- Procesos clave de TI que incluyan desarrollo y entrega del servicio
- Actividades orientadas a futuro, por ejemplo, la tecnología emergente, la infraestructura re-utilizable, habilidades del personal de TI y del negocio

Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.

ME1.3 Método de monitoreo
Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.

ME1.4 Evaluación del desempeño
Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.

ME1.5 Reportes al consejo directivo y a ejecutivos
Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas administrativas adecuadas.

APENDICE2

ME1.6 Acciones correctivas Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con:

- Revisión, negociación y establecimiento de respuestas administrativas
- Asignación de responsabilidades por la corrección
- Rastreo de los resultados de las acciones comprometidas

APENDICE 2

Modelo de Madurez

La administración del proceso de *Monitorear y evaluar el desempeño de TI* que satisfaga los requerimientos de negocio para TI de *transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI, de acuerdo con los requisitos de gobierno* es:

0 **No existente** cuando
La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de forma independiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de los procesos no se reconoce.

1 **Inicial/Ad Hoc** cuando
La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.

2 **Repetible pero intuitiva** cuando
Se han identificado algunas mediciones básicas a ser monitoreadas. Los métodos y las técnicas de recolección y evaluación existen, pero los procesos no se han adoptado en toda la organización. La interpretación de los resultados del monitoreo se basa en la experiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.

3 **Proceso definido** cuando
La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se han definido, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de satisfacción del cliente y los niveles de servicio están definidas. Se ha definido un marco de trabajo para medir el desempeño.

4 **Administrado y medible** cuando
La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechan en toda la organización para recolectar y monitorear la información operativa de las aplicaciones, sistemas y procesos. La gerencia puede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas. Las mediciones de la función de TI están alienadas con las metas de toda la organización.

5 **Optimizado** cuando
Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos, tales como el Balanced Scorecard. El monitoreo de los procesos y el rediseño continuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización. Benchmarks contra la industria y los competidores clave se han formalizado, con criterios de comparación bien entendidos.

APENDICE 2

ME2 MONITOREAR Y EVALUAR EL CONTROL INTERNO

Descripción del Proceso

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

ME2.1 Monitorear el marco de trabajo de control interno
Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se debería utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI.

ME2.2 Revisiones de Auditoría
Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.

ME2.3 Excepciones de control
Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones se deberían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas.

ME2.4 Auto-evaluación de control
Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.

ME2.5 Aseguramiento del control interno
Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros. Dichas revisiones pueden ser realizadas por la función de cumplimiento corporativo o, a solicitud de la gerencia, por auditoría interna o por auditores y consultores externos o por organismos de certificación. Se deben verificar las aptitudes de los individuos que realicen la auditoria, por ej. Un Auditor de Sistemas de Información Certificado™ (CISA® por sus siglas en Inglés) debe asignarse.

ME2.6 Control interno para terceros
Determinar el estado de los controles internos de cada proveedor externos de servicios. Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales. Esto puede ser provisto por una auditoría externa o se puede obtener de una revisión por parte de auditoría interna y por los resultados de otras auditorias.

ME2.7 Acciones correctivas
Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con:

- La revisión, negociación y establecimiento de respuestas administrativas
- La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos)
- El rastreo de los resultados de las acciones comprometidas

APENDICE 2

Modelo de Madurez

La administración del proceso de *Monitorear y evaluar el control interno* que satisfaga el requisito de negocio de TI de *proteger el logro de los objetivos de TI y cumplir con las leyes y regulaciones relacionadas con TI* es:

0 **No existente** cuando
La organización carece de procedimientos para monitorear la efectividad de los controles internos. Los métodos de reporte de control interno gerenciales no existen. Existe una falta generalizada de conciencia sobre la seguridad operativa y el aseguramiento del control interno de TI. La gerencia y los empleados no tienen conciencia general sobre el control interno.

1 **Inicial/Ad Hoc** cuando
La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.

2 **Repetible pero intuitiva** cuando
La organización utiliza reportes de control informales para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. La gerencia de servicios de información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.

3 **Proceso definido** cuando
La gerencia apoya y ha institucionalizado el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI. Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos.

4 **Administrado y medible** cuando
La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno. Se realizan revisiones entre pares para verificar el monitoreo del control interno.

5 **Optimizado** cuando
La gerencia ha implantado un programa de mejora continua en toda la organización que toma en cuenta las lecciones aprendidas y las mejores prácticas de la industria para monitorear el control interno. La organización utiliza herramientas integradas y actualizadas, donde es apropiado, que permiten una evaluación efectiva de los controles críticos de TI y una detección rápida de incidentes de control de TI. La compartición del conocimiento, específico de la función de servicios de

información, se encuentra implantada de manera formal. El benchmarking con los estándares de la industria y las mejores prácticas está formalizado.

COBIT Y PRODUCTOS RELACIONADOS

El marco COBIT, a partir de la versión 4.0 y posteriores, incluye todo lo siguiente:

- Marco—Explica la forma en que COBIT organiza el Gobierno de TI, la administración y los objetivos de control y buenas prácticas por dominios y procesos de TI, y su vinculación con los requerimientos del negocio
- Descripciones de Procesos —Incluye 34 procesos de TI que cubren las responsabilidades de TI de principio a fin.
- Objetivos de Control—Provee mejores prácticas genéricas de gestión de objetivos para los procesos de TI.
- Directrices de Gestión—Ofrece herramientas para ayudar en la asignación de responsabilidades, la medición del desempeño así como el benchmarking y la identificación de brechas de habilidades.
- Modelos de Madurez—Provee perfiles de los procesos de TI, describiendo estados actuales y futuros.

Desde sus principios, el contenido esencial de COBIT ha evolucionado y continúa haciéndolo, incrementando los productos relacionados y derivados de COBIT:

- *Informe al Consejo sobre el Gobierno de TI, 2da Edición*—Diseñado para ayudar a la Dirección a entender porqué el Gobierno de TI es importante y cuál es su responsabilidad en su gestión.
- COBIT® Online—Permite a los usuarios personalizar una versión COBIT para su empresa y luego almacenar y actualizar dicha versión según sea necesario. Ofrece encuestas en línea y tiempo real, preguntas frecuentes, benchmarking y un foro de discusión para compartir experiencias y preguntas.
- *Prácticas de Control de COBIT®: Guía para alcanzar los Objetivos de Control para un exitoso Gobierno de TI, 2da Edición*—Provee una guía respecto de los riesgos a ser evitados y el valor a ser obtenido por la implementación de un objetivo de control, así como instrucciones acerca de cómo implementar el objetivo. Se recomienda utilizar las Prácticas de Control con la *Guía de Implementación de Gobierno de TI: Utilizando COBIT® and Val IT™, 2da Edición.*
- *Guía de Aseguramiento de TI: Utilizando COBIT®*—Provee una guía sobre cómo utilizar COBIT como soporte a una gran variedad de actividades de aseguramiento y también pruebas sugerida para todos los procesos de TI y los objetivos de control de COBIT. Reemplaza la información de las Directrices de Auditoría para auditoría y autoevaluación contra los objetivos de control de *COBIT 4.1*.
- *Objetivos de Control de TI para Sarbanes-Oxley: El Rol de TI en el Diseño e Implementación de Controles Internos sobre el Reporting Financiero, 2da Edición*—Guía sobre cómo asegurar el cumplimiento en el entorno de TI, basado en los objetivos de control de COBIT.
- *Guía de Implementación de Gobierno de TI: Utilizando COBIT® y Val IT™, 2da Edición*—Provee un mapa de ruta genérico para implementar el gobierno de TI utilizando los recursos de COBIT and Val IT y herramientas de soporte.
- COBIT® *Quickstart*—Provee bases mínimas de control para organizaciones mas pequeñas y una posible etapa inicial para las empresas mas grandes.
- COBIT® *Security Baseline*—Centrada en pasos esenciales para implementar seguridad de la información dentro de la organización.
- Mapas de COBIT—Actualmente disponibles en www.isaca.org/downloads:
  - *Aligning COBIT®, ITIL and ISO 17799 for Business Benefit*
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
  - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 for Software With COBIT® 4.0*
- *Gobierno de la Seguridad de la Información: Guía para el Consejo de Administración y Gerencia Ejecutiva, 2daEdición*—Presenta la seguridad de la información en términos de negocio y contiene técnicas y herramientas de ayuda para descubrir problemas relacionados con la seguridad.

Val IT es el término abarcativo utilizado para describir las publicaciones y futuros productos y actividades adicionales relacionados con el Marco Val IT.

COBIT Y PRODUCTOS RELACIONADOS

Las publicaciones vigentes relacionadas con Val IT son:

- *Valor para la Empresa: Buen Gobierno para las Inversiones de TI—El Marco Val IT™*, que explica cómo una empresa puede obtener el valor óptimo de las inversiones posibilitadas por TI y está basada en el marco COBIT. Está organizada en:
  - Tres procesos—Buen Gobierno del Valor, Gestión del Portafolio de Inversiones y Gestión de Inversiones
  - Prácticas clave de gestión de TI—Prácticas de gestión esenciales que influyen positivamente en el logro de resultados o propósitos de una actividad en particular. Soportan los procesos de Val IT y cumplen a grandes ragos el mismo rol que los objetivos de control de COBIT.
- *Valor para la Empresa: Buen Gobierno para las Inversiones de TI—El Caso de Negocio*, centrado en un elemento clave del procesos de gestión de inversiones
- *Valor para la Empresa: Buen Gobierno para las Inversiones de TI—El Caso de Estudio ING*, describe cómo una empresa de servicios financieros globales gestiona un portafolio de inversiones de TI dentro del contexto del marco Val IT.

Para una completa y actualizada información sobre COBIT, Val IT y productos relacionados, casos de estudio, oportunidades de formación, newsletters y otra información específica sobre marcos: *www.itgi.org*, *www.isaca.org/cobit* y *www.isaca.org/valit.*