GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

4.1

Marco de Trabajo

Objetivos de Control

Directrices Gerenciales

Modelos de Madurez

COBIT 4.1

El IT Governance Institute®
El IT Governance Institute (ITGI™, por sus siglas en Inglés) (*www.itgi.org*) se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. Un gobierno de TI efectivo, ayuda a garantizar que TI soporte las metas del negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociados a la TI. El IT Governance Institute ofrece investigación original, recursos electrónicos y casos de estudio para ayudar a los líderes de las empresas y a sus consejos directivos en sus responsabilidades de Gobierno de TI.

Cláusula de limitación de responsabilidad
El IT Governance Institute (el dueño) diseñó y creó esta publicación titulada COBIT® 4.1 (el Trabajo), en primer lugar como un recurso educacional para los directores ejecutivos de información, para la dirección general, y para los profesionales de administración y control de TI. El dueño no garantiza que el uso de alguna parte del Trabajo asegure un resultado exitoso. No se debe considerar que el Trabajo incluya alguna información, procedimientos o pruebas propias o exclusivas de otra información, procedimientos y pruebas que estén dirigidas a obtener los mismos resultados de modo razonable. Al determinar la propiedad de cualquier información, procedimiento o prueba específica, los directores ejecutivos de información, la dirección general, la gerencia de TI y los profesionales de control, deben aplicar su propio juicio profesional a las circunstancias específicas que surjan de los sistemas específicos o del entorno de tecnología de información.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 EE.UU.
Teléfono: +1.847.590.7491
Fax: +1.847.253.1443
Correo electrónico: *info@itgi.org*
Sitio Web: *www.itgi.org*

COBIT® 4.1
Printed in the United States of America

AGRADECIMIENTOS

IT Governance Institute desea reconocer a:

Desarrolladores Expertos y Revisores

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox TI, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Edward Chavannes, CISA, CISSP, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche LLP, South Africa
Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, TI Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA
Philip Le Grand, Capita Education Services, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA

AGRADECIMIENTOS *CONT.*

Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., South Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
Martin Rosenberg, Ph.D., TI Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Denmark
Jaco Sadie, Sasol, South Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix TI Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgium
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

Junta de Síndicos de ITGI
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, 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 and IGM Financial, Canada, Trustee

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

COBIT 4.1

COBIT 4.1

Índice

Tus comentarios sobre COBIT 4.1 serán bienvenidos. Por favor visita *www.isaca.org/cobitfeedback* para enviar comentarios.

RESUMEN EJECUTIVO

RESUMEN EJECUTIVO

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales.

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte a COSO (Committee Of Sponsoring Organisations Of The Treadway Commission) Marco de Referencia Integrado – Control Interno, el marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como a marcos compatibles similares.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:
- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque hacia procesos de COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de la TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

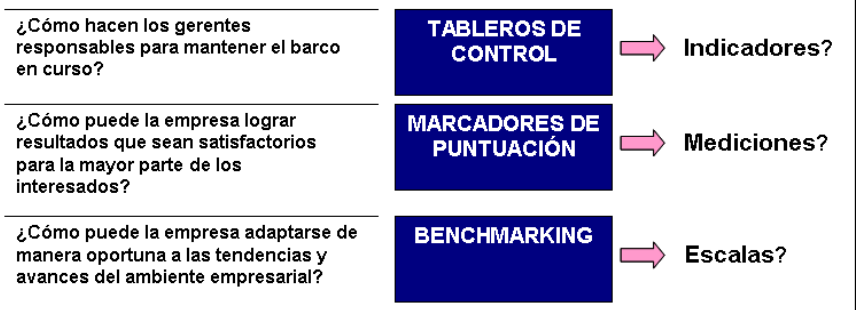
En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

Pero, ¿cómo puede la empresa poner bajo control TI de tal manera que genere la información que la empresa necesita? ¿Cómo puede administrar los riesgos y asegurar los recursos de TI de los cuales depende tanto? ¿Cómo puede la empresa asegurar que TI logre sus objetivos y soporte los del negocio?

Primero, la dirección requiere objetivos de control que definan la meta final de implementar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar un aseguramiento razonable de que:
- Se alcancen los objetivos del negocio.
- Se prevengan o se detecten y corrijan los eventos no deseados.

En segundo lugar, en los complejos ambientes de hoy en día, la dirección busca continuamente información oportuna y condensada, para tomar decisiones difíciles respecto a riesgos y controles, de manera rápida y exitosa. ¿Qué se debe medir y cómo? Las empresas requieren una medición objetiva de dónde se encuentran y dónde se requieren mejoras, y deben implementar una caja de herramientas gerenciales para monitorear esta mejora. La **Figura 1** muestra algunas preguntas frecuentes y las herramientas gerenciales de información usadas para encontrar las respuestas, aunque estos tableros de control requieren indicadores, los marcadores de puntuación requieren mediciones y los Benchmarking requieren una escala de comparación.

Figura 1 – Administración de la Información



Una respuesta a los requerimientos de determinar y monitorear el nivel apropiado de control y desempeño de TI son las definiciones específicas de COBIT de los siguientes conceptos:

- **Benchmarking** de la capacidad de los procesos de TI, expresada como modelos de madurez, derivados del Modelo de Madurez de la Capacidad del Instituto de Ingeniería de Software
- **Metas y métricas** de los procesos de TI para definir y medir sus resultados y su desempeño, basados en los principios de Balanced Scorecard de Negocio de Robert Kaplan y David Norton
- **Metas de actividades** para controlar estos procesos, con base en los objetivos de control detallados de COBIT

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelo de madurez permite identificar y demostrar a la dirección las brechas en la capacidad. Entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.

COBIT da soporte al gobierno de TI (**Figura 2**) al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso). Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para el gobierno de TI. Mientras las otras áreas consideradas contribuyen, la transparencia se logra de forma principal por medio de la medición del desempeño.

Figura 2 – Áreas de Enfoque del Gobierno de TI

- **Alineación Estratégica** se enfoca en garantizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.
- **Entrega de Valor** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.
- **Administración de Recursos** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: , aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.
- **Administración de Riesgos** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.
- **Medición del Desempeño** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

Estas áreas de enfoque de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención para gobernar a TI en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI. COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operativos de TI y del negocio. Se establecieron equivalencias entre los modelos de procesos COBIT y las áreas de enfoque del gobierno de TI (vea Apéndice II, Equivalencia entre procesos de TI y las áreas de enfoque del gobierno de TI, COSO, recursos TI de COBIT y criterios de información COBIT), ofreciendo así un puente entre lo que los gerentes operativos deben realizar y lo que los ejecutivos desean gobernar.

Para lograr un gobierno efectivo, los ejecutivos esperan que los controles a ser implementados por los gerentes operativos se encuentren dentro de un marco de control definido para todo los procesos de TI. Los objetivos de control de TI de COBIT están organizados por proceso de TI; por lo tanto, el marco de trabajo brinda una alineación clara entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

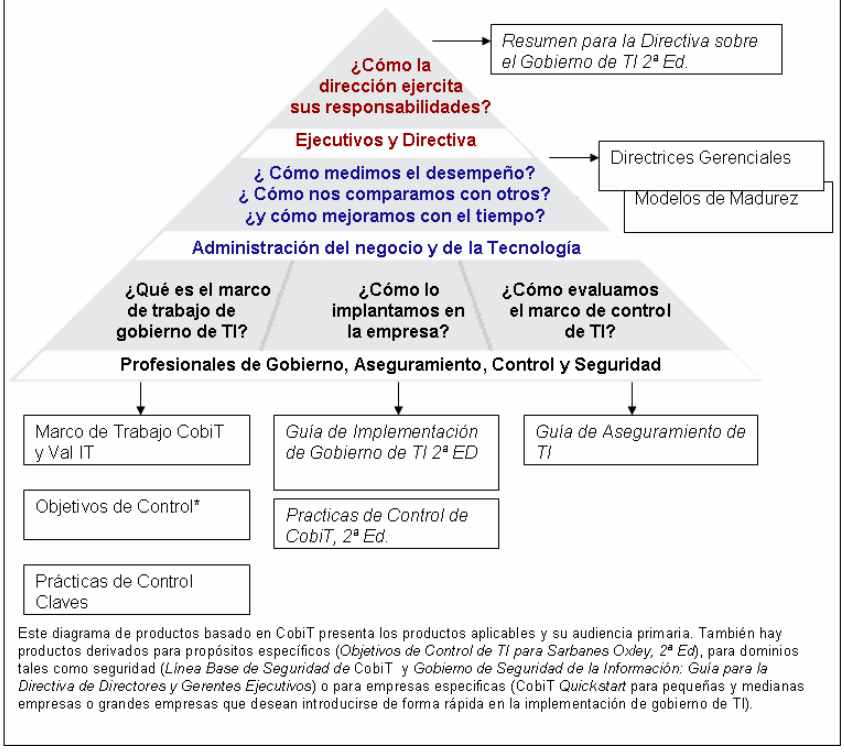
COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI, (vea Apéndice IV). COBIT actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobierno y de negocios.

COSO (y marcos de trabajo compatibles similares) es generalmente aceptado como el marco de trabajo de control interno para las empresas. COBIT es el marco de trabajo de control interno generalmente aceptado para TI.

Los productos COBIT se han organizado en tres niveles (**Figura 3**) diseñados para dar soporte a:

- Administración y consejos ejecutivos
- Administración del negocio y de TI
- Profesionales en Gobierno, aseguramiento, control y seguridad.

Figura 3 – Productos COBIT



Este diagrama de productos basado en CobiT presenta los productos aplicables y su audiencia primaria. También hay productos derivados para propósitos específicos (*Objetivos de Control de TI para Sarbanes Oxley, 2ª Ed*), para dominios tales como seguridad (*Línea Base de Seguridad de* CobiT y *Gobierno de Seguridad de la Información: Guía para la Directiva de Directores y Gerentes Ejecutivos*) o para empresas específicas (CobiT *Quickstart* para pequeñas y medianas empresas o grandes empresas que desean introducirse de forma rápida en la implementación de gobierno de TI).

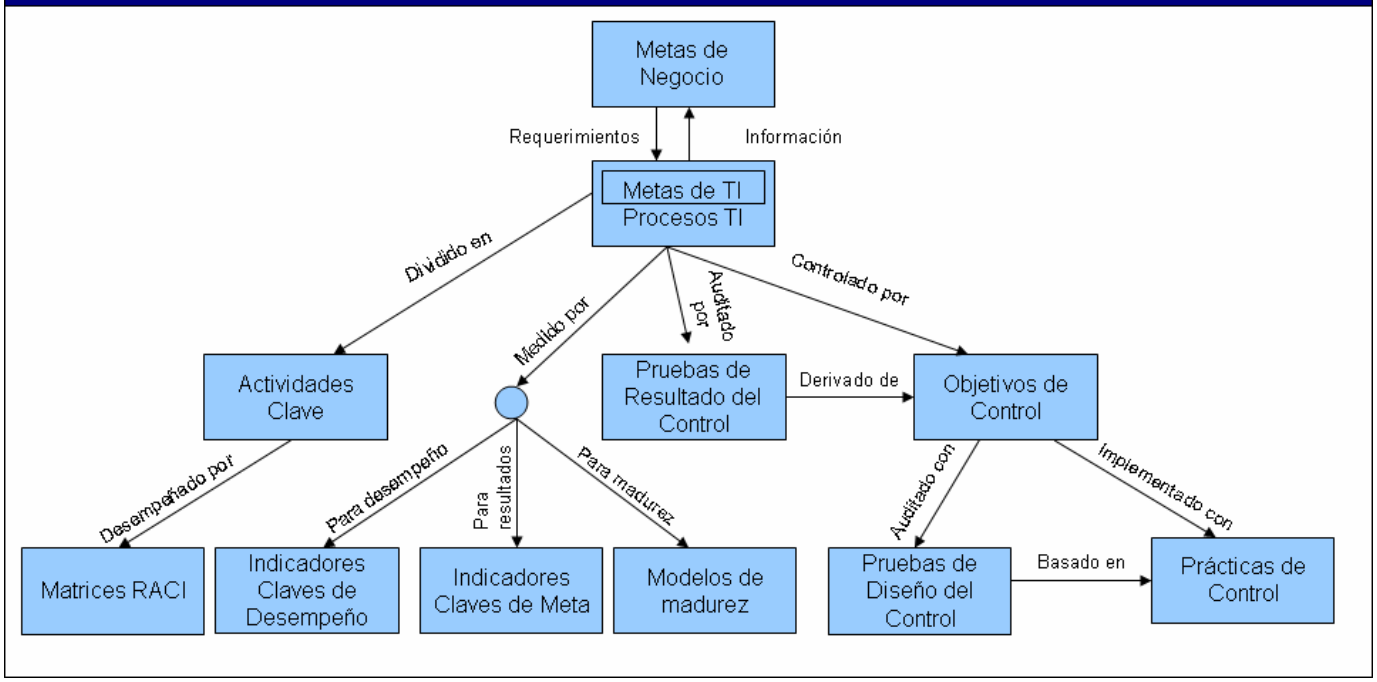
Brevemente, los productos COBIT incluyen:

- El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición—Diseñado para ayudar a los ejecutivos a entender porqué el gobierno de TI es importante, cuáles son sus intereses y cuales son sus responsabilidades para administrarlo.
- Directrices Gerenciales / Modelos de madurez—Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad.
- Marco de Referencia—Explica cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.
- Objetivos de control—Brindan objetivos a la dirección basados en las mejores prácticas genéricas para todas los procesos de TI
- Guía de Implementación de Gobierno de TI: Usando COBIT y Val TI 2ª Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI
- Prácticas de Control de COBIT: Guía para Conseguir los Objetivos de Control para el Éxito del Gobierno de TI 2ª Edición – Proporciona una guía de por qué vale la pena implementar controles y cómo implementarlos.
- Guía de Aseguramiento de TI: Usando COBIT – Proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control.

El diagrama de contenido de COBIT mostrado en la **figura 3** presenta las audiencias principales, sus preguntas sobre gobierno TI y los productos que generalmente les aplican para proporcionar las respuestas. También hay productos derivados para propósitos específicos, para dominios tales como seguridad o empresas especificas.

Todos estos componentes de COBIT se interrelacionan, ofreciendo soporte para las necesidades de gobierno, de administración, de control y de auditoría de los distintos interesados, como se muestra en la **Figura 4**.

Figura 4 – Interrelaciones de los componentes de COBIT



COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:
- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI

El resto de este documento brinda una descripción del marco de trabajo COBIT, así como todos los componentes esenciales organizados por los dominios TI de COBIT y 34 procesos de TI. Esto proporciona un útil libro de referencia para toda la guía principal de COBIT. También se ofrecen varios apéndices como referencias útiles.

La información más reciente sobre COBIT y los productos relacionados, incluyendo herramientas en línea, guías de implementación, casos de estudio, Newsletter y materiales educativos se pueden consultar en *www.isaca.org/cobit.*

Marco de Trabajo CobiT

MARCO DE TRABAJO COBIT

La Misión de COBIT:

Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

LA NECESIDAD DE UN MARCO DE TRABAJO DE CONTROL PARA EL GOBIERNO DE TI

Un marco de control para el Gobierno TI define las razones de por qué se necesita el Gobierno de TI, los interesados y que se necesita cumplir en el gobierno de TI

Por qué

Cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse
- Cuente con un manejo juicioso de los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas

Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI, y encuentran maneras para:

- Alinear la estrategia de TI con la estrategia del negocio
- Asegurar que los inversionistas y accionistas logran un debido cuidado estandarizado para la mitigación de los riesgos de TI
- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa
- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas
- Crear relaciones constructivas y comunicaciones efectivas entre el negocio y TI, y con socios externos
- Medir el desempeño de TI

Las empresas no pueden responder de forma efectiva a estos requerimientos de negocio y de gobierno sin adoptar e implementar un marco de Referencia de gobierno y de control para TI, de tal manera que:

- Se forme un vínculo con los requerimientos del negocio
- El desempeño real con respecto a estos requerimientos sea transparente
- Se organicen sus actividades en un modelo de procesos generalmente aceptado
- Se identifiquen los principales recursos a ser apalancados
- Se definan los objetivos de control Gerenciales a ser considerados

Además, el gobierno y los marcos de trabajo de control están siendo parte de las mejores prácticas de la administración de TI y sirven como facilitadores para establecer el gobierno de TI y cumplir con el constante incremento de requerimientos regulatorios.

Las mejores prácticas de TI se han vuelto significativas debido a varios factores:

- Directores de negocio y consejos directivos que demandan un mayor retorno de la inversión sobre TI, es decir, que TI genere lo que el negocio necesita para mejorar el valor de los Interesados (Stakeholders)
- Preocupación por el creciente nivel de gasto en TI
- La necesidad de satisfacer requerimientos regulatorios para controles de TI en áreas como privacidad y reportes financieros (por ejemplo, Sarbanes-Oxley Act, Basel II) y en sectores específicos como el financiero, farmacéutico y de atención a la salud
- La selección de proveedores de servicio y el manejo de Outsourcing y de Adquisición de servicios
- Riesgos crecientemente complejos de TI como la seguridad de redes
- Iniciativas de gobierno de TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de TI, aumentar el valor del negocio y reducir los riesgos de éste
- La necesidad de optimizar costos siguiendo, siempre que sea posible, un enfoque estandarizado en lugar de enfoques desarrollados en forma especial
- La madurez creciente y la consecuente aceptación de marcos de trabajo respetados tales como COBIT, ITIL, ISO 17799, ISO 9001, CMM y PRINCE2
- La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia (Benchmarking)

Quién

Un marco de referencia de gobierno y de control requiere servir a una variedad de interesados internos y externos, cada uno de los cuales tiene necesidades específicas:

- Interesados dentro de la empresa que tienen interés en generar valor de las inversiones en TI:
  - Aquellos que toman decisiones de inversiones
  - Aquellos que deciden respecto a los requerimientos
  - Aquellos que utilizan los servicios de TI
- Interesados internos y externos que proporcionan servicios de TI:
  - Aquellos que administran la organización y los procesos de TI
  - Aquellos que desarrollan capacidades
  - Aquellos que operan los servicios
- Interesados internos y externos con responsabilidades de control/riesgo:
  - Aquellos con responsabilidades de seguridad, privacidad y/o riesgo
  - Aquellos que realizan funciones de cumplimiento
  - Aquellos que requieren o proporcionan servicios de aseguramiento

Qué

Para satisfacer los requerimientos previos, un marco de referencia para el gobierno y el control de TI, debe satisfacer las siguientes especificaciones generales:

- Brindar un enfoque de negocios que permita la alineación entre las metas de negocio y de TI.
- Establecer una orientación a procesos para definir el alcance y el grado de cobertura, con una estructura definida que permita una fácil navegación en el contenido.
- Ser generalmente aceptable al ser consistente con las mejores prácticas y estándares de TI aceptados, y que sea independiente de tecnologías específicas.
- Proporcionar un lenguaje común, con un juego de términos y definiciones que sean comprensibles en general para todos los Interesados.
- Ayudar a satisfacer requerimientos regulatorios, al ser consistente con estándares de gobierno corporativo generalmente aceptados (COSO) y con controles de TI esperados por reguladores y auditores externos.

Como Satisface COBIT La Necesidad

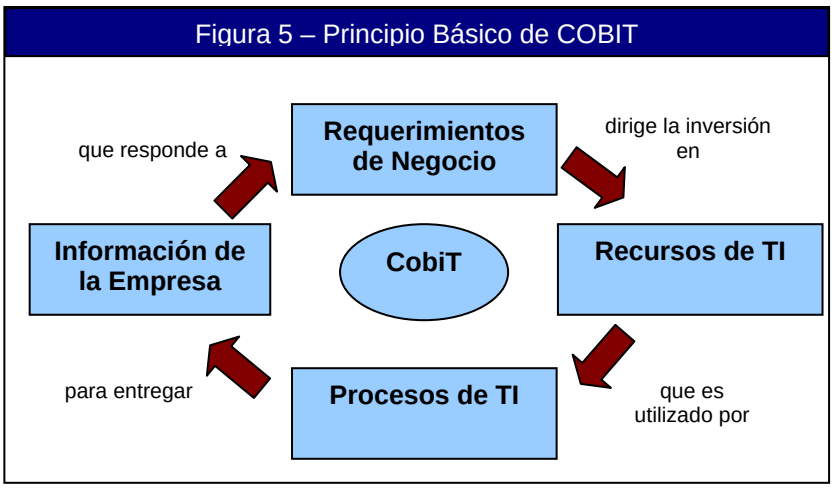
Como respuesta a las necesidades descritas en la sección anterior, el marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

Orientado al negocio

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio (**Figura 5**): Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida.

Figura 5 – Principio Básico de COBIT



El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

CRITERIOS DE INFORMACIÓN DE COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- La **efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La **eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.

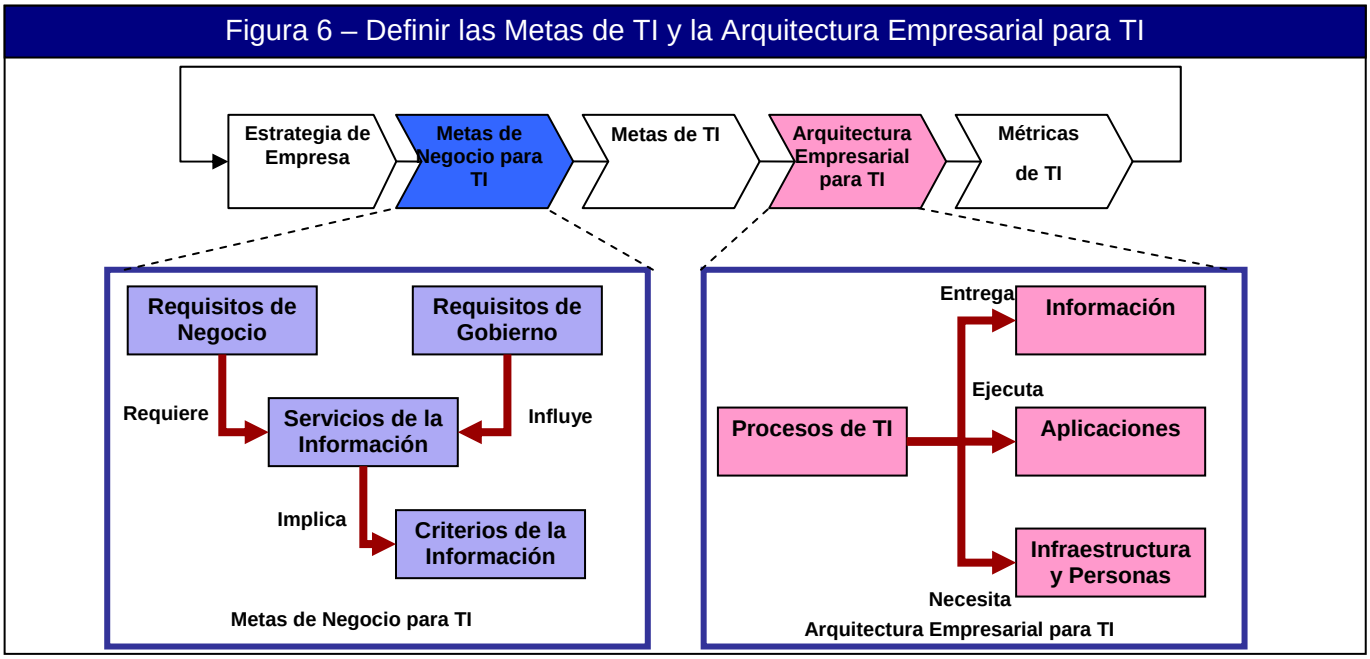
- La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- El **cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La **confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

METAS DE NEGOCIOS Y DE TI

Mientras que los criterios de información proporcionan un método genérico para definir los requerimientos del negocio, la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas. Toda empresa usa TI para habilitar iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI. El Apéndice I proporciona una matriz de metas genéricas de negocios y metas de TI y como se asocian con los criterios de la información. Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.

Si se pretende que TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio (el cliente) y un claro entendimiento para TI, de cómo y qué debe entregar (el proveedor). La **Figura 6** ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos relacionados con iniciativas habilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar, de forma exitosa la parte que le corresponde a TI de la estrategia empresarial. Para que el cliente entienda las metas y los Scorecard de TI, todos estos objetivos y sus métricas asociadas se deben expresar en términos de negocio significativos para el cliente, y esto, combinado con una alineación efectiva de la jerarquía de objetivos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio[1].

Figura 6 – Definir las Metas de TI y la Arquitectura Empresarial para TI



Una vez que han sido definidas las metas alineadas, estás requieren ser monitoreadas para garantizar que la entrega cumple con las expectativas. Esto se logra con métricas derivadas de las metas y capturadas en el scorecard de TI.

Para que el cliente pueda entender las metas de TI y el scorecard de TI, todos estos objetivos y métricas asociadas deben expresarse en términos de negocio significativos para el cliente. Esto, combinado con un alineamiento efectivo de los objetivos jerárquicos aseguraría que el negocio puede confirmar que es probable que TI soporte los objetivos de la empresa.

El apéndice I, Tablas de enlace entre metas y procesos, proporciona una visión global de cómo las metas genéricas de negocio se relacionan con las metas de TI, los procesos de TI y los criterios de la información. Las tablas ayudan a demostrar el ámbito de COBIT y las relaciones completas de negocio entre COBIT y los impulsores de la empresa. La **figura 6** ilustra, que estos impulsores vienen del negocio y desde la capa de Gobierno Corporativo, en primer lugar enfocándose más en las funcionalidades y velocidad de la entrega, mas tarde en la relación costo-eficiencia, retorno de inversión (ROI) y cumplimiento.

RECURSOS DE TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las

[1] Es necesario señalar que la definición e implementación de una arquitectura empresarial para TI creara tambien metas que contribuyen a, pero no se han derivado de, los objetivos de negocio.

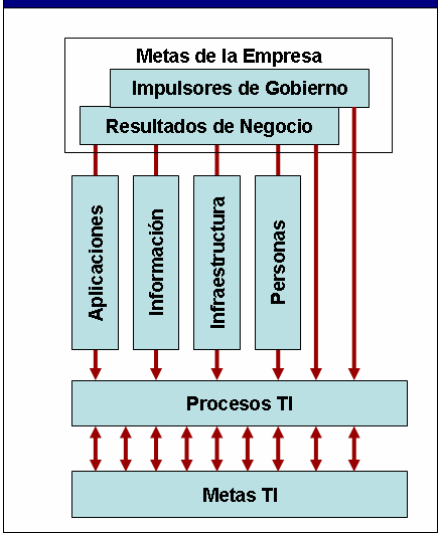
habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI, como se muestra en la **figura 6**.

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (Ej., un sistema de planeación de recursos empresariales [ERP]) para dar soporte a la capacidad del negocio (Ej., implementando una cadena de suministro) que genere el resultado deseado (Ej., mayores ventas y beneficios financieros).

Los recursos de TI identificados en COBIT se pueden definir como sigue:
- Las **aplicaciones** incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La **información** son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- La **infraestructura** es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las **personas** son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

La **Figura 7** resume cómo las metas de negocio para TI influencian la manera en que se manejan los recursos necesarios de TI por parte de los procesos de TI para lograr las metas de TI.

Figura 7 – Gestión de los Recursos de TI para Entregar Metas de TI



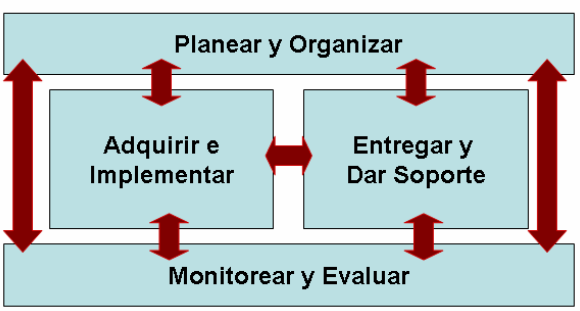
Orientado a Procesos

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. La incorporación de un modelo operativo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas de administración. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios, como se muestra en la **Figura 8**, se llaman:
- **Planear y Organizar (PO)** – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI)** – Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS)** – Recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y Evaluar (ME)** -Monitorear todos los procesos para asegurar que se sigue la dirección provista.

Figura 8 – Los Cuatro Dominios Interrelacionados de COBIT



PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:
- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está

cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:
- ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)
Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos. Por lo general cubre las siguientes preguntas de la gerencia:
- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

MONITOREAR Y EVALUAR (ME)
Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:
- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

A lo largo de estos cuatro dominios, COBIT ha identificado 34 procesos de TI generalmente usados (ver **figura 22** para la lista completa). Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de COBIT. COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aun más, se pueden combinar como se necesite por cada empresa.

Para cada uno de estos 34 procesos, tiene un enlace a las metas de negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuales son sus actividades clave y entregables principales, y quién es el responsable de ellas.

Basado en controles

COBIT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación.

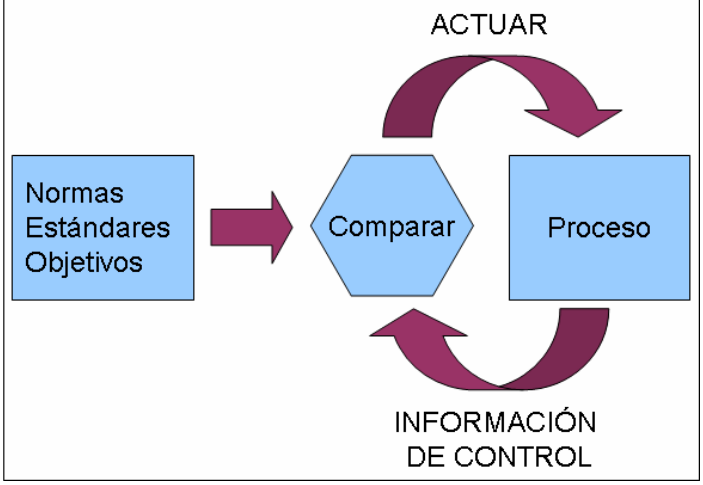
LOS PROCESOS REQUIEREN CONTROLES
Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Ellos:
- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:
- Seleccionando aquellos aplicables.
- Decidir aquellos que deben implementarse.
- Elegir como implementarlos (frecuencia, extensión, automatización, etc.)
- Aceptar el riesgo de no implementar aquellos que podrían aplicar.

La guía se puede obtener del modelo de control estándar mostrado en la **figura 9**. Sigue los principios que se evidencian en la siguiente analogía: cuando se ajusta la temperatura ambiente (estándar) para el sistema de calefacción (proceso), el sistema verificará de forma constante (comparar) la temperatura ambiente (inf. de control) e indicará (actuar) al sistema de calefacción para que genere más o menos calor.

Figura 9 – Modelo de Control



La gerencia de operaciones usa los procesos para organizar y administrar las actividades de TI en curso. COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia de operaciones de TI y para la gerencia de negocios. Para lograr un gobierno efectivo, los gerentes de operaciones deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y varios de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa Control de Proceso número. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.

PC1 Metas y Objetivos del Proceso
Definir y comunicar procesos, metas y objetivos específicos, medibles, accionables, reales, orientados a resultado y en tiempo (SMARRT) para la ejecución efectiva de cada proceso de TI. Asegurando que están enlazados a las metas de negocio y se soportan por métricas adecuadas.

PC2 Propiedad del Proceso
Asignar un dueño para cada proceso de TI, y definir claramente los roles y responsabilidades del dueño del proceso. Incluye, por ejemplo, responsabilidad del diseño del proceso, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño del proceso y la identificación de mejora de las oportunidades.

PC3 Proceso Repetible
Diseñar y establecer cada proceso clave de TI de tal manera que sea repetible y consecuentemente produzca los resultados esperados. Proveer una secuencia lógica pero flexible y escalable de actividades que lleve a los resultados deseados y que sea lo suficientemente ágil para manejar las excepciones y emergencias. Usar procesos consistentes, cuando sea posible, y ajustarlos sólo cuando no se pueda evitar.

PC4 Roles y Responsabilidades
Definir las actividades clave y entregables finales del proceso. Asignar y comunicar roles y responsabilidades no ambiguas para la ejecución efectiva y eficiente de las actividades clave y su documentación, así como la rendición de cuentas para los entregables finales del proceso.

PC5 Políticas, Planes y Procedimientos
Definir y comunicar cómo todas las políticas, planes y procedimientos que dirigen los procesos de TI están documentados, revisados, mantenidos, aprobados, almacenados, comunicados y usados para el entrenamiento. Asignar responsabilidades para cada una de estas actividades y en momentos oportunos, revisar si se ejecutan correctamente. Asegurar que las políticas, planes y procedimientos son accesibles, correctos, entendidos y actualizados

PC6 Desempeño del Proceso
Identificar un conjunto de métricas que proporcionen visión de las salidas y el desempeño del proceso. Establecer objetivos que se reflejen en las metas del proceso y los indicadores de desempeño de tal manera que permitan el logro de las metas de los procesos. Definir como los datos son obtenidos. Comparar las medidas actuales con los objetivos y tomar las acciones sobre las desviaciones cuando sea necesario. Alinear métricas, objetivos y métodos con el enfoque de monitoreo global del desempeño de TI.

Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia, debido a que habrá menos errores y un enfoque de administración más consistente.

Además, COBIT ofrece ejemplos ilustrativos para cada proceso, los cuales no son exhaustivos o preceptivos de:
- Entradas y salidas genéricas
- Actividades y guías sobre roles y responsabilidades en una matriz RACI
- Metas de actividades clave (las cosas más importantes a realizar)
- Métricas

Además de evaluar qué controles son requeridos, los dueños de procesos deben entender qué entradas requieren de otros procesos y qué requieren otros de sus procesos. COBIT brinda ejemplos genéricos de las entradas y salidas clave para cada proceso incluyendo los requerimientos externos de TI. Existen algunas salidas que son entradas a todos los demás procesos, marcadas como "TODOS" en las tablas de salidas, pero no se mencionan como entradas en todos los procesos, y por lo general incluyen estándares de calidad y requerimientos de métricas, el marco de trabajo de procesos de TI, roles y responsabilidades documentados, el marco de control empresarial de TI, las políticas de TI, y roles y responsabilidades del personal.

El entendimiento de los roles y responsabilidades para cada proceso es clave para un gobierno efectivo. COBIT proporciona una matriz RACI (quién es responsable, quién rinde cuentas, quién es consultado y quien informado) para cada proceso. Rendir cuentas significa la responsabilidad termina aquí'—ésta es la persona que provee autorización y direccionamiento a una actividad. Responsabilidad se refiere a la persona que realiza la actividad. Los otros dos roles (consultado e informado) garantizan que todas las personas que son requeridas están involucradas y dan soporte al proceso.

CONTROLES DEL NEGOCIO Y DE TI

El sistema de control interno de la empresa impacta en TI a tres niveles:

- Al nivel de dirección ejecutiva, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.
- Al nivel de procesos de negocio, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.
- Para soportar los procesos de negocio, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operativos y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad.

CONTROLES GENERALES DE TI Y CONTROLES DE APLICACIÓN

Los controles generales son aquellos que están inmersos en los procesos y servicios de TI. Algunos ejemplos son:

- Desarrollo de sistemas
- Administración de cambios
- Seguridad
- Operaciones de computo

Los controles incluidos en las aplicaciones de los procesos del negocio se conocen por lo general como controles de aplicación. Ejemplos:

- Integridad (Completitud)
- Precisión
- Validez
- Autorización
- Segregación de funciones

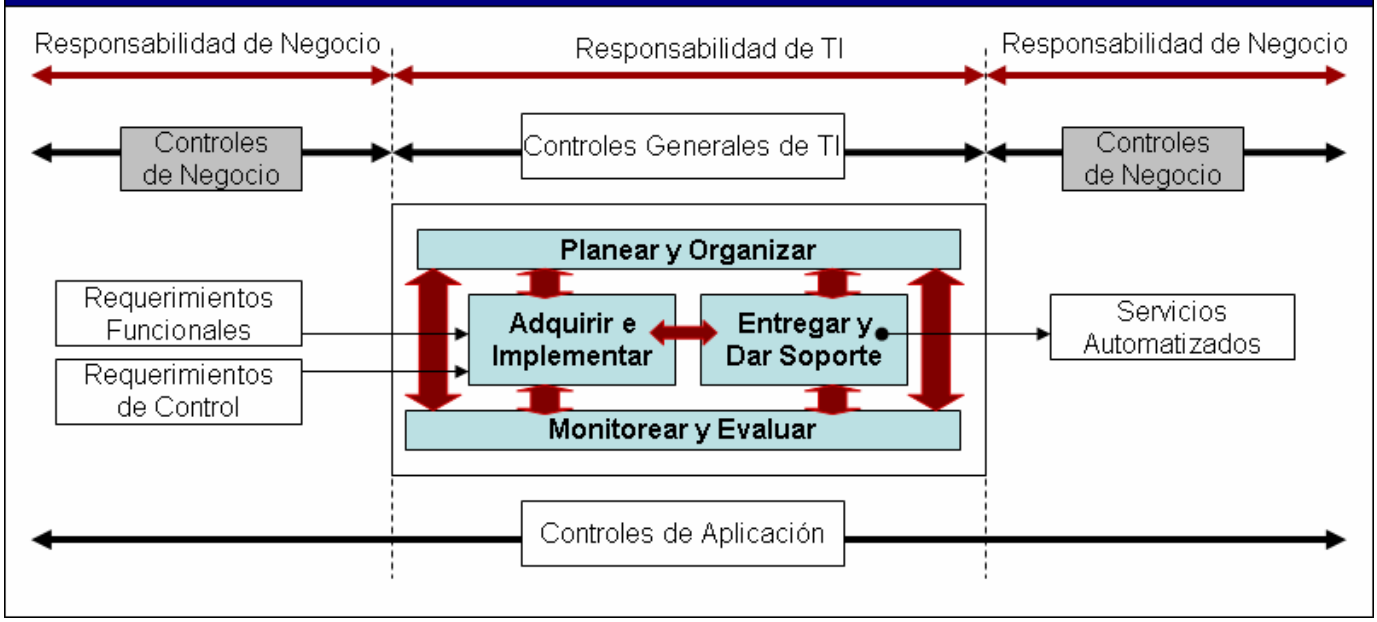
COBIT asume que el diseño e implementación de los controles de aplicación automatizados son responsabilidad de TI, y están cubiertos en el dominio de Adquirir e Implementar, con base en los requerimientos de negocio definidos, usando los criterios de información de COBIT. La responsabilidad operativa de administrar y controlar los controles de aplicación no es de TI, sino del dueño del proceso de negocio.

Por lo tanto, la responsabilidad de los controles de aplicación es una responsabilidad conjunta, fin a fin, entre el negocio y TI, pero la naturaleza de la responsabilidad cambia de la siguiente manera:

- La empresa es responsable de:
  - Definir apropiadamente los requisitos funcionales y de control
  - Uso adecuadamente los servicios automatizados
- TI es responsable de:
  - Automatizar e implementar los requisitos de las funciones de negocio y de control
  - Establecer controles para mantener la integridad de controles de aplicación.

Por lo tanto, los procesos de TI de COBIT abarcan a los controles generales de TI, pero sólo los aspectos de desarrollo de los controles de aplicación; la responsabilidad de definir y el uso operativo es de la empresa.

Figura 10 – Fronteras de los Controles de Negocio, Generales y Aplicación



La siguiente lista ofrece el conjunto recomendado de objetivos de control de aplicaciones. Identificados por ACn, de Control de Aplicación número (por sus siglas en inglés):

AC1 Preparación y Autorización de Información Fuente.
Asegurar que los documentos fuente están preparados por personal autorizado y calificado siguiendo los procedimientos establecidos, teniendo en cuenta una adecuada segregación de funciones respecto al origen y aprobación de estos documentos. Los errores y omisiones pueden ser minimizados a través de buenos diseños de formularios de entrada. Detectar errores e irregularidades para que sean informados y corregidos.

AC2 Recolección y Entrada de Información Fuente.
Establecer que la entrada de datos se realice en forma oportuna por personal calificado y autorizado. Las correcciones y reenvíos de los datos que fueron erróneamente ingresados se deben realizar sin comprometer los niveles de autorización de las transacciones originales. En donde sea apropiado para reconstrucción, retener los documentos fuente originales durante el tiempo necesario.

AC3 Chequeos de Exactitud, Integridad y Autenticidad
Asegurar que las transacciones son exactas, completas y válidas. Validar los datos ingresados, y editar o devolver para corregir, tan cerca del punto de origen como sea posible.

AC4 Integridad y Validez del Procesamiento
Mantener la integridad y validación de los datos a través del ciclo de procesamiento. Detección de transacciones erróneas no interrumpe le procesamiento de transacciones validas.

AC5 Revisión de Salidas, Reconciliación y Manejo de Errores
Establecer procedimientos y responsabilidades asociadas para asegurar que la salida se maneja de una forma autorizada, entregada al destinatario apropiado, y protegida durante la transmisión; que se verifica, detecta y corrige la exactitud de la salida; y que se usa la información proporcionada en la salida.

AC6 Autenticación e Integridad de Transacciones
Antes de pasar datos de la transacción entre aplicaciones internas y funciones de negocio/operativas (dentro o fuera de la empresa), verificar el apropiado direccionamiento, autenticidad del origen e integridad del contenido. Mantener la autenticidad y la integridad durante la transmisión o el transporte.

Impulsado por la medición

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar. Para decidir el nivel correcto, la gerencia debe preguntarse: ¿Hasta dónde debemos ir?, y ¿está el costo justificado por el beneficio?

La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. COBIT atiende estos temas a través de:

- Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad
- Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard)
- Metas de actividades para facilitar el desempeño efectivo de los procesos

MODELOS DE MADUREZ

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que consideren qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo beneficio y éstas preguntas relacionadas:

- ¿Qué está haciendo nuestra competencia en la industria, y cómo estamos posicionados en relación a ellos?
- ¿Cuáles son las mejores prácticas aceptables en la industria, y cómo estamos posicionados con respecto a estas prácticas?
- Con base en estas comparaciones, ¿se puede decir que estamos haciendo lo suficiente?
- ¿Cómo identificamos lo que se requiere hacer para alcanzar un nivel adecuado de administración y control sobre nuestros procesos de TI?

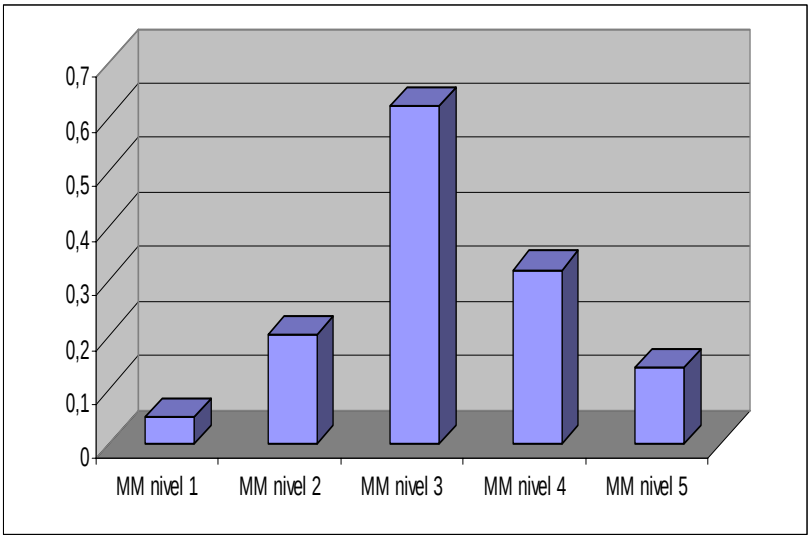
Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación para benchmarking y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el dueño del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control. Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, a diferencia de la aproximación del CMM original de SEI, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud. Una evaluación de la madurez de COBIT resultara en un perfil donde las condiciones relevantes a diferentes niveles de madurez se han conseguido, como se muestra en el ejemplo gráfico de la **figura 11**.

Figura 11 – Posible Nivel de Madurez de un Proceso de TI



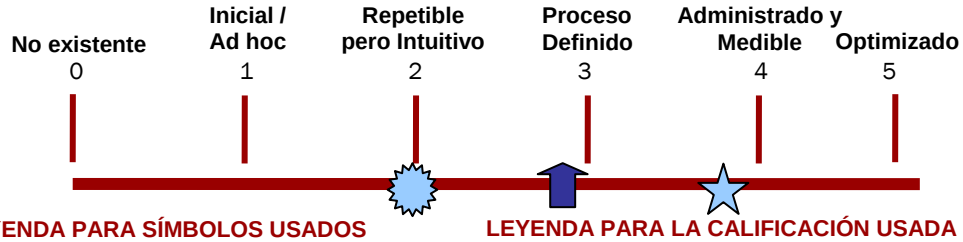
Posible nivel de madurez de un proceso de TI: El ejemplo ilustra un proceso que esta ampliamente en el nivel 3, pero cumple algunas acciones con menor nivel de requerimiento mientras sigue investigando en la medición del desarrollo

Esto se debe a que cuando se emplea la evaluación de la madurez con los modelos de COBIT, a menudo algunas implementaciones estarán en diferentes niveles aunque no esté completa o suficiente. Estas fortalezas pueden apalancarse para seguir mejorando la madurez. Por ejemplo, algunas partes del proceso pueden estar bien definidas, y, aún cuando esté incompleto, sería erróneo decir que no está definido del todo.

Utilizando los modelos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la gerencia podrá identificar:
- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa
- El crecimiento requerido entre “como es” y “como será”

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método gráfico de presentación (**figura 12**).

Figura 12 – Representación Gráfica de los Modelos de Madurez



LEYENDA PARA SÍMBOLOS USADOS

- Estado actual de la empresa
- Promedio de la industria
- Objetivo de la empresa

LEYENDA PARA LA CALIFICACIÓN USADA

0 - No se aplican procesos administrativos en lo absoluto
1 - Los procesos son ad-hoc y desorganizados
2 - Los procesos siguen un patrón regular
3 - Los procesos se documentan y se comunican
4 - Los procesos se monitorean y se miden
5 - Las buenas prácticas se siguen y se automatizan

El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la **figura 13**.

COBIT es un marco de referencia desarrollado para la administración de procesos de TI con un fuerte enfoque en el control. Estas escalas deben ser prácticas en su aplicación y razonablemente fáciles de entender. El tema de procesos de TI es esencialmente complejo y subjetivo, por lo tanto, es más fácil abordarlo por medio de evaluaciones fáciles que aumenten la conciencia, que logren un consenso amplio y que motiven la mejora. Estas evaluaciones se pueden realizar ya sea contra las descripciones del modelo de madurez como un todo o con mayor rigor, en cada una de las afirmaciones individuales de las descripciones. De cualquier manera, se requiere experiencia en el proceso de la empresa que se está revisando.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. La escala incluye al 0 ya que es muy posible que no existan procesos en lo absoluto. La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

Sin embargo, la capacidad administrativa de un proceso no es lo mismo que el desempeño. La capacidad requerida, como se determina en el negocio y en las metas de TI, puede no requerir aplicarse al mismo nivel en todo el ambiente de TI, es decir, de forma inconsistente o sólo a un número limitado de sistemas o unidades. La medición del desempeño, como se cubre en los próximos párrafos, es esencial para determinar cual es el desempeño real de la empresa en sus procesos de TI.

Figura 13 – Modelo Genérico de Madurez

0 No Existente- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

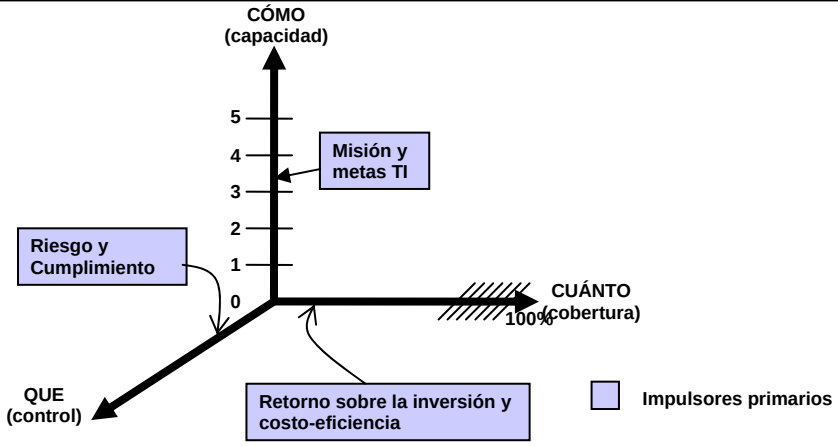
4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Aunque una capacidad aplicada de forma apropiada reduce los riesgos, una empresa debe analizar los controles necesarios para asegurar que el riesgo sea mitigado y que se obtenga el valor de acuerdo al apetito de riesgo y a los objetivos del negocio. Estos controles son dirigidos por los objetivos de control de COBIT. El Apéndice III brinda un modelo de madurez para el control interno que ilustra la madurez de una empresa con respecto al establecimiento y desempeño del control interno. Con frecuencia, este análisis se inicia como respuesta a impulsores externos, aunque idealmente debería ser institucionalizado como se documenta en los procesos de COBIT *PO6 Comunicar las aspiraciones y la dirección de la Gerencia* y ME2 *Monitorear y evaluar el control interno*.

La capacidad, el desempeño y el control son dimensiones de la madurez de un proceso como se ilustra en la **figura 14**.

Figura 14 – Las Tres Dimensiones de la Madurez



El modelo de madurez es una forma de medir qué tan bien están desarrollados los procesos administrativos, esto es, qué tan capaces son en realidad. Qué tan bien desarrollados o capaces deberían ser, principalmente dependen de las metas de TI y en las necesidades del negocio subyacentes a las cuales sirven de base. Cuánta de esa capacidad es realmente utilizada actualmente para retornar la inversión deseada en una empresa. Por ejemplo, habrá procesos y sistemas críticos que requieren de una mayor administración de la seguridad que otros que son menos críticos. Por otro lado, el grado y sofisticación de los controles que se requiere aplicar en un proceso están más definidos por el apetito de riesgo de una empresa y por los requerimientos aplicables.

Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran. El nivel de madurez correcto estará influenciado por los objetivos de negocio de una empresa, por el ambiente operativo y por las prácticas de la industria. Específicamente, el nivel de madurez en la administración se basará en la dependencia que tenga la empresa en TI, en su sofisticación tecnológica y, lo más importante, en el valor de su información.

Un punto de referencia estratégico para una empresa que ayuda a mejorar la administración y el control de los procesos de TI se

puede encontrar observando los estándares internacionales y las mejores prácticas. Las prácticas emergentes de hoy en día se pueden convertir en el nivel esperado de desempeño del mañana y por lo tanto son útiles para planear dónde desea estar la empresa en un lapso de tiempo.

Los modelos de madurez se desarrollan empezando con el modelo genérico cualitativo (consulte la **figura 13**) al cual se añaden, en forma creciente, algunos principios contenidos en los siguientes atributos, a través de niveles:
- Conciencia y comunicación
- Políticas, estándares y procedimientos
- Herramientas y automatización
- Habilidades y experiencia
- Responsabilidad y rendición de cuentas
- Establecimiento y medición de metas

La tabla de atributos de madurez que se muestra en la **figura 15** lista las características de cómo se administran los procesos de TI y describe cómo evolucionan desde un proceso no existente hasta uno optimizado. Estos atributos se pueden usar para una evaluación más integral, para un análisis de brechas y para la planeación de mejoras.

En resumen, los modelos de madurez brindan un perfil genérico de las etapas a través de las cuales evolucionan las empresas para la administración y el control de los procesos de TI, estos son:
- Un conjunto de requerimientos y los aspectos que los hacen posibles en los distintos niveles de madurez
- Una escala donde la diferencia se puede medir de forma sencilla
- Una escala que se presta a sí misma para una comparación práctica
- La base para establecer el estado actual y el estado deseado
- Soporte para un análisis de brechas para determinar qué se requiere hacer para alcanzar el nivel seleccionado
- Tomado en conjunto, una vista de cómo se administra TI en la empresa

Los modelos de madurez COBIT se enfocan en la capacidad, y no necesariamente en el desempeño. No son un número al cual hay que llegar, ni están diseñados para ser una base formal de certificación con niveles discretos que formen umbrales difíciles de atravesar. Sin embargo, se diseñaron para ser aplicables siempre, con niveles que brindan una descripción que una empresa pueda reconocer como la mejor para sus procesos. El nivel correcto está determinado por el tipo de empresa, por su medio ambiente y por la estrategia.

El desempeño, o la manera en que la capacidad se usa y se implanta, es una decisión de rentabilidad. Por ejemplo, un alto nivel de administración de la seguridad quizá se tenga que enfocar sólo en los sistemas empresariales más críticos.

Para finalizar, mientras los niveles de madurez más altos aumentan el control del proceso, la empresa aún necesita analizar, con base en los impulsores de riesgo y de valor, cuáles mecanismos de control debe aplicar. Las metas genéricas de negocio y de TI, como se definen en este marco de trabajo, ayudarán a realizar este análisis. Los objetivos de control de COBIT guían los mecanismos de control y éstos se enfocan en qué se hace en el proceso; los modelos de madurez se enfocan principalmente en qué tan bien se administra un proceso. El Apéndice III brinda un modelo de madurez genérico que muestra el estatus del ambiente de control interno y el establecimiento de controles en una empresa.

Un ambiente de control implantado de forma adecuada, se logra cuando se han conseguido los tres aspectos de madurez (capacidad, desempeño y control). El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menos errores, más procesos predecibles y un uso rentable de los recursos.

MEDICIÓN DEL DESEMPEÑO

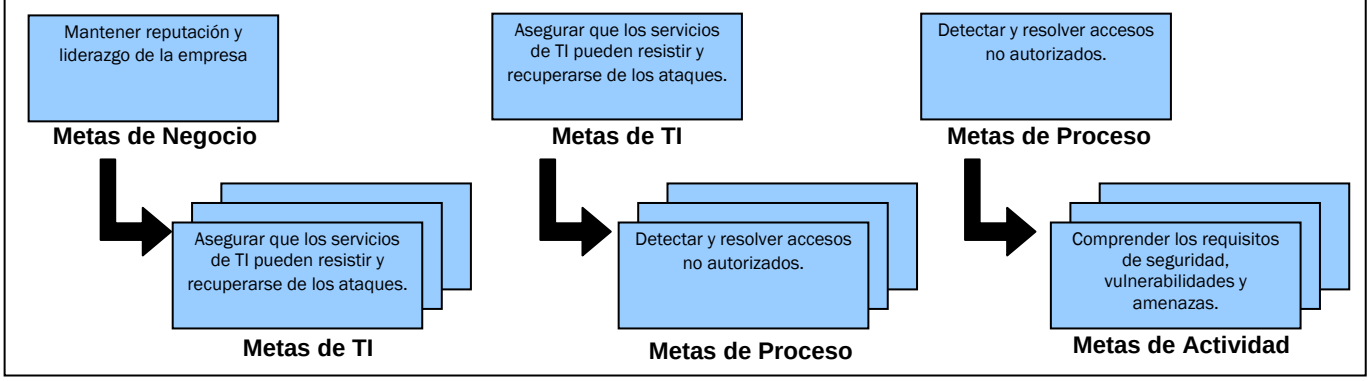
Las métricas y las metas se definen en COBIT a tres niveles:
- Las metas y métricas de TI que definen lo que el negocio espera de TI (lo que el negocio usaría para medir a TI)
- Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI (cómo sería medido el dueño del proceso de TI)
- Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas).

Figura 15 - Tabla de Atributos de Madurez

	Conciencia y Comunicación	Políticas, Estándares y Procedimientos	Herramientas y Automatización	Habilidades y Experiencia	Responsabilidad y Rendición de Cuentas	Establecimiento y Medición de Metas
1	Surge el reconocimiento de la necesidad del proceso. Existe comunicación esporádica de los problemas.	Existen enfoques ad hoc hacia los procesos y las prácticas. Los procesos y las prácticas no están definidos	Pueden existir algunas herramientas; el uso se basa en herramienta estándar de escritorio. No existe un enfoque planeado para el uso de herramientas	No están definidas las habilidades requeridas para el proceso. No existe un plan de entrenamiento y no hay entrenamiento formal.	No existe definición de responsabilidades y de rendición de cuentas. Las personas toman la propiedad de los problemas con base en su propia iniciativa de manera reactiva.	Las metas no están claras y no existen las mediciones.
2	Existe conciencia de la necesidad de actuar. La gerencia comunica los problemas generales.	Surgen procesos similares y comunes pero en su mayoría son intuitivos y parten de la experiencia individual. Algunos aspectos de los procesos son repetibles debido a la experiencia individual, y puede existir alguna documentación y entendimiento informal de políticas y procedimientos.	Existen enfoques comunes para el uso de herramientas pero se basan en soluciones desarrolladas por individuos clave. Pueden haberse adquirido herramientas de proveedores, pero probablemente no se aplican de forma correcta o incluso no usarse.	Se identifican los requerimientos mínimos de habilidades para áreas críticas. Se da entrenamiento como respuesta a las necesidades, en lugar de hacerlo con base en un plan acordado. Existe entrenamiento informal sobre la marcha.	Un individuo asume su responsabilidad, y por lo general debe rendir cuentas aún si esto no está acordado de modo formal. Existe confusión acerca de la responsabilidad cuando ocurren problemas y una cultura de culpas tiende a existir.	Existen algunas metas; se establecen algunas mediciones financieras pero solo las conoce la alta dirección. Hay monitoreo inconsistente en áreas aisladas.
3	Existe el entendimiento de la necesidad de actuar. La gerencia es más formal y estructurada en su comunicación.	Surge el uso de buenas prácticas. Los procesos, políticas y procedimientos están definidos y documentados para todas las actividades clave.	Existe un plan para el uso y estandarización de las herramientas para automatizar el proceso. Se usan herramientas por su propósito básico, pero pueden no estar de acuerdo al plan acordado, y	Se definen y documentan los requerimientos y habilidades para todas las áreas. Existe un plan de entrenamiento formal pero todavía se basa en iniciativas individuales.	La responsabilidad y la rendición de cuentas sobre los procesos están definidas y se han identificado a los dueños de los procesos de negocio. Es poco probable que el dueño del proceso tenga la autoridad plena para	Se establecen algunas mediciones y metas de efectividad, pero no se comunican, y existe una relación clara con las metas del negocio. Surgen los procesos de medición pero no se aplican de modo consistente. Se adoptan ideas de
4	Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.	El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento.	Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas. Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.	Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación. Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta la compartición del conocimiento.	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar sus responsabilidades. Existe una cultura de recompensas que activa la acción positiva.	La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balanced scorecard de TI en algunas áreas, con excepciones conocidas por la gerencia y se está estandarizando el anál
5	Existe un entendimiento avanzado y a futuro de los requerimientos. Existe una comunicación proactiva de los problemas, basada en las tendencias, se aplican técnicas maduras de comunicación y se usan herramientas integradas de comunicación	Se aplican las mejores prácticas y estándares externos. La documentación de procesos ha evolucionado a flujos de trabajo automatizados. Los procesos, las políticas y los procedimientos están estandarizados e integrados para permitir una administración y mejora extremo a extremo.	Se usan juegos de herramientas estandarizados a lo largo de la empresa. Las herramientas están completamente integradas con otras herramientas relacionadas para permitir un soporte integral de los procesos. Se usan las herramientas para dar soporte a la mejora de los procesos y automáticamente detectar excepciones a los controles.	La organización fomenta de manera formal la mejora continua de las habilidades, con base en metas personales y organizacionales claramente definidas. El entrenamiento y la educación dan soporte a las mejores prácticas externas y al uso de conceptos y técnicas. Compartir el conocimiento es una cultura empresarial, y se están desarrollando sistemas basados en el conocimiento. Expertos externos y líderes industriales se emplean como guía.	Los dueños de procesos tienen la facultad de tomar decisiones y medidas. La aceptación de la responsabilidad ha descendido en cascada a través de la organización de forma consistente.	Existe un sistema de medición de desempeño integrado que liga al desempeño de TI con las metas del negocio por la aplicación global del balanced scorecard de TI. La dirección nota las excepciones de forma global y consistente y el análisis de causas raíz

Las metas están definidas de arriba hacia abajo por lo que una meta de negocio determinará varias metas de TI que la soporten. Una meta de TI se logra por un proceso o la interacción de varios procesos. Por lo tanto, las metas de TI ayudan a definir las diferentes metas de proceso. A su vez, cada meta de proceso requiere varias actividades, estableciendo así las metas de actividad. La figura 16 proporciona un ejemplo de las relaciones de las metas de negocio, TI, procesos y actividades.

Figura 16 – Ejemplo de Relaciones entre Metas

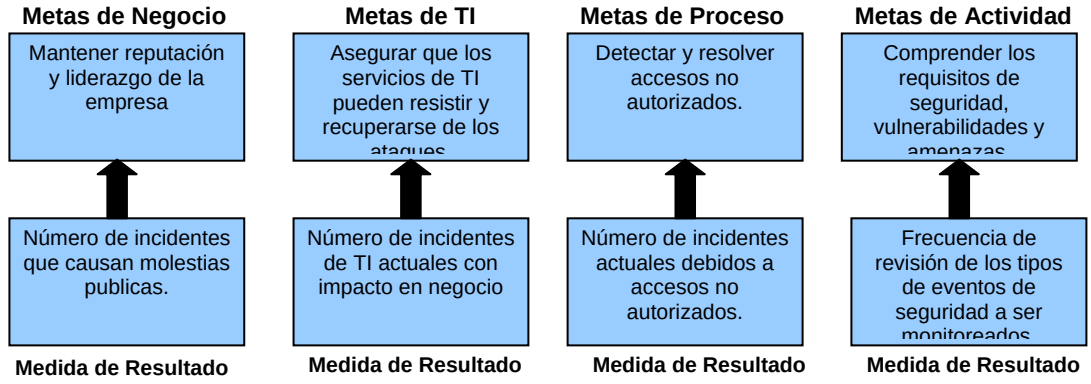


Los términos KGI y KPI, empleados en versiones anteriores de COBIT, se han sustituido por dos tipos de métricas:

- Medidas de Resultado, anteriormente indicador clave de meta (KGIs), indican cuando las metas se han conseguido. Estas pueden medirse sólo después el hecho y, por eso, se llaman 'indicadores pasados'.
- Los Indicadores de Desempeño, anteriormente indicadores clave de desempeño (KPIs), indican si es probable conseguir la meta. Se pueden medir antes de que el resultado sea claro y, por eso, se llaman 'indicadores futuros'.

La **figura 17** proporciona posibles metas o medidas de resultado para los ejemplos utilizados.

Figura 17 – Posibles Medidas de Resultados para el Ejemplo de la Figura 16



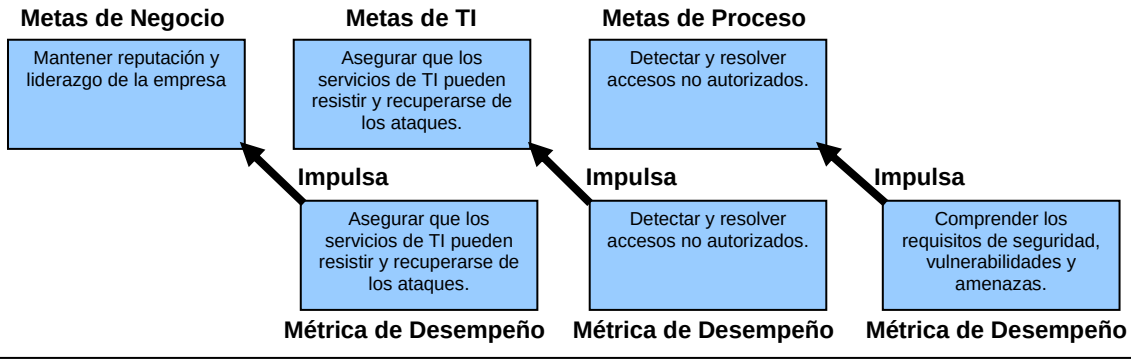
Las medidas de resultado de el nivel mas bajo se convierten en indicadores de desempeño para las de nivel mas alto. Como por ejemplo en la **figura 16**, una medida de resultado indica que la detección y resolución de accesos no autorizados tienen como objetivo indicar que los servicios de TI pueden resistir y recuperarse de los ataques. Como decíamos, la medida de resultados se ha convertido en indicador de desempeño para la meta de mayor nivel. La **figura 18** ilustra como las medidas de resultados del ejemplo se convierten en métricas de desempeño.

Los indicadores de resultado definen mediciones que informan a gerencia—después del hecho—cuando una función, proceso o actividad de TI ha alcanzado sus metas. Los indicadores de resultados de las funciones de TI a menudo se expresan en términos de criterios de la información:

- Disponibilidad de información necesaria para dar soporte a las necesidades del negocio
- Ausencia de riesgos de integridad y de confidencialidad
- Eficiencia en costos de procesos y operaciones
- Confirmación de confiabilidad, efectividad y cumplimiento

Los indicadores de desempeño definen las medidas que determinan lo bien que el negocio, la función de TI o los procesos de TI se están realizando para que se consigan las metas. Son indicadores futuros de que las metas serán probablemente conseguidas, impulsando así a las metas de nivel más alto. A menudo miden la disponibilidad de capacidades, prácticas y habilidades apropiadas, y el resultado de las actividades subyacentes. Por ejemplo, un servicio entregado por TI es una meta para TI pero es un indicador de desempeño y una capacidad para el negocio. Esto es debido a que los indicadores de desempeño se refieren a veces como impulsores de desempeño, particularmente en balanced scorecards.

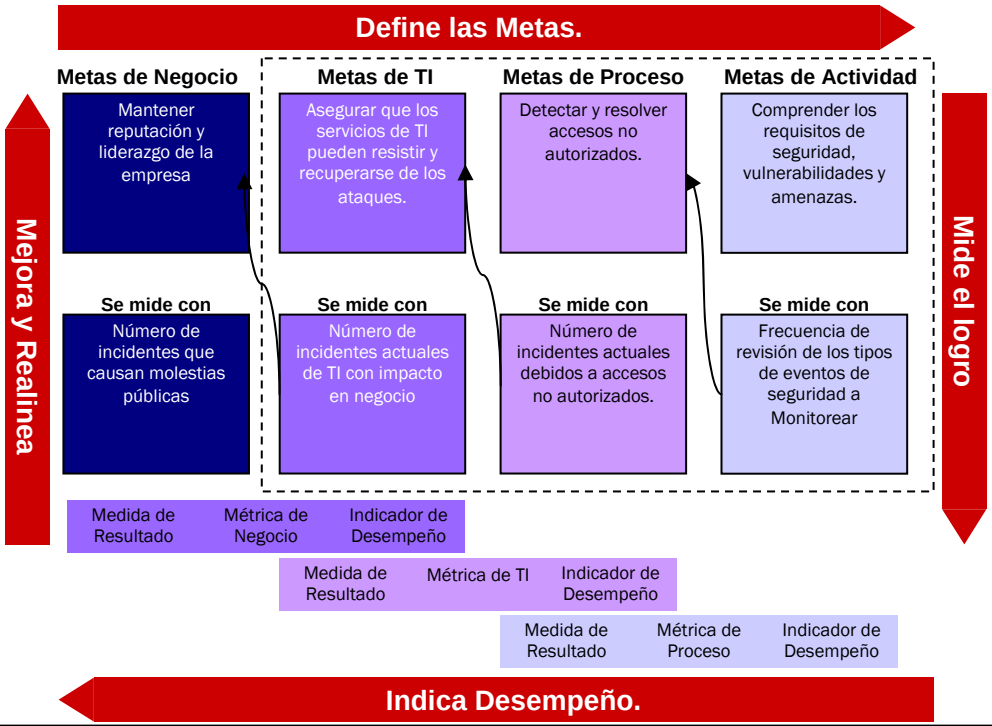
Figura 18 – Posibles Impulsores de Desempeño para el Ejemplo de la Figura 16



Por lo tanto, las métricas provistas son tanto medidas de resultado de la función de TI, proceso de TI o meta de la actividad que miden, como un indicador de desempeño que impulsa las metas de más alto nivel del negocio, función de TI o proceso de TI.

La **figura 19** ilustra la relación entre las metas de negocio, de TI, de proceso y de las actividades, y las diferentes métricas. La cascada de metas es ilustrada desde arriba a la izquierda hasta arriba a la derecha. Debajo de la meta está su medida de resultado. La flecha indica que la misma métrica es un indicador de desempeño para la meta de más alto nivel.

Figura 19 – Relación entre Procesos, Metas y Métricas (DS5)



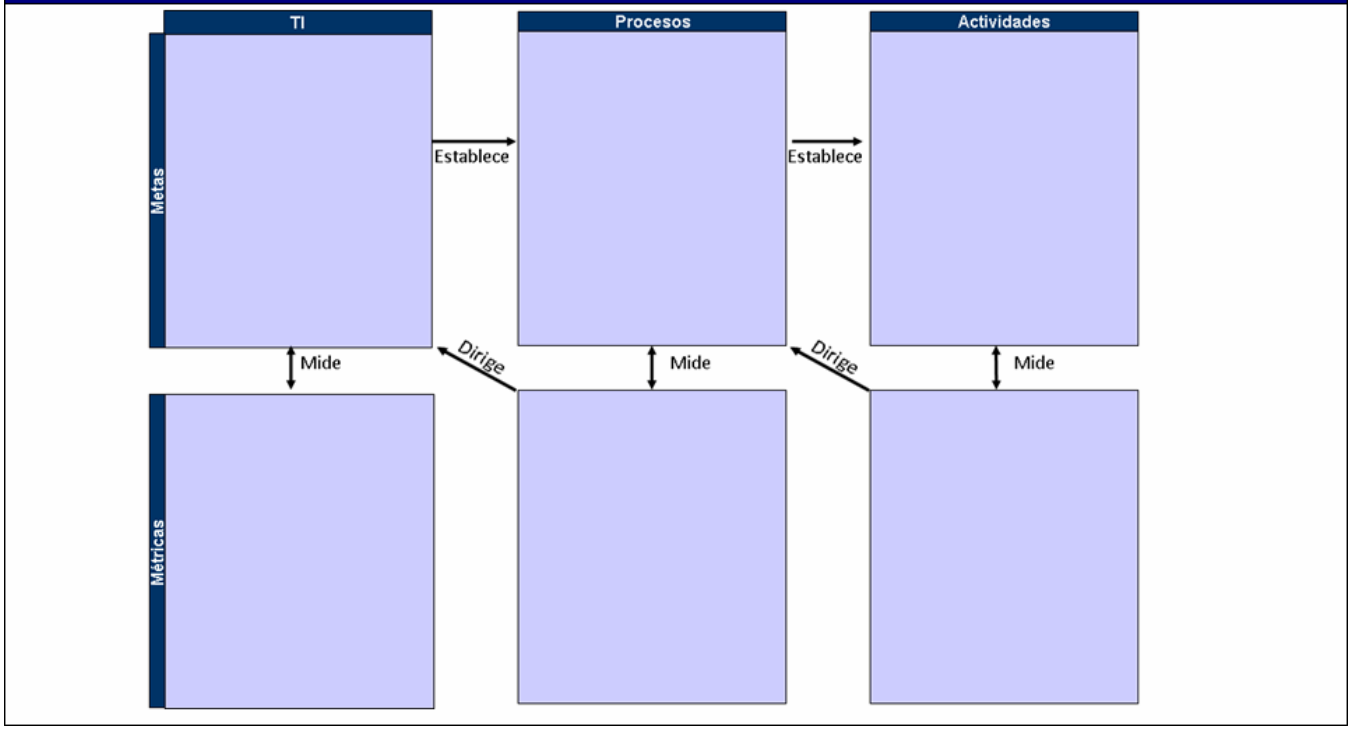
El ejemplo proporcionado es del DS5 Garantizar la Seguridad de los Sistemas. COBIT proporciona métricas sólo para los resultados de las metas de TI marcadas por la línea punteada. Mientras que también son indicadores de desempeño para las metas de negocio para TI, COBIT no proporciona medidas de resultado para las metas de negocio.

Las metas de negocio y TI utilizadas en la sección de metas y métricas de COBIT, incluyendo su relación, son proporcionas en el apéndice I. Para cada proceso de TI en COBIT, las metas y métricas se presentan, como se indica en la **figura 20**.

Las métricas se han desarrollado con las características siguientes en mente:

- Un alto ratio de visión a esfuerzo (Ej., visión del desempeño y logro de las metas comparado con el esfuerzo de capturarlas)
- Comparable internamente (Ej. Porcentaje contra una base o números en el tiempo)
- Comparable externamente sin tener en cuenta el tamaño de la empresa o industria.
- Mejor tener pocas métricas buenas (puede incluso ser una muy buena que puede ser influenciadas por diferentes significados) que una lista más larga de métricas de poca calidad.
- Fácil de medir, no confundir con los objetivos.

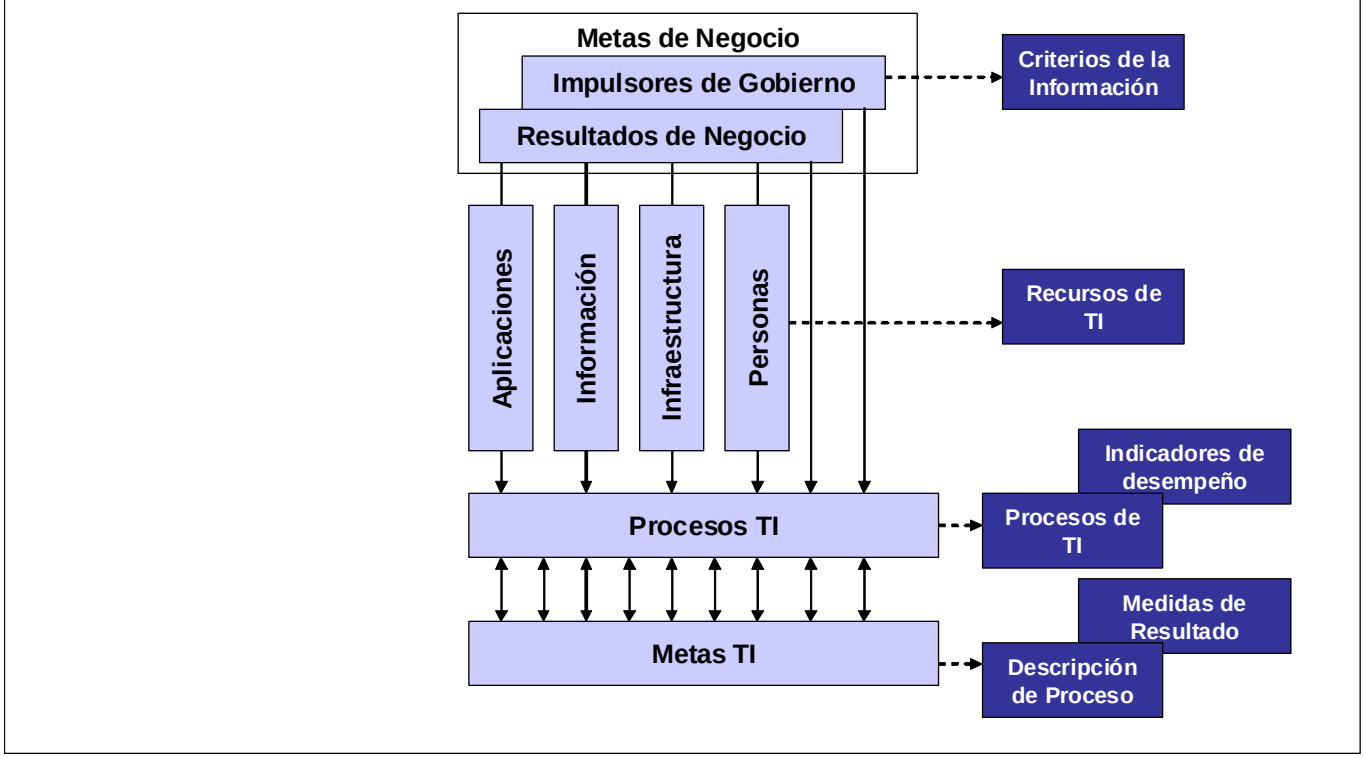
Figura 20 – Presentación de Metas y Métricas



El Modelo del Marco de Trabajo de COBIT

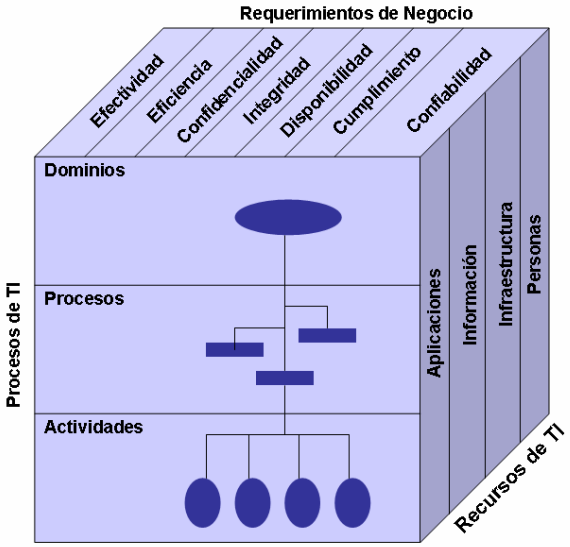
El marco de trabajo COBIT, por lo tanto, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicios de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las metas y métricas de COBIT, como se ilustra en la **figura 21**.

Figura 21 – COBIT Gestión, Control, Alineamiento y Monitoreo



Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT (**figura 22**).

Figura 22 – El Cubo de COBIT



En detalle, el marco de trabajo general COBIT se muestra gráficamente en la **figura 23**, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

Aceptabilidad General de COBIT

COBIT se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes y se adapta a principios de gobierno generalmente aceptados. Está posicionado a un nivel alto, impulsado por los requerimientos del negocio, cubre el rango completo de actividades de TI, y se concentra en lo *que* se debe lograr en lugar de *cómo* lograr un gobierno, administración y control efectivos. Por lo tanto, funciona como un integrador de prácticas de gobierno de TI y es de interés para la dirección ejecutiva; para la gerencia del negocio, para la gerencia y gobierno de TI; para los profesionales de aseguramiento y seguridad; así como para los profesionales de auditoría y control de TI. Está diseñado para ser complementario y para ser usado junto con otros estándares y mejores prácticas.

La implantación de las mejores prácticas debe ser consistente con el gobierno y el marco de control de la empresa, debe ser apropiada para la organización, y debe estar integrada con otros métodos y prácticas que se utilicen. Los estándares y las mejores prácticas no son una panacea y su efectividad depende de cómo hayan sido implementados en realidad y de cómo se mantengan actualizados. Son más útiles cuando se aplican como un conjunto de principios y como un punto de partida para adaptar procedimientos específicos. La gerencia y el equipo deben entender qué hacer, cómo hacerlo y porqué es importante hacerlo para garantizar que se utilicen las prácticas.

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en general a toda empresa. Las prácticas y los estándares específicos que cubren áreas discretas, se pueden equiparar con el marco de trabajo de COBIT, brindando así una jerarquía de materiales guía.

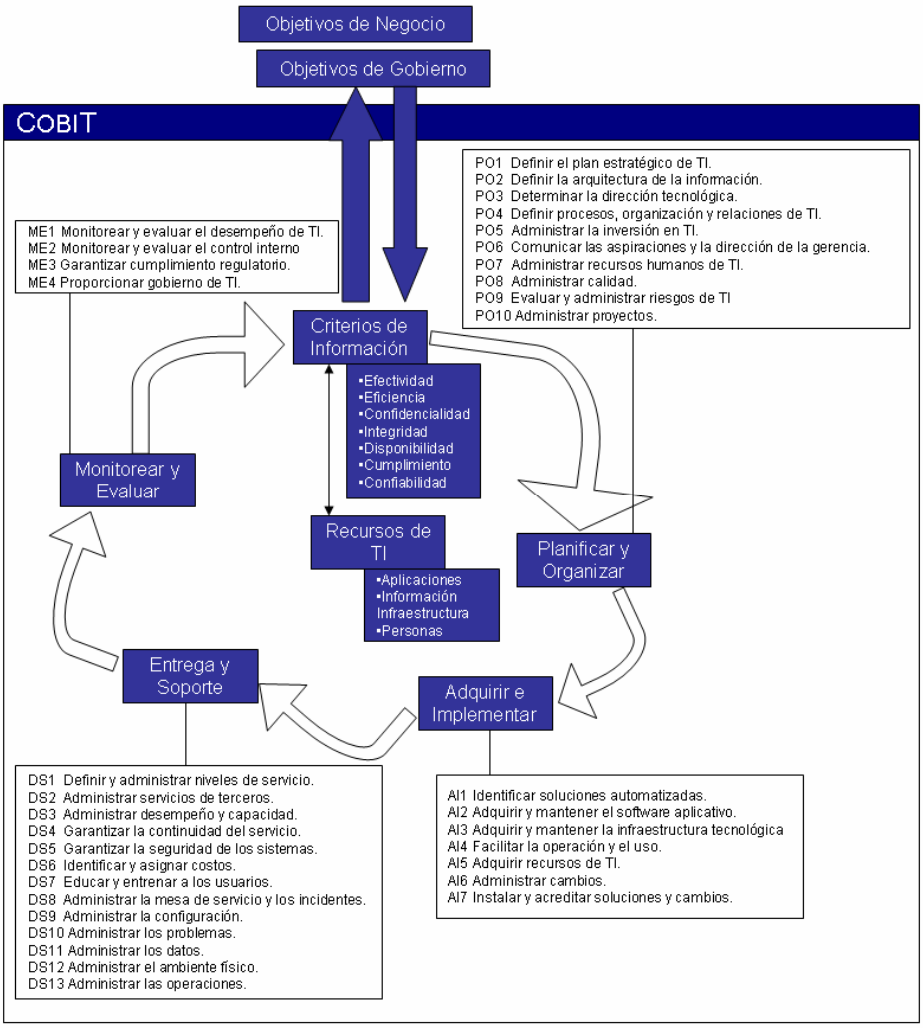
COBIT resulta de interés a distintos usuarios:

- **Dirección ejecutiva**— Para obtener valor de las inversiones y para balancear las inversiones en riesgo y control en un ambiente de TI con frecuencia impredecible
- **Gerencia del negocio**—Para obtener certidumbre sobre la administración y control de los servicios de TI, proporcionados internamente o por terceros
- **Gerencia de TI**—Para proporcionar los servicios de TI que el negocio requiere para dar soporte a la estrategia del negocio de una forma controlada y administrada
- **Auditores**—Para respaldar sus opiniones y/o para proporcionar asesoría a la gerencia sobre controles internos

COBIT ha sido desarrollado y es mantenido por un instituto de investigación sin ánimo de lucro, tomando la experiencia de los miembros de sus asociaciones afiliadas, de los expertos de la industria, y de los profesionales de control y seguridad. Su contenido se basa en una investigación continua sobre las mejores prácticas de TI y se le da un mantenimiento continuo, proporcionando así un recurso objetivo y práctico para todo tipo de usuario.

COBIT está orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que esté alineado con los principios de Gobierno Corporativo y, por lo tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva, para los auditores y reguladores. En el Apéndice II, se ofrece un mapa que muestra cómo los objetivos de control detallados de COBIT se relacionan con las cinco áreas de enfoque del gobierno de TI y con las actividades de control de COSO.

Figura 23 – Marco de Trabajo Completo de COBIT



La **figura 24** resume cómo los distintos elementos del marco de trabajo de COBIT se relacionan con las áreas de enfoque del gobierno de TI.

Figura 24 – Marco de trabajo CobiT y Áreas de Enfoque de Gobierno de TI

	Metas	Métricas	Practicas	Modelos de Madurez
Alineamiento Estratégico	P	P		
Entrega de Valor		P	S	P
Gestión de Riesgos		S	P	S
Gestión de Recursos		S	P	P
Medición del Desempeño	P	P		S

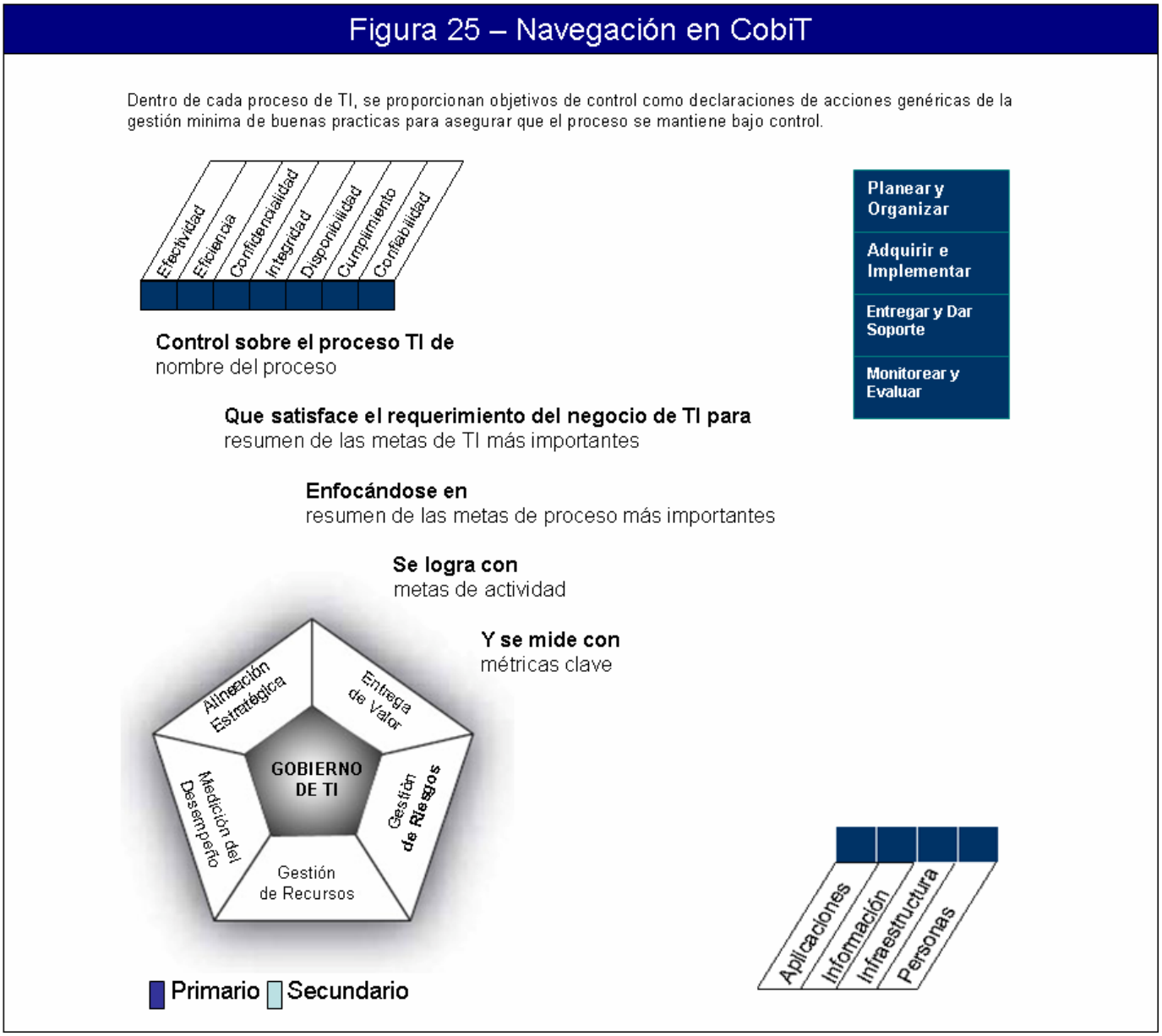
P = Facilitador Primario S = Facilitador Secundario

CÓMO UTILIZAR ESTE LIBRO

Navegación en el Marco de Trabajo COBIT

Para cada uno de los procesos TI de COBIT, se proporciona un objetivo de control de alto nivel, junto con las metas y métricas clave en forma de cascada (**figura 25**).

Figura 25 – Navegación en CobiT



Introducción a los Componentes Esenciales de COBIT

El marco de trabajo de COBIT está compuesto de los siguientes componentes esenciales, incluidos en el resto de esta publicación y organizados en los 34 procesos de TI, brindando así una visión completa de cómo controlar, administrar y medir cada proceso. Cada proceso está cubierto en cuatro secciones, y cada sección constituye aproximadamente una página, de la manera siguiente:

- La sección 1 (**figura 25**) contiene una descripción del proceso que resume los objetivos del proceso, con el objetivo de control de alto nivel representado en formada de cascada. Esta página también muestra el mapeo de este proceso con los criterios de información, con los recursos de TI y con las áreas de enfoque de gobierno de TI, indicando con una P la relación primaria y con una S la secundaria.
- La sección 2 contiene los objetivos de control detallados para este proceso.
- La sección 3 contiene las entradas y salidas del proceso, la matriz RACI, las metas y las métricas.
- La sección 4 contiene el modelo de madurez para el proceso.

Otra forma de visualizar el contenido del desempeño del proceso es:
- Las entradas del proceso son lo que el dueño del proceso requiere de otros.
- Los objetivos de control en la descripción del proceso describen lo que el dueño requiere hacer.
- Las salidas del proceso son lo que el dueño debe entregar.
- Las metas y las métricas describen cómo se debe medir el proceso.
- La matriz RACI define qué se debe delegar y a quién.
- El modelo de madurez muestra qué se debe hacer para mejorar.

Los roles en la matriz RACI están clasificados para todos los procesos como sigue:
- Director ejecutivo (CEO)
- Director financiero (CFO)
- Ejecutivos del negocio
- Director de Informática (CIO)
- Dueño del proceso de negocio
- Jefe de operaciones
- Arquitecto en jefe
- Jefe de desarrollo
- Jefe de administración de TI (para empresas grandes, el jefe de funciones como recursos humanos, presupuestos y control interno)
- La oficina o función de administración de proyectos (PMO)
- Cumplimiento, auditoría, riesgo y seguridad (grupos con responsabilidades de control que no tienen responsabilidades operativas de TI)

Ciertos procesos específicos tienen un rol adicional especializado específico para ese proceso, Ej., mesa de servicio/administrador de incidentes para DS8.

Se debe observar que, a pesar de que el material es recolectado de cientos de expertos, después de una rigurosa investigación y revisión, las entradas, salidas, responsabilidades, métricas y metas son ilustrativas y no así preceptivas o exhaustivas. Proporcionan una base de conocimiento base del cual cada empresa debe seleccionar lo que aplica de forma eficiente y efectiva, con base en las metas y políticas de la estrategia empresarial.

Usuarios de los Componentes de COBIT

La gerencia puede emplear el material de COBIT para evaluar los procesos de TI empleando las metas de negocio y las metas de TI detalladas en el apéndice I para clarificar los objetivos de los procesos de TI y los procesos de los modelos de madurez para evaluar el desempeño actual.

Los implementadores y auditores pueden identificar requisitos de control aplicables desde los objetivos de control y responsabilidades desde las actividades y matrices RACI asociadas.

Todos los usuarios potenciales se pueden beneficiar del uso del contenido de COBIT como una aproximación completa a la gestión y gobierno de TI, junto con otros modelos de estándares detallados como:
- ITIL para la entrega de servicio
- CMM para la entrega de soluciones
- ISO 17799 para seguridad de la información
- PMBOK o PRINCE2 para la administración de proyectos

Apéndices

Se proporcionan las siguientes secciones de referencia adicional al final del libro:
- I. Relación entre metas de negocio y metas de TI (tres tablas)
- II. Equivalencia entre procesos de TI y las áreas de enfoque del gobierno de TI, COSO, recursos TI de COBIT y criterios de información COBIT
- III. Modelo de madurez para el control interno
- IV. Material primario de referencia para COBIT 4.1
- V. Referencias cruzadas entre COBIT® 3ª Edición© y COBIT 4.1
- VI. Enfoque hacia la investigación y desarrollo
- VII. Glosario
- VIII. COBIT y Productos Relacionados.

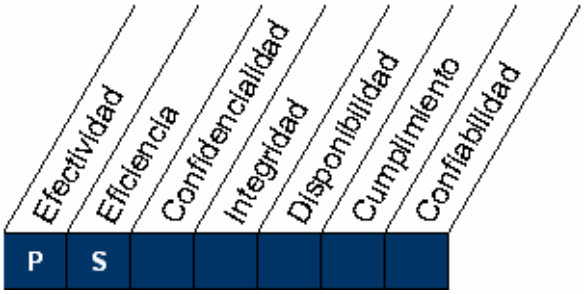
PLANEAR Y ORGANIZAR

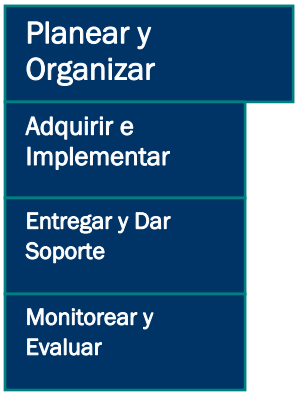
PO1	Definir un Plan Estratégico de TI
PO2	Definir la Arquitectura de la Información
PO3	Determinar la Dirección Tecnológica
PO4	Definir los Procesos, Organización y Relaciones de TI
PO5	Administrar la Inversión en TI
PO6	Comunicar las Aspiraciones y la Dirección de la Gerencia
PO7	Administrar Recursos Humanos de TI
PO8	Administrar la Calidad
PO9	Evaluar y Administrar los Riesgos de TI
PO10	Administrar Proyectos

DESCRIPCIÓN DEL PROCESO.

P01 Definir un Plan Estratégico de TI.

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. La estrategia de negocio y prioridades se reflejarán en portafolios y se ejecutarán por los planes estratégicos de TI, que especifican objetivos concisos, planes de acción y tareas que están comprendidas y aceptadas tanto por el negocio como por TI.





Control sobre el proceso TI de

Definir un plan estratégico para TI

Que satisface el requerimiento del negocio de TI para

Sostener o extender los requerimientos de gobierno y de la estrategia del negocio, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos

Enfocándose en

La incorporación de TI y de la gerencia del negocio en la traducción de los requerimientos del negocio a ofertas de servicio, y el desarrollo de estrategias para entregar estos servicios de una forma transparente y rentable

Se logra con

- El compromiso con la alta gerencia y con la gerencia del negocio para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras
- El entendimiento de las capacidades actuales de TI
- La aplicación de un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del negocio

Y se mide con

- El porcentaje de objetivos de TI en el plan estratégico de TI, que dan soporte al plan estratégico del negocio
- El porcentaje de proyectos TI en el portafolio de proyectos que se pueden rastrear hacia el plan táctico de TI
- El retraso entre las actualizaciones del plan estratégico de TI y las actualizaciones de los planes tácticos de TI

OBJETIVOS DE CONTROL

PO1 Definir un Plan Estratégico de 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, cronograma 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 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 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 y la Capacidad 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 Plan Estratégico de TI
Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán 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 obtención, 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 Planes Tácticos de TI
Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir 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 de proyectos. 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 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 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 comisionar los proyectos requeridos al momento de lanzar el programa.

DIRECTRICES GERENCIALES

P01 Definir un Plan Estratégico de TI.

Desde	Entradas
PO5	Reportes de costo / beneficio
PO9	Evaluación de riesgo
PO10	Portafolio de proyectos actualizado
DS1	Requerimientos de servicio nuevos / actualizados; portafolio de servicios actualizado
*	Estrategia y prioridades del negocio
*	Portafolio de programas
ME1	Entradas a desempeño de planeación de TI
ME4	Reporte del estado del gobierno de TI; dirección estratégica de la empresa para TI

* Entradas provenientes de fuentes externas a COBIT

Salidas	Hacia						
Plan estratégico de TI	PO2..PO6	PO8	PO9	AI1	DS1		
Plan táctico de TI	PO2..PO6	PO9	AI1	DS1			
Portafolios de proyectos de TI	PO5	PO6	PO10	AI6			
Portafolio de servicios de TI	PO5	PO6	PO9	DS1			
Estrategia de contratación externa de TI	DS2						
Estrategia de adquisición de TI	AI5						

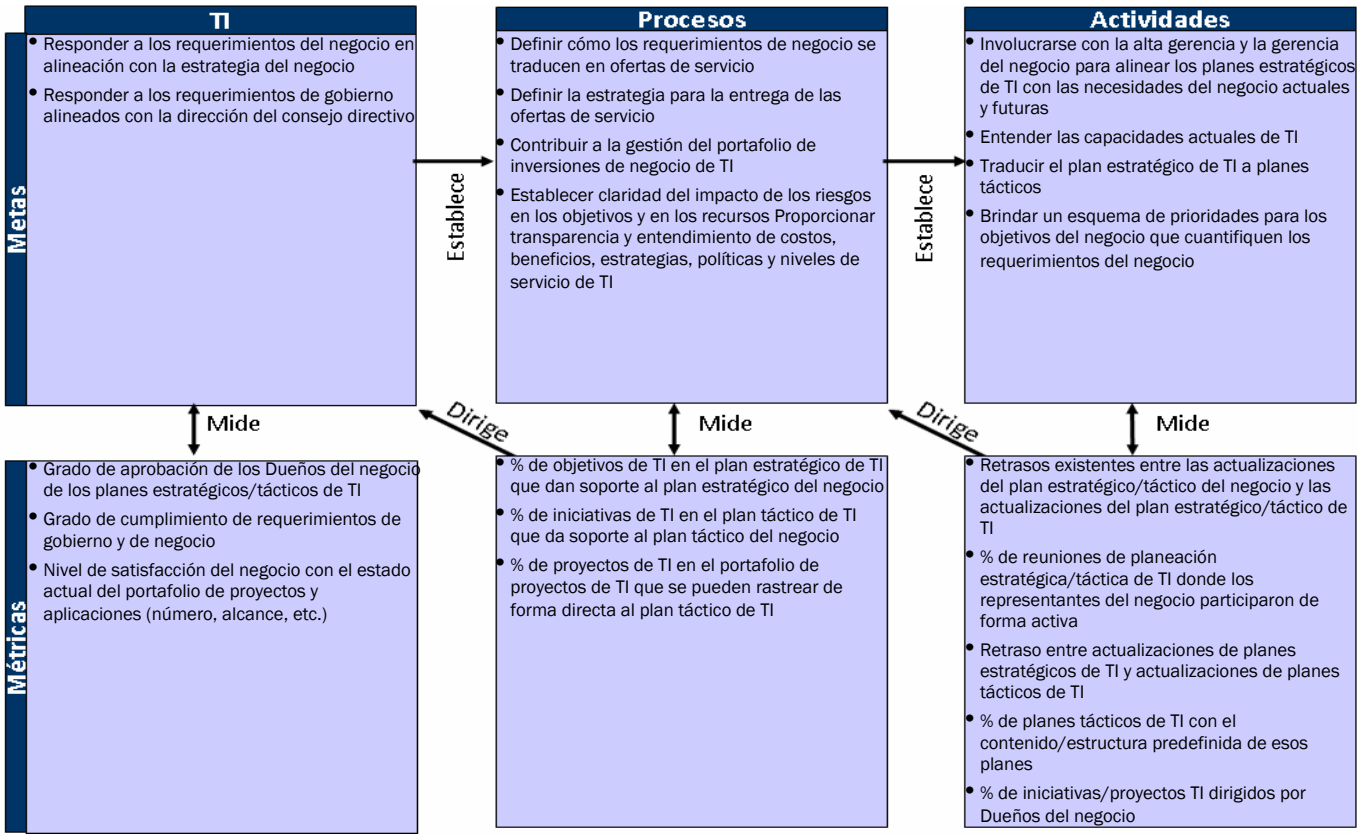
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Relacionar las metas del negocio con las de TI	C	I	A/R	R	C						
Identificar dependencias críticas y desempeño actual	C	C	R	A/R	C	C	C	C	C		C
Construir un plan estratégico para TI	A	C	C	R	I	C	C	C	C	I	C
Construir planes tácticos para TI	C	I		A	C	C	C	C	C	R	I
Analizar portafolios de programas y administrar portafolios de servicios y proyectos	C	I	I	A	R	R	C	R	C	C	I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P01 Definir un Plan Estratégico de TI.

Administración del proceso de *Definir un plan estratégico de TI* que satisfaga el requerimiento 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 requerimiento 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 Intuitivo 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 Definido cuando
Una política define cómo y cuando 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.

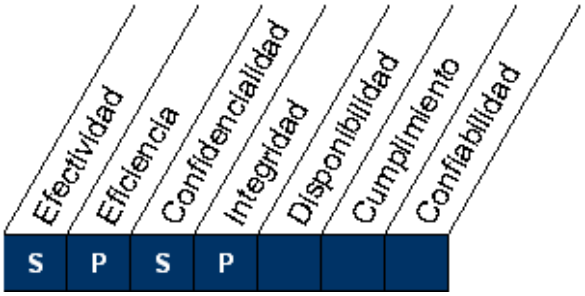
4 Administrado y Medible cuando
La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La planeación estratégica de TI es una función administrativa definida con responsabilidades de alto nivel. La dirección puede monitorear el proceso estratégico 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 apalancar 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.

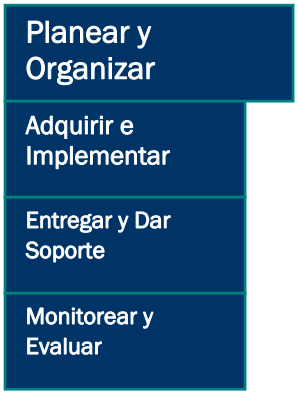
5 Optimizado cuando
La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Las consideraciones de riesgo y de valor agregado 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 especifica cómo los nuevos avances tecnológicos pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.

DESCRIPCIÓN DEL PROCESO.

P02. Definir la Arquitectura de la Información.

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.





Control sobre el proceso TI de

Definir la arquitectura de la información

Que satisface el requerimiento del negocio de TI para

Agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio

Enfocándose en

El establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos

Se logra con

- El aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos
- La asignación de propiedad de datos
- La clasificación de la información usando un esquema de clasificación acordado

Y se mide con

- El porcentaje de elementos de datos redundantes / duplicados
- El porcentaje de aplicaciones que no cumplen con la metodología de arquitectura de la información usada por la empresa
- La frecuencia de actividades de validación de datos

OBJETIVOS DE CONTROL

PO2. Definir la Arquitectura de la Información.

PO2.1 Modelo de Arquitectura de Información Empresarial
Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en PO1. El modelo debe facilitar la creación, uso y el compartir en forma óptima la información por parte del negocio de tal manera que se mantenga su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos.

PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización. El diccionario facilita compartir elementos de datos entre las aplicaciones y los sistemas, fomenta un entendimiento común de datos entre los usuarios de TI y del negocio, y previene la creación de elementos de datos incompatibles

PO2.3 Esquema de Clasificación de Datos
Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.

PO2.4 Administración de Integridad
Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

DIRECTRICES GERENCIALES

P02. Definir la Arquitectura de la Información.

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI
AI1	Estudio de Viabilidad de Requerimientos de Negocio
AI7	Revisión post implementación
DS3	Información de desempeño y capacidad
ME1	Entrada de Desempeño a planes de TI

Salidas	Hacia						
Esquema de clasificación de datos	AI2						
Plan de sistemas de negocio optimizado	PO3	AI2					
Diccionario de datos	AI2	DS11					
Arquitectura de la información	PO3	DS5					
Clasificación de datos asignada	DS1	DS4	DS5	DS11	DS12		
Procedimientos y herramientas de clasificación	*						

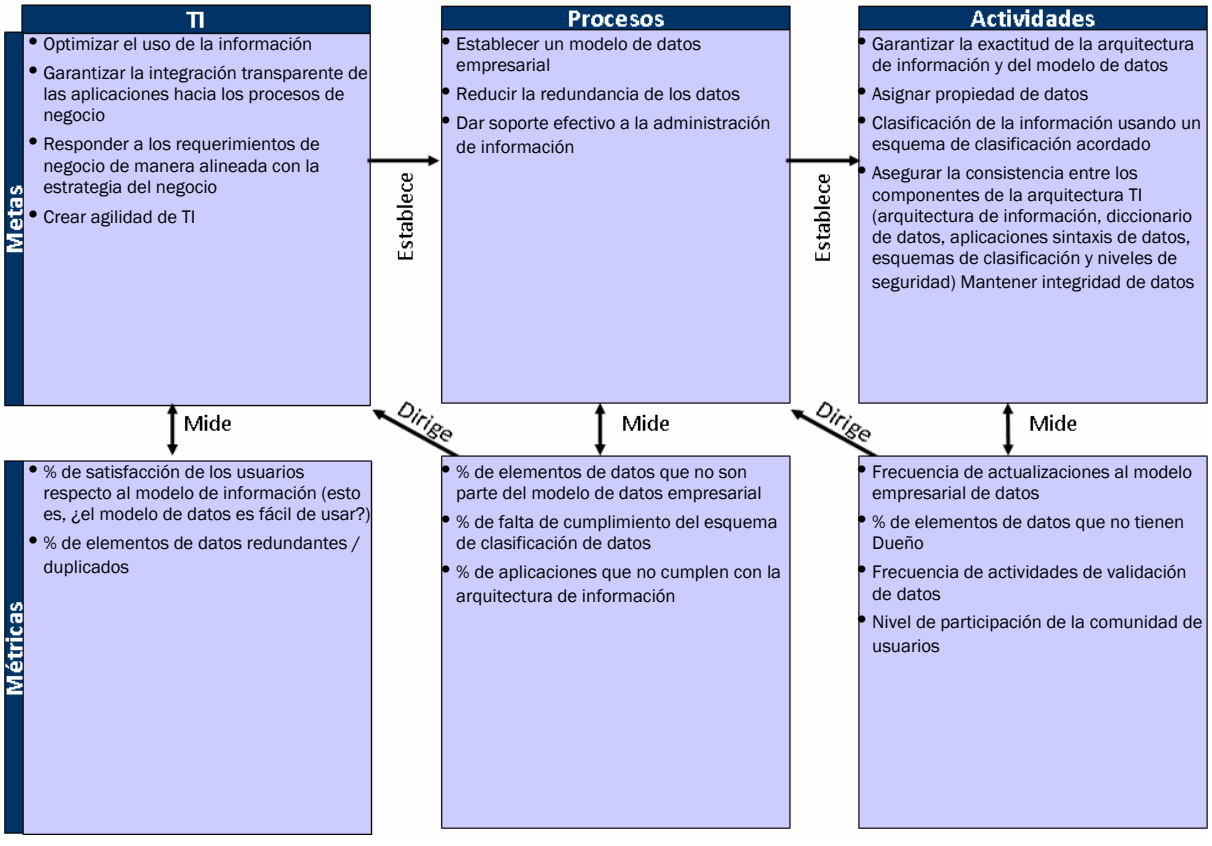
* Salidas externas a COBIT

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Crear y mantener modelo de información corporativo / empresarial		C	I	A	C		R	C	C		C
Crear y mantener diccionario de datos corporativo				I	C		A/R	R			C
Establecer y mantener esquema de clasificación de datos	I	C	A	C	C	I	C	C			R
Brindar a los dueños procedimientos y herramientas para clasificar los sistemas de información	I	C	A	C	C	I	C	C			R
Usar el modelo de información, el diccionario de datos y el esquema de clasificación para planear los sistemas optimizados de negocio	C	C	I	A	C		R	C			I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P02. Definir la Arquitectura de la Información.

La administración del proceso de *Definir la arquitectura de la información* que satisface el requerimiento de negocio de TI de *agilizar la respuesta a los requerimientos, para brindar información confiable y consistente y para integrar de forma transparente las aplicaciones hacia los procesos de negocio* es:

0 No Existente cuando
No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.

1 Inicial / Ad Hoc cuando
La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.

2 Repetible pero Intuitivo cuando
Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas. Los requerimientos tácticos impulsan el desarrollo de los componentes de la arquitectura de la información por parte de los individuos.

3 Definido cuando
La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información. Las herramientas automatizadas se empiezan a utilizar, aunque los procesos y reglas son definidos por los proveedores de software de bases de datos. Un plan formal de entrenamiento ha sido desarrollado, pero el entrenamiento formal se basa en iniciativas individuales.

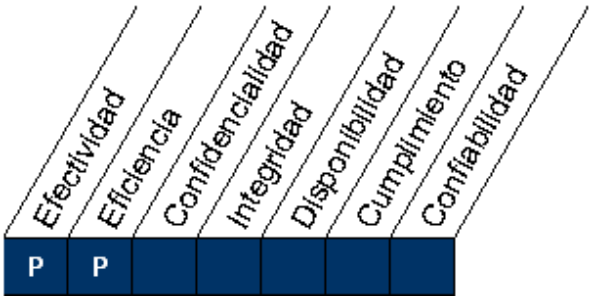
4 Administrado y Medible cuando
Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. La responsabilidad sobre el desempeño del proceso de desarrollo de la arquitectura se refuerza y se mide el éxito de la arquitectura de información. Las herramientas automatizadas de soporte están ampliamente generalizadas, pero todavía no están integradas. Se han identificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es proactivo y se enfoca en resolver necesidades futuras del negocio. La organización de administración de datos está activamente involucrada en todos los esfuerzos de desarrollo de las aplicaciones, para garantizar la consistencia. Un repositorio automatizado está totalmente implementado. Se encuentran en implantación modelos de datos más complejos para aprovechar el contenido informativo de las bases de datos. Los sistemas de información ejecutiva y los sistemas de soporte a la toma de decisiones aprovechan la información existente.

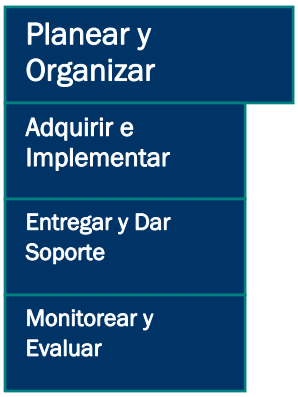
5 Optimizado cuando
La arquitectura de información es reforzada de forma consistente a todos los niveles. El valor de la arquitectura de la información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio. La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua. La estrategia para el aprovechamiento de la información por medio de tecnologías de bodega de datos y minería de datos está bien definida. La arquitectura de la información se encuentra en mejora continua y toma en cuenta información no tradicional sobre los procesos, organizaciones y sistemas.

DESCRIPCIÓN DEL PROCESO.

P03. Determinar la Dirección Tecnológica.

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones.





Control sobre el proceso TI de

Determinar la dirección tecnológica

Que satisface el requerimiento del negocio de TI para

Contar con sistemas aplicativos estándares, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio, actuales y futuros

Enfocándose en

La definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas

Se logra con

- El establecimiento de un foro para dirigir la arquitectura y verificar el cumplimiento
- El establecimiento de un plan de infraestructura tecnológica equilibrado versus costos, riesgos y requerimientos.
- La definición de estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información

Y se mide con

- El número y tipo de desviaciones con respecto al plan de infraestructura tecnológica
- Frecuencia de las revisiones /actualizaciones del plan de infraestructura tecnológica
- Número de plataformas de tecnología por función a través de toda la empresa

OBJETIVOS DE CONTROL

P03. Determinar la Dirección Tecnológica.

P03.1 Planeación de la Dirección Tecnológica
Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

P03.2 Plan de Infraestructura Tecnológica
Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala para inversiones y personal en sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

P03.3 Monitoreo de Tendencias y Regulaciones Futuras
Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

P03.4 Estándares Tecnológicos
Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos.

P03.5 Consejo de Arquitectura de TI
Establecer un comité de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación, y que verifique el cumplimiento. Esta entidad orienta el diseño de la arquitectura de TI garantizando que facilite la estrategia del negocio y tome en cuenta el cumplimiento regulatorio y los requerimientos de continuidad. Estos aspectos se vinculan con el PO2 *Definir arquitectura de la información*.

DIRECTRICES GERENCIALES

P03. Determinar la Dirección Tecnológica.

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI
PO2	Plan optimizado de sistemas del negocio y arquitectura de información
AI3	Actualizaciones de los estándares tecnológicos
DS3	Información de desempeño y capacidad

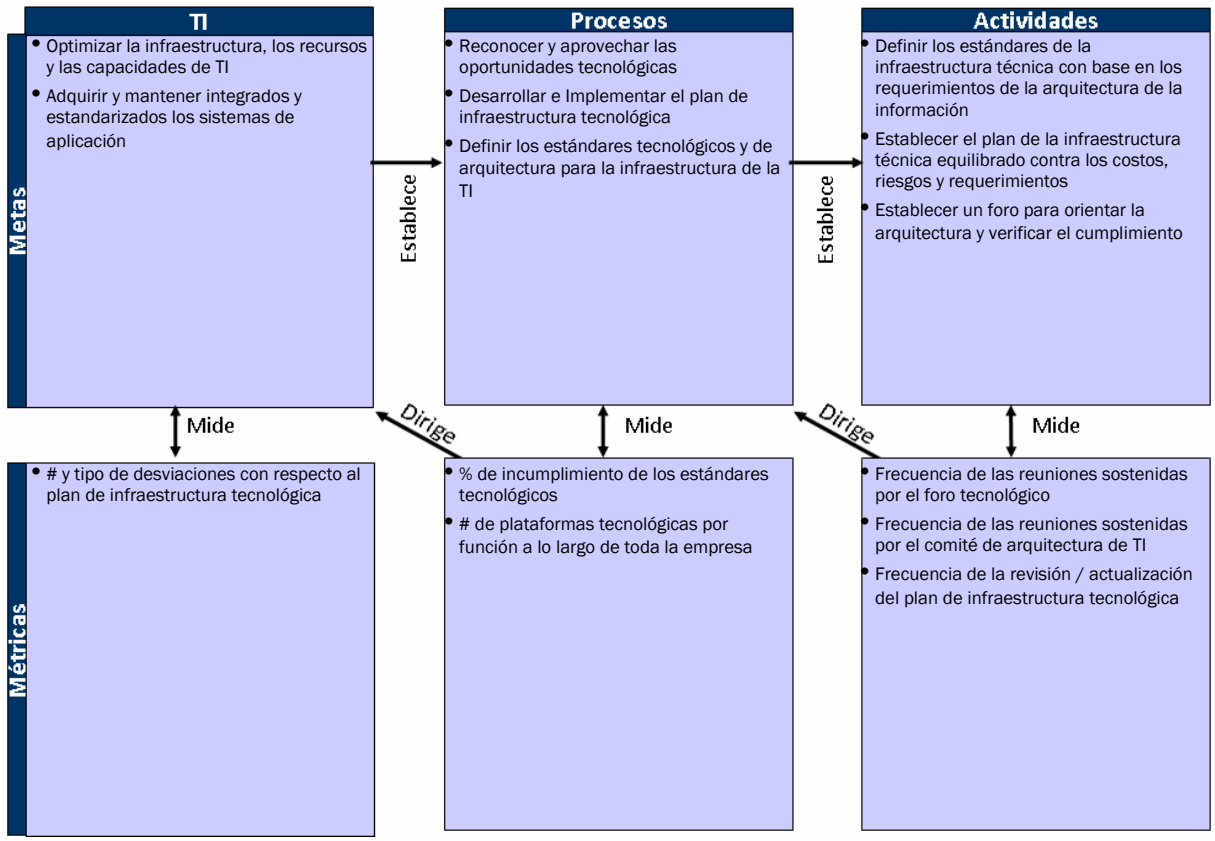
Salidas	Hacia						
Oportunidades tecnológicas	AI3						
Estándares tecnológicos	AI1	AI3	AI7	DS5			
Actualizaciones rutinarias del "estado de la tecnología"	AI1	AI2	AI3				
Plan de infraestructura tecnológica	AI3						
Requerimientos de infraestructura	PO5						

Matriz RACI

Actividades / Funciones	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Crear y mantener un plan de infraestructura tecnológica		I	I	A		C	R	C	C		C
Crear y mantener estándares tecnológicos				A		C	R	C	I	I	I
Publicar estándares tecnológicos		I	I	A		I	R	I	I	I	I
Monitorear la evolución tecnológica		I	I	A		C	R	C		C	C
Definir el uso (futuro) (estratégico) de la nueva tecnología		C	C	A		C	R	C		C	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P03. Determinar la Dirección Tecnológica.

Administración del proceso de *Determinar la dirección tecnológica* que satisfaga el requerimiento de negocio de TI de *contar con sistemas aplicativos estables, rentables e integrados, así como con recursos y capacidades que satisfagan los requerimientos de negocio, actuales y futuros* es:

0 No Existente cuando
No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento de que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.

1 Inicial / Ad Hoc cuando
La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implementación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.

2 Repetible pero Intuitivo cuando
Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de los cambios tecnológicos se delega a individuos que siguen procesos intuitivos, aunque similares. Las personas obtienen sus habilidades sobre planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. Están surgiendo técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.

3 Definido cuando
La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional. Los proveedores clave se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos, de forma consistente con la dirección de la organización.

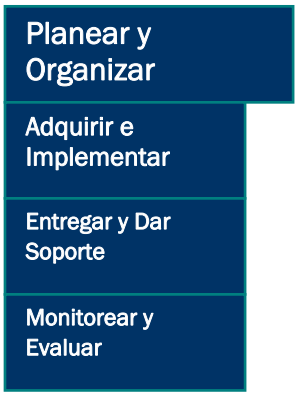
4 Administrado y Medible cuando
La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidades necesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentes se toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica ha sido asignada. El proceso para desarrollar el plan de infraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. La estrategia de recursos humanos está alineada con la dirección tecnológica, para garantizar que el equipo de TI pueda administrar los cambios tecnológicos. Los planes de migración para la introducción de nuevas tecnologías están definidos. Los recursos externos y las asociaciones se aprovechan para tener acceso a la experiencia y a las habilidades necesarias. La dirección ha evaluado la aceptación del riesgo de usar la tecnología como líder, o rezagarse en su uso, para desarrollar nuevas oportunidades de negocio o eficiencias operativas.

5 Optimizado cuando
Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avances industriales e internacionales, en lugar de estar orientada por los proveedores de tecnología. El impacto potencial de los cambios tecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe una aprobación ejecutiva formal para el cambio de la dirección tecnológica o para adoptar una nueva. La entidad cuenta con un plan robusto de infraestructura tecnológica que refleja los requerimientos del negocio, es sensible a los cambios en el ambiente del negocio y puede reflejar los cambios en éste. Existe un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica. Las mejores prácticas de la industria se usan de forma amplia para determinar la dirección técnica.

DESCRIPCIÓN DEL PROCESO.

P04. Definir los Procesos, Organización y Relaciones de TI.

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, y uno ó más comités de dirección, en los cuales participen tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión.



Control sobre el proceso TI de

Definir los procesos, organización y relaciones de TI

Que satisface el requerimiento del negocio de TI para

Agilizar la respuesta a las estrategias del negocio mientras se cumplen los requerimientos de gobierno y se establecen puntos de contacto definidos y competentes

Enfocándose en

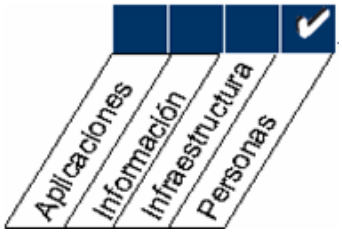
El establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implementación de procesos de TI con dueños, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión

Se logra con

- La definición de un marco de trabajo de procesos de TI
- El establecimiento de un cuerpo y una estructura organizacional apropiada
- La definición de roles y responsabilidades

Y se mide con

- El porcentaje de roles con descripciones de puestos y autoridad documentados
- El número de unidades/procesos de negocio que no reciben soporte de TI y que deberían recibirlo, de acuerdo con la estrategia
- Número de actividades clave de TI fuera de la organización de TI que no son aprobadas y que no están sujetas a los estándares organizacionales de TI



OBJETIVOS DE CONTROL

P04. Definir los Procesos, Organización y Relaciones de TI.

P04.1 Marco de Trabajo de Procesos de TI
Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de la empresa, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno.

P04.2 Comité Estratégico de TI
Establecer un comité estratégico de TI a nivel del consejo. Este comité deberá asegurar que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las inversiones principales a nombre del consejo completo.

P04.3 Comité Directivo de TI
Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para:
- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa
- Dar seguimiento al estatus de los proyectos y resolver los conflictos de recursos
- Monitorear los niveles de servicio y las mejoras del servicio.

P04.4 Ubicación Organizacional de la Función de TI
Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

P04.5 Estructura Organizacional
Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

P04.6 Establecimiento de Roles y Responsabilidades
Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definían las responsabilidades y rendición de cuentas para alcanzar las necesidades del negocio.

P04.7 Responsabilidad de Aseguramiento de Calidad de TI
Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA) y proporcionar al grupo de QA sistemas de QA, los controles y la experiencia para comunicarlos. Asegurar que la ubicación organizacional, las responsabilidades y el tamaño del grupo de QA satisfacen los requerimientos de la organización.

P04.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel superior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización para manejar los problemas a nivel de toda la empresa. Puede ser necesario asignar responsabilidades adicionales de administración de la seguridad a nivel de sistema específico para manejar problemas relacionados con seguridad. Obtener orientación de la alta dirección con respecto al apetito de riesgo de TI y la aprobación de cualquier riesgo residual de TI.

P04.9 Propiedad de Datos y de Sistemas
Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los dueños toman decisiones sobre la clasificación de la información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.

P04.10 Supervisión
Implementar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.

P04.11 Segregación de Funciones
Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también se asegura de que el personal realice sólo las tareas autorizadas, relevantes a sus puestos y posiciones respectivas.

P04.12 Personal de TI
Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de recursos para soportar adecuada y apropiadamente a las metas y objetivos del negocio.

PO4.13 Personal Clave de TI
Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo crítica.

PO4.14 Políticas y Procedimientos para Personal Contratado
Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan con las políticas organizacionales de protección de los activos de información de la empresa de tal manera que se logren los requerimientos contractuales acordados.

PO4.15 Relaciones
Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI, tales como el consejo directivo, ejecutivos, unidades de negocio, usuarios individuales, proveedores, oficiales de seguridad, gerentes de riesgo, el grupo de cumplimiento corporativo, los contratistas externos y la gerencia externa (offsite).

Página dejada en blanco intencionadamente.

DIRECTRICES GERENCIALES

P04. Definir los Procesos, Organización y Relaciones de TI.

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI
PO7	Políticas y procedimientos de TI y RH, matriz de habilidades de TI, descripciones de puestos
PO8	Actividades de mejoramiento de calidad
PO9	Planes de actividades para corregir riesgos relacionados con TI
ME1	Planes de acciones correctivas
ME2	Reportes de efectividad de los controles de TI
ME3	Catálogo de requerimientos legales y regulatorios relacionados con los servicios de TI
ME4	Mejoras al marco de procesos

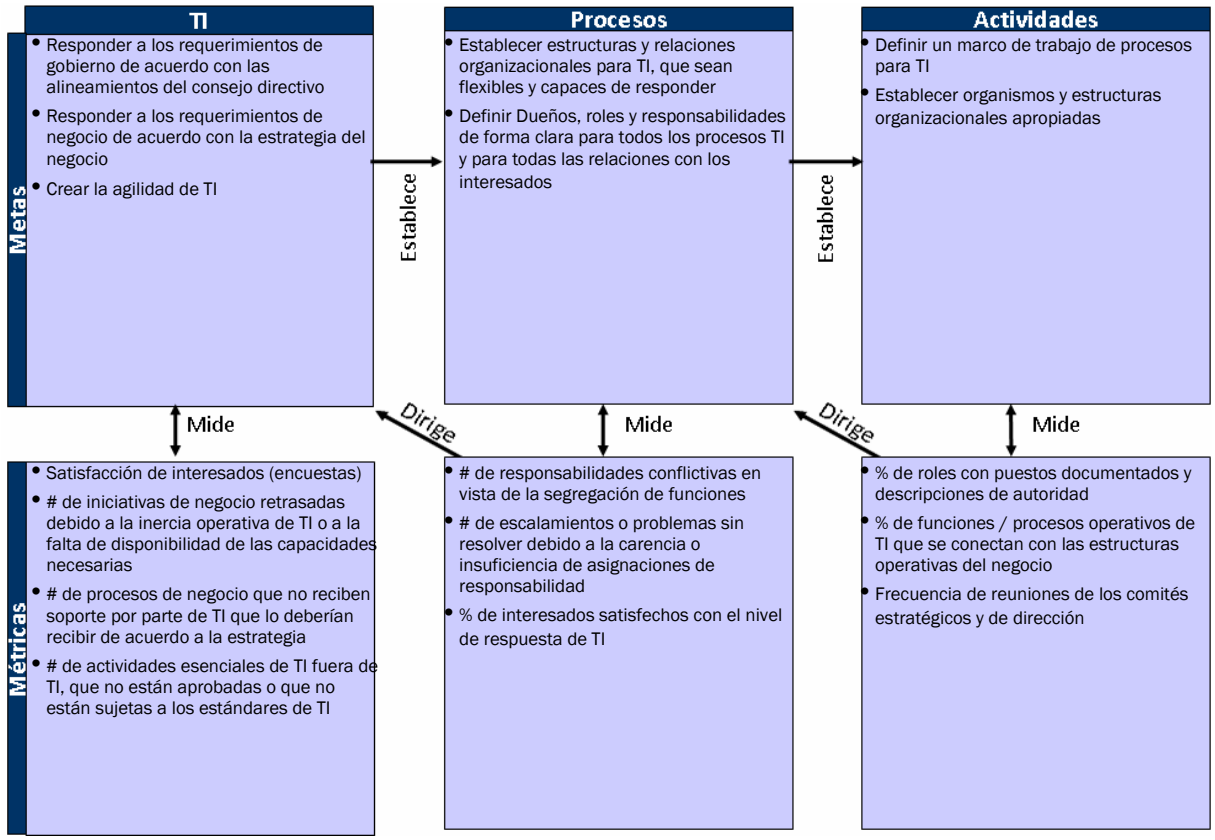
Salidas	Hacia						
Marco de trabajo para el proceso de TI	ME4						
Dueños de sistemas documentados	AI7	DS6					
Organización y relaciones de TI	PO7						
Marco de procesos, roles documentados y responsabilidades de TI	Todos						
Roles y responsabilidades documentados	PO7						

Matriz RACI

Actividades / Funciones	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Establecer estructura organizacional de TI, incluyendo comités y ligas a los interesados y proveedores	C	C	C	A		C	C	C	R	C	I
Diseñar marco de trabajo para el proceso de TI	C	C	C	A		C	C	C	R	C	C
Identificar dueños de sistemas		C	C	A	C	R	I	I	I	I	I
Identificar dueños de datos		I	A	C	C	I	R	I	I	I	C
Establecer e implantar roles y responsabilidades de TI, incluida la supervision y segregación de funciones		I	I	A	I	C	C	C	R	C	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P04. Definir los Procesos, Organización y Relaciones de TI.

La administración del proceso de *Definir los procesos, organización y relaciones de TI* que satisfaga el requerimiento de negocio de TI de *agilizar la respuesta a la estrategia del negocio mientras se cumplen los requerimientos de gobierno y se establecen puntos de contacto definidos y competentes* es:

0 No Existente cuando
La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.

1 Inicial / Ad Hoc cuando
Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. TI se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizados ni reforzados.

2 Repetible pero Intuitivo cuando
La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores.

3 Definido cuando
Existen roles y responsabilidades definidos para la organización de TI y para terceros. La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno. Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores. La organización de TI está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. Existe una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades está definida e implantada.

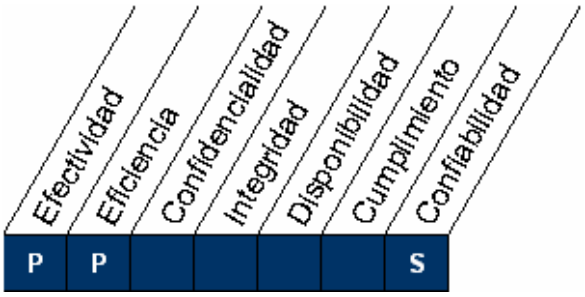
4 Administrado y Medible cuando
La organización de TI responde de forma proactiva al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas. Se han aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implementar y monitorear la organización deseada y las relaciones. Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional. El equilibrio entre las habilidades y los recursos disponibles internamente, y los que se requieren de organizaciones externas están definidos y reforzados. La estructura organizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesos estratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.

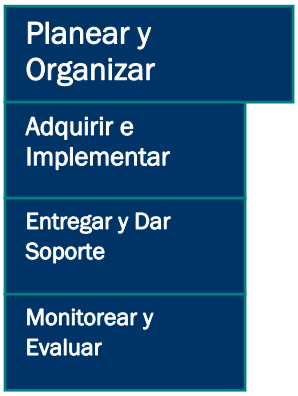
5 Optimizado cuando
La estructura organizacional de TI es flexible y adaptable. Se ponen en funcionamiento las mejores prácticas de la industria. Existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI. La tecnología se aprovecha para apoyar la complejidad y distribución geográfica de la organización. Un proceso de mejora continua existe y está implantado.

DESCRIPCIÓN DEL PROCESO.

P05. Administrar la Inversión en TI.

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias. El proceso fomenta la asociación entre TI y los interesados del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI.





Control sobre el proceso TI de

Administrar la Inversión en TI

Que satisface el requerimiento del negocio de TI para

Mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan las expectativas del usuario.

Enfocándose en

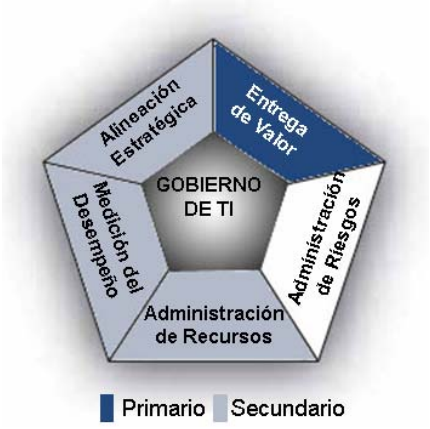
Decisiones de portafolio e inversión en TI efectivas y eficientes, y el establecimiento y seguimiento de presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión.

Se logra con

- El pronóstico y la asignación de presupuestos
- La definición de criterios formales de inversión (retorno de inversión -ROI, periodo de reintegro, valor presente neto -NPV)
- La medición y evaluación del valor del negocio en comparación con el pronóstico

Y se mide con

- El porcentaje de reducción en el costo unitario del servicio de TI
- Porcentaje del valor de la desviación respecto al presupuesto en comparación con el presupuesto total
- Porcentaje de gasto de TI expresado en impulsores de valor del negocio (Ej. Incremento en ventas / servicios debidos a la mejora en conectividad



OBJETIVOS DE CONTROL

P05. Administrar la Inversión en TI.

P05.1 Marco de Trabajo para la Administración Financiera
Establecer y mantener un marco de trabajo financiero para administrar las inversiones y el costo de los activos y servicios de TI a través del portafolios de inversiones habilitadas por TI, casos de negocio y presupuestos de TI.

P05.2 Prioridades Dentro del Presupuesto de TI
Implementar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI

P05.3 Proceso Presupuestal
Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual. El proceso debe dar soporte al desarrollo de un presupuesto general de TI así como al desarrollo de presupuestos para programas individuales, con énfasis especial en los componentes de TI de esos programas. El proceso debe permitir la revisión, el refinamiento y la aprobación constantes del presupuesto general y de los presupuestos de programas individuales

P05.4 Administración de Costos de TI
Implementar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar. Cuando existan desviaciones, éstas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar.

P05.5 Administración de Beneficios
Implementar un proceso de monitoreo de beneficios. La contribución esperada de TI a los resultados del negocio, ya sea como un componente de programas de inversión en TI o como parte de un soporte operativo regular, se debe identificar, acordar, monitorear y reportar. Los reportes se deben revisar y, donde existan oportunidades para mejorar la contribución de TI, se deben definir y tomar las medidas apropiadas. Siempre que los cambios en la contribución de TI tengan impacto en el programa, o cuando los cambios a otros proyectos relacionados impacten al programa, el caso de negocio deberá ser actualizado.

DIRECTRICES GERENCIALES

P05. Administrar la Inversión en TI.

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI, portafolios de proyectos y servicios
PO3	Requerimientos de infraestructura
PO10	Portafolio de proyectos de TI actualizado
AI1	Información sobre el desempeño y la capacidad
AI7	Revisiones post-implantación
DS3	Plan de desempeño y de capacidad (requerimientos)
DS6	Finanzas de TI
ME4	Resultados esperados de las inversiones en el negocio habilitadas por TI

Salidas	Hacia						
Reportes de costo / beneficio	PO1	AI2	DS6	ME1	ME4		
Presupuestos de TI	DS6						
Portafolio actualizado de servicios de TI	DS1						
Portafolio actualizado de proyectos de TI	PO10						

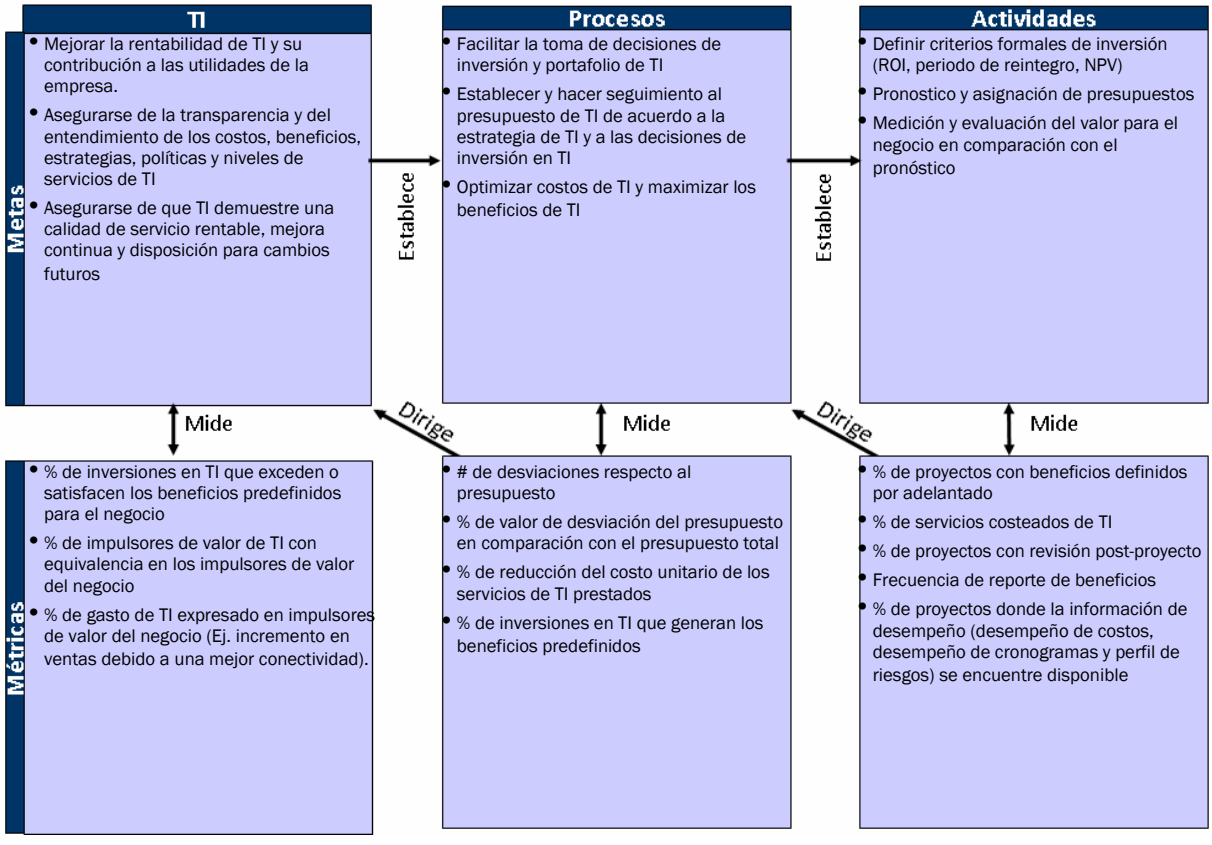
Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Dar mantenimiento al portafolio de programas de inversión	A	R	R	R	C					I	I
Dar mantenimiento al portafolio de proyectos	I	C	A/R	A/R	C		C	C		C	I
Dar mantenimiento al portafolio de servicios	I	C	A/R	A/R	C	C				C	I
Establecer y mantener proceso presupuestal de TI	I	C	C	A		C	C	C	R	C	
Identificar, comunicar y monitorear la inversión, costo y valor de TI para el negocio	I	C	C	A/R		C	C	C	R	C	C

Funciones

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P05. Administrar la Inversión en TI.

La administración del proceso de *Administrar la inversión en TI* que satisfaga el requerimiento de negocio de TI de *mejorar de forma constante y demostrable la rentabilidad de TI y su contribución a la utilidad del negocio con servicios integrados y estándar que satisfagan las expectativas del usuario final* es:

0 No Existente cuando
No existe conciencia de la importancia de la selección y presupuesto de las inversiones en TI. No existe seguimiento o monitoreo de las inversiones y gastos de TI.

1 Inicial / Ad Hoc cuando
La organización reconoce la necesidad de administrar la inversión en TI, aunque esta necesidad se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal. Las inversiones en TI se justifican de una forma ad hoc. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.

2 Repetible pero Intuitivo cuando
Existe un entendimiento implícito de la necesidad de seleccionar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. El cumplimiento depende de la iniciativa de individuos dentro de la organización. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.

3 Definido cuando
Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología. El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio. Los procesos de selección de inversiones en TI y de presupuestos están formalizados, documentados y comunicados. Surge el entrenamiento formal aunque todavía se basa de modo principal en iniciativas individuales. Ocurre la aprobación formal de la selección de inversiones en TI y presupuestos. El personal de TI cuenta con la experiencia y habilidades necesarias para desarrollar el presupuesto de TI y recomendar inversiones apropiadas en TI.

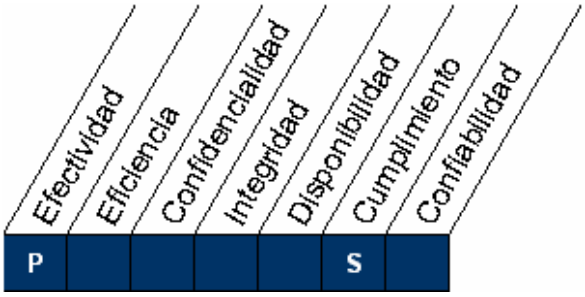
4 Administrado y Medible cuando
La responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan a un individuo específico. Las diferencias en el presupuesto se identifican y se resuelven. Se realizan análisis formales de costos que cubren los costos directos e indirectos de las operaciones existentes, así como propuestas de inversiones, considerando todos los costos a lo largo del ciclo completo de vida. Se usa un proceso de presupuestos proactivo y estándar. El impacto en los costos operativos y de desarrollo debidos a cambios en hardware y software, hasta cambios en integración de sistemas y recursos humanos de TI, se reconoce en los planes de inversión. Los beneficios y los retornos se calculan en términos financieros y no financieros.

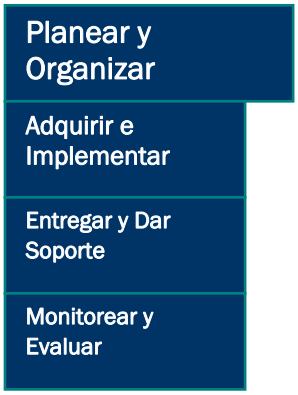
5 Optimizado cuando
Se utilizan las buenas prácticas de la industria para evaluar los costos por comparación (benchmark) e identificar la efectividad de las inversiones. Se utiliza el análisis de los avances tecnológicos en el proceso de selección y presupuesto de inversiones. El proceso de administración de inversiones se mejora de forma continua con base en las lecciones aprendidas provenientes del análisis del desempeño real de las inversiones. Las decisiones de inversiones incluyen las tendencias de mejora de precio/desempeño. Se investigan y evalúan formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital existente en la organización, mediante el uso de métodos formales de evaluación. Existe la identificación proactiva de varianzas. Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión.

DESCRIPCIÓN DEL PROCESO.

P06. Comunicar las Aspiraciones y la Dirección de la Gerencia.

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes.





Control sobre el proceso TI de

Comunicar las aspiraciones y la dirección de la gerencia

Que satisface el requerimiento del negocio de TI para

Una información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades

Enfocándose en

Proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de TI a los interesados

Se logra con

- La definición de un marco de trabajo de control para TI
- La elaboración e implantación de políticas para TI
- El refuerzo de políticas de TI

Y se mide con

- El número de interrupciones en el negocio debidas a interrupciones en el servicio de TI
- Porcentaje de interesados que entienden el marco de trabajo de control de TI de la empresa
- Porcentaje de interesados que no cumple las políticas

OBJETIVOS DE CONTROL

PO6. Comunicar las Aspiraciones y la Dirección de la Gerencia.

PO6.1 Ambiente de Políticas y de Control
Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad. El ambiente de control se basa en una cultura que apoya la entrega de valor, mientras administra riesgos significativos, fomenta la colaboración entre divisiones y el trabajo en equipo, promueve el cumplimiento y la mejora continua de procesos, y maneja las desviaciones (incluyendo las fallas) de forma adecuada.

PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y el control que se alinee con la política de TI, el ambiente de control y el marco de trabajo de riesgo y control de la empresa.

PO6.3 Administración de Políticas para TI
Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir su intención, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Su relevancia se debe confirmar y aprobar en forma regular.

PO6.4 Implantación de Políticas de TI
Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.

PO6.5 Comunicación de los Objetivos y la Dirección de TI
Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a los interesados apropiados y a los usuarios de toda la organización.

DIRECTRICES GERENCIALES

P06. Comunicar las Aspiraciones y la Dirección de la Gerencia.

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI, portafolios de proyectos y servicios
PO9	Directrices de administración de riesgos relativos a TI
ME2	Reportes sobre la efectividad de los controles de TI

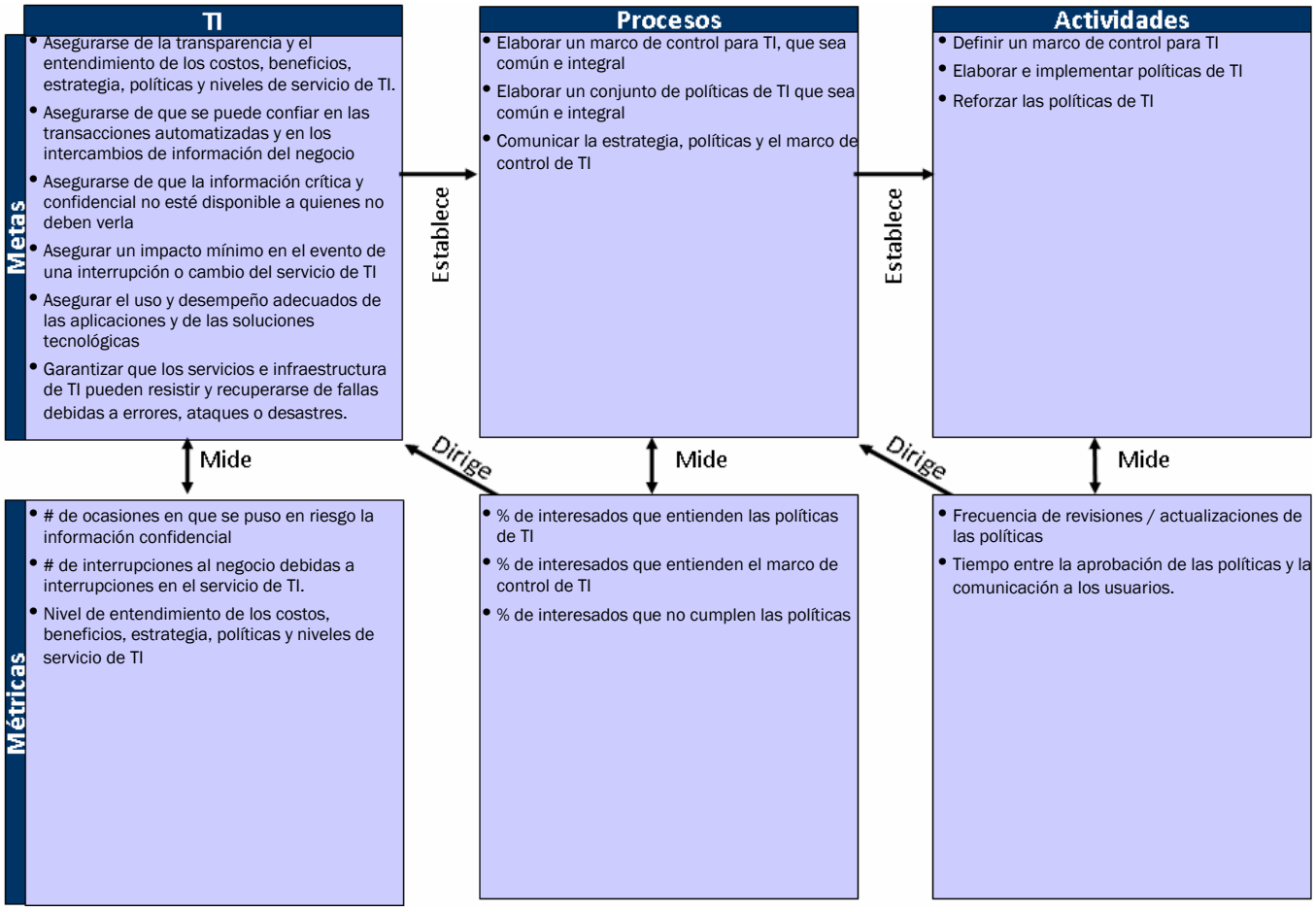
Salidas	Hacia
Marco de control empresarial para TI	TODAS
Políticas para TI	TODAS

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Elaborar y mantener un ambiente y marco de control de TI	I	C	I	A/R	I	C		C	C		C
Elaborar y mantener políticas de TI	I	I	I	A/R		C	C	C	R		C
Comunicar el marco de control y los objetivos y dirección de TI	I	I	I	A/R					R		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P06. Comunicar las Aspiraciones y la Dirección de la Gerencia.

La administración del proceso de *Comunicar las aspiraciones y la dirección de la gerencia* que satisfaga el requerimiento de negocio de TI de *información precisa y oportuna sobre los servicios actuales de TI, riesgos asociados y responsabilidades* es:

0 No Existente cuando
La gerencia no ha establecido un ambiente positivo de control de información. No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.

1 Inicial / Ad Hoc cuando
La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.

2 Repetible pero Intuitivo cuando
La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales. La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción de gerentes y áreas de negocio individuales. La calidad se reconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales. El entrenamiento se realiza de forma individual, según se requiera.

3 Definido cuando
La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.

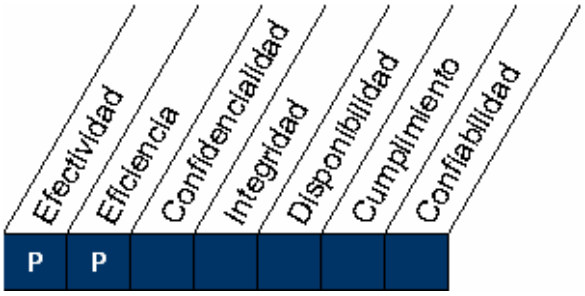
4 Administrado y Medible cuando
La gerencia asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad y asigna suficientes recursos para mantener el ambiente en línea con los cambios significativos. Se ha establecido un ambiente de control de información positivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen y comunican, y forman un componente de buenas prácticas internas. Se ha establecido un marco de trabajo para la implantación y las verificaciones subsiguientes de cumplimiento.

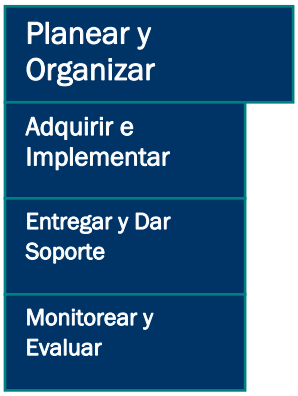
5 Optimizado cuando
El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora. Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación. El monitoreo, la auto-evaluación y las verificaciones de cumplimiento están extendidas en la organización. La tecnología se usa para mantener bases de conocimiento de políticas y de concienciación y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado en computadora.

DESCRIPCIÓN DEL PROCESO.

P07. Administrar los Recursos Humanos de TI.

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal.





Control sobre el proceso TI de

Administrar los recursos humanos de TI

Que satisface el requerimiento del negocio de TI para

Adquirir gente competente y motivada para crear y entregar servicios de TI

Enfocándose en

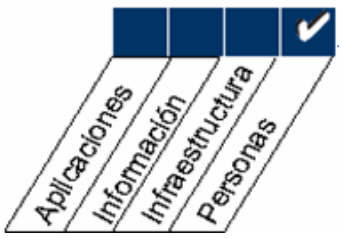
La contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de descripción de puestos y el aseguramiento de la conciencia de la dependencia sobre los individuos

Se logra con

- La revisión del desempeño del personal
- La contratación y entrenamiento de personal de TI para apoyar los planes tácticos de TI
- La mitigación del riesgo de sobre-dependencia de recursos clave

Y se mide con

- El nivel de satisfacción de los interesados respecto a la experiencia y habilidades del personal
- La rotación de personal de TI
- Porcentaje de personal de TI certificado de acuerdo a las necesidades del negocio



OBJETIVOS DE CONTROL

P07. Administrar los Recursos Humanos de TI.

P07.1 Reclutamiento y Retención del Personal
Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (Ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

P07.2 Competencias del Personal
Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

P07.3 Asignación de Roles
Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

P07.4 Entrenamiento del Personal de TI
Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

P07.5 Dependencia Sobre los Individuos
Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

P07.6 Procedimientos de Investigación del Personal
Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

P07.7 Evaluación del Desempeño del Empleado
Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

P07.8 Cambios y Terminación de Trabajo
Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

DIRECTRICES GERENCIALES

P07. Administrar los Recursos Humanos de TI.

Desde	Entradas
PO4	Organización y relaciones de TI; roles y responsabilidades documentados
AI1	Estudio de factibilidad de los requerimientos del negocio

Salidas	Hacia						
Políticas y procedimientos de recursos humanos de TI	PO4						
Matriz de habilidades de TI	PO4	PO10					
Descripciones de puestos	PO4						
Aptitudes y habilidades de los usuarios, incluyendo el entrenamiento individual	DS7						
Requerimientos específicos de entrenamiento	DS7						
Roles y responsabilidades	TODOS						

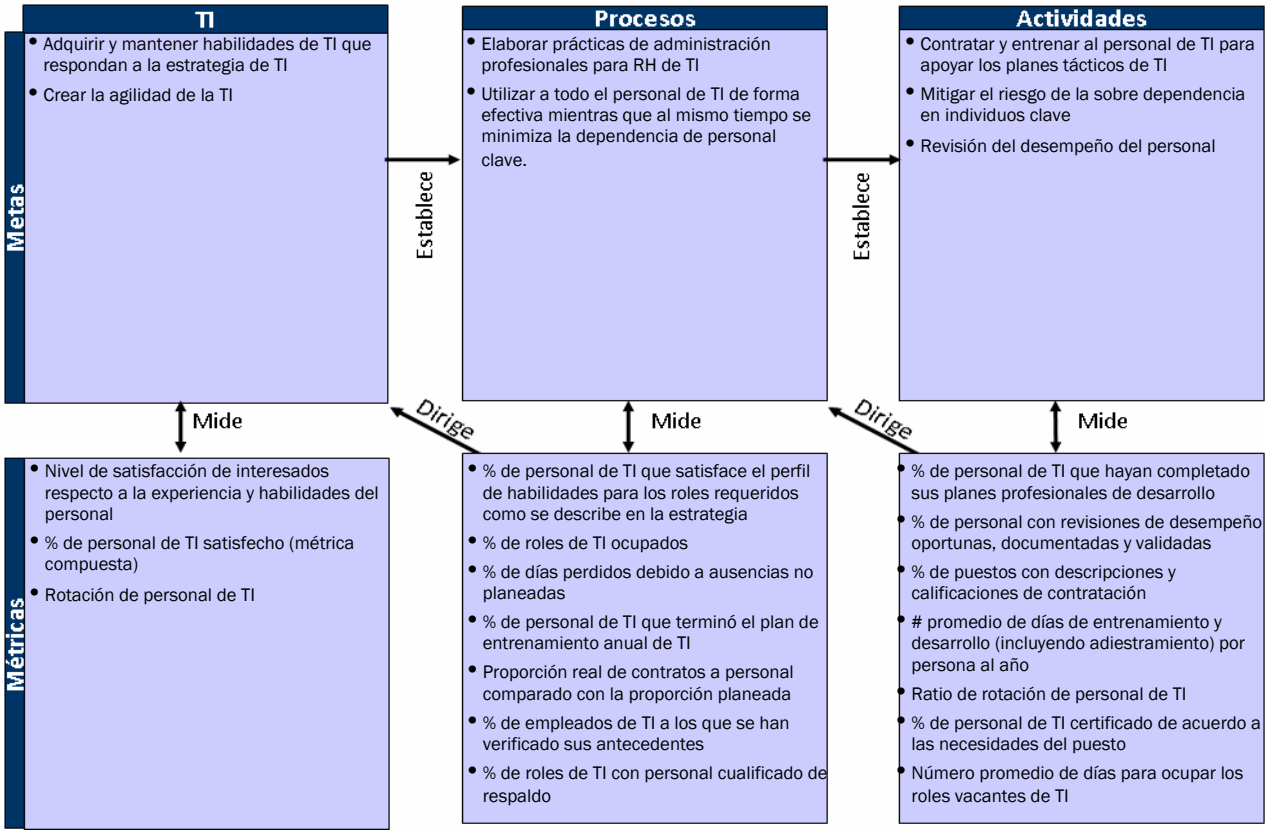
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Identificar las habilidades de TI, benchmarks sobre descripciones de puesto, rango de salarios y desempeño del personal		C		A		C	C	C	R	C	
Ejecutar las políticas y procedimientos relevantes de RH para TI (reclutar, contratar, investigar, compensar, entrenar, evaluar, promover y terminar)				A		R	R	R	R	R	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P07. Administrar los Recursos Humanos de TI.

La administración del proceso de *Administrar los recursos humanos* de TI que satisfaga el requerimiento de negocio de TI de *personal competente y motivado para crear y entregar servicios de TI* es:

0 No Existente cuando
No existe conciencia sobre la importancia de alinear la administración de recursos humanos de TI con el proceso de planeación de la tecnología para la organización. No hay persona o grupo formalmente responsable de la administración de los recursos humanos de TI.

1 Inicial / Ad Hoc cuando
La gerencia reconoce la necesidad de contar con administración de recursos humanos de TI. El proceso de administración de recursos humanos de TI es informal y reactivo. El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal de TI. Se está desarrollando la conciencia con respecto al impacto que tienen los cambios rápidos de negocio y de tecnología, y las soluciones cada vez más complejas, sobre la necesidad de nuevos niveles de habilidades y de competencia.

2 Repetible pero Intuitivo cuando
Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar de hacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.

3 Definido cuando
Existe un proceso definido y documentado para administrar los recursos humanos de TI. Existe un plan de administración de recursos humanos. Existe un enfoque estratégico para la contratación y la administración del personal de TI. El plan de entrenamiento formal está diseñado para satisfacer las necesidades de los recursos humanos de TI. Está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.

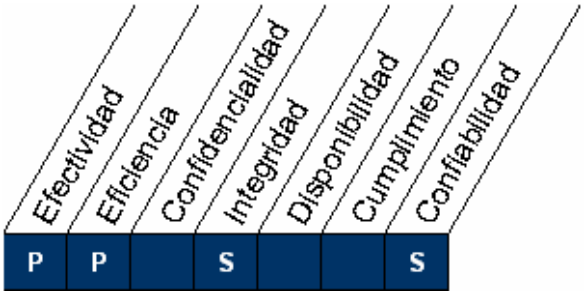
4 Administrado y Medible cuando
La responsabilidad de la elaboración y el mantenimiento de un plan de administración de recursos humanos para TI ha sido asignado a un individuo o grupo con las habilidades y experiencia necesarias para elaborar y mantener el plan. El proceso para elaborar y mantener el plan de administración de recursos humanos de TI responde al cambio. La organización cuenta con métricas estandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de TI con énfasis especial en el manejo del crecimiento y rotación del personal. Las revisiones de compensación y de desempeño se están estableciendo y se comparan con otras organizaciones de TI y con las mejores prácticas de la industria. La administración de recursos humanos es proactiva, tomando en cuenta el desarrollo de un plan de carrera.

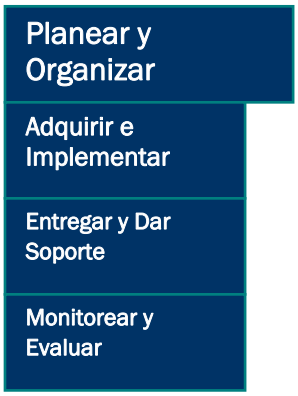
5 Optimizado cuando
El plan de administración de recursos humanos de TI se actualiza de forma constante para satisfacer los cambiantes requerimientos del negocio. La administración de recursos humanos de TI está integrada y responde a la dirección estratégica de la entidad. Los componentes de la administración de recursos humanos de TI son consistentes con las mejores prácticas de la industria, tales como compensación, revisiones de desempeño, participación en foros de la industria, transferencia de conocimiento, entrenamiento y adiestramiento. Los programas de entrenamiento se desarrollan para todos los nuevos estándares tecnológicos y productos antes de su implantación en la organización.

DESCRIPCIÓN DEL PROCESO.

P08. Administrar la Calidad.

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. Los requerimientos de calidad se deben manifestar y documentar con indicadores cuantificables y alcanzables. La mejora continua se logra por medio del constante monitoreo, corrección de desviaciones y la comunicación de los resultados a los interesados. La administración de calidad es esencial para garantizar que TI está dando valor al negocio, mejora continua y transparencia para los interesados.





Control sobre el proceso TI de

Administrar la calidad

Que satisface el requerimiento del negocio de TI para

La mejora continua y medible de la calidad de los servicios prestados por TI

Enfocándose en

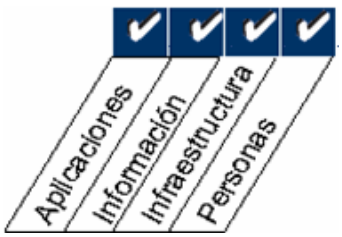
La definición de un sistema de administración de calidad (QMS, por sus siglas en inglés), el monitoreo continuo del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI

Se logra con

- La definición de estándares y prácticas de calidad
- El monitoreo y revisión interna y externa del desempeño contra los estándares y prácticas de calidad definidas
- La mejorara del QMS de manera continua

Y se mide con

- Porcentaje de Interesados (Stakeholders) satisfechos con la calidad (ponderado por importancia)
- Porcentaje de procesos de TI revisados de manera formal por aseguramiento de calidad de modo periódico que satisfaga las metas y objetivos de calidad
- Porcentaje de procesos que reciben revisiones de aseguramiento de calidad (QA)



OBJETIVOS DE CONTROL

P08. Administrar la Calidad.

P08.1 Sistema de Administración de Calidad
Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario.

P08.2 Estándares y Prácticas de Calidad
Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las buenas prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.

P08.3 Estándares de Desarrollo y de Adquisición
Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

P08.4 Enfoque en el Cliente de TI
Enfocar la administración de calidad en los clientes, determinando sus requerimientos y alineándolos con los estándares y prácticas de TI. Definir roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI.

P08.5 Mejora Continua
Mantener y comunicar regularmente un plan global de calidad que promueva la mejora continua.

P08.6 Medición, Monitoreo y Revisión de la Calidad
Definir, planear e implementar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que el QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

DIRECTRICES GERENCIALES

P08. Administrar la Calidad.

Desde	Entradas
PO1	Plan estratégico de TI
PO10	Planes detallados de proyectos
ME1	Planes de acciones correctivas

Salidas	Hacia						
Estándares de adquisición	AI1	AI2	AI3	AI5	DS2		
Estándares de desarrollo	PO10	AI1	AI2	AI3	AI7		
Requerimientos de estándares y métricas de calidad	TODAS						
Medidas para la mejora de la calidad	PO4	AI6					

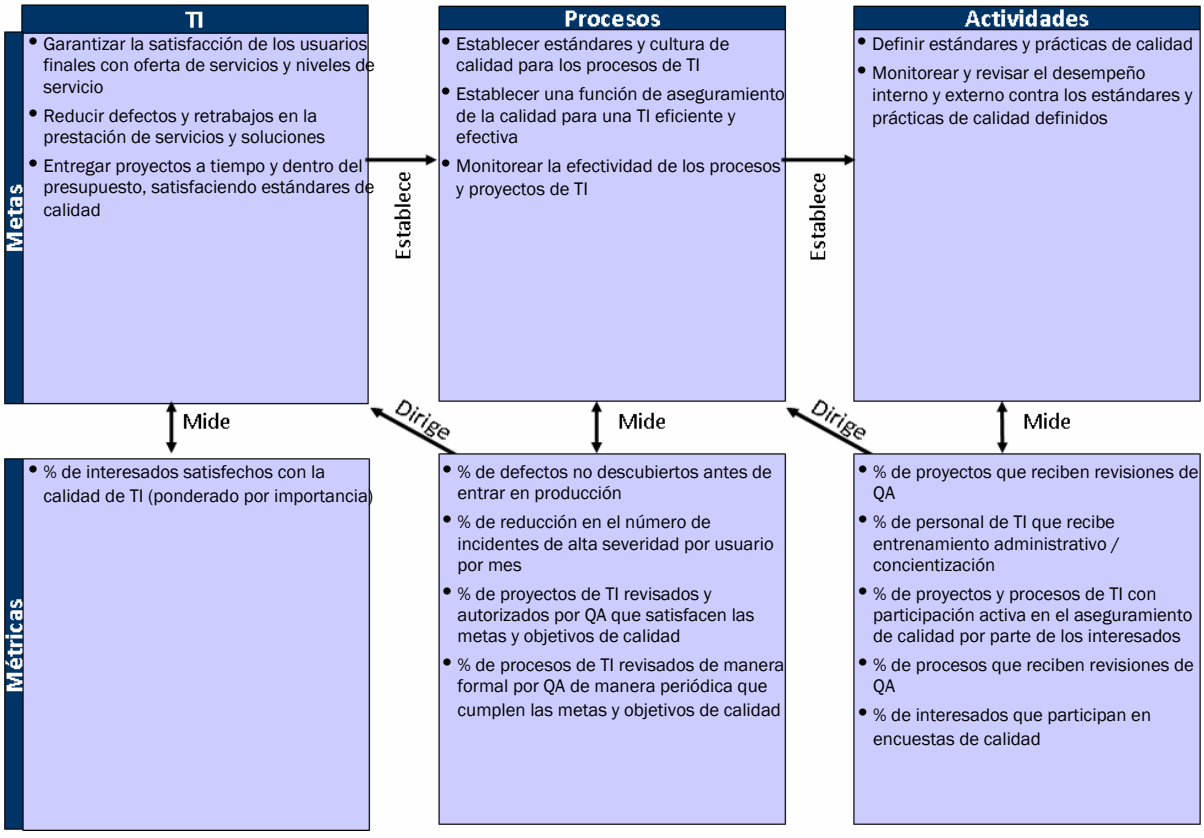
Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir un sistema de administración de calidad	C		C	A/R	I	I	I	I	I	I	C
Establecer y mantener un sistema de administración de calidad	I	I	I	A/R	I	C	C	C	C	C	C
Crear y comunicar estándares de calidad a toda la organización		I		A/R	I	C	C	C	C	C	C
Crear y administrar el plan de calidad para la mejora continua				A/R	I	C	C	C	C	C	C
Medir, monitorear y revisar el cumplimiento de las metas de calidad				A/R	I	C	C	C	C	C	C

Funciones

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P08. Administrar la Calidad.

La administración del proceso de *Administrar la calidad* que satisfaga el requerimiento de negocio de TI de *mejora continua y medible de la calidad de los servicios prestados por TI* es:

0 No Existente cuando
La organización carece de un sistema de un proceso de planeación de QMS y de una metodología de ciclo de vida de desarrollo de sistemas (SDLC, por sus siglas en inglés). La alta dirección y el equipo de TI no reconocen que un programa de calidad es necesario. Nunca se revisa la calidad de los proyectos y las operaciones.

1 Inicial / Ad Hoc cuando
Existe conciencia por parte de la dirección de la necesidad de un QMS. El QMS es impulsado por individuos cuando éste ocurre. La dirección realiza juicios informales sobre la calidad.

2 Repetible pero Intuitivo cuando
Se establece un programa para definir y monitorear las actividades de QMS dentro de TI. Las actividades de QMS que ocurren están enfocadas en iniciativas orientadas a procesos y proyectos, no a procesos de toda la organización.

3 Definido cuando
La dirección ha comunicado un proceso definido de QMS e involucra a TI y a la gerencia del usuario final. Un programa de educación y entrenamiento está surgiendo para instruir a todos los niveles de la organización sobre el tema de la calidad. Se han definido expectativas básicas de calidad y éstas se comparten dentro de los proyectos y la organización de TI. Están surgiendo herramientas y prácticas comunes para administrar la calidad. Las encuestas de satisfacción de la calidad se planean y ocasionalmente se aplican.

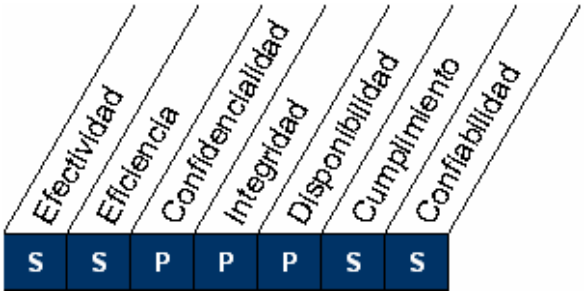
4 Administrado y Medible cuando
El QMS está incluido en todos los procesos, incluyendo aquellos que dependen de terceros. Se está estableciendo una base de conocimiento estandarizada para las métricas de calidad. Se usan métodos de análisis de costo/beneficio para justificar las iniciativas de QMS, Surge el uso de benchmarking contra la industria y con los competidores. Se ha institucionalizado un programa de educación y entrenamiento para educar a todos los niveles de la organización en el tema de la calidad. Se están estandarizando herramientas y prácticas y el análisis de causas raíz se aplica de forma periódica. Se conducen encuestas de satisfacción de calidad de manera consistente. Existe un programa bien estructurado y estandarizado para medir la calidad. La gerencia de TI está construyendo una base de conocimiento para las métricas de calidad.

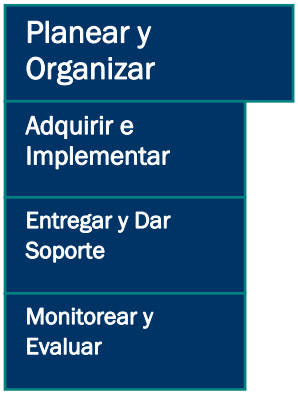
5 Optimizado cuando
El QMS está integrado y se aplica a todas las actividades de TI. Los procesos de QMS son flexibles y adaptables a los cambios en el ambiente de TI. Se mejora la base de conocimientos para métricas de calidad con las mejores prácticas externas. Se realiza benchmarking contra estándares externos rutinariamente. Las encuestas de satisfacción de la calidad constituyen un proceso constante y conducen al análisis de causas raíz y a medidas de mejora. Existe aseguramiento formal sobre el nivel de los procesos de administración de la calidad.

DESCRIPCIÓN DEL PROCESO.

P09. Evaluar y Administrar los Riesgos de TI.

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. 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 Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia.





Control sobre el proceso TI de

Evaluar y administrar los riesgos de TI

Que satisface el requerimiento del negocio de TI para

Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio

Enfocándose en

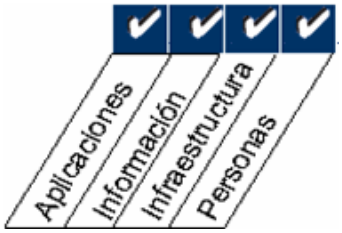
La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales

Se logra con

- La garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente
- La realización de evaluaciones de riesgo
- La recomendación y comunicación de planes de acción para remediar riesgos

Y se mide con

- Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos
- Porcentaje de riesgos críticos de TI identificados con planes de acción elaborados
- Porcentaje de planes de acción de administración de riesgos aprobados para su implantación



OBJETIVOS DE CONTROL

P09. Evaluar y Administrar los Riesgos de TI.

P09.1 Marco de Trabajo de Administración de Riesgos
Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.

P09.2 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.

P09.3 Identificación de Eventos
Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.

P09.4 Evaluación de Riesgos de TI
Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

P09.5 Respuesta a los Riesgos
Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición en forma continua. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

P09.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos
Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

DIRECTRICES GERENCIALES

P09. Evaluar y Administrar los Riesgos de TI.

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI, portafolio de servicios de TI
PO10	Plan de administración de riesgos de proyectos
DS2	Riesgos de proveedores
DS4	Resultados de pruebas de contingencia
DS5	Amenazas y vulnerabilidades de seguridad
ME1	Tendencias y eventos de riesgos históricos
ME4	Apetito empresarial de riesgos de TI

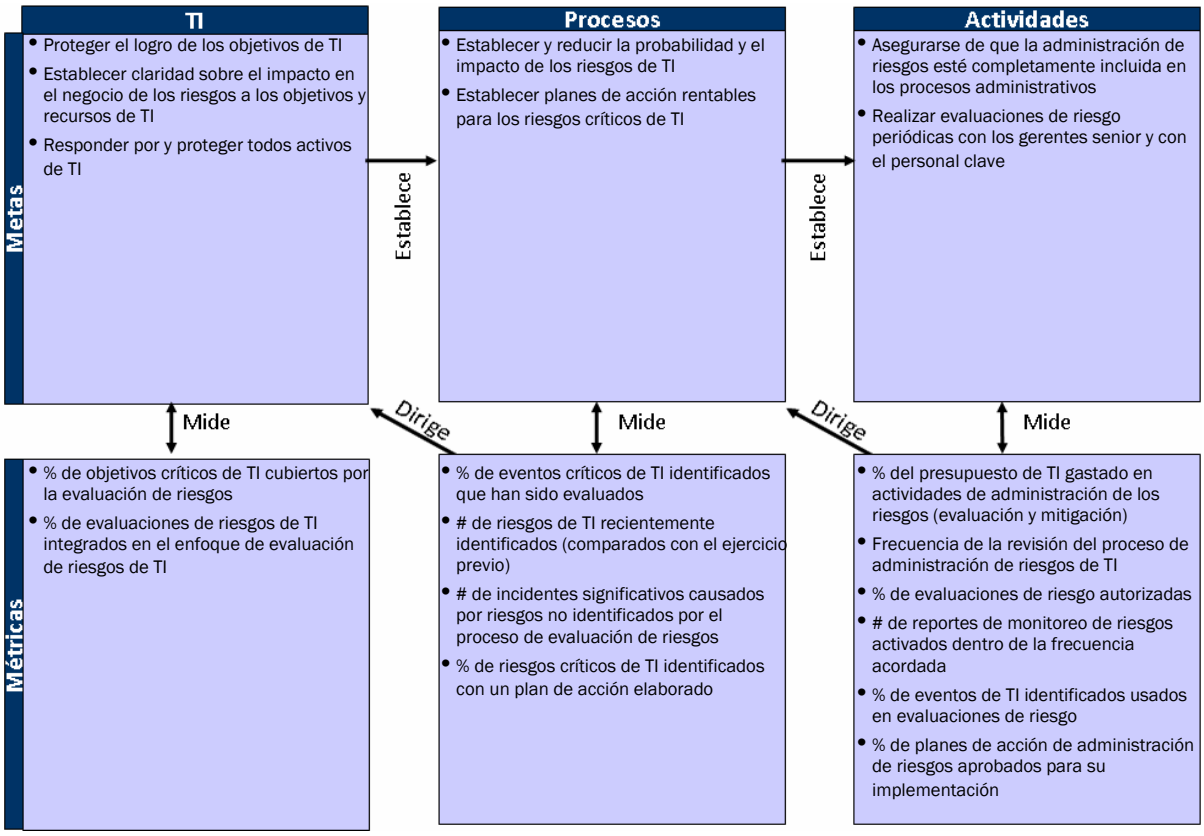
Salidas	Hacia						
Evaluación de riesgos	PO1	DS4	DS5	DS12	ME4		
Reporte de riesgos	ME4						
Directrices de administración de riesgos relacionados con TI	PO6						
Planes de acciones correctivas para riesgos relacionados con TI	PO4	AI6					

Matriz RACI

Actividades \ Funciones	CEO	CFO	Ejecutivo del Negocio	CIO	Consejo de Administración	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Determinar la alineación de la administración de riesgos (ej: Evaluar riesgo)	A	A/R	C	C	A/R	I					I
Entender los objetivos de negocio estratégicos relevantes		C	C	A/R	C	C					I
Entender los objetivos de los procesos de negocio relevantes				C	C	A/R					I
Identificar los objetivos internos de TI y establecer el contexto del riesgo					A/R		C	C	C		I
Identificar eventos asociados con objetivos (algunos eventos están orientados a negocio (negocio es A); algunos están orientados a TI (TI es A, negocio es C)	I			A/C	A	R	R	R	R		C
Asesorar el riesgo con los eventos				A/C	A	R	R	R	R		C
Evaluar y seleccionar respuestas a riesgos	I	I	A	A/C	A	R	R	R	R		C
Priorizar y Planear actividades de control	C	C	A	A	R	R	C	C	C		C
Aprobar y asegurar fondos para planes de acción de riesgos		A	A		R	I	I	I	I		I
Mantener y Monitorear un plan de acción de riesgos	A	C	I	R	R	C	C	C	C	C	R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P09. Evaluar y Administrar los Riesgos de TI.

La administración del proceso de *Evaluar y administrar los riesgos de TI* que satisfaga el requerimiento 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 rara vez a gerentes específicos. 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 a 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 Intuitivo cuando
Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.

3 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 deja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio 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 consideran las responsabilidades de administración de riesgos.

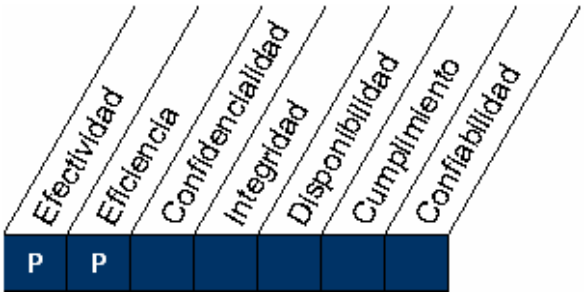
4 Administrado y Medible cuando
La evaluación y administración de riesgos son procedimientos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan 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 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 dueño nombrado, 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 un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular. Se establece una base de datos de administración de riesgos, y parte del proceso de administración de riesgos se empieza a automatizar. La gerencia de TI considera las estrategias de mitigación de riesgo.

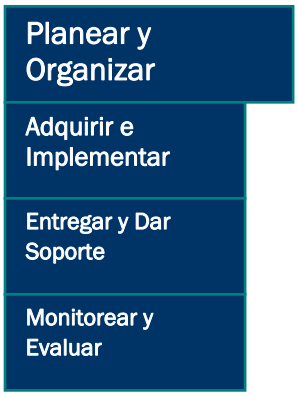
5 Optimizado cuando
La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están 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 detecta y actúa cuando se toman decisiones grandes de inversión o de operación de TI, sin considerar el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.

DESCRIPCIÓN DEL PROCESO.

P10. Administrar Proyectos.

Establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos. 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 post-implantación después de la instalación 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 la contribución a los programas de inversión facilitados por TI.





Control sobre el proceso TI de

Administrar proyectos

Que satisface el requerimiento del negocio de TI para

La entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados

Enfocándose en

Un programa y un enfoque de administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los interesados y el monitoreo de los riesgos y los avances de los proyectos

Se logra con

- La definición e implantación de marcos de trabajo y enfoques de programas y de proyectos
- La emisión de directrices de administración para proyectos
- La planeación de proyectos para todos los proyectos incluidos en el portafolio de proyectos

Y se mide con

- Porcentaje de proyectos que satisfacen las expectativas de los interesados (a tiempo, dentro del presupuesto, y con satisfacción de los requerimientos – ponderados por importancia)
- Porcentaje de proyectos con revisión post-implantación
- Porcentaje de proyectos que siguen estándares y prácticas de administración de proyectos

OBJETIVOS DE CONTROL

P10. Administrar Proyectos.

PO10.1 Marco de Trabajo para la Administración de Programas
Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversiones facilitadas por 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.

PO10.2 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 en cada proyecto emprendido. El marco de trabajo y los métodos de soporte se deben integrar con los procesos de administración de programas.

PO10.3 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 de proyectos, 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.

PO10.4 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 inversiones facilitadas por TI.

PO10.5 Declaración 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 inversiones facilitadas por TI. La definición se debe aprobar de manera formal por parte de los patrocinadores del programa y del proyecto antes de iniciar el proyecto.

PO10.6 Inicio de las Fases del Proyecto
Aprobar el inicio de las etapas importantes del proyecto y comunicarlo 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.

PO10.7 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.

PO10.8 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.

PO10.9 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, respuesta, 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, Reporte y Monitoreo del Proyecto

Medir el desempeño del proyecto contra los criterios clave del proyecto (Ej. alcance, cronograma, 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, Implementar 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 relevante 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.

Página dejada en blanco intencionadamente.

DIRECTRICES GERENCIALES

P10. Administrar Proyectos.

Desde	Entradas
PO1	Portafolio de proyectos
PO5	Portafolio de proyectos de TI actualizado
PO7	Matriz de habilidades de TI
PO8	Estándares de desarrollo
AI7	Revisión post-implantación

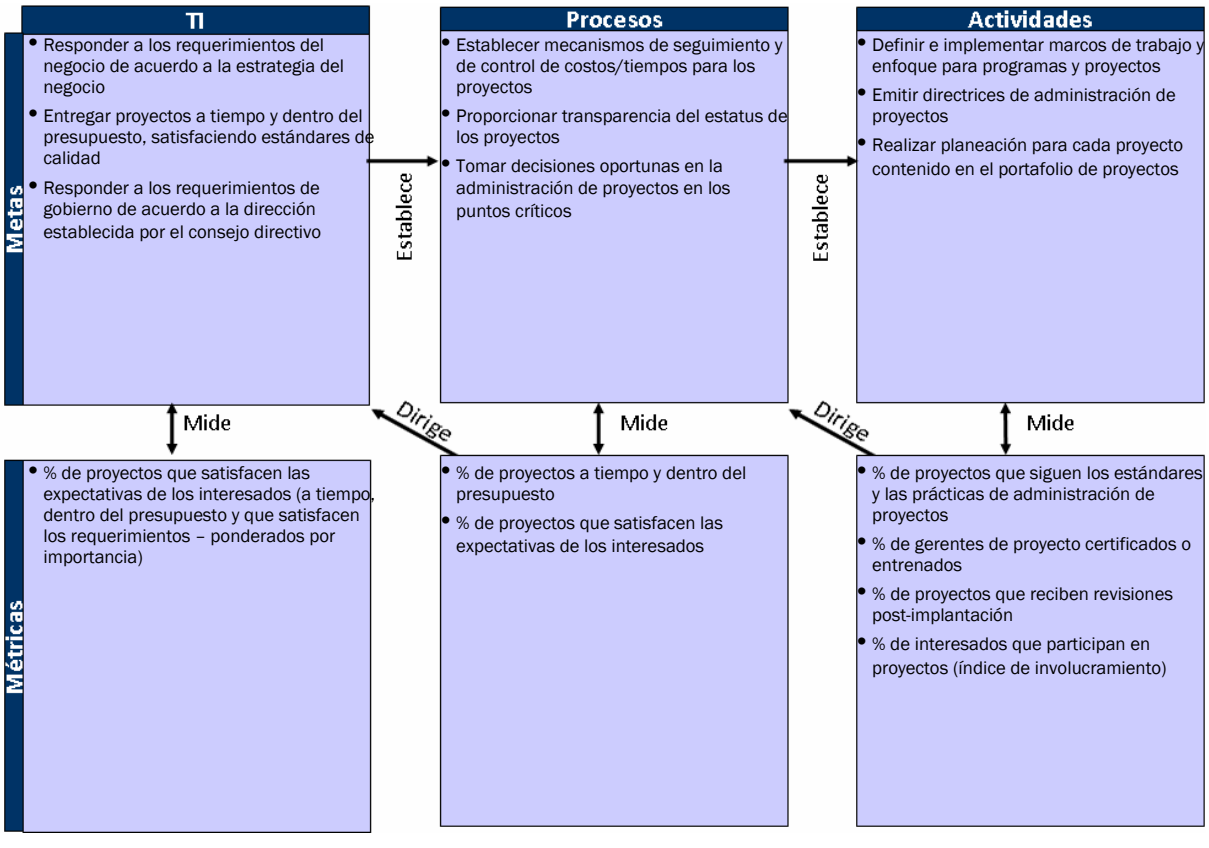
Salidas	Hacia
Reportes de desempeño del proyecto	ME1
Plan de administración de riesgos del proyecto	PO9
Directrices de administración del proyecto	AI1...AI7
Planes detallados del proyecto	PO8, AI1... AI7, DS6
Portafolio actualizado de proyectos de TI	PO1, PO5

Matriz RACI

Actividades / Funciones	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir un marco de administración de programas/portafolio para inversiones en TI	C	C	A	R						C	C
Establecer y mantener un marco de trabajo para la administración de proyectos de TI	I	I	I	A/R	I	C	C	C	C	R	C
Establecer y mantener un sistema de monitoreo, medición y administración de sistemas	I	I	I	R		C	C	C	C	A/R	C
Elaborar, estatutos, calendarios, planes de calidad, presupuestos, y planes de comunicación y de administración de riesgos			C	C	C	C	C	C	C	A/R	C
Asegurar la participación y compromiso de los interesados del proyecto	I		A	R	C						C
Asegurar el control efectivo de los proyectos y de los cambios a proyectos			C	C		C	C	C		A/R	C
Definir e Implementar métodos de aseguramiento y revisión de proyectos			I	C				I		A/R	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

P10. Administrar Proyectos.

La administración del proceso de *Administrar proyectos* que satisfaga el requerimiento 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, cronogramas 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 Intuitivo cuando
La alta dirección ha obtenido y comunicado la conciencia de la necesidad de la administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos proyecto por 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 de cada gerente de proyecto.

3 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, cronogramas 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 sólo 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 implementa 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
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. Una oficina de administración de proyectos integrada 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.

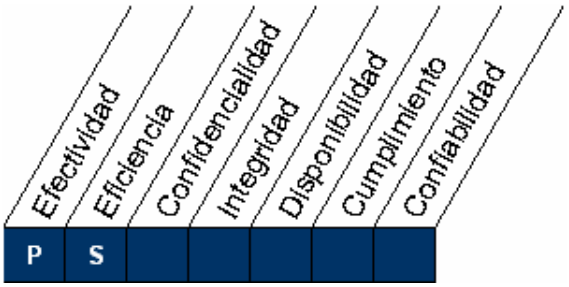
ADQUIRIR E IMPLEMENTAR

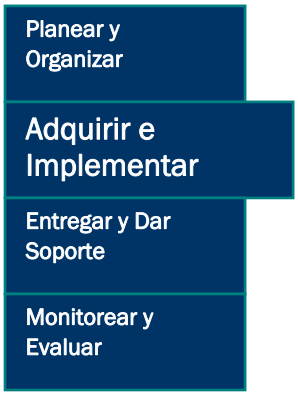
- **AI1** Identificar soluciones automatizadas
- **AI2** Adquirir y mantener software aplicativo
- **AI3** Adquirir y mantener infraestructura tecnológica
- **AI4** Facilitar la operación y el uso
- **AI5** Adquirir recursos de TI
- **AI6** Administrar cambios
- **AI7** Instalar y acreditar soluciones y cambios

DESCRIPCIÓN DEL PROCESO.

AI1 Identificar Soluciones Automatizadas

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de "desarrollar" o "comprar". Todos estos pasos permiten a las organizaciones minimizar el costo para Adquirir e Implementar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.





Control sobre el proceso TI de

Identificar soluciones automatizadas

Que satisface el requerimiento del negocio de TI para

Traducir los requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas

Enfocándose en

La identificación de soluciones técnicamente factibles y rentables

Se logra con

- La definición de los requerimientos técnicos y de negocio
- Realizar estudios de factibilidad como se define en los estándares de desarrollo
- Aprobar (o rechazar) los requerimientos y los resultados de los estudios de factibilidad

Y se mide con

- Número de proyectos donde los beneficios establecidos no se lograron debido a suposiciones de factibilidad incorrectas
- Porcentaje de estudios de factibilidad autorizados por el dueño del proceso
- Porcentaje de usuarios satisfechos con la funcionalidad entregada

OBJETIVOS DE CONTROL

AI1 Identificar Soluciones Automatizadas

AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio
Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI.

AI1.2 Reporte de Análisis de Riesgos
Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.

AI1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos
Desarrollar un estudio de factibilidad que examine la posibilidad de Implementar los requerimientos. La administración del negocio, apoyada por la función de TI, debe evaluar la factibilidad y los cursos alternativos de acción y realizar recomendaciones al patrocinador del negocio.

AI1.4 Requerimientos, Decisión de Factibilidad y Aprobación
Verificar que el proceso requiere al patrocinador del negocio para aprobar y autoriza los requisitos de negocio, tanto funcionales como técnicos, y los reportes del estudio de factibilidad en las etapas clave predeterminadas. El patrocinador del negocio tiene la decisión final con respecto a la elección de la solución y al enfoque de adquisición.

DIRECTRICES GERENCIALES

AI1 Identificar Soluciones Automatizadas

Desde	Entradas
PO1	Planes estratégicos y tácticos de TI
PO3	Actualizaciones periódicas del "estado de la tecnología"; estándares tecnológicos
PO8	Estándares de adquisición y desarrollo
PO10	Directrices de administración del proyecto y planes detallados del proyecto
AI6	Descripción del proceso de cambio
DS1	SLAs
DS3	Plan de desempeño y capacidad (requerimientos)

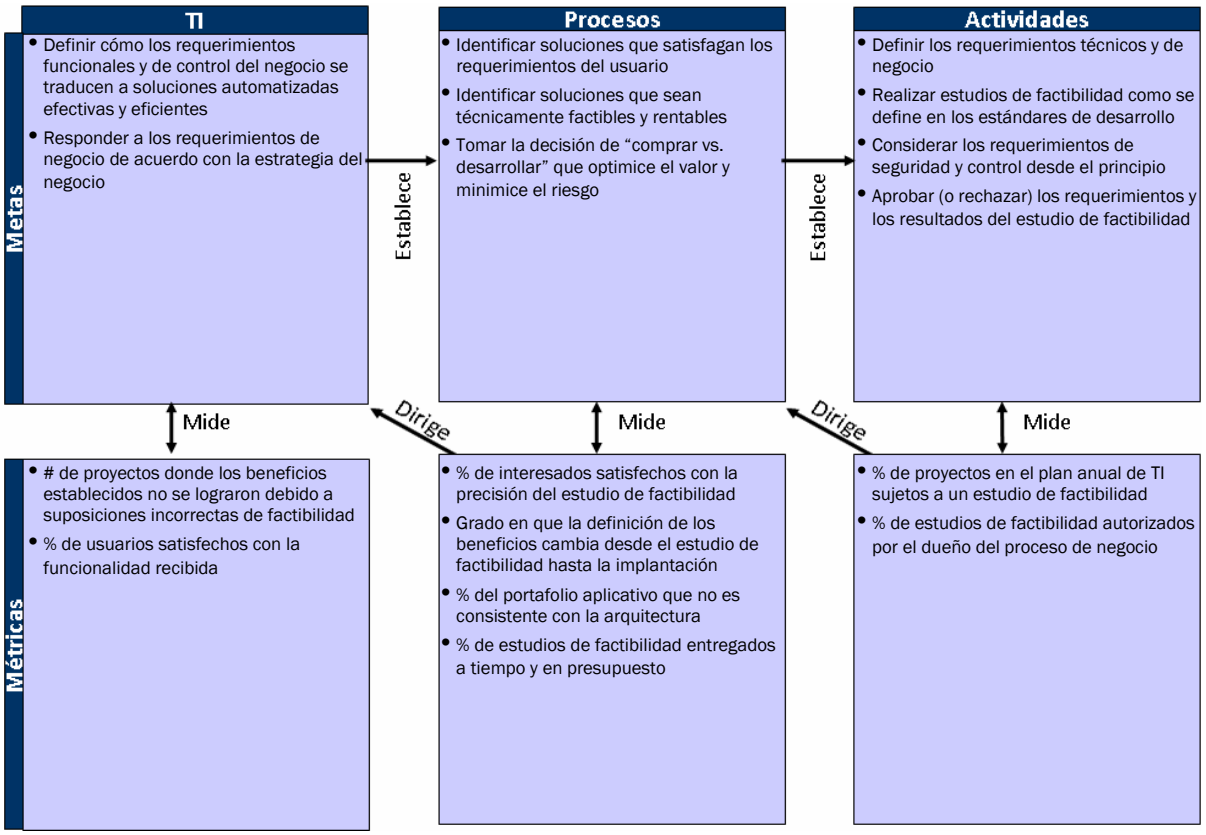
Salidas	Hacia						
Estudio de factibilidad de los requerimientos del negocio	PO2	PO5	PO7	AI2	AI3	AI4	AI5

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir los requerimientos funcionales y técnicos del negocio			C	C	R	C	R	R		A/R	I
Establecer procesos para la integridad / validez de los requerimientos				C		C		C		A/R	C
Identificar, documentar y analizar el riesgo del proceso de negocio			A/R	R	R	R	C	R		R	C
Conducir un estudio de factibilidad / evaluación de impacto con respecto a la implantación de los requerimientos de negocio propuestos			A/R	R	R	C	C	C		R	C
Evaluar los beneficios operativos de TI para las soluciones propuestas		I	R	A/R	R	I	I	I		R	
Evaluar los beneficios de negocio de las soluciones propuestas			A/R	R		C	C	C	I	R	
Elaborar un proceso de aprobación de requerimientos			C	A		C	C	C		R	C
Aprobar y autorizar soluciones propuestas		C	A/R	R	R	C	C	C	I	R	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI1 Identificar Soluciones Automatizadas

La administración del proceso de *Identificar soluciones automatizadas* que satisfaga el requerimiento de negocio de TI de *traducir los requerimientos funcionales y de control del negocio a diseño efectivo y eficiente de soluciones automatizadas* es:

0 No Existente cuando
La organización no requiere de la identificación de los requerimientos funcionales y operativos para el desarrollo, implantación o modificación de soluciones, tales como sistemas, servicios, infraestructura y datos. La organización no está consciente de las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.

1 Inicial / Ad Hoc cuando
Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas. Grupos individuales se reúnen para analizar las necesidades de manera informal y los requerimientos se documentan algunas veces. Los individuos identifican soluciones con base en una conciencia limitada de mercado o como respuesta a ofertas de proveedores. Existe una investigación o análisis estructurado mínimo de la tecnología disponible.

2 Repetible pero Intuitivo cuando
Existen algunos enfoques intuitivos para identificar que existen soluciones de TI y éstos varían a lo largo del negocio. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de unos cuantos individuos clave. La calidad de la documentación y de la toma de decisiones varía de forma considerable. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.

3 Definido cuando
Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.

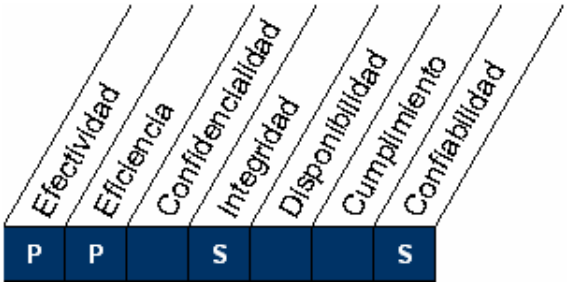
4 Administrado y Medible cuando
Existe una metodología establecida para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos. La documentación de los proyectos es de buena calidad y cada etapa se aprueba adecuadamente. Los requerimientos están bien articulados y de acuerdo con las estructuras predefinidas. Se consideran soluciones alternativas, incluyendo el análisis de costos y beneficios. La metodología es clara, definida, generalmente entendida y medible. Existe una interfaz definida de forma clara entre la gerencia de TI y la del negocio para la identificación y evaluación de las soluciones de TI.

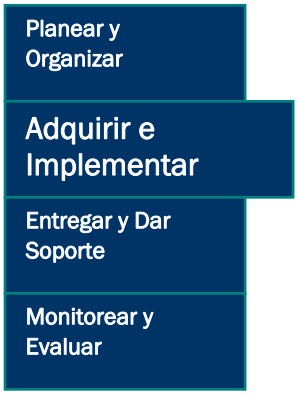
5 Optimizado cuando
La metodología para la identificación y evaluación de las soluciones de TI está sujeta a una mejora continua. La metodología de adquisición e implantación tiene la flexibilidad para proyectos de grande y de pequeña escala. La metodología está soportada en bases de datos de conocimiento internas y externas que contienen material de referencia sobre soluciones tecnológicas. La metodología en sí misma genera documentación en una estructura predefinida que hace que la producción y el mantenimiento sean eficientes. Con frecuencia, se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general. La gerencia detecta y toma medidas si las soluciones de TI se aprueban sin considerar tecnologías alternativas o los requerimientos funcionales del negocio.

DESCRIPCIÓN DEL PROCESO.

AI2 Adquirir y Mantener Software Aplicativo

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





Control sobre el proceso TI de

Adquirir y dar mantenimiento a software aplicativo

Que satisface el requerimiento del negocio de TI para

Construir las aplicaciones de acuerdo con los requerimientos del negocio y haciéndolas a tiempo y a un costo razonable

Enfocándose en

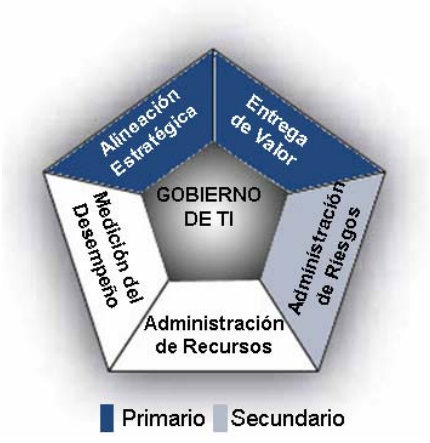
Garantizar que exista un proceso de desarrollo oportuno y confiable

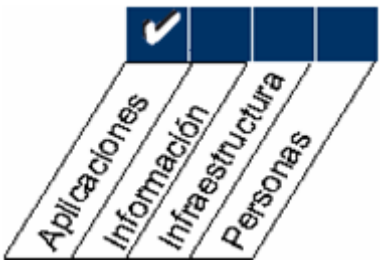
Se logra con

- La traducción de requerimientos de negocio a especificaciones de diseño
- La adhesión a los estándares de desarrollo para todas las modificaciones
- La separación de las actividades de desarrollo, de pruebas y operativas

Y se mide con

- Número de problemas en producción por aplicación, que causan tiempo perdido significativo
- Porcentaje de usuarios satisfechos con la funcionalidad entregada





OBJETIVOS DE CONTROL

AI2 Adquirir y Mantener Software Aplicativo

AI2.1 Diseño de Alto Nivel
Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para la adquisición de software, teniendo en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización. Tener aprobadas las especificaciones de diseño por gerencia para garantizar que el diseño de alto nivel responde a los requerimientos. Reevaluar cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento.

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. Realizar reevaluaciones cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento.

AI2.3 Control y Posibilidad de Auditar las Aplicaciones
Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que el procesamiento sea exacto, completo, oportuno, autorizado y auditable.

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 y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización.

AI2.5 Configuración e Implantación de Software Aplicativo Adquirido
Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio.

AI2.6 Actualizaciones Importantes en Sistemas Existentes
En caso de cambios importantes a los sistemas existentes que resulten en cambios significativos al diseño actual y/o funcionalidad, seguir un proceso de desarrollo similar al empleado para el desarrollo de sistemas nuevos.

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, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifican y direccionan para el software aplicativo desarrollado por terceros.

AI2.8 Aseguramiento de la Calidad del Software
Desarrollar, Implementar 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.

AI2.9 Administración de los Requerimientos de Aplicaciones
Seguir el estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el diseño, desarrollo e implementación, y aprobar los cambios a los requerimientos a través de un proceso de gestión de cambios establecido.

AI2.10 Mantenimiento de Software Aplicativo
Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software.

DIRECTRICES GERENCIALES

AI2 Adquirir y Mantener Software Aplicativo

Desde	Entradas
PO2	Diccionario de datos; esquema de clasificación de datos, plan optimizado de sistema del negocio
PO3	Actualizaciones periódicas del "estado de la tecnología"
PO5	Reporte de costo/beneficio
PO8	Estándares de adquisición y desarrollo
PO10	Directrices de administración del proyecto y planes detallados del proyecto
AI1	Estudio de factibilidad de los requerimientos del negocio
AI6	Descripción del proceso de cambio

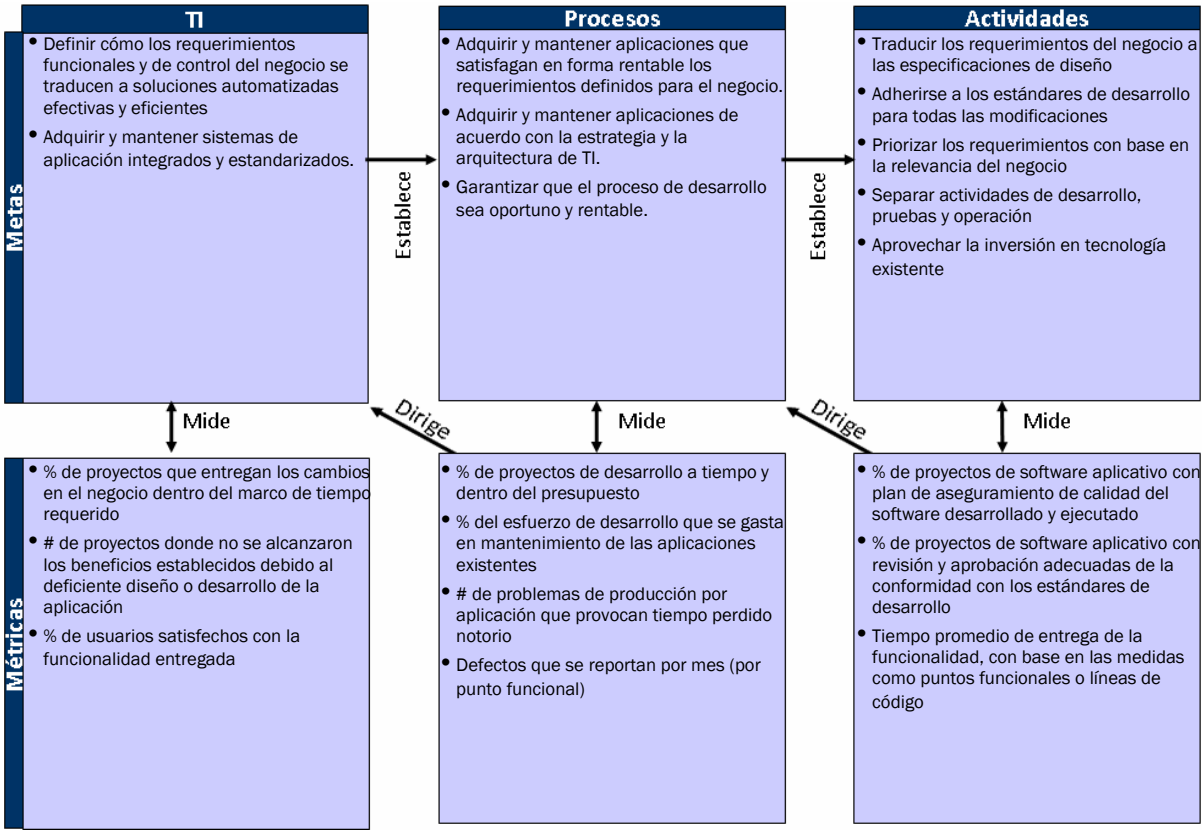
Salidas	Hacia						
Especificación de los controles de seguridad de la aplicación	DS5						
Conocimientos de la aplicación y del paquete de software	AI4						
Decisiones de adquisición	AI5						
SLAs de planeados inicialmente	DS1						
Especificación de disponibilidad, continuidad y recuperación	DS3	DS4					

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Traducir los requerimientos del negocio en especificaciones de diseño de alto nivel					C		C	A/R		R	C
Preparar diseño detallado y los requerimientos técnicos del software aplicativo				I	C	C	C	A/R		R	C
Especificar los controles de aplicación dentro del diseño					R	C		A/R		R	R
Personalizar e implementar la funcionalidad automatizada adquirida					C	C		A/R		R	C
Desarrollar las metodologías y procesos formales para administrar el proceso de desarrollo de la aplicación				C		C	C	A	C	R	C
Crear un plan de aseguramiento de la calidad del software para el proyecto					I		C	R		A/R	C
Dar seguimiento y administrar los requerimientos de la aplicación								R		A/R	
Desarrollar un plan para el mantenimiento de aplicaciones de software				C		C		A/R		C	

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI2 Adquirir y Mantener Software Aplicativo

La administración del proceso de *Adquirir y mantener software aplicativo* que satisfaga el requerimiento 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 Intuitivo 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 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

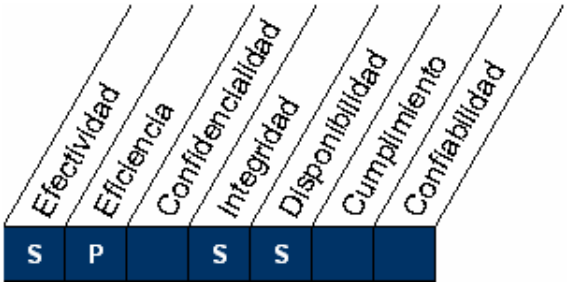
4 Administrado y Medible cuando
Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación. Existen mecanismos de aprobación documentados y acordados, para garantizar que se 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.

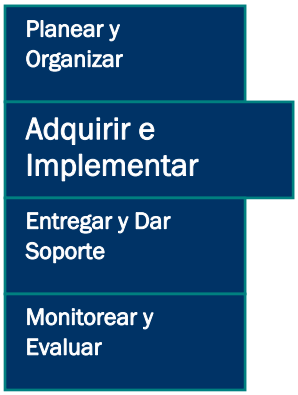
5 Optimizado cuando
Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base en componentes, con aplicaciones predefinidas y estandarizadas que corresponden a las necesidades del negocio. El enfoque se extiende para toda la empresa. 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.

DESCRIPCIÓN DEL PROCESO.

AI3 Adquirir y Mantener Infraestructura Tecnológica

Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.





Control sobre el proceso TI de

Adquirir y dar mantenimiento a la infraestructura tecnológica

Que satisface el requerimiento del negocio de TI para

Adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI

Enfocándose en

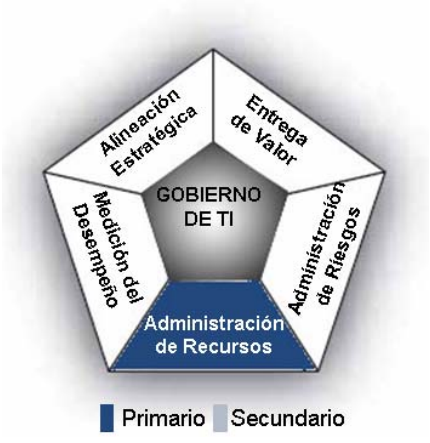
Proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología

Se logra con

- El establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica
- La planeación de mantenimiento de la infraestructura
- La implantación de medidas de control interno, seguridad y auditabilidad

Y se mide con

- El porcentaje de plataformas que no se alinean con la arquitectura de TI definida y los estándares de tecnología
- El número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será)
- El número de componentes de infraestructura que ya no se pueden soportar (o que ya no se podrán en el futuro cercano)



OBJETIVOS DE CONTROL

AI3 Adquirir y Mantener Infraestructura Tecnológica

AI3.1 Plan de Adquisición de Infraestructura Tecnológica
Generar un plan para adquirir, Implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica.

AI3.2 Protección y Disponibilidad del Recurso de Infraestructura
Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso.

AI3.3 Mantenimiento de la Infraestructura
Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

AI3.4 Ambiente de Prueba de Factibilidad
Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo. Hay que considerar la funcionalidad, la configuración de hardware y software, pruebas de integración y desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad.

DIRECTRICES GERENCIALES

AI3 Adquirir y Mantener Infraestructura Tecnológica

Desde	Entradas
PO3	Plan de infraestructura de tecnología; estándares y oportunidades, actualizaciones periódicas del "estado de tecnología"
PO8	Estándares de adquisición y desarrollo
PO10	Directrices de administración de proyecto y planes detallados de proyecto
AI1	Estudio de factibilidad de los requerimientos del negocio
AI6	Descripción del proceso de cambio
DS3	Plan de desempeño y capacidad (requerimientos)

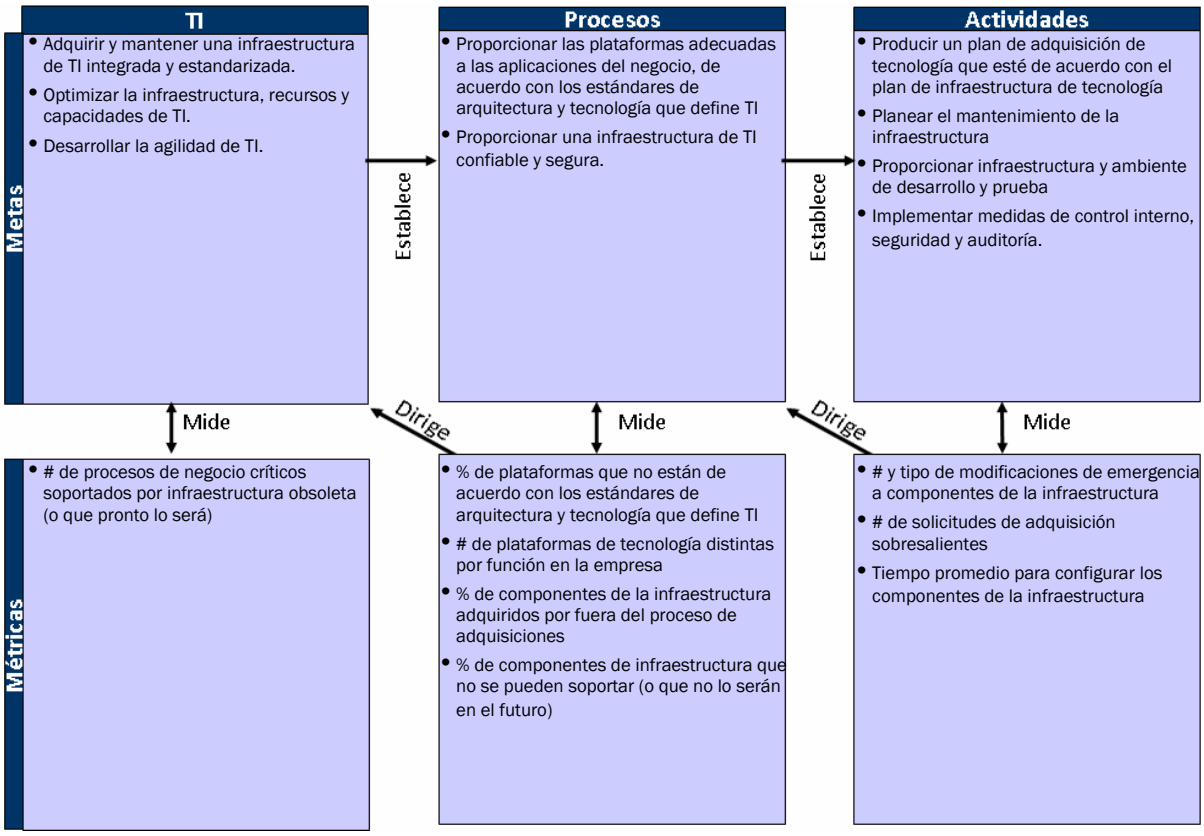
Salidas	Hacia
Decisiones de adquisición	AI5
Sistema configurado para realizar prueba / instalación	AI7
Requerimientos de ambiente físico	DS12
Actualizaciones de estándares de tecnología	PO3
Requerimientos de monitoreo del sistema	DS3
Conocimiento de la infraestructura	AI4
OLAs planeadas inicialmente	DS1

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir el procedimiento / proceso de adquisición		C		A		C	C	C	R		I
Negociar la compra y adquirir la infraestructura requerida con proveedores (aprobados)		C/I		A	I	R	C	C	R		I
Definir estrategia y Planear el mantenimiento de infraestructura				A		R	R	R	C		
Configurar componentes de la infraestructura				A		R	C				I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI3 Adquirir y Mantener Infraestructura Tecnológica

La administración del proceso de *Adquirir y mantener infraestructura de tecnología* que satisfaga el requerimiento de negocio de TI de *adquirir y mantener una infraestructura de TI integrada y estandarizada* es:

0 No Existente cuando
No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.

1 Inicial / Ad Hoc cuando
Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.

2 Repetible pero Intuitivo cuando
No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.

3 Definido cuando
Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.

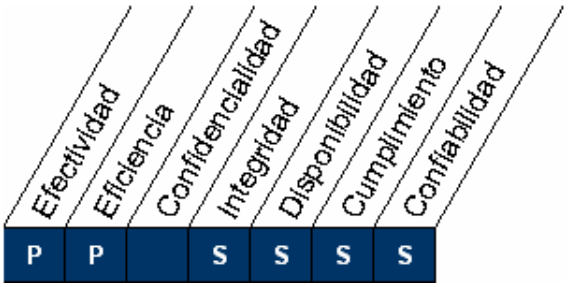
4 Administrado y Medible cuando
Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.

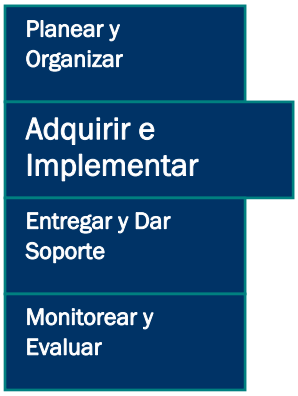
5 Optimizado cuando
El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología. Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración. Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización. Con un alto nivel de conciencia se pueden identificar los medios óptimos para mejorar el desempeño en forma preventiva, incluyendo el considerar la opción de contratar servicios externos. La infraestructura de TI se entiende como el apoyo clave para impulsar el uso de TI.

DESCRIPCIÓN DEL PROCESO.

AI4 Facilitar la Operación y el Uso

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.





Control sobre el proceso TI de

Facilitar la operación y el uso

Que satisface el requerimiento del negocio de TI para

Garantizar la satisfacción de los usuarios finales mediante ofrecimientos de servicios y niveles de servicio, y de forma transparente integrar las soluciones de aplicación y tecnología dentro de los procesos del negocio

Enfocándose en

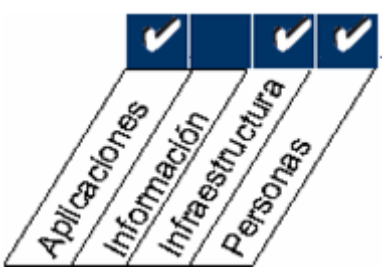
Proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitosos del sistema.

Se logra con

- El desarrollo y la disponibilidad de documentación para transferir el conocimiento
- Comunicación y entrenamiento a usuarios y a la gerencia del negocio, al personal de apoyo y al personal de operación
- La generación de materiales de entrenamiento

Y se mide con

- El número de aplicaciones en que los procedimientos de TI se integran en forma transparente dentro de los procesos de negocio
- El porcentaje de dueños de negocios satisfechos con el entrenamiento De aplicación y los materiales de apoyo.
- El número de aplicaciones que cuentan con un adecuado entrenamiento de apoyo al usuario y a la operación



OBJETIVOS DE CONTROL

AI4 Facilitar la Operación y el Uso

AI4.1 Plan para Soluciones de Operación
Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operativos, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.

AI4.2 Transferencia de Conocimiento a la Gerencia del Negocio
Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación. La transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente.

AI4.3 Transferencia de Conocimiento a Usuarios Finales
Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y al continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación del usuario clave, y evaluación.

AI4.4 Transferencia de Conocimiento al Personal de Operaciones y Soporte
Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoyen y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir al entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.

DIRECTRICES GERENCIALES

AI4 Facilitar la Operación y el Uso

Desde	Entradas
PO10	Directrices de administración del proyecto y planes detallados de proyecto
AI1	Estudio de factibilidad de requerimientos del negocio
AI2	Conocimientos de la aplicación y de software de paquete
AI3	Conocimiento de la infraestructura
AI7	Errores conocidos y admitidos
DS7	Actualizaciones de documentación requeridas

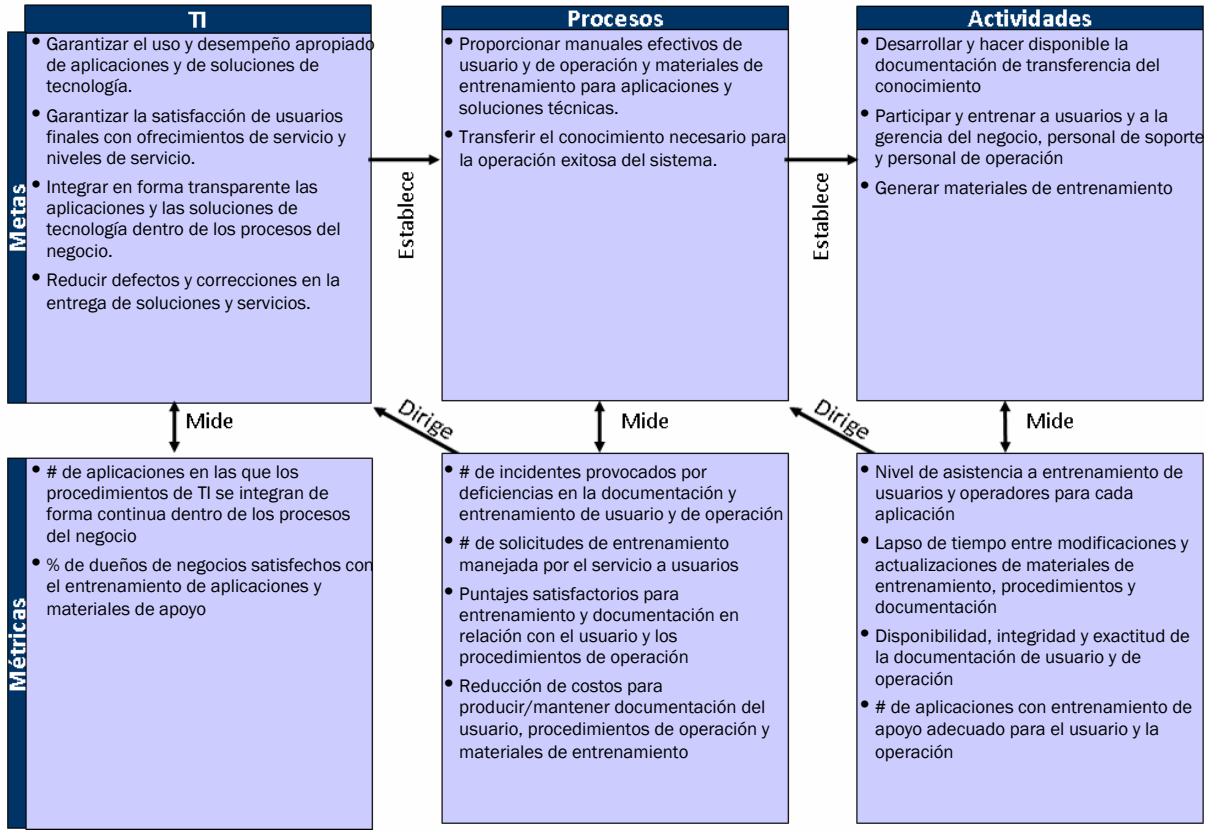
Salidas	Hacia						
Manuales de usuario, de operación, de soporte, técnicos y de administración	AI7	DS4	DS8	DS9	DS11	DS13	
Requerimientos de transferencia de conocimiento para implantación de soluciones	DS7						
Materiales de entrenamiento	DS7						

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Equipo de Despliegue	Departamento de entrenamiento
Desarrollar estrategia para que la solución sea operativa				A	A	R		R			I	R	C
Desarrollar metodología de transferencia de conocimiento				C	A							C	R
Desarrollar manuales de procedimiento del usuario final					A/R			R			C	C	
Desarrollar documentación de soporte técnica para operaciones y personal de soporte						A/R		C			C		
Desarrollar y dar entrenamiento					A	A		R					R
Evaluar los resultados del entrenamiento y ampliar la documentación como se requiera					A	A						R	R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI4 Facilitar la Operación y el Uso

La administración del proceso de *Facilitar la operación y el uso* que satisfaga el requerimiento de negocio de TI de *garantizar la satisfacción de los usuarios finales con ofrecimiento de servicios y niveles de servicio, e integrar de forma transparente aplicaciones y soluciones de tecnología dentro de los procesos del negocio* es:

0 No Existente cuando
No existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento. Los únicos materiales existentes son aquellos que se suministran con los productos que se adquieren.

1 Inicial / Ad Hoc cuando
Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.

2 Repetible pero Intuitivo cuando
Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.

3 Definido cuando
Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.

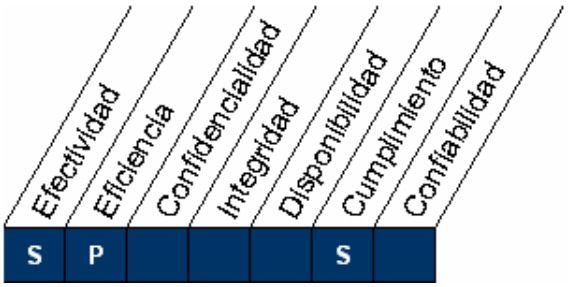
4 Administrado y Medible cuando
Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas y las unidades de negocio, de manera que se pueden observar los procesos desde una perspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfases. Existen controles para garantizar que se adhieren los estándares y que se desarrollan y mantienen procedimientos para todos los procesos. La retroalimentación del negocio y del usuario sobre la documentación y el entrenamiento se recopila y evalúa como parte de un proceso continuo de mejora. Los materiales de documentación y entrenamiento se encuentran generalmente a un buen nivel, predecible, de confiabilidad y disponibilidad. Se implanta un proceso emergente para el uso de documentación y administración automatizada de procedimiento. El desarrollo automatizado de procedimientos se integra cada vez más con el desarrollo de sistemas aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega de documentación, materiales y programas de entrenamiento.

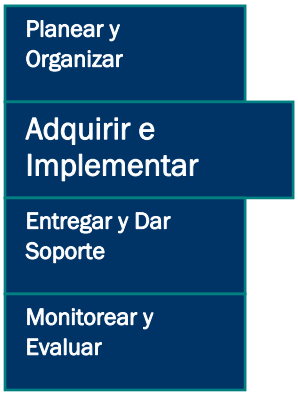
5 Optimizado cuando
El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante que se mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, flujo de trabajo y tecnologías de distribución, que los hacen accesibles y fáciles de mantener. El material de documentación y entrenamiento se actualiza para reflejar los cambios en la organización, en la operación y en el software. Tanto el desarrollo de materiales de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones de proceso del negocio, siendo así un apoyo a los requerimientos de toda la organización y no tan sólo procedimientos orientados a TI.

DESCRIPCIÓN DEL PROCESO.

AI5 Adquirir Recursos de TI

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.





Control sobre el proceso TI de

Adquirir recursos de TI

Que satisface el requerimiento del negocio de TI para

Mejorar la rentabilidad de TI y su contribución a la utilidad del negocio

Enfocándose en

Adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI

Se logra con

- La obtención de asesoría profesional legal y contractual
- La definición de procedimientos y estándares de adquisición
- La adquisición de hardware, software y servicios requeridos de acuerdo con los procedimientos definidos

Y se mide con

- El número de controversias en relación con los contratos de adquisición
- La reducción del costo de compra
- El porcentaje de interesados clave satisfechos con los proveedores

OBJETIVOS DE CONTROL

AI5 Adquirir Recursos de TI

AI5.1 Control de Adquisición
Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada con TI, instalaciones, hardware, software y servicios necesarios por el negocio.

AI5.2 Administración de Contratos con Proveedores
Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

AI5.3 Selección de Proveedores
Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar la mejor viable y encajable según los requerimientos especificados. Los requerimientos deben estar optimizados con las entradas de los proveedores potenciales.

AI5.4 Adquisición de Recursos de TI
Proteger y hacer cumplir los intereses de la organización en todo los contratos de adquisiciones, incluyendo los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software, recursos de desarrollo, infraestructura y servicios.

DIRECTRICES GERENCIALES

AI5 Adquirir Recursos de TI

Desde	Entradas
PO1	Estrategia de adquisición de TI
PO8	Estándares de adquisición
PO10	Directrices de administración de proyecto y planes detallados de proyecto
AI1	Estudio de factibilidad de requerimientos del negocio
AI2-3	Decisiones de adquisición
DS2	Catálogo de proveedores

Salidas	Hacia
Requerimientos de administración de la relación con terceros	DS2
Artículos provistos	AI7
Arreglos contractuales	DS2

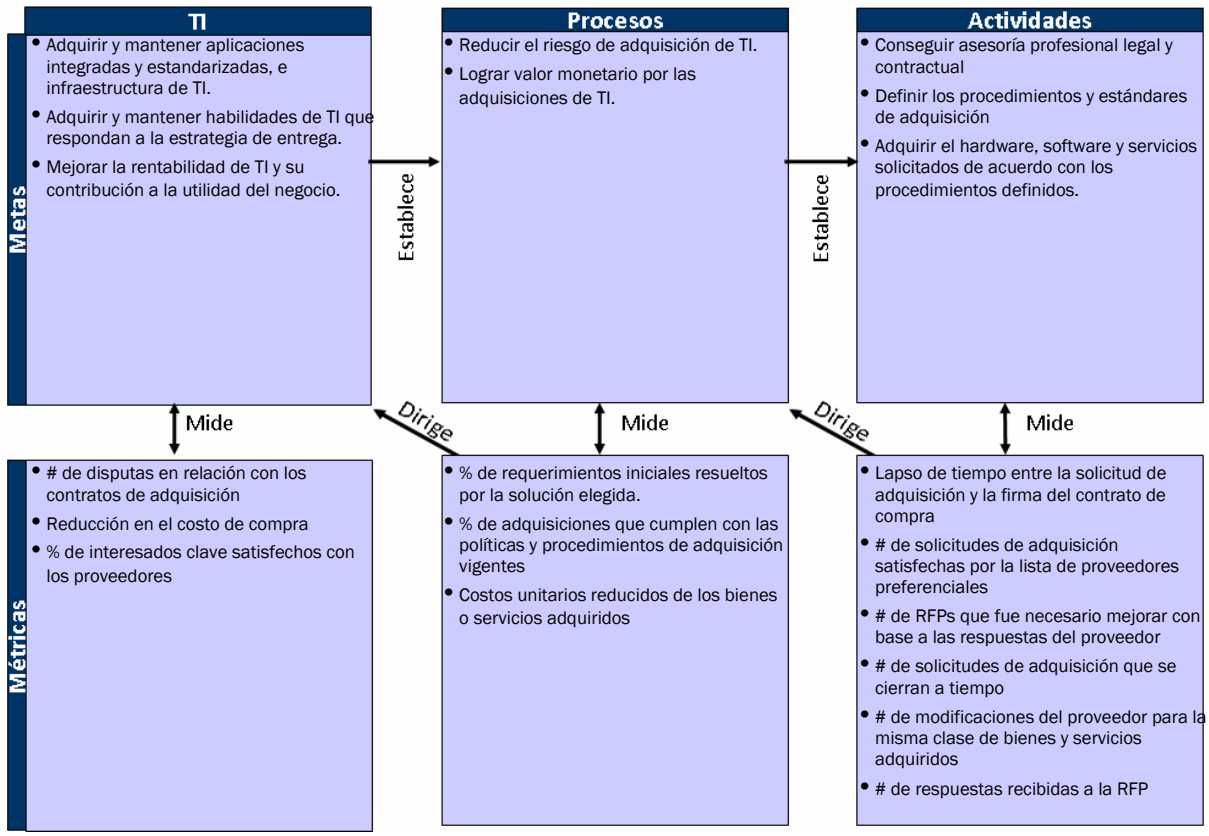
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Desarrollar políticas y procedimientos de adquisición de TI de acuerdo con las políticas de adquisiciones a nivel corporativo	I	C		A		I	I	I	R		C
Establecer / mantener una lista de proveedores acreditados									A/R		
Evaluar y seleccionar proveedores a través de un proceso de solicitud de propuesta (RFP)	C	C		A		R		R	R	R	C
Desarrollar contratos que protejan los intereses de la organización	R	C		A		R		R	R		C
Realizar adquisiciones de conformidad con los procedimientos establecidos				A		R		R	R		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI5 Adquirir Recursos de TI

La administración del proceso de *Adquirir recursos de TI* que satisfaga el requerimiento de negocio de TI de *mejorar la rentabilidad de TI y su contribución a la utilidad del negocio* es:

0 No Existente cuando
No existe un proceso definido de adquisición de recursos de TI. La organización no reconoce la necesidad de tener políticas y procedimientos claros de adquisición para garantizar que todos los recursos de TI se encuentren disponibles y de forma oportuna y rentable.

1 Inicial / Ad Hoc cuando
La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe un relación ad hoc entre los procesos de administración de adquisiciones y contratos corporativos y TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.

2 Repetible pero Intuitivo cuando
Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización del negocio. Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.

3 Definido cuando
La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos. La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de TI.

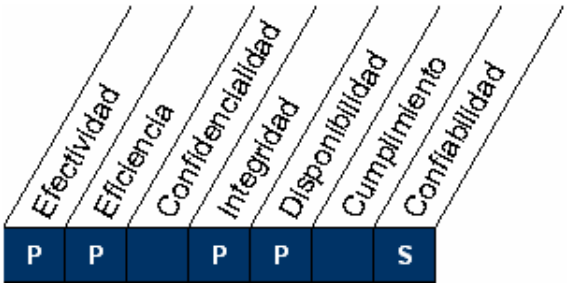
4 Administrado y Medible cuando
La adquisición de TI se integra totalmente con los sistemas generales de adquisición de la organización. Se utilizan los estándares para la adquisición de recursos de TI en todos los procesos de adquisición. Se toman medidas para la administración de contratos y adquisiciones relevantes para los casos de negocio que requieran la adquisición de TI. Se dispone de reportes que sustentan los objetivos de negocio. La administración está consciente por lo general, de las excepciones a las políticas y procedimientos para la adquisición de TI. Se está desarrollando una administración estratégica de relaciones. La administración de TI implanta el uso de procesos de administración para adquisición y contratos en todas las adquisiciones mediante la revisión de medición al desempeño

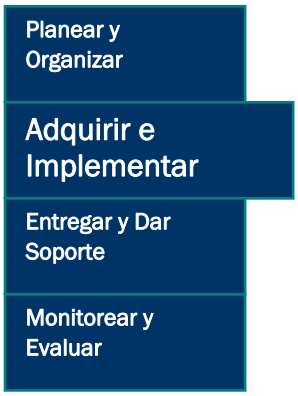
5 Optimizado cuando
La administración instituye y da recursos a procesos exhaustivos para la adquisición de TI. La administración impulsa el cumplimiento de las políticas y procedimientos de adquisición de TI. Se toman las medidas en la administración de contratos y adquisiciones, relevantes en casos de negocio para adquisición de TI. Se establecen buenas relaciones con el tiempo con la mayoría de los proveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Los estándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejan estratégicamente y responden a la medición del proceso. La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI.

DESCRIPCIÓN DEL PROCESO.

AI6 Administrar Cambios

Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formalmente y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.





Control sobre el proceso TI de

Administrar cambios

Que satisface el requerimiento del negocio de TI para

Responder a los requerimientos del negocio de acuerdo con la estrategia de negocio, mientras se reducen los defectos y la repetición de trabajos en la prestación del servicio y en la solución.

Enfocándose en

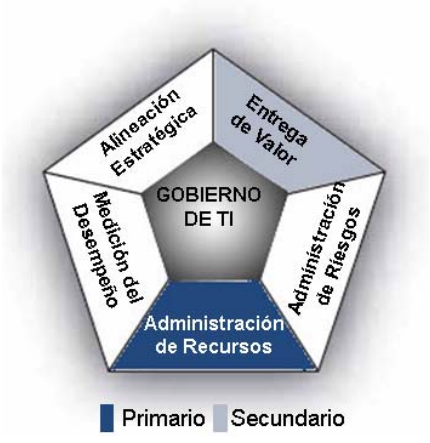
Controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados

Se logra con

- La definición y comunicación de los procedimientos de cambio, que incluyen cambios de emergencia
- La evaluación, la asignación de prioridad y autorización de cambios
- Seguimiento del estatus y reporte de los cambios

Y se mide con

- El número de interrupciones o errores de datos provocados por especificaciones inexactas o una evaluación de impacto incompleta
- La repetición de aplicaciones o infraestructura debida a especificaciones de cambio inadecuadas
- El porcentaje de cambios que siguen procesos de control de cambio formales



OBJETIVOS DE CONTROL

AI6 Administrar Cambios

AI6.1 Estándares y Procedimientos para Cambios
Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

AI6.2 Evaluación de Impacto, Priorización y Autorización
Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.

AI6.3 Cambios de Emergencia
Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia.

AI6.4 Seguimiento y Reporte del Estatus de Cambio
Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

AI6.5 Cierre y Documentación del Cambio
Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

DIRECTRICES GERENCIALES

AI6 Administrar Cambios

Desde	Entradas
PO1	Portafolio de proyectos TI
PO8	Acciones de mejora de la calidad
PO9	Planes de acción para solución de riesgos relacionados con TI
PO10	Directrices de administración de proyecto y plan de proyecto detallado
DS3	Cambios requeridos
DS5	Cambios de seguridad requeridos
DS8	Solicitudes de servicio / solicitudes de cambio
DS9-10	Solicitudes de cambio (dónde y cómo aplicar la solución)
DS10	Registros de problemas

Salidas	Hacia						
Descripción de proceso de cambio	AI1..AI3						
Reportes de estatus de cambio	ME1						
Autorización de cambio	AI7	DS8	DS10				

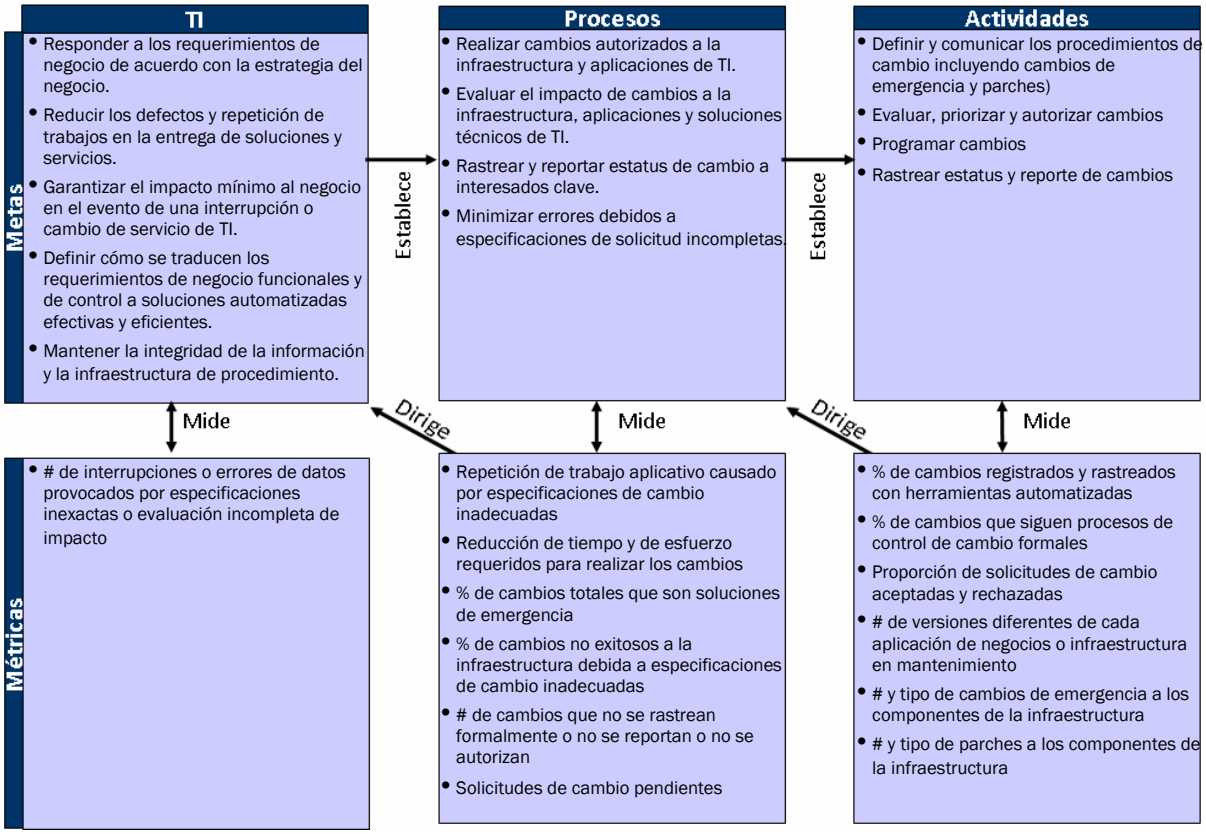
Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Desarrollar e implementar un proceso para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio				A	I	R	C	R	C	C	C
Evaluar impacto y dar prioridad a cambios en base a las necesidades del negocio				I	R	A/R	C	R	C	R	C
Garantizar que cualquier cambio crítico y de emergencia sigue el proceso aprobado				I	I	A/R	I	R			C
Autorizar cambios				I	C	A/R		R			
Administrar y diseminar la información relevante referente a cambios				A	I	R	C	R	I	R	C

Funciones

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI6 Administrar Cambios

La administración del proceso de *Administrar cambios* que satisfaga el requerimiento de negocio de TI de *responder a los requerimientos de acuerdo con la estrategia del negocio, mientras que se reducen los defectos y repeticiones de trabajos en la entrega de soluciones y servicios* es:

0 No Existente cuando
No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio.

1 Inicial / Ad Hoc cuando
Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.

2 Repetible pero Intuitivo cuando
Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio.

3 Definido cuando
Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado. Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente. El análisis de impacto de los cambios de TI en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.

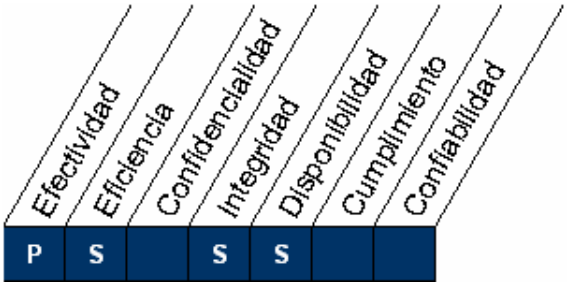
4 Administrado y Medible cuando
El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. El proceso es eficiente y efectivo, pero se basa en manuales de procedimientos y controles considerables para garantizar el logro de la calidad. Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción. Se da un proceso de aprobación para cambios. La documentación de administración de cambios es vigente y correcta, con seguimiento formal a los cambios. La documentación de configuración es generalmente exacta. La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio. Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio. Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.

5 Optimizado cuando
El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas. El proceso de revisión refleja los resultados del monitoreo. La información de la configuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.

DESCRIPCIÓN DEL PROCESO.

AI7 Instalar y Acreditar Soluciones y Cambios

Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operativos estén en línea con las expectativas convenidas y con los resultados.



Control sobre el proceso TI de

Instalar y acreditar soluciones y cambios

Que satisface el requerimiento del negocio de TI para

Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación

Enfocándose en

Probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libres de errores, y planear las liberaciones a producción

Se logra con

- El establecimiento de una metodología de prueba
- Realizar la planeación de la liberación (release)
- Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio
- Ejecutar revisiones posteriores a la implantación

Y se mide con

- Tiempo perdido de la aplicación o problemas de datos provocados por pruebas inadecuadas
- Porcentaje de sistemas que satisfacen los beneficios esperados, medidos en el proceso posterior a la implantación
- Porcentaje de proyectos con plan de prueba documentado y aprobado

OBJETIVOS DE CONTROL

AI7 Instalar y Acreditar Soluciones y Cambios

AI7.1 Entrenamiento
Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de sistemas de la información de desarrollo, implementación o modificación.

AI7.2 Plan de Prueba
Establecer un plan de pruebas basado en los estándares de la organización que define roles, responsabilidades, y criterios de entrada y salida. Asegurar que el plan esta aprobado por las partes relevantes.

AI7.3 Plan de Implantación
Establecer un plan de implantación y respaldo y vuelta atrás. Obtener aprobación de las partes relevantes.

AI7.4 Ambiente de Prueba
Definir y establecer un entorno seguro de pruebas representativo del entorno de operaciones planeado relativo a seguridad, controles internos, practicas operativos, calidad de los datos y requerimientos de privacidad, y cargas de trabajo.

AI7.5 Conversión de Sistemas y Datos
Plan de conversión de datos y migración de infraestructuras como parte de los métodos de desarrollo de la organización, incluyendo pistas de auditoria, respaldo y vuelta atrás.

AI7.6 Pruebas de Cambios
Pruebas de cambios independientemente en acuerdo con los planes de pruebas definidos antes de la migración al entorno de operaciones. Asegurar que el plan considera la seguridad y el desempeño.

AI7.7 Prueba de Aceptación Final.
Asegurar que el dueño de proceso de negocio y los interesados de TI evalúan los resultados de los procesos de pruebas como determina el plan de pruebas. Remediar los errores significativos identificados en el proceso de pruebas, habiendo completado el conjunto de pruebas identificadas en el plan de pruebas y cualquier prueba de regresión necesaria. Siguiendo la evaluación, aprobación promoción a producción.

AI7.8 Promoción a Producción
Seguimiento a pruebas, controlar la entrega de los sistemas cambiados a operaciones, manteniéndolo en línea con el plan de implantación. Obtener la aprobación de los interesados clave, tales como usuarios, dueño de sistemas y gerente de operaciones. Cuando sea apropiado, ejecutar el sistema en paralelo con el viejo sistema por un tiempo, y comparar el comportamiento y los resultados.

AI7.9 Revisión Posterior a la Implantación
Establecer procedimientos en línea con los estándares de gestión de cambios organizacionales para requerir una revisión posterior a la implantación como conjunto de salida en el plan de implementación.

DIRECTRICES GERENCIALES

AI7 Instalar y Acreditar Soluciones y Cambios

Desde	Entradas
PO3	Estándares de tecnología
PO4	Dueños de sistema documentado
PO8	Estándares de desarrollo
PO10	Directrices de administración de proyecto y plan de proyecto detallado
AI3	Sistema configurado a ser probado/instalado
AI4	Manuales de usuario, operativos, de soporte, técnicos y de administración
AI5	Adquisición de productos
AI6	Autorización de cambio

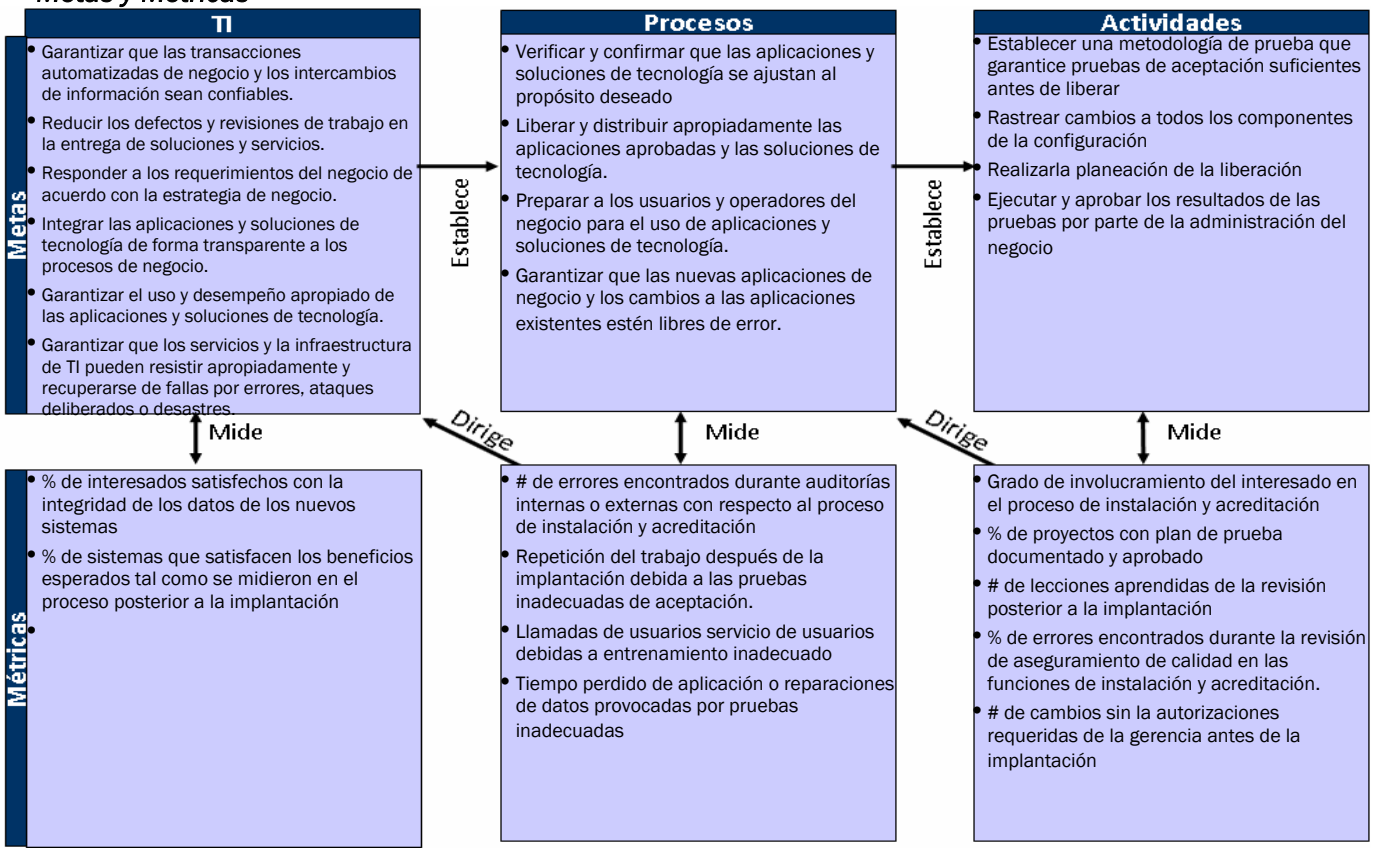
Salidas	Hacia						
Componentes de configuración liberados	DS8	DS9					
Errores conocidos y aceptados	AI4						
Liberación a producción	DS13						
Liberación de software y plan de distribución	DS13						
Revisión posterior a la implantación	PO2	PO5	PO10				
Monitoreo de control interno	ME2						

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Construir y revisar planes de investigación			C	A	I	C	C	R		C	C
Definir y revisar una estrategia de prueba (criterio de entrada y salida) y una metodología de plan de prueba operacional			C	A	C	C	C	R		C	C
Construir y mantener un repositorio de requerimientos de negocio y técnicos y casos de prueba para sistemas acreditados				A				R			
Ejecutar la conversión del sistema y las pruebas de integración en ambiente de prueba			I	I	R	C	C	A/R		I	C
Establecer ambiente de prueba y conducir pruebas de aceptación finales			I	I	R	A	C	A/R		I	C
Recomendar la liberación a producción con base en los criterios de acreditación convenidos			I	R	A	R	C	R		I	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

AI7 Instalar y Acreditar Soluciones y Cambios

La administración del proceso de *Instalar y acreditar soluciones y cambios* que satisfagan el requerimiento de negocio de TI de *implementar sistemas nuevos o modificados que funcionen sin mayores problemas después de su instalación* es:

0 No Existente cuando
Hay una ausencia completa de procesos formales de instalación o acreditación y ni la gerencia senior ni el personal de TI reconocen la necesidad de verificar que las soluciones se ajustan para el propósito deseado.

1 Inicial / Ad Hoc cuando
Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares y los enfoques que se toman varían. La acreditación formal y la autorización son raras o no existentes.

2 Repetible pero Intuitivo cuando
Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología. Los equipos individuales de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.

3 Definido cuando
Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto. El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales. La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación.

4 Administrado y Medible cuando
Los procedimientos son formales y se desarrollan para ser organizados y prácticos con ambientes de prueba definidos y con procedimientos de acreditación. En la práctica, todos los cambios mayores de sistemas siguen este enfoque formal. La evaluación de la satisfacción a los requerimientos del usuario es estándar y medible, y produce mediciones que la gerencia puede revisar y analizar de forma efectiva. La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, aún con niveles razonables de problemas posteriores a la implantación. La automatización del proceso es ad hoc y depende del proyecto. Es posible que la gerencia esté satisfecha con el nivel actual de eficiencia a pesar de la ausencia de una evaluación posterior a la implantación. El sistema de prueba refleja adecuadamente el ambiente de producción. La prueba de stress para los nuevos sistemas y la prueba de regresión para sistemas existentes se aplican para proyectos mayores.

5 Optimizado cuando
Los procesos de instalación y acreditación se han refinado a un nivel de buena práctica, con base en los resultados de mejora continua y refinamiento. Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente de entrenamiento, pruebas y transición a producción para los nuevos sistemas. Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción. La acreditación toma lugar regularmente sin repetición de trabajos, y los problemas posteriores a la implantación se limitan normalmente a correcciones menores. Las revisiones posteriores a la implantación son estándar, y las lecciones aprendidas se canalizan nuevamente hacia el proceso para asegurar el mejoramiento continuo de la calidad. Las pruebas de stress para los nuevos sistemas y las pruebas de regresión para sistemas modificados se aplican en forma consistente.

ENTREGAR Y DAR SOPORTE

DS1 Definir y administrar los niveles de servicio

DS2 Administrar los servicios de terceros

DS3 Administrar el desempeño y la capacidad

DS4 Garantizar la continuidad del servicio

DS5 Garantizar la seguridad de los sistemas

DS6 Identificar y asignar costos

DS7 Educar y entrenar a los usuarios

DS8 Administrar la mesa de servicio y los incidentes

DS9 Administrar la configuración

DS10 Administrar los problemas

DS11 Administrar los datos

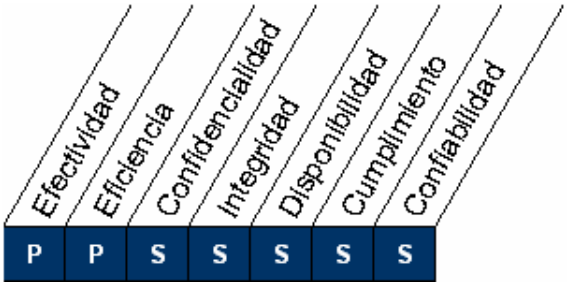
DS12 Administrar el ambiente físico

DS13 Administrar las operaciones

DESCRIPCIÓN DEL PROCESO.

DS1 Definir y Administrar los Niveles de Servicio

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.



Control sobre el proceso TI de

Definir y manejar niveles de servicio

Que satisface el requerimiento del negocio de TI para

Asegurar la alineación de los servicios claves de TI con la estrategia del negocio

Enfocándose en

La identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio

Se logra con

- La formalización de acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega
- La notificación del cumplimiento de los niveles de servicio (reportes y reuniones)
- La identificación y comunicación de requerimientos de servicios actualizados y nuevos para planeación estratégica

Y se mide con

- El porcentaje de Interesados satisfechos de que la entrega del servicio cumple con los niveles previamente acordados.
- El número de servicios entregados que no están en el catálogo
- El número de reuniones formales de revisión del Acuerdo de Niveles de Servicio (SLA) con las personas de negocio por año

OBJETIVOS DE CONTROL

DS1 Definir y Administrar los Niveles de Servicio

DS1.1 Marco de Trabajo de la Administración de los Niveles de Servicio
Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio (SLAs), acuerdos de niveles de operación (OLAs) y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes.

DS1.2 Definición de Servicios
Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

DS1.3 Acuerdos de Niveles de Servicio
Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

DS1.4 Acuerdos de Niveles de Operación
Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima. Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.

DS1.5 Monitoreo y Reporte del Cumplimento de los Niveles de Servicio
Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos
Revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

DIRECTRICES GERENCIALES

DS1 Definir y Administrar los Niveles de Servicio

Desde	Entradas
PO1	Planes de TI tácticos y estratégicos, portafolio de servicios de TI
PO2	Clasificaciones de datos asignadas
PO5	Portafolio de servicios de TI actualizado
AI2	Planes iniciales de SLAs
AI3	Planes iniciales de OLAs
DS4	Requerimientos de servicio en caso de desastre incluyendo roles y responsabilidades
ME1	Entrada de desempeño hacia la planeación de TI

Salidas	Hacia						
Reporte de revisión de contrato	DS2						
Reportes de desempeño de los procesos	ME1						
Requerimientos de servicio nuevos / actualizados	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Portafolio de servicios actualizado	PO1						

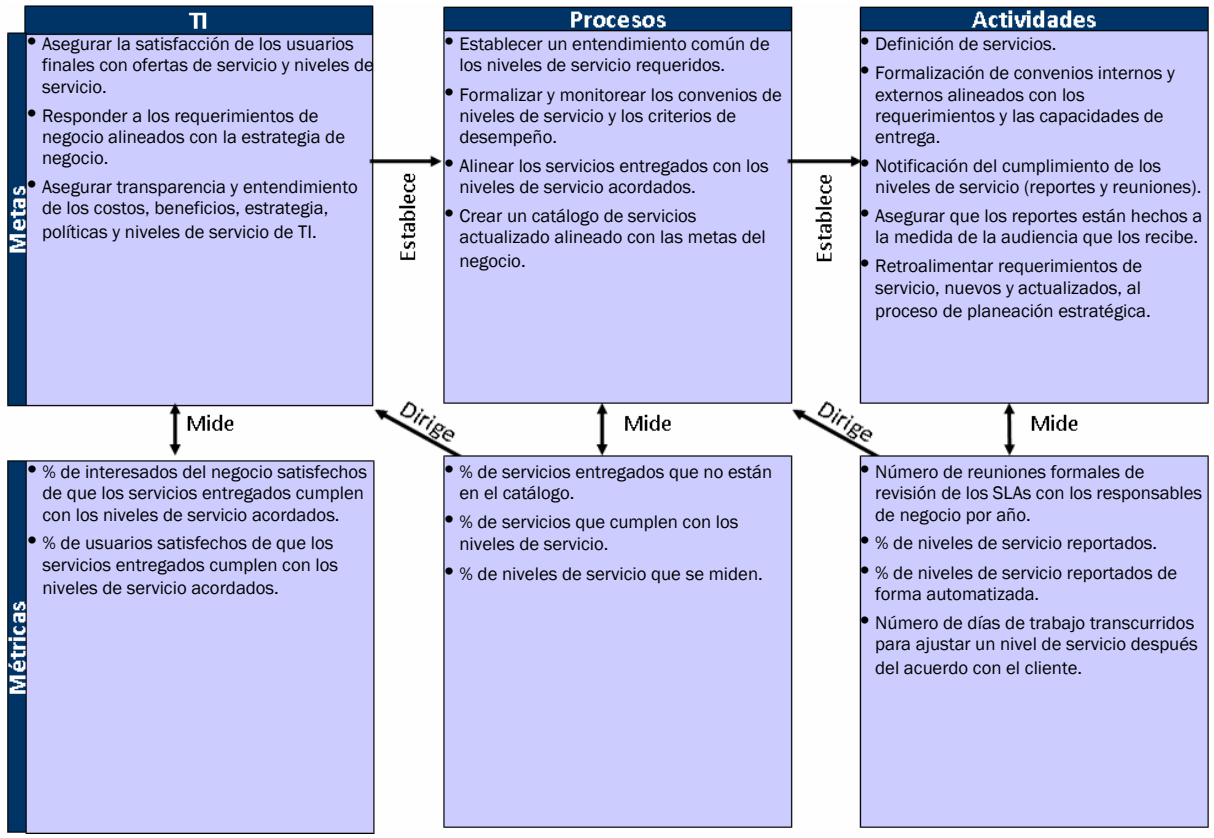
Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Administrador de servicio
Crear un marco de trabajo para los servicios de TI			C	A	C	C	I	C	C	I	C	R
Construir un catálogo de servicios de TI			I	A	C	C	I	C	C	I	I	R
Definir los convenios de niveles de servicio (SLAs) para los servicios críticos de TI		I	I	C	C	R	I	R	R	C	C	A/R
Definir los convenios de niveles de operación (OLAs) para soportar los SLAs				I	C	R	I	R	R	C	C	A/R
Monitorear y reportar el desempeño del servicio de punta a punta				I	I	R		I	I		I	A/R
Revisar los SLAs y los contratos de apoyo		I		I	C	R		R	R		C	A/R
Revisar y actualizar el catálogo de servicios de TI			I	A	C	C	I	C	C	I	I	R
Crear un plan de mejora de servicios			I	A	I	R	I	R	C	C	I	R

Funciones

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS1 Definir y Administrar los Niveles de Servicio

La administración del proceso de *Definir y administrar niveles de servicio* que satisfacen el requerimiento de negocio para TI de *asegurar la alineación de servicios claves de TI con la estrategia de negocio* es:

0 No Existente cuando
La gerencia no reconoce la necesidad de un proceso para definir los niveles de servicio. La responsabilidad y la rendición de cuentas sobre el monitoreo no está asignada.

1 Inicial / Ad Hoc cuando
Hay conciencia de la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas sobre para la definición y la administración de servicios no está definida. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa. La notificación es informal, infrecuente e inconsistente.

2 Repetible pero Intuitivo cuando
Los niveles de servicio están acordados pero son informales y no están revisados. Los reportes de los niveles de servicio están incompletos y pueden ser irrelevantes o engañosos para los clientes. Los reportes de los niveles de servicio dependen, en forma individual, de las habilidades y la iniciativa de los administradores. Está designado un coordinador de niveles de servicio con responsabilidades definidas, pero con autoridad limitada. Si existe un proceso para el cumplimiento de los acuerdos de niveles de servicio es voluntario y no está implementado.

3 Definido cuando
Las responsabilidades están bien definidas pero con autoridad discrecional. El proceso de desarrollo del acuerdo de niveles de servicio esta en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción de cliente. Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar. Las deficiencias en los niveles de servicio están identificadas pero los procedimientos para resolver las deficiencias son informales. Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado. Los niveles de servicio están acordados pero pueden no responder a las necesidades del negocio.

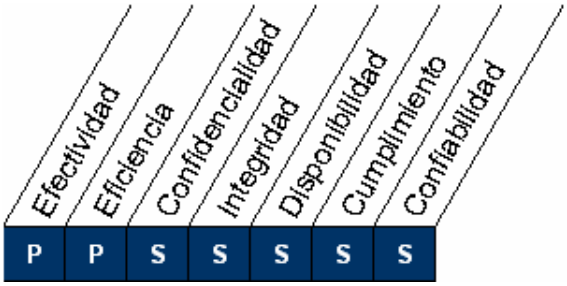
4 Administrado y Medible cuando
Aumenta la definición de los niveles de servicio en la fase de definición de requerimientos del sistema y se incorporan en el diseño de la aplicación y de los ambientes de operación. La satisfacción del cliente es medida y valorada de forma rutinaria. Las medidas de desempeño reflejan las necesidades del cliente, en lugar de las metas de TI. Las medidas para la valoración de los niveles de servicio se vuelven estandarizadas y reflejan los estándares de la industria. Los criterios para la definición de los niveles de servicio están basados en la criticidad del negocio e incluyen consideraciones de disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad. Cuando no se cumplen los niveles de servicio, se llevan a cabos análisis causa-raíz de manera rutinaria. El proceso de reporte para monitorear los niveles de servicio se vuelve cada vez más automatizado. Los riesgos operativos y financieros asociados con la falta de cumplimiento de los niveles de servicio, están definidos y se entienden claramente. Se implementa y mantiene un sistema formal de medición de los KPIs y los KGIs.

5 Optimizado cuando
Los niveles de servicio son continuamente reevaluados para asegurar la alineación de TI y los objetivos del negocio, mientras se toma ventaja de la tecnología incluyendo le relación costo-beneficio. Todos los procesos de administración de niveles de servicio están sujetos a mejora continua. Los niveles de satisfacción del cliente son administrados y monitoreados de manera continua. Los niveles de servicio esperados reflejan metas estratégicas de las unidades de negocio y son evaluadas contra las normas de la industria. La administración de TI tiene los recursos y la asignación de responsabilidades necesarias para cumplir con los objetivos de niveles de servicio y la compensación está estructurada para brindar incentivos por cumplir con dichos objetivos. La alta gerencia monitorea los KPIs y los KGIs como parte de un proceso de mejora continua.

DESCRIPCIÓN DEL PROCESO.

DS2 Administrar los Servicios de Terceros

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.



Control sobre el proceso TI de

Administrar servicios de terceros

Que satisface el requerimiento del negocio de TI para

Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos

Enfocándose en

El establecimiento de relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios

Se logra con

- La identificación y categorización de los servicios del proveedor
- La identificación y mitigación de riesgos del proveedor
- El monitoreo y la medición del desempeño del proveedor

Y se mide con

- El número de quejas de los usuarios debidas a los servicios contratados
- El porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio
- El porcentaje de los principales proveedores sujetos a monitoreo

OBJETIVOS DE CONTROL

DS2 Administrar los Servicios de Terceros

DS2.1 Identificación de Todas las Relaciones con Proveedores
Identificar todos los servicios de los proveedores, y categorizar los de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados, y credenciales de los representantes de estos proveedores.

DS2.2 Gestión de Relaciones con Proveedores
Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia. (Ej.: a través de SLAs).

DS2.3 Administración de Riesgos del Proveedor
Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de entrega de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legales y regulatorios de los estándares universales del negocio. 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 adhiere continuamente a los acuerdos del contrato y a SLAs, y que el desempeño es competitivo con proveedores alternativos y las condiciones del mercado.

DIRECTRICES GERENCIALES

DS2 Administrar los Servicios de Terceros

Desde	Entradas
PO1	Estrategia de contratación de TI
PO8	Estándares de adquisición
AI5	Arreglos contractuales, requerimientos de administración de relaciones con terceros
DS1	SLAs, reporte de revisión de contrato
DS4	Requerimientos de servicio contra desastre incluyendo roles y responsabilidades

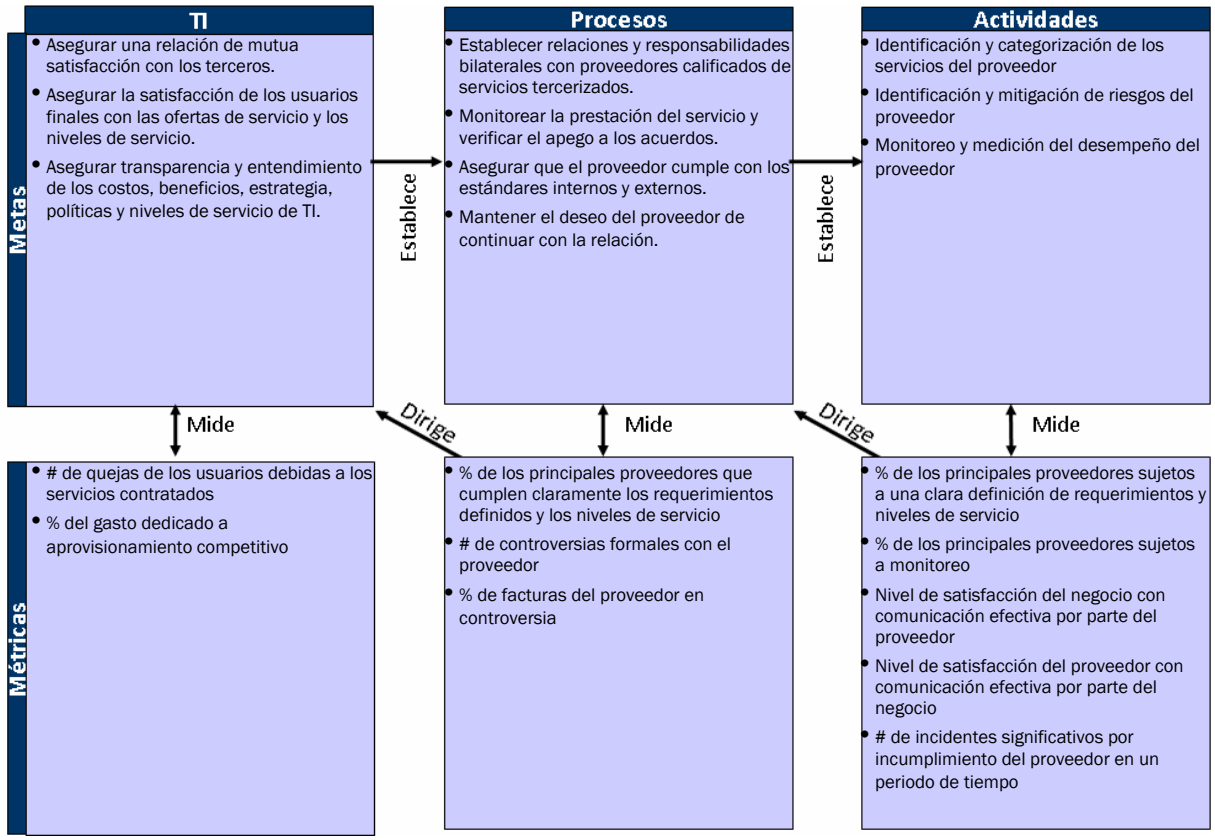
Salidas	Hacia
Reportes de desempeño de los procesos	ME1
Catálogo del proveedor	AI5
Riesgos del proveedor	PO9

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Identificar y categorizar las relaciones de los servicios de terceros				I	C	R	C	R	A/R	C	C
Definir y documentar los procesos de administración del proveedor		C		A	I	R	I	R	R	C	C
Establecer políticas y procedimientos de evaluación y suspensión de proveedores		C		A	C	C		C	R	C	C
Identificar, valorar y mitigar los riesgos del proveedor		I		A		R		R	R	C	C
Monitorear la prestación del servicio del proveedor				R	A	R		R	R	C	C
Evaluar las metas de largo plazo de la relación del servicio para todos los interesados	C	C	C	A/R	C	C	C	C	R	C	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS2 Administrar los Servicios de Terceros

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 Hoc cuando
La gerencia está conciente 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 Intuitivo 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 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, operativos 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 esta valorado y reportado.

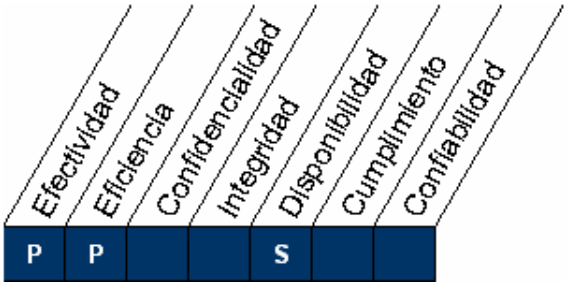
4 Administrado y Medible cuando
Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades 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 operativas, 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.

DESCRIPCIÓN DEL PROCESO.

DS3 Administrar el Desempeño y la Capacidad

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.



Control sobre el proceso TI de

Administrar el desempeño y la capacidad

Que satisface el requerimiento del negocio de TI para

Optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades del negocio

Enfocándose en

Cumplir con los requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición.

Se logra con

- La planeación y la entrega de capacidad y disponibilidad del sistema
- Monitoreando y reportando el desempeño del sistema
- Modelando y pronosticando el desempeño del sistema.

Y se mide con

- Número de horas perdidas por usuario por mes, debidas a la falta de planeación de la capacidad
- Porcentaje de picos donde se excede la meta de utilización
- Porcentaje de SLAs de tiempo de respuesta que no se satisfacen

OBJETIVOS DE CONTROL

DS3 Administrar el Desempeño y la Capacidad

DS3.1 Planeación del Desempeño y la Capacidad
Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelo apropiadas para producir un modelo de desempeño, de capacidad y de desempeño de los recursos de TI, tanto actual como pronosticado.

DS3.2 Capacidad y Desempeño Actual
Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.

DS3.3 Capacidad y Desempeño Futuros
Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

DS3.4 Disponibilidad de Recursos de TI
Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.

DS3.5 Monitoreo y Reporte
Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:
- Mantener y poner a punto el desempeño actual dentro de TI y atender temas como elasticidad, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
- Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs.

Acompañar todos los reportes de excepción con recomendaciones para acciones correctivas

DIRECTRICES GERENCIALES

DS3 Administrar el Desempeño y la Capacidad

Desde	Entradas
AI2	Especificaciones de disponibilidad, continuidad y de recuperación
AI3	Requerimientos de monitoreo del sistema
DS1	SLAs

Salidas	Hacia						
Información sobre desempeño y capacidad	PO2	PO3					
Plan de desempeño y capacidad (requerimientos)	PO5	AI1	AI3	ME1			
Cambios requeridos	AI6						
Reportes de desempeño del proceso	ME1						

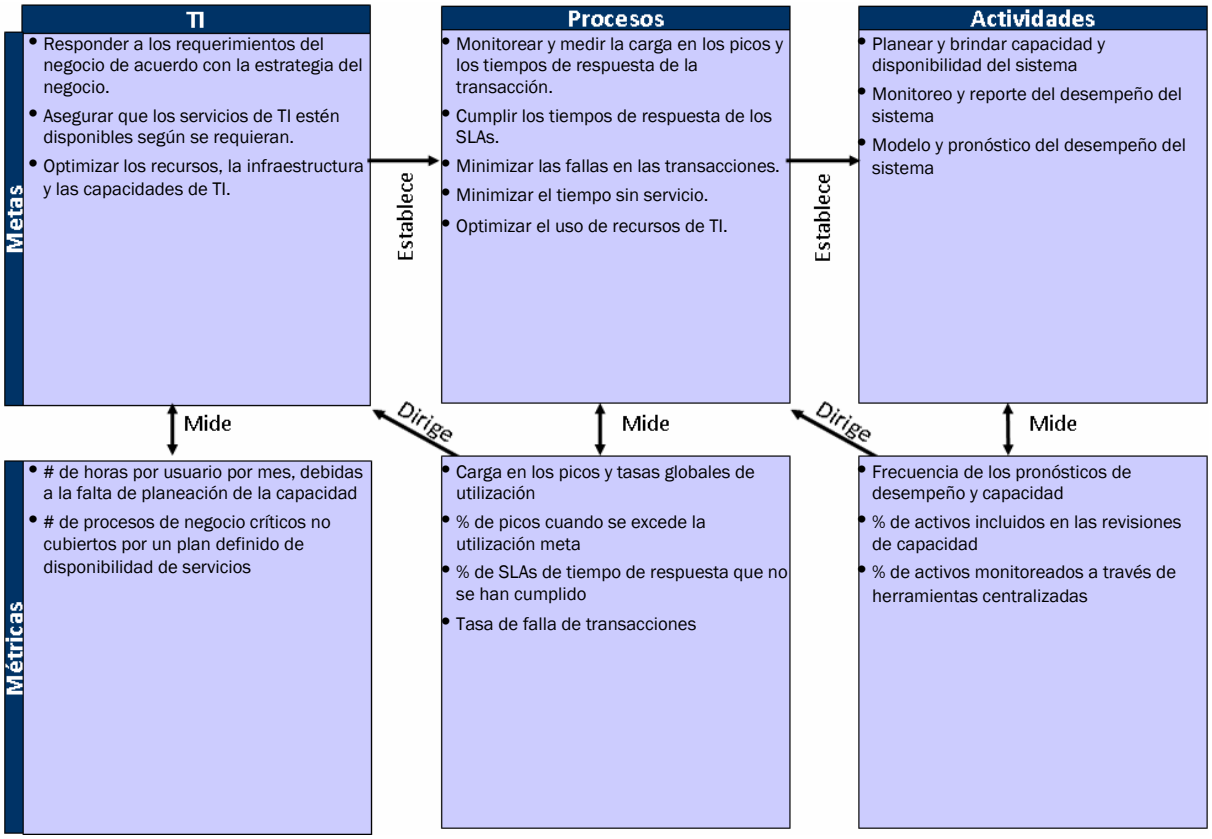
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Establecer un proceso de Planeación para la revisión del desempeño y la capacidad de los recursos de TI				A		R	C	C	C	C	
Revisar el desempeño y la capacidad actual de los recursos de TI				C	I	A/R		C	C	C	
Realizar pronósticos de desempeño y capacidad de los recursos de TI				C	C	A/R	C	C	C	C	
Realizar análisis de brecha para identificar incompatibilidad de los recursos de TI				C	I	A/R		R	C	C	I
Realizar un plan de contingencia respecto a una falta potencial de disponibilidad de recursos de TI				C	I	A/R		C	C	I	C
Monitorear y reportar continuamente la disponibilidad, el desempeño y la capacidad de				I	I	A/R		I	I	I	I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS3 Administrar el Desempeño y la Capacidad

La administración del proceso de *Administrar el desempeño y la capacidad* que satisfaga el requerimiento de *optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI, en respuesta a las necesidades de negocio* es:

0 No Existente cuando
La gerencia no reconoce que los procesos clave del negocio pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.

1 Inicial / Ad Hoc cuando
Los usuarios, con frecuencia, tienen que llevar acabo soluciones alternas para resolver las limitaciones de desempeño y capacidad. Los responsables de los procesos del negocio valoran poco la necesidad de llevar a cabo una planeación de la capacidad y del desempeño. Las acciones para administrar el desempeño y la capacidad son típicamente reactivas. El proceso de planeación de la capacidad y el desempeño es informal. El entendimiento sobre la capacidad y el desempeño de TI, actual y futuro, es limitado

2 Repetible pero Intuitivo cuando
Los responsables del negocio y la gerencia de TI están concientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.

3 Definido cuando
Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.

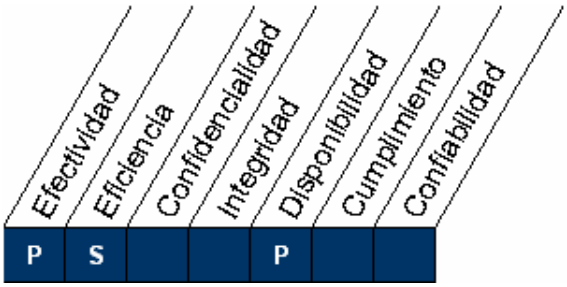
4 Administrado y Medible cuando
Hay procesos y herramientas disponibles para medir el uso del sistema, el desempeño y la capacidad, y los resultados se comparan con metas definidas. Hay información actualizada disponible, brindando estadísticas de desempeño estandarizadas y alertando sobre incidentes causados por falta de desempeño o de capacidad. Los problemas de falta de desempeño y de capacidad se enfrentan de acuerdo con procedimientos definidos y estandarizados. Se utilizan herramientas automatizadas para monitorear recursos específicos tales como espacios en disco, redes, servidores y compuertas de red. Las estadísticas de desempeño y capacidad son reportadas en términos de los procesos de negocio, de forma que los usuarios y los clientes comprendan los niveles de servicio de TI. Los usuarios se sienten por lo general satisfechos con la capacidad del servicio actual y pueden solicitar nuevos y mejores niveles de disponibilidad. Se han acordado los KGIs y KPIs para medir el desempeño y la capacidad de TI, pero puede ser que se aplican de forma esporádica e inconsistente.

5 Optimizado cuando
Los planes de desempeño y capacidad están completamente sincronizados con las proyecciones de demanda del negocio. La infraestructura de TI y la demanda del negocio están sujetas a revisiones regulares para asegurar que se logre una capacidad óptima con el menor costo posible. Las herramientas para monitorear recursos críticos de TI han sido estandarizadas y usadas a través de diferentes plataformas y vinculadas a un sistema de administración de incidentes a lo largo de toda la organización. Las herramientas de monitoreo detectan y pueden corregir automáticamente problemas relacionados con la capacidad y el desempeño. Se llevan a cabo análisis de tendencias, los cuales muestran problemas de desempeño inminentes causados por incrementos en los volúmenes de negocio, lo que permite planear y evitar problemas inesperados. Las métricas para medir el desempeño y la capacidad de TI han sido bien afinadas dentro de los KGIs y KPIs para todos los procesos de negocio críticos y se miden de forma regular. La gerencia ajusta la planeación del desempeño y la capacidad siguiendo los análisis de los KGIs y KPIs.

DESCRIPCIÓN DEL PROCESO.

DS4 Garantizar la Continuidad del Servicio

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.



Control sobre el proceso TI de

Garantizar la continuidad del servicio

Que satisface el requerimiento del negocio de TI para

Asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI

Enfocándose en

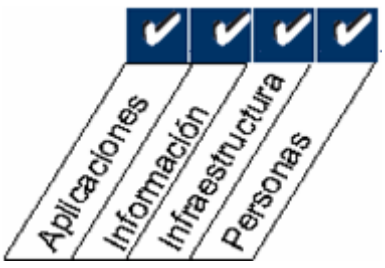
El desarrollo de resistencia (resilience) en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI

Se logra con

- Desarrollando y manteniendo (mejorando) los planes de contingencia de TI
- Con entrenamiento y pruebas de los planes de contingencia de TI
- Guardando copias de los planes de contingencia y de los datos fuera de las instalaciones

Y se mide con

- Número de horas perdidas por usuario por mes, debidas a interrupciones no planeadas
- Número de procesos críticos de negocio que dependen de TI, que no están cubiertos por un plan de continuidad



OBJETIVOS DE CONTROL

DS4 Garantizar la Continuidad del Servicio

DS4.1 Marco de Trabajo de Continuidad de TI
Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

DS4.2 Planes de Continuidad de TI
Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

DS4.3 Recursos Críticos de TI
Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS4.4 Mantenimiento del Plan de Continuidad de TI
Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

DS4.5 Pruebas del Plan de Continuidad de TI
Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

DS4.6 Entrenamiento del Plan de Continuidad de TI
Asegurarse de que todos las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

DS4.7 Distribución del Plan de Continuidad de TI
Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

DS4.8 Recuperación y Reanudación de los Servicios de TI
Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

DS4.10 Revisión Post Reanudación
Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

DIRECTRICES GERENCIALES

DS4 Garantizar la Continuidad del Servicio

Desde	Entradas
PO2	Clasificaciones de datos asignados
PO9	Valoración de riesgo
AI2	Especificación de disponibilidad, continuidad y recuperación
AI4	Manuales, de usuario, técnicos, operativos, de soporte y de administración
DS1	SLAs y OLAs

Salidas	Hacia						
Resultados de las prueba de contingencia	PO9						
Criticidad de puntos de configuración de TI	DS9						
Plan de almacenamiento de respaldos y de protección	DS11	DS13					
Umbrales de incidente/desastre	DS8						
Requerimientos de servicios contra desastres incluyendo roles y responsabilidades	DS1	DS2					
Reportes de desempeño de los procesos	ME1						

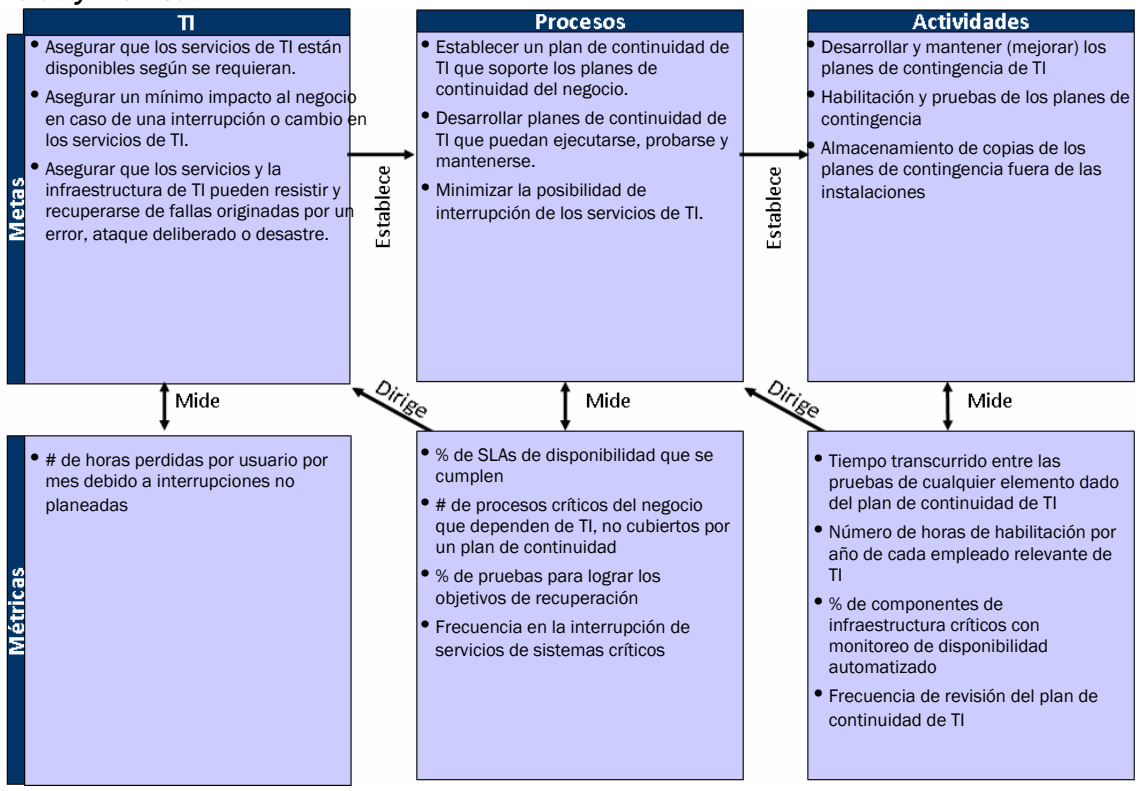
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Desarrollar un marco de trabajo de continuidad de TI		C	C	A	C	R	R	R	C	C	R
Realizar un análisis de impacto al negocio y valoración de riesgo		C	C	C	C	A/R	C	C	C	C	C
Desarrollar y mantener planes de continuidad de TI	I	C	C	C	I	A/R		C	C	C	C
Identificar y categorizar los recursos de TI con base en los objetivos de recuperación				C		A/R		C	I	C	I
Definir y ejecutar procedimientos de control de cambios para asegurar que el plan de continuidad sea vigente				I		A/R		R	R	R	I
Probar regularmente el plan de continuidad de TI				I	I	A/R		C	C	I	I
Desarrollar un plan de acción a seguir con base en los resultados de las pruebas				C	I	A/R	C	R	R	R	I
Planear y llevar a cabo capacitación sobre los planes de continuidad de TI				I	R	A/R		C	R	I	I
Planear la recuperación y reanudación de los servicios de TI		I	I	C	C	A/R	C	R	R	R	C
Planear e implementar el almacenamiento y la protección de respaldos				I		A/R		C	C	I	I
Establecer los procedimientos para llevar a cabo revisiones post reanudación				C	I	A/R		C	C		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS4 Garantizar la Continuidad del Servicio

La administración del proceso de *Garantizar la continuidad del servicio* que satisfaga el requerimiento de TI del negocio para *asegurar el mínimo impacto al negocio en caso de interrupción de un servicio de TI* es:

0 No Existente cuando
No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.

1 Inicial / Ad Hoc cuando
Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio

2 Repetible pero Intuitivo cuando
Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.

3 Definido cuando
La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir habilitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.

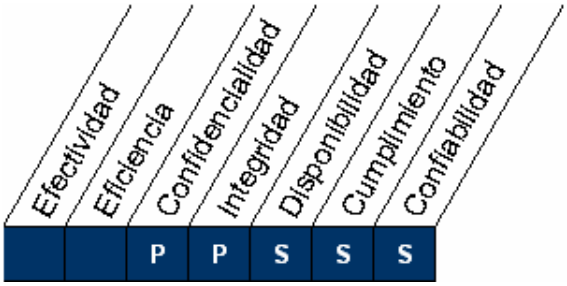
4 Administrado y Medible cuando
Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda habilitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.

5 Optimizado cuando
Los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de disponibilidad y la continua planeación de la continuidad están totalmente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirá como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática. La gerencia ajusta la planeación de continuidad como respuesta a los KGIs y KPIs

DESCRIPCIÓN DEL PROCESO.

DS5 Garantizar la Seguridad de los Sistemas

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 realizar monitoreos de 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.



Control sobre el proceso TI de

Garantizar la seguridad de los sistemas

Que satisface el requerimiento del negocio de TI para

Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad

Enfocándose en

La definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad

Se logra con

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.
- Probando la seguridad de forma regular

Y se mide con

- El número de incidentes que dañan la reputación con el público
- El número de sistemas donde no se cumplen los requerimientos de seguridad
- El número de de violaciones en la segregación de tareas

OBJETIVOS DE CONTROL

DS5 Garantizar la Seguridad de los Sistemas

DS5.1 Administración de la Seguridad de TI
Administrar la seguridad de TI al nivel más alto 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 negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

DS5.3 Administración de Identidad
Asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan 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 despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados 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 un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión 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.

DS5.6 Definición de Incidente de Seguridad
Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.

DS5.7 Protección de la Tecnología de Seguridad
Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.

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
Poner medidas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).

DS5.10 Seguridad de la Red
Uso de 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
Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

DIRECTRICES GERENCIALES

DS5 Garantizar la Seguridad de los Sistemas

Desde	Entradas
PO2	Arquitectura de Información; clasificación de datos asignados
PO3	Estándares de tecnología
PO9	Evaluación de riesgo
AI2	Especificaciones de controles de seguridad en las aplicaciones
DS1	OLAs

Salidas	Hacia
Definición de incidentes de seguridad	DS8
Requerimientos específicos de entrenamiento sobre conciencia de seguridad	DS7
Reportes de desempeño del proceso	ME1
Cambios de seguridad requeridos	AI6
Amenazas y vulnerabilidades de seguridad	PO9
Politicas y Planes de Seguridad de TI	DS11

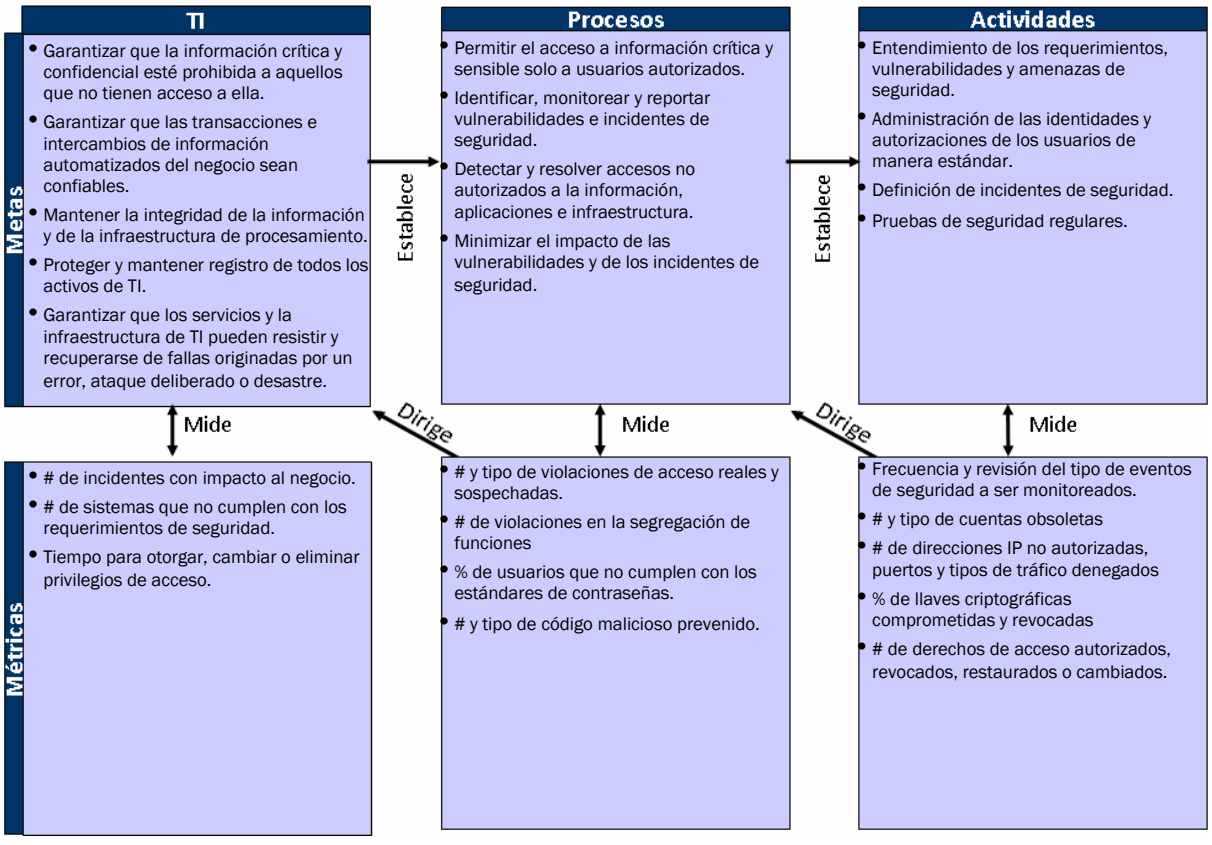
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir y mantener un plan de seguridad de TI	I	C	C	A	C	C	C	C	I	I	R
Definir, establecer y operar un proceso de administración de identidad (cuentas)			I	A	C	R	R	I			C
Monitorear incidentes de seguridad, reales y potenciales				A	I	R	C	C			R
Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios				I	A	C					R
Establecer y mantener procedimientos para mantener y salvaguardar las llaves criptográficas				A		R			I		C
Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red				A	C	C	R	R			C
Realizar evaluaciones de vulnerabilidad de manera regular		I		A	I	C	C	C			R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS5 Garantizar la Seguridad de los Sistemas

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 habilitación 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 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 habilitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

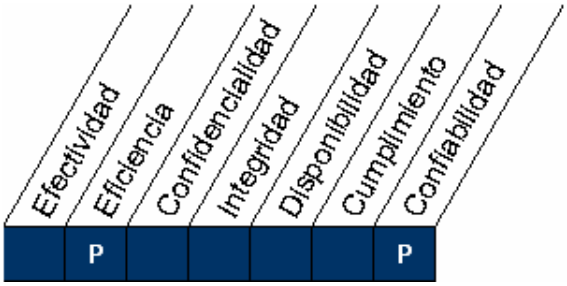
4 Administrado y Medible cuando
Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad 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 habilitación sobre seguridad se imparte tanto para TI como para el negocio. La habilitación 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 acabo 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

DESCRIPCIÓN DEL PROCESO.

DS6 Identificar y Asignar Costos

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 un 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.



Control sobre el proceso TI de

Identificar y asignar costos

Que satisface el requerimiento del negocio de TI para

Transparentar y entender los costos de TI y mejorar la rentabilidad a través del uso bien informado de los servicios de TI

Enfocándose en

el registro completo y preciso de los costos de TI, un sistema equitativo para asignación acordado con los usuarios de negocio, y un sistema para reportar oportunamente el uso de TI y los costos asignados

Se logra con

- La alineación de cargos con la calidad y cantidad de los servicios brindados
- La construcción y aceptación de un modelo de costos completo
- La aplicación de cargos con base en la política acordada

Y se mide con

- Porcentaje de facturas de servicios de TI aceptadas/pagadas por la gerencia del negocio.
- Porcentaje de variación entre los presupuestos, pronósticos y costos actuales.
- Porcentaje de costos totales de TI que son distribuidos de acuerdo con los modelos acordados

OBJETIVOS DE CONTROL

DS6 Identificar y Asignar Costos

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 alinearse 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.

DIRECTRICES GERENCIALES

DS6 Identificar y Asignar Costos

Desde	Entradas
PO4	Dueños de sistemas documentados
PO5	Reportes costo/beneficio, presupuestos de TI
PO10	Planes de proyecto detallados
DS1	SLAs y OLAs

Salidas	Hacia
Finanzas de TI	PO5
Reportes de desempeño de procesos	ME1

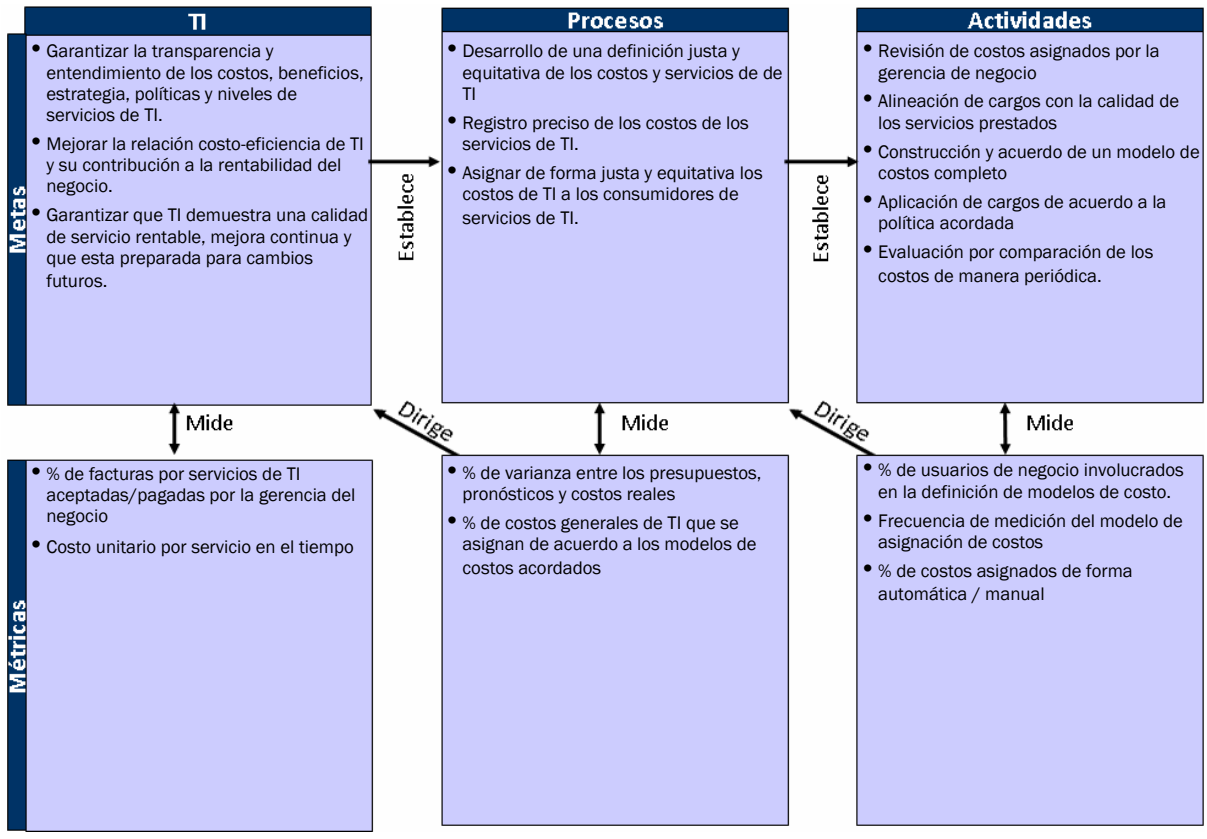
Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Mapear la infraestructura con los servicios brindados / procesos de negocio soportados		C	C	A	C	C	C	C	R	C	
Identificar todos los costos de TI (personas, tecnología, etc) y mapearlos a los servicios de TI con base en costos unitarios		C		A		C	C	C	R	C	
Establecer y mantener un proceso de control de contabilización de TI y de costos		C	C	A	C	C	C	C	R	C	
Establecer y mantener procedimientos y políticas de facturación		C	C	A	C	C	C	C	R	C	

Funciones

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS6 Identificar y Asignar Costos

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 esta 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 habilitación 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 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.

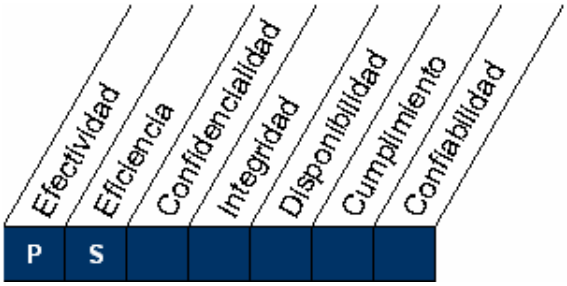
4 Administrado y Medible cuando
Las responsabilidades sobre la administración de costos de los servicios de información están bien definidas y bien entendidas a todos los niveles, y son soportadas con habilitación formal. Los costos directos e indirectos están identificados y se reportan de forma oportuna y automatizada a la gerencia, a los dueños 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 esta ligado a los objetivos del negocio y los acuerdos de niveles de servicio, y son vigilados por los dueños 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.

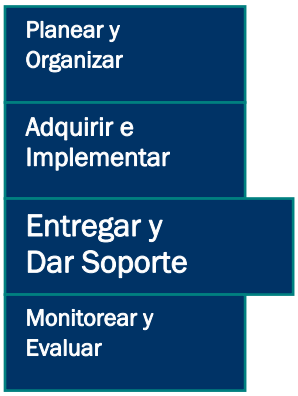
5 Optimizado cuando
Los costos de los servicios prestados se identifican, registran, resumen y reportan a la gerencia, a los dueños de los procesos de negocio y a los usuarios. Los costos se identifican como productos cobrables y pueden soportar un sistema de cobro que cargue a los usuarios por los servicios 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

DESCRIPCIÓN DEL PROCESO.

DS7 Educar y Entrenar a los Usuarios

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.





Control sobre el proceso TI de

Educar y entrenar a los usuarios

Que satisface el requerimiento del negocio de TI para

El uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos

Enfocándose en

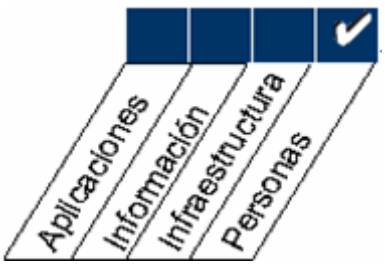
Un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados

Se logra con

- Establecer un programa de entrenamiento
- Organizar el entrenamiento
- Impartir el entrenamiento
- Monitorear y reportar la efectividad del entrenamiento

Y se mide con

- Número de llamadas de soporte debido a problemas de entrenamiento
- Porcentaje de satisfacción de los Interesados con el entrenamiento recibido
- Lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo



OBJETIVOS DE CONTROL

DS7 Educar y Entrenar a los Usuarios

DS7.1 Identificación de Necesidades de Entrenamiento y Educación

Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya:

- Estrategias y requerimientos actuales y futuros del negocio.
- Valores corporativos (valores éticos, cultura de control y seguridad, etc.)
- Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)
- Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias.
- Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo.

DS7.2 Impartición de Entrenamiento y Educación

Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

DS7.3 Evaluación del Entrenamiento Recibido

Al finalizar el entrenamiento, evaluar el contenido del entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

DIRECTRICES GERENCIALES

DS7 Educar y Entrenar a los Usuarios

Desde	Entradas
PO7	Habilidades y competencias de los usuarios, incluyendo el entrenamiento individual y los requerimientos específicos de entrenamiento.
AI4	Materiales de entrenamiento; requerimientos de transferencia del conocimiento para implementación de soluciones
DS1	SLAs
DS5	Requerimientos específicos de entrenamiento sobre conocimientos de seguridad
DS8	Reportes de satisfacción de usuario

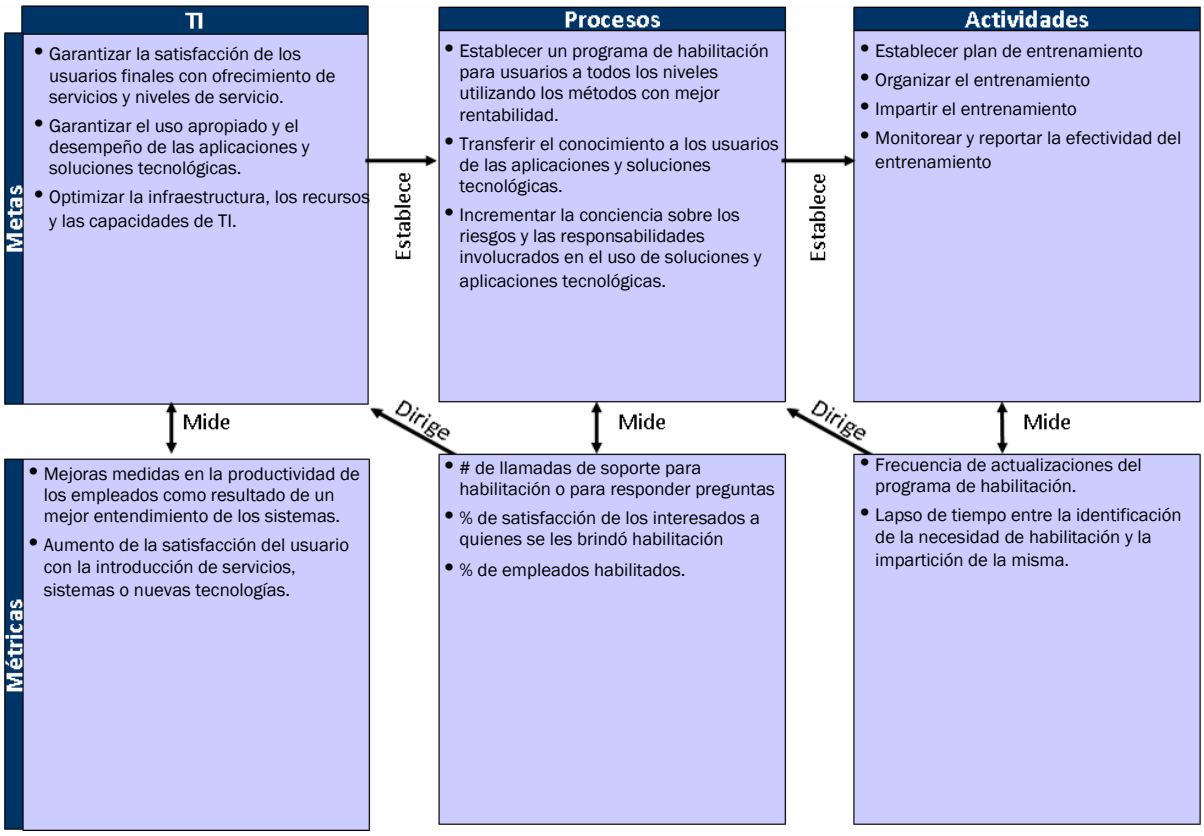
Salidas	Hacia
Reportes de desempeño de procesos	ME1
Actualizaciones de documentación requeridas	AI4

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Departamento de Capacitación
Identificar y categorizar las necesidades de capacitación de los usuarios			C	A	R	C	C	C	C	C	C	R
Construir un programa de capacitación			C	A	R	C	I	C	C	C	I	R
Realizar actividades de capacitación, intrusión y concienciación			I	A	C	C	I	C	C	C	I	R
Llevar a cabo evaluaciones de la capacitación			I	A	R	C	I	C	C	C	I	R
Identificar y evaluar los mejores métodos y herramientas para impartir la capacitación			I	A/R	R	C	C	C	C	C	C	R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS7 Educar y Entrenar a los Usuarios

La administración del proceso de *Educar y entrenar a los usuarios* que satisfagan los requerimientos del negocio de TI de *tener un uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y lograr que los usuarios cumplan con las políticas y los procedimientos* es:

0 No Existente cuando
Hay una total falta de programas de entrenamiento y educación. La organización no reconoce que hay un problema a ser atendido respecto al entrenamiento y no hay comunicación sobre el problema.

1 Inicial / Ad Hoc cuando
Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre la seguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación

2 Repetible pero Intuitivo cuando
Hay conciencia sobre la necesidad de un programa de entrenamiento y educación, y sobre los procesos asociados a lo largo de toda la organización. El entrenamiento está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se han desarrollado hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores, cubriendo los mismos temas de materias con diferentes puntos de vista. Algunas de las clases abordan los temas de conducta ética y de conciencia sobre prácticas y actividades de seguridad en los sistemas. Hay una gran dependencia del conocimiento de los individuos. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.

3 Definido cuando
El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento y educación son monitoreados, pero no todas las desviaciones son susceptibles de detección por parte de la gerencia. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.

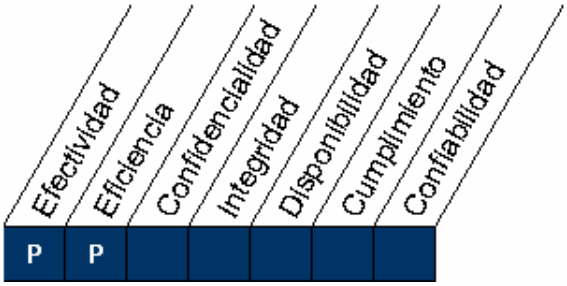
4 Administrado y Medible cuando
Hay un programa completo de entrenamiento y educación que produce resultados medibles. Las responsabilidades son claras y se establece la propiedad sobre los procesos. El entrenamiento y la educación son componentes de los planes de carrera de los empleados. La gerencia apoya y asiste a sesiones de entrenamiento y de educación. Todos los empleados reciben entrenamiento sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. Todos los empleados reciben el nivel apropiado de entrenamiento sobre prácticas de seguridad en los sistemas para proteger contra daños originados por fallas que afecten la disponibilidad, la confidencialidad y la integridad. La gerencia monitorea el cumplimiento por medio de revisión constante y actualización del programa y de los procesos de entrenamiento. Los procesos están en vía de mejora y fomentan las mejores prácticas internas.

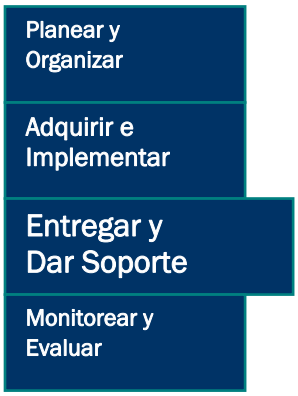
5 Optimizado cuando
El entrenamiento y la educación dan como resultado la mejora del desempeño individual. El entrenamiento y la educación son componentes críticos de los planes de carrera de los empelados. Se asignan suficientes presupuestos, recursos, instalaciones e instructores para los programas de entrenamiento y educación. Los procesos se afinan y están en continua mejora, tomando ventaja de las mejores prácticas externas y de modelos de madurez de otras organizaciones. Todos los problemas y desviaciones se analizan para identificar las causas de raíz, se identifican y llevan a cabo acciones de forma expedita. Hay una actitud positiva con respecto a la conducta ética y respecto a los principios de seguridad en los sistemas. TI se utiliza de manera amplia, integral y óptima para automatizar y brindar herramientas para los programas de entrenamiento y educación. Se utilizan expertos externos en entrenamiento y se utilizan benchmarks del mercado como orientación.

DESCRIPCIÓN DEL PROCESO.

DS8 Administrar la Mesa de Servicio y los Incidentes.

Responder de manera oportuna y efectiva a las consultas y problemas de los usuarios de TI, requiere de una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raiz y resolución. Los beneficios del negocio incluyen el incremento en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.





Control sobre el proceso TI de

Administrar la mesa de servicio y los incidentes

Que satisface el requerimiento del negocio de TI para

Permitir el efectivo uso de los sistemas de TI garantizando la resolución y el análisis de las consultas de los usuarios finales, incidentes y preguntas

Enfocándose en

Una función profesional de mesa de servicio, con tiempo de respuesta rápido, procedimientos de escalamiento claros y análisis de tendencias y de resolución

Se logra con

- Instalación y operación de un servicio de una mesa de servicios
- Monitoreo y reporte de tendencias
- Definición de procedimientos y de criterios de escalamiento claros

Y se mide con

- Satisfacción del usuario con el soporte de primera línea
- Porcentaje de incidentes resueltos dentro de un lapso de tiempo aceptable / acordado.
- Índice de abandono de llamadas

OBJETIVOS DE CONTROL

DS8 Administrar la Mesa de Servicio y los Incidentes.

DS8.1 Mesa de Servicios
Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI

DS8.2 Registro de Consultas de Clientes
Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Debe trabajar estrechamente con los procesos de administración de incidentes, administración de problemas, administración de cambios, administración de capacidad y administración de disponibilidad. Los incidentes deben clasificarse de acuerdo al negocio y a la prioridad del servicio y enrutarse al equipo de administración de problemas apropiado y se debe mantener informados a los clientes sobre el estatus de sus consultas.

DS8.3 Escalamiento de Incidentes
Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas. Garantizar que la asignación de incidentes y el monitoreo del ciclo de vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.

DS8.4 Cierre de Incidentes
Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes. Cuando se resuelve el incidente la mesa de servicios debe registrar la causa raíz, si la conoce, y confirmar que la acción tomada fue acordada con el cliente.

DS8.5 Análisis de Tendencias
Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

DIRECTRICES GERENCIALES

DS8 Administrar la Mesa de Servicio y los Incidentes.

Desde	Entradas
AI4	Manuales de usuario, de operación, técnicos y de administración
AI6	Autorización de cambios
AI7	Puntos de configuración liberados
DS1	SLAs y OLAS
DS4	Umbrales de incidente/ desastre
DS5	Definición de incidente de seguridad
DS9	Detalles de configuración/activos de TI
DS10	Problemas conocidos, errores conocidos y soluciones alternas
DS13	Tiquetes de incidente

Salidas	Hacia
Solicitud de servicio / solicitud de cambio	AI6
Reportes de incidentes	DS10
Reportes de desempeño de procesos	ME1
Reportes de satisfacción de usuarios	DS7, ME1

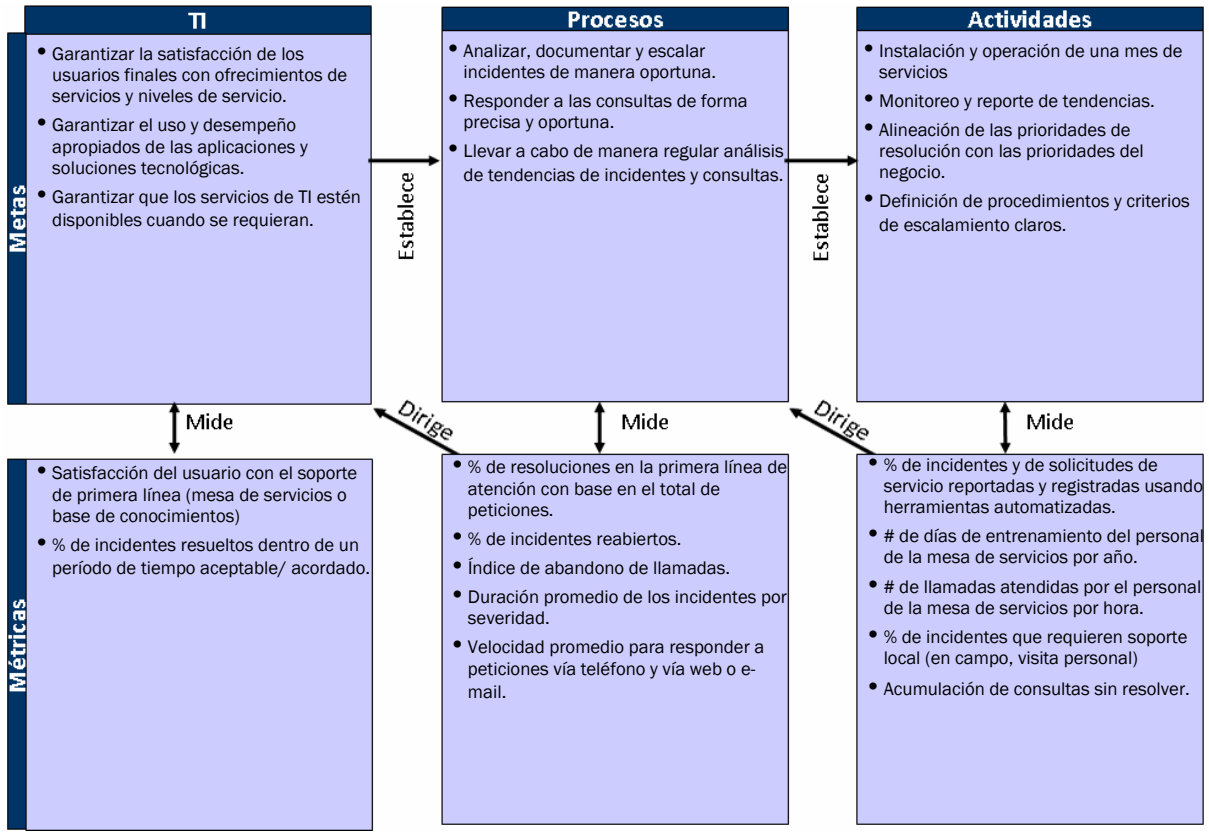
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Mesa de servicios a usuarios / Gerentes de Incidentes
Crear procedimientos de clasificación (severidad e impacto) y de escalamiento (funcional y jerárquicos)				C	C	C	C	C	C		C	A/R
Detectar y registrar incidentes / solicitudes de servicio / solicitudes de información												A/R
Clasificar, investigar y diagnosticar consultas				I		C	C	C			I	A/R
Resolver, recuperar y cerrar incidentes					I	R	R	R			C	A/R
Informar a usuarios (por ejemplo, actualizaciones de estatus)				I	I							A/R
Hacer reportes para la gerencia	I			I	I	I			I		I	A/R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS8 Administrar la Mesa de Servicio y los Incidentes.

La administración del proceso de *Administrar la mesa de servicio y los incidentes* que satisfaga el requerimiento del negocio de TI de *permitir el uso efectivo de sistemas de TI garantizando el análisis y la resolución de las consultas, preguntas e incidentes del usuario final* es:

0 No Existente cuando
No hay soporte para resolver problemas y preguntas de los usuarios. Hay una completa falta de procesos para la administración de incidentes. La organización no reconoce que hay un problema que atender.

1 Inicial / Ad Hoc cuando
La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan

2 Repetible pero Intuitivo cuando
Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo.

3 Definido cuando
Se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes. Los procedimientos se estandarizan y documentan, pero se lleva acabo entrenamiento informal. Se deja la responsabilidad al individuo de conseguir entrenamiento y de seguir los estándares. Se desarrollan guías de usuario y preguntas frecuentes (FAQs), pero los individuos deben encontrarlas y puede ser que no las sigan. Las consultas y los incidentes se rastrean de forma manual y se monitorean de forma individual, pero no existe un sistema formal de reporte. No se mide la respuesta oportuna a las consultas e incidentes y los incidentes pueden quedar sin resolución. Los usuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes.

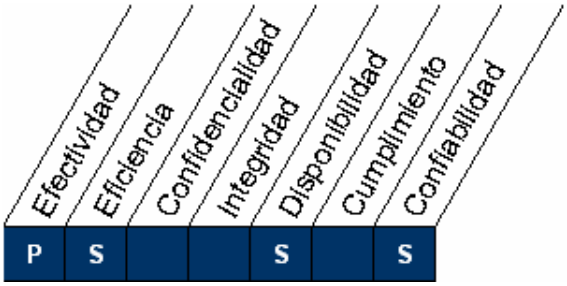
4 Administrado y Medible cuando
En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está habilitado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.

5 Optimizado cuando
El proceso de administración de incidentes y la función de mesa de servicio están bien organizados y establecidos y se llevan a cabo con un enfoque de servicio al cliente ya que son expertos, enfocados al cliente y útiles. Los KPIs y KGIs son medidos y reportados sistemáticamente. Una amplia y extensa cantidad de preguntas frecuentes son parte integral de la base de conocimientos. Existen a disposición del usuario, herramientas para llevar a cabo autodiagnósticos y para resolver incidentes. La asesoría es consistente y los incidentes se resuelven de forma rápida dentro de un proceso estructurado de escalamiento. La gerencia utiliza una herramienta integrada para obtener estadísticas de desempeño del proceso de administración de incidentes y de la función de mesa de servicio. Los procesos han sido afinados al nivel de las mejores prácticas de la industria, con base en los resultados del análisis de los KPIs y KGIs, de la mejora continua y de benchmarking con otras organizaciones.

DESCRIPCIÓN DEL PROCESO.

DS9 Administrar la Configuración

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.



Control sobre el proceso TI de

Administrar la configuración

Que satisface el requerimiento del negocio de TI para

Optimizar la infraestructura, recursos y capacidades de TI, y llevar registro de los activos de TI.

Enfocándose en

Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual

Se logra con

- El establecimiento de un repositorio central de todos los elementos de la configuración
- La identificación de los elementos de configuración y su mantenimiento
- Revisión de la integridad de los datos de configuración

Y se mide con

- El número de problemas de cumplimiento del negocio debido a inadecuada configuración de los activos.
- El número de desviaciones identificadas entre el repositorio de configuración y la configuración actual de los activos.
- Porcentaje de licencias compradas y no registradas en el repositorio

OBJETIVOS DE CONTROL

DS9 Administrar la Configuración

DS9.1 Repositorio y Línea Base de Configuración
Establecer una herramienta de soporte y un repositorio central que contenga toda la información relevante sobre los elementos de configuración. Monitorear y grabar todos los activos y los cambios a los activos. Mantener una línea base de los elementos de la configuración para todos los sistemas y servicios como punto de comprobación al que volver tras el cambio.

DS9.2 Identificación y Mantenimiento de Elementos de Configuración
Establecer procedimientos de configuración para soportar la gestión y rastro de todos los cambios al repositorio de configuración. Integrar estos procedimientos con la gestión de cambios, gestión de incidentes y procedimientos de gestión de problemas.

DS9.3 Revisión de Integridad de la Configuración
Revisar periódicamente los datos de configuración para verificar y confirmar la integridad de la configuración actual e histórica. Revisar periódicamente el software instalado contra la política de uso de software para identificar software personal o no licenciado o cualquier otra instancia de software en exceso del contrato de licenciamiento actual. Reportar, actuar y corregir errores y desviaciones.

DIRECTRICES GERENCIALES

DS9 Administrar la Configuración

Desde	Entradas
AI4	Manuales, de usuario, técnicos, de soporte y de administración
AI7	Elementos de configuración liberados
DS4	Criticidad de los elementos de configuración de TI

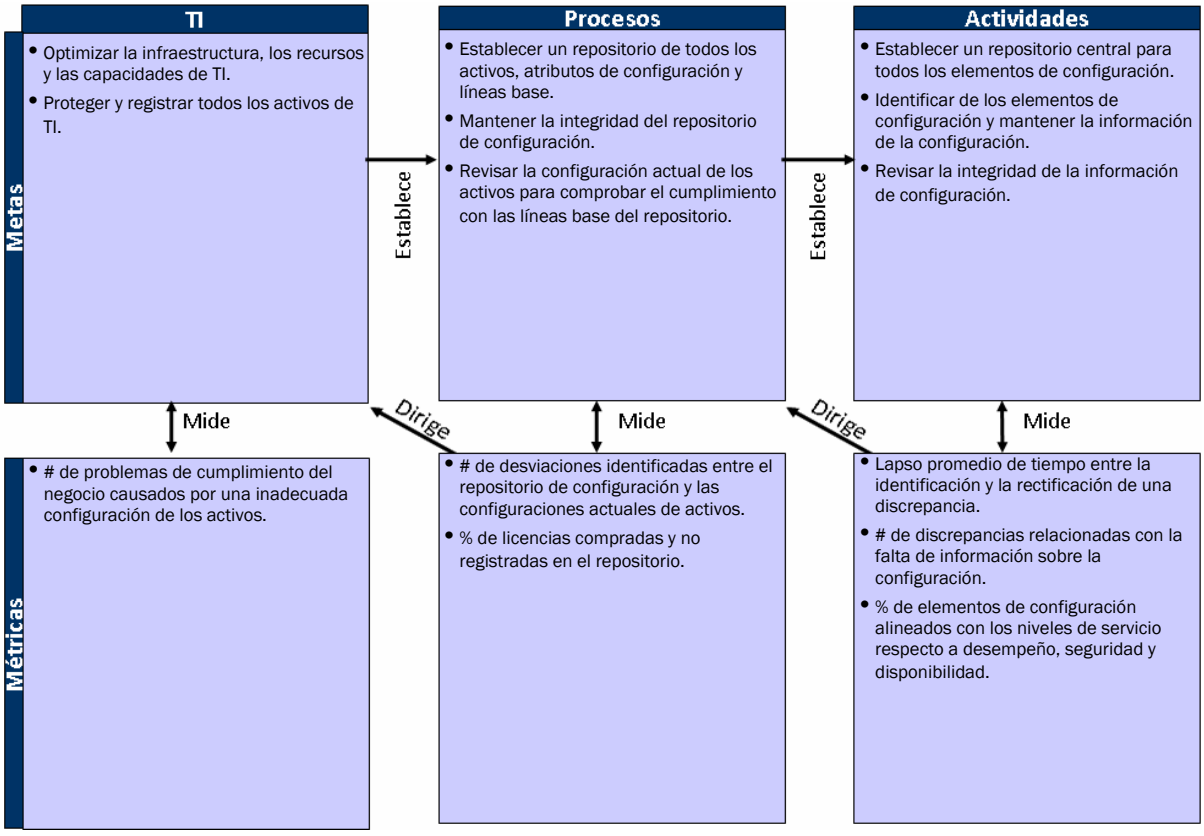
Salidas	Hacia						
Configuración de TI / detalles de activos	DS8	DS10	DS13				
RFC (donde y como aplicar el parche)	AI6						
Reportes de desempeño del proceso	ME1						

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Gerente de configuración
Desarrollar procedimientos de planeación de administración de la configuración					C	A	C	I	C		C	R
Recopilar información sobre la configuración inicial y establecer líneas base						C	C	C			I	A/R
Verificar y auditar la información de la configuración (incluye la detección de software no autorizado)		I				A			I		I	A/R
Actualizar el repositorio de configuración						R	R	R			I	A/R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS9 Administrar la Configuración

La administración del proceso de *Administrar la configuración* que satisfaga el requerimiento de TI del negocio de *optimizar la infraestructura, los recursos y las capacidades de TI, y rendir cuantas de los activos de TI* es:

0 No Existente cuando
La gerencia no valora los beneficios de tener un proceso implementado que sea capaz de reportar y administrar las configuraciones de la infraestructura de TI, tanto para configuraciones de hardware como de software.

1 Inicial / Ad Hoc cuando
Se reconoce la necesidad de contar con una administración de configuración. Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de hardware y software pero de manera individual. No están definidas prácticas estandarizadas.

2 Repetible pero Intuitivo cuando
La gerencia esta conciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales como administración de cambios y administración de problemas.

3 Definido cuando
Los procedimientos y las prácticas de trabajo se han documentado, estandarizado y comunicado, pero la habilitación y la aplicación de estándares dependen del individuo. Además se han implementado herramientas similares de administración de configuración entre plataformas. Es poco probable detectar las desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se lleva a cabo algún tipo de automatización para ayudar a rastrear cambios en el software o en el hardware. La información de la configuración es utilizada por los procesos interrelacionados.

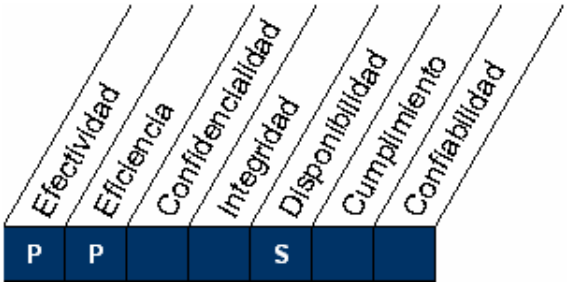
4 Administrado y Medible cuando
En todos los niveles de la organización se reconoce la necesidad de administrar la configuración y las buenas prácticas siguen evolucionando. Los procedimientos y los estándares se comunican e incorporan a la habilitación y las desviaciones son monitoreadas, rastreadas y reportadas. Se utilizan herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad. Los sistemas de administración de configuraciones cubren la mayoría de los activos de TI y permiten una adecuada administración de liberaciones y control de distribución. Los análisis de excepciones, así como las verificaciones físicas, se aplican de manera consistente y se investigan las causas desde su raíz.

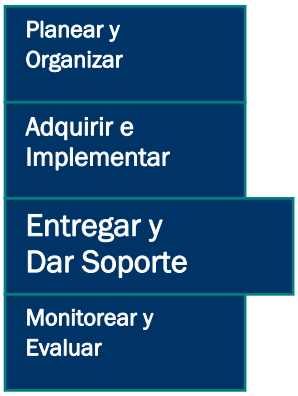
5 Optimizado cuando
Todos los activos de TI se administran en un sistema central de configuraciones que contiene toda la información necesaria acerca de los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Hay una completa integración de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los reportes de auditoría de los puntos de referencia, brindan información esencial sobre el software y hardware con respecto a reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se fomentan las reglas para limitar la instalación de software no autorizado. La gerencia proyecta las reparaciones y las actualizaciones utilizando reportes de análisis que proporcionan funciones de programación de actualizaciones y de renovación de tecnología. El rastreo de activos y el monitoreo de activos individuales de TI los protege y previene de robo, de mal uso y de abusos.

DESCRIPCIÓN DEL PROCESO.

DS10 Administración de Problemas

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario





Control sobre el proceso TI de

Administración de problemas

Que satisface el requerimiento del negocio de TI para

Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir el retrabajo y los defectos en la prestación de los servicios y de las soluciones

Enfocándose en

Registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados

Se logra con

- Realizando un análisis de causas raíz de los problemas reportados
- Analizando las tendencias
- Tomando propiedad de los problemas y con una resolución de problemas progresiva.

Y se mide con

- Número de problemas recurrentes con impacto en el negocio
- Porcentaje de problemas resueltos dentro del período de tiempo solicitado
- Frecuencia de los reportes o actualizaciones sobre un problema en curso, con base en la severidad del problema

OBJETIVOS DE CONTROL

DS10 Administración de Problemas

DS10.1 Identificación y Clasificación de Problemas

Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizar se de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte.

DS10.2 Rastreo y Resolución de Problemas

El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando:

- Todos los elementos de configuración asociados
- Problemas e incidentes sobresalientes
- Errores conocidos y sospechados
- Seguimiento de las tendencias de los problemas.

Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema, tal vez refiriéndolo a un comité determinado para incrementar la prioridad de la solicitud del cambio (RFC) o para implementar un cambio urgente, lo que resulte más pertinente. El avance de la resolución de un problema debe ser monitoreado contra los SLAs.

DS10.3 Cierre de Problemas

Disponer de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.

DS10.4 Integración de las Administraciones de Cambios, Configuración y Problemas

Para garantizar una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas. Monitorear cuánto esfuerzo se aplica en apagar fuegos, en lugar de permitir mejoras al negocio y, en los casos que sean necesarios, mejorar estos procesos para minimizar los problemas.

DIRECTRICES GERENCIALES

DS10 Administración de Problemas

Desde	Entradas
AI6	Autorización de cambio
DS8	Reportes de incidentes
DS9	Detalles de activos / configuración de TI
DS13	Bitácoras de errores

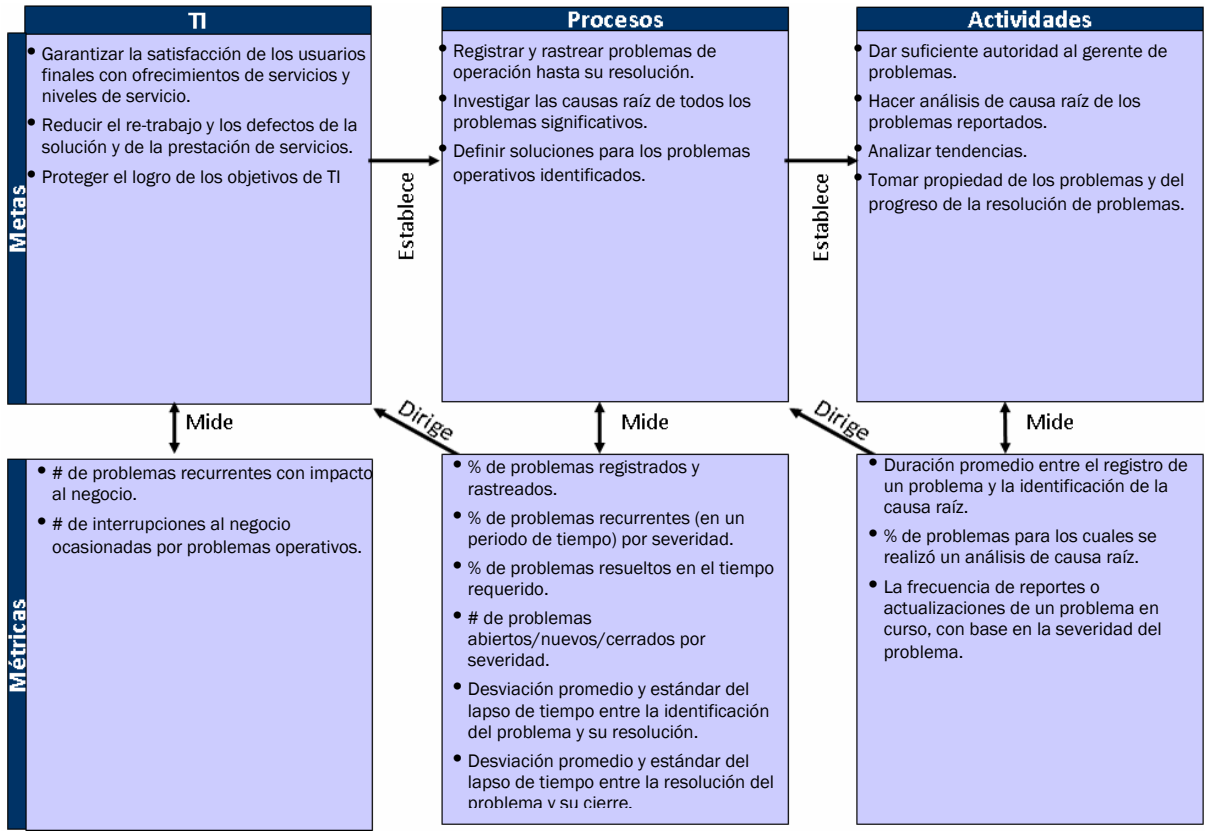
Salidas	Hacia
Solicitud de cambio	AI6
Registros de problemas	AI6
Reportes de desempeño del proceso	ME1
Problemas conocidos, errores conocidos y soluciones alternas	DS8

Matriz RACI

Actividades / Funciones	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Gerente de problemas
Identificar y clasificar problemas			I	I	C	A	C	C			I	R
Realizar análisis de causa raíz						C		C				A/R
Resolver problemas					C	A	R	R		R	C	C
Revisar el estatus de problemas			I	I	C	A/R	C	C		C	C	R
Emitir recomendaciones para mejorar y crear una solicitud de cambio relacionada					I	A	I	I		I		R
Mantener registros de los problemas					I	I		I			I	A/R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS10 Administración de Problemas

La administración del proceso de *Administrar problemas* que satisfaga el requerimiento de negocio de TI de *garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, y reducir el retrabajo y los defectos de la prestación de los servicios y de las soluciones* es:

0 No Existente cuando
No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.

1 Inicial / Ad Hoc cuando
Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.

2 Repetible pero Intuitivo cuando
Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.

3 Definido cuando
Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y habilitación. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.

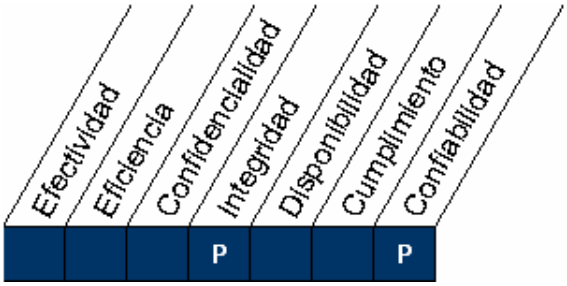
4 Administrado y Medible cuando
El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramente establecidas. Los métodos y los procedimientos son documentados, comunicados y medidos para evaluar su efectividad. La mayoría de los problemas están identificados, registrados y reportados, y su solución ha iniciado. El conocimiento y la experiencia se cultivan, mantienen y desarrollan hacia un nivel más alto a medida que la función es vista como un activo y una gran contribución al logro de las metas de TI y a la mejora de los servicios de TI. La administración de problemas está bien integrada con los procesos interrelacionados, tales como administración de incidentes, de cambios, y de configuración, y ayuda a los clientes para administrar información, instalaciones y operaciones. Se han acordado los KPIs y KGIs para el proceso de administración de problemas.

5 Optimizado cuando
El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.

DESCRIPCIÓN DEL PROCESO

DS11 Administración de Datos

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.



Control sobre el proceso TI de

Administración de datos

Que satisface el requerimiento del negocio de TI para

Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.

Enfocándose en

Mantener la integridad, exactitud, disponibilidad y protección de los datos

Se logra con

- Respaldando los datos y probando la restauración
- Administrando almacenamiento de datos en sitio y fuera de sitio.
- Desechando de manera segura los datos y el equipo

Y se mide con

- Satisfacción del usuario con la disponibilidad de los datos.
- Porcentaje de restauraciones exitosas de datos.
- Número de incidentes en los que tuvo que recuperarse datos sensitivos después que los medios habían sido desechados

OBJETIVOS DE CONTROL

DS11 Administración de Datos

DS11.1 Requerimientos del Negocio para Administración de Datos
Verificar que todos los datos que se espera procesar se reciben y procesan completamente, de forma precisa y a tiempo, y que todos los resultados se entregan de acuerdo a los requerimientos de negocio. Las necesidades de reinicio y reproceso están soportadas.

DS11.2 Acuerdos de Almacenamiento y Conservación
Definir e implementar procedimientos para el archivo, almacenamiento y retención de los datos, de forma efectiva y eficiente para conseguir los objetivos de negocio, la política de seguridad de la organización y los requerimientos regulatorios.

DS11.3 Sistema de Administración de Librerías de Medios
Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.

DS11.4 Eliminación
Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

DS11.5 Respaldo y Restauración
Definir e implementar procedimientos de respaldo y restauración de los sistemas, aplicaciones, datos y documentación en línea con los requerimientos de negocio y el plan de continuidad.

DS11.6 Requerimientos de Seguridad para la Administración de Datos
Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo, procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos regulatorios.

DIRECTRICES GERENCIALES

DS11 Administración de Datos

Desde	Entradas
PO2	Diccionario de datos; clasificaciones de datos asignados
AI4	Manuales de usuario, de operación, de soporte, técnicos y de administración
DS1	OLAs
DS4	Plan de protección y de almacenamiento de respaldos

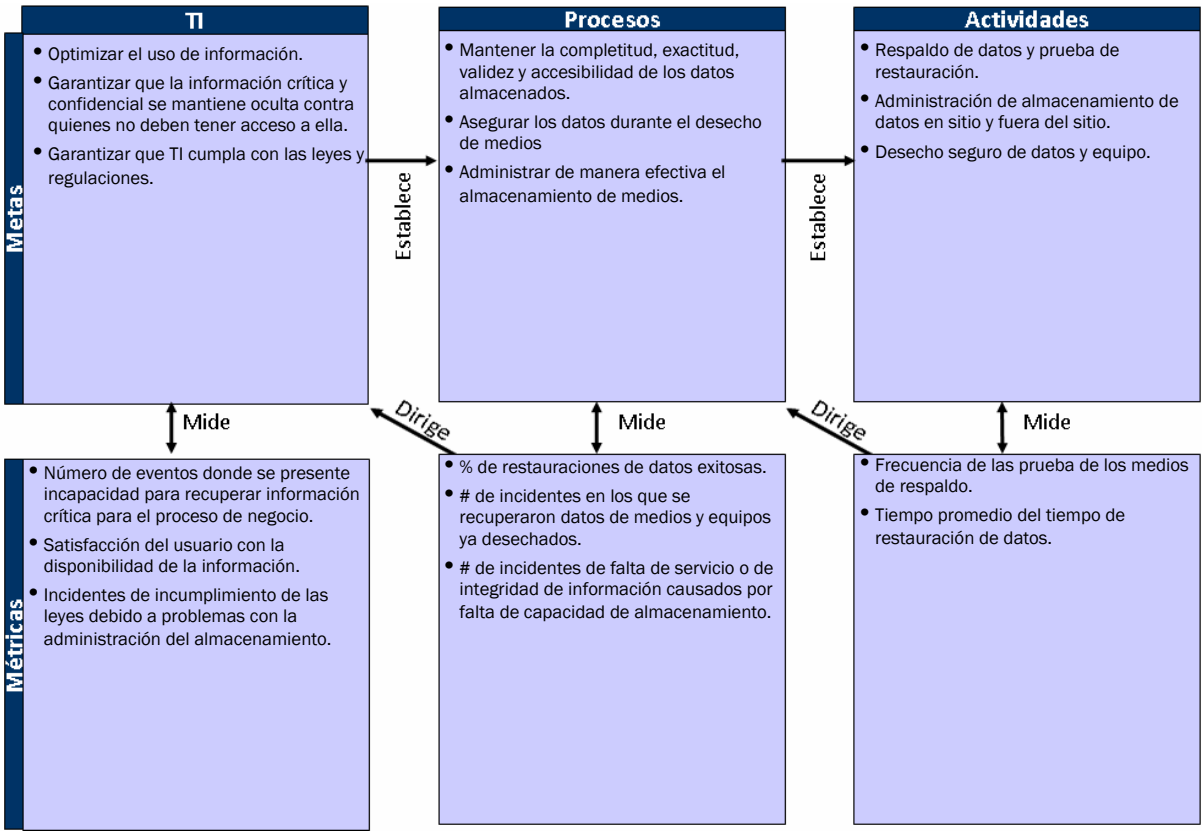
Salidas	Hacia
Reportes de desempeño del proceso	ME1
Instrucciones del operador para administración de datos	DS13

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Traducir los requerimientos de almacenamiento y conservación a procedimientos				A	I	C	R				C
Definir, mantener e implementar procedimientos para administrar librerías de medios				A		R	C	C	I		C
Definir, mantener e implementar procedimientos para desechar de forma segura, medios y equipo				A	C	R			I		C
Respaldar los datos de acuerdo al esquema				A		R					
Definir, mantener e implementar procedimientos para restauración de datos				A	C	R	C	C			I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS11 Administración de Datos

La administración del proceso de *Administrar los datos* que satisfaga el requerimiento de negocio de TI de *optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera* es:

0 No Existente cuando
Los datos no son reconocidos como parte de los recursos y los activos de la empresa. No está asignada la propiedad sobre los datos o sobre la rendición de cuentas individual sobre la administración de los datos. La calidad y la seguridad de los datos son deficientes o inexistentes.

1 Inicial / Ad Hoc cuando
La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal. No se lleva a cabo habilitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Los procedimientos de respaldo y recuperación y los acuerdos sobre desechos están en orden.

2 Repetible pero Intuitivo cuando
A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos son documentados por individuos clave. Se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.

3 Definido cuando
Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos / recuperación y desecho de equipo. Se lleva a cabo algún tipo de monitoreo sobre la administración de datos. Se definen métricas básicas de desempeño. Comienza a aparecer el entrenamiento sobre administración de información.

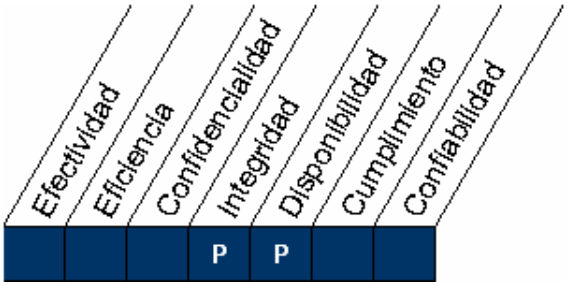
4 Administrado y Medible cuando
Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización. La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización. Los procedimientos se formalizan y son ampliamente conocidos, el conocimiento se comparte. Comienza a aparecer el uso de herramientas. Se acuerdan con los clientes los indicadores de desempeño y meta y se monitorean por medio de un proceso bien definido. Se lleva a cabo entrenamiento formal para el personal de administración de los datos.

5 Optimizado cuando
Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva. Las responsabilidades sobre la propiedad de los datos y la administración de los mismos están establecidas de forma clara, se conocen ampliamente a lo largo de la organización y se actualizan periódicamente. Los procedimientos se formalizan y se conocen ampliamente, la compartición del conocimiento es una práctica estándar. Se utilizan herramientas sofisticadas con un máximo de automatización de la administración de los datos. Se acuerdan con los clientes los indicadores de desempeño y meta, se ligan con los objetivos del negocio y se monitorean de manera regular utilizando un proceso bien definido. Se exploran constantemente oportunidades de mejora. El entrenamiento para el personal de administración de datos se institucionaliza.

DESCRIPCIÓN DEL PROCESO.

DS12 Administración del Ambiente Físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.



Control sobre el proceso TI de

Administración del ambiente físico

Que satisface el requerimiento del negocio de TI para

Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio

Enfocándose en

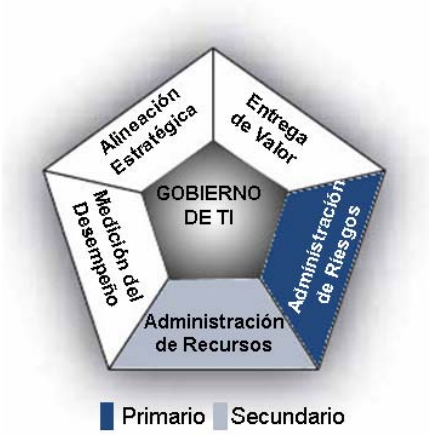
Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo

Se logra con

- Implementando medidas de seguridad físicas.
- Seleccionando y administrando las instalaciones

Y se mide con

- Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico
- Número de incidentes ocasionados por fallas o brechas de seguridad física
- Frecuencia de revisión y evaluación de riesgos físicos.



OBJETIVOS DE CONTROL

DS12 Administración del Ambiente Físico

DS12.1 Selección y Diseño del Centro de Datos
Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

DS12.2 Medidas de Seguridad Física
Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

DS12.3 Acceso Físico
Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

DS12.4 Protección Contra Factores Ambientales
Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente.

DS12.5 Administración de Instalaciones Físicas
Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

DIRECTRICES GERENCIALES

DS12 Administración del Ambiente Físico

Desde	Entradas
PO2	Clasificaciones asignadas a los datos
PO9	Evaluación de riesgo
AI3	Requerimientos del ambiente físico

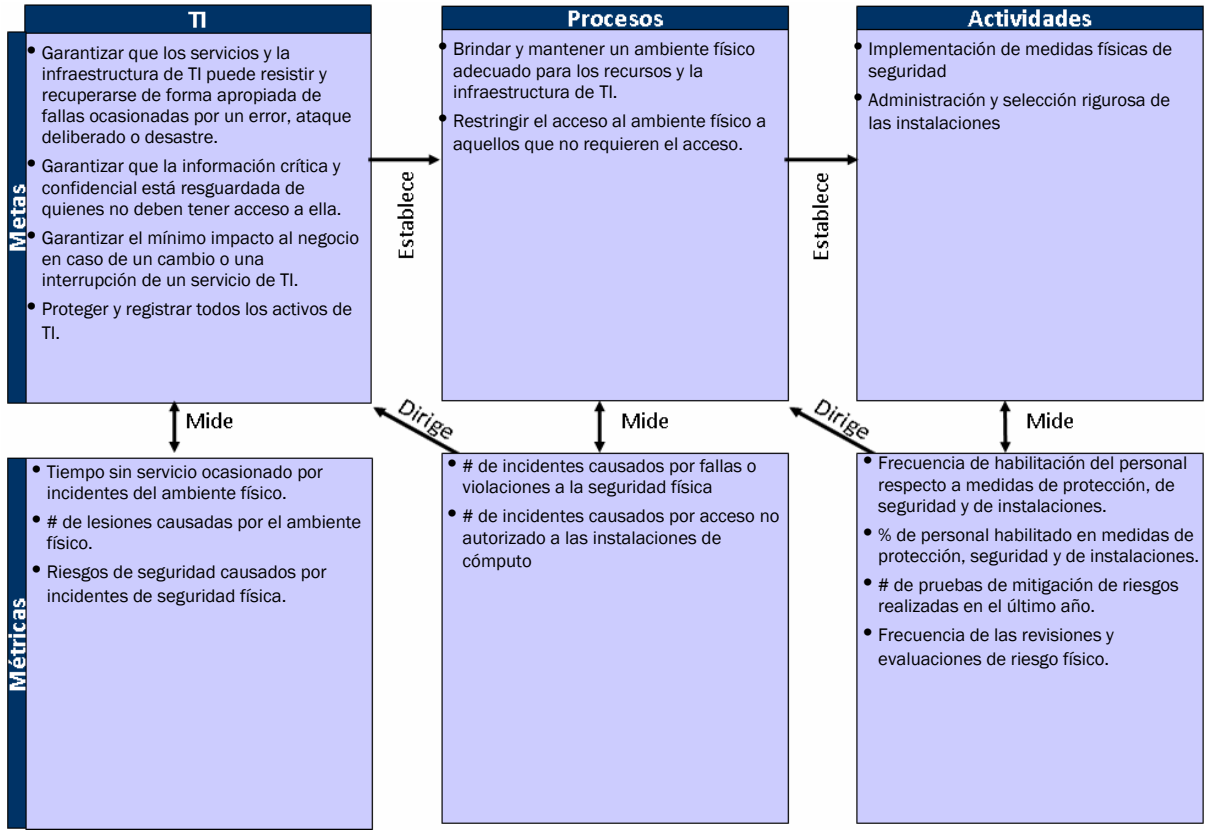
Salidas	Hacia
Reportes de desempeño de los procesos	ME1

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir el nivel requerido de protección física					C	A/R	C				C
Seleccionar y comisionar el sitio (centro de datos, oficina, etc)	I	C	C	C	C	A/R	C		C	C	C
Implementar medidas de ambiente físico					I	A/R	I	I			C
Administrar el ambiente físico (mantenimiento, monitoreo y reportes incluidos)						A/R	C				
Definir e implementar procesos para mantenimiento y autorización de acceso físico				C	I	A/R	I	I	I		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS12 Administración del Ambiente Físico

La administración del proceso de *Administrar el ambiente físico* que satisface el requerimiento del negocio de TI de *proteger los activos de TI y la información del negocio y minimizar el riesgo de interrupciones en el negocio* es:

0 No Existente cuando
No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.

1 Inicial / Ad Hoc cuando
La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.

2 Repetible pero Intuitivo cuando
Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.

3 Definido cuando
Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.

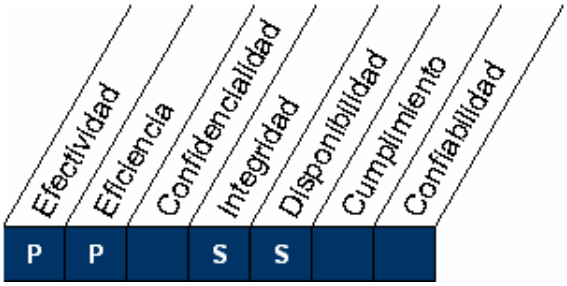
4 Administrado y Medible cuando
Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, cronograma, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades 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
Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente cómputo de la organización. Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.). Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan sin operadores humanos. Los KPIs y KGIs se miden regularmente. Los programas de mantenimiento preventivo fomentan un estricto apego a los horarios y se aplican pruebas regulares a los equipos sensibles. Las estrategias de instalaciones y de estándares están alineadas con las metas de disponibilidad de los servicios de TI y están integradas con la administración de crisis y con la planeación de continuidad del negocio. La gerencia revisa y optimiza las instalaciones utilizando los KPIs y KGIs de manera continua, capitalizando oportunidades para mejorar la contribución al negocio

DESCRIPCIÓN DEL PROCESO.

DS13 Administración de Operaciones

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.



Control sobre el proceso TI de

Administrar operaciones

Que satisface el requerimiento del negocio de TI para

Mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperase de errores y fallas

Enfocándose en

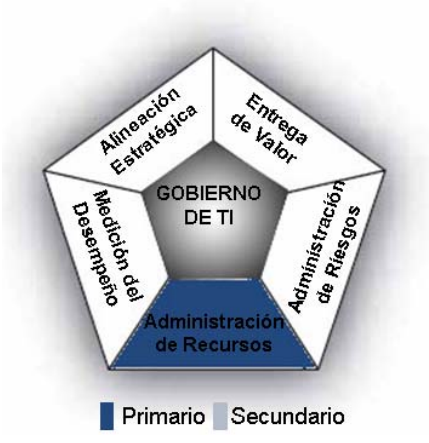
Cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura

Se logra con

- Operando el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas
- Manteniendo la infraestructura de TI

Y se mide con

- Número de niveles de servicio afectados a causa de incidentes en la operación.
- Horas no planeadas de tiempo sin servicio a causa de incidentes en la operación.
- Porcentaje de activos de hardware incluidos en los programas de mantenimiento.



OBJETIVOS DE CONTROL

DS13 Administración de Operaciones

DS13.1 Procedimientos e Instrucciones de Operación
Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

DS13.2 Programación de Tareas
Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el desempeño y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar agendados.

DS13.3 Monitoreo de la Infraestructura de TI
Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

DS13.4 Documentos Sensitivos y Dispositivos de Salida
Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.

DS13.5 Mantenimiento Preventivo del Hardware
Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

DIRECTRICES GERENCIALES

DS13 Administración de Operaciones

Desde	Entradas
AI4	Manuales de usuario, técnicos, operación y administración.
AI7	Promoción a producción y liberación del software y planes de distribución
DS1	SLAs y OLAS
DS4	Plan de almacenamiento y protección de respaldos
DS9	Configuración de TI / detalle de los activos de TI
DS11	Instrucciones del operador para administración de datos

Salidas	Hacia
Tiquetes de incidentes	DS8
Bitácoras de errores	DS10
Reportes de desempeño de los procesos	ME1

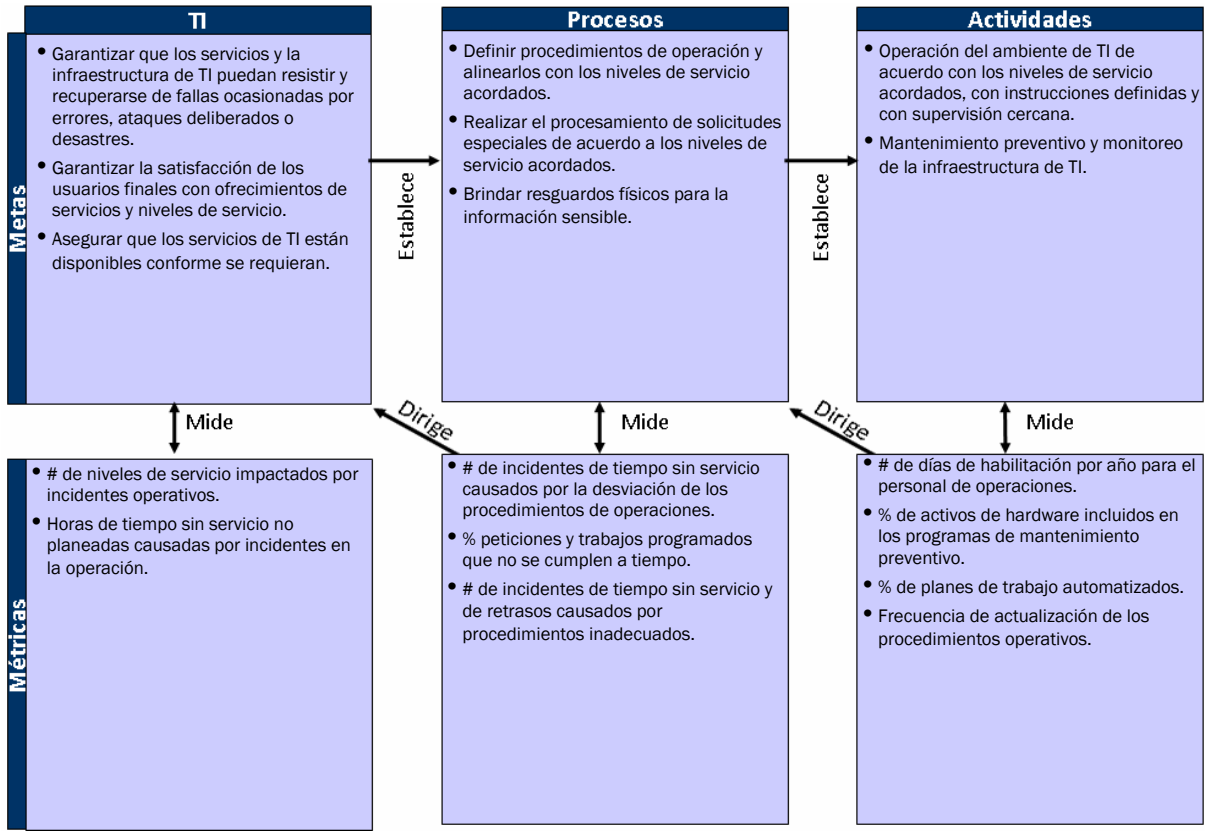
Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Crear / modificar procedimientos de operación (incluyendo manuales, planes de cambios, procedimientos de escalamiento, etc)						A/R					I
Programación de cargas de trabajo y de programas en lote					C	A/R	C	C			
Monitorear la infraestructura y procesar y resolver problemas						A/R					I
Administrar y asegurar la salida física de información (reportes, medios, etc)						A/R					C
Aplicar cambios o arreglos al programa y la infraestructura					C	A/R	C	C			C
Implementar / establecer un proceso para salvaguardar los dispositivos de autenticación contra interferencia, perdida o robo				A		R			I		C
Programar y llevar a cabo mantenimiento preventivo						A/R					

Funciones

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

DS13 Administración de Operaciones

La administración del proceso de *Administrar las operaciones* que satisface el requerimiento de negocio de TI de *mantener la integridad de la información y garantizar que la infraestructura de TI pueda resistir y recuperarse de errores y fallos* es:

0 No Existente cuando
La organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.

1 Inicial / Ad Hoc cuando
La organización reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen

2 Repetible pero Intuitivo cuando
La organización esta conciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Se asignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de habilitación para el operador y hay algunos estándares de operación formales.

3 Definido cuando
Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna habilitación durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal. Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia. Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.

4 Administrado y Medible cuando
Las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y la propiedad está asignada. Las operaciones se soportan a través de presupuestos de recursos para gastos de capital y de recursos humanos. La habilitación se formaliza y está en proceso. Las programaciones y las tareas se documentan y comunican, tanto a la función interna de TI como a los clientes del negocio. Es posible medir y monitorear las actividades diarias con acuerdos estandarizados de desempeño y de niveles de servicio establecidos. Cualquier desviación de las normas establecidas es atendida y corregida de forma rápida. La gerencia monitorea el uso de los recursos de cómputo y la terminación del trabajo o de las tareas asignadas. Existe un esfuerzo permanente para incrementar el nivel de automatización de procesos como un medio de mejora continua. Se establecen convenios formales de mantenimiento y servicio con los proveedores. Hay una completa alineación con los procesos de administración de problemas, capacidad y disponibilidad, soportados por un análisis de causas de errores y fallas.

5 Optimizado cuando
Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima. Los procesos de administración de operaciones de TI están estandarizados y documentados en una base de conocimiento, y están sujetos a una mejora continua. Los procesos automatizados que soportan los sistemas contribuyen a un ambiente estable. Todos los problemas y fallas se analizan para identificar la causa que los originó. Las reuniones periódicas con los responsables de administración del cambio garantizan la inclusión oportuna de cambios en las programaciones de producción. En colaboración con los proveedores, el equipo se analiza respecto a posibles síntomas de obsolescencia y fallas, y el mantenimiento es principalmente de naturaleza preventiva.

MONITOREAR Y EVALUAR

ME1 Monitorear y Evaluar el Desempeño de TI

ME2 Monitorear y Evaluar el Control Interno

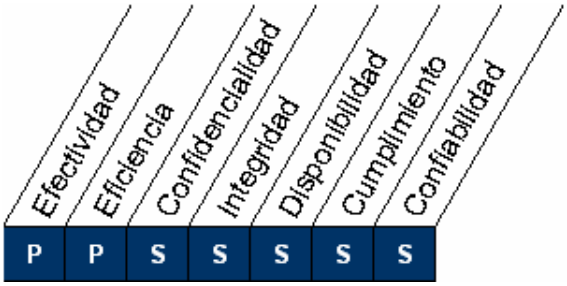
ME3 Garantizar el Cumplimiento Regulatorio

ME4 Proporcionar Gobierno de TI

DESCRIPCIÓN DEL PROCESO.

ME1 Monitorear y Evaluar el Desempeño de TI

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.



Control sobre el proceso TI de

Monitorear y evaluar el desempeño de TI

Que satisface el requerimiento del negocio de TI para

Transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos de gobierno

Enfocándose en

Monitorear y reportar las métricas del proceso e identificar e implementar acciones de mejoramiento del desempeño

Se logra con

- Cotejar y traducir los reportes de desempeño de proceso a reportes gerenciales
- Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias

Y se mide con

- Satisfacción de la gerencia y de la entidad de gobierno con los reportes de desempeño
- Número de acciones de mejoramiento impulsadas por las actividades de monitoreo
- Porcentaje de procesos críticos monitoreados

OBJETIVOS DE CONTROL

ME1 Monitorear y Evaluar el Desempeño de TI

ME1.1 Enfoque del Monitoreo
Establecer un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI, y Monitorear la contribución de TI al negocio. Integrar el marco de trabajo con el sistema de administración del desempeño corporativo.

ME1.2 Definición y Recolección de Datos de Monitoreo
Trabajar con el negocio para definir un conjunto balanceado de objetivos de desempeño y tenerlos aprobados por el negocio y otros interesados relevantes. Definir referencias con las que comparar los objetivos, e identificar datos disponibles a recolectar para medir los objetivos. 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 de administración adecuadas.

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 de administración
- Asignación de responsabilidades por la corrección
- Rastreo de los resultados de las acciones comprometidas.

DIRECTRICES GERENCIALES

ME1 Monitorear y evaluar el desempeño de TI

Desde	Entradas
PO5	Reportes de costo-beneficio
PO10	Reportes de desempeño del proyecto
AI6	Reportes del estatus de los cambios
DS1-13	Reportes de desempeño del proceso
DS8	Reportes de satisfacción del usuario
ME2	Reportes de la efectividad de los controles de TI
ME3	Reportes sobre el cumplimiento de las actividades de TI respecto a requerimientos legales y regulatorios externos
ME4	Reportes sobre el estatus del gobierno de TI

Salidas	Hacia						
Indicadores de desempeño a planeación de TI	PO1	PO2	DS1				
Planes de acciones correctivas	PO4	PO8					
Tendencias y eventos de riesgos históricos	PO9						
Reporte de desempeño del proceso	ME2						

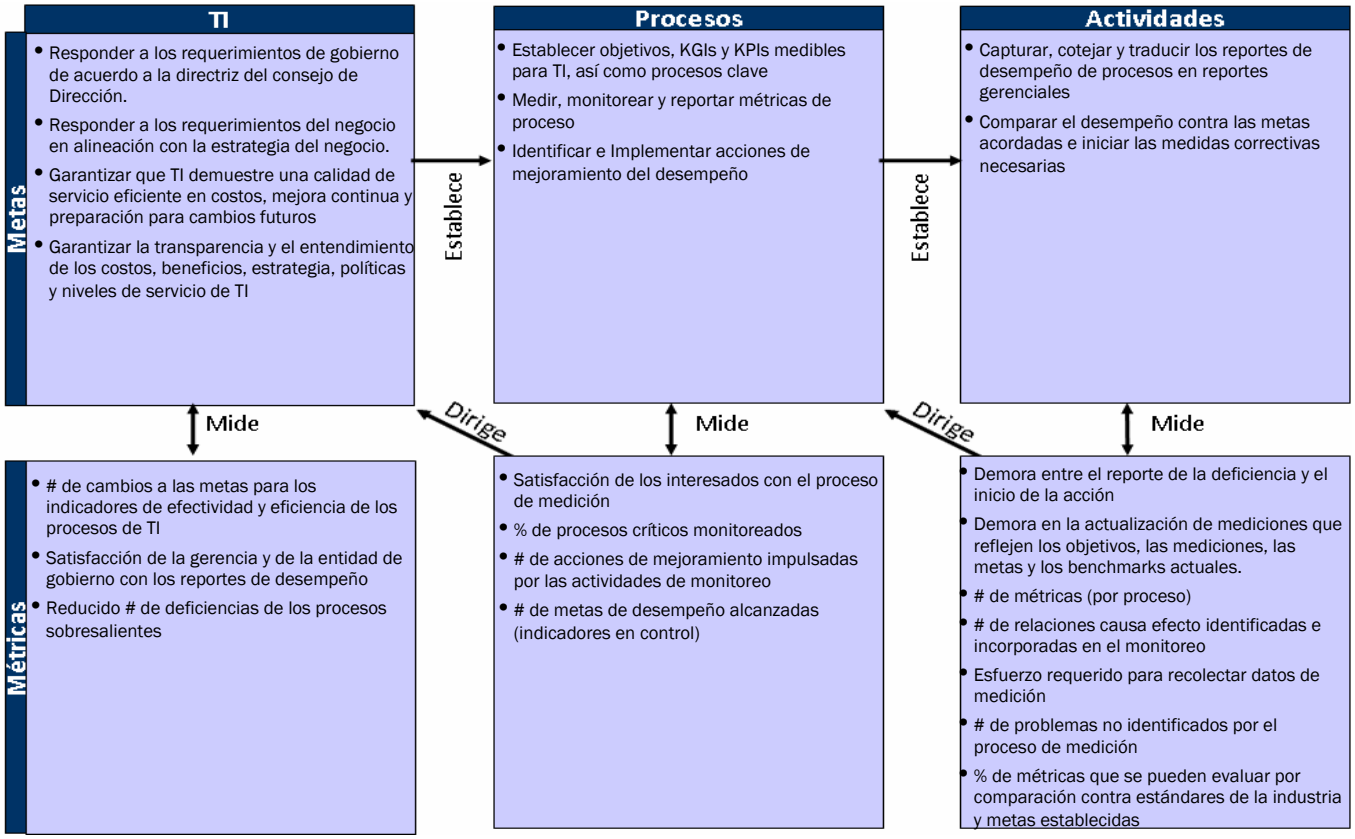
Matriz RACI

Funciones

Actividades	Consejo de Directores	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Establecer el enfoque de monitoreo		A	R	C	R	I	C	I	C	I		C
Identificar y recolectar objetivos medibles que apoyen a los objetivos del negocio		C	C	C	A	R	R		R			
Crear cuadro de mandos					A		R	C	R	C		
Evaluar el desempeño			I	I	A	R	R	C	R	C		
Reportar el desempeño	I	I	I	R	A	R	R	C	R	C		I
Identificar y monitorear las medidas de mejora del desempeño					A	R	R	C	R	C		C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

ME1 Monitorear y Evaluar el Desempeño de TI

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 Intuitivo 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 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.

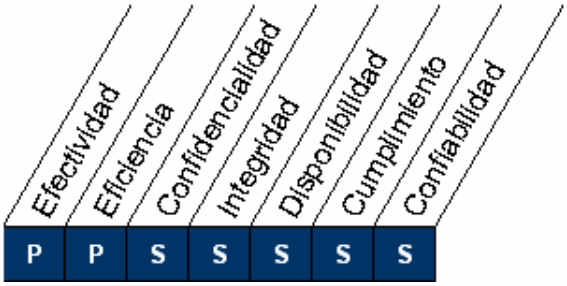
4 Administrado y Medible cuando
La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas 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.

DESCRIPCIÓN DEL PROCESO.

ME2 Monitorear y Evaluar el Control Interno

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.



Control sobre el proceso TI de

Monitorear y evaluar el control interno

Que satisface el requerimiento del negocio de TI para

Proteger el logro de los objetivos de TI y cumplir las leyes y reglamentos relacionados con TI

Enfocándose en

El monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento

Se logra con

- La definición de un sistema de controles internos integrados en el marco de trabajo de los procesos de TI
- Monitorear y reportar la efectividad de los controles internos sobre TI
- Reportar las excepciones de control a la gerencia para tomar acciones

Y se mide con

- Número de brechas importantes del control interno
- Número de iniciativas para la mejora del control
- Número y cubrimiento de auto evaluaciones de control

OBJETIVOS DE CONTROL

ME2 Monitorear y Evaluar el Control Interno

ME2.1 Monitoreo del Marco de Trabajo de Control Interno
Monitorear de forma continua, comparar y mejorar el ambiente de control de TI y el marco de trabajo de control de TI para satisfacer los objetivos organizacionales.

ME2.2 Revisiones de Auditoría
Monitorear y evaluar la eficiencia y efectividad de los controles internos de revisión de la gerencia de TI.

ME2.3 Excepciones de Control
Identificar las excepciones de control, y analizar e identificar sus causas raíz subyacentes. Escalar las excepciones de control y reportar a los interesados apropiadamente. Establecer acciones correctivas necesarias.

ME2.4 Control de Auto Evaluación
Evaluar la completitud y efectividad de los controles de gerencia sobre 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.

ME2.6 Control Interno para Terceros
Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicios externos cumplen con los requerimientos legales y regulatorios y obligaciones contractuales.

ME2.7 Acciones Correctivas
Identificar, iniciar, rastrear e implementar acciones correctivas derivadas de los controles de evaluación y los informes.

DIRECTRICES GERENCIALES

ME2 Monitorear y Evaluar el Control Interno

Desde	Entradas
AI7	Monitoreo de Controles Internos
ME1	Reporte de desempeño de procesos

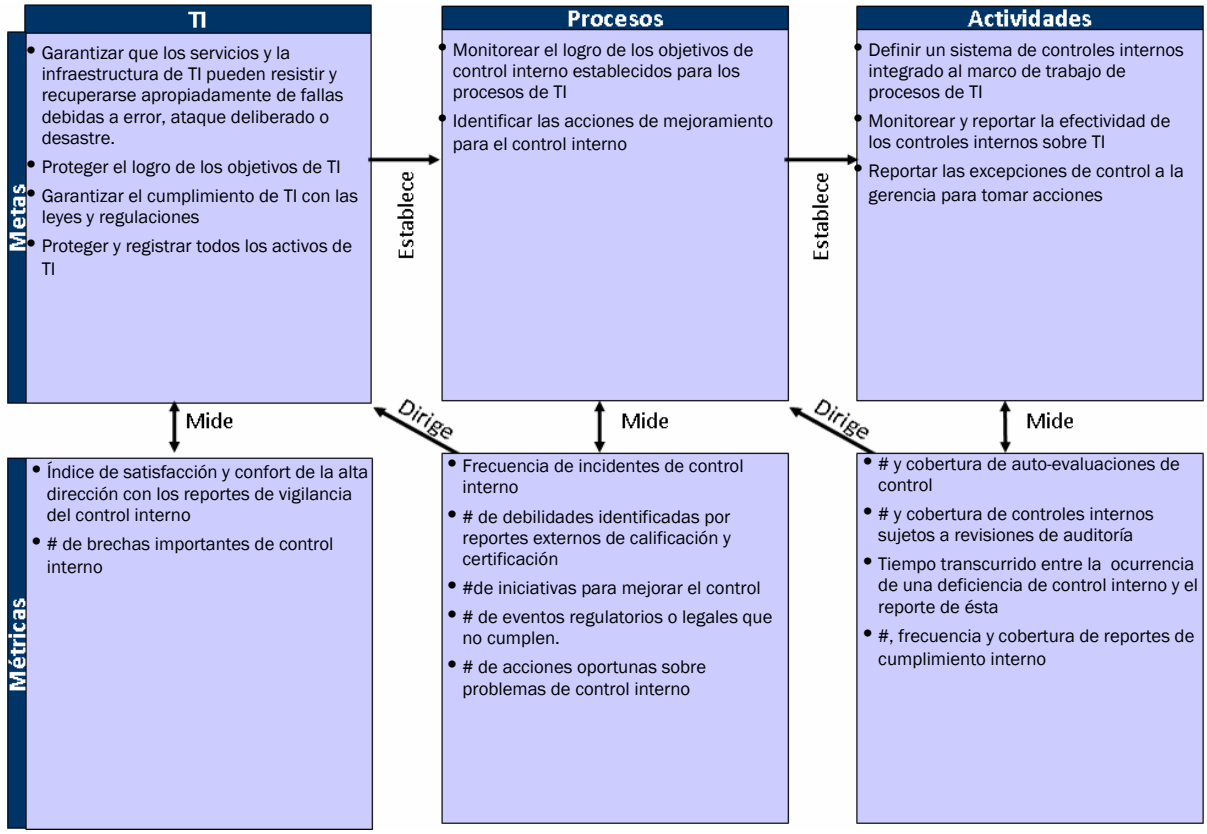
Salidas	Hacia						
Reporte sobre la efectividad de los controles de TI	PO4	PO6	ME1	ME4			

Matriz RACI

Actividades	Consejo de Directores	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Monitorear y controlar las actividades de control interno de TI					A		R		R	R		R
Monitorear el proceso de auto evaluación				I	A		R		R	R		C
Crear cuadro de mandos				I	A		R		R	R		C
Monitorear el proceso para obtener aseguramiento sobre los controles operados por terceros		I	I	I	A		R		R	R		C
Monitorear el proceso para identificar y evaluar las excepciones de control		I	I	I	A	I	R		R	R		C
Monitorear el proceso para identificar y evaluar y remediar las excepciones de control		I	I	I	A	I	R		R	R		C
Reportar a los interesados clave	I	I	I		A/R							I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

ME2 Monitorear y Evaluar el Control Interno

La administración del proceso de *Monitorear y evaluar el control interno* que satisfaga el requerimiento 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 Intuitivo 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 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.

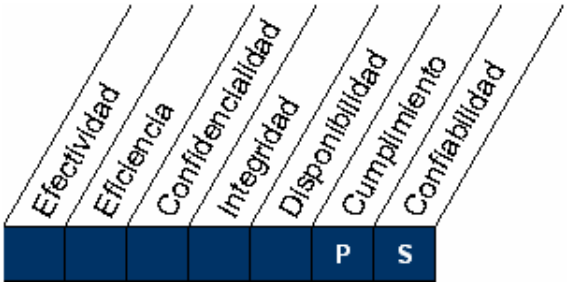
4 Administrado y Medible cuando
La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar 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 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.

DESCRIPCIÓN DEL PROCESO.

ME3 Garantizar el Cumplimiento con Requerimientos Externos

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio.



Control sobre el proceso TI de

Garantizar el cumplimiento regulatorio

Que satisface el requerimiento del negocio de TI para

Cumplir las leyes y regulaciones

Enfocándose en

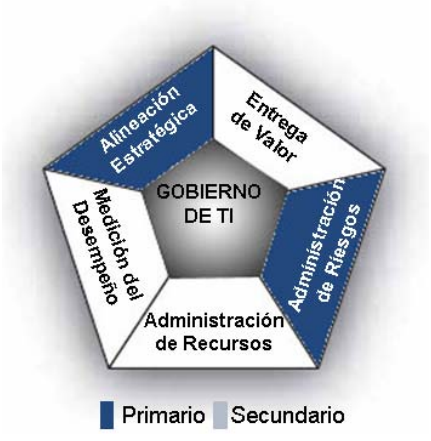
La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento

Se logra con

- La identificación de los requisitos legales y regulatorios relacionados con TI
- La evaluación del impacto de los requisitos regulatorios
- El monitoreo y reporte del cumplimiento de los requisitos regulatorios

Y se mide con

- El costo del no cumplimiento de TI, incluyendo arreglos y multas
- Tiempo promedio de demora entre la identificación de los problemas externos de cumplimiento y su resolución
- Frecuencia de revisiones de cumplimiento



OBJETIVOS DE CONTROL

ME3 Garantizar el Cumplimiento con Requerimientos Externos

ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
Identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben de cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización.

ME3.2 Optimizar la Respuesta a Requerimientos Externos
Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, regulatorios y contractuales son direccionados y comunicados.

ME3.3 Evaluación del Cumplimiento con Requerimientos Externos
Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios.

ME3.4 Aseguramiento Positivo del Cumplimiento
Obtener y reportar garantía de cumplimiento y adhesión a todas las políticas internas derivadas de directivas internas o requerimientos legales externos, regulatorios o contractuales, confirmando que se ha tomado cualquier acción correctiva para resolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna.

ME3.5 Reportes Integrados
Integrar los reportes de TI sobre requerimientos legales, regulatorios y contractuales con las salidas similares provenientes de otras funciones del negocio.

DIRECTRICES GERENCIALES

ME3 Garantizar el Cumplimiento con Requerimientos Externos

Desde	Entradas
*	Requerimientos de cumplimiento legal y regulatorio
PO6	políticas de TI

* Entradas provenientes de fuentes externas a COBIT

Salidas	Hacia	
Catálogo de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI	PO4	ME4
Reporte sobre el cumplimiento de las actividades de TI con los requerimientos externos legales y regulatorios	ME1	

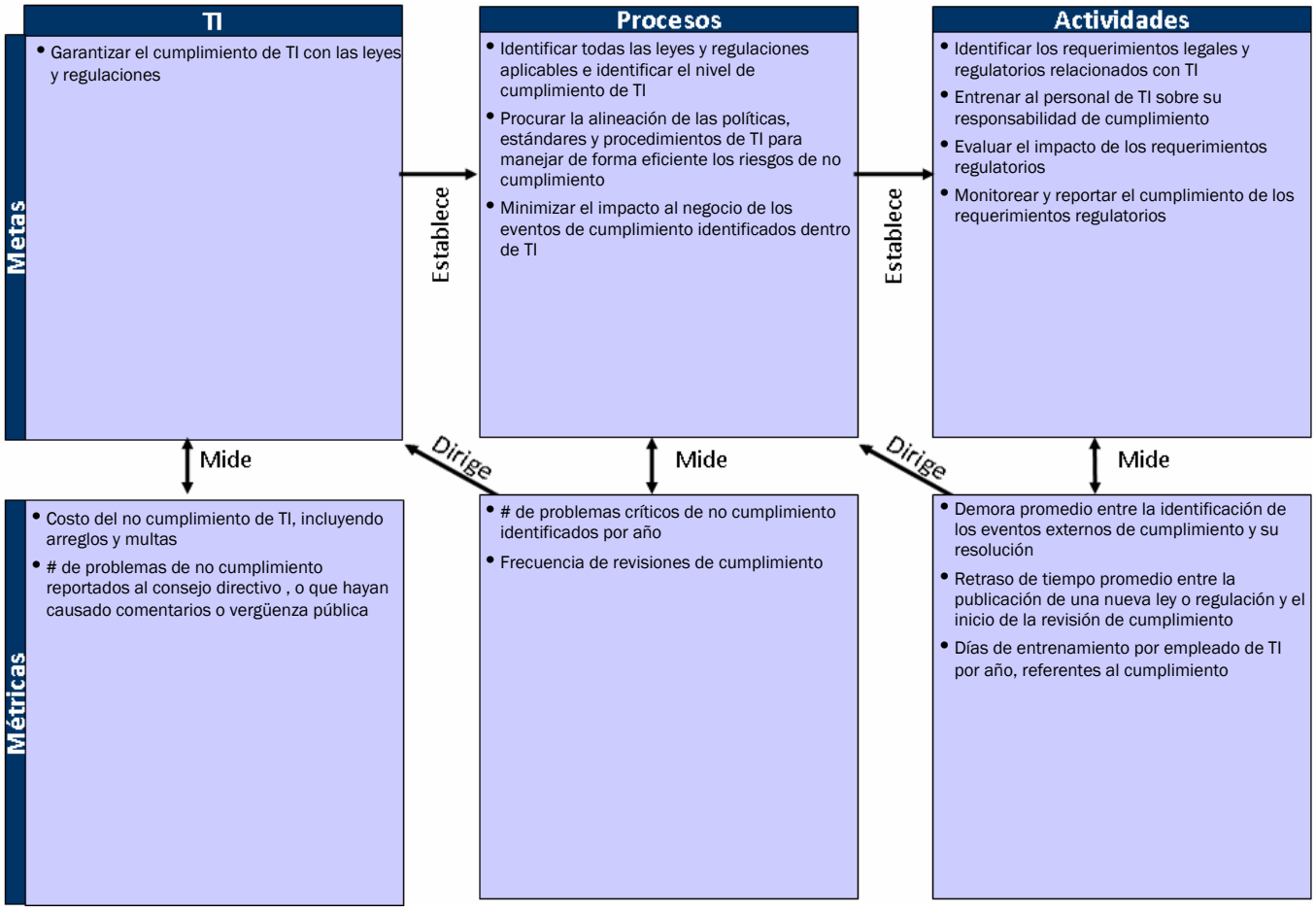
Matriz RACI

Funciones

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad	Consejo de Directores
Definir y ejecutar un proceso para identificar los requerimientos legales, contractuales de políticas y regulatorios				A/R	C	I	I	I	C	I	R	
Evaluar cumplimiento de actividades de TI con políticas, estándares y procedimientos de TI	I	I	I	A/R	I	R	R	R	R	R	R	I
Reportar aseguramiento positivo del cumplimiento de las actividades de TI con las políticas, planes y procedimientos de TI				A/R	C	C	C	C	C	C	R	
Brindar retro alimentación para alinear las políticas, estándares y procedimientos de TI con los requerimientos de cumplimiento				A/R	C	C	C	C	C		R	
Integrar los reportes de TI sobre requerimientos regulatorios con similares provenientes de otras funciones del negocio				A/R		I	I	I	R	I	R	

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

ME3 Garantizar el Cumplimiento con Requerimientos Externos

La administración del proceso de *Garantizar el cumplimiento con requerimientos externos* que satisfaga el requerimiento de negocio de TI de *asegurar el cumplimiento de las leyes, regulaciones y requerimientos contractuales* es:

0 No Existente cuando
Existe poca conciencia respecto a los requerimientos externos que afectan a TI, sin procesos referentes al cumplimiento de requisitos regulatorios, legales y contractuales.

1 Inicial / Ad Hoc cuando
Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorías o revisiones.

2 Repetible pero Intuitivo cuando
Existe el entendimiento de la necesidad de cumplir con los requerimientos externos y la necesidad se comunica. En los casos en que el cumplimiento se ha convertido en un requerimiento recurrente, como en los requerimientos financieros o en la legislación de privacidad, se han desarrollado procedimientos individuales de cumplimiento y se siguen año a año. No existe, sin embargo, un enfoque estándar. Hay mucha confianza en el conocimiento y responsabilidad de los individuos, y los errores son posibles. Se brinda entrenamiento informal respecto a los requerimientos externos y a los temas de cumplimiento.

3 Definido cuando
Se han desarrollado, documentado y comunicado políticas, procedimientos y procesos, para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizá no se sigan y algunas quizá estén desactualizadas o sean poco prácticas de implementar. Se realiza poco monitoreo y existen requisitos de cumplimiento que no han sido resueltos. Se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y se instruye respecto a los procesos de cumplimiento definidos. Existen contratos pro forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales.

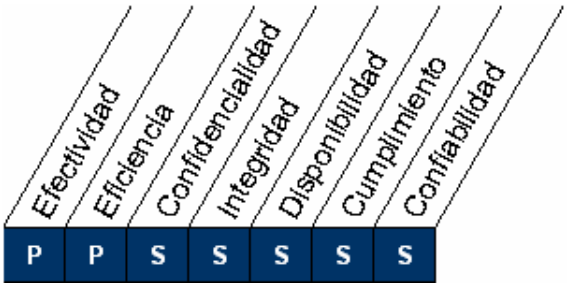
4 Administrado y Medible cuando
Existe un entendimiento completo de los eventos y de la exposición a requerimientos externos, y la necesidad de asegurar el cumplimiento a todos los niveles. Existe un esquema formal de entrenamiento que asegura que todo el equipo esté consciente de sus obligaciones de cumplimiento. Las responsabilidades son claras y se entiende el empoderamiento de los procesos. El proceso incluye una revisión del entorno para identificar requerimientos externos y cambios recurrentes. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos externos, reforzar las prácticas internas e implementar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas raíz, con el objetivo de identificar soluciones sostenibles. Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos vigentes y contratos recurrentes de servicio.

5 Optimizado cuando
Existe un proceso bien organizado, eficiente e implantado para cumplir con los requerimientos externos, basado en una sola función central que brinda orientación y coordinación a toda la organización. Hay un amplio conocimiento de los requerimientos externos aplicables, incluyendo sus tendencias futuras y cambios anticipados, así como la necesidad de nuevas soluciones. La organización participa en discusiones externas con grupos regulatorios y de la industria para entender e influenciar los requerimientos externos que la puedan afectar. Se han desarrollado mejores prácticas que aseguran el cumplimiento de los requisitos externos, y esto ocasiona que haya muy pocos casos de excepciones de cumplimiento. Existe un sistema central de rastreo para toda la organización, que permite a la gerencia documentar el flujo de trabajo, medir y mejorar la calidad y efectividad del proceso de monitoreo del cumplimiento. Un proceso externo de auto-evaluación de requerimientos existe y se ha refinado hasta alcanzar el nivel de buena práctica. El estilo y la cultura administrativa de la organización referente al cumplimiento es suficientemente fuerte, y se elaboran los procesos suficientemente bien para que el entrenamiento se limite al nuevo personal y siempre que ocurra un cambio significativo.

DESCRIPCIÓN DEL PROCESO.

ME4 Proporcionar Gobierno de TI

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales.



Control sobre el proceso TI de

Proporcionar gobierno de TI

Que satisface el requerimiento del negocio de TI para

La integración de un gobierno de TI con objetivos de gobierno corporativo y el cumplimiento con las leyes y regulaciones

Enfocándose en

La elaboración de informes para el consejo directivo sobre la estrategia, el desempeño y los riesgos de TI y responder a los requerimientos de gobierno de acuerdo a las directrices del consejo directivo

Se logra con

- El establecimiento de un marco de trabajo para el gobierno de TI, integrado al gobierno corporativo
- La obtención de aseguramiento independientes sobre el estatus del gobierno de TI

Y se mide con

- La frecuencia de informes del consejo directivo sobre TI a los interesados (incluyendo el nivel de madurez)
- La frecuencia de los reportes de TI hacia el consejo directivo (incluyendo el nivel de madurez)
- Frecuencia de revisiones independientes del cumplimiento de TI

OBJETIVOS DE CONTROL

ME4 Proporcionar Gobierno de TI

ME4.1 Establecimiento de un Marco de Gobierno de TI
Definir, establecer y alinear el marco de gobierno de TI con la visión completa del entorno de control y Gobierno Corporativo. Basar el marco de trabajo en un adecuado proceso de TI y modelo de control y proporcionar la rendición de cuentas y prácticas inequívocas para evitar una rotura en el control interno y la revisión. Confirmar que el marco de gobierno de TI asegura el cumplimiento con las leyes y regulaciones y que esta alineado, y confirma la entrega de, la estrategia y objetivos empresariales. Informa del estado y cuestiones de gobierno de TI.

ME4.2 Alineamiento Estratégico
Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio. Trabajar con el consejo directivo para definir e implementar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI, garantizando así que tanto la estrategia como los objetivos se distribuyan en cascada hacia las unidades de negocio y hacia las unidades de TI y que se desarrolle certidumbre y confianza entre el negocio y TI. Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre el negocio y TI en la toma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.

ME4.3 Entrega de Valor
Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales. Asegurarse de que los resultados de negocio esperados de las inversiones habilitadas por TI y el alcance completo del esfuerzo requerido para lograr esos resultados esté bien entendido, que se generen casos de negocio integrales y consistentes, y que los aprueben los interesados, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa del logro de los beneficios, tales como la contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a los requerimientos de los clientes. Implementar un enfoque disciplinado de la administración del portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades de TI.

ME4.4 Administración de Recursos
Revisar inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas de las iniciativas y operaciones de TI para asegurar recursos y alineamiento apropiados con los objetivos estratégicos y los imperativos de negocio actuales y futuros.

ME4.5 Administración de Riesgos
Trabajar con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa y obtener garantía razonable que las practicas de administración de riesgos de TI son apropiadas para asegurar que el riesgo actual de TI no excede el riesgo aceptable de dirección. Introducir las responsabilidades de administración de riesgos en la organización, asegurando que el negocio y TI regularmente evalúan y reportan riesgos relacionados con TI y su impacto y que la posición de los riesgos de TI de la empresa es transparente a los interesados.

ME4.6 Medición del Desempeño
Confirmar que los objetivos de TI confirmados se han conseguido o excedido, o que el progreso hacia las metas de TI cumple las expectativas. Donde los objetivos confirmados no se han alcanzado o el progreso no es el esperado, revisar las acciones correctivas de gerencia. Informar a dirección los portafolios relevantes, programas y desempeños de TI, soportados por informes para permitir a la alta dirección revisar el progreso de la empresa hacia las metas identificadas.

ME4.7 Aseguramiento Independiente
Garantizar de forma independiente (interna o externa) la conformidad de TI con la legislación y regulación relevante; las políticas de la organización, estándares y procedimientos; practicas generalmente aceptadas; y la efectividad y eficiencia del desempeño de TI.

DIRECTRICES GERENCIALES

ME4 Proporcionar Gobierno de TI

Desde	Entradas
PO4	Marco de trabajo del proceso de TI
PO5	Reportes de costo/beneficio
PO9	Evaluación y reportes de riesgo
ME2	Reportar la efectividad de los controles de TI
ME3	Catálogo de requisitos legales y regulatorios relacionados con la prestación de servicios de TI

Salidas	Hacia						
Mejoras al marco de trabajo de los procesos	PO4						
Reportar el estatus del gobierno de TI	PO1	ME1					
Resultados de negocio esperados de las inversiones en TI	PO5						
Dirección estratégica empresarial para TI	PO1						
Apetito empresarial de riesgos de TI	PO9						

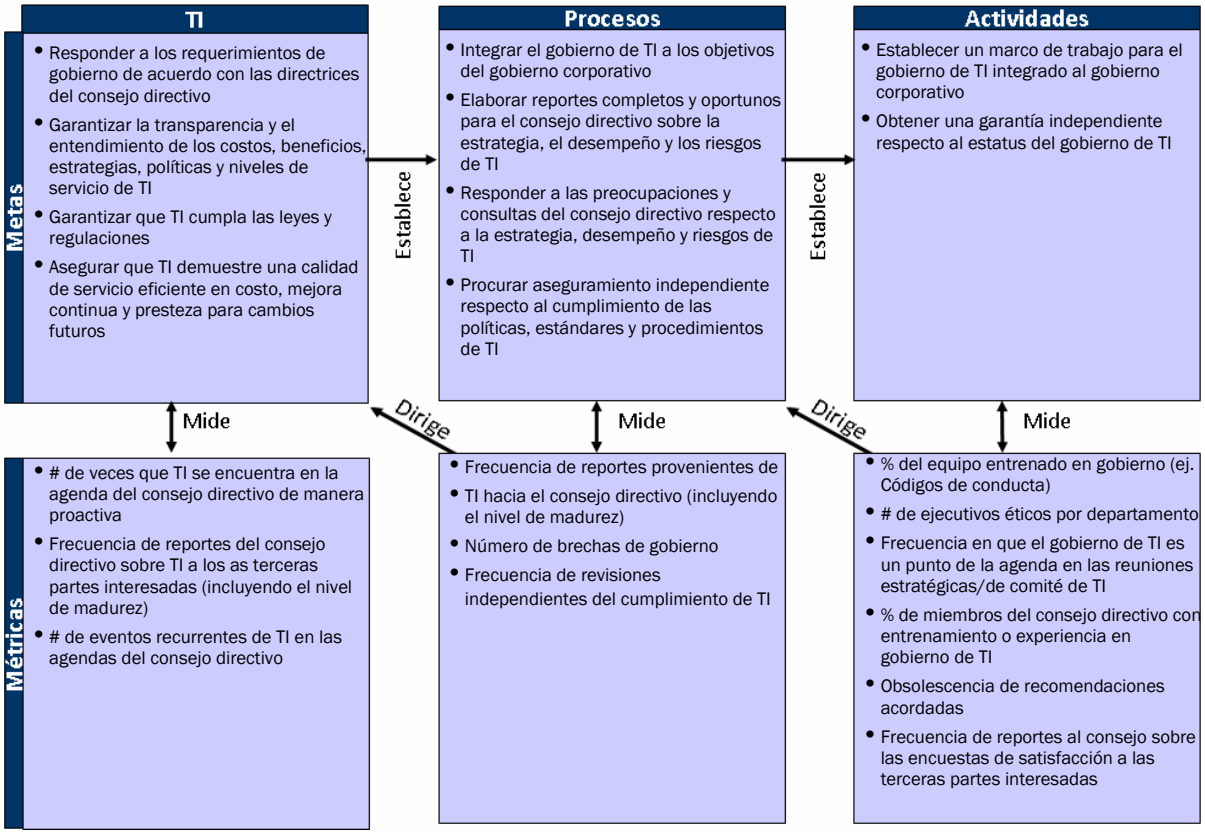
Matriz RACI

Funciones

Actividades	Consejo de Directores	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Establecer visibilidad y facilitación del consejo y de los ejecutivos hacia las actividades de TI	A	R	C	C	C							C
Revisar, avalar, alinear y comunicar es desempeño de TI, la estrategia de TI, el manejo de recursos y riesgos de TI con respecto a la estrategia empresarial	A	R	I	I	R							C
Crear cuadro de mandos	A	R	C	I	C		I	I	I	I	I	R
Resolver los hallazgos de las evaluaciones independientes y garantizar la implantación por parte de la gerencia de las recomendaciones acordadas	A	R	C	I	C		I	I	I	I	I	R
Generar un reporte de gobierno de TI	A	C	C	C	R	C	I	I	I	I	I	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Metas y Métricas



MODELO DE MADUREZ

ME4 Proporcionar Gobierno de TI

La administración del proceso de *Proporcionar Gobierno de TI* que satisfaga el requerimiento de negocio de TI de *integrar el gobierno de TI con los objetivos de gobierno corporativos y el cumplimiento con las leyes y regulaciones* es:

0 No Existente cuando
Existe una carencia completa de cualquier proceso reconocible de gobierno de TI. La organización ni siquiera ha reconocido que existe un problema a resolver; por lo tanto, no existe comunicación respecto al tema.

1 Inicial / Ad Hoc cuando
Se reconoce que el tema del gobierno de TI existe y que debe ser resuelto. Existen enfoques ad hoc aplicados individualmente o caso por caso. El enfoque de la gerencia es reactivo y solamente existe una comunicación esporádica e inconsistente sobre los temas y los enfoques para resolverlos. La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio. La gerencia solo responde de forma reactiva a los incidentes que hayan causado pérdidas o vergüenza a la organización.

2 Repetible pero Intuitivo cuando
Existe una conciencia sobre los temas de gobierno de TI. Las actividades y los indicadores de desempeño del gobierno de TI, los cuales incluyen procesos planeación, entrega y supervisión de TI, están en desarrollo. Los procesos de TI seleccionados se identifican para ser mejorados con base en decisiones individuales. La gerencia ha identificado mediciones básicas para el gobierno de TI, así como métodos de evaluación y técnicas; sin embargo, el proceso no ha sido adoptado a lo largo de la organización. La comunicación respecto a los estándares y responsabilidades de gobierno se deja a los individuos. Los individuos impulsan los procesos de gobierno en varios proyectos y procesos de TI. Los procesos, herramientas y métricas para medir el gobierno de TI están limitadas y pueden no usarse a toda su capacidad debido a la falta de experiencia en su funcionalidad.

3 Definido cuando
La importancia y la necesidad de un gobierno de TI se reconocen por parte de la gerencia y se comunican a la organización. Un conjunto de indicadores base de gobierno de TI se elaboran donde se definen y documentan los vínculos entre las mediciones de resultados y los impulsores del desempeño. Los procedimientos se han estandarizado y documentado. La gerencia ha comunicado los procedimientos estandarizados y el entrenamiento está establecido. Se han identificado herramientas para apoyar a la supervisión del gobierno de TI. Se han definido tableros de control como parte de los Balanced Scorecard de TI. Sin embargo, se delega al individuo su entrenamiento, el seguimiento de los estándares y su aplicación. Puede ser que se monitoreen los procesos sin embargo la mayoría de desviaciones, se resuelven con iniciativa individual y es poco probable que se detecten por parte de la gerencia.

4 Administrado y Medible cuando
Existe un entendimiento completo de los temas de gobierno a todos los niveles. Hay un entendimiento claro de quién es el cliente y se definen y supervisan las responsabilidades por medio de acuerdos de niveles de servicio. Las responsabilidades son claras y la propiedad de procesos está establecida. Los procesos de TI y el gobierno de TI están alineados e integrados con la estrategia corporativa de TI. La mejora de los procesos de TI se basa principalmente en un entendimiento cuantitativo y es posible monitorear y medir el cumplimiento con procedimientos y métricas de procesos. Todos los interesados en los procesos están conscientes de los riesgos, de la importancia de TI, y de las oportunidades que ésta puede ofrecer. La gerencia ha definido niveles de tolerancia bajo los cuales los procesos pueden operar. Existe un uso limitado, principalmente táctico, de la tecnología con base en técnicas maduras y herramientas estándar ya implantadas. El gobierno de TI ha sido integrado a los procesos de planeación estratégica y operativa, así como a los procesos de monitoreo. Los indicadores de desempeño de todas las actividades de gobierno de TI se registran y siguen, y esto lidera mejoras a nivel de toda la empresa. La rendición general de cuentas del desempeño de los procesos clave es clara, y la gerencia recibe recompensas con base en las mediciones clave de desempeño.

5 Optimizado cuando
Existe un entendimiento avanzado y a fututo de los temas y soluciones del gobierno de TI. El entrenamiento y la comunicación se basan en conceptos y técnicas de vanguardia. Los procesos se han refinado hasta un nivel de mejor práctica de la industria, con base en los resultados de las mejoras continuas y en el modelo de madurez con respecto a otras organizaciones. La implantación de las políticas de TI ha resultado en una organización, personas y procesos que se adaptan rápidamente, y que dan soporte completo a los requisitos de gobierno de TI. Todos los problemas y desviaciones se analizan por medio de la técnica de causa raíz y se identifican e implementan medidas eficientes de forma rápida. TI se utiliza de forma amplia, integrada y optimizada para automatizar el flujo de trabajo y brindar herramientas para mejorar la calidad y efectividad. Los riesgos y los retornos de los procesos de TI están definidos, balanceados y comunicados en toda la empresa. Se aprovechan a los expertos externos y se usan evaluaciones por comparación para orientarse. El monitoreo, la auto-evaluación y la comunicación respecto a las expectativas de gobierno están en toda la organización y se de un uso óptimo a la tecnología para apoyar las mediciones, el análisis, la comunicación y el entrenamiento. El Gobierno Corporativo y el gobierno de TI están vinculados de forma estratégica, aprovechando la tecnología y los recursos humanos y financieros para mejorar la ventaja competitiva de la empresa. Las actividades de gobierno de TI están integradas al proceso de Gobierno Corporativo.

APÉNDICE I

TABLA DE ENLACES ENTRE METAS Y PROCEDIMIENTOS.

Este apéndice brinda una visión global de cómo se relacionan las metas genéricas del negocio con las metas de TI con los procesos de TI y con los criterios de información. Se proporcionan tres tablas:

1. La primera tabla muestra las equivalencias de las metas del negocio, de acuerdo al balanced scorecard, con las metas de TI y con los criterios de información[1]. Esto ayuda a mostrar, para una meta genérica de negocios determinada, las metas de TI que por lo general dan soporte a esta meta, y los criterios de información de COBIT que se relacionan con la meta del negocio.
2. La segunda tabla muestra las equivalencias de las metas de TI con los procesos de TI de COBIT, así como los criterios de información sobre los cuales se basa la meta de TI[2].
3. La tercera tabla proporciona un mapeo inverso que muestra para cada proceso de TI, las metas de TI que son soportadas.

Las tablas ayudan a demostrar el alcance de COBIT y la relación general de negocio entre COBIT y los impulsores del negocio, permitiendo así establecer la equivalencia entre las metas típicas de negocio, por medio de las metas de TI, y los procesos de TI requeridos para darles soporte. Las tablas se basan en metas orgánicas y, por lo tanto, se deben usar como guía y adaptarse a la empresa determinada.

Para proporcionar una liga hacia los criterios de información usados para los requisitos de negocio de la 3ª edición de COBIT, las tablas también contienen una indicación de los criterios de información más importantes soportados por el negocio y por las metas de TI.

Notas:

[1] Los criterios de información contenidos en la gráfica de metas de negocio se basan en un agregado de los criterios para las metas de TI relacionadas y en una evaluación subjetiva de aquellos que son más relevantes para la meta del negocio. No se hizo el intento para indicar si son primarios o secundarios. Estos son tan solo indicativos y los usuarios pueden seguir un proceso similar al evaluar sus propias metas de negocio

[2] Las referencias primarias y secundarias de los criterios de información en la gráfica de metas de TI se basan en un agregado de los criterios para cada proceso de TI y en una evaluación subjetiva de qué es primario y qué es secundario para la meta de TI., debido a que algunos procesos tienen mayor impacto en la meta de TI que otros. Estos son tan solo indicativos y los usuarios pueden seguir un proceso similar al evaluar sus propias metas de TI

Apendice I – Tablas de Enlace Entre Metas y Procesos

ENLACE DE LAS METAS DE NEGOCIO A PROCESOS DE TI

		Metas de Negocio	Metas de TI								Criterios de Información de COBIT						
											Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI-permitiendo inversión en negocio	24	28								✓					
	2	Gestionar los riesgos de TI que afecten a negocio	2	14	17	18	19	20	21	22			✓	✓	✓		
	3	Mejorar gobierno corporativo y transparencia	2	18													✓
Perspectiva del cliente	4	Mejorar la orientación y servicio al cliente	3	23							✓						
	5	Ofrecer productos y servicios competitivos.	5	24							✓	✓					
	6	Establecer continuidad y disponibilidad de servicios	10	16	22	23					✓				✓		
	7	Crear agilidad en la respuesta a los cambios de los requerimientos de negocio	1	5	25						✓	✓					
	8	Lograr optimización de costes de la entrega de servicios	7	8	10	24						✓					
	9	Obtener información fiable y útil para tomar decisiones estratégicas	2	4	12	20	26				✓			✓			✓
Perspectiva Interna	10	Mejorar y mantener funcionalidad de procesos de negocio	6	7	11						✓	✓					
	11	Reducir el coste de los procesos	7	8	13	15	24					✓					
	12	Proporcionar cumplimiento con leyes externas, regulaciones y contratos	2	19	20	21	22	26	27				✓			✓	
	13	Proporcionar cumplimiento con políticas internas	2	13									✓			✓	
	14	Gestionar cambios de negocio	1	5	6	11	28				✓	✓					
	15	Mejorar y mantener productividad operacional y de personal	7	8	11	13					✓	✓					
Perspectiva de Aprendizaje y Crecimiento	16	Gestionar productos e innovación de negocio.	5	25	28						✓	✓					
	17	Adquirir y mantener personal cualificado y motivado	9								✓	✓					

ENLACE DE LAS METAS DE TI A PROCESOS DE TI

	Metas de TI	Procesos											Criterios de Información de CobiT: Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
1	Responder a requerimientos de negocio alineado con la estrategia de negocio	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	Responder a los requerimientos de gobierno en línea con la dirección ejecutiva	PO1	PO4	PO10	ME1	ME4							P	P					
3	Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	Optimizar el uso de la información	PO2	DS11											S		P			S
5	Crear agilidad de TI	PO2	PO4	PO7	AI3								P	P		S			
6	Definir como la funcionalidad de negocio y requerimientos de control se trasladan en soluciones efectivas y	AI1	AI2	AI6									P	P				S	
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados	PO3	AI2	AI5									P	P				S	
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada	AI3	AI5										S	P					
9	Adquirir y mantener habilidades de TI que responden a la estrategia de TI	PO7	AI5										P	P					
10	Asegurar la satisfacción mutua de relaciones con terceras partes	DS2											P	P	S	S	S	S	S
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio	PO2	AI4	AI7									P	P		S	S		
12	Asegurar la transparencia y comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnológica	PO6	AI4	AI7	DS7	DS8							P	S					
14	Tener en cuenta y proteger todos los activos de TI	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	Optimizar la infraestructura, recursos y capacidades de TI	PO3	AI3	DS3	DS7	DS9							S	P					
16	Reducir los defectos de la solución y entrega de servicio y reelaborar	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	Proteger el logro de los objetivos de TI	PO9	DS10	ME2									P	P	S	S	S	S	S
18	Establecer la claridad del impacto de negocio de los riesgos a los objetivos y recursos de TI	PO9											S	S	P	P	P	S	S
19	Asegurar que la información critica y confidencial se retiene a aquellos que no deben tener acceso	PO6	DS5	DS11	DS12										P	P	S	S	S
20	Asegurar que las transacciones de negocio automatizadas y los cambios a la información son confiables	PO6	AI7	DS5									P			P	S	S	
21	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperar de fallos debidos a errores, ataques deliberados o desastres.	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios	PO6	AI6	DS4	DS12								P	S		S	P		
23	Estar seguros que los servicios de TI están disponibles según se requiere	DS3	DS4	DS8	DS13								P	P			P		
24	Mejorar la eficiencia de costes de TI y sus contribuciones a la rentabilidad de negocio	PO5	DS6										S	P					S
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad	PO8	PO10										P	P		S			S
26	Mantener la integridad de la información e infraestructura de procesamiento	AI6	DS5										P	P		P	P		S
27	Asegurar que TI cumple con la legislación, regulación y contratos	DS11	ME2	ME3	ME4										S	S		P	S
28	Asegurar que TI demuestra la eficiencia de costes de la calidad de servicios, mejora continua y disposición para cambios futuros	PO5	DS6	ME1	ME4								P	P					P

APÉNDICE I

COBIT 4.1

MATRIZ DE PROCESOS DE TI A METAS DE TI

APÉNDICE I

COBIT 4.1

	1 Responder a requerimientos de negocio alineado con la estrategia de negocio	2 Responder a los requerimientos de gobierno en línea con la dirección ejecutiva	3 Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio	4 Optimizar el uso de la información	5 Crear agilidad de TI	6 Definir como la funcionalidad de negocio y requerimientos de control se trasladan en soluciones efectivas y eficientes automatizadas	7 Adquirir y mantener sistemas de aplicación integrados y estandarizados	8 Adquirir y mantener una infraestructura de TI integrada y estandarizada	9 Adquirir y mantener habilidades de TI que respondan a la estrategia de TI	10 Asegurar la satisfacción mutua de relaciones con terceras partes	11 Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio	12 Asegurar la transparencia y comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio	13 Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnológica	14 Tener en cuenta y proteger todos los activos de TI	15 Optimizar la infraestructura, recursos y capacidades de TI	16 Reducir los defectos de la solución y entrega de servicio y reelaborar	17 Proteger el logro de los objetivos de TI	18 Establecer la claridad del impacto de negocio de los riesgos a los objetivos y recursos de TI	19 Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso	20 Asegurar que las transacciones de negocio automatizadas y los cambios a servicios de TI o cambios	21 Asegurar que los servicios de TI y la infraestructura puedan resistir apropiadamente y recuperar de fallos debidos a errores, ataques	22 Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios	23 Estar seguros que los servicios de TI están disponibles según se requiere	24 Mejorar la eficiencia de costes de TI y sus contribuciones a la rentabilidad de negocio	25 Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad	26 Mantener la integridad de la información e infraestructura de procesamiento	27 Asegurar que TI cumple con la legislación, regulación y contratos	28 Asegurar que TI demuestra la eficiencia de costes de la calidad de servicios, mejora continua y disposición para cambios futuros
Planear y Organizar																													
PO1 Definir un plan estratégico de TI	V	V																											
PO2 Definir la arquitectura de la información	V			V	V						V																		
PO3 Determinar la dirección tecnológica							V								V														
PO4 Definir los procesos, organización y relaciones de TI	V	V			V																								
PO5 Administrar la inversión en TI												V														V			V
PO6 Comunicar las aspiraciones y la dirección de la gerencia												V	V						V	V	V	V							
PO7 Administrar recursos humanos de TI					V				V																				
PO8 Administrar la calidad			V													V										V			
PO9 Evaluar y administrar los riesgos de TI														V			V	V											
PO10 Administrar proyectos	V	V																								V			
Adquirir e Implementar																													
AI1 Identificar soluciones automatizadas	V					V																							
AI2 Adquirir y mantener software aplicativo						V	V																						
AI3 Adquirir y mantener infraestructura tecnológica					V			V							V														
AI4 Facilitar la operación y el uso			V								V		V			V													
AI5 Adquirir recursos de TI							V	V	V																				
AI6 Administrar cambios	V					V										V							V				V		
AI7 Instalar y acreditar soluciones y cambios	V										V		V			V					V	V							
Entregar y Dar Soporte																													
DS1 Definir y administrar los niveles de servicio	V		V									V																	
DS2 Administrar los servicios de terceros			V							V		V																	
DS3 Administrar el desempeño y la capacidad	V														V										V				
DS4 Garantizar la continuidad del servicio																					V	V	V						
DS5 Garantizar la seguridad de los sistemas														V					V	V	V					V			
DS6 Identificar y asignar costos												V													V				V
DS7 Educar y entrenar a los usuarios			V										V		V														
DS8 Administrar la mesa de servicio y los incidentes			V										V												V				
DS9 Administrar la configuración														V	V														
DS10 Administrar los problemas			V													V	V												
DS11 Administrar los datos				V															V								V		
DS12 Administrar el ambiente físico														V					V		V	V							
DS13 Administrar las operaciones			V																		V		V						
Monitorear y Evaluar																													
ME1 Monitorear y evaluar el desempeño de TI	V	V										V																	V
ME2 Monitorear y evaluar el control interno														V			V				V							V	
ME3 Garantizar el cumplimiento regulatorio																												V	
ME4 Proporcionar gobierno de TI		V										V																V	V

APÉNDICE II

MAPEO ENTRE LOS PROCESOS DE TI Y LAS ÁREAS FOCALES DE GOBIERNO DE TI, COSO, LOS RECURSOS TI DE COBIT Y LOS CRITERIOS DE INFORMACIÓN DE COBIT

Este apéndice proporciona las equivalencias entre los procesos de TI de CobiT y las cinco áreas focales del gobierno de TI, los recursos de TI y los criterios de información. La tabla también contiene un indicador de importancia relativa (alta, media y baja), con base en la evaluación por comparación (benchmarking) vía CobiT ONLINE. Esta matriz en una página, y a alto nivel como el marco de trabajo de CobiT resuelve los requisitos de gobierno de TI y de COSO, y muestra la relación entre los procesos de TI, los recursos y criterios de información de TI. La P se usa cuando hay una relación primaria y la S cuando solamente existe una relación secundaria. El hecho de que no exista una P ni una S no significa que no exista relación, sólo que es menos importante o marginal. Los valores de importancia se basan en una encuesta y en la opinión de expertos, y se incluyen sólo como una guía. Los usuarios deben considerar qué procesos son importantes dentro de sus propias organizaciones.

Apendice II – Mapeo de Procesos de TI a las Areas Focales de Gobierno TI, COSO, Recursos de TI de CobiT y Criterios de Información de CobiT

		Áreas de enfoque de Gobierno TI					COSO					Recursos TI de CobiT				Criterios de Información de CobiT						
	IMPORTANCIA	Alineación estratégica	Entrega de valor	Administración de	Administración de	Medición del desempeño	Entorno de Control	Evaluación de riesgos	Actividades de control	Información y	Monitoreo	Aplicación	Información	Infraestructura	Personas	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar																						
PO1 Definir un plan estratégico de TI	A	P		S	S			P		S	S					P	S					
PO2 Definir la arquitectura de la información	B	P	S	P	S				P	P						S	P	S	P			
PO3 Determinar la dirección tecnológica	M	S	S	P	S			S	P	S						P	P					
PO4 Definir los procesos, organización y relaciones de TI	B	S		P	P		P			S	S					P	P					S
PO5 Administrar la inversión en TI	M	S	P	S		S		S	P							P	P					
PO6 Comunicar las aspiraciones y la dirección de la gerencia	M	P			P		P			P						P					S	
PO7 Administrar recursos humanos de TI	B	P		P	S	S	P			S						P	P					
PO8 Administrar la calidad	M	P	S		S		P		P	S	P					P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	A	P			P			P								S	S	P	P	P	S	S
PO10 Administrar proyectos	A	P	S	S	S	S	S	S	P		S					P	P					
Adquirir e Implementar																						
AI1 Identificar soluciones automatizadas	M	P	P	S	S				P							P	S					
AI2 Adquirir y mantener software aplicativo	M	P	P		S				P							P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	B			P					P							S	P		S	S		
AI4 Facilitar la operación y el uso	B	S	P	S	S				P	S						P	P		S	S	S	S
AI5 Adquirir recursos de TI	M		S	P					P							S	P				S	
AI6 Administrar cambios	A		P	S				S	P		S					P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S					P	S		S	S		
Entregar y Dar Soporte																						
DS1 Definir y administrar los niveles de servicio	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	B		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	B	S	S	P	S	S			P		S					P	P			S		
DS4 Garantizar la continuidad del servicio	M	S	P	S	P	S	S		P	S						P	S			P		
DS5 Garantizar la seguridad de los sistemas	A				P				P	S	S							P	P	S	S	S
DS6 Identificar y asignar costos	B		S	P		S			P								P					P
DS7 Educar y entrenar a los usuarios	B	S	P	S	S		P			S						P	S					
DS8 Administrar la mesa de servicio y los incidentes	B		P			S	S			P	P					P	P					
DS9 Administrar la configuración	M		P	P	S				P							P	S			S		S
DS10 Administrar los problemas	M		P		S	S			P	S	S					P	P			S		
DS11 Administrar los datos	A		P	P	P				P										P			P
DS12 Administrar el ambiente físico	B			S	`P			S	P										P	P		
DS13 Administrar las operaciones	B			P					P	S						P	P		S	S		
Monitorear y Evaluar																						
ME1 Monitorear y evaluar el desempeño de TI	A	S	S	S	S	P				S	P					P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	M		P		P						P					P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio	A	P			P				P	S	S										P	S
ME4 Proporcionar gobierno de TI	A	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

(P=Primario, S=Secondario).

Nota: El mapeo COSO esta basado sobre el marco original COSO. El mapeo también aplica sobre el ultimo COSO Administración de Riesgos Empresarial - Marco Integrado, que expande sobre los controles internos proporcionando un enfoque mas robusto y extensivo sobre el sujeto de la gestión de riesgos de la empresa. Mientras ni intenta ni reemplaza el marco de control interno COSO, sino mas bien incorpora el marco de control interno dentro, los usuarios de CobiT pueden elegir referir a ambos marcos de gestión de riesgos de la empresa para satisfacer sus necesidades de control interno y moverse a través de un proceso de gestión de riesgos mas completo.

Página dejada en blanco intencionadamente.

APÉNDICE III
MODELO DE MADUREZ PARA EL CONTROL INTERNO

Este apéndice muestra un modelo genérico de madurez que describe el estatus del ambiente de control interno y el establecimiento de controles internos en una empresa. Muestra cómo la administración del control interno, y la conciencia de la necesidad de establecer mejores controles internos, por lo general evoluciona de algo *ad hoc*, hasta un nivel optimizado. El modelo brinda una guía de alto nivel para ayudar a los usuarios de COBIT a apreciar lo que se requiere para un control interno efectivo en TI y ayudar a posicionar a su empresa en la escala de madurez.

APÉNDICE III – MODELO DE MADUREZ PARA EL CONTROL INTERNO

Nivel de Madurez	Estado del Entorno de Control Interno	Establecimiento de Control Interno
0 No existente	No se reconoce la necesidad del control interno. El control no es parte de la cultura o misión organizacional. Existe un alto riesgo de deficiencias e incidentes de control.	No existe la intención de evaluar la necesidad del control interno. Los incidentes se manejan conforme van surgiendo.
1 Inicial / *ad hoc*	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es *ad hoc* y desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están concientes de sus responsabilidades.	No existe la conciencia de la necesidad de evaluar lo que se necesita en términos de controles de TI. Cuando se llevan a cabo, son solamente de forma *ad hoc*, a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente.
2 Repetible pero Intuitivo	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consistentes ni tienen prioridades. Los empleados pueden no estar concientes de sus responsabilidades.	La evaluación de la necesidad de control sucede solo cuando se necesita para ciertos procesos seleccionados de TI para determinar el nivel actual de madurez del control, el nivel meta que debe ser alcanzado, y las brechas existentes. Se utiliza un enfoque de taller informal, que involucra a los gerentes de TI y al equipo interesado en el proceso, para definir un enfoque adecuado hacia el control para los procesos, y para generar un plan de acción acordado.
3 Definido	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están concientes de sus responsabilidades de control.	Los procesos críticos de TI se identifican con base en impulsores de valor y de riesgo. Se realiza un análisis detallado para identificar requisitos de control y la causa raíz de las brechas, así como para desarrollar oportunidades de mejora. Además de facilitar talleres, se usan herramientas y se realizan entrevistas para apoyar el análisis y garantizar que los dueños de los procesos de TI son realmente los dueños e impulsan al proceso de evaluación y mejora.
4 Administrado y Medible	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consistente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.	Se define de forma periódica qué tan críticos son los procesos de TI con el apoyo y acuerdo completo por parte de los dueños de los procesos correspondientes. La evaluación de los requisitos de control se basa en las políticas y en la madurez real de estos procesos, siguiendo un análisis meticuloso y medido, involucrando a los Interesados (Stakeholders) clave. La rendición de cuentas sobre estas evaluaciones es clara y está reforzada. Las estrategias de mejora están apoyadas en casos de negocio. El desempeño para lograr los resultados deseados se supervisa de forma periódica. Se organizan de forma ocasional revisiones externas de control.
5 Optimizado	Un programa organizacional de riesgo y control proporciona la solución continua y efectiva a problemas de control y riesgo. El control interno y la administración de riesgos se integran a las prácticas empresariales, apoyadas con una supervisión en tiempo real, y una rendición de cuentas completa para la vigilancia de los controles, administración de riesgos, e implantación del cumplimiento. La evaluación del control es continua y se basa en auto-evaluaciones y en análisis de brechas y de causas raíz. Los empleados se involucran de forma pro-activa en las mejoras de control.	Los cambios en el negocio toman en cuenta que tan críticos son los procesos de TI, y cubren cualquier necesidad de re-evaluar la capacidad del control de los procesos. Los dueños de los procesos realizan auto-evaluaciones de forma periódica para confirmar que los controles se encuentran en el nivel correcto de madurez para satisfacer las necesidades del negocio, y toman en cuenta los atributos de madurez para encontrar maneras de hacer que los controles sean más eficientes y efectivos. La organización evalúa por comparación con las mejoras prácticas externas y busca asesoría externa sobre la efectividad de los controles internos. Para procesos críticos, se realizan evaluaciones independientes para proporcionar seguridad de que los controles se encuentran al nivel deseado de madurez y funcionan como fue planeado.

Página dejada en blanco intencionadamente.

APÉNDICE IV
COBIT 4.1 MATERIAL DE REFERENCIA PRIMARIO

APÉNDICE IV – COBIT 4.1 MATERIAL DE REFERENCIA PRIMARIO

Para las actividades de desarrollo y actualización de COBIT ya mencionadas, se usó una amplia base de más de 40 estándares de TI, marcos de trabajo, directrices y mejores prácticas para garantizar la integridad de COBIT en la resolución de todas las áreas de gobierno y control de TI.

Debido a que COBIT se enfoca en el *qué* se requiere para lograr una administración y control adecuados de TI, se posiciona a un alto nivel. Los estándares de TI más detallados y las mejores prácticas se encuentran a un nivel de detalle inferior describiendo *cómo* gestionar y controlas específicos aspectos de TI. COBIT actúa como integrador de estos diferentes materiales de guía, resumiendo los objetivos clave bajo un marco de trabajo paraguas que también enlaza los requerimientos de gobierno y negocio.

Para esta versión actualizada de COBIT (COBIT 4.1), seis de los principales estándares mundiales relacionados con TI, marcos de trabajo y practicas como las principales referencias de soporte para garantizar una cobertura, consistencia y alineación adecuada. Estas son:

- COSO:
  Control Interno – Marco de Trabajo Integrado, 1994
  Administración de Riesgos Empresarial – Marco de Trabajo Integrado, 2004
- Oficina de Comercio Gubernamental (OGC®):
  Biblioteca de Infraestructura de TI® (ITIL®), 1999-2004
- Organización Internacional para la Estandarización:
  ISO/IEC 27000
- Instituto de Ingeniería de Software (SEI®):
  SEI Modelo de madurez de la capacidad (CMM®), 1993
  SEI Integración del modelo de madurez de la capacidad (CMMI®), 2000
- Instituto de Gestión de Proyectos (PMI®):
  Guía para el Cuerpo de Conocimiento de Gestión de Proyectos (PMBOK®), 2004
- Foro de Seguridad de Información (ISF):
  El estándar de buenas prácticas para la seguridad de la información, 2003

Referencias adicionales utilizadas en el desarrollo de COBIT 4.1 incluyen:

- *Objetivos de Control de TI para Sarbanes-Oxley: El Rol de TI en el Diseño e Implementación de Controles Internos Sobre Informes Financieros, 2ª Edición*, Instituto de Gobierno de TI, USA, 2006
- *Manual de Revisión CISA*, ISACA, 2006

Página dejada en blanco intencionadamente.

APÉNDICE V

REFERENCIAS CRUZADAS ENTRE LA 3ª EDICIÓN Y COBIT 4.1

APÉNDICE V – REFERENCIAS CRUZADAS ENTRE LA 3ª EDICIÓN DE COBIT Y COBIT 4.1

CAMBIOS A NIVEL DE MARCO DE TRABAJO

Los cambios principales al marco de trabajo de COBIT como resultado de la actualización a COBIT 4.0 son los siguientes:

- El dominio M se ha convertido ahora a ME, y significa Monitorear y Evaluar.
- M3 y M4 eran procesos de auditoría y no procesos de TI. Fueron eliminados debido a que están cubiertos de forma adecuada por un número de estándares de auditoría de TI, aunque se han proporcionado referencias dentro del marco de trabajo actualizado para enfatizar la necesidad que tiene la gerencia de usar funciones de aseguramiento.
- ME3 es el proceso relacionado con la supervisión regulatoria, el cual estaba cubierto en PO8 previamente.
- ME4 cubre el proceso de supervisión del gobierno sobre TI, conservando el propósito de COBIT de fungir como un marco de trabajo de gobierno de TI. Al posicionar ese proceso al final de la cadena, se subraya el apoyo que cada proceso previo brinda a la última meta de implementar un gobierno efectivo de TI en la empresa.
- Con la eliminación de PO8 y la necesidad de mantener la numeración para PO9 *Evaluar riesgos* y PO10 *Administrar proyectos* de modo consistente con la 3ª edición de COBIT, PO8 ahora se convierte en *Administrar la calidad*, que anteriormente era el proceso PO11. El dominio PO ahora tiene 10 procesos en lugar de 11.
- El dominio AI requirió dos cambios: la adición de un proceso de procuración y la necesidad de incluir en AI5 los aspectos de administración de versiones. El último cambio sugirió que este debería ser el último proceso en el dominio AI y por lo tanto se convirtió en AI7. El hueco que se creó en AI5 se usó para añadir el nuevo proceso de procuración. El dominio AI ahora tiene siete procesos en lugar de seis.

COBIT una actualización incremental a COBIT 4.0, incluye:

- Visión general ejecutiva mejorada.
- Explicación de metas y métricas en la sección del marco de trabajo
- Mejores definiciones de los conceptos del núcleo. Es importante mencionar que la definición de objetivo de control se ha cambiado, desplazándose mas hacia una declaración de prácticas de gestión
- Se han mejorado los objetivos de control resultado de unas prácticas de control actualizadas y la actividad de desarrollo de Val TI. Algunos objetivos de control se agruparon y / o reformularon pare evitar superposiciones y hacer la lista de objetivos de control dentro de un proceso mas consistente. Estos cambios resultan en la renumeración de los objetivos de control restantes. Algunos de los otros objetivos de control fueron reordenados para hacerlos mas orientados a la acción y consistentes en la redacción. Las revisiones especificas incluyen:
  - AI5.5 y AI5.6 que fueron combinadas en AI5.4
  - AI7.9, AI7.10 y AI7.11 que fueron combinadas en AI7.8
  - ME3 fue revisada para incluir cumplimiento con los requerimientos contractuales además de requerimientos legales y regulatorios.
- Los controles de aplicación han sido revisados para ser más efectivos, basados en el trabajo para soportar la evaluación e informe de la eficacia de los controles. Resultando en una lista de seis controles de aplicación que sustituyen a los 18 controles de aplicación de COBIT 4.0, proporcionado con mayor detalle en *Practicas de Control de COBIT, 2ª Edición*.
- Se ha mejorado la lista de metas de negocio y de metas de TI en el Apéndice I, basado en nuevas visiones obtenidas durante la investigación de validación realizada por la Universidad de Antwerp Management School (Bélgica).
- La extracción se ha expandido a proporcionar una lista de referencias rápidas de los procesos de COBIT, y el diagrama de visión general que representa los dominios revisados para incluir la referencia para el proceso y elementos de control de aplicación del marco de trabajo de COBIT.
- Las mejoras identificadas por los usuarios de COBIT (COBIT 4.0 y COBIT Online) se han revisado e incorporado de forma apropiada.

OBJETIVOS DE CONTROL DETALLADOS

Como se puede observar en la descripción anterior a nivel del marco de trabajo y en el trabajo para aclarar y enfocar el contenido de los objetivos de control, la actualización del marco de trabajo COBIT ha cambiado significativamente los objetivos de control dentro de éste. Estos componentes se han reducido de 215 a 210, porque todos los materiales genéricos ahora sólo se conservan al nivel de marco de trabajo y no se repiten en cada proceso. Así mismo, todas las referencias a controles aplicativos se movieron al marco de trabajo y los objetivos específicos de control se agregaron en nuevas declaraciones. Para apoyar la actividad de transición en relación con los objetivos de control, los siguientes dos juegos de tablas muestran las referencias cruzadas entre los nuevos y viejos objetivos de control.

DIRECTRICES GERENCIALES

Las entradas y salidas se han añadido para ilustrar lo que los procesos necesitan de otros y lo que típicamente generan. También se proporcionan actividades y responsabilidades asociadas. Las entradas y las metas de las actividades reemplazan a los factores críticos de éxito de COBIT 3ª Edición. Las métricas ahora se basan en una cascada consistente de metas de negocio, de TI, de proceso y de actividades. El juego de métricas de COBIT 3ª Edición también se reviso y mejoró para hacerlo más representativo y medible.

COBIT 4.1

Referencia Cruzada. COBIT 3ª Edición a COBIT 4.1

COBIT 3ª edición	COBIT 4.1
PO1 Definir plan estratégico para TI.	
1.1 TI Como parte del plan organizacional a corto y a largo plazo	1.4
1.2 Plan de TI a largo plazo	1.4
1.3 Plan de TI a largo plazo — enfoque y estructura	1.4
1.4 Cambios al plan de TI a largo plazo	1.4
1.5 Planeación a corto plazo para la función de TI	1.5
1.6 Comunicación de los Planes de TI	1.4
1.7 Monitoreo y evaluación de los planes de TI	1.3
1.8 Evaluación de Sistemas existentes	1.3
PO2 Definir arquitectura de información.	
2.1 Modelo de arquitectura de información	2.1
2.2 Diccionario corporativo de datos y reglas de sintaxis	2.2
2.3 Esquema de clasificación de datos	2.2
2.4 Niveles de seguridad	2.3
PO3 Determinar la dirección tecnológica.	
3.1 Planeación de la infraestructura tecnológica	3.1
3.2 Monitorear tendencias y reglamentos futuros.	3.3
3.3 Contingencia de la infraestructura tecnológica	3.1
3.4 Planes de adquisición de Hardware y software	3.1, AI3.1
3.5 Estándares tecnológicos	3.4, 3.5
PO4 Definir la organización y las relaciones De TI.	
4.1 Planeación de TI ó Comité directivo	4.3
4.2 Ubicación organizacional de la función de TI	4.4
4.3 Revisión de los logros organizacionales	4.5
4.4 Roles y responsabilidades	4.6
4.5 Responsabilidad del Aseguramiento de la calidad	4.7
4.6 Responsabilidad de la seguridad lógica y física	4.8
4.7 Propiedad y custodia	4.9
4.8 Propiedad de datos y de sistemas	4.9
4.9 Supervisión	4.10
4.10 Segregación de tareas	4.11
4.11 Equipo de trabajo de TI	4.12
4.12 Descripciones de Puesto para equipo de TI	4.6
4.13 Personal clave de TI	4.13
4.14 Políticas y procedimientos para personal subcontratado	4.14
4.15 Relaciones	4.15
PO5 Administrar la inversión en TI.	
5.1 Presupuesto operativo Anual para TI	5.3
5.2 Supervisión de costos y beneficios	5.4
5.3 Justificación de costos y beneficios	1.1, 5.3, 5.4, 5.5
PO6 Comunicar metas y dirección de la gerencia.	
6.1 Ambiente positivo de control de información	6.1
6.2 Responsabilidad de la gerencia por políticas	6.3, 6.4, 6.5
6.3 Comunicación de las políticas organizacionales	6.3, 6.4, 6.5
6.4 Recursos para implantación de políticas	6.4
6.5 Mantenimiento de políticas	6.3, 6.4, 6.5
6.6 Cumplimiento de políticas, procedimientos y estándares	6.3, 6.4, 6.5
6.7 Compromiso de calidad	6.3, 6.4, 6.5
6.8 Política de seguridad y control interno	6.2
6.9 Derechos de propiedad intelectual	6.3, 6.4, 6.5
6.10 Políticas de temas específicos	6.3, 6.4, 6.5
6.11 Comunicación de la conciencia de seguridad de TI	6.3, 6.4, 6.5
PO7 Administrar los recursos humanos.	
7.1 Reclutamiento y Selección de personal	7.1
7.2 Aptitudes del personal	7.2
7.3 Roles y responsabilidades	7.4
7.4 Entrenamiento personal	7.5
7.5 Entrenamiento cruzado o respaldos de personal	7.6
7.6 Procedimientos de acreditación de personal	7.7
7.7 Evaluaciones de desempeño del trabajo	7.8
7.8 Cambios de puesto y terminación	7.8
PO8 Garantizar el cumplimiento de los requisitos externos.	
8.1 Revisión de requisitos	ME3.1
8.2 Prácticas y procedimientos para cumplir los requisitos externos	ME3.2
8.3 Cumplimiento Ergonómico y de seguridad	ME3.1
8.4 Privacidad, propiedad Intelectual y flujo de datos	ME3.1
8.5 Comercio electrónico	ME3.1
8.6 Cumplimiento de Contratos de seguridad	ME3.1
PO9 Evaluar riesgos.	
9.1 Evaluación de riesgos de negocio	9.1, 9.2, 9.4
9.2 Enfoque de evaluación De riesgos	9.4
9.3 Identificación de riesgos	9.3
9.4 Medición de riesgos	9.1, 9.2, 9.3, 9.4
9.5 Plan de acción de riesgos	9.5
9.6 Aceptación de riesgos	9.5
9.7 Selec. de salvaguardas	9.5
9.8 Comité de evaluación de riesgos	9.1
PO10 Administrar proyectos.	
10.1 Marco de administración de proyectos	10.2
10.2 Participación del Departamento usuario en el Inicio de los proyectos	10.4
10.3 Membresía del equipo de Trabajo y responsabilidades	10.8
10.4 Definición de proyectos	10.5
10.5 Aprobación de proyectos	10.6
10.6 Aprobación de fases de proyectos	10.6
10.7 Plan maestro de proyectos	10.7
10.8 Plan de aseguramiento de calidad de sistemas	10.10
10.9 Planeación de métodos de aseguramiento	10.12
10.10 Administración formal de riesgos de proyectos	10.9
10.11 Plan de pruebas	AI7.2
10.12 Plan de entrenamiento	AI7.1
10.13 Plan de revisión Post-implantación	10.14 (parte)
PO11 Administrar la calidad.	
11.1 Plan general de calidad	8.5
11.2 Enfoque de aseguramiento de la calidad (QA)	8.1
11.3 Planeación de QA	8.1
11.4 Revisión de QA de la adherencia a estándares y procedimientos de TI	8.1, 8.2
11.5 Metodología de ciclo de vida (SDLC) para desarrollo de sistemas .	8.2, 8.3
11.6 Metodología SDLC Para cambios importantes a la tecnología existente	8.2, 8.3
11.7 Actualización de la Metodología SDLC	8.2, 8.3
11.8 Coordinación y comunicación	8.2
11.9 Marco de adquisición y mantenimiento para la infraestructura tecnológica	8.2
11.10 Relaciones con Implantadores terceros	8.2, DS2.3
11.11 Estándares de Documentación de programas	AI4.2, AI4.3, AI4.4
11.12 Estándares de prueba de programas	AI7.2, AI7.4
11.13 Estándares de prueba de sistemas	AI7.2, AI7.4
11.14 Pruebas paralelas/piloto	AI7.2, AI7.4
11.15 Documentación de pruebas de sistemas	AI7.2, AI7.4
11.16 Evaluación QA de la adherencia a los estándares de desarrollo	8.2
11.17 Revisión QA del logro De los objetivos de TI	8.2
11.18 Métricas de calidad	8.6
11.19 Reportes de revisiones QA	8.2

APÉNDICE V

COBIT 3ª edición	COBIT 4.1
AI1 Identificar soluciones automatizadas.	
1.1 Definición de requerimientos de información	1.1
1.2 Formular cursos Alternativos de acción	1.3, 5.1, PO1.4
1.3 Formulación de estrategia de adquisiciones	1.3, 5.1, PO1.4
1.4 Requisitos de servicio de terceros	5.1, 5.3
1.5 Estudio de factibilidad tecnológica	1.3
1.6 Estudio de factibilidad económica	1.3
1.7 Arquitectura de la información	1.3
1.8 Reportes de análisis de riesgos	1.2
1.9 Controles de seguridad rentables	1.1, 1.2
1.10 Diseño de pistas de auditoría	1.1, 1.2
1.11 Ergonomía	1.1
1.12 Selección de software de sistemas	1.1, 1.3
1.13 Control de procuración	5.1
1.14 Adquisición de productos de software	5.1
1.15 Mantenimiento de software de terceros	5.4
1.16 Programación de aplicaciones subcontratadas	5.4
1.17 Aceptación de instalaciones	5.4
1.18 Aceptación de la Tecnología	3.1, 3.2, 3.3, 5.4
AI2 Adquirir y mantener software aplicativo.	
2.1 Métodos de diseño	2.1
2.2 Cambios importantes a Sistemas existentes	2.1, 2.2, 2.6
2.3 Aprobación del diseño	2.1
2.4 Definición y documentación de requisitos De archivo	2.2
2.5 Especificaciones de	2.2

COBIT 3ª edición	COBIT 4.1
programas	
2.6 Diseño de recolección de datos fuente	2.2
2.7 Definición y documentación de requisitos de entradas	2.2
2.8 Definición de interfases	2.2
2.9 Interfaz usuario-máquina	2.2
2.10 Definición y documentación de requisitos de procesamiento	2.2
2.11 Definición y documentación de requisitos De salidas	2.2
2.12 Capacidad de control	2.3, 2.4
2.13 Disponibilidad como Factor clave de diseño	2.2
2.14 Disposiciones de integridad de TI en software de programas aplicativos	2.3, DS11.5
2.15 Pruebas de software	2.8, 7.4
2.16 Materiales de apoyo y Referencia para el usuario	4.3. 4.4
2.17 Re-evaluación del Diseño del sistema	2.2
AI3 Adquirir y mantener infraestructura de software.	
3.1 Evaluación de nuevo hardware y software	3.1, 3.2, 3.3
3.2 Mantenimiento preventivo de hardware	DS13.5
3.3 Seguridad del software De sistemas	3.1, 3.2, 3.3
3.4 Instalación del software De sistemas	3.1, 3.2, 3.3
3.5 Mantenimiento del Software de sistemas	3.3
3.6 Controles de cambio para el software de sistemas	6.1, 7.3
3.7 Uso y vigilancia de las utilerías del sistema	3.2, 3.3, DS9.3
AI4 Elaborar y mantener procedimientos.	
4.1 Reqs operativos y niveles de servicio	4.1

COBIT 3ª edición	COBIT 4.1
4.2 Manual de procedimientos de usuario	4.2
4.3 Manual de operaciones	4.4
4.4 Materiales de entrenamiento	4.3, 4.4
AI5 Instalar y acreditar sistemas.	
5.1 Entrenamiento	7.1
5.2 Dimensionar desempeño De software aplicativo	7.6, DS3.1
5.3 Plan de implantación	7.2, 7.3
5.4 Conversión de sistemas	7.5
5.5 Conversión de datos	7.5
5.6 Estrategias y planes de	7.2
5.7 Pruebas de cambios	7.4, 7.6
5.8 Criterios y desempeño de de pruebas paralela./piloto	7.6
5.9 Pruebas de acept. final	7.7
5.10 Pruebas y acreditación de seguridad	7.6
5.11 Pruebas operativas	7.6
5.12 Cambio producción	7.8
5.13 Evaluación de satisfacción de los requerimientos del usuario	7.9
5.14 Revisión de la gerencia post-implantación	7.9
AI6 Administrar cambios.	
6.1 Inicio y control de solicitudes de cambio	61, 6.4
6.2 Evaluación de impacto	6.2
6.3 Control de cambios	7.9
6.4 Cambios de emergencia	6.3
6.5 Documentación y requerimientos	6.5
6.6 Mantenimiento autorizado	DS5.3
6.7 Política De liberación de software	7.9
6.8 Distribución de software	7.9

COBIT 3ª edición	COBIT 4.1
DS1 Definir y administrar niveles de servicio.	
1.1 Marco para acuerdos de (SLA) niveles de servicio	1.1
1.2 Aspectos de los SLAs	1.3
1.3 Procesos de desempeño	1.1
1.4 Vigilancia y reportes	1.5
1.5 Revisión de SLAs y contratos	1.6
1.6 Componentes cobrables	1.3
1.7 Programa de mejora de servicios	1.6
DS2 Administrar servicios de terceros.	
2.1 Interfases con proveedores	2.1
2.2 Relaciones con dueños	2.2
2.3 Contratos de terceros	AI5.2
2.4 Aptitudes de terceros	AI5.3
2.5 Sub-contrataciones	AI5.2
2.6 Continuidad de servicios	2.3
2.7 Relaciones de seguridad	2.3
2.8 Vigilancia	2.4
DS3 Admin. De desempeño y capacidad.	
3.1 Requisitos de disponibilidad Y desempeño	3.1
3.2 Plan de disponibilidad	3.4
3.3 Vigilancia y reportes	3.5

COBIT 3ª edición	COBIT 4.1
3.4 Herramientas de modelaje	3.1
3.5 Admin. Pro-activa de desempeño	3.3
3.6 Pronósticos de carga de trabajo	3.3
3.7 Admin. de la capacidad de los recursos	3.2
3.8 Disponibilidad de recursos	3.4
3.9 Cronograma de recursos	3.4
DS4 Garantizar servicio continuo.	
4.1 Marco de continuidad de TI	4.1
4.2 Plan de continuidad de TI estrategia y filosofía	4.1
4.3 Contenido del plan de continuidad de TI	4.2
4.4 Minimizar requisitos de continuidad de TI	4.3
4.5 Dar mtto. al plan de continuidad de TI	4.4
4.6 Pruebas del plan de continuidad de TI	4.5
4.7 Entrenamiento en el plan de continuidad de TI	4.6
4.8 Distribución del plan de continuidad de TI	4.7
4.9 Procs. de respaldo para	4.8

COBIT 3ª edición	COBIT 4.1
proceso alternativo del depto. usuario	
4.10 Recursos críticos de TI	4.3
4.11 Sitio y hardware de respaldo	4.8
4.12 Almac. de respaldo fuera de sitio	4.9
4.13 Procs de conclusión	4.10
DS5 Garantizar seguridad de sistemas.	
5.1 Administrar medidas de seguridad.	5.1
5.2 Identificación, autenticación y acceso	5.3
5.3 Seguridad de acceso en línea a datos	5.3
5.4 Admin. de cuentas de usuarios	5.4
5.5 Revisión gerencial de cuentas de usuarios	5.4
5.6 Control de las cuentas por parte del usuario	5.4, 5.5
5.7 Supervisión de seguridad	5.5
5.8 Clasificación de datos	PO2.3
5.9 Administración de identificación central y derechos de acceso	5.3

COBIT 4.1

COBIT 3ª edición	COBIT 4.1
5.10 Reportes de actividades de violaciones y seguridad	5.5
5.11 Manejo de incidentes	5.6
5.12 Re-acreditación	5.1
5.13 Contrapartes	5.3, AC6
5.14 Autorización de transacciones	5.3
5.15 No-repudio	5.11
5.16 Ruta confiable	5.11
5.17 Protección de funciones de seguridad	5.7
5.18 Admin. de claves criptográficas	5.8
5.19 Prevención detección y corrección de software malicioso	5.9
5.20 Arqs. de firewall y conexiones con redes públicas	5.10
5.21 Protección del valor electrónico	13.4
DS6 Identificar y asignar costos.	
6.1 Componentes cobrables	6.1
6.2 Procs. de costeo	6.3
6.3 Procs. de cobro y reintegros al usuario	6.2, 6.4
DS7 Educar y entrenar a los usuarios.	
7.1 Identificación de necesidades de entrenamiento	7.1
7.2 Org. de entrenamiento	7.2
7.3 Entrenamiento en principios y conciencia de seguridad	PO7.4
DS8 Ayuda y asesoría a clientes.	
8.1 Atención a usuarios	8.1, 8.5
8.2 Registro de consultas de clientes	8.2, 8.3, 8.4
8.3 Escalamiento de consultas de clientes	8.3
8.4 Supervisión de acreditación	10.3
8.5 Análisis y reportes de tendencias	10.1
DS9 Administrar la configuración.	
9.1 Registro de config.	9.1
9.2 Línea base de config	9.1
9.3 Contabilización de estatus	9.3
9.4 Control de config.	9.3
9.5 Software no autorizado	9.3
9.6 Almacenamiento de software	AI3.4
9.7 Procedimientos de admin. de la config.	9.2
9.8 Responsabilidad por el software	9.1, 9.2

COBIT 3ª edición	COBIT 4.1
DS10 Admin. de problemas e incidentes.	
10.1 Sistema de admin. de problemas	10.1,10.2, 10.3,10.4
10.2 Escalamiento de problemas	10.2
10.3 Rastreo y pistas de auditoría para problemas	8.2,10.2
10.4 Autorizaciones de emergencia y accesos temporales	5.4, 12.3, AI6.3
10.5 Prioridades para procesamiento de emergencia	10.1, 8.3
DS11 Administración de datos.	
11.1 Procs. de preparación de datos	AC1
11.2 Procs.de autorización de documentos fuente	AC1
11.3 Recolección de datos en documentos fuente	AC1
11.4 Manejo de errores en documentos fuente	AC1
11.5 Retención de documentos fuente	DS11.2
11.6 Procs. de autorización para entrada de datos	AC2
11.7 Verif. de precisión, Integridad y autorización	AC3
11.8 Manejo de errores en la entrada de datos	AC2, AC4
11.9 Integridad en el procesamiento de datos	AC4
11.10 Validación y edición del procesamiento de datos	AC4
11.11 Manejo de errores en el procesamiento de datos	AC4
11.12 Manejo y retención de salidas	AC5, 11.2
11.13 Distr. de salidas	AC5, AC6
11.14 Balance y conciliación de salidas	AC5
11.15 Revisión de salidas y manejo de errores	AC5
11.16 Disposiciones de seguridad para reportes de salida	11.6
11.17 Protección de información delicada durante el traslado y la transmisión	AC6, 11.6
11.18 Protección de información delicada eliminada	11.4, AC.6
11.19 Admin. de almacenamiento	11.2
11.20 Periodos de retención y condiciones de almacenamiento	11.2

COBIT 3ª edición	COBIT 4.1
11.21 Sistema de admin. de librerías de medios	11.3
11.22 Responsabilidades del manejo de librerías de medios	11.3
11.23 Respaldo y restauración	11.5
11.24 Puestos de respaldo	11.4
11.25 Almacenamiento de respaldos	4.9, 11.3
11.26 Archivo	11.2
11.27 Protección de mensajes delicados	11.6
11.28 Autenticación e integridad	AC6
11.29 Integridad de transacciones electrónicas	5.11
11.30 Integridad continua de datos almacenados	11.2
DS12 Administrar instalaciones.	
12.1 Seguridad física	12.1, 12.2
12.2 Perfil bajo del sitio de TI	12.1, 12.2
12.3 Escolta para visitantes	12.3
12.4 Salud y seguridad del Personal	12.1,12.5, ME3.1
12.5 Protección contra factores ambientales	12.4, 12.9
12.6 Suministro de energía ininterrumpible	12.5
DS13 Administrar las operaciones.	
13.1 Procedimientos y manual de instrucciones para operaciones de procesamiento	13.1
13.2 Proceso de arranque y otra documentación de operaciones	13.1
13.3 Programación de tareas	13.2
13.4 Desviaciones de los cronogramas de tareas estándar	13.2
13.5 Continuidad de procesamiento	13.1
13.6 Bitácoras de operación	13.1
13.7 Formas especiales de salvaguarda y dispositivos de salida	13.4
13.8 Operaciones remotas	5.11

APÉNDICE V

COBIT 3ª edición	COBIT 4.1
M1 Monitorear los procesos.	
1.1 Recolectar datos de vigilancia	1.2
1.2 Evaluar desempeño	1.4
1.3 Evaluar la satisfacción del cliente	1.2
1.4 Reportes a la gerencia	1.5
M2 Evaluar suficiencia de controles internos.	
2.1 Vigilancia de controles internos	2.2
2.2 Operación oportuna de controles internos	2.1
2.3 Reportes sobre el nivel de los controles internos	2.2, 2.3
2.4 Seguridad operativa y Aseguramiento del control interno	2.4
M3 Recabar aseguramiento independiente.	
3.1 Certificación/acreditación independiente de seguridad	2.5, 4.7

COBIT 3ª edición	COBIT 4.1
y controles Internos de los servicios de TI	
3.2 Certificación/acreditación independiente de seguridad y controles internos de proveedores de servicio en tercería	2.5, 4.7
3.3 Evaluación independiente de la efectividad de los servicios de TI	2.5, 4.7
3.4 Evaluación independiente de la efectividad de proveedores de servicio en tercería	2.5, 4.7
3.5 Aseg. independiente del cumplimiento de leyes, requisitos regulatorios y compromisos contractuales	2.5, 4.7
3.6 Aseguramiento independiente del cumplimiento de leyes,	2.5, 2,6, 4.7

COBIT 3ª edición	COBIT 4.1
requisitos regulatorios y compromisos contractuales por parte de proveedores de servicio en tercería.	
3.7 Competencia de la función de aseguramiento independiente	2.5, 4.7
3.8 Participación proactiva de auditoría	2.5, 4.7
M4 Brindar auditorías independientes.	
4.1 Declaración de auditoría	2.5, 4.7
4.2 Independencia	2.5, 4.7
4.3 Ética y estándares profesionales	2.5, 4.7
4.4 Competencia	2.5, 4.7
4.5 Planeación	2.5, 4.7
4.6 Desempeño de la labor de auditoría	2.5, 4.7
4.7 Reportes	2.5, 4.7
4.8 Actividades de seguimiento	2.5, 4.7

COBIT 4.1

Referencia Cruzada: COBIT 4.1 a COBIT 3ª Edición

CobiT 4.1	CobiT 3ª Edición
PO1 Definir un plan estratégico de TI.	
1.1 Administrar el valor de TI	5.3
1.2 Alineación de TI con el negocio	Nuevo
1.3 Evaluación del desempeño y la capacidad actual	1.7, 1.8
1.4 Plan estratégico de TI	1.1, 1.2, 1.3,1.4, 1.6, AI1.2,AI1.3
1.5 Planes tácticos de TI	1.5
1.6 Administración del portafolio de TI	Nuevo
PO2 Definir la Arquitectura de la Información	
2.1 Modelo de arquitectura de información empresarial	2.1
2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	2.2
2.3 Esquema de clasificación de datos	2.3, 2.4, DS5.8
2.4 Administración de integridad	Nuevo
PO3 Determinar la Dirección Tecnológica.	
3.1 Planeación de la dirección tecnológica	3.1, 3.3, 3.4
3.2 Plan de infraestructura tecnológica	Nuevo
3.3 Monitoreo de tendencias y regulaciones futuras	3.2
3.4 Estándares tecnológicos	3.5
3.5 Consejo de arquitectura de TI	3.5
PO4 Definir los procesos, organización y relaciones de TI.	
4.1 Marco de trabajo de procesos de TI	Nuevo
4.2 Comité estratégico de TI	Nuevo
4.3 Comité directivo de TI	4.1
4.4 Ubicación organizacional de la función de TI	4.2
4.5 Estructura Organizacional	4.3
4.6 Establecimiento de roles y responsabilidades	4.4, 4.12
4.7 Responsabilidad de aseguramiento de calidad de TI	4.5
4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	4.6
4.9 Propiedad de datos y de sistemas	4.7, 4.8
4.10 Supervisión	4.9
4.11 Segregación de funciones	4.10
4.12 Personal de TI	4.11
4.13 Personal clave de TI	4.13
4.14 Políticas y procedimientos para personal contratado	4.14
4.15 Relaciones	4.15
PO5 Administrar la inversión en TI.	
5.1 Marco de trabajo para la administración financiera	Nuevo
5.2 Prioridades dentro del presupuesto de TI	Nuevo
5.3 Proceso Presupuestal	5.1, 5.3
5.4 Administración de costos de TI	5.2, 5.3
5.5 Administración de beneficios	5.3
PO6 Comunicar las aspiraciones y la dirección de la gerencia.	
6.1 Ambiente de políticas y de control	6.1
6.2 Riesgo corporativo y marco de referencia de control interno de TI	6.8
6.3 Administración de políticas para TI	6.2, 6.3, 6.5, 6.6, 6.7, 6.9,6.10, 6.11
6.4 Implantación de políticas de TI	6.2, 6.3, 6.4,6.5, 6.6, 6.7,6.9, 6.10, 6.11
6.5 Comunicación de los objetivos y la dirección de TI	6.2, 6.3, 6.5,6.6, 6.7, 6.9, 6.10, 6.11
PO7 Administrar recursos humanos de TI.	
7.1 Reclutamiento y retención del personal	7.1
7.2 Competencias del personal	7.2
7.3 Asignación de roles	Nuevo
7.4 Entrenamiento del personal de TI	7.3, DS7.3
7.5 Dependencia sobre los individuos	7.4
7.6 Procedimientos de investigación del personal	7.5
7.7 Evaluación del desempeño del empleado	7.6
7.8 Cambios y terminación de trabajo	7.7, 7.8
PO8 Administrar la calidad.	
8.1 Sistema de administración de calidad	11.2, 11.3,11.4
8.2 Estándares y prácticas de calidad	11.5, 11.6,11.7, 11.8,11.9,
	11.10, 11.16, 11.17,11.19
8.3 Estándares de desarrollo y de adquisición	11.5, 11.6,11.7
8.4 Enfoque en el cliente de TI	Nuevo
8.5 Mejora continua	Nuevo
8.6 Medición, monitoreo y revisión de la calidad	11.18
PO9 Evaluar y administrar los riesgos de TI.	
9.1 Alineación de la administración de riesgos de TI y del negocio	9.1, 9.4, 9.8
9.2 Establecimiento del contexto del riesgo	9.1, 9.4
9.3 Identificación de eventos	9.3, 9.4
9.4 Evaluación de riesgos de TI	9.1, 9.2, 9.4
9.5 Respuesta a los riesgos	9.5, 9.6, 9.7
9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	Nuevo
PO10 Administrar proyectos.	
10.1 Marco de trabajo para la administración de programas	Nuevo
10.2 Marco de trabajo para la administración de proyectos	10.1
10.3 Enfoque de administración de proyectos	Nuevo
10.4 Compromiso de los interesados	10.2
10.5 Declaración de alcance del proyecto	10.4
10.6 Inicio de las fases del proyecto	10.5, 10.6
10.7 Plan integrado del proyecto	10.7
10.8 Recursos del proyecto	10.3
10.9 Administración de riesgos del proyecto	10.10
10.10 Plan de calidad del proyecto	10.8
10.11 Control de cambios del proyecto	Nuevo
10.12 Planeación del proyecto y métodos de aseguramiento	10.9
10.13 Medición del desempeño, reportes y monitoreo del proyecto	Nuevo
10.14 Cierre del proyecto	10.13 (part)

CobiT 4.1	CobiT 3ª Edición
AI1 Identificar soluciones automatizadas	
1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio	1.1, 1.9, 1.10, 1.11, 1.12
1.2 Reporte de análisis de riesgos	1.8, 1.9, 1.10
1.3 Estudio de factibilidad y formulación de cursos de acción alternativos	1.3, 1.7, 1.12
1.4 Requerimientos, decisión de factibilidad y aprobación	Nuevo

CobiT 4.1	CobiT 3ª Edición
AI2 Adquirir y mantener software aplicativo.	
2.1 Diseño de alto nivel	2.1, 2.2
2.2 Diseño detallado	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 Control y posibilidad de auditar las aplicaciones	2.12, 2.14
2.4 Seguridad y disponibilidad de las aplicaciones	2.12

CobiT 4.1	CobiT 3ª Edición
2.5 Configuración e implantación de software aplicativo adquirido	Nuevo
2.6 Actualizaciones importantes en sistemas existentes	2.2
2.7 Desarrollo de software aplicativo	Nuevo
2.8 Aseguramiento de la calidad del software	2.15
2.9 Administración de los requerimientos de aplicaciones	Nuevo
2.10 Mantenimiento de	Nuevo

APÉNDICE V

CobiT 4.1	CobiT 3ª Edición
software aplicativo	
AI3 Adquirir y mantener infraestructura tecnológica.	
3.1 Plan de adquisición de infraestructura tecnológica	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 Protección y disponibilidad del recurso de infraestructura	1.18, 3.1, 3.3, 3.4, 3.7
3.3 Mantenimiento de la infraestructura	1.18, 3.1, 3.3,3.4, 3.5, 3.7
3.4 Ambiente de prueba de factibilidad	Nuevo
AI4 Facilitar la operación y el uso.	
4.1 Plan para soluciones de operación	4.1
4.2 Transferencia de conocimiento a la gerencia del negocio	PO11.11, 4.2
4.3 Transferencia de conocimiento a usuarios finales	PO11.11,2.16, 4.4
4.4 Transferencia de conocimiento al personal de operaciones y soporte	PO11.11,2.16, 4.3, 4.4

CobiT 4.1	CobiT 3ª Edición
AI5 Adquirir recursos de TI.	
5.1 Control de adquisición	1.2, 1.3, 1.4, 1.13, 1.14
5.2 Administración de contratos con proveedores	DS2.3, DS2.5
5.3 Selección de proveedores	1.4, DS2.4
5.4 Adquisición de recursos de TI	1.15, 1.16, 1.17, 1.18
AI6 Administrar cambios.	
6.1 Estándares y procedimientos para cambios	3.6, 6.1
6.2 Evaluación de impacto, priorización y autorización	6.2
6.3 Cambios de emergencia	DS10.4, 6.4
6.4 Seguimiento y reporte del estatus de cambio	6.1
6.5 Cierre y documentación del cambio	6.5
AI7 Instalar y acreditar soluciones y cambios.	
7.1 Entrenamiento	PO10.11, PO10.12, 5.1
7.2 Plan de prueba	PO10.11, PO11.12,

CobiT 4.1	CobiT 3ª Edición
	PO11.13, PO11.14, PO11.15, 5.3, 5.6
7.3 Plan de implantación	3.6, 5.3
7.4 Ambiente de prueba	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 Conversión de sistemas y datos	5.4, 5.5
7.6 Prueba de cambios	5.2, 5.7, 5.8, 5.10, 5.11
7.7 Prueba de aceptación final	5.9
7.8 Promoción a producción	5.12
7.9 Revisión posterior a la implantación	5.13, 5.14

CobiT 4.1	CobiT 3ª Edición
DS1 Definir y administrar los niveles de servicio.	
1.1 Marco de trabajo de la administración de los niveles de servicio	1.1, 1.3
1.2 Definición de servicios	Nuevo
1.3 SLA	1.2, 1.6
1.4 OLA	Nuevo
1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	1.4
1.6 Revisión de los SLA y de los contratos	1.5, 1.7
DS2 Administrar los servicios de terceros.	
2.1 Identificación de todas las relaciones con proveedores	2.1
2.2 Gestión de relaciones con proveedores	2.2
2.3 Administración de riesgos del proveedor	PO11.10, 2.6,2.7
2.4 Monitoreo del desempeño del proveedor	2.8
DS3 Administrar el desempeño y la capacidad.	
3.1 Planeación del desempeño y la capacidad	AI5.2, 3.1, 3.4
3.2 Capacidad y desempeño actual	3.7
3.3 Capacidad y desempeño futuros	3.5, 3.6
3.4 Disponibilidad de recursos de TI	3.2, 3.8, 3.9
3.5 Monitoreo y reporte	3.3
DS4 Garantizar la continuidad del servicio.	
4.1 Marco de trabajo de continuidad de TI	4.1, 4.2
4.2 Planes de continuidad de TI	4.3

CobiT 4.1	CobiT 3ª Edición
4.3 Recursos críticos de TI	4.4, 4.10
4.4 Mantenimiento del plan de continuidad de TI	4.5
4.5 Pruebas del plan de continuidad de TI	4.6
4.6 Entrenamiento del plan de continuidad de TI	4.7
4.7 Distribución del plan de continuidad de TI	4.8
4.8 Recuperación del plan de continuidad de TI	4.9, 4.11
4.9 Almacenamiento de respaldos fuera de las instalaciones	4.12, 11.25
4.10 Revisión post reanudación	4.13
DS5 Garantizar la seguridad de los sistemas.	
5.1 Administración de la seguridad de TI	5.1, 5.12
5.2 Plan de seguridad de TI	Nuevo
5.3 Administración de identidad	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 Administración de cuentas de usuario	5.4, 5.5, 5.6,5.13, 10.4
5.5 Pruebas, vigilancia y monitoreo de la seguridad	5.6, 5.7, 5.10
5.6 Definición de incidente de seguridad	5.11
5.7 Protección de la tecnología de seguridad	5.17
5.8 Administración de llaves criptográficas	5.18
5.9 Prevención, detección y corrección de software malicioso	5.19
5.10 Seguridad de la red	5.20
5.11 Intercambio de datos sensitivos	5.15, 5.16, 11.29, 13.8
DS6 Identificar y asignar costos.	
6.1 Definición de servicios	6.1
6.2 Contabilización de TI	6.3

CobiT 4.1	CobiT 3ª Edición
6.3 Modelación de costos y cargos	6.2
6.4 Mantenimiento del modelo de costos	6.3
DS7 Educar y entrenar a los usuarios.	
7.1 Identificación de necesidades de entrenamiento y educación	7.1
7.2 Impartición de entrenamiento y educación	7.2
7.3 Evaluación del entrenamiento recibido	Nuevo
DS8 Administrar la mesa de servicio y los incidentes.	
8.1 Mesa de servicios	8.1
8.2 Registro de consultas de clientes	8.2, 10.3
8.3 Escalamiento de incidentes	8.2, 8.3, 10.5
8.4 Cierre de incidentes	8.2
8.5 Análisis de tendencias	8.1
DS9 Administrar la configuración.	
9.1 Repositorio y línea base de configuración	9.1, 9.2, 9.8
9.2 Identificación y mantenimiento de elementos de configuración	9.7, 9.8
9.3 Revisión de integridad de la configuración	9.3, 9.4, 9.5
DS10 Administrar los problemas.	
10.1 Identificación y clasificación de problemas	8.5, 10.1, 10.5
10.2 Rastreo y resolución de problemas	Nuevo
10.3 Cierre de problemas	8.4, 10.1
10.4 Integración de las administraciones de cambios, configuración y problemas	10.1
DS11 Administrar los datos.	
11.1 Requerimientos del	Nuevo

COBIT 4.1

CobiT 4.1	CobiT 3ª Edición
negocio para administración de datos	
11.2 Acuerdos de almacenamiento y conservación	11.12, 11.19, 11.20, 11.26, 11.30
11.3 Sistema de administración de librerías de medios	11.21, 11.22, 11.25
11.4 Eliminación	11.18, 11.24
11.5 Respaldo y restauración	AI2.14, 11.23
11.6 Requerimientos de	11.16, 11.17,

CobiT 4.1	CobiT 3ª Edición
seguridad para la administración de datos	11.27
DS12 Administrar el ambiente físico.	
12.1 Selección y diseño del centro de datos	12.1, 12.2, 12.4
12.2 Medidas de seguridad física	12.1, 12.2
12.3 Acceso físico	10.4, 12.3
12.4 Protección contra factores ambientales	12.5
12.5 Administración de instalaciones físicas	12.4, 12.6, 12.9

CobiT 4.1	CobiT 3ª Edición
DS13 Administrar las operaciones.	
13.1 Procedimientos e instrucciones de operación	13.1, 13.2, 13.5, 13.6
13.2 Programación de tareas	13.3, 13.4
13.3 Monitoreo de la infraestructura de TI	Nuevo
13.4 Documentos sensitivos y dispositivos de salida	5.21, 13.7
13.5 Mantenimiento preventivo del hardware	AI3.2

CobiT 4.1	CobiT 3ª Edición
ME1 Monitorear y evaluar el desempeño de TI	
1.1 Enfoque del monitoreo	1.0*
1.2 Definición y recolección de datos de monitoreo	1.1, 1.3
1.3 Método de monitoreo	Nuevo
1.4 Evaluación del desempeño	1.2
1.5 Reportes al consejo directivo y a ejecutivos	1.4
1.6 Acciones correctivas	Nuevo
ME2 Monitorear y evaluar el control interno.	
2.1 Monitoreo del marco de trabajo de control interno	2.0*, 2.2
2.2 Revisiones de auditoría	2.1, 2.3
2.3 Excepciones de control	Nuevo
2.4 Control de auto evaluación	2.4

CobiT 4.1	CobiT 3ª Edición
2.5 Aseguramiento del control interno	Nuevo
2.6 Control interno para terceros	3.6
2.7 Acciones correctivas	Nuevo
ME3 Garantizar el cumplimiento con requisitos externos	
3.1 Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales	P08.1, P08.3, P08.4, P08.5,P08.6, DS12.4
3.2 Optimizar la respuesta a requerimientos externos	P08.2
3.3 Evaluación del cumplimiento con requerimientos externos	Nuevo
3.4 Aseguramiento positivo	Nuevo

CobiT 4.1	CobiT 3ª Edición
del cumplimiento	
3.5 Reportes integrados	Nuevo
ME4 Proporcionar gobierno de TI	
4.1 Establecimiento de un marco de gobierno de TI	Nuevo
4.2 Alineamiento estratégico	Nuevo
4.3 Entrega de valor	Nuevo
4.4 Administración de recursos	Nuevo
4.5 Administración de riesgos	Nuevo
4.6 Medición del desempeño	Nuevo
4.7 Aseguramiento independiente	Nuevo

* ME1.0 y ME2.0 se introdujeron en las Prácticas de Control publicadas por ITGI en 2004.

APÉNDICE VI

APROXIMACIÓN A LA INVESTIGACIÓN Y EL DESARROLLO

APÉNDICE VI – APROXIMACIÓN A INVESTIGACIÓN Y DESARROLLO

El desarrollo del contenido del marco de trabajo de COBIT es supervisado por el Comité Directivo de COBIT, formado por representantes internacionales de la industria, la academia, el gobierno corporativo, gobierno de TI, aseguramiento, control y seguridad de TI. Se han establecido grupos internacionales de trabajo con el propósito del aseguramiento de la calidad y la revisión experimentada de los entregables provisionales del proyecto, tanto de investigación como de desarrollo. La conducción general del proyecto la realiza el Instituto de gobierno de TI (ITGI) (IT Governance Institute).

EDICIONES PREVIAS DE COBIT

Empezando con el marco de trabajo de COBIT definido en la primera edición, la aplicación de estándares internacionales, las directrices y la investigación de las mejores prácticas condujeron a la elaboración de los objetivos de control. Después se desarrollaron las directrices de auditoría para evaluar si estos objetivos de control se implementan de forma apropiada. La investigación en la primera y segunda edición incluyó la recolección y el análisis de fuentes internacionales identificadas y fue realizada por nuestros equipos en Europa (Universidad Free de Ámsterdam), los EUA (Universidad Politécnica de California) y Australia (Universidad de Nuevo Gales del Sur). Los investigadores se encargaron de la recopilación, revisión, evaluación y la adecuada inclusión de estándares técnicos internacionales, códigos de conducta, estándares de calidad, estándares profesionales de auditoría, y prácticas y requisitos industriales, conforme su relación al marco de trabajo y a los objetivos individuales de control. Después de la recolección y el análisis, los investigadores se enfrentaron al reto de examinar cada dominio y proceso a profundidad, y sugerir objetivos de control nuevos o modificados aplicables a ese proceso de TI en particular. La consolidación de los resultados la realizó el Comité Directivo de COBIT.

El proyecto de la 3ª Edición de COBIT consistió en el desarrollo de directrices gerenciales y de la actualización de la 2ª Edición de COBIT con base en referencias internacionales nuevas y corregidas. Además, el marco de trabajo de COBIT se revisó y se mejoró para apoyar un mejor control administrativo, introducir la administración del desempeño y evolucionar más aún el gobierno de TI. Para proporcionar a la gerencia una aplicación del marco de trabajo, de tal forma que pueda evaluar y tomar decisiones de implantación y mejora de los controles sobre su información y sobre la tecnología relacionada, así como medir el desempeño, las directrices de administración incluyen modelos de madurez, factores críticos de éxito, KGIs y KPIs relacionados con los objetivos de control.

Las directrices gerenciales se elaboraron usando un panel mundial de 40 expertos provenientes de la academia, del gobierno y de la profesión de gobierno, aseguramiento, control y seguridad de TI. Estos expertos participaron en un taller residencial dirigido por facilitadores profesionales, usando directrices de desarrollo definidas por el comité directivo de COBIT. El taller recibió un fuerte apoyo del Grupo Gartner y de PricewaterhouseCoopers, quienes brindaron no solo un liderazgo de pensamiento, sino que también enviaron a varios de sus expertos en control, administración del desempeño y seguridad de información. Los resultados del taller fueron bosquejos de modelos de madurez, CSFs, KGIs y KPIs para cada uno de los 34 objetivos de alto nivel de COBIT. El aseguramiento de la calidad de los entregables iniciales fue conducido por el comité directivo de COBIT y los resultados se publicaron en el sitio web de ISACA. El documento de directrices gerenciales ofreció un nuevo conjunto de herramientas orientadas a la administración, mientras que al mismo tiempo brindaron integración y consistencia con el marco de trabajo de COBIT.

La actualización de los objetivos de control en la 3ª Edición de COBIT, con base en referencias internacionales nuevas y corregidas, fue realizada por miembros de los capítulos de ISACA, bajo la dirección de los miembros del Comité Directivo de COBIT. La intención no fue realizar un análisis global de todo el material o re-elaborar los objetivos de control, sino proporcionar un proceso de actualización creciente. Los resultados de la elaboración de las directrices gerenciales se usaron entonces para corregir el marco de trabajo de COBIT, en especial las consideraciones, metas y declaraciones facilitadores de los objetivos de control de alto nivel. La 3ª edición de COBIT se publicó en Julio del 2000.

LA ÚLTIMA ACTIVIDAD DEL PROYECTO DE ACTUALIZACIÓN

En su esfuerzo por evolucionar de forma continua el cuerpo de conocimiento de COBIT, El Comité Directivo de COBIT dio inicio en los últimos dos años a actividades de investigación sobre varios aspectos detallados de COBIT. Estos proyectos de investigación focalizados contemplaron a los componentes de los objetivos de control y a las directrices gerenciales. Algunas áreas específicas que se abarcaron se listan a continuación:

Investigación de los Objetivos de Control

- COBIT— Alineación de abajo hacia arriba del gobierno de TI.
- COBIT— Alineación de arriba hacia abajo del gobierno de TI.
- COBIT y otros estándares detallados—Equivalencias detalladas entre COBIT y ITIL, CMM, COSO, PMBOK, *Los estándares de Buenas Practicas para la Seguridad de la Información* de ISF y ISO 27000 para facilitar la armonización con esos estándares en idioma, definiciones y conceptos.

Investigación de las Directrices Gerenciales

- Análisis de relaciones causales KGI-KPI
- Revisión de la calidad de los KGIs/KPIs/CSFs—con base en el análisis de reacciones causales de los KPI/KGI, separando los CSFs (factores críticos de éxito), en "lo que se necesita de otros" y en "lo que usted necesita hacer por usted mismo"
- Análisis detallado de los conceptos de métricas—Elaboración detallada con expertos en métricas para mejorar los conceptos de éstas, por medio de la construcción de una cascada de métricas "proceso-TI-negocio" y por medio de la definición de criterios de calidad para las métricas
- Unión de las metas del negocio, las metas de TI y los procesos de TI—Investigación detallada de ocho diferentes industrias, lo que generó un entendimiento más detallado de cómo los procesos de COBIT dan soporte al logro de metas específicas de TI y, como consecuencia natural, de las metas del negocio; los resultados entonces se generalizaron.
- Revisión del contenido del modelo de madurez — Consistencia y calidad aseguradas de los niveles de madurez, entre y dentro de los procesos, incluyendo mejores definiciones de los atributos del modelo de madurez.

Todos estos proyectos fueron iniciados y supervisados por el Comité Directivo de COBIT, mientras que la administración y el seguimiento del día a día fueron ejecutados por un equipo central más pequeño de COBIT. La ejecución de la mayoría de los proyectos de investigación antes mencionados, se basó de manera considerable en la experiencia y en el equipo voluntario de los miembros de ISACA, en los usuarios de COBIT, y en consultores y académicos expertos. Se establecieron grupos locales de desarrollo en Bruselas (Bélgica), Londres (Inglaterra), Chicago (Illinois, EUA), Canberra (Territorio capital Australiano), Ciudad del Cabo (Sudáfrica), Washington (DC, EUA) y Copenhague (Dinamarca), en donde se reunieron en promedio de 5 a 10 usuarios de COBIT, dos o tres veces al año, para trabajar sobre investigaciones específicas o para revisar las tareas asignadas por el equipo central de COBIT. Además, algunos proyectos específicos de investigación se asignaron a escuelas de negocio, tales como la Escuela de Administración de Amberes (UAMS, por sus siglas en inglés) y la Universidad de Hawai.

Los resultados de estos esfuerzos de investigación, junto con la retroalimentación proporcionada por los usuarios de COBIT a lo largo de los años, y los problemas observados durante el desarrollo de nuevos productos como las prácticas de control, se han introducido al proyecto principal de COBIT para actualizar y mejorar los objetivos de control de COBIT, las directrices gerenciales y el marco de trabajo. Se condujeron dos laboratorios importantes, cada uno con la participación de más de 40 expertos en gobierno, administración y control de TI (administradores, consultores, académicos y auditores) provenientes de todo el mundo, para revisar y para actualizar a fondo los objetivos de control y el contenido de las directrices gerenciales. Grupos más pequeños adicionales trabajaron para refinar o finalizar los productos significativos generados en estos importantes eventos.

El borrador final estuvo sujeto a un proceso de revisión con exposición completa con 100 interesados aproximadamente. Los numerosos comentarios recibidos fueron analizados en un taller de revisión final por el Comité Directivo de COBIT.

El Comité Directivo de COBIT, el equipo central de COBIT e ITGI procesaron los resultados de estos talleres, para crear el nuevo material de COBIT disponible en este volumen. La existencia de COBIT Online® significa que hoy en día existe la tecnología para mantener actualizado el contenido central de COBIT de forma más sencilla, y este recurso se utilizará como el repositorio maestro del contenido de COBIT. Se le dará mantenimiento con los comentarios provenientes de la base de usuarios, así como con revisiones periódicas de áreas de contenido específico. Se generarán publicaciones periódicas (en papel y electrónicas) para dar soporte a las referencias fuera de línea hacia el contenido de COBIT.

APÉNDICE VII
GLOSARIO

APÉNDICE VII - GLOSARIO

Actividad—Las medidas principales tomadas para operar el proceso COBIT.

Administración de la configuración—El control de cambios realizados a un conjunto de componentes de la configuración a lo largo del ciclo de vida del sistema.

Administración del desempeño—La capacidad de administrar cualquier tipo de medición incluyendo mediciones de empleados, equipo, proceso, operativas o financieras. El término denota un control de ciclo cerrado y la vigilancia periódica de la medición.

Análisis de causa raíz—Proceso de aprendizaje a partir de las consecuencias, típicamente de los errores y problemas.

Arquitectura de la información—Ver arquitectura de TI.

Arquitectura de TI—Un marco integrado para evolucionar o dar mantenimiento a TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

Arquitectura empresarial para TI—Respuesta en la entrega de TI, provista por procesos claramente definidos usando sus recursos (aplicaciones, información, infraestructura y personas).

Arquitectura empresarial—Mapa de rutas tecnológicas orientada al negocio para el logro de las metas y objetivos de negocio.

Atención al usuario—El único punto de contacto dentro de la organización de TI para los usuarios de los servicios prestados por TI.

Autenticación—El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas.

Capacidad—Contar con los atributos necesarios para realizar o lograr.

CEO—Director ejecutivo.

CFO—Director financiero.

CIO—Director de información [algunas veces Director de Tecnología (CTO, por sus siglas en inglés)].

Cliente—Una persona o una entidad externa o interna que recibe los servicios empresariales de TI

Comité estratégico de TI—Comité al nivel del Consejo Directivo para garantizar que el consejo participe en las principales decisiones del tema de TI.

Componente de la configuración (CI) — Componente de una infraestructura—o un artículo, como una solicitud de cambio, asociado con una infraestructura—la cual está (o estará) bajo el control de la administración de configuraciones. Los CIs pueden variar ampliamente en complejidad, tamaño y tipo, desde un sistema completo (incluyendo todo el hardware, software y documentación) hasta un solo módulo o un componente menor de hardware.

Continuidad—Prevenir, mitigar y recuperarse de una interrupción. Los términos “planear la reanudación del negocio”, “planear la recuperación después de un desastre” y “planear contingencias” también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad.

Control aplicativo—Un conjunto de controles integrados dentro de las soluciones automatizadas (aplicaciones).

Control de accesos —El proceso que limita y controla el acceso a los recursos de un sistema computacional; un control lógico o físico diseñado para brindar protección contra la entrada o el uso no autorizados.

Control de detección—Un control que se usa para identificar eventos (indeseables o deseados), errores u otras ocurrencias con efecto material sobre un proceso o producto final, de acuerdo a lo definido por la empresa.

Control general—También control general de TI. Un control que se aplica al funcionamiento general de los sistemas de TI de la organización y a un conjunto amplio de soluciones automatizadas (aplicaciones).

Control Interno —Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos

Control preventivo—Un control interno que se usa para prevenir eventos indeseables, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización.

Control—Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados

COSO—Comité de organizaciones patrocinadoras de la comisión Treadway. Estándar aceptado a nivel internacional para el gobierno corporativo. Ver www.coso.org.

CSF—Factor crítico de éxito (FCE).

DCO—Objetivos de control detallados. Los DCOs son componentes de un objetivo de control en particular.

Declaración de auditoría—Documento que define el propósito, la autoridad y la responsabilidad de la actividad de auditoría interna, aprobado por el consejo.

Desempeño—La implantación real o el logro de un proceso.

Diccionario de datos empresarial—El nombre, tipo, rango de valores, fuente, sistema de registro, y autorización de acceso para cada elemento de datos utilizado en la empresa. Indica cuáles programas aplicativos usan esos datos, de tal forma que cuando se contemple una estructura de datos, se pueda generar una lista de los programas afectados. Ver PO2.2.

Diccionario de datos—Un conjunto de meta-datos que contiene definiciones y representaciones de elementos de datos.

Directriz—La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento.

Dominio—Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI

Dueños de datos—Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados

Empresa—Un grupo de individuos que trabajan juntos para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, entidad de caridad o fondo.

Esquema de clasificación de datos—Un esquema empresarial para clasificar los datos por factores tales como criticidad, sensibilidad y propiedad.

Estándar—Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden Implementar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.

Evaluación por comparación (Benchmarking)—Un proceso utilizado en administración, en particular en la administración estratégica, en el cual las compañías evalúan varios aspectos de sus procesos de negocio con respecto a las mejores prácticas, por lo general dentro de su propia industria.

Gobierno—El método por medio del cual una organización es dirigida, administrada o controlada.

Incidente—Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

Infraestructura—La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

ISO 17799—Código de práctica para la administración de la seguridad de la información de la Organización Internacional para la Estandarización (ISO).

ISO 27001—Gestión de Seguridad de la Información- Especificación con guía para su uso; la sustituta a la BS7799-2. Ideada para proporcionar los fundamentos en auditoria a terceros e armonización con otros estándares, tales como ISO/IEC 9001 y 14001.

ISO 9001:2000—Código de práctica para la administración de la calidad de la Organización internacional para la Estandarización (ISO). El ISO 9001:2000 especifica los requisitos para un sistema de administración de calidad para cualquier organización que necesite demostrar su habilidad para ofrecer productos de manera consistente que satisfagan al cliente, a los requisitos regulatorios aplicables y que desee aumentar la satisfacción del cliente.

ITIL—Librería de Infraestructura de TI de la Oficina de Gobierno Gubernamental del Reino Unido (OGC).Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

KGI—Indicador clave de meta.

KPI—Indicador clave de desempeño.

Madurez—Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Marcador de puntuación balanceado—Un método para medir las actividades de una empresa en términos de su visión y estrategias, proporcionando una vista rápida e integral del desempeño del negocio a la gerencia. Es una herramienta administrativa cuyo fin es medir un negocio desde las siguientes perspectivas: financiera, del cliente, del negocio y del aprendizaje (Robert S. Kaplan y David Norton, 1992).

Marco de control—Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Marco de trabajo—Ver Marco de control.

Matriz RACI—Ilustra quién es responsable, quién debe rendir cuentas, a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar.

Métrica—Un estándar para medir el desempeño contra la meta.

Modelo de madurez de la capacidad (CMM)—El modelo de madurez de la capacidad para software (CMM), del Instituto de Ingeniería de Software (SEI), es un modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorarla madurez de su proceso de desarrollo de software.

Objetivo de control—Una declaración del resultado o propósito que se desea alcanzar al Implementar procedimientos de control en un proceso en particular.

APÉNDICE VII

OLA—Acuerdo a nivel operativo. Un acuerdo interno que cubre la prestación de servicios que da soporte a la organización de TI en su prestación de servicios.

Organización—La manera en que una empresa está estructurada.

Plan de infraestructura tecnológica—Un plan para el mantenimiento y desarrollo de la infraestructura tecnológica.

Plan estratégico de TI—Un plan a largo plazo, Ej., con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas)

Plan táctico de TI—Un plan a mediano plazo, Ej., con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados

PMBOK—Cuerpo de conocimiento de administración de proyectos, un estándar para administración de proyectos desarrollado por el Instituto de Administración de Proyectos (PMI).

PMO—Director de administración de proyectos.

Política—Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

Portafolio —Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.

Práctica de control—Mecanismo clave de control que apoya el logro de los objetivos de control por medio del uso responsable de recursos, la administración apropiada de los riesgos y la alineación de TI con el negocio

Prácticas de administración clave—Las principales prácticas de administración que el dueño del proceso debe realizar para alcanzar las metas del proceso

PRINCE2—Proyectos en un ambiente controlado, un método de administración de proyectos que cubre la administración, el control y la organización de un proyecto

Problema—Causa subyacente desconocida de uno o más incidentes

Procedimiento—Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.

Proceso de negocio—Ver Proceso.

Proceso—Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.

Programa aplicativo—Un programa que procesa los datos del negocio a lo largo de las actividades, tales como la captura, actualización o consulta de datos. Contrasta con los programas de sistemas, tales como un sistema operativo o un programa de control de redes, y con los programas utilitarios, tales como copiar (copy) o clasificar (sort).

Programa—Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.

Proveedor de servicios—Organización externa que presta servicios a la organización.

Proyecto—Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no suficiente para lograr un resultado de negocios requerido) con base en un cronograma y presupuesto acordado.

QMS—Sistema de administración de la calidad. Un sistema que describe las políticas y procedimientos necesarios para mejorar y controlar los distintos procesos que al final conducirán a un desempeño mejorado del negocio.

Resistencia—La capacidad de un sistema o red para recuperarse de forma automática de una interrupción, por lo general con un efecto reconocible mínimo.

Riesgo—El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

SDLC—Ciclo de vida del desarrollo de sistemas. Las fases utilizadas en el desarrollo o adquisición de un sistema de software. Las fases típicas incluyen al estudio de factibilidad, el estudio de los requerimientos, la definición de requerimientos, el diseño detallado, la programación, las pruebas, la instalación y la revisión post-implantación.

Segregación/separación de tareas—Un control interno básico que previene y detecta errores o irregularidades por medio de la asignación a individuos diferentes, de la responsabilidad de iniciar y registrar las transacciones y la custodia de los activos.

SLA—Acuerdo de nivel de servicio. Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado.

Tablero de control de inversión en TI—Graficar costos y retornos sobre la inversión de los proyectos de inversión en TI en términos de valor de negocio para la empresa.

Tablero de control—Una herramienta para establecer las expectativas de una organización en cada nivel y para comparar de forma continúa el desempeño contra las metas establecidas.

TCO—Costo total de la propiedad. En TI incluye:
- Coste original del ordenador y del software
- Actualizaciones de hardware y software
- Mantenimiento
- Soporte técnico
- Entrenamiento
- Ciertas actividades desarrolladas por los usuarios.

TI—Tecnología de información.

Usuario—Una persona que utiliza los sistemas empresariales.

APÉNDICE VIII - COBIT Y PRODUCTOS RELACIONADOS

El marco COBIT, en las versiones 4.0 y superiores, incluye todos los siguientes:

- Marco de trabajo – Explica como COBIT organiza la gestión de gobierno de TI y los objetivos de control y las mejores prácticas por dominios de TI y procesos y los enlaza a requerimientos de negocio.
- Descripciones de procesos – Incluyen 34 procesos de TI cubriendo las áreas de responsabilidad de TI desde inicio a fin.
- Objetivos de control – Proporcionan las mejores practicas genéricas de los objetivos de gestión para los procesos de TI
- Directrices Gerenciales – Ofrece herramientas para ayudar a asignar responsabilidad, medición del desempeño, y benchmark y brechas de direccionamiento en capacidad.
- Modelos de madurez – Proporciona perfiles de procedimientos de TI describiendo posibles estados actuales y futuros.

En los años desde su inicio, el núcleo de contenido de COBIT ha continuado para evolucionar, y el número de trabajos derivados basados en COBIT ha aumentado. Lo siguiente son las publicaciones actuales derivadas de COBIT:

- *Board Briefing on IT Governance, 2nd Edition* – Diseñado para ayudar a los ejecutivos a comprender porque el gobierno TI es importante, cuales son sus preguntas y cual es su responsabilidad para la gestión.
- COBIT Online – Permite a los usuarios personalizar una versión de COBIT a su propia empresa, entonces almacenar y manipular que versión desea. Ofrece en línea, encuestas en tiempo real, preguntas resueltas frecuentes, comparativas y lugares de discusión para compartir experiencias y cuestiones.
- *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* – Proporciona una guía sobre los riesgos a evitar y el valor a ganar desde la implementación de los objetivos de control, y instrucción de cómo implementar el objetivo. Las prácticas de control son muy recomendadas para el uso con la guía de implementación de Gobierno de TI: Utilizando COBIT y Val TI, 2ª edición.
- *IT Assurance Guide: Using COBIT* -Proporciona guía de cómo COBIT puede emplearse para soportar una variedad de actividades de aseguramiento y ofrece pasos de prueba sugeridos para todos los procesos de TI de COBIT y objetivos de control. Reemplaza la información en las guías de Auditoria para auditar y asesorar por si mismo contra los objetivos de control en COBIT 4.1
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition* - Proporciona guía sobre como asegurar cumplimiento para el entorno de TI basado en el control de los objetivos de control.
- *IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition* - Proporciona un mapa ruta genérico para la implementación de gobierno de TI empleando los recursos COBIT y Val TI y un kit de herramientas de soporte.
- COBIT *Quickstart* – proporciona una línea base de control para lar organizaciones más pequeñas y un posible primer paso para las grandes empresas.
- *COBIT Security Baseline*– Enfocado en los pasos esenciales para implementar la seguridad de la información dentro de la empresa. La segunda edición esta en desarrollo en el momento de escribir este documento.
- Mapeos de COBIT – actualmente publicados 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 ISO/IEC 17799:2000 With COBIT, 2nd Edition*
  - *COBIT Mapping: Mapping of PMBOK With COBIT 4.0*
  - *COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0*
  - *COBIT Mapping: Mapping of ITIL With COBIT 4.0*
  - *COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* - Presenta la seguridad de la información en términos de negocio y contiene herramientas y técnicas para ayudar a cubrir problemas de seguridad relacionados.

Val TI es el paraguas empleado para describir las publicaciones y productos futuros adicionales y actividades de direccionamiento del marco Val TI

Las publicaciones actuales relacionadas con Val TI son:

- *Enterprise Value: Governance of IT Investments—The Val IT Framework*, que explica como una empresa puede extraer valor optimo de investigaciones permitidas de TI y esta basado en el marco COBIT. Se organiza en:
  - Tres procesos- Valor de gobierno, gestión de porta folios y gestión de inversiones.
  - Practicas de gestión claves de TI-Prácticas de gestión esencial que influyen positivamente para conseguir el resultado deseado o el propósito de una actividad particular. Soportan los procesos de Val TI y juegan aproximadamente el mismo role que los objetivos de control de COBIT.
- *Enterprise Value: Governance of IT Investments—The Business Case*, que enfoca en un elemento clave de la inversión de los procesos de gestión
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, que describe como una compañía de servicios financieros mundial gestiona un porta folio de inversiones de TI en el contexto del marco Val TI.

Para una completa y actualizada información sobre COBIT, Val TI y productos relacionados, casos de estudio, oportunidades de entrenamiento, novedades y otra información específica de marcos de trabajo, visitar *www.isaca.org/cobit* y *www.isaca.org/valit.*

Página dejada en blanco intencionadamente.