

Universidad Cenfotec

Maestría en Tecnología de Bases de Datos



Definición de la arquitectura de la información basada en COBIT en BAC Credomatic

Autor

Marco A. Hernández Vásquez

Ingeniero en Sistemas

Coordinador

Ing. Julio Córdoba Retana, MIS, (Phd Cand)

Julio, 2013

Dedicatoria

A todas aquellas personas que han sido un gran soporte por su apoyo incondicional y su paciencia, empezando por mi familia, a mi esposa Vivian y mis hijos Abigail, Daniela y Gabriel que representan la motivación e inspiración suficiente para buscar la superación constante en mi vida, además a todos mis amigos, compañeros y jefes de BAC Credomatic que me han dado la oportunidad de crecimiento y de desarrollo en esta tan especial empresa
y obviamente al Señor mi Dios que me ha dado la oportunidad.

Índice de Contenido

Contenido

Introducción	8
El objeto de la investigación.....	11
Objetivo General	12
Objetivos Específicos.....	12
Método de trabajo.....	12
Contexto del Problema	14
Importancia del Problema	22
Estado de la cuestión	29
Modelos y estándares estudiados	31
<i>Payment Card Industry Data Security Standard (PCI DSS)</i>	31
<i>Ley SOX</i>	31
<i>ISO 9001:2008</i>	32
<i>ITIL</i>	33
<i>Cobit 4.1</i>	33
Similitud entre modelos y estándares estudiados.....	34
COBIT (PO2) e ITIL.....	35
COBIT (PO2) e ISO	42
COBIT (PO2) y PCI DSS v2.0.....	47
COBIT (PO2) Y SOX.....	51
Estado Actual.....	55
Historia de BAC Credomatic	56
Dirección Regional de Informática	58
<i>Estándar</i>	60
<i>Descentralizados</i>	62
ESTÁNDARES Y LINEAMIENTOS ACTUALES EN BAC CREDOMATIC	63
Flujo de Desarrollo y Mantenimiento de Sistemas de Información.....	64
Estándar De Clasificación De La Información.....	66
Plan De Seguridad de la Información	68

Esquema de la Información	68
Elementos de Clasificación de la Información	68
Clasificación De Activos De La Información	69
Planteamiento de Necesidades.....	70
<i>Mejora en la participación directa de Negocio.....</i>	<i>72</i>
<i>Mejoramiento de la arquitectura para la toma oportuna de decisiones</i>	<i>73</i>
<i>Mejora en la implementación del Diccionario de datos Empresarial</i>	<i>74</i>
<i>Mejora en la unificación de enfoques sobre estándares ya implementados.</i>	<i>74</i>
<i>Mejora en el mecanismo de clasificación de datos</i>	<i>75</i>
<i>Mejora en el proceso para la determinación de la propiedad de los datos.....</i>	<i>75</i>
<i>Mejora en el proceso de identificación de datos a los cuales asignarles controles de seguridad.....</i>	<i>76</i>
<i>Mejora en la validación de los acuerdos del diseño con respecto a lo implementado.....</i>	<i>77</i>
<i>Mejora en la determinación de la correcta instalación en equipos regionales</i>	<i>78</i>
<i>Mejora en el mecanismo de monitoreo de la integridad estructural en los computadores de la región</i>	<i>79</i>
Solución propuesta	81
Esencia de COBIT.....	83
Modelo de Arquitectura de información empresarial	85
PO2.1 Modelo de arquitectura de información empresarial.....	87
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	87
PO2.3 Esquema de clasificación de datos	87
PO2.4 IT Administración de la integridad.....	87
PASOS DE IMPLEMENTACIÓN PO2 EN BAC CREDOMATIC	88
DEFINICIÓN DEL DICCIONARIO DE DATOS EMPRESARIAL	89
PROCESO PARA EJECUTAR EL ESQUEMA DE CLASIFICACIÓN DE DATOS	94
PROCESO DE ASIGNACIÓN DE PROPIEDAD DE DATOS	97
PROCESO DE VALIDACIÓN DE INTEGRIDAD DE DISEÑO ANTES DE ENVÍO DE PASE A PRODUCCIÓN.....	107
PROCESO DE VALIDACIÓN DE INTEGRIDAD A LA HORA DE LA INSTALACIÓN DEL PASE EN CADA COMPUTADOR DE PRODUCCIÓN	111
PROCESO DE MONITOREO DE INTEGRIDAD ESTRUCTURAL EN LOS COMPUTADORES DE PRODUCCIÓN	113

Indicadores para el proceso	115
Productos No Conformes (PNCs) del Proceso.....	116
Resumen del Proceso PO2.....	117
Conclusiones y trabajos futuros.....	118
Conclusiones.....	119
Trabajos Futuros.....	120
Bibliografía	121
Anexos.....	125
Anexo 1	126

Índice de imágenes

Ilustración 1 Factores Influyentes Gobernabilidad de TI [GOV-001]	15
Ilustración 2 Prácticas Implementadas [GOV-001]	15
Ilustración 3 El efecto sombrilla de COBIT [REG-001]	18
Ilustración 4 Categorización de Procesos [SUG-001]	19
Ilustración 5 Gobernanza de Empresas TI - GEIT [SIS-001]	21
Ilustración 6 Intersección de Factores comunes [SIS-001]	22
Ilustración 7 Integración del Gobierno de TI [REG-001]	23
Ilustración 8 Guía del marco de trabajo [ISA-001]	24
Ilustración 9 Preferencia por marco de trabajo [SIS-001]	25
Ilustración 10 Objetivos de la Arquitectura de la Información	26
Ilustración 11 Ventajas del Diccionario de Datos	27
Ilustración 12 Administración de la Integridad	28
Ilustración 13 Dominios de COBIT	33
Ilustración 14 Funciones de ITIL [REG-001]	36
Ilustración 15 Ciclo de vida de ITIL [ITI-005]	36
Ilustración 16 Framework de ITIL [ISA-001]	37
Ilustración 17 Diseño del Servicio [ITI-004]	41
Ilustración 18 PDCA [COB-006]	43
Ilustración 19 Infraestructura de la empresa	59
Ilustración 20 Resumen de flujo de Desarrollo	61
Ilustración 21 Punto de Control en Flujo de Desarrollo	65
Ilustración 22 Modelo de Información Empresarial	73
Ilustración 23 Requerimientos del Negocio COBIT	82
Ilustración 24 Dominios COBIT [GOV-007]	84
Ilustración 25 Diccionario de Datos Empresarial	90
Ilustración 26 Perspectivas del Diccionario de Datos	92
Ilustración 27 Insumo del Diccionario de Datos	93
Ilustración 28 Flujo del Diccionario de Datos	93
Ilustración 29 Proceso de clasificación de Datos	96
Ilustración 30 Datos Empresariales - Estrategia	101
Ilustración 31 Datos Empresariales - Servicio de Negocio	102
Ilustración 32 Datos Empresariales - Por Conceptos	103
Ilustración 33 Jerarquía de Datos Empresariales	104
Ilustración 34 Esquema de Autoridad - Datos Empresariales	105
Ilustración 35 Datos Empresariales en la región	106
Ilustración 36 Proceso generación metadata	110
Ilustración 37 Validación de Integridad en la instalación	113
Ilustración 38 Monitoreo regular de la integridad	113
Ilustración 39 Proceso completo de Arquitectura de la Información	117

Índice de Tablas

Tabla 1 Generalidades de ITIL [ALI-001].....	35
Tabla 2 Tópicos principales de ITIL [ALI-001]	37
Tabla 3 Comparación ITIL - COBIT [COB-004] [ITI-006]	38
Tabla 4 Mapeo ITIL vrs COBIT PO2 [ALI-001]	39
Tabla 5 Descripción de lineamientos ITIL relacionados	41
Tabla 6 Generalidades ISO	42
Tabla 7 Mapeo ISO vrs COBIT PO2 [ALI-001][COB-006].....	44
Tabla 8 Descripción de lineamientos ISO relacionados [ISO-1799]	46
Tabla 9 Elementos de control PCI DSS [PCI-001].....	48
Tabla 10 Generalidades PCI DSS.....	48
Tabla 11 Mapeo PCI vrs COBIT [ALI-001] [COB-006].....	49
Tabla 12 Descripción de lineamientos PCI relacionados [COB-002]	50
Tabla 13 Leyes o títulos de SOX.....	52
Tabla 14 Mapeo de procesos SOX - COBIT [SOX-003].....	53
Tabla 15 Controles SOX [COB-003][SOX-001]	54
Tabla 16 Principios Norma ISO 9001:2008 [BAC-003].....	58
Tabla 17 Requerimientos en implementación de PO2	66
Tabla 18 Ventajas en la implementación de PO2	86
Tabla 19 Indicadores del Proceso PO2	115
Tabla 20 Productos No Conformes del Proceso PO2	116

Introducción

Frente a los retos que cada día, las empresas financieras están destinadas a superar, es necesario conocer tanto las necesidades propias de la cultura y el quehacer de la empresa, como las recomendaciones y buenas prácticas que ya de por sí se encuentran documentadas en estándares y lineamientos generalmente aceptados.

Dado lo anterior, esta investigación y trabajo centra su atención alrededor de una necesidad surgida en la operativa de la organización, como lo es, la búsqueda de un grupo de procesos que sea la base de la implementación de un modelo de arquitectura de la información dentro de la organización. A partir de esta necesidad se determina los modelos o estándares que se combinan con la necesidad planteada, y principalmente, que estos modelos o estándares hayan tenido algún tipo de implementación dentro de la empresa, lo cual pueda permitir su reutilización y aprovechamiento de recursos, con el fin único de que todos los procesos implementados y por implementar puedan trabajar en forma conjunta y ordenada.

Conociendo los factores implementados dentro de la organización que pueden ser reutilizados, se procederá en la implementación de los procesos que sean necesarios con el fin de alcanzar la meta establecida, y que sean completamente funcionales con las necesidades actuales de la empresa pero que además se alineen con las mejores prácticas encontradas.

Dado lo anterior, este trabajo consta de cinco capítulos, a saber:

Capítulo 1: *El objeto de la investigación*, se establece la finalidad del trabajo y los aspectos formales relacionados con el caso de estudio.

Capítulo 2: *Estado de la cuestión*, se presentan los planteamientos teóricos de cada uno de los estándares estudiados y la relación que se puede encontrar en cada uno de ellos con respecto a una arquitectura de información empresarial, todo esto guiado principalmente en el objetivo de control PO2 de Cobit.

Capítulo 3: *Estado Actual*, muestra una semblanza de la realidad y cultura operativa de la organización BAC Credomatic sobre la cual se realiza el trabajo.

Capítulo 4: *Planteamiento de Necesidades*, en el cual se muestran cada una de los elementos funcionales requeridos en los procesos de la organización y que se solicitan plantear su solución.

Capítulo 5: *Solución Propuesta*, en la cual se detalla cada uno de los procesos y elementos que se consideran necesarios para ser capaces de satisfacer las necesidades expuestas.

Capítulo 1

El objeto de la investigación

Objetivo General

Mapear los distintos elementos que forman parte de los estándares ISO, PCI DSS, Ley de SOX e ITIL con respecto al marco de trabajo PO2 de Cobit 4.0 y cumplir con los requerimientos dados por la empresa en busca de la arquitectura de la información requerida.

Objetivos Específicos

- Clasificar y delimitar las directrices y lineamientos con que la compañía actualmente cuenta para determinar su correspondiente mapeo con el marco de trabajo de COBIT.
- Definir nuevas directrices, lineamientos y procesos o flujos alineados con COBIT.
- Analizar y mapear las distintas características de los estándares mencionados con respecto al marco de trabajo de COBIT.

Método de trabajo

Para efectos de la elaboración de este trabajo, se procedió con la siguiente metodología:

- Investigación y análisis de información con respecto a cada uno de los estándares identificados y su relación con la arquitectura de información empresarial.
- Mapeo de todo el material existente dentro de la documentación formal de la organización relacionado con los estándares anteriormente vistos y que

puedan ser aprovechados en la solución de los requerimientos o necesidades indicadas.

- Conformación de un grupo de expertos dentro de la organización que permitan tener los distintos puntos de vista a tomar en cuenta en la generación del proceso de arquitectura de información empresarial que se busca. En este grupo participan los siguientes roles:
 - Seguridad de Sistemas
 - Operaciones (encargados de instalación de pases a producción)
 - Unidad de apoyo a desarrollo
 - Arquitectos de datos
- Desarrollo de procesos y lineamientos con el fin de tener la base para la implementación de la arquitectura de información empresarial buscada.

Contexto del Problema

El uso de las mejores prácticas en la gobernabilidad de la información dentro de las compañías se ha convertido en uno de los elementos esenciales para la administración efectiva de los recursos y por ende, en un aumento en la eficiencia empresarial.

Lo anterior ha sido impulsado por varios frentes, por un lado, una necesidad creciente impulsada dentro de la misma empresa debido a experiencias en los procesos típicos y normales de la empresa, y que en muchas ocasiones ha provocado fallas continuas e incrementales, cuyas soluciones en ocasiones, han sido simplemente formas temporales para mantener la funcionalidad activa durante un lapso de tiempo, pero susceptible a nuevas y más complejas situaciones.

Por otro lado, entidades gubernamentales preocupadas por la estandarización de correctos mecanismos dentro de las empresas, han impulsado la implementación de buenas prácticas, de tal modo que permitan garantizar la sostenibilidad de los aspectos básicos en lo que a gobernabilidad y gestión de datos se refiere, lo anterior además influenciado tanto por el mercado financiero como los inversionistas que urgen de un fuerte respaldo de las entidades financieras, de tal manera que puedan generar algún tipo de seguridad en el cumplimiento de los requerimientos regulatorios en conformidad con unas buenas prácticas del gobierno corporativo.

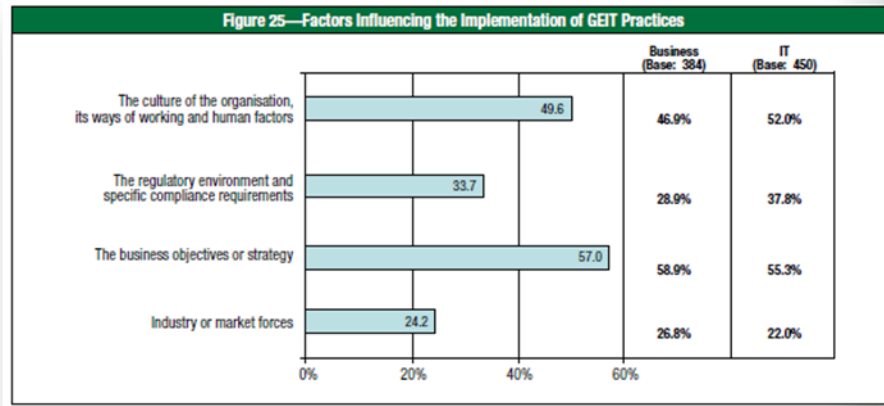


Ilustración 1 Factores Influyentes Gobernabilidad de TI [GOV-001]

Debido a lo anterior, las empresas se han visto en la obligación de implantar en sus sistemas, una serie de prácticas que si bien mejoran sus procesos, pero por otro lado podrían incrementar la complejidad de sus actividades, por tanto la necesidad de cumplir con la implantación de los mismos pero de una manera ordenada, controlada y orientada a los objetivos de la empresa.

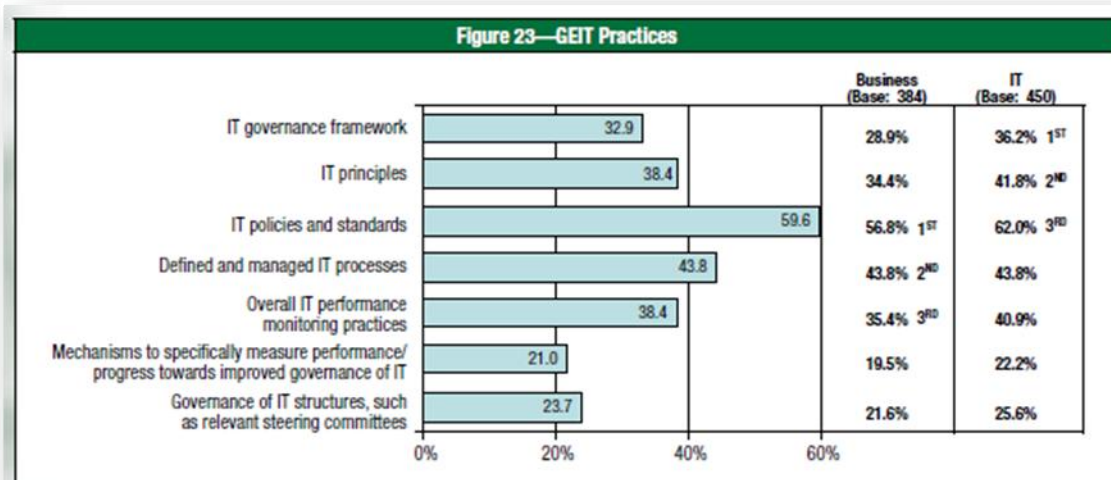


Ilustración 2 Prácticas Implementadas [GOV-001]

Ya sea implementado para satisfacer requerimientos regulatorios o bien como un proyecto interno en la búsqueda de la aplicación de mejores prácticas, estos elementos deben ser tratados dentro del planteamiento estratégico de la compañía en vez de un gasto simplemente de cumplimiento. Para poder cumplir con lo anterior es necesaria la adaptación, reutilización y creación de procesos, políticas y procedimientos para permitir al personal de la compañía su aplicación correcta y así cumplir con los objetivos propuestos.

El reto propuesto es la implementación de los requerimientos regulatorios junto con los objetivos internos de la empresa de tal manera que permitan una evolución planificada de nuestra arquitectura a la vez del cumplimiento regulatorio, de tal manera que en todo caso se pueda obtener un beneficio real al desempeño de las metas de la empresa.

La mayoría de las actuales regulaciones que se deben aplicar en las entidades financieras vienen en búsqueda de ciertos factores muy importantes, como lo son:

- Automatización de procesos
- Registro adecuado de cada uno de los procesos de tal manera que permita su auditoría de forma eficiente y oportuna.
- Administración del riesgo

No obstante a lo anterior, las regulaciones generalmente se encuentran enfocadas en aspectos de prioridad para el mercado y por otro lado, las empresas obviamente están interesadas en alcanzar la implementación de dichas regulaciones lo antes posible. Esta carrera por avanzar en contra del tiempo y enfocándose en aspectos muy importantes genera sacrificio de áreas sumamente necesarios para la correcta generación de una adecuada gobernabilidad.

Actualmente en Costa Rica se requiere la implementación de dos regulaciones muy importantes para efectos de la gobernabilidad de TI:

- *Norma Técnica para la Gestión y Control de Tecnologías de Información en las instituciones públicas* (N-2-2007-CO-DFOE) de la **Contraloría General de la República**
- *SUGEF 14-09* Para instituciones financieras supervisadas

La normativa 14-09 de la SUGEG con respecto al **REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN** aprobado en el 2009 señala en su capítulo III artículo 9:

"La evaluación de la Gestión de TI se basará en el marco conceptual de la versión 4.0 de Cobit®..."

La superintendencia de entidades, con esta regulación, está interesada en la implementación del marco COBIT, la cual permite atender las recomendaciones emitidas por el Comité de Basilea, particularmente las disposiciones de Basilea II con respecto a la gestión de riesgos operativos en su dimensión tecnológica. Basilea II incluye recomendaciones sobre la legislación y regulación, con el propósito de crear un estándar internacional de referencia a los reguladores bancarios de cada país, con el objeto de establecer los requerimientos de capitales necesarios, para asegurar la protección de las entidades frente a riesgos operativos y financieros.

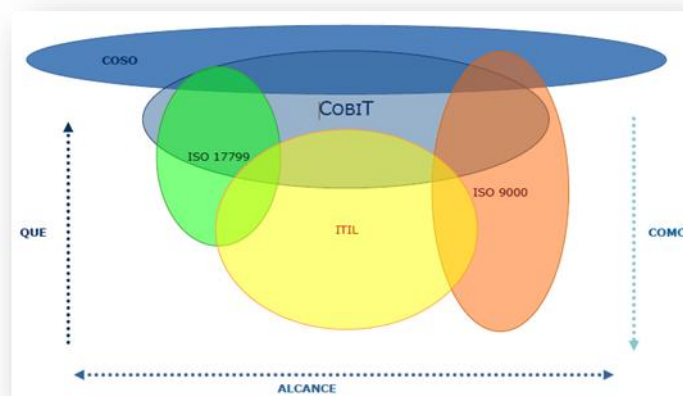


Ilustración 3 El efecto sombrilla de COBIT [REG-001]

La *normativa 14-09* de la Superintendencia General de Entidades Financieras (SUGEF) indica:

- **Artículo 1.** *Objeto:* Establece la definición de criterios y metodologías necesarias para la evaluación y calificación de la gestión de la tecnología de Información (TI).
- **Artículo 6.** *Marco para la Gestión de TI:* Definición de la obligación de la entidad en lo que respecta al diseño, implementación y monitoreo de un marco adecuado para la gestión de la tecnología de información.
- **Artículo 9.** *Marco Referencial:* La evaluación de la gestión de TI se basará en el marco conceptual de la versión 4.0 de *Cobit®*, considerando sus cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y Monitorear y Evaluar.

La gestión de la tecnología de información se encuentra enfocada en dos objetivos fundamentales:

- **Alineación estratégica**: Comprobación de que los mecanismos y procesos estratégicos se encuentran enfocados coordinadamente con los objetivos de la empresa.
- **Administración del Riesgo de TI**: Comprobación de que los riesgos de TI se han identificado y se monitorean debidamente.

La Superintendencia ha categorizado los procesos aplicándole cierto nivel de madurez y por ende priorizando su implementación entre las compañías, a continuación la categorización:

**ANEJO 1
CATEGORIZACIÓN DE PROCESOS Y NIVEL DE MADUREZ REQUERIDO**

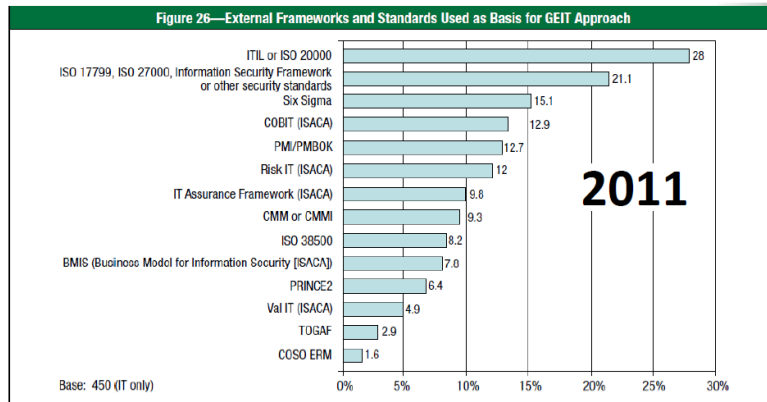
Dominio	Procesos COBIT® 4.0	Marco para la Gestión De TI
PO	PO1 Definir un plan estratégico de TI	Procesos obligatorios Nivel de madurez requerido: Tres
	PO3 Determinar la dirección tecnológica	
	PO5 Administrar la inversión en TI	
	PO9 Evaluar y administrar los riesgos de TI	
	PO10 Administrar proyectos	
AI	AI3 Adquirir y mantener infraestructura tecnológica	
	AI5 Adquirir recursos de TI	
	AI6 Administrar cambios	
DS	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	
	DS9 Administrar la configuración	
	DS10 Administrar los problemas	
	DS11 Administrar los datos	
DS12 Administrar el ambiente físico		
ME	ME2 Monitorear y evaluar el control interno	
PO	PO2 Definir la arquitectura de la Información	Procesos seleccionables según perfil de TI de la entidad Nivel de madurez requerido: Tres
	PO4 Definir los procesos, organización y relaciones de TI	
	PO6 Comunicar las aspiraciones y la dirección de la gerencia	
	PO7 Administrar recursos humanos de TI	
	PO8 Administrar la calidad	
AI	AI1 Identificar soluciones automatizadas	
	AI2 Adquirir y mantener software aplicativo	
	AI4 Facilitar la operación y el uso	
	AI7 Instalar y acreditar soluciones y cambios	
DS	DS1 Definir y administrar los niveles de servicio	
	DS6 Identificar y asignar costos	
	DS7 Educar y entrenar a los usuarios	
	DS8 Administrar la mesa de servicio y los incidentes	
	DS13 Administrar las operaciones	
ME	ME1 Monitorear y evaluar el desempeño de TI	
	ME3 Garantizar el cumplimiento regulatorio	
	ME4 Proporcionar gobierno de TI	

Ilustración 4 Categorización de Procesos [SUG-001]

En BAC Credomatic se ha dado a la tarea de cumplir a cabalidad con cada uno de los puntos indicados por la Superintendencia de Entidades Financieras, mucho de lo que ya se había implementado vía otras regulaciones venía a cubrir muchas de los requerimientos que a la fecha realizaba la superintendencia.

A pesar de que la Arquitectura de la Información Empresarial posee un nivel de madurez tres y no será requerido en la primera auditoría, la empresa ha sentido la necesidad de ir trabajando en este proceso de tal manera que se encamine sobre la arquitectura de información, con el fin de proveer un mecanismo más formal de administración de los datos en la compañía.

En BAC Credomatic se ha avanzado en la implementación de normas, estándares y principios con el fin de promover la calidad y gobernanza de TI, cada uno de ellos promovido por regulaciones de gobiernos o bien regulaciones empresariales. Toda esta gama de implementaciones tiene como objetivo la salvaguardia de TI y por ende su gobernabilidad, por lo tanto no queda duda que existen intersecciones entre cada uno de ellos, y más aún que se podrá encontrar factores concordantes con respecto a la implementación formal según COBIT de la arquitectura de información que la empresa desea iniciar.

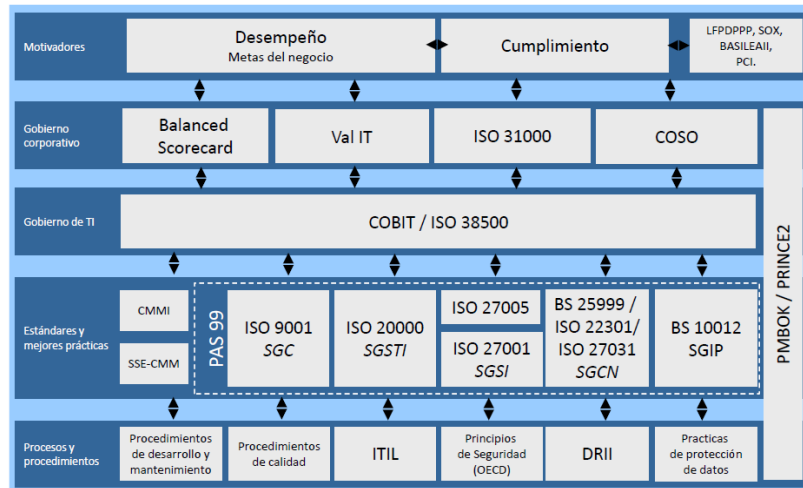


Fuente: ISACA Global Status Report 2011.

Ilustración 5 Gobernanza de Empresas TI - GEIT [SIS-001]

Lo anterior plantea varios retos, entre ellos se encuentra el “encajar” de forma correcta cualquier nuevo proceso que sea necesario diseñar para efectos de PO2 con respecto a los procesos que actualmente ya cuenta la empresa, y que fueron generados debido a otros estándares o regulaciones particulares. El crear esta intersección de factores entre procesos existentes y los nuevos a crear, provocará una implementación más robusta, ordenada y consecuente con los objetivos planteados por la empresa.

Dado la anterior, el presente documento desarrollará el análisis de forma incremental, iniciando con la determinación de los puntos clave de los estándares estudiados en los cuales existe un emparejamiento de concepto en lo que a Arquitectura de Información se refiere.



Fuente: Mario Ureña - *SecureInformationTechnologies 2011* 

Ilustración 6 Intersección de Factores comunes [SIS-001]

Posterior a identificar los puntos clave en que se relacionan los estándares de interés, se procederá a mapearlos con lo implementado dentro de la organización, y de esta manera contar con un panorama mucho más amplio de las necesidades aun no implementadas para la construcción del proceso de Arquitectura de la información que se desea realizar.

Importancia del Problema

Es bien conocida la importante cantidad de información que actualmente las empresas manejan, y que mucha de esta información es usada para la toma de decisiones; las cuales pueden generar en buenas inversiones para la empresa y por ende al mercado, como también podría generar grandes tropiezos en la elaboración de productos debido a la mala gestión de datos. Teniendo esto presente, es sencillo deducir que tanto las empresas como el mercado están interesados en la correcta administración de los datos [GOV-07]

Las mejores prácticas de TI son importantes debido a [ALI-001]:

- La demanda de retornos de las inversiones en TI.
- Preocupación por incremento en gastos de TI
- Cumplimiento de aspectos regulatorios para los controles de TI
- Selección de proveedores de servicios
- Incremento de complejidad en riesgos relacionados a TI.
- Iniciativas de gobierno de TI
- Optimización de costos por medio de enfoques estandarizados
- Creciente madurez y consecuente aceptación de prestigiosos marcos de referencia.
- Necesidad de evaluación de desempeño con respecto a estándares generalmente aceptados.
- Recomendaciones de expertos.

Estas mejores prácticas deben ajustarse a los requisitos del negocio y ser integradas entre sí con los procedimientos internos.

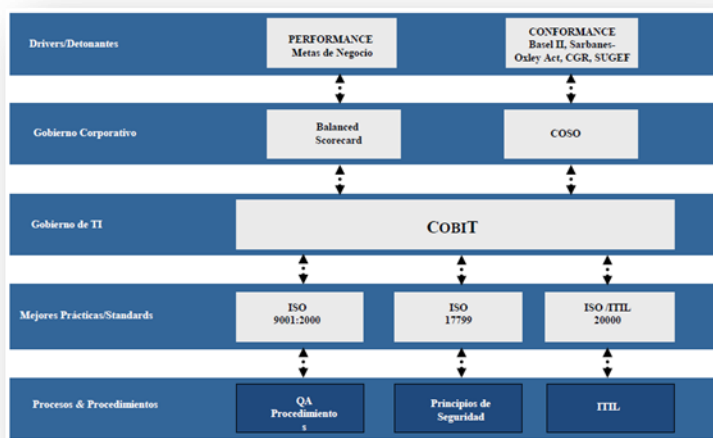


Ilustración 7 Integración del Gobierno de TI [REG-001]

El éxito de TI se encuentra basado en la satisfacción de los requerimientos de negocio estableciendo un vínculo con dichos requerimientos, organizando las actividades de TI, administrando los recursos necesarios y definiendo los objetivos de control a ser considerados. [GOV-07]

Estos objetivos de control deben permitir una mejor alineación al enfoque de negocios, una visión de negocio con respecto a las funciones de TI, una distribución explícita de la propiedad y responsabilidades de sus procesos, un cumplimiento efectivo de lo solicitado por los reguladores y por terceros, un lenguaje común entre todos los interesados y un cumplimiento a cabalidad del ambiente de control de TI. [GOV-07]

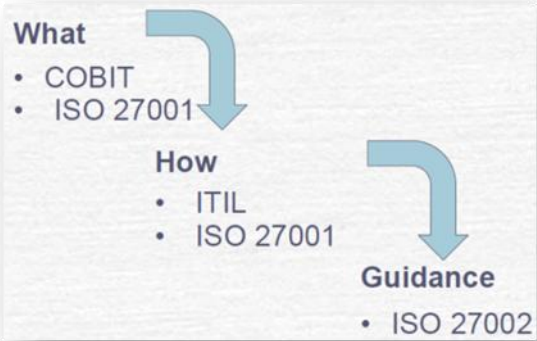


Ilustración 8 Guía del marco de trabajo [ISA-001]

La implementación de un proceso que permita la conformación de una buena gestión de datos y por ende una correcta gobernabilidad de TI es uno de los objetivos que el Banco está interesado en fomentar, no solamente por aspectos regulatorios sino por su naturaleza de control y orden. Es por esta razón que se ha decidido expandir los requerimientos para la implementación de COBIT dentro de la empresa, no solamente tomando en consideración los objetivos de control solicitados con prioridad por la Superintendencia de Entidades Financieras sino expandiendo su marco de acción y llevando al diseño y posterior implementación

del objetivo de control para la correcta Arquitectura de la Información dentro de la compañía.

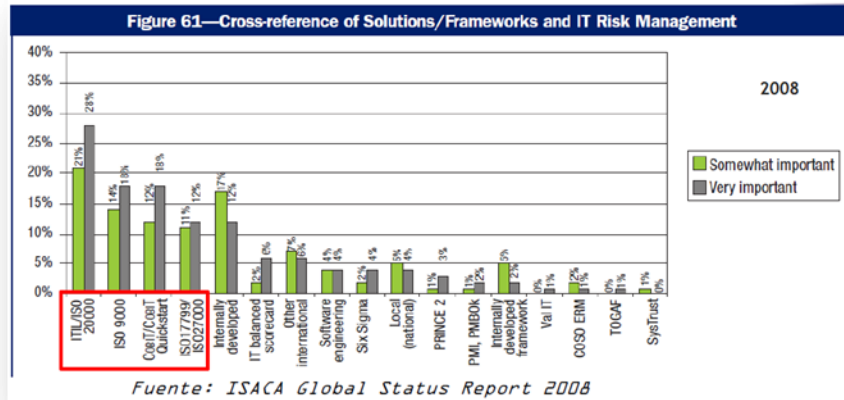


Ilustración 9 Preferencia por marco de trabajo [SIS-001]

Sin importar el avance tecnológico con que se cuenta, COBIT permite, haciendo uso de las principales normas técnicas internacionales, crear un grupo de buenas prácticas en aspectos tan fundamentales tales como Seguridad, calidad y eficiencia, de tal manera que permita una correcta alineación de TI con el negocio, identificando conjuntamente los riesgos, acuerdos de entrega de productos, aspectos fundamentales de la gestión de recursos y permitiendo la medición del desempeño en el cumplimiento de metas de tal manera que sea posible identificar el nivel de madurez de los procesos de la organización.

Uno de los aspectos fundamentales en el diseño de los procesos de COBIT dentro de una empresa es la edificación de la arquitectura de la información, dentro de la cual se permite la interrelación entre TI y el negocio.

El término de Arquitectura de la Información es un concepto no tan sencillo de explicar pero que hoy en día está siendo usado ampliamente en la literatura de

calidad de la información. Para su definición se podría iniciar indicando que en su forma más general tiene una relación directa con los sistemas informáticos, que busca generar una transparencia entre el contenido y su aplicabilidad de los datos dentro de una organización, y que permite poder aprovechar adecuadamente y de forma oportuna los datos e información en los almacenes de datos. En resumen le ofrece a la empresa la oportunidad de obtener beneficios de sus datos resguardados por TI. [AIF-01]

Pero además uno de los objetivos fundamentales de la Arquitectura de la Información es permitir a TI agilizar la respuesta a los requerimientos plasmados por negocio, de tal manera que pueda brindar información confiable y consistente, integrando de forma transparente las aplicaciones hacia los procesos de negocio.



Ilustración 10 Objetivos de la Arquitectura de la Información

Por otro lado, una de las ventajas de la Arquitectura de la información es la creación del diccionario de datos empresarial el cual permite el 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. Utilizando este mismo diccionario de datos, se puede generar una clasificación de datos particular para la empresa,

permitiendo determinar qué tan crítica y sensible es la información, además identificando o especificando explícitamente la propiedad de cada uno de los datos de la empresa con el fin de definir los niveles apropiados de seguridad y cualquier otro tipo de control que se crea necesaria.

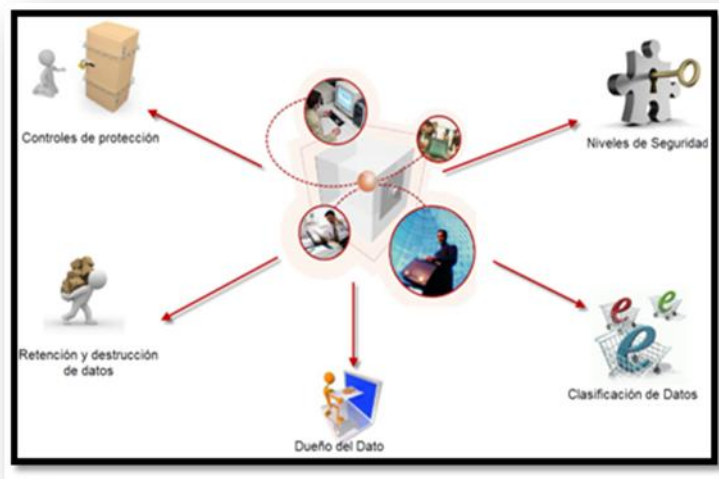


Ilustración 11 Ventajas del Diccionario de Datos

Finalmente, un buen diseño y una apropiada implementación de la Arquitectura de la información, permitirá a la empresa una administración efectiva de la integridad, de tal manera que se pueda definir e implantar procedimientos que serán de gran ayuda en busca de la integridad y consistencia de los datos almacenados.



Ilustración 12 Administración de la Integridad

En resumen, lo que se busca con este trabajo es investigar la interrelación entre los siguientes estándares con el objetivo del diseño de PO2 de Cobit.

Capítulo 2

Estado de la cuestión

En este capítulo se presenta el estado de la cuestión de los distintos estándares y lineamientos regulatorios que en estos momentos son aplicables a las entidades financieras en Costa Rica, específicamente a las aplicables en Bac Credomatic. Para situar la gestión del diseño de la Arquitectura de la información por medio de la aplicación de PO2 de Cobit, se revisarán los distintos estándares y sus similitudes o puntos de encuentro.

La estructura de este apartado es el siguiente:

- Similitud entre estándares y modelos estudiados
- Cada uno de los modelos estudiados
 - Alcance del modelo
 - Relación del modelo con la Arquitectura de la información
 - Consideraciones para la implementación de PO2.

Modelos y estándares estudiados

Payment Card Industry Data Security Standard (PCI DSS)

Las principales marcas de tarjetas (Visa, MasterCard, American Express, JCB y Discover) han desarrollado el estándar Payment Card Industry Data Security Standard (PCI DSS), que establece un conjunto de medidas para garantizar la seguridad en el tratamiento de la información asociada a pagos realizados con tarjeta. Estas medidas son aplicables a todos aquellos sistemas que almacenan, procesan o transmiten datos de titulares de tarjetas.

En relación a la implantación del estándar, cabe destacar que los requerimientos establecidos por PCI DSS están alineados con las buenas prácticas de seguridad exigidas por estándares ampliamente reconocidos, como es el caso de la Norma ISO 27002 o COBIT.

Ley SOX

La Ley Sarbanes - Oxley nace en el 2002 en Estados Unidos, con el fin de monitorear a las empresas que cotizan en la bolsa, evitando la alteración de las acciones; fue promovida por el Senador Paul Sarbanes y el Representante Michael Oxley con el objetivo de evitar fraudes y riesgo de bancarrota además de proteger a los inversores.

Esta ley, más allá del ámbito estadounidense, afectó a todas las empresas que cotizan en la Bolsa de Valores de Nueva York, así como a sus filiales.

Esta ley hace a las empresas recurrir a COSSO para poder cumplir los requerimientos que esta dispone.

En julio del 2010, el Grupo Aval de Colombia, el conglomerado financiero más grande ese país -conformado por el Banco de Bogotá, el Banco de Occidente, el Banco AV Villas, el Banco Popular y el fondo de pensiones AP Porvenir-, suscribió un contrato de compraventa de acciones con GE Consumer Finance relativo a la adquisición del 100% de las acciones del Grupo BAC Credomatic. Esto convierte al BAC Credomatic como una filial del grupo Aval y por tanto debe cumplir con la Ley SOX debido que el Grupo Aval cotiza en la bolsa de valores de los Estados Unidos.

ISO 9001:2008

La ISO 9001:2008 es la base del sistema de gestión de la calidad ya que es una norma internacional y que se centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios.

BAC Credomatic cuenta con esta certificación desde hace cierto tiempo en cada una de sus empresas a lo largo de la región centroamericana.

ITIL

ITIL proporciona un marco de trabajo de mejores prácticas para la gestión de servicios, enfocándose en la planificación, aprovisionamiento, diseño, implementación, operación y soporte a servicios de TI ligadas al negocio.

Para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio fin de lograr una eficacia óptima. [ALI-001]

Cobit 4.1

“COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.” [ALI-001]

Es un marco de referencia que relaciona a los requerimientos de información y de gobierno, a los objetivos de la función de servicios de TI

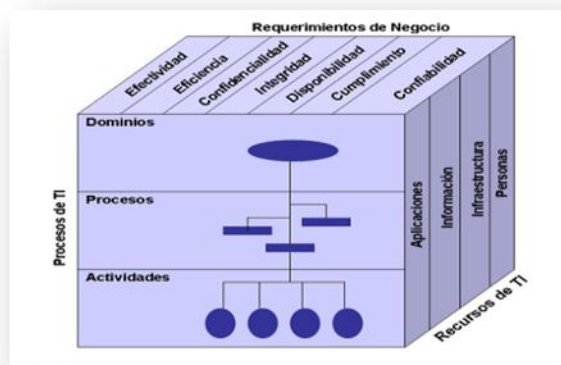


Ilustración 13 Dominios de COBIT

Similitud entre modelos y estándares estudiados

Las mejores prácticas de TI deben ajustarse a los requisitos del negocio y ser integradas entre sí con los procedimientos internos, por otro lado, las regulaciones enfocadas en la gobernabilidad de TI deben fundirse con esas mejores prácticas y juntos proveer un marco "*tropicalizado*" para la mantenibilidad de los sistemas de la empresa.

COBIT puede ser utilizado en el más alto nivel, ofreciendo un marco general de control basado en un modelo de procesos de TI que debería adaptarse a la empresa. Al ser COBIT un marco de alto nivel, se recomienda adaptar los demás estándares o lineamientos a este, esto por interpretarse que estos últimos abarcan áreas más discretas y su mapeo a COBIT no debe ser tan complicada.

A continuación se presenta un mapeo de estos lineamientos y estándares tomando como base a COBIT.

COBIT (PO2) e ITIL

La idea fundamental de ITIL es respaldar los esfuerzos de las compañías en lo que a procesos de negocio se refiere. De esta manera, ITIL describe los enfoques, las funciones, los roles y procesos bases para que una empresa pueda guiarse. [ALI-001]

<i>Estándar:</i> ITIL (Librería de Infraestructura de TI)	<i>Organismo Emisor:</i> OGC y CCTA (Oficina de comercio gubernamental y la central computer and telecommunications Agency del Reino Unido)
ITIL consiste en un “Framework” que encierra las mejores prácticas para proporcionar una adecuada entrega de servicios de tecnologías de la información dentro de las organizaciones. Abarca un amplio conjunto de procedimientos de gestión de TI formulados para facilitar a las organizaciones altos niveles de calidad y eficiencia en sus operaciones de TI, abarcando la infraestructura, desarrollo y operaciones de TI.	

Tabla 1 Generalidades de ITIL [ALI-001]

ITIL posee tres objetivos claves:

1. Alinear los servicios de TI con las necesidades de Negocio
2. Mejorar la calidad de los servicios entregados
3. Reducir costos en la provisión de servicios

ITIL adopta un enfoque orientado a procesos, además establece la gestión de servicios de TI de una forma relacionada e integrada. [REG-001]

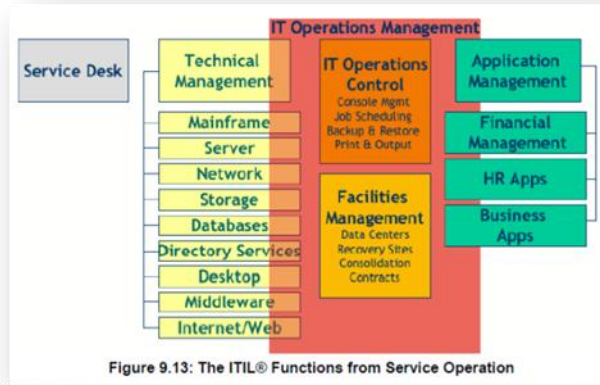


Ilustración 14 Funciones de ITIL [REG-001]

ITIL V3 está orientado al Ciclo de Vida del Servicio. Según la perspectiva empresarial, los servicios de TI, al igual que los productos, también se encuentran condicionados a un ciclo de vida típico, que empieza con la introducción del servicio al mercado y finaliza con la exclusión del mismo del portafolio de servicios. [ITI-005].

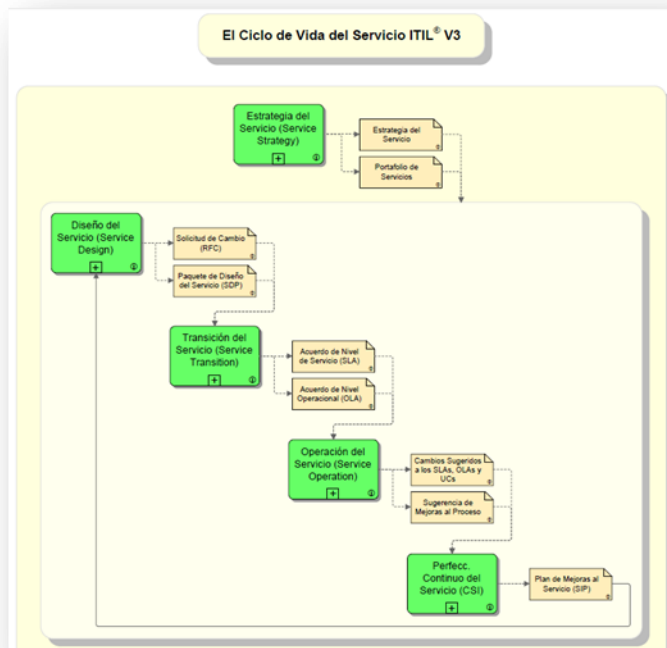


Ilustración 15 Ciclo de vida de ITIL [ITI-005]

ITIL comprende todos los procesos que se hacen en la Administración de Servicios del área de Tecnología. Esos procesos están agrupados en las siguientes áreas, cada una con su correspondiente libro:



Ilustración 16 Framework de ITIL [ISA-001]

ITIL v3 consiste en un sistema sobre la base de 5 libros:

Figura 3 — Tópicos principales ITIL				
Estrategia de Servicio (SS)	Diseño del Servicio (SD)	Transición del Servicio (ST)	Operación del Servicio (SO)	Mejora Continua del Servicio (CSI)
<ul style="list-style-type: none"> Gestión del servicio Ciclo de vida del servicio Activos del servicio y creación de valor Tipos y estructuras de proveedores de servicios Estrategia, mercados y oferta Gestión financiera Gestión del portafolio de servicios Gestión de la demanda Diseño organizacional, cultura y desarrollo Estrategia de aprovisionamiento Automatización e interfaces de servicios Herramienta para estrategias Desafíos y riesgos 	<ul style="list-style-type: none"> Diseño balanceado Requisitos, indicadores, actividades y limitantes Arquitectura orientada al servicio Gestión de servicios de negocio Modelos de diseño de servicios Gestión del catálogo de servicios Gestión de niveles de servicios Capacidad y disponibilidad Continuidad de servicios de TI Seguridad de la información Gestión de proveedores Gestión de datos y de la información Gestión de aplicaciones Roles y herramientas Análisis de impacto en el negocio Desafíos y riesgos Paquete de diseño de servicios Criterios de aceptación de servicios Documentación Aspectos ambientales Marco de trabajo de maduración de procesos 	<ul style="list-style-type: none"> Objetivos, principios, políticas, contexto, roles y modelos Planificación y soporte Gestión del cambio Activos del servicio y gestión de la configuración Liberación y distribución Validación y prueba del servicio Evaluación Gestión del conocimiento Gestionando las comunicaciones y el compromiso Gestión de partes interesadas Sistema de gestión de configuraciones Introducción por etapas Desafíos y riesgos Tipos de activos 	<ul style="list-style-type: none"> Equilibrio en la operación del servicio Salud operacional Comunicación Documentación Eventos, incidentes y problemas Atención de requerimientos Gestión de accesos Monitoreo y control Gestión de la infraestructura y el servicio Gestión de instalaciones y del Data Center Seguridad física y de la información Mesa de servicios Gestión técnica de operaciones de TI y de aplicaciones Roles, responsabilidades y estructuras organizacionales Soporte tecnológico a la operación del servicio Gestionando los cambios, proyectos y riesgos Desafíos Guía complementaria 	<ul style="list-style-type: none"> Objetivos, métodos y técnicas Cambio organizacional Propiedad Drivers Gestión de niveles de servicios Medición del servicio Gestión del conocimiento Benchmarking Modelos, estándares y calidad Proceso de mejoramiento de los siete pasos CSI Retorno sobre la inversión (ROI) y aspectos de negocio Roles Matriz RACI Herramientas de soporte Implementación Gobierno Comunicaciones Desafíos y riesgos Innovación, corrección y mejoramiento Apoyo de las mejores prácticas a la mejora continua del servicio (CSI)

Tabla 2 Tópicos principales de ITIL [ALI-001]

Los procesos de ITIL pueden ser utilizados para lograr y demostrar el cumplimiento con los objetivos de control COBIT.

COBIT	ITIL V3
<p>COBIT es un conjunto de objetivos de Control - un grupo de expertos dicen qué se debe hacer para ofrecer garantías suficientes a los interesados para que se haga un buen trabajo.</p>	<p>ITIL utiliza el término "proceso" para definir muchos componentes que en realidad son funciones.</p>
<p>El propósito de COBIT es apoyar el gobierno de TI al proporcionar un marco de control común que garantice que TI está alineada con el negocio</p>	<p>Este adopta un enfoque gradual en el ciclo de vida, y la mayoría de los componentes descritos en la primera fase también se aplican, en mayor o menor medida, a otras fases.</p>
<p>COBIT se estructuró para estar centrado en las empresas, orientadas a los procesos, controles y basados en la medición.</p> <p>Como resultado de ello, el marco proporciona un modelo de proceso de referencia y un lenguaje común para todo el mundo empresarial de tal manera que ayude a visualizar y gestionar las actividades de TI.</p>	<p>Persigue tener en cuenta el ciclo de vida completo, dando un enfoque más holístico y global a las buenas prácticas.</p> <p>ITIL ofrece una amplia orientación sobre la estrategia de servicios, proporcionando una base teórica para las decisiones estratégicas, al explicar el "qué" hacer.</p>
<p>El marco de modelo de proceso consta de los siguientes cuatro dominios de ciclo de vida:</p> <ul style="list-style-type: none"> • Planificar y organizar • Adquirir e Implementar • Entrega y Soporte • monitoreo y evaluación 	<p>El ciclo de vida de servicio consta de cinco componentes. Cada volumen de los libros fundamentales de ITIL V3 describe uno de estos componentes:</p> <ul style="list-style-type: none"> • Estrategia del Servicio • Diseño del Servicio • Transición del Servicio • Servicio de Operaciones • Servicio de Mejora Continua
<p>COBIT es un marco de gobierno y de control y se centra en lo que debe abordarse para garantizar la buena gobernanza de todos los procesos relacionados con TI, incluyendo los procesos de gestión de servicios</p>	<p>ITIL proporciona las mejores prácticas que describen la forma de planificar, diseñar e implementar procesos de gestión de servicios efectivos.</p>
<p>COBIT brinda orientación, el marco y las herramientas en lograr los niveles deseados de la conformidad y de rendimiento de los procesos de TI necesaria para satisfacer las necesidades del negocio.</p>	<p>Al aprovecharse de la orientación de COBIT, una empresa puede garantizar que sus esfuerzos de gestión de servicios está alineada con su negocio en general, la gobernanza y los requisitos de control interno.</p>

Tabla 3 Comparación ITIL - COBIT [COB-004] [ITI-006]

Tal y como se puede observar en el cuadro comparativo, la mayoría de los puntos de control de PO2 se pueden mapear con los servicios definidos de la etapa de Diseño del Servicio de ITIL, esto permite apoyar el gobierno de TI (cobit) usando funciones orientadas sobre la estrategia de servicios de ITIL.

Objetivos de Control COBIT 4.1	Áreas Clave	Información de Soporte ITIL V3
PO2.1 Modelo de arquitectura de información empresarial	<ul style="list-style-type: none"> * Análisis de soporte a las decisiones * Mantenimiento del modelo de arquitectura de información * Modelo corporativo de datos 	<ul style="list-style-type: none"> * SD 3.6 Aspectos de diseño * SD 3.6.3 Diseño de la arquitectura tecnológica * SD 3.9 Arquitectura orientada al servicio * SD 3.10 Gestión de servicio al negocio * SD 5.2 Gestión de los datos y la información * ST 4.7 Gestión del conocimiento
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	<ul style="list-style-type: none"> * Diccionario corporativo de datos * Comprensión general de los datos 	<ul style="list-style-type: none"> * SD 5.2 Gestión de los datos y la información * SD 7 Consideraciones tecnológicas
PO2.3 Esquema de clasificación de datos	<ul style="list-style-type: none"> * Clases de información * Propietarios * Retención * Reglas de acceso * Niveles de seguridad para cada clase de información 	<ul style="list-style-type: none"> * SD 5.2 Gestión de los datos y la información
PO2.4 Gestión de Integridad	<ul style="list-style-type: none"> * Integridad y consistencia de los datos 	<ul style="list-style-type: none"> * SD 5.2 Gestión de los datos y la información * ST 4.7 Gestión del conocimiento

Tabla 4 Mapeo ITIL vrs COBIT PO2 [ALI-001]

Diseño del Servicio

Es la actividad o proceso orientado a la identificación de los requerimientos y su posible resolución, creando nuevos servicios o bien modificando los existentes. Esta etapa es fundamental para el proceso de ITIL debido a que contribuye fuertemente en el alcance los de los objetivos del Negocio, colocando énfasis en el ahorro de tiempo y dinero, minimizando el riesgo, evaluando la efectividad de los servicios y apoyando las políticas, estándares y calidad de servicios de TI. [ITI-003]

Descripción de lineamientos ITIL relacionados

Gestión de la Arquitectura de TI

Trazar un plan para el desarrollo futuro del panorama tecnológico, tomando en consideración la Estrategia del Servicio y las nuevas tecnologías disponibles.

Provee un programa estratégico general para el desarrollo e implementación de infraestructura y aplicaciones de TI. La Arquitectura de TI también incluye los estándares y las guías que orientan el uso de tecnologías y el diseño y evolución de aplicaciones y componentes de infraestructura de TI. Los sub-componentes de la Arquitectura de TI son las arquitecturas de aplicación, de infraestructura y de información.

Gestión de la Seguridad de TI

Asegurar la confidencialidad, la integridad y la disponibilidad de las informaciones, datos y servicios de TI de una organización. Normalmente, la Gestión de la Seguridad de TI forma parte del acercamiento de una organización a la gestión de seguridad, cuyo alcance es más amplio que el del proveedor de Servicios de TI.

Diseñar técnicas y medidas organizativas adecuadas que aseguren la confidencialidad, la integridad, la seguridad y la disponibilidad de los activos de una organización, así como su información, datos y servicios.

Gestión del Conocimiento

Recopilar, analizar, archivar y compartir conocimientos e información dentro de una organización. El propósito primordial de esta gestión es mejorar la eficiencia reduciendo la necesidad de redescubrir conocimientos.

El Sistema de Gestión del Conocimiento en Servicios (Service Knowledge Management System, SKMS) es el depósito central de todos los datos, informaciones y conocimientos de una organización de TI. Se ocupa de extender el concepto de un Sistema de Gestión de la Configuración que se enfoca en la infraestructura para incluir más información acerca de los servicios, capacidades e iniciativas.

Gestión del Catálogo de Servicios

Asegurarse de que se realice y se edite debidamente un Catálogo de Servicios que contenga información precisa y actualizada de todos los servicios operacionales y de los próximos a ofrecerse. La gestión de este catálogo provee información fundamental para el resto de los procesos de Gestión de Servicios: detalles de servicios, estatus actual e interdependencia de los mismos.

Tabla 5 Descripción de lineamientos ITIL relacionados

ITIL persigue la generación de un proceso que este acorde con las necesidades del negocio y que estas queden plasmadas en la implementación de cada uno de los servicios que formaran la cartera de servicios corporativo, los cuales se encuentran conformados por las distintas arquitecturas, estándares y servicios disponibles en la empresa.

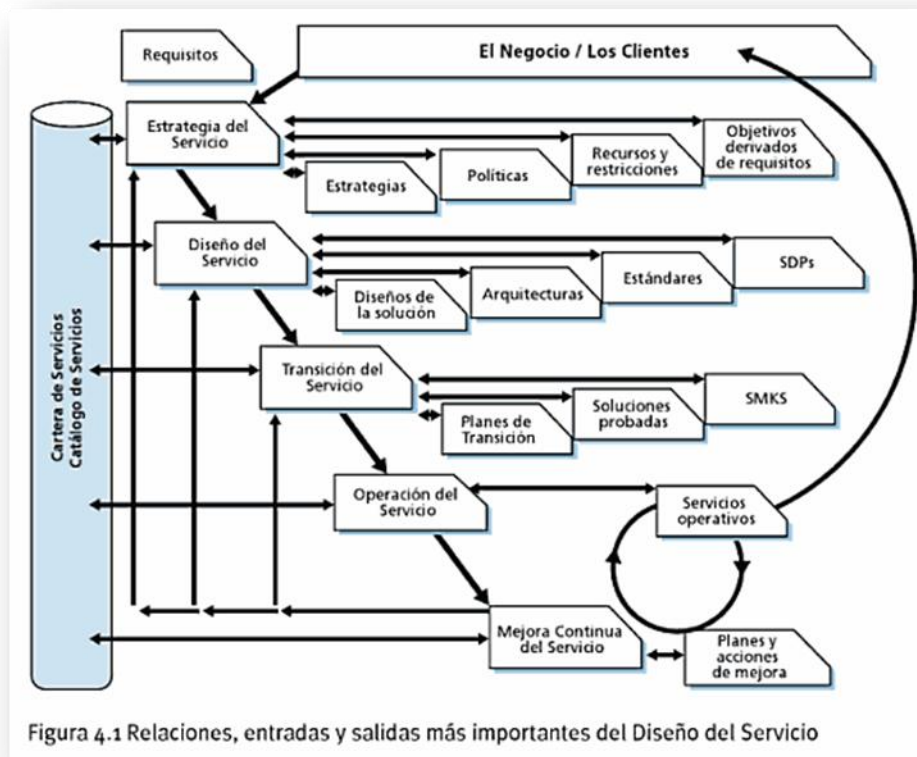


Figura 4.1 Relaciones, entradas y salidas más importantes del Diseño del Servicio

Ilustración 17 Diseño del Servicio [ITI-004]

COBIT (PO2) e ISO

El ISO 27001 es un estándar publicado por la *International Standard Organization* (ISO). Su objetivo es proveer un marco de trabajo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) [ISO-05].

Estándar: ISO 17799 e ISO 27000 (Estándares de Administración de Control y Seguridad de la Tecnología de Información)	Organismo Emisor: ISO (Organización Internacional de Estándares)
Ambos estándares pertenecen a la familia de los ISO, el uno como precedente del otro y presentan “las mejores prácticas” para la implementación de un Sistema de Control y Seguridad de Tecnología de la información. Se estructuran en diferentes áreas de control.	

Tabla 6 Generalidades ISO

El ISO 27001 hace énfasis en los siguientes objetivos:

- Promueve la comprensión de requerimientos de seguridad de información en lo que respecta al establecimiento de políticas y objetivos.
- Implementa y administra controles para la administración de riesgos de seguridad de la información.
- Administra rendimiento y efectividad de los sistemas de seguridad de la información
- Busca una mejora continua basada en mediciones objetivas.

Establece 4 bases fundamentales para la implementación adecuada de este estándar:

- **Planificar:** Diseño del Sistema de gestión de seguridad de la información y toma de decisiones sobre las políticas y controles a implementar.
- **Ejecutar:** Ejecución de políticas y controles de la etapa previa.
- **Revisar:** Monitoreo y control
- **Actuar:** Ajustes del sistema en base a hallazgos encontrados en el monitoreo.

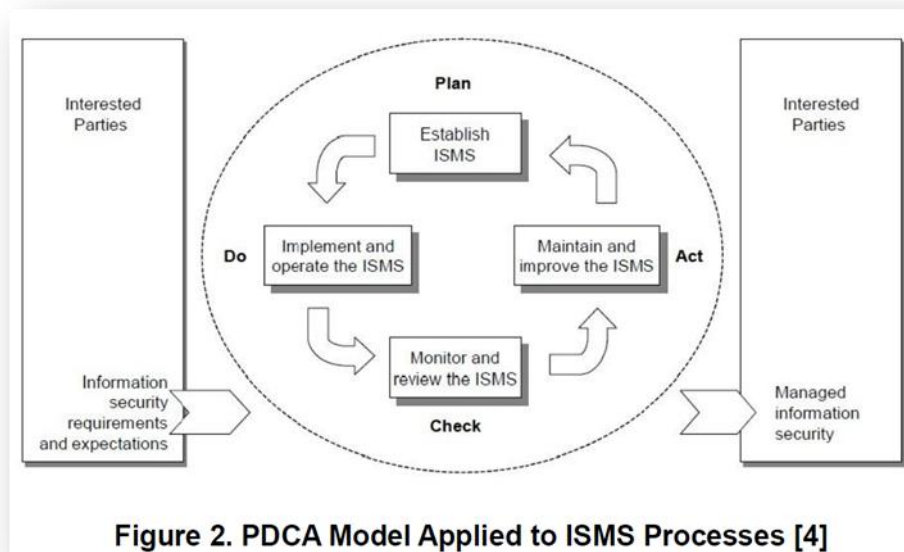


Figure 2. PDCA Model Applied to ISMS Processes [4]

Ilustración 18 PDCA [COB-006]

Tanto COBIT como ISO/IEC 27002 ayudan a definir el "**Qué**" debería hacerse dejándole a ITIL el "**Cómo**" hacerlo. Estos estándares generalmente son utilizadas para:

- Apoyar la gobernabilidad (alineación con los objetivos de negocio).

- Definición de requisitos del servicio y definiciones del proyecto (objetivos claros).
- Verificación de la capacidad y competencia (evaluaciones y compromisos)
- Mejora continua (madurez)
- Auditoría, evaluación y visión externa (criterios objetivos)

[ALI-001]

Objetivos de Control COBIT 4.1	Áreas Clave	Información de Soporte ISO/IEC 27002:2005
PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	* Diccionario corporativo de datos * Comprensión general de los datos	* 7.1.1 Inventario de activos * 11.1.1 Políticas de control de acceso
PO2.3 Esquema de clasificación de datos	* Clases de información * Propietarios * Retención * Reglas de acceso * Niveles de seguridad para cada clase de información	* 7.2.1 Lineamientos para la clasificación * 10.7.1 Gestión de medios removibles * 10.8.1 Políticas y procedimientos para el intercambio de información * 10.8.2 Acuerdos de intercambio * 11.1.1 Políticas de control de acceso

Tabla 7 Mapeo ISO vrs COBIT PO2 [ALI-001][COB-006]

Descripción de lineamientos ISO relacionados

7.1 Responsabilidad por los activos

Lograr y mantener una apropiada protección de los activos organizacionales.

Todos los activos debieran ser inventariados y contar con un propietario nombrado

Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados.

La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos

7.2 Clasificación de la Información

Asegurar que la información reciba un nivel de protección apropiado.

La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debiera utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

10.7 Gestión de medios

Evitar la divulgación no-autorizada, modificación, eliminación o destrucción de activos, y la interrupción de las actividades comerciales.

Los medios se debieran controlar y proteger físicamente.

Se debieran establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo cintas y discos), input/output de data y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

10.8 Intercambio de Información

Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.

Los intercambios de información y software dentro de las organizaciones se debieran basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio y debiera cumplir con cualquier legislación relevante (cláusula 15).

Se debieran establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en-tránsito.

11.1 Requerimientos del negocio para el Control del Acceso

Controlar el acceso a la información.

Se debiera controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad.

Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.

Tabla 8 Descripción de lineamientos ISO relacionados [ISO-1799]

ISO 9001:2000- Quality management system

Cubre los requisitos para sistemas de calidad que soportan todo el ciclo de vida del producto, desde acuerdos iniciales sobre entregables, a través del diseño, desarrollo y soporte del producto, al promover la adopción de un enfoque basado en procesos mediante el establecimiento, documentación, implementación y mantenimiento y continua mejora de la eficacia de un sistema de gestión de la calidad, para aumentar la satisfacción del cliente mediante el cumplimiento de requisitos.

ISO 9001:2000 se enfoca más a cómo debe actuar la organización y la dirección en cuanto a responsabilidades, haciendo más énfasis en el control de resultados de revisiones.

ISO 9001:2000 remarca la importancia de contar con información que sirva de evidencia para demostrar que el proyecto se está desarrollando de acuerdo a los requisitos establecidos. [MEJ-001]

COBIT (PO2) y PCI DSS v2.0

Las Normas de Seguridad de Datos (DSS) de la Industria de tarjetas de Pago (PCI), se desarrolló para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

La siguiente imagen muestra los elementos de los datos de titulares de tarjetas y datos confidenciales de autenticación que habitualmente se utilizan, y que PCI DSS considera de alguna manera.

	Elemento de datos	Almacenamiento permitido	Protección requerida	PCI DSS req. 3.4
Datos del titular de la tarjeta	Número de cuenta principal (PAN)	Sí	Sí	Sí
	Nombre del titular de la tarjeta ¹	Sí	Sí ¹	No
	Código de servicio ¹	Sí	Sí ¹	No
	Fecha de vencimiento ¹	Sí	Sí ¹	No
Datos confidenciales de autenticación ²	Datos completos de la banda magnética ³	No	N/C	N/C
	CAV2/CVC2/CVV2/CID	No	N/C	N/C
	PIN/Bloqueo de PIN	No	N/C	N/C

Tabla 9 Elementos de control PCI DSS [PCI-001]

¹ Estos elementos de datos deben quedar protegidos si se los almacena con el PAN. Esta protección debe brindarse por cada requisito de las DSS de la PCI, a fin de asegurar una protección integral del entorno de los datos del titular de la tarjeta. Además, es posible que otras leyes (por ejemplo, las leyes relacionadas con la protección, la privacidad, el robo de identidad o la seguridad de los datos personales del consumidor) exijan protección específica de esos datos o la debida divulgación de las prácticas de una empresa en caso de que se recopilen datos personales sobre el consumidor durante el transcurso de los negocios.

Sin embargo, las DSS de la PCI no rigen si no se almacenan, procesan ni transmiten los PAN.

² No se deben almacenar los datos confidenciales de autenticación después de la autorización (incluso si están cifrados).

³ Contenido completo de la pista de banda magnética, imagen de la banda magnética que está en el chip o en cualquier otro dispositivo.

<p>Estándar:</p> <p>PCI DSS (Payment Card Industry Data Security Standard)</p>	<p>Organismo Emisor:</p> <p>Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council)</p>
<p>Guía que ayuda a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito</p>	

Tabla 10 Generalidades PCI DSS

Los objetivos de control de este estándar y sus requisitos son los siguientes:

- **Desarrollar y Mantener una Red Segura**
 - Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.
 - Requisito 2: No usar contraseñas del sistema y otros parámetros de seguridad predeterminados provistos por los proveedores.
- **Proteger los Datos de los propietarios de tarjetas.**
 - Requisito 3: Proteger los datos almacenados de los propietarios de tarjetas.
 - Requisito 4: Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
- **Mantener un Programa de Gestión de Vulnerabilidades**
 - Requisito 5: Usar y actualizar regularmente un software antivirus.
 - Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.
- **Implementar Medidas sólidas de control de acceso**
 - Requisito 7: Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
 - Requisito 8: Asignar una Identificación única a cada persona que tenga acceso a un computador.
 - Requisito 9: Restringir el acceso físico a los datos de los propietarios de tarjetas.
- **Monitorear (Monitorizar) y Probar regularmente las redes**
 - Requisito 10: Rastrear y monitorizar (monitorear) todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.
 - Requisito 11: Probar regularmente los sistemas y procesos de seguridad.
- **Mantener una Política de Seguridad de la Información**
 - Requisito 12: Mantener una política que contemple la seguridad de la información

Objetivos de Control COBIT 4.1	Áreas Clave	PCI DSS v2.0 Control Requirements
PO2.3 Esquema de clasificación de datos	<ul style="list-style-type: none"> * Clases de información * Propietarios * Retención * Reglas de acceso * Niveles de seguridad para cada clase de información 	<p>Requerimiento 2: No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema u otros parámetros de seguridad.</p> <p>Requerimiento 8: Asigne una ID única a cada persona que tenga acceso a una computadora.</p> <p>Requerimiento 11: Seguimiento regular de sistemas y procesos de seguridad</p>

Tabla 11 Mapeo PCI vs COBIT [ALI-001] [COB-006]

Los requisitos de seguridad de las DSS de la PCI rigen para todos los componentes del sistema. Los "componentes del sistema" se definen como todo componente de la red, del servidor o de la aplicación que se incluye en el entorno de los datos del titular de la tarjeta o que está conectado a éste. Son la base fundamental de la norma y su implementación es obligatoria para los operadores de tarjetas.

Descripción de lineamientos PCI relacionados

Req. 2	No use contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores
	Los delincuentes (externos e internos a la empresa), por lo general, utilizan las contraseñas predeterminadas por los proveedores y otros parámetros que el proveedor predetermine para afectar los sistemas. Estas contraseñas y parámetros son conocidos entre las comunidades de hackers y se establecen fácilmente por medio de información pública.
Req. 8	Asigne una ID única a cada persona que tenga acceso a equipos
	La asignación de una identificación (ID) única a cada persona que tenga acceso garantiza que cada una de ellas es responsable de sus actos. Cuando se ejerce dicha responsabilidad, las acciones en datos críticos y sistemas las realizan usuarios conocidos y autorizados, y además se pueden realizar seguimientos.
Req. 11	Pruebe con regularidad los sistemas y procesos de seguridad
	Las vulnerabilidades ocasionadas por personas malintencionadas e investigadores se descubren continuamente, y se introducen mediante software nuevo. Los componentes, procesos y software personalizado del sistema se deben probar con frecuencia para garantizar que los controles de seguridad continúen reflejando un entorno dinámico

Tabla 12 Descripción de lineamientos PCI relacionados [COB-002]

COBIT (PO2) Y SOX

El acta Sarbanes Oxley, SOX, fue emitida en el año 2002, para evitar fraudes de cuello blanco (Enron, etc.).

SOX requiere:

- Certificación de la administración acerca del control interno de la compañía
- Reporte de controles internos en información financiera.

El acta incluye varias secciones, con finalidades específicas. Sarbanes Oxley requiere que las compañías adopten un marco de control y aplica a todas las empresas que están registradas en la New York Stock Exchange (NYSE) y la National Association of Securities Dealers by Automatic Quotation, conocida como NASDAQ y bajo la supervisión de la Securities and Exchange Commission (SEC).

SOX no menciona explícitamente seguridad, pero tiene claras implicaciones en esta área, pero el acta exige mejor integridad de los datos lo que implica que se deben reforzar las prácticas de seguridad.

SOX demanda un reforzamiento de las prácticas de control interno, incluyendo las relacionadas con control de accesos, que invariablemente están asociadas a la seguridad.

La jerarquía de controles recomendada para cumplir con SOX implícita y explícitamente requiere confidencialidad y disponibilidad. [SOX-001]

Leyes o Títulos de SOX

I Junta de Supervisión de Firmas de Auditoría	
	Sección 101, sobre retención y salvaguardia de documentos
II Independencia de los Auditores	
	Sección 201, sobre monitoreo y pre aprobación de servicios de no auditoría
III Responsabilidad Corporativa	
	Sección 302, sobre Certificación por parte del CEO y CFO de los reportes entregados a la SEC Sección 306, sobre monitoreo y prevención de operaciones con información privilegiada
IV Revelaciones Financieras Mejoradas	
	Sección 404, sobre control interno Sección 409, sobre revelación oportuna de cualquier cambio materia
IV Conflicto de Intereses	
	Sección 501, sobre monitoreo y revelación de analista de valores
VI Recursos y Autoridad de la Comisión	
VII Estudios e Informes	
VIII Responsabilidad Corporativa y Fraude	
	Sección 802, sobre la retención y protección de documentos y registros de auditoría Sección 806, sobre comunicación y recepción de denuncias
IX Sanciones por crímenes de cuello y corbata	
	Sección 906, sobre certificación de la información financiera
X Declaraciones de Impuestos Corporativos	
XI Responsabilidad por Fraudes Corporativos	
	Sección 1102, sobre retención y salvaguardia de la información

Tabla 13 Leyes o títulos de SOX

Lo primero que hace la ley SOX es crear el "*Public Company Accounting Oversight Board*" más conocido como PCAOB, que es la Junta de Supervisión de Firmas de Contabilidad Pública y que comenzó a operar en abril del 2003. Su principal función es llevar el registro de las firmas auditoras, inspeccionar su trabajo y verificar que cumplan con los estándares de control de calidad y principios éticos. El PCAOB puede aplicar sanciones y medidas disciplinarias. [SOX-002]

Los 12 objetivos de control de COBIT se encuentra fuertemente alineados con las líneas guías para sistemas de TI de la US Public Accounting Oversight Board (PCAOB).

COBIT Control Objective heading	PCAOB IT General Control Heading			
	Program Development	Program Changes	Computer Operations	Access to Programs and Data
1. Acquire and develop application software	•	•	•	•
2. Acquire technology infrastructure	•	•	•	
3. Develop and maintain policies and procedures	•	•	•	•
4. Install and test application software and technology infrastructure	•	•	•	•
5. Manage changes		•		•
6. Define and manage service levels	•	•	•	•
7. Manage third-party services	•	•	•	•
8. Ensure systems security			•	•
9. Manage the configuration			•	•
10. Manage problems and incidents			•	
11. Manage data			•	•
12. Manage operations			•	•

Tabla 14 Mapeo de procesos SOX - COBIT [SOX-003]

El uso de controles manuales y automáticos tiene como objetivo el aseguramiento de que la información dentro del proceso de negocio se encuentre:

- Completa (*Completeness*)
- Exacta (*Accuracy*)
- Valida y autorizada (*Validity*)
- Salvaguardada de accesos no autorizados. (*Restricted Access*)

Una combinación de controles es necesaria para PREVENIR, DETECTAR y CORREGIR los errores de procesamiento.

Completitud
<ul style="list-style-type: none"> • Todas las transacciones son obtenidas, procesadas y aceptadas una vez y solamente una vez.
<ul style="list-style-type: none"> • Todas las transacciones que son ingresadas y aceptadas para procesamiento son actualizadas en el apropiado archivo.
<ul style="list-style-type: none"> • Los duplicados son rechazados
<ul style="list-style-type: none"> • Transacciones rechazadas son evaluadas y re insertadas
<ul style="list-style-type: none"> • Una vez que el dato es actualizado a un archivo, ese dato permanece correcto y actualizado sobre el archivo representando un saldo real.
Exacto
<ul style="list-style-type: none"> • Elementos de datos clave se registran y se guardan al sistema con precisión a través de las características de diseño de entrada de datos.
<ul style="list-style-type: none"> • Los cambios en los datos formalizados son guardados con precisión
<ul style="list-style-type: none"> • Todas las transacciones de inserción y aceptadas actualizan el archivo correcto.
<ul style="list-style-type: none"> • Todas las transacciones afectan el correcto periodo de contabilidad
Validez
<ul style="list-style-type: none"> • Transacciones son autorizadas
<ul style="list-style-type: none"> • Transacciones no son ficticias y se relacionan con la compañía
<ul style="list-style-type: none"> • Cambios a los datos estándar son autorizados y revisados.
Accesos restringidos
<ul style="list-style-type: none"> • Protección contra modificaciones no autorizadas de datos
<ul style="list-style-type: none"> • Asegura confidencialidad del dato
<ul style="list-style-type: none"> • Protección de activos físicos tales como efectivo e inventario de robos o usos indebidos.

Tabla 15 Controles SOX [COB-003][SOX-001]

Capítulo 3

Estado Actual

Historia de BAC Credomatic

A mediados de 1952 se fundó el Banco de América en Nicaragua, no obstante fue hasta los años setenta cuando se incursionó en el mercado de las tarjetas de crédito a través de las empresas Credomatic, y fue ahí donde inicio a incursionar a través de toda la región centroamericana colocando su sede en Costa Rica.

En el año 2004, el grupo inició sus operaciones de tarjetas de crédito en México, y realizó una alianza estratégica con GE Consumer Finance (subsidiaria de GE Capital Corporation), la cual adquirió el 49.99% del capital de BAC Credomatic.

A lo largo de estos años, BAC Credomatic generó una estrategia de expansión adquiriendo varias empresas financieras a lo largo del área centroamericana, entre los que sobresalen el Banco Mercantil (*BAMER*) de Honduras, uno de los bancos privados más importantes y grandes de ese país, Propemi (*Programa de promoción a la pequeña y Microempresa*) en El Salvador y la Corporación Financiera Miravalles en Costa Rica.

A mediados del 2009, GE Capital Corporation aumentó su participación al 75% convirtiéndose en el accionista mayoritario. En Julio del 2010, el Grupo Aval de Colombia, el conglomerado financiero más grande de ese país –conformado por el Banco de Bogotá, el Banco de Occidente, el Banco AV Villas, el Banco Popular y el fondo de Pensiones AP Porvenir-, suscribió un contrato de compraventa de acciones con GE Consumer Finance para adquirir el 100% de las acciones del Grupo Bac Credomatic.

Una cosa interesante a resaltar, es que a pesar de los cambios de control accionario, la estrategia de negocios y la identidad centroamericana que mantiene el grupo Bac Credomatic se encuentra intacta, y más bien, a raíz de la adquisición

ha sido posible ofrecer productos de mayor valor agregado a los clientes y mantener como líder financiero en la región. [BAC-001]

El desarrollo de servicios y productos financieros usando avanzados recursos tecnológicos y la calidad de sus equipos, han permitido ocupar a BAC Credomatic de una posición de liderazgo en el Mercado financiero centroamericano. [BAC-002]

La Corporación BAC Credomatic Sociedad Anónima, conocida como Grupo Financiero BAC Credomatic de Costa Rica, está conformada por las siguientes sociedades:

- Banco BAC San José Sociedad Anónima.
- Credomatic de Costa Rica Sociedad Anónima.
- BAC San José Puesto de Bolsa Sociedad Anónima
- BAC San José Sociedad de Fondos de Inversión Sociedad Anónima.
- BAC San José Pensiones Operadora de Planes de Pensiones Complementarias Sociedad Anónima
- BAC Credomatic Corredora de Seguros Sociedad Anónima
- BAC San José Leasing, S.A
- Inmobiliaria Credomatic Sociedad Anónima.

Todos los miembros del grupo han obtenido el certificado de calidad ISO 9001:2008 cumpliendo los requisitos de calidad. Este certificado es un conjunto de reglas elaboradas por distintos comités técnicos, subcomités y grupos de trabajo, formados por miembros de varios países, cuyo objetivo principal es establecer normas para una gestión de calidad eficaz. Se basa en desarrollar, implementar y mejorar la eficacia de la gestión de cada proceso para aumentar la satisfacción del cliente mediante el cumplimiento de sus requisitos.

Los principios de la Norma ISO 9001:2008:

<p>Principio 1</p> <p>Organización orientada al cliente. Las organizaciones dependen de sus clientes y por lo tanto deberían comprender las necesidades actuales y futuras de los mismos, satisfacer sus requisitos y esforzarse en exceder sus expectativas.</p>	<p>Principio 2</p> <p>Liderazgo. Los líderes establecen la unidad de propósito y la orientación de la dirección de la organización. Ellos deberían crear y mantener un ambiente interno, en el cual el personal pueda llegar a involucrarse totalmente en el logro de los objetivos de la organización.</p>
<p>Principio 3</p> <p>Participación del personal. El personal, a todos los niveles, es la esencia de una organización y su total implicación posibilita que sus habilidades sean usadas para el beneficio de la organización.</p>	<p>Principio 4</p> <p>Enfoque basado en procesos. Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso.</p>
<p>Principio 5</p> <p>Enfoque de sistema para la gestión. Identificar, entender y gestionar los procesos interrelacionados como un sistema, contribuye a la eficacia y eficiencia de una organización en el logro de sus objetivos.</p>	<p>Principio 6</p> <p>Mejora continua. La mejora continua en el desempeño global de la organización debería ser un objetivo permanente de ésta.</p>
<p>Principio 7</p> <p>Enfoque basado en hechos para la toma de decisiones. Las decisiones eficaces se basan en el análisis de los datos y la información.</p>	<p>Principio 8</p> <p>Relación mutuamente beneficiosa con el proveedor. Una organización y sus proveedores son interdependientes, y una relación mutuamente beneficiosa aumenta la capacidad de ambos para crear valor.</p>

Tabla 16 Principios Norma ISO 9001:2008 [BAC-003]

Dirección Regional de Informática

La Dirección Regional de Informática fue creada para la atención de servicios de tecnología a nivel regional del grupo BAC Credomatic, la cual genera servicios a los países del grupo, a decir Honduras, El Salvador, Guatemala, Nicaragua, Costa Rica, Panamá y México.

DICA posee una serie de pilares:

- Centralización y estandarización
- Costos e Inversiones
- Continuidad y riesgos
- Calidad
- Cumplimiento ("*time to market*")
- Capacidad productiva
- Productividad
- Clima organizacional
- Alineamiento organizacional

Tal y como se indicó anteriormente, una de las responsabilidades de la *Dirección Regional de Informática* es mantener la estandarización de sus sistemas en todos los países en los cuales opera Bac Credomatic.

Cada país donde opera posee sus propios servidores sobre los cuales residen los sistemas estándar de la compañía.



Ilustración 19 Infraestructura de la empresa

Esto conlleva a una estrategia de TI que la empresa ha implementado durante mucho tiempo, el cual se puede resumir con la siguiente frase:

Sus sistemas son "estándar" y descentralizados

Estándar

La idea principal es que las características de sus sistemas se encuentren de forma íntegra y completa en todos y cada uno de los países en los cuales opera Bac Credomatic, permitiendo de esta manera ofrecer los mismos productos y la misma calidad a cada país en cuestión, esto además implica que su sistema es altamente parametrizable, permitiendo la flexibilidad necesaria para "*tropicalizar*" los elementos suficientes, con el fin de satisfacer los requerimientos y regulaciones particulares a cada país.

Por otro lado, esto conlleva todo un reto, pues generalmente cada país cuenta con más de un servidor, y cada uno de ellos debe estar preparado con los elementos suficientes para permitir un adecuado funcionamiento del sistema estándar. En resumen, el sistema estándar debe estar instalado correctamente en cada país donde el banco procesa, pero además dentro de cada país debe estar disponible en cada computador o servidor usado, de tal manera que permita la funcionalidad de los procesos propios del banco de forma normal y oportuna con el fin de proporcionar el servicio esperado por sus clientes.

Esta estandarización del sistema se lleva a cabo por medio de un proceso formal y regulado por una serie de directrices y un flujo de desarrollo debidamente respetado por todos los colaboradores, que de una u otra manera intervienen en alguna etapa del proceso de desarrollo.



Ilustración 20 Resumen de flujo de Desarrollo

Dentro del anterior flujo de desarrollo, el cual es un resumen general del verdadero, se puede apreciar por lo menos cuatro etapas del mismo:

- La etapa de análisis, en la cual se realizan todas aquellas actividades necesarias para poder identificar, clasificar y monitorear la implementación de los requerimientos solicitados por negocio.
- La etapa de Diseño, en la cual se determina el impacto en que se verá afectado el sistema estándar según los requerimientos recolectados en la etapa anterior. En esta etapa, se toman las debidas decisiones sobre la reutilización de elementos existentes en el sistema, o bien los nuevos elementos a ser implementados. En lo que respecta a base de datos, en esta etapa se determina el flujo de los datos en el diseño actual, o bien se determinan y revisan los diseños propuestos, los cuales deberán integrarse de forma ingenieril en la base de datos actual.
- En la etapa de programación, se ejecutarán una serie de actividades que servirán para implementar la solución planteada, así como las pruebas respectivas para su verificación. En esta etapa se crea toda la parametrización deseada con el fin de afectar solamente al país, al producto o al aplicativo en cuestión. Por lo delicada de esta etapa, esta

generalmente representa la mayor cantidad de tiempo en el cronograma del proyecto mismo.

- La etapa de "*Avance de Pase a producción*" es una serie de pasos que se deben cumplir con respecto al resguardo de la configuración del sistema, además se preparan los elementos que sean necesarios con el fin de realizar una instalación del proyecto en cada país y consecuentemente en cada servidor de producción de una manera lo más automáticamente posible. Posterior a esta etapa, se envían los elementos de instalación a cada servidor para su debida instalación.

Este flujo de desarrollo ha sido utilizado por el transcurrir del tiempo y ha dado resultados bastante satisfactorios, a pesar de cierta cantidad de incidentes y riesgos con que cuenta, que más adelante se detallará.

Descentralizados

Cuando se habla de sistemas descentralizados, se está haciendo hincapié en que la administración de los datos es responsabilidad de cada país, por tanto, cada uno de ellos posee su propia organización local junto con sus propios requerimientos que deben ser tomados en cuenta en el sistema estándar.

Lo anterior conlleva con ciertas características:

- Un equipo local de TI debe existir, el cual vela por el entendimiento de "*primer mano*" de los requerimientos locales y de esta manera validar la efectividad de las implementaciones locales dentro del sistema estándar

- La presencia de uno o varios servidores de producción sobre los cuales se instala el sistema estándar y se realizarán todos y cada uno de los cambios, que con el tiempo y debido a los cambios de negocio generen sobre el mismo sistema.
- La coordinación de un equipo local de operaciones que posee la responsabilidad de aplicar la instalación de cualquier cambio en el sistema.

ESTÁNDARES Y LINEAMIENTOS ACTUALES EN BAC CREDOMATIC

Objetivos del Sistema de Gestión de Calidad

- Asegurar que los productos y servicios prestados sean congruentes con los requisitos establecidos por los clientes
- Velar por que los productos y servicios proporcionados se encuentren dentro de los requerimientos legales, regulatorios y operativos de la región
- Contribuir a lograr y mejorar permanentemente la satisfacción del cliente y los resultados de negocio.
- Mejorar continuamente la organización, buscando siempre la eficiencia en sus procesos.

BAC Credomatic ha considerado como referencia primordial para su SGQ (Sistema de Gestión de Calidad) la norma Internacional ISO 9001:2008 además de otros documentos y normas de referencia tales como:

- Constitución de la república de cada país
- Ley de Bancos
- Normativas de las Superintendencias del Sistema Financiero

- Normas Prudenciales para Bancos
- Leyes de Lavado de Dinero
- Normativas y Políticas de Marcas de Tarjetas de Crédito
- Códigos de Comercio
- Normas de los Bancos Centrales
- Otras leyes o requisitos gubernamentales que sean necesarios
- Norma ISO 14001:2004 (Costa Rica)
- OSHAS 18001 (Costa Rica)
- Ley Sarbanes - Oxley (SOX)

Un resumen de algunas de las normas y/o directrices existentes en instituciones financieras, y que se usarán en la implementación de PO2 de Cobit son los siguientes:

Flujo de Desarrollo y Mantenimiento de Sistemas de Información

Su propósito es el de asegurarse que todos los cambios a las aplicaciones se realicen y controlen de manera ordenada, efectiva, consistente y estandarizada.

En este proceso se determinan todas las fases necesarias según la clasificación del proyecto, las cuales deben ser cumplidas a cabalidad con el objetivo de proveer una base sólida de elementos en busca de la máxima calidad posible de los sistemas.

Todo cambio al sistema estándar debe ser tramitado en varias instancias obteniendo la retroalimentación de las áreas de expertos con el fin de que el cambio signifique eventualmente algún tipo de mejora y evitando hasta donde sean posibles los impactos negativos.

Dentro de las áreas de expertos se encuentra el área de base de datos, de tal manera que cualquier cambio estructural deberá ser evaluado por la Gerencia de Arquitectura de TI, la cual dictará las pautas necesarias para que los cambios tomen

en cuenta las mejores prácticas y las directrices de diseño que contempla la organización, así como también que el diseño de base de datos sea el más adecuado según los requerimientos de negocio, los requerimientos técnicos y se acople de forma correcta con el estándar existente.

Por otro lado, no se desea generar alta complejidad sobre el actual proceso de desarrollo, por lo que se solicita procurar que cualquier cambio en dicho proceso no genere en sí un aumento en el tiempo que conlleva la finalización de los proyectos.

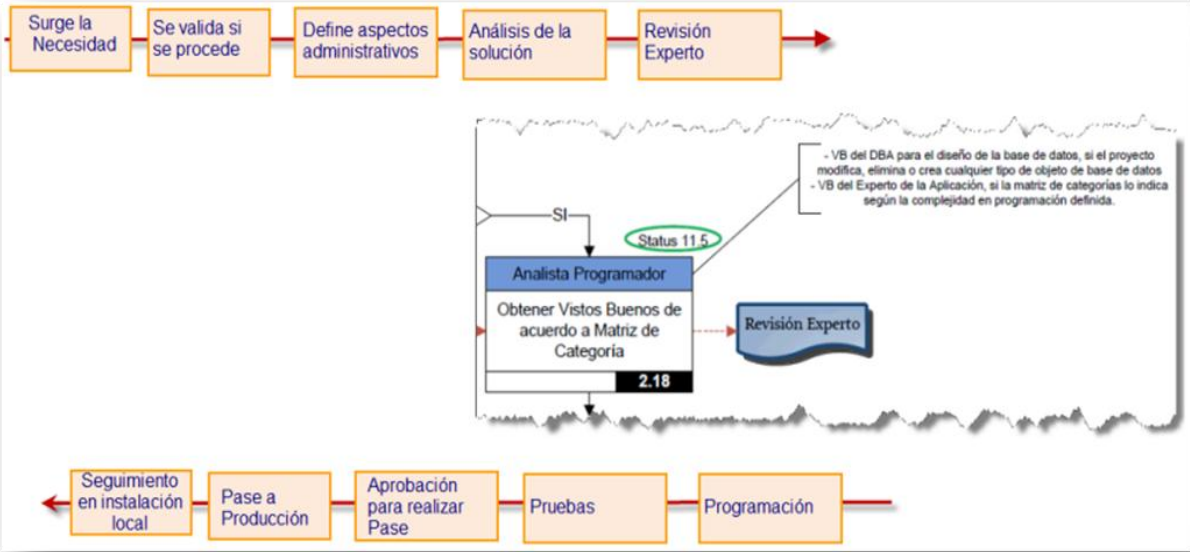


Ilustración 21 Punto de Control en Flujo de Desarrollo

Dentro de las etapas del flujo de desarrollo que interesarían en la implementación de PO2 de COBIT sobresalen las siguientes:

Etapa del Flujo	Descripción	Relación con PO2
Surge la Necesidad	Negocio identifica un problema y busca la forma de satisfacerla.	Comunicación Negocio-TI. <ul style="list-style-type: none"> • Necesidad del Diccionario de Datos
Revisión Experto	Momento en el desarrollo de proyectos en donde se tiene la definición de la solución y se pueden tomar decisiones.	<ul style="list-style-type: none"> • Modelo de arquitectura de información empresarial. • Implementación de reglas de sintaxis. • Alimentar Diccionario de Datos • Clasificación de Datos
Pase a Producción	Momento en que se envía a todos los computadores de la región la solución implementada.	<ul style="list-style-type: none"> • Actualización del Diccionario de Datos • Validación de controles de seguridad • Administración de la integridad
Seguimiento en Instalación local	Proceso manual de verificar que se instaló según lo esperado.	<ul style="list-style-type: none"> • Administración de la integridad
Monitoreo de la integridad en Producción	Proceso Manual.	<ul style="list-style-type: none"> • Administración de la integridad

Tabla 17 Requerimientos en implementación de PO2

Estándar De Clasificación De La Información

Su propósito es el de normar las reglas generales para la ejecución del Proceso de Clasificación de los Activos de Información de la empresa, con el objetivo de identificar los Activos de Información que debe proteger acorde al nivel de importancia que la Unidad de Negocio les asigne.

Se define la clasificación de datos de la siguiente forma:

- Clase1. **Pública:** Información pública (incluida información que ha sido categorizada como lista para ser enviada al público en general).
- Clase2. **Interna:** Información que es sensitiva fuera del negocio y debe ser protegida, información que solo debe ser conocida por colaboradores y personas que por razones del negocio necesiten conocer de dicha información, esto con la debida autorización.
- Clase3. **Confidencial:** Información sensitiva que se encuentra disponible solo para grupos específicos de personas.
- Clase4. **Restringida:** Información altamente sensitiva que se encuentra disponible solo para un selecto grupo de personas.

Resumen de Lineamientos:

- Todo activo de información debe poseer un dueño de la información
- Todo activo de información debe ser protegido según el valor para la unidad de negocio
- La información requiere la aplicación de controles de acuerdo a su sensibilidad

Relación con PO2: Establecerá las pautas a tomar en cuenta para la correcta clasificación de los datos. Se deberá actualizar con el objetivo de indicar claramente los aspectos a tomar en cuenta en lo que información electrónica se refiere, específicamente a objetos de base de datos.

Plan De Seguridad de la Información

Su propósito es el de administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio. Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.

Relación con PO2: Se fomenta la creación de un comité de alto nivel dentro de la compañía para la generación de proyectos alineados específicamente en aspectos de Seguridad.

Esquema de la Información

Su propósito es el de brindar la guía para que las áreas de negocio puedan inventariar y clasificar su información de una forma estandarizada y además garantizar que la ejecución de este proceso sea sostenible en el tiempo.

Se encuentra orientado hacia la administración, inventario y clasificación de la información física que cada Unidad de Negocio posee.

Relación con estándares: Se encuentra alineada con la normativa de la industria de tarjetas de Pago PCI-DSS, las secciones respectivas del Manual de Calidad de la organización, a la regulación emitida por SUGEF y a los estándares ISO 27001 y 27002.

Elementos de Clasificación de la Información

Este estándar contiene la matriz de activos de información que las áreas de negocio han pre clasificado de acuerdo al valor que estos representan para la empresa. Las áreas de Negocio deben utilizarla como apoyo a la ejecución del proceso de clasificación de información.

Aspectos Importantes: Enlista los criterios que deben ser tomados en consideración al momento de intentar clasificar un dato específico.

Clasificación De Activos De La Información

Este formulario es la base que sirve para recopilar toda la información relacionada con los activos de información del GFBC. Su uso principal es para efectos de permitir levantar inventarios de activos de información, clasificarlos y permitir la definición de responsabilidades a un alto nivel.

Capítulo 4

Planteamiento de Necesidades

En BAC Credomatic se han realizado esfuerzos bastante importantes en lo que respecta a formalismo y orden en la elaboración de los proyectos de mantenimiento del sistema estándar, pero a pesar de esto es necesario mejorar algunos procesos importantes en lo que respecta a la implementación de una debida Arquitectura de Información Empresarial .

En lo que a integridad se refiere, se ha estado trabajando a nivel técnico, determinando controles que vienen a asegurar de cierta manera, la integridad de los datos:

- Uso de llaves foráneas (*integridad referencial*)
- Uso de restricciones sobre campos (*check constraints*)
- Uso de tipificación (*Types*)
- Lógica de negocio a nivel de base de datos (*Triggers, Funciones, Stored Procedures*)
- Abstracción y protección de datos (*Vistas, Tablas materializadas*)
- Estrategias de modernización (*vistas lógicas*)

No obstante a lo anterior, y guiado por la tendencia de un proceso de mejoramiento continuo, se ha determinado la necesidad de algunos esfuerzos extra en lo que a integridad se refiere dentro de los computadores de producción.

Algunas de las situaciones especiales detectadas en pro de una mejora en sus procesos se presentan a continuación.

Mejora en la participación directa de Negocio

Hasta el día de hoy, la participación principal de Negocio en los desarrollos del sistema estándar ha sido, la colocación de nuevos requerimientos, los cuales nacen por el movimiento del mercado esencialmente, no obstante la injerencia de TI en la implementación tiene un papel protagonista, pues cuenta con un control completo sobre los elementos implementados en el sistema estándar y que algunos de estos elementos le son desconocidos a Negocio.

Se considera necesario un protagonismo más efectivo de Negocio en lo que respecto a los datos almacenados por el sistema estándar, al final y al cabo, los datos son considerados el activo más indispensable para la toma efectiva de decisiones, y si estos no se encuentran identificados, protegidos y administrados por negocio, será muy difícil la determinación de los mejores mecanismos para mantener la integridad de datos.

Todo lo anterior conlleva a la necesidad de un compromiso y a una toma de responsabilidad más efectiva con respecto a los datos que maneja la compañía por parte de las áreas de negocio, de esta manera la participación de Negocio no será únicamente para el desarrollo de nuevos requerimientos, sino también para la mantenibilidad y persistencia de los datos que actualmente cuenta la empresa y que le son necesarios para la elaboración de nuevos productos y nuevas decisiones.

Mejoramiento de la arquitectura para la toma oportuna de decisiones

Actualmente la empresa cuenta con mecanismos totalmente orientados a nivel técnico para el análisis de las estructuras de base de datos que se encuentra en producción, pero se deben realizar los esfuerzos necesarios con el objetivo de mejorar la arquitectura actual, de tal manera que permita de una manera ágil y oportuna mostrar los diferentes elementos con que se compone el sistema estándar, lo cual permitirá la debida toma de decisiones ya sea de implementar nuevos productos con el sistema tal y como se encuentra hoy en día, o bien, el nacimiento de nuevos requerimientos para la mejora del sistema de tal manera que facilite a negocio la entrega de productos oportunos a sus clientes.

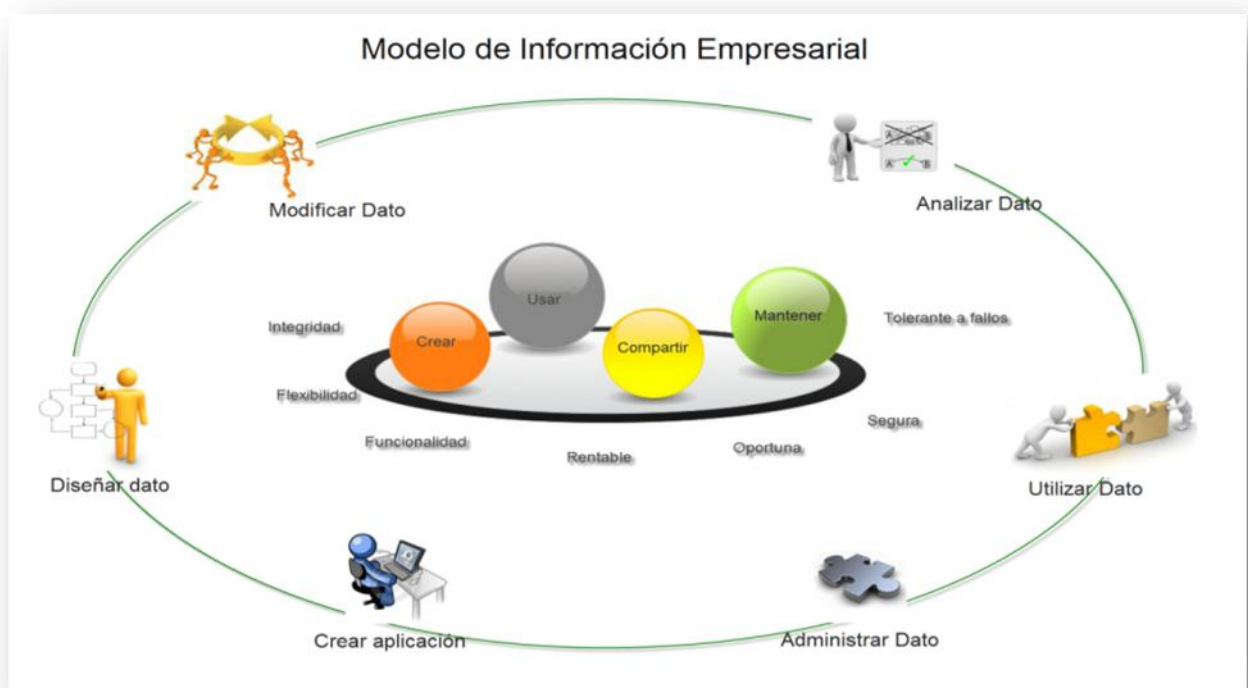


Ilustración 22 Modelo de Información Empresarial

Mejora en la implementación del Diccionario de datos Empresarial

Es necesario la implementación de un mecanismo sencillo en donde se puedan incluir las distintas reglas de sintaxis sobre los datos de la organización.

La idea esencial del Diccionario de datos Empresarial es que permita el compartir elementos de datos a través de las distintas aplicaciones que soporta la empresa así como de sus distintos sistemas existentes, de tal manera que pueda promover o fomentar un entendimiento común de datos entre los usuarios de TI y los usuarios de negocio, y la comunicación entre ambos sea muchísimo más fluida.

Además del entendimiento común, lo que se busca es un cumplimiento efectivo de las reglas de sintaxis acordadas en el diccionario de datos empresarial, de tal manera que estas sean respetadas a lo largo y ancho de la empresa, y así evitar problemas de ambigüedad, duplicidad o malos entendidos en lo que a conceptos e impacto se refiere de los distintos elementos de dato pertenecientes a la compañía.

Mejora en la unificación de enfoques sobre estándares ya implementados.

BAC Credomatic como entidad financiera que es, se encuentra regulada por una serie de estándares y regulaciones que le son dados tanto por aspectos internos como externos. Muchos de estos estándares velan por la calidad e integridad de la información resguardada por la compañía, no obstante cada uno de estos aplica su propio enfoque llevando sus controles a un objetivo específico.

Se considera necesario aprovechar el esfuerzo realizado en la implementación de cada uno de estos estándares, alineando los aspectos en común, con el objetivo de permitir la adaptación correcta y efectiva para una implementación de arquitectura de información empresarial. Este alineamiento de aspectos en común hará más

robusta la implementación de la arquitectura y permitirá la reutilización de elementos ya implementados y posiblemente probados con el tiempo, y que de una u otra manera afectan procesos internos de la empresa.

Mejora en el mecanismo de clasificación de datos

Actualmente se cuenta con lineamientos para la correcta clasificación de datos, en la cual se permite determinar cuan sensible y crítica puede ser un elemento de datos, no obstante es necesario mejorar el mecanismo de clasificación de tal manera que logre determinar la inclusión de nuevos elementos de datos al sistema y por ende, se logre su correcta clasificación.

Por medio de una correcta clasificación sobre elementos de datos, se podrá ser capaz de implantar controles de protección de dichos elementos, además de tomar decisiones tales como la retención de dichos datos y su posible destrucción.

Mejora en el proceso para la determinación de la propiedad de los datos

Tal y como se comentó anteriormente, la arquitectura con que cuenta la empresa es la de un sistema estándar pero descentralizado, por tanto, cada país tendrá la oportunidad de operar el sistema estándar, no obstante los datos son particulares para dicho país. La propiedad de datos es un aspecto sumamente importante para la determinación de decisiones con respecto al dato almacenado en la base de datos, decisiones tales como tipos de respaldos que se deben hacer, su frecuencia, la limpieza de datos en los archivos, los controles para la determinación de la validez de la integridad de los datos en cualquier momento, etc. Cada uno de estos aspectos viene a corresponder a las distintas responsabilidades que el propietario de datos debe asumir.

Al ser un sistema descentralizado, y al conocer que el comportamiento de los datos en los distintos países podrían ser distintos en lo que respecta a tamaño y calidad de los mismos, además que la toma de decisiones de productos es particular a cada país, es donde nace la necesidad de mejorar hacia un proceso efectivo y sencillo para la determinación de los dueños de los datos según el país y servidor en cuestión.

Es necesario la mejora dentro de la metodología actual que sea capaz de asignar la propiedad de los datos de una manera efectiva, enfrentándose con las situaciones antes citadas, además abarcando tanto las estructuras de datos que actualmente existen como las nuevas implementaciones. La metodología además tiene que delimitar las responsabilidades y derechos de los propietarios de los datos, así como también se deberá definir la injerencia de los administradores regionales sobre los locales, de tal manera que exista una debida sincronización de los roles y que las estrategias de resguardo de datos se coordinen según las necesidades del negocio de una forma general y estandarizada.

Mejora en el proceso de identificación de datos a los cuales asignarles controles de seguridad

Debido a los cambios en el mercado, cada día nacen nuevos requerimientos que en muchas ocasiones provocaran la creación o modificación de datos de la actual base de datos, por tanto es necesario ser capaces de identificar cuando esos nuevos datos o el cambio de alguna estructura existente, provocará la presencia de datos sensibles, los cuales se le deberá colocar sus respectivos controles de seguridad según los lineamientos que para tales efectos existen.

Este proceso deberá ser mejorado teniendo en mente ciertas características fundamentales:

- *Debe ser oportuno.* De tal manera que permita que la asignación de los debidos controles de seguridad sobre los datos en cuestión se desarrollen de forma coordinada con la elaboración del proyecto en sí, de tal manera que no venga a generar un desfase en la calendarización completa del proyecto.
- *Asignación correcta de controles.* De tal manera que los debidos controles se asignen a los datos correctos, evitando:
 - la asignación de controles a datos que no los requieren
 - no asignación de controles a datos sensibles que si lo requieren
 - Asignación de controles incorrectos a datos sensibles
- *Atención particular al dato.* Se debe identificar el dato sensible que se desea almacenar en la base de datos, y determinar la conveniencia o no de que dicho dato se encuentre allí, de tal manera que se validen las regulaciones con que la empresa actualmente cuenta, como por ejemplo, según la regulación de PCI DSS no se debe almacenar el número de tarjeta de ninguna manera dentro de la base de datos.

Mejora en la validación de los acuerdos del diseño con respecto a lo implementado

Tal y como se indicó anteriormente, existe una etapa de análisis y diseño, en el cual se evalúa el modelo de datos, y es precisamente en este momento en que junto con los requerimientos del proyecto, así como también teniendo en mente la arquitectura de la base de datos, se determina los elementos de datos más adecuados.

Posterior a estas etapas, continúan las otras etapas igualmente importantes, como son la etapa de desarrollo, implementación, pruebas, etc. Durante el transcurso de dichas etapas podrían presentarse cambios, nuevas necesidades o imprevistos que

de una u otra manera podrían impactar al modelo de datos acordado en la etapa de diseño, y si estos nuevos insumos no son presentados nuevamente para su revisión por las áreas respectivas, podría generar posibilidad de acarrear las siguientes consecuencias:

- Incorrecta actualización de la documentación del modelo de datos del proyecto en cuestión.
- Falta de análisis y revisión de los nuevos cambios en el modelo de datos
- Ausencia de controles de seguridad si fuese necesario su aplicación
- Posibilidad de no cumplimiento de regulaciones en el resguardo de datos
- Riesgos que rompan la arquitectura actual de la base de datos
- Ausencia de clasificación, propiedad y sintaxis estándar de los nuevos elementos de datos

Esto además es importante para poder determinar que todos los controles acordados, así como todas las características del modelo acordado en dichas etapas tempranas del proceso de desarrollo se hayan implementado de la forma correcta y esperada que se tenía en mente cuando se diseñaron, de tal manera que mantengan una consistencia entre el diseño y su implementación.

Es importante señalar, que en cualquier momento pueden existir cambios en el modelo, pero estos deben ser validados por las áreas responsables y colocados los procesos adecuados de resguardo de datos, y estos cambios formarían los nuevos acuerdos a validar al final del proceso.

Mejora en la determinación de la correcta instalación en equipos regionales

Debido a la infraestructura con que cuenta Bac Credomatic a lo largo de la región, se puede tener presente que la cantidad de servidores de producción en los cuales el sistema estándar reside es una cantidad importante. Dado lo anterior, se ha

intentado que la instalación de los pases a producción se realice lo más automáticamente posible, con la participación mínima de procesos manuales. Esto aunado con la complejidad y particularidad de cada proyecto generan en sí todo un reto, y en ocasiones procesos muy complejos para la evaluación de la correcta instalación de los pases en cada servidor.

Dicha evaluación en la mayoría de los casos, es un proceso muy particular del proyecto en cuestión, y depende fuertemente de las destrezas y experiencias de los desarrolladores responsables del proyecto, lo cual en sí genera un riesgo pues en muchas ocasiones, debido al *"time to market"* de negocio, los analistas se encuentran desprovistos del tiempo y mecanismos adecuados para realizar dicha evaluación, por lo que realizan entonces, una evaluación subjetiva y rápida, generando un riesgo en la ejecución correcta de dicho aplicativo.

Todo lo anterior genera la necesidad de un control más automático y estándar para la validación de la integridad estructural de todo cambio en la arquitectura de la base de datos, el cual se realice de una forma objetiva y que le sirva de insumo tanto al analista como a los responsables de los servidores locales para poder con certeza determinar la instalación correcta de cada uno de los elementos de dato impactados por el pase a producción instalado.

Mejora en el mecanismo de monitoreo de la integridad estructural en los computadores de la región

Debido al riesgo de poder detectar inconsistencias entre las estructuras que deberían estar y las que se encuentran efectivamente en producción, es que es necesario el mejoramiento del monitoreo de la integridad estructural. Algunos de estos riesgos, podrían ser los siguientes:

- Falta de validación a la hora de la instalación del pase a producción, y no detección oportuna de errores o problemas presentado en dicho paso.
- Eliminación involuntaria de estructuras de base de datos por parte de los operadores de los equipos de producción debido a desconocimiento del impacto de realizar ciertas operaciones. Por ejemplo, la eliminación y nuevamente creación de una tabla sin tener el cuidado de recrear la integridad referencial, o la colocación de los respectivos triggers.
- Generación de nuevas estructuras en producción permitiendo acceder a datos sensibles sin los controles debidos. Nuevas estructuras tales como vistas, triggers, etc.
- Alteración de estructuras de datos que podrían generar riesgo principalmente en lo que al estándar del sistema se refiere. Por ejemplo, procedimientos almacenados conteniendo lógica de negocio que podría haber sido alterada en algún equipo de producción ya sea cambiando la regla de negocio o bien, incrementando algún tipo de proceso colocando en riesgo la exposición de los datos.

Es necesario el mejoramiento del mecanismo para el monitoreo constante de las estructuras de datos que se encuentran en producción de tal manera que se pueda certificar a negocio la integridad estructural del sistema estándar y de esta manera se puedan tomar las decisiones que se consideren más adecuadas sobre la base del sistema.

Capítulo 5

Solución propuesta

Luego de haber definido todos y cada uno de las situaciones a tomar en cuenta en los procesos actuales de BAC Credomatic y aunado con la proyección de tener que implementar PO2 en algún momento, se ha llegado a la conclusión de que el diseñar el proceso de PO2 vendría a satisfacer muchas de las necesidades que actualmente se tienen, además se tendría la oportunidad de encausar muchos de los procesos que ya hoy en día existen dentro de la compañía hacia el objetivo que se persigue, que fundamentalmente es, la búsqueda de una Arquitectura de Información Empresarial adecuada.

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.



Ilustración 23 Requerimientos del Negocio COBIT

Esencia de COBIT

“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...” [GOV-007]

“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”.

[GOV-007]

Es precisamente esta esencia de COBIT que se ajusta perfectamente a las necesidades identificadas dentro del proceso de la empresa. COBIT ofrece los controles mínimos que debería aplicar una organización de TI, donde un Control podría ser definido como:

“Las Políticas, Procedimientos, Prácticas y Estructura Organizacional, diseñadas para proveer una razonable seguridad de que los objetivos del negocio serán alcanzados y los eventos indeseados serán prevenidos o detectados y corregidos.” [COS-001]

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. [GOV-07]

Dentro del marco de COBIT esos dominios son conocidos como:

- 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. [GOV-07]

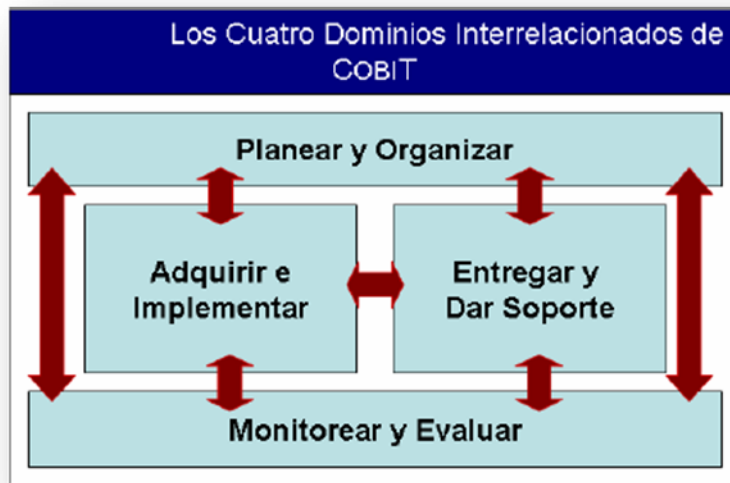


Ilustración 24 Dominios COBIT [GOV-007]

Con respecto al dominio de Planear y Organizar (PO) este cubre las estrategias y tácticas con el objetivo de identificar la mejor manera en que TI puede contribuir a alcanzar los objetivos de negocio, en este dominio se debe implementar una estructura organizacional y una estructura tecnológica adecuada, en resumen se cubren cuestionamientos tales como:

- ¿Están correctamente alineadas las estrategias de TI y de negocio?
- ¿Se hace uso óptimo de los recursos?
- ¿Los objetivos de TI son conocidos y entendidos?
- ¿Se administran los riesgos de TI?

- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio? [GOV-07]

Entendiendo lo anterior, es que se determina que PO2 "Definir la arquitectura de Información" es la base sobre la cual se desea implementar.

PO2 de Cobit

Modelo de Arquitectura de información empresarial

La idea de este dominio es generar los siguientes elementos dentro de los procesos de la empresa:

- Sistemas de información debe crear y actualizar de forma regular y ordenada un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esa información.
- Se debe desarrollar un diccionario corporativo de datos que mantenga las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad.
- Este proceso debe asegurar que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias de 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.

PO2 intenta satisfacer 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.

Entre las ventajas más relevantes de la implementación de PO2 se encuentran:





<ul style="list-style-type: none">• Mejora la calidad de la toma de decisiones	
<ul style="list-style-type: none">• Racionaliza los recursos de los sistemas de información.	
<ul style="list-style-type: none">• Genera responsabilidad sobre la integridad y seguridad de los datos	
<ul style="list-style-type: none">• Mejora la efectividad y control de la información	

Tabla 18 Ventajas en la implementación de PO2

Este dominio se encuentra compuesto de cuatro objetivos de control:

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. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de manera que conserva la integridad y es flexible, funcional, rentable, oportuna, segura y tolerante a fallas. [GOV-07]

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., facilitando la compartición de elementos de datos entre las aplicaciones y los sistemas, fomentando un entendimiento común de datos entre los usuarios de TI y del negocio, y previniendo la creación de elementos de datos incompatibles. [GOV-07]

PO2.3 Esquema de clasificación de datos

Establecer un esquema de clasificación que aplique a toda la empresa, basado en qué tan crítica y sensible es la información 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, una breve descripción de los requerimientos de retención y destrucción de datos y finalmente la forma de determinar qué tan críticos y sensibles son los datos. [GOV-07]

PO2.4 IT Administración de la integridad

Definir e implantar 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. [GOV-07]

PASOS DE IMPLEMENTACIÓN PO2 EN BAC CREDOMATIC

Luego de haber realizado el análisis presentado previamente, tanto de los factores en común de los estándares aplicados dentro de Bac Credomatic que afectan de una u otra manera la Arquitectura de Información Empresarial, como la identificación de los factores a implementar dentro de la empresa, todo esto orientado por el dominio de PO2 de COBIT, es que se han identificado 7 elementos indispensables para alcanzar los objetivos propuestos:

- Definición del Diccionario de Datos Empresarial
- Proceso de asignación de propiedad de Datos
- Metodología para ejecutar el esquema de Clasificación de datos
- Cambios en el Proceso de revisión de Base de Datos
- Proceso de validación de integridad de diseño antes de envío de pase a producción
- Proceso de validación de integridad a la hora de la instalación del pase en cada computador de producción
- Proceso de monitoreo de integridad estructural en los computadores de producción

Cada uno de estos 7 elementos son esenciales para alcanzar la implementación de la arquitectura empresarial que se requiere, dado esto, cada uno de estos se relaciona con un proceso descrito en los anexos del presente documento, pero antes se justificará cada uno de estos.

DEFINICIÓN DEL DICCIONARIO DE DATOS EMPRESARIAL

La definición de datos empresariales es una muy buena práctica con el objetivo de usarlas a través de procesos funcionales, servicios y controles. Esta definición trae consigo claridad y consistencia a la integración de sistemas, y otros proyectos empresariales, además es la base para la implementación del proceso de PO2 que se desea en la compañía.

El diccionario de datos que se desea implementar contempla básicamente la definición de cada uno de los datos que la empresa posee, de tal manera que se pueda proporcionar una comunicación abierta entre Negocio y TI, además entre las distintas áreas de TI, de tal manera que los conceptos en sí mismo sean estándar y vengán a convertirse en comunes para todos los interesados.

Tal y como se indicó anteriormente, el diccionario de datos viene a traer una equivalencia entre los conceptos de negocio con respecto a los elementos de datos que técnicamente se están generando, de tal manera que se provoque una comunicación fluida.

Por otro lado, cada concepto de negocio posee su propio grupo de hechos o reglas de negocio, que deben ser implementadas de una u otra manera, y es necesario también determinar la forma en que negocio podrá visualizar dichas implementaciones de una manera sencilla y correcta.

Con el objetivo de poder implementar dicha equivalencia de conceptos, y por ende, la generación del diccionario de datos, se cuenta con los siguientes elementos de acción:

- Negocio genera sus propios conceptos de negocio con el objetivo de determinar de una manera específica una funcionalidad o necesidad y poderle dar el seguimiento adecuado.
- Estos conceptos o términos de negocio serán incluidos como definiciones de datos dentro del Diccionario de datos.
- Estos conceptos o términos de negocio generan por sí mismos una serie de hechos o sentencias que definen asociaciones entre los datos.

- Estos hechos se convertirán en reglas de negocio que servirán para proveer el comportamiento esperado sobre la manipulación de dichos términos o datos.
- Cada uno de esos términos o conceptos deben ser representados en TI como elementos de datos, que a su nivel más básico representarán entidades, atributos u objetos de base de datos.
- Cada una de las reglas de negocio o Hechos identificados por Negocio, deberán ser interpretados por TI como parte del modelo de datos representando asociaciones entre datos y demás elementos de implementación de reglas de negocio.
- Todos estos elementos deben coordinada y ordenadamente ser agregados dentro del diccionario de datos de tal manera que provea una fuente de insumo tanto para la toma de decisiones de negocio como para el análisis y diseño en TI.



Ilustración 25 Diccionario de Datos Empresarial

Los principios básicos que se buscan con la generación del diccionario de datos son los siguientes:

- Posea toda la terminología o conceptos de negocio, por medio del cual negocio pueda abstraer la información que requiere y pueda realizar la toma de decisiones que sea necesaria.
- Se definan explícitamente todas las reglas de sintaxis de los datos en común de tal manera, que haya uniformidad entre ellos, y exista un conocimiento de dicha información para todos los interesados.
- Se determinen cada una de las reglas de negocio más apropiadas para cada uno de los conceptos de negocio colocado dentro del diccionario de datos, de tal manera que se permita ver los requerimientos y/o restricciones de una manera eficiente, sencilla y entendible por todos.
- Para cada término de negocio determinar los elementos de datos a satisfacer dicho requerimiento permitiendo una interpretación fluida entre negocio y TI.
- Una definición completa y actualizada del modelo de datos implementado en la compañía
- Para cada elemento de datos se debe contar con su respectiva clasificación de datos lo cual permita una trazabilidad de la ubicación de datos sensibles dentro del modelo de datos.
- Sobre elementos de datos sensibles, se debe tener descrito los procesos de seguridad aplicados según las normas actuales para dicho fin.
- Se debe contar con una amplia documentación de definición del dato para validar su consistencia e impacto.
- Los datos podrán tener distintos estados que indicarán la factibilidad de su uso. Entre los estados de los datos sobresalen su existencia en producción o bien un estado de desarrollo e implementación.
- Se podrá ser capaz de identificar de forma exacta el propietario de cada uno de los elementos de datos siendo esta forma la manera centralizada de validar que los controles realmente se están implementando de la forma deseada.
- El diccionario de Datos permitirá el acceso tanto de usuarios de negocio como de usuarios técnicos, centralizando así la fuente de conocimiento y convirtiéndose en la base de la Arquitectura de información que se anda buscando.

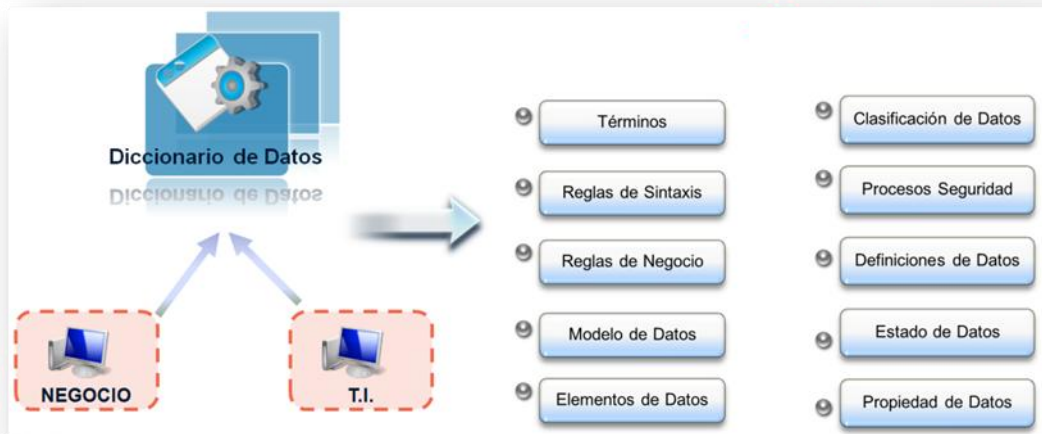


Ilustración 26 Perspectivas del Diccionario de Datos

Proceso del Diccionario de Datos

Tal y como se comentó en capítulos previos, actualmente se encuentra dentro del flujo de desarrollo, un punto de control de revisión del diseño de base de datos. Este punto de control por estándar es de carácter obligatorio y la idea es generar el diseño de base de datos más adecuado posible para la satisfacción de los requerimientos de negocio del proyecto actual así como también para mantener la consistencia con la arquitectura actual de la base de datos del sistema estándar.

En esta etapa de diseño de los proyectos de la empresa, se cuenta con los siguientes elementos:

- Requerimientos de negocio
- Requerimientos técnicos
- Definición del modelo de datos para satisfacer los requerimientos dados.

Durante esta etapa de definición del modelo de datos para el proyecto, se deben definir claramente tanto los conceptos como reglas de negocio a ser aplicados dentro del modelo de datos. Con estos insumos, y en acuerdo con todos los involucrados, se llega a la solución encontrada de tal manera que se permita continuar con el desarrollo del proyecto.

Es precisamente en esta etapa que se requiere sea alimentado el Diccionario de Datos, pues es en esta etapa en donde se aclaran todas las dudas de diseño del proyecto en cuestión, y se define los elementos de datos adecuados para satisfacer cada uno de los requerimientos de negocio.



Ilustración 27 Insumo del Diccionario de Datos

Alimentando el diccionario de datos en esta etapa del proyecto, se podrá ser capaz de identificar el avance del desarrollo de los proyectos, cuales ya se encuentran en producción y cuales aún están en desarrollo, facilitando la toma de decisiones tanto a nivel de negocio como técnico. Permitirá además llevar un control sobre el diseño acordado, sobre los controles de seguridad impuestos sobre los datos y la propiedad de datos encontrada de tal manera que pueda ser consultada aún antes de que sea enviado a producción el desarrollo final del proyecto.

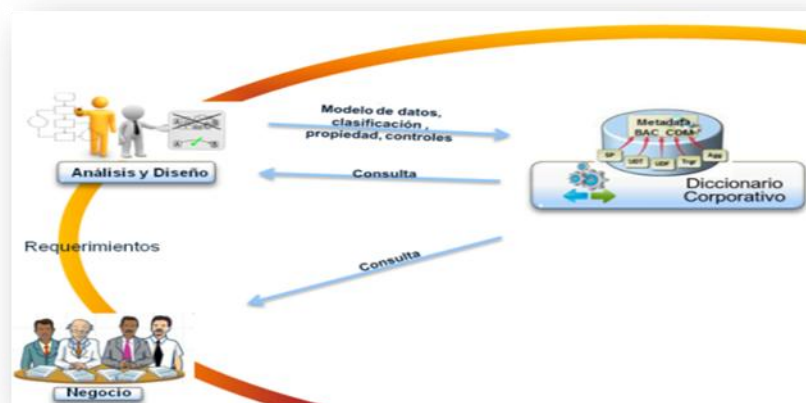


Ilustración 28 Flujo del Diccionario de Datos

PROCESO PARA EJECUTAR EL ESQUEMA DE CLASIFICACIÓN DE DATOS

Dentro del mismo punto de control de revisión del diseño de base de datos que actualmente existe en el flujo de desarrollo aplicado en los proyectos de la empresa, se desea generar el proceso de clasificación de los datos, pues tal y como se mencionó anteriormente, es precisamente en esta etapa en donde se definirán los elementos y reglas de datos necesarios para satisfacer los requerimientos de negocio y por ende es totalmente factible la identificación de cada una de las clases de datos a ser implementadas.

Para tal efecto, se encuentra disponible una serie de estándares y lineamientos que con anterioridad fueron expuestos en el presente documento, y que servirán de base para ser capaces de identificar la sensibilidad de los datos, y así clasificarlos y posteriormente solicitar los controles que sean necesarios de acuerdo a dicha clasificación, con el fin de salvaguardar dichos datos.

Es importante aclarar que en esta etapa, y de acuerdo a la sensibilidad determinada de los datos, la participación del departamento de Seguridad de Información es fundamental, pues son precisamente ellos los que determinarán los controles que serán exigidos según los lineamientos publicados al momento del análisis.

Al involucrar al departamento de Seguridad de Información, cabe la posibilidad de que el requerimiento de datos sea rechazado por intentar violentar alguna regulación vigente, no obstante todos los involucrados deberán coordinar esfuerzos para poder llegar a acuerdos satisfactorios y de una u otra manera, satisfacer los requerimientos a alto nivel que negocio solicita.

Proceso de Clasificación de Datos

Para poder ser capaces de realizar una clasificación adecuada de los datos en cada uno de los proyectos siguiendo las pautas de estándares que rigen actualmente a la compañía es que se definió el siguiente flujo:

- En la etapa de diseño, y específicamente en el punto de control de revisión de diseño y tomando como base el "Estándar de clasificación de la información" y el lineamiento de "Los elementos de clasificación de la información", el Arquitecto de Datos determinará si dentro del modelo analizado, existe la presencia de datos sensibles.
- De presentarse la situación anterior, se solicitará una reunión con el departamento de Seguridad de Información para analizar conjuntamente los datos sensibles encontrados.
- El departamento de Seguridad de Sistemas aplicará la "Política de Seguridad de la información" para evaluar la factibilidad o no de mantener el dato sensible en el modelo de datos analizado.
- A partir del punto anterior, será posible una reclasificación del dato, o bien, se determinarán los controles de seguridad requeridos según la sensibilidad del dato.
- Luego de llegar a los acuerdos anteriores, se registrará en el diccionario de datos dichas decisiones, documentando los controles que sean necesarios y que deberán ser implementados en el desarrollo del proyecto en cuestión.

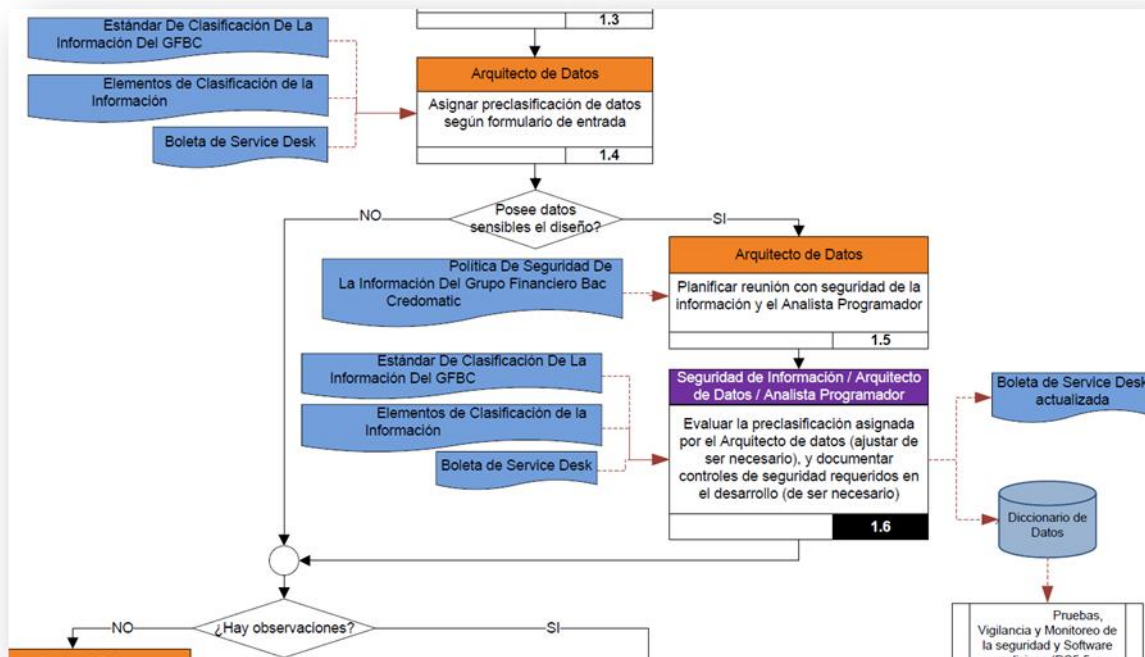


Ilustración 29 Proceso de clasificación de Datos

Cabe señalar que existe un compromiso fuerte entre el departamento de base de datos; encargada de realizar el punto de control de revisión de base de datos; y el departamento de Seguridad de la Información en lo que respecta a mantener una sincronización efectiva con el objetivo de mantener actualizado el diccionario de datos y que la clasificación de los datos se realice de la manera más efectiva posible, con el objetivo de que no haya contradicciones u omisiones que podrían acarrear problemas de exposición de datos.

PROCESO DE ASIGNACIÓN DE PROPIEDAD DE DATOS

Uno de los objetivos de COBIT y específicamente PO2 es el involucramiento de negocio en la administración de los datos que le son particularmente importantes. La "propiedad de datos" permite que negocio asuma el rol de dueño del dato, y TI el rol de custodio de dicha información.

El objetivo de este punto es el de asegurarse que todos los activos de información (datos) cuenten con un dueño asignado que tome decisiones sobre la manipulación, integridad, consistencia de los datos, clasificación y derechos de acceso.

El propietario se deberá apoyar en los grupos de operaciones y seguridad de información con el objetivo de permitir el cumplimiento de las directrices internas, sin embargo, el propietario permanecerá como el responsable general del dato.

Lo primero que se determinó fueron las responsabilidades que tendría cada uno de los propietarios de datos, entre las que sobresalen las siguientes:

- *Determinación del borrado (depuración) del dato según los requerimientos de negocio y las regulaciones del país.*

En la empresa se tiene actualmente un proceso denominado "Housekeeping", el cual es un proceso automático para la limpieza controlada y calendarizada de datos en cada una de las tablas registradas en el proceso, y que es parametrizable de tal manera que permite el borrado de datos a un país en particular y hasta por servidor en especial.

El objetivo es que el propietario del dato, sea quién según sus necesidades y regulaciones indique la parametrización más adecuada para cada una de los datos bajo su tutela.

- *Determinación de la política de respaldo de sus datos según los requerimientos de negocio y las regulaciones del país.*

Se requiere el que el propietario de los datos sea quién; según sus criterios y necesidades; determine los rangos de tiempo más adecuados para el respaldo de la información de tal manera que se cumplan con las regulaciones pero además que se permita la disponibilidad suficiente de la información necesaria en los computadores de producción.

- *Determina controles que considere necesario se implemente sobre el dato en particular.*

A parte de los controles que Seguridad de Sistemas está interesada en aplicar sobre los datos, también es necesario determinar cualquier otro tipo de control que debido a la naturaleza del dato se considere también necesario. Ejemplos de estos tipos de control son la mancomunación o autorización previa de cambios de datos sobre maestros, el monitoreo de cambios vía bitácoras de eventos, etc.

- *Aprueba o no RFC para cambios de datos cuando lo requiera el CAB*

Toda solicitud de cambio de datos (RFC) es enviada al grupo evaluador de dicho cambio (CAB) y este órgano determinará cuando es necesaria la

aprobación de un propietario del dato con el fin de no impactar de forma negativa ninguno de los aplicativos vigentes a la fecha.

- *Definir los roles de usuario autorizados para acceder a los datos de su pertenencia*

El propietario será el responsable de definir quiénes pueden acceder a los datos y quiénes de ellos podrían alterar de alguna manera dichos datos.

Esta definición de roles debe estar alineada con la política de protección de datos, pero además está orientada a que se pueda proteger el acceso a dichos datos según las necesidades propias del aplicativo.

- *Aprueba o rechaza requerimientos de extracción de datos de su propiedad*

El propietario del dato será el responsable de autorizar o no la extracción y manipulación de datos fuera de su fuente, de esta manera hay seguridad de que dicha manipulación se realiza con los mecanismos y los objetivos claros y correctos.

- *Asigna y monitorea la clasificación sobre el Activo de información según lineamientos publicados*

El propietario de los datos es el responsable por la correcta clasificación de los datos siguiendo los lineamientos estipulados para tal caso, de tal manera que se tenga la seguridad que todos los datos han sido debidamente clasificados.

- *Definir los principios de disponibilidad, confidencialidad, consistencia e integridad del dato*

Definir claramente todos los aspectos necesarios alrededor del dato bajo su responsabilidad de tal manera que dichos aspectos sean públicos y formales, de tal manera que pueda aclarar cualquier ambigüedad o duda que alguien pudiese tener al respecto.

- *Conocer el flujo del dato a través de las aplicaciones*

Por ser propietario de los datos también será responsable del flujo o camino que recorran dichos datos a través de las aplicaciones y dentro y fuera del sistema, manteniendo de esta manera un control sobre los movimientos de los datos a través de la empresa.

Para efectos de administrar correctamente el proceso de "Propiedad de datos" se ha creado un concepto que internamente se ha denominado "Datos empresariales".

Datos Empresariales

Es una terminología interna en Bac Credomatic para clasificar o agrupar un conjunto de datos almacenados, esto dentro de un contexto general y útil para negocio.

Un "Dato Empresarial" es un término usado para determinar de forma atómica un conjunto de datos, que puede ser desde una tabla, un servicio de negocio,

una aplicación de TI, una base de datos hasta todos los datos almacenados dentro de un computador específico.

Cada dato empresarial debe tener un propietario, y un propietario puede tener más de un dato empresarial.



Ilustración 30 Datos Empresariales - Estrategia

Por otro lado, un propietario es un rol, pero se debe determinar explícitamente la persona sobre la cual recae dicha responsabilidad, además este propietario puede tener un "respaldo", el cual es otra persona sobre la cual se puede depositar la administración o gestión de las tareas de la propiedad de datos, más la responsabilidad siempre recaerá sobre el propietario del activo.

Tipos de Datos Empresariales

Se ha podido determinar por lo menos tres tipos de agrupación de conceptos de datos, que se pueden usar dentro de la empresa en lo que se refiere a "Datos Empresariales":

- Por Servicio de Negocio

Dícese de toda aquella agrupación de datos que tiene un sentido común y particular para un servicio determinado de negocio, de tal manera que se encuentran interesados no en una parte sino en todo el conjunto de datos pues todos juntos representan un producto o poseen un mismo objetivo.



Ilustración 31 Datos Empresariales - Servicio de Negocio

- Por Conceptos

El dato empresarial por concepto, se refiere al interés de negocio de resguardar los datos de algo en particular y no tan genérico como un Servicio de negocio. Esto se da por ejemplo cuando hay interés de resguardar tablas altamente sensibles, o bien, datos que son usados por distintos servicios y es necesario definir explícitamente el responsable de dicho dato. Esto sucede por ejemplo, con el maestro de clientes, donde actualmente es responsabilidad directa del CEO de la empresa y así ha estado durante mucho tiempo.

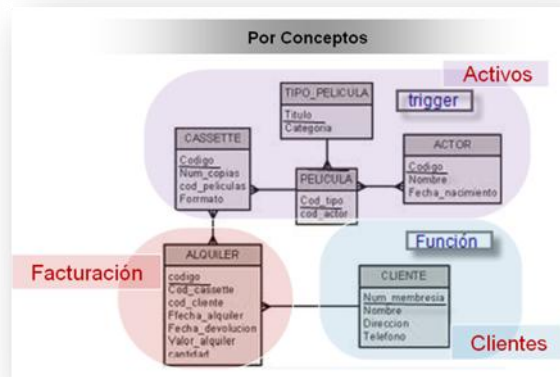


Ilustración 32 Datos Empresariales - Por Conceptos

- Mixto

Se refiere a la unión de las dos anteriores estrategias, en otras palabras cuando existen agrupaciones por servicios junto con agrupaciones por conceptos específicos o de interés de negocio.

Proceso de Propiedad de Datos

En cada país se tiene por lo menos tres niveles de jerarquía para la asignación del propietario de datos:

- A nivel de campos y tablas. Es el nivel más básico
- A nivel de Servicio de Negocios. Incluye muchos datos alrededor de un contexto.
- A nivel del Servidor de Producción.



Ilustración 33 Jerarquía de Datos Empresariales

La lógica a seguir para la asignación del propietario de datos es la siguiente:

- Si la tabla no posee un propietario explícito, entonces hereda el propietario del Servicio de Negocio al cual pertenece.
- Si la aplicación o Servicio de Negocio no posee un propietario explícito, entonces hereda el propietario del Servidor en el cual se encuentra.
- Todos los datos sin un propietario asignado explícitamente dentro de un servidor de producción le pertenecen automáticamente al Gerente General del país en donde reside dicho servidor.



Ilustración 34 Esquema de Autoridad - Datos Empresariales

Por medio de este patrón de asignación de la propiedad de datos, todos los datos tendrán su propio dueño. Esto no implica que sea el dueño más adecuado, por esa razón se le está asignando al Gerente General la propiedad de todos los datos no asignados, de tal manera que se ejerza cierta presión para la correcta asignación de dichas responsabilidades.

Debido a que el sistema es estándar, el área regional recomendará los roles sobre los cuales la responsabilidad de ciertos datos deberá de aplicarse, de tal manera que haya cierta sincronización con respecto a las políticas ejecutadas sobre un mismo tipo de datos en particular. Con esto, lo que se busca es que el rol de propietario de un dato específico sea el mismo para todos los países, pero la persona asignada sobre dicho rol será determinado explícitamente en cada país.



Ilustración 35 Datos Empresariales en la región

Para efectos de la selección del propietario de los datos dentro del flujo de desarrollo, se tienen las siguientes pautas:

- Antes de avanzar un pase a producción, se debe tener correctamente definido los propietarios de las estructuras a enviar.
- La asignación de propietarios de datos debe contar con el visto bueno del rol de negocio al cual se le estará asignando dicha responsabilidad.
- Por medio del Diccionario de Datos Empresarial se ayudará a determinar un posible propietario de datos para un dato empresarial determinado.
- La creación de nuevas tablas inicialmente se asumirá pertenece al propietario del Servicio de Negocio al cual pertenece. En caso de no haber dicho servicio de negocio, entonces inicialmente se le asignará al propietario del equipo.
- De forma regular se generarán reportes a los propietarios de datos, con respecto a los cambios estructurales realizados en tablas que se encuentran bajo su responsabilidad.

- De forma regular se generarán reportes a cada propietario por país y servidor sobre el estatus de la integridad de las estructuras bajo su responsabilidad.
- Todos los aspectos de propiedad de datos serán registrados en el diccionario de datos corporativo.

PROCESO DE VALIDACIÓN DE INTEGRIDAD DE DISEÑO ANTES DE ENVÍO DE PASE A PRODUCCIÓN

Se desea implementar un punto de control en el momento justo antes de enviar los cambios a ser instalados en los computadores de producción, esto con la idea de validar si efectivamente se respetaron los acuerdos llevados a cabo en lo que respecta al modelo de datos además de la implementación de los controles de seguridad de sistemas sobre aquellos datos que así se requieran.

Esta validación es muy importante, pues uno de los fundamentos de la Arquitectura de Información recae sobre la confianza en la integridad de los datos que TI pueda otorgar a negocio con respecto a las implementaciones hechas en todos los computadores de la región.

Tal y como se mencionó anteriormente, existe el punto de control de revisión de base de datos, y cualquier otro cambio que sea necesario debe validarse con el departamento de arquitectura de base de datos de tal manera que se actualice la información ingresada en el diccionario de datos y que dicho conocimiento sea publicado a toda aquella persona interesada. La experiencia ha demostrado, que entre la etapa de diseño del modelo de datos y la etapa de "avance de pase a producción", que es la etapa que envía los desarrollos a producción, puede transcurrir una cantidad significativa de tiempo, que hasta años inclusive podría conllevar.

Durante ese tiempo, se tendrá la información recopilada durante las sesiones de trabajo en diseño, pero podría presentarse un desfase o inconsistencia que podría provocar que la información del diccionario de datos no fuera completamente correcta. Es precisamente por esta causa que es necesaria una validación previa al envío a producción.

Metadata

Llámesese metada a todo aquel dato relacionado con el diseño y especificación de las estructuras del modelo de datos. Hoy en día, la mayoría de los motores de base de datos cuentan con facilidades por medio de las cuales, de forma explícita, se puede identificar las estructuras implementadas dentro del propio motor de base de datos.

Precisamente la estrategia que se desea implementar con el objetivo de guardar la consistencia entre los acuerdos del diseño del modelo de datos y el modelo de datos enviado en el pase a producción, es en el uso de la metadata.

Los datos que se pueden obtener consultando la metadata, son todos aquellos datos importantes y fundamentales de cada una de las estructuras implementadas. Por ejemplo, cuando se crea una tabla, los datos que se podrían obtener usando la metadata son los siguientes:

- Nombre de la tabla
- Características generales de la tabla
- Nombre de cada campo
- Características principales de cada campo
- Constraints y su definición
- Triggers y su definición
- etc.

Proceso de Validación de integridad previo al pase

Para poder realizar la validación de las estructuras que se desean avanzar a producción se debe comparar en esa etapa con las estructuras acordadas en las sesiones de diseño, para tal motivo se seguirán los siguientes pasos:

- Al momento de hacer las sesiones de análisis del diseño del modelo de datos, y llegar a acuerdos satisfactorios; se guardará la metadata del modelo de datos dentro del diccionario de datos
- La metadata permanecerá en el diccionario de datos de tal manera que pueda ser accedida por los interesados, y actualizada en caso de que alguna parte del diseño cambiara en una nueva sesión de diseño.
- Cuando un pase a producción llegue a la etapa de "Avance de Pase a Producción" se realizarán las siguientes verificaciones:
 - Se comparará la metada de las estructuras que pertenecen a dicho pase a producción con la metada almacenada en el diccionario de datos.
 - Si hay diferencias, y se pueden corregir, se realizará por parte del analista y se volverá a ejecutar la validación.
 - Si hay diferencias, y no se pueden corregir, se ingresará una Petición de Acción Correctiva al sistema de calidad de tal manera que se permita el avance del pase pero que además, que exista un elemento de acción para realizar el cambio posterior a la instalación.
 - Se verifican que los controles de seguridad hayan sido implementados tal y como se solicitó.
 - Si hay diferencias, y se pueden corregir, se realizará por parte del analista y se volverá a ejecutar la validación.

- Si hay diferencias, y no se pueden corregir, se ingresará una Petición de Acción Correctiva al sistema de calidad de tal manera que se permita el avance del pase pero que además, que exista un elemento de acción para realizar el cambio posterior a la instalación.
- Se procede a permitir el avance del pase.

Un resumen del proceso anteriormente visto se puede apreciar en la siguiente imagen:

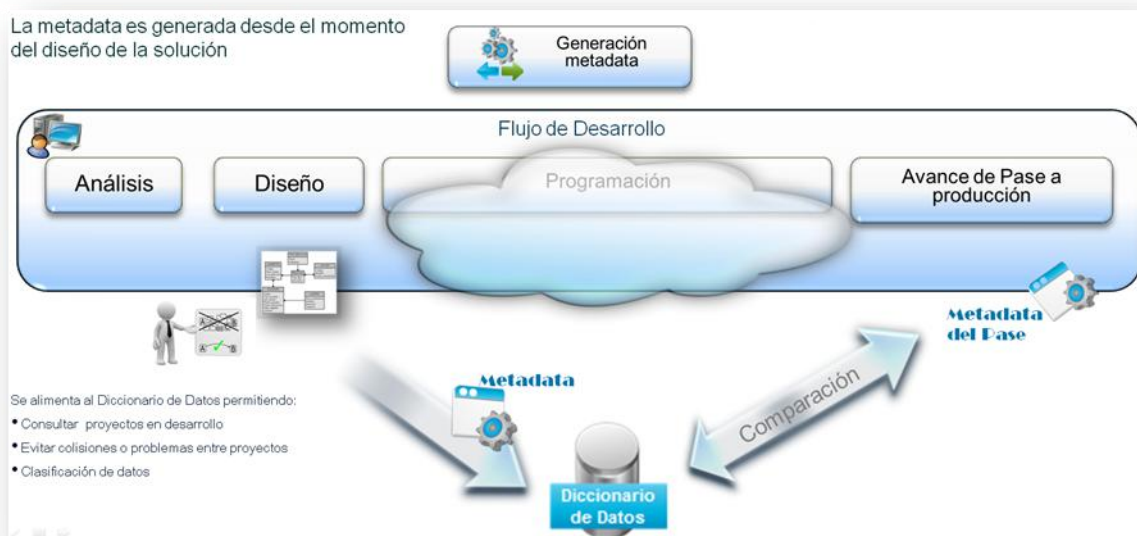


Ilustración 36 Proceso generación metadata

Cabe señalar que una de las intenciones es evitar cualquier tipo de contratiempo en los avances de pases a producción, por tanto estas validaciones se realizarán por medio de una mezcla de validación automática y manual, esta última entrará al proceso si la automática detecta algún tipo de inconsistencia.

PROCESO DE VALIDACIÓN DE INTEGRIDAD A LA HORA DE LA INSTALACIÓN DEL PASE EN CADA COMPUTADOR DE PRODUCCIÓN

Tal y como se señaló anteriormente, la infraestructura de BAC Credomatic, permite tener un número importante de servidores en la región compartiendo el sistema estándar instalado en cada uno de ellos; y es precisamente en cada uno de ellos, que se debe realizar la instalación de nuevos cambios en el sistema estándar, pero dicha validación y dicho control podría convertirse en una tarea tediosa y hasta cierto punto no mantenible con el tiempo.

Dado lo anterior, uno de los escenarios de este proceso de Arquitectura de Información que en cierta manera, es vital para asegurar la integridad de las estructuras en los servidores de producción, es el validar la correcta instalación de los pases o cambios a producción, de tal manera que se utilice un mecanismo estándar y controlado para determinar si las estructuras de base de datos se instalaron como se esperaba, esto en cada uno de los computadores de la región, y esto en el preciso momento de la instalación del pase.

Esta validación se hará tomando la metadata de las estructuras de base de datos acordada originalmente en el diseño de la aplicación y enviada en el pase a producción a cada uno de los servidores en donde se instalará. Es importante tener en cuenta, que cada vez que se crea una nueva estructura de base de datos dentro de los servidores, la metadata de ese servidor será actualizada de forma automática con los nuevos datos de la estructura creada.

En este proceso de validar la instalación del pase se aprovechará esa característica de los motores de base de datos, y en conjunto con la metadata enviada en el pase a producción se determinará si la instalación se ejecutó

correctamente en lo que respecta a la creación de las estructuras de base de datos.

Proceso de Validación de integridad instalación del pase

- A la hora de distribuir el "paquete" del pase a producción a cada servidor de producción, se añadirá la metadata acordada de la base de datos.
- La instalación del pase en cada servidor se realizará de forma normal tal y como se ha realizado hasta el momento. Esto permitirá que la metadata del servidor sea actualizada con las nuevas estructuras instaladas.
- Al finalizar la instalación del pase, se compararán las metadatas tanto la enviada dentro del pase como la generada en el servidor de producción
- Si hay concordancia entre las metadatas comparadas, se actualizará la tabla de monitoreo de instalación para dejar evidencia de la correcta instalación.
- En caso de que no haya concordancia, se le notificará de forma automática al auditor de la instalación del pase, el cual determinará si es subsanable la inconsistencia.
- En caso de ser subsanable, se realizarán las correcciones necesarias y se volverá a ejecutar el proceso de revisión.
- En caso de no ser subsanable, se colocará al pase una maraca de Error en la instalación y se procederá según se indica el lineamiento "Guía de Seguimiento Post-Instalación del Pase".



Ilustración 37 Validación de Integridad en la instalación

PROCESO DE MONITOREO DE INTEGRIDAD ESTRUCTURAL EN LOS COMPUTADORES DE PRODUCCIÓN

Luego de haber realizado la validación de la correcta instalación del pase a producción, la metadata de las estructuras nuevas del pase serán guardadas en una base de datos creada en cada servidor precisamente para ese efecto y que será de insumo para los monitoreos que se requieren realizar regularmente. Estos monitoreos tienen como fin principal, asegurar tanto a negocio como a TI de que el sistema estándar mantiene su integridad en todos los servidores monitoreados.



Ilustración 38 Monitoreo regular de la integridad

Proceso de monitoreo de integridad estructural

El proceso se está diseñando para que se ejecute una vez a la semana como mínimo, y los pasos a realizar serían los siguientes:

- Se realiza la comparación entre la metadata BAC Credomatic con la metadata del equipo local.
- En caso de que no se encuentren inconsistencias, se generará la evidencia correspondiente para ser respaldada, la cual se le podrá solicitar en caso de auditoría de objetos en producción.
- En caso de encontrarse algún tipo de inconsistencia, se alertará al operador del equipo en cuestión.
- El operador analizará la inconsistencia, y si es factible corregirla, lo hará y se ejecutará nuevamente el monitoreo.
- En caso de que no se pueda corregir la inconsistencia debido a conocimiento de la aplicación o sensibilidad del cambio, se procederá a notificar al grupo de Incidentes la situación presentada.
- Se procede a la ejecución de los procesos de continuidad de negocio activos en la compañía.
- Se guardará toda la evidencia recolectada por el monitoreo como insumo para poder retroalimentar a los expertos cuando intente corregir la inconsistencia.

Indicadores para el proceso

Todo proceso debe contar con su respectivo grupo de métricas de tal manera se pueda monitorear el avance y cumplimiento de las metas propuestas y la efectividad de los mismos.

Cada uno de los procesos definidos anteriormente cuenta con su respectivo indicador. Algunos de los indicadores diseñados son los siguientes:

Nombre	Tipo de Indicador	Razón de Ser	Formula
Indice de actualizaciones en el Diccionario de Datos basado en boletas aprobadas con cambios en BD	Indicador Operativo "IO"	Medir la actualización oportuna del Diccionario de Datos	$\frac{\text{(Cantidad de objetos y/o cambios de BD actualizados en el DD)}}{\text{(Cantidad de objetos y/o cambios de BD aprobados)}}$
Indice de integridad en los cambios de BD antes de la instalación del pase	Indicador Operativo "IO"	Medir que los cambios a la base de datos aprobados en la etapa de diseño se respeten hasta la conclusión del	Cantidad de inconsistencias encontradas en el avance del pase con respecto a la metadata registrada en el DD
Indice de integridad en la instalación de cambios a Base de datos en el Pase a producción	Indicador Operativo "IO"	Medir la cantidad de pases "marcados" por error debido a inconsistencia en la metadata de BD	Cantidad de pases marcados con error debido a inconsistencia en la metadata instalada de BD
Indice de integridad de Base de datos en en computadores de producción	Indicador Operativo "IO"	Medir la cantidad de inconsistencias encontradas en Base de Datos según monitoreo semanal.	Cantidad de inconsistencias encontradas en el monitoreo por servidor
Promedio de calificación del Diccionario de Datos	Indicador de negocio "KPI"	Controlar que se este usando y atendiendo las mejoras tanto de Negocio como de TI	Promedio de la nota de la evaluación obtenida anualmente.
Indice de integridad de Linea Base	Indicador Operativo "IO"	Medir la estandarización e integridad de los objetos de la Linea Base con respecto a la	$\frac{\text{Cantidad de objetos de BD en Linea Base}}{\text{Cantidad de objetos de BD que deben estar instalados (según PDE)}}$

Tabla 19 Indicadores del Proceso PO2

Productos No Conformes (PNCs) del Proceso

Para los procesos antes definidos, se diseñaron PNC's que son elementos de calidad con el objetivo de hacer cumplir características de calidad definidas previamente.

Se diseñaron dos PNC's que fueron definidos dentro del proceso de validación de integridad de diseño antes de envío de pase a producción

Paso del Proceso	A quién le corresponde el PNC	Causa	Cómo se resuelve
2.4	Al analista responsable del Pase a Producción	Se encuentran diferencias sustanciales entre el modelo de datos acordado en la etapa de diseño con el formalizado y listo a enviar en el pase a producción.	Inclusión de los cambios acordados en un pase posterior.
2.11	Al analista responsable del Pase a Producción	Se detectan deficiencias o ausencia de los controles de Seguridad de Datos acordados desde la etapa de diseño. Esto en la etapa de avance del Pase a producción	Aplicación de los controles de Seguridad de datos acordados en los computadores de producción indicados por Seguridad de Sistemas.

Tabla 20 Productos No Conformes del Proceso PO2

Resumen del Proceso PO2

El proceso PO2 ha sido diseñado de tal manera que abarque desde las etapas tempranas del desarrollo de aplicaciones, hasta el monitoreo de lo colocado en producción para validar su integridad, en otras palabras se ha intentado cubrir con todo el ciclo de desarrollo manteniendo una completa documentación y validando en cada etapa con el objetivo de mantener la integridad de lo diseñado y publicado en el Diccionario de Datos.

Dentro de los siguientes pasos a seguir, se procederá en la correcta y adaptable implementación de este proceso, con el fin de ir alcanzando la arquitectura de información empresarial requerida.

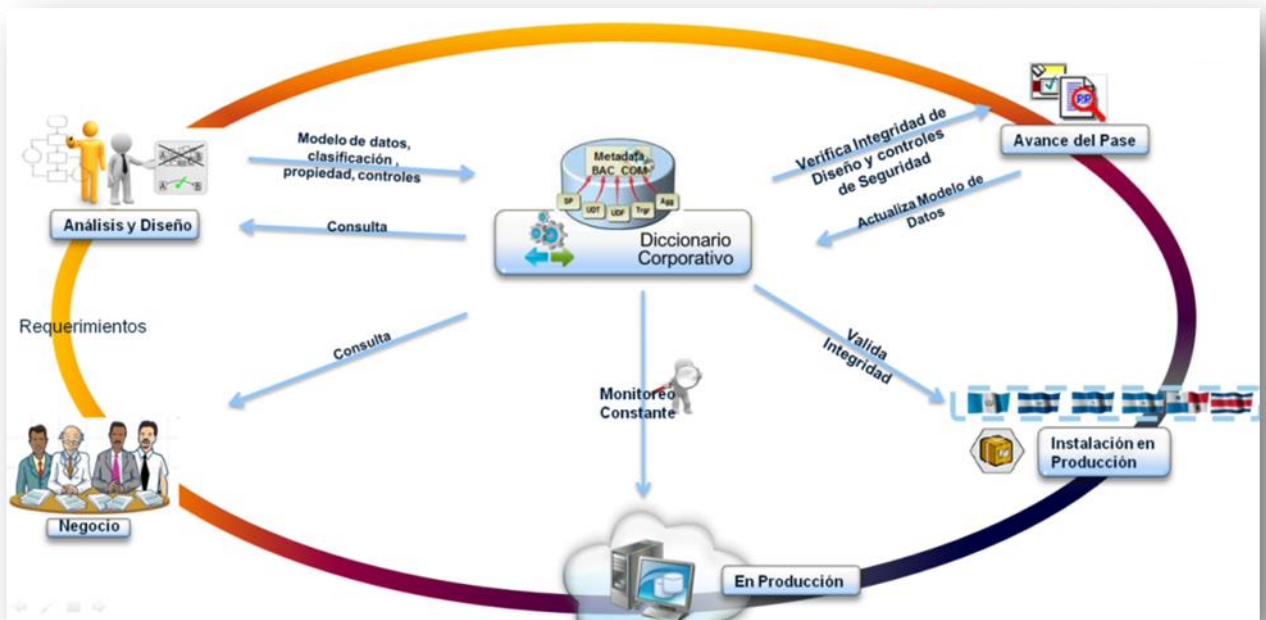


Ilustración 39 Proceso completo de Arquitectura de la Información

Conclusiones y trabajos futuros

Conclusiones

1. Los estándares y lineamientos generalmente aplicados a entidades financieras poseen factores en común bastante relevantes pero enfocados específicamente en el alcance del estándar en sí, por tanto se considera necesario que al momento de la implementación de procesos según dichos estándares, se tenga en mente esos elementos de tal manera que se pueda consolidar y trabajar en conjunto, a expensas de consolidar objetivos en común que a la postre beneficiaran en muchos ámbitos a la misma empresa.
2. Los marcos de referencia tales como COBIT permiten ir solucionando necesidades particulares pero enfocados en una meta mucho más general como es la gobernabilidad de las tecnologías de la información, y ese proceso puede adaptarse al ritmo que así lo requiera la organización en cuanto exista visión y conocimiento tanto de los requerimientos funcionales necesitados por la empresa como los elementos básicos de dichos marcos de referencia.
3. El alcanzar una arquitectura de información empresarial es un proyecto bastante significativo, que puede desglosarse o segmentarse según las necesidades particulares e inmediatas de la empresa. Además, por su complejidad, control y orden, es recomendado trabajar en forma modular, priorizando los elementos particulares y alcanzables por la empresa, pero generando una base para poder ir madurando poco a poco e ir determinando el avance en los distintos factores de éxito.

4. Para poder llevar a cabo cualquier esfuerzo en lo que a arquitectura de información empresarial se refiere, es necesario el apoyo de distintos roles, departamentos y personas de poder dentro de la organización, de tal manera que "apadrinen" el proyecto y pueda existir una disponibilidad más eficiente de recursos y garantías para el buen éxito del proyecto.

Trabajos Futuros

Luego de la elaboración de este trabajo y la aprobación que la Gerencia de Arquitectura de TI de BAC Credomatic otorgó, se acordó además proseguir con los siguientes pasos:

1. Publicación de los procesos y directrices en la herramienta de documentación formal ISO de la compañía con la salvedad de se encuentran en proceso de implementación.
2. Junto con los Gerentes de Desarrollo se determinará la prioridad de implementación de los procesos señalados.
3. La Gerencia de Arquitectura de TI determinará las distintas opciones para la implementación de los procesos acordados.
4. Capacitación al personal involucrado; principalmente a los analistas y programadores con respecto a los procesos acordados.
5. Implementación, pruebas y puesta en marcha de los procesos acordados

Bibliografía

[BAC-001] Bac International Bank. *Historia del Grupo BAC Credomatic*. Recuperado de <https://www.bac.net/regional/esp/banco/acerca.html>

[BAC-002] Bac International Bank. *Nuestra Historia*. Recuperado de <http://www.credomatic.com/costarica/esp/credo/nuecomp/nushistoria.html>

[BAC-003] Bac International Bank. *Misión, Visión Valores*. Recuperado de <http://www.credomatic.com/costarica/esp/credo/nuecomp/nuemision.html>

[BAC-004] Bac International Bank. *Productos y Programa de Bac | Credomatic*. Recuperado de <http://www.credomatic.com/costarica/esp/credo/afiliados/afiservprogrespextra.html>

[COB-001] Bankar, Pritam, et al., *Mapping PCI DSS v2.0 With COBIT 4.1*. (2011)

[COS-001] COSO. *Internal Control -Integrated Framework*.(1992)

[COB-003] Bannister, Gary A. (2006). *Using COBIT for Sarbanes Oxley, Japan*

[SOX-002] Chiriboga mendez, Maria Gabriela. *Diseño de Pruebas de cumplimiento para el control interno, basadas en la Ley Sarbanes Oxley*. Ecuador. (2008).

[CBT-001] Comité Directivo de COBIT y la Information Systems Audit and Control Foundation. *COBIT Resumen*. 2da Edición. (1998)

[CGR-007] Contraloría General de la República. (2007). "Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE)". Aprobadas mediante Resolución del Despacho de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007. Publicado en La Gaceta Nro.119 del 21 de junio, 2007.

[ISA-001] Coop, Marianne. *Linking COBIT, ITIL & ISO27001/2*. ISACA

[REG-001] García, Sandra. *ITIL, Gobierno de TI y las regulaciones en Costa Rica*.

- [AIF-01] Gonzales Cam, Celso. (2003). *Arquitectura de la Información: diseño e implementación*. Departamento de Ciencias de la Información Pontificia Universidad Católica del Perú . Lima. Perú
- [GOV-001] ISACA, *Global Status Report on the Governance of Enterprise TI*. (2011).
- [ALI-001] IT Governance Institute. *Alineando Cobit 4.1, ITIL V3 e ISO/IEC 27002 en beneficio del negocio. Un reporte para gestión del ITGI y la OGC*. (2008).
- [GOV-07] IT Governance Institute. *COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. (2007).
- [COB-003] IT Governance Institute. *COBIT Mapping, Overview of International IT Guidance*. 2da Edición, 2006
- [COB-002] . IT Governance Institute. *IT Control Objectives For Sarbanes-Oxley*. 2nd Edition. (2006)
- [ISO-1799] ITIL Diseño del Servicio. [http://wiki.es.it-processmaps.com/index.php/ITIL Dise%C3%B1o del Servicio](http://wiki.es.it-processmaps.com/index.php/ITIL_Dise%C3%B1o_del_Servicio), 18 de Julio, 2013
- [ITI-005] Kempter, Stefan y Kempter, Andrea. *Introducción a ITIL® Versión 3 y al Mapa de Procesos ITIL® V3*. (2010)
- [GAR-001] La Rosa, Mariagrazia. (2004). *L'approccio Gartner all'analisi e al miglioramento dei processi ICT*. Convention itSMF Italia. Genova.
- [MEJ-001] Muñoz Mata, Mirna Ariadna. *Análisis de estándares y modelos de referencia de mejores prácticas*. (2006).
- [ITI-006] Patiño, María del Pilar. *ITIL VE3: El manual de las buenas prácticas de TI*. (2010)
- [PCI-001] PCI Security Standars Council. *Normas de Seguridad de Datos. Requisitos y procedimientos de evaluación de seguridad*. Versión 1.2, (2008).
- [SOX-001] Peña Ibarra , José Ángel. *Seguridad desde el punto de vista SOX y Gobernabilidad*. Mexico. (2006)

[ITI-002] Ramírez Bravo, Pía y Donoso Jaurés, Felipe. *Metodología ITIL* (2006).

[SUG-001] Reglamento sobre la gestión de la Tecnología de Información. SUGEF 14-09. Superintendencia de Entidades Financieras. Costa Rica. 2009.

[COB-006] Sheikhpour , Razieh y Modiri , Nasser. *An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls*. (2012).

[COB-004] Stroud, Robert. *Using COBIT and ITIL*. (2010)

[SOX-001] *Using QualysGuard to Meet SO X Compliance & IT Control Objectives*. 2005

[ITI-004] Van Bon, Jan, et al. *Fundamentos de la Gestión de Servicios de TI basada en ITIL V3*. (2008)

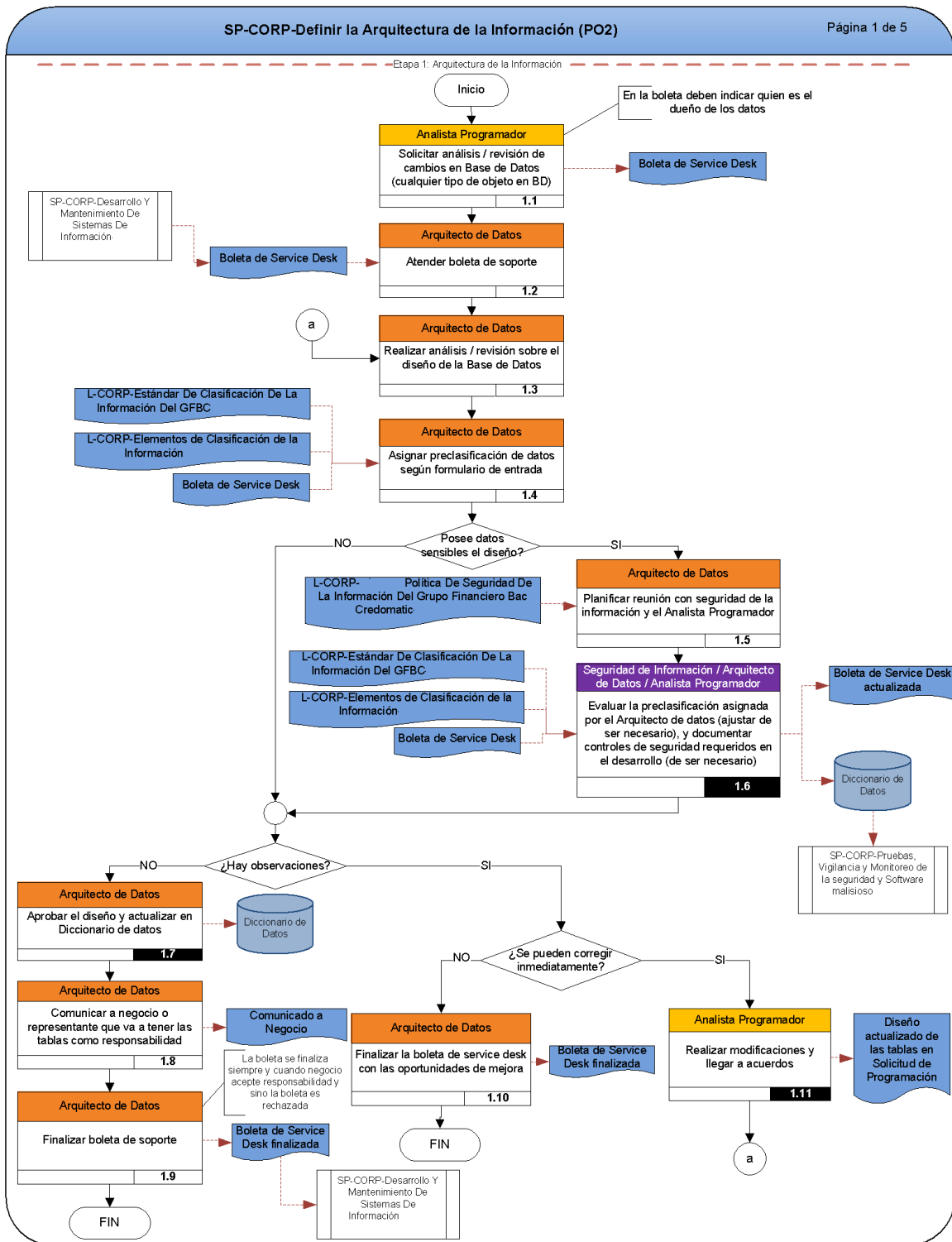
[ITI-001] Vilches, Ernesto. *Guía de Gestión de Servicios basada en Fundamentos de ITIL v3*. Luarna ediciones, S.L. (2010)

[SIS-001] Ureña Cuate, Mario. *Sistema de Gestión Integral con PAS 99, ISO 9001, ISO 27001, ISO 20000, COBIT, BS 25999 / ISO 22301*. ISACA, (2011)

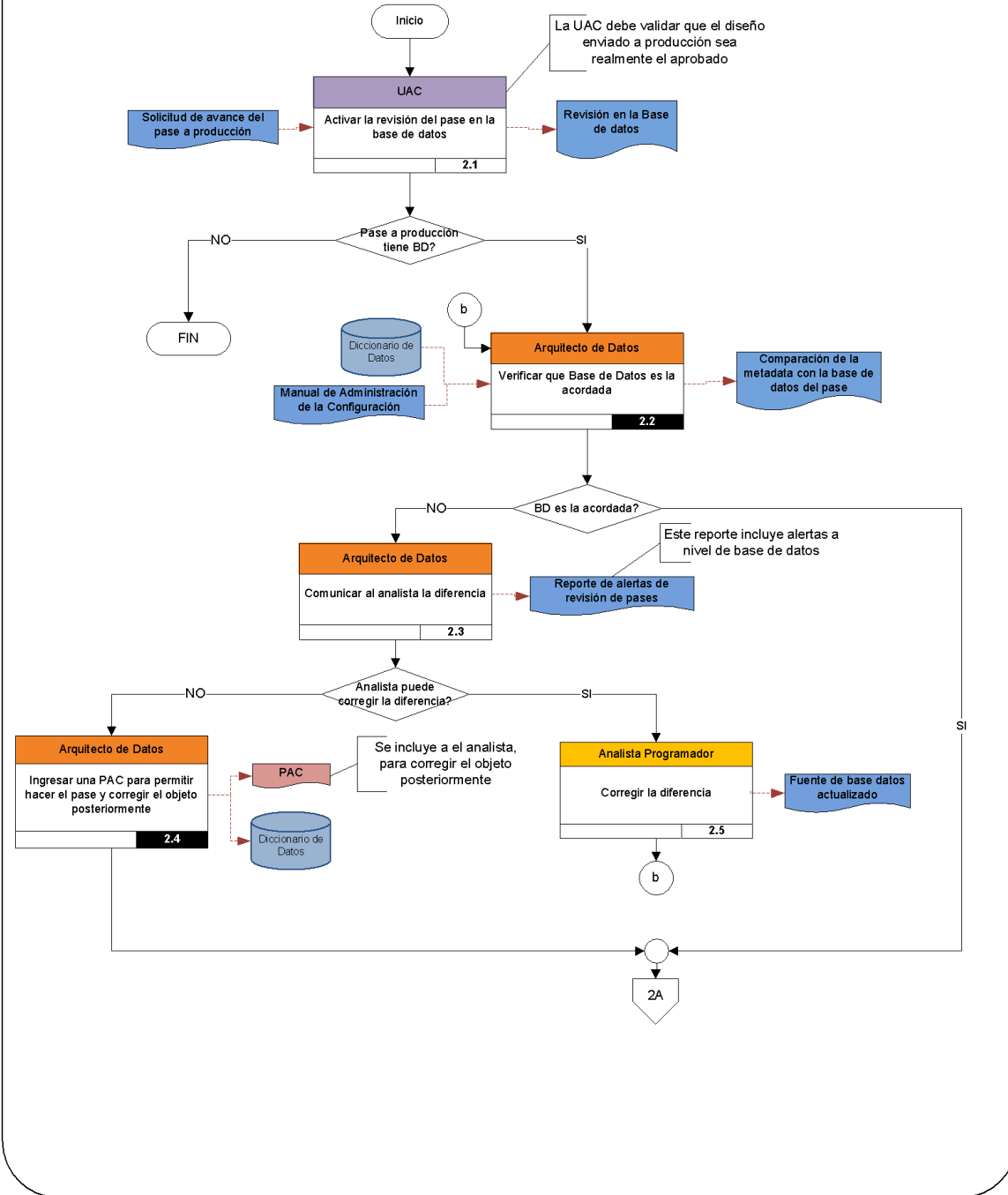
[SOX-003] Ugochuku , Ike. *SOX 404 & IT CONTROLS. IT Control Recommendations for small and Mid-size companies*. (2006).

Anexos

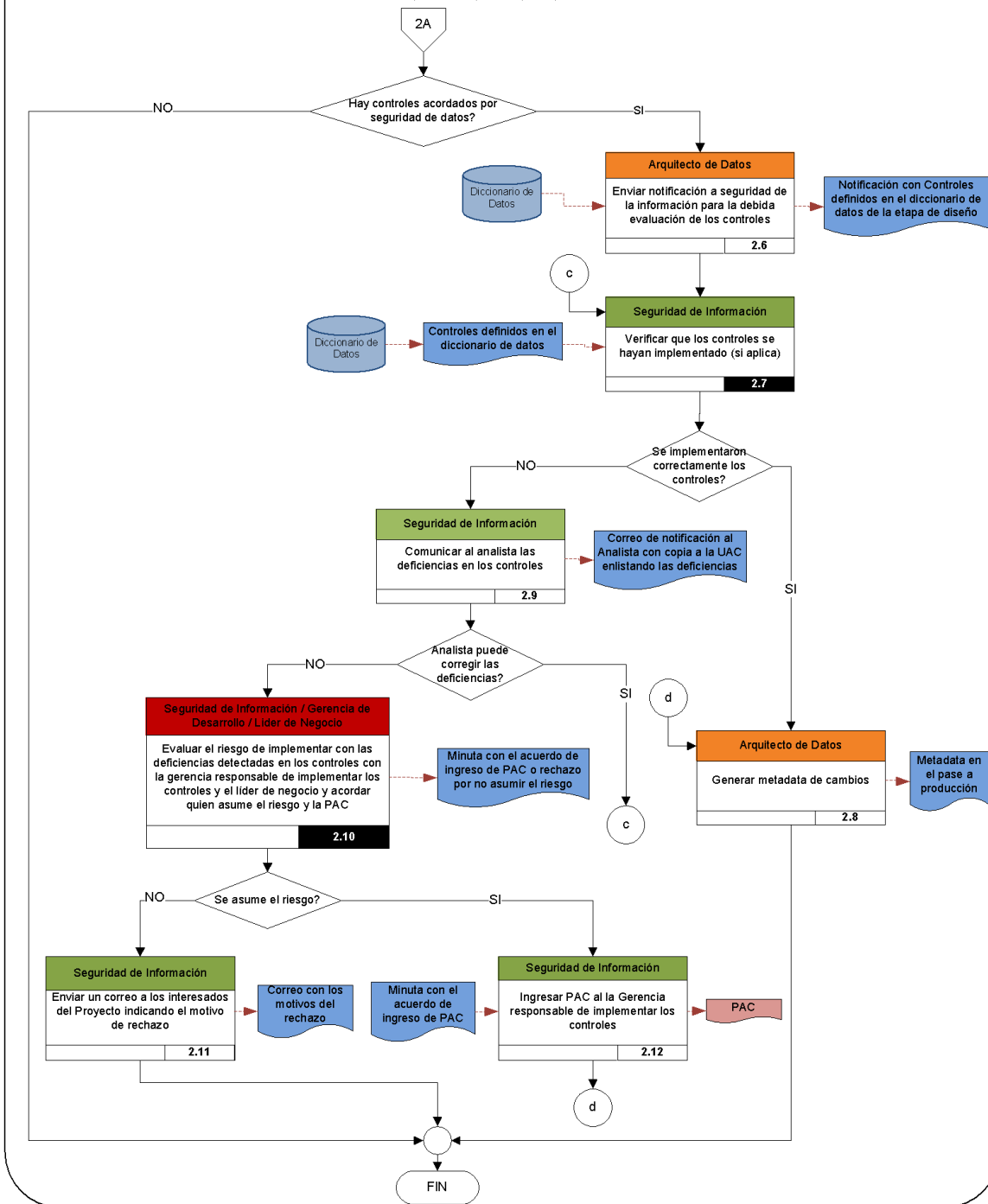
Anexo 1



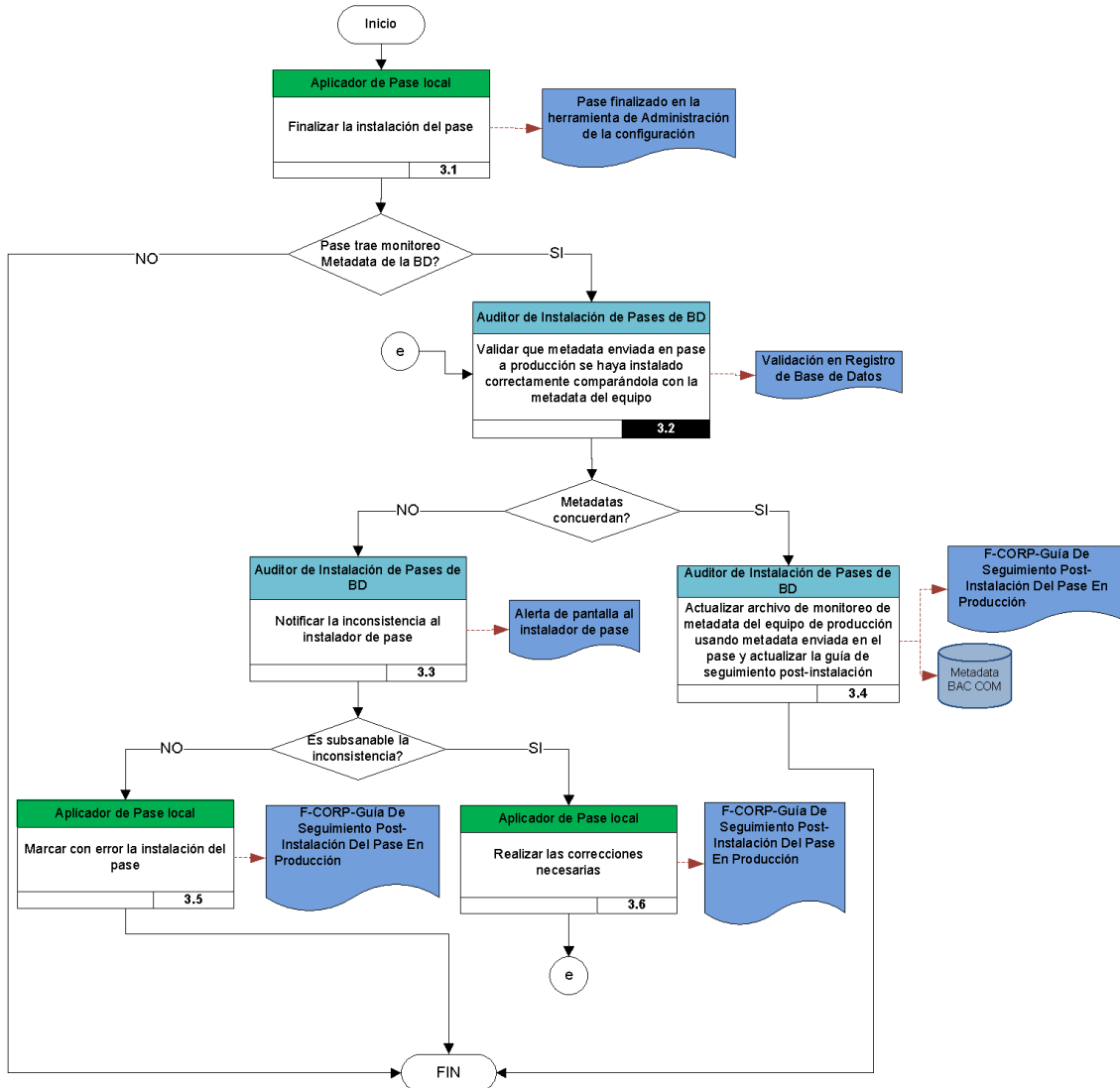
Etapa 2: Análisis previo del pase a producción



Etapa 2: Análisis previo del pase a producción



-Etapa 3. Instalación del pase de Base de Datos-



—Etapas 4 Monitoreo de la Integridad de Base de Datos en Producción—

