PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR

FACULTAD DE INGENIERIA

MAESTRÍA EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

DESARROLLO DE UNA GUÍA METODOLÓGICA PARA LA GESTIÓN DE TECNOLOGÍA QUE ASEGURE EL CONTROL INTERNO EN EMPRESAS DEL SECTOR FINANCIERO

TORRES PROAÑO GEOVANNY FERNANDO

Quito, 2013

AGRADECIMIENTO

Agradezco a todos los profesores y colegas que tuve como compañeros en esta vivencia maestrante quienes compartieron su experiencia profesional complementando todo lo aprendido en las aulas. Así también a mi familia que ha sido el puntal principal de motivación para alcanzar cada uno de mis retos de vida.

DEDICATORIA

Dedico este proyecto a mi familia y amistades quienes de una u otra manera me ayudaron con su apoyo incondicional para culminar este reto maestrante. Esto no sería posible sin la ayuda de Dios quien me brindo salud y la oportunidad de conocer personas que tienen un lugar muy especial dentro de mi vida.

ÍNDICE

INTRODUCCIÓN 6
CAPÍTULO 1. MARCO TEÓRICO DEL CONTROL INTERNO 7
1.1 CONTROL INTERNO 7
1.1.1 OBJETIVOS 8
1.1.2 DIRECTRICES 9
1.1.3 NORMAS Y ESTÁNDARES INTERNACIONALES 9
1. 2 PROCESOS Y CONTROLES 11
1.2.1 PROCESO 11
1.2.2 CONTROL 12
1.2.3 CATEGORIZACIÓN DE CONTROLES 13
1.3 COSO ERM 15
1.3.1 DEFINICIÓN 15
1.3.2 COMPONENTES 17
1.4 COBIT 18
1.4.1 INTRODUCCIÓN 18
1.4.2 GENERALIDADES 19
1.4.3 DOMINIOS 25
1.5 ITIL 26
1.5.1 ORIGEN Y DEFINICIÓN 26
1.5.2 LIBROS 28
CAPÍTULO 2. SITUACIÓN ACTUAL 30
2.1 ENTORNO MACRO 30
2.1.1 CONTROL INTERNO EN ENTIDADES FINANCIERAS A NIVEL INTERNACIONAL 30
2.1.2 CASOS REALES DE FALENCIAS ENCONTRADAS EN ATAQUES EFECTUADOS A LA INTEGRIDAD DE LA INFORMACIÓN 32
2.2 ENTORNO MICRO 34
2.2.1 CONTROL INTERNO EN ENTIDADES FINANCIERAS EN EL ECUADOR 35
2.2.2 MODELO COMPARATIVO DEL MANEJO DE CONTROL INTERNO ENTRE EL ECUADOR Y PAÍSES DEL PRIMER MUNDO 41
CAPÍTULO 3. TECNOLOGÍAS DE APOYO PARA LA PROTECCIÓN DE LA INFORMACIÓN 46
3.1 SISTEMAS PARA EL CONTROL DE FUGA DE INFORMACIÓN 46
3.2 NUEVAS TECNOLOGÍAS PARA EL CONTROL DE TARJETAS DE PAGO (CRÉDITO) 50

3.3 HERRAMIENTAS PARA LA PREVENCIÓN DE ATAQUES EN LÍNEA 55
CAPÍTULO 4. DESARROLLO DE LA GUÍA METODOLÓGICA PARA LA GESTIÓN DEL CONTROL INTERNO 58
4.1 PLANIFICACIÓN E IMPLEMENTACIÓN DE LA GESTIÓN DEL SERVICIO....58
4.2 PLANIFICACIÓN E IMPLEMENTACIÓN DE NUEVOS SERVICIOS O DE SERVICIOS MODIFICADOS 61
4.3 PROCESOS DE PROVISIÓN DE SERVICIO 63
4.3.1 GESTIÓN DE NIVEL DE SERVICIO.....63
4.3.2 GESTIÓN DE LA CONTINUIDAD Y DISPONIBILIDAD DEL SERVICIO..67
4.3.3 GESTIÓN DE LA CAPACIDAD 69
4.3.4 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....71
4.4 PROCESOS DE RELACIONES.....72
4.5 GESTION DEL PROBLEMA 73
4.6 PROCESO DE CONTROL.....75
CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES.....78
ANEXO I. RESUMEN EJECUTIVO GUÍA METODOLÓGICA PARA LA GESTIÓN DEL CONTROL INTERNO 80
BIBLIOGRAFÍA Y REFERENCIAS.....100

ÍNDICE DE FIGURAS

Figura 1-01 Tres enfoques principales del marco referencial.....20
Figura 2-01 La relación entre los recursos TI y la entrega de servicios 22
Figura 3-01 Relación del Marco Referencial con las necesidades de la empresa.....23
Figura 4-01 Niveles de Actividades de TI.....24
Figura 5-01 Puntos de Enfoque del marco referencial 24
Figura 6-01 ITIL Framework 27
Figura 7-04 Metodología PDCA orientado a TI.....59
Figura 8-04 Mejora continua 60
Figura 9-04 Cadena de Valor Gestión Niveles de Servicio 63
Figura 10-04 Gestión Niveles de Servicio.....64
Figura 11-04 Proceso de Control 77

ÍNDICE DE TABLAS

Tabla 1-02 Normativas aplicadas en los Países consultados 45

INTRODUCCIÓN

Cada día, se desarrollan nuevos métodos que hacen vulnerable el control interno de las organizaciones del sector financiero, es por ello la necesidad de una estrategia completa de seguridad para mitigar el riesgo dentro de los procesos, de manera de prevenir fugas y fallas en los sistemas. A lo antes expuesto se suman vulnerabilidades internas que son un factor de riesgo no menor, y por lo tanto, existe alta probabilidad de pérdida de dinero y repercusiones en la confiabilidad por parte de usuarios, clientes y socios de negocios.

Los gastos de capital y operativos son indicadores mensurables del costo por la pérdida de información. Aunque estos costos sean dolorosos, no son nada en comparación con una faceta de la pérdida que no puede medirse en términos presupuestarios. Dicha faceta es el uso de datos confidenciales para socavar la reputación de una entidad financiera, la integridad de la marca o la confianza de los clientes. Estos factores pueden alterar el panorama competitivo.

No se pueden obviar los factores de riesgos por desastres que al no estar previstos eficientemente y sin planes de contingencia y/o de recuperación pueden provocar daños irreparables en tiempo y costos de recuperación.

Esto, que es difícilmente cuantificable, puede incluso determinar la continuidad de una organización. En este trabajo se desarrolla una guía metodológica basada en estándares y normas internacionales, para evitar y/o disminuir el mal manejo de la información sobre sistemas, redes y datos antes que éstos ocurran, a través de un proceso de establecimiento de políticas, procedimientos, registros, controles y documentación. Esta guía metodológica puede ser utilizada como base para iniciar un cambio en el manejo de la información en empresas del sector financiero.

CAPÍTULO 1. MARCO TEÓRICO DEL CONTROL INTERNO

En este capítulo se presenta el sustento teórico referente al control interno alineado con la tecnología, que en la actualidad se convierte en un eje estratégico en el ámbito empresarial.

1.1 CONTROL INTERNO

El control interno es el conjunto de procesos debidamente alineados a los objetivos de la empresa con el fin de asegurar que la Misión se cumpla, a continuación se detallan los conceptos, metodologías y marcos de referencia que hacen que este conjunto de procesos tengan éxito.

Para las personas no tiene el mismo significado, esto puede dificultar su comprensión dentro de una organización. Resulta importante establecer un marco que permita obtener una definición común; siendo el control interno un proceso llevado a cabo por las personas de una organización, diseñado con el fin de proporcionar un grado de seguridad medible y factible para la consecución de sus objetivos, dentro de las siguientes categorías:

- Eficiencia y eficacia operativa
- Fiabilidad de la información
- Cumplimiento de las leyes y normas

Por lo mencionado podemos entonces definir ciertos conceptos fundamentales del control interno:

- El control interno es un medio para alcanzar un fin.
- Al control interno lo realizan las personas, no son sólo políticas y procedimientos.

- El control interno sólo brinda un grado de seguridad razonable, no es la seguridad total.
- El control interno tiene como fin facilitar el alcance de los objetivos de una organización.

(SCRIBD)

En resumen control interno, es una expresión que utilizamos con el fin de describir las acciones adoptadas por los directores de entidades, gerentes o administradores, para evaluar y monitorear las operaciones en sus entidades. El sistema de control interno comprende el plan de la organización y todos los métodos coordinados, medidas adoptadas dentro de una empresa con el fin de salvaguardar sus activos.

1.1.1 OBJETIVOS

Objetivo General

Desarrollar una guía metodológica que permita asegurar el control interno dentro de los procesos y servicios tecnológicos que se brindan en empresas del sector financiero ecuatoriano.

Objetivos Específicos

- Identificar marcos de referencia, metodologías y estándares internacionales que se adapten a la realidad ecuatoriana.
- Delimitar las responsabilidades de la Gerencia en TI[1]en el ámbito que le corresponde en la administración del control interno.
- Incorporar controles y mejores prácticas para la evaluación sobre la disponibilidad de la información.
- Diagramar una guía metodológica de referencia.

[1] **Tecnologías de la Información**

1.1.2 DIRECTRICES

Las tareas de análisis y gestión del control interno no son un fin en sí mismas sino que se encajan en la actividad continua de la gestión de tecnología. El análisis de control interno permite determinar cómo es, cuánto vale y cuan protegidos se encuentran los activos. En coordinación con los objetivos, estrategias y políticas de la Organización, las actividades de control interno permiten elaborar un plan que satisfaga los objetivos propuestos con el nivel de criticidad que acepta la Dirección.

La implantación de los controles internos requiere una gestión orientada a procesos y la participación activa de todo el personal que trabaja con los servicios de TI. Este personal es responsable de la operación diaria, de la reacción ante incidencias y del monitoreo en general del sistema para determinar si satisface con eficiencia los objetivos propuestos. Este esquema de trabajo exige una revisión periódica ya que los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), finalmente se aprende de la experiencia y se adapta al nuevo contexto.

El control interno proporciona un modelo en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.

1.1.3 NORMAS Y ESTÁNDARES INTERNACIONALES

COSO[2]

La normativa está principalmente orientada al control de la administración financiera y contable de las organizaciones. Sin embargo, dada la gran cercanía que hoy existe entre esta área y los sistemas de información, resulta importante entender el alcance y uso de esta norma.

[2] **Committee of Sponsoring Organizations of the Treadway Commission**

Junto a esto son muchas otras las normas alrededor de 240 que están directa o indirectamente relacionadas. En resumen, el Informe COSO es un documento que contiene directivas e indicaciones para la implantación, gestión y control de un **"Sistema de Control Interno"**, con alcances a los servicios de TI.

(Mantilla, 2013)

ITIL[3]

Es una norma de mejores prácticas para la administración de servicios de Tecnología de Información (TI), desarrollada a finales del año 1980 por entidades públicas y privadas con el fin de considerar las mejores prácticas a nivel mundial. El organismo propietario de este marco de referencia de estándares es el Office of Government Commerce, una entidad independiente de la tesorería del gobierno británico. ITIL fue utilizado inicialmente como una guía para el gobierno de británico, pero es aplicable a cualquier tipo de organización.

(OSIATIS)

COBIT[4]

Acrónimo de "Control Objectives for Information and related Technology" (Objetivos de Control para la Información y Tecnologías Relacionadas), es un estándar desarrollado por ISACA[5], la cual fue fundada en 1969 en Estados Unidos y que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TI. Actualmente tiene más de 60.000 miembros en alrededor de 100 países. Esta organización realiza eventos y 239 conferencias, y desarrolla estándares en TI de gobierno, aseguramiento y seguridad, siendo COBIT el más importante. En los últimos 5 años ha cobrado fuerza debido a que fue desarrollado en específico para el ámbito de las TIC.

(Torres & Villegas, [C], 2008)

[3] **Information Technology Infrastructure Library**
[4] **Control Objectives for Information and related Technology**
[5] **Information Systems Audit and Control Foundation**

ISO[6] 20000

Es un estándar internacional para proporcionar servicios de TI con calidad para los clientes de una determinada organización, enfocado a empresas proveedoras de servicios TI. Surge con ITIL.

Consta de 13 procesos definidos, un proceso de planificación e implementación de servicios, requisitos de un sistema de gestión y un ciclo de mejora constante.

(Telefónica, 2010)

1. 2 PROCESOS Y CONTROLES

1.2.1 PROCESO

Un proceso es un grupo estructurado de actividades diseñado para lograr un objetivo en específico.

Los Procesos:

- Crean valor para todos los participantes claves del proceso.
- Toman uno o más entradas y las convierten en salidas definidas.
- Están organizados alrededor de un grupo de objetivos.
- Incluyen todos los roles, las responsabilidades, herramientas y controles de gestión (medidas y métricas) para entregar los resultados.
- Una vez definidos y documentados, deben ser controlados para asegurar resultados repetibles.

(Torres & Villegas, [C], 2008)

[6] International Organization for Standardization

El control de procesos es "la actividad de planear y regular un proceso, con el objetivo de ejecutarlos de una manera consistente, eficiente y efectiva"

CARACTERÍSTICAS DEL PROCESO

Las características de los procesos son:

- **Medible**
  - Enfocado por el rendimiento.
  - Costes, calidad, duración, productividad, y demás.

- **Resultados Específicos**
  - Entrega de un resultado específico.
  - Identificable de manera individual y numerable.

- **Clientes**
  - Que cumpla las expectativas del cliente.
  - Puede ser interno o externo.
  - Responder a un evento en específico.
  - Modificar datos de una tabla dentro de la base de datos.

(Torres & Villegas, [C], 2008)

1.2.2 CONTROL

Un control en si es un proceso establecido por la Junta Directiva, la alta gerencia y todos los niveles de personal para proveer una seguridad razonable de que los objetivos de la organización serán alcanzados. Los controles internos se clasifican en:

- Preventivos
- Correctivos

Los objetivos de control en un ambiente de tecnología permanecen invariables en relación a los de un ambiente manual. Sin embargo, las características de los controles pueden ser diferentes. Los objetivos de control interno, por lo tanto necesitan, ser dirigidos en una manera específica a procesos relacionados con los sistemas de información.

(Torres & Villegas, [C], 2008)

1.2.3 CATEGORIZACIÓN DE CONTROLES

CONTROLES GENERALES

Son controles diseñados e implantados para asegurar que el ambiente computadorizado de la organización sea estable y adecuadamente administrado a fin de reforzar la efectividad de los controles de aplicación.

Los Controles Generales (a veces denominados también controles de la organización TI) fueron agrupados en las siguientes categorías:

- **Controles Gerenciales del Departamento de TI:** Los controles de monitoreo son definidos para verificar las normas teóricamente existentes en el departamento de Informática y su coherencia con las del resto de la empresa, la calidad del control interno y su ejecución sobre el tiempo, se logra a través de actividades de monitoreo, separada de evaluaciones o una combinación de las dos.

- **Controles sobre la Seguridad de la Información:** El objetivo principal de comprender, evaluar y validar los controles sobre la seguridad de la información es asegurar que solo se otorga acceso autorizado a los programas y datos, si y sólo si se autentifica la identidad del usuario.

- **Controles sobre la Operación del Computador:** El objetivo principal para las operaciones del computador es asegurar que los sistemas de producción se procesan en forma completa y correcta de acuerdo con los objetivos que Gerencia ha definido, que los problemas de procesamiento son identificados y resueltos en forma completa y correcta para mantener la integridad de los datos.

- **Controles sobre las Actividades de Mantenimiento de Sistemas***:* Los cambios o mantenimientos en los sistemas se pueden realizar por personal interno como externo del departamento de sistemas, los controles definidos para las actividades de mantenimiento tienen como objetivo, asegurar que los cambios y los componentes de la infraestructura relacionada sean debidamente solicitados, priorizados, realizados aprobados e implementados de acuerdo a los objetivos de la Gerencia y principalmente de la empresa.

- **Controles sobre el Desarrollo e Implementación de Nuevos Sistemas:** Los controles sobre la implantación de programas deben asegurar que los nuevos sistemas sólo son implantados en el entorno de producción luego de haberse realizado pruebas adecuadas, de haberse obtenido la aprobación del promotor del negocio y de haberse desarrollado planes de implantación y contingencia.

(Torres & Villegas, [C], 2008)

CONTROLES DE APLICACIÓN

Son controles diseñados para asegurar la integridad de la información que se almacena en la base de datos, los controles de aplicación brindan soporte directamente a los objetivos de control:

- Valor correcto
- Validez
- Acceso restringido

Los controles de aplicación pueden ser procedimientos manuales llevados a cabo por los usuarios de procedimientos automatizados desarrollados por los programas de computación.

(Torres & Villegas, [C], 2008)

1.3 COSO ERM

1.3.1 DEFINICIÓN

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

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

Completan la definición algunos conceptos fundamentales:

- El control interno es un proceso, es decir un medio para alcanzar un fin y no un fin en sí mismo.
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.
- Está pensado para facilitar la consecución de objetivos en una o más de las categorías señaladas las que, al mismo tiempo, suelen tener puntos en común.

(Mantilla, 2013)

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

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

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

(Mantilla, 2013)

Para la alta dirección es primordial lograr los mejores resultados con economía de esfuerzos y recursos, es decir al menor costo posible. Para ello debe controlarse que sus decisiones se cumplan adecuadamente, en el sentido que las acciones ejecutadas se correspondan con aquéllas, dentro de un esquema básico que permita la iniciativa y contemple las circunstancias vigentes en cada momento.

Por consiguiente, siguiendo los lineamientos de INTOSAI[7], incumbe a la autoridad superior la responsabilidad en cuanto al establecimiento de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica. Ambas definiciones (COSO e INTOSAI) se complementan y conforman una versión amplia del control interno: la primera enfatizando respecto a su carácter de proceso constituido por una cadena de acciones integradas a la gestión, y la segunda atendiendo fundamentalmente a sus objetivos.

1.3.2 COMPONENTES

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

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

El ambiente de control refleja el espíritu ético vigente en una entidad respecto del comportamiento de los agentes, la responsabilidad con que encaran sus actividades, y la importancia que le asignan al control interno.

Sirve de base de los otros componentes, ya que es dentro del ambiente reinante que se evalúan los riesgos y se definen las actividades de control tendientes a neutralizarlos, simultáneamente se capta la información relevante y se realizan las comunicaciones pertinentes, dentro de un proceso supervisado y corregido de acuerdo con las circunstancias.

[7] **Organización Internacional de Entidades Fiscalizadoras Superiores**

El modelo refleja el dinamismo propio de los sistemas de control interno. Así, la evaluación de riesgos no sólo influye en las actividades de control, sino que puede también poner de relieve la conveniencia de reconsiderar el manejo de la información y la comunicación.

No se trata de un proceso en serie, en el que un componente incide exclusivamente sobre el siguiente, sino que es interactivo multidireccional en tanto cualquier componente puede influir, y de hecho lo hace, en cualquier otro.

Existe también una relación directa entre los objetivos (Eficiencia de las operaciones, confiabilidad de la información y cumplimiento de leyes y reglamentos) y los cinco componentes referenciados, la que se manifiesta permanentemente en el campo de la gestión: las unidades operativas y cada agente de la organización conforman secuencialmente un esquema orientado a los resultados que se buscan, y la matriz constituida por ese esquema es a su vez cruzada por los componentes.

(COSO)

1.4 COBIT

1.4.1 INTRODUCCIÓN

La información y las tecnologías que la soportan se han convertido en el activo más valioso de las organizaciones en la actualidad, aunque para muchos este concepto no sea aún entendido, las empresas que lo tienen claro reconocen los beneficios de la tecnología para impulsar su crecimiento y generar riqueza.

Estas organizaciones entienden más claramente aún los riesgos asociados con el uso de la tecnología en los procesos del negocio y conocen como administrarlos o mitigarlos.

En la administración del riesgo hay aprovechar al máximo las inversiones en tecnología, asegurar el cumplimiento regulatorio, monitorear y evaluar los indicadores en busca de resultados, son algunos de los elementos claves del gobierno de la empresa y constituyen la esencia del gobierno de TI.

El gobierno de TI es responsabilidad de los ejecutivos o consejo directivo quienes deben proporcionar liderazgo, estructuras y procesos organizacionales que garanticen que la información y las tecnologías relacionadas son la base de las estrategias y objetivos organizacionales.

De esta forma el gobierno de TI asegura que se aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades, y ganando ventajas competitivas. Es necesario indicar que para satisfacer los requerimientos de calidad, seguridad, leyes y regulaciones se debe optimizar el uso de los recursos tanto físicos como intelectuales disponibles en TI y entender claramente su infraestructura para decidir el tipo de gobierno de TI a implementarse.

El objetivo de este marco de referencia es alinear las metas de TI con las metas del negocio con un modelo de procesos que brinda métricas y modelos de madurez para medir sus logros.

(REPOSITORIO UASB) (Torres & Villegas, [C], 2008)

1.4.2 GENERALIDADES

El modelo COBIT intenta responder a las necesidades del negocio, siendo a la vez independiente de la plataforma técnica de TI adoptada en la organización. Dos son los modelos mundialmente conocidos orientados a la implantación de mejoras en las prácticas de control, unos los que tienen su base en el control de los procesos del negocio y los otros orientados a la administración tecnológica.

El marco referencial de COBIT visualiza la información necesaria para dar soporte a los procesos del negocio y la combina con los recursos tecnológicos los que deben ser administrados por los procesos de TI, siendo este el fuerte de COBIT los "requerimientos de negocio para la información" combinándolos con los principios referenciales existentes.

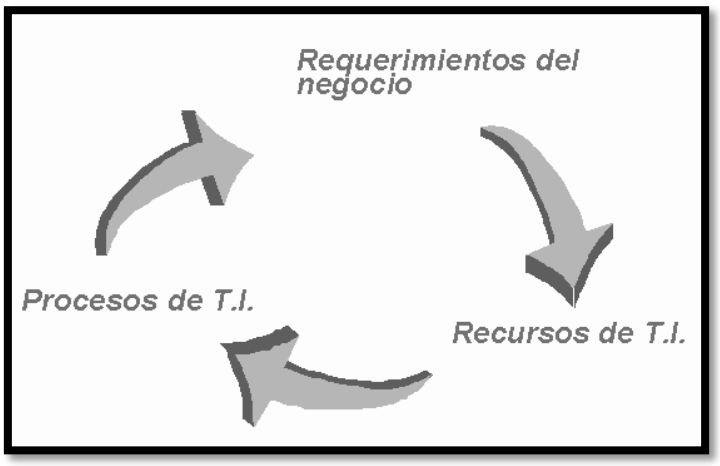

Figura 1-01 Tres enfoques principales del marco referencial

(UNAP)

Al establecer la lista de requerimientos, COBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

- Requerimientos de Calidad (Calidad, Costo y Entrega y Distribución).
- Requerimientos Fiduciarios (Cumplimiento de las leyes y regulaciones).
- Requerimientos de Seguridad (Confidencialidad, Integridad y Disponibilidad).

COBIT considera los requerimientos de calidad dentro de su metodología con los criterios de integridad, efectividad, compara a la calidad de entrega y servicio con la disponibilidad este es el resultado del manejo apropiado del riesgo como resultado de la comparación de oportunidades, el costo es considerado por la eficiencia.

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas de criterios de información y sus definiciones:

- **Efectividad:** Quiere decir que la información importante sea pertinente al proceso del negocio, además oportuna en el momento de su entrega, correcta, consistente y utilizable.
- **Eficiencia:** Es la optimización (más económico, más productivo) de los recursos que se utilizan para la provisión de la información.
- **Confidencialidad:** Es la protección de información sensible contra divulgaciones no autorizadas.
- **Integridad:** Es la precisión y suficiencia de la información, así como también la validez de la información de acuerdo a los valores y expectativas del negocio.
- **Disponibilidad:** Es la disponibilidad de la información para los procesos del negocio en el presente y en el futuro, también la protección de los recursos necesarios y capacidades asociadas.
- **Cumplimiento:** Es el cumplimiento de las leyes, regulaciones, acuerdos contractuales a los que el proceso del negocio está sujeto, ejemplo criterios del negocio impuestos por una fuente externa
- **Confiabilidad de la Información:** Es la provisión de información apropiada para la administración con el fin de operar la entidad y para la obtención de reportes financieros y de cumplimiento.

Las categorías expuestas identifican los recursos de TI que se definen y explican de la siguiente manera:

- **Datos:** Son objetos internos o externos. Estructurados tales como: procesos, funciones, etc. y no estructurados como: gráficos, sonidos, etc.
- **Sistemas de Aplicación:** Es el conjunto de procedimientos manuales y programados.

- **Tecnología:** Abarca hardware, sistemas de administración de base de datos, redes, multimedia, etc.
- **Instalaciones:** Son aquellos recursos que sirven para alojar o para dar soporte a los sistemas de información.
- **Personal:** Se refiere a las habilidades del personal, apreciación, conocimiento para planificar, organizar, adquirir, entregar, dar soporte y monitorear servicios y sistemas de información.

La figura 2-01 describe la relación entre los recursos TI y la entrega de servicios:

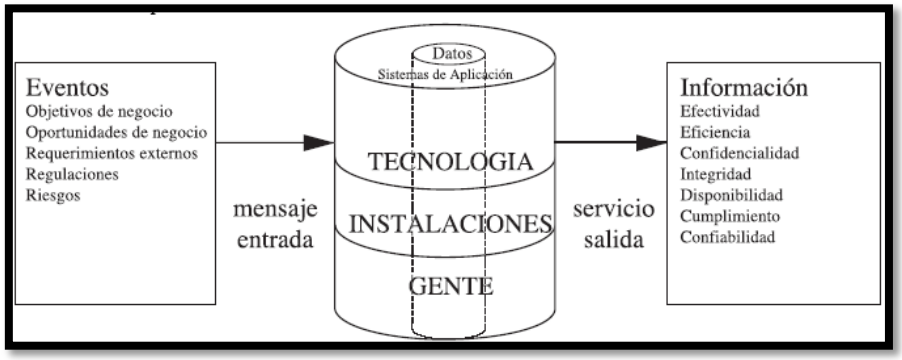

Figura 2-01 La relación entre los recursos TI y la entrega de servicios
(Torres & Villegas, [C], 2008)

Con el fin de asegurar que los requerimientos de negocio para la información sean satisfechos, se deben definir, implementar y monitorear medidas de control adecuadas para estos recursos. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión. Lo cual puede ser identificado mediante la siguiente figura.

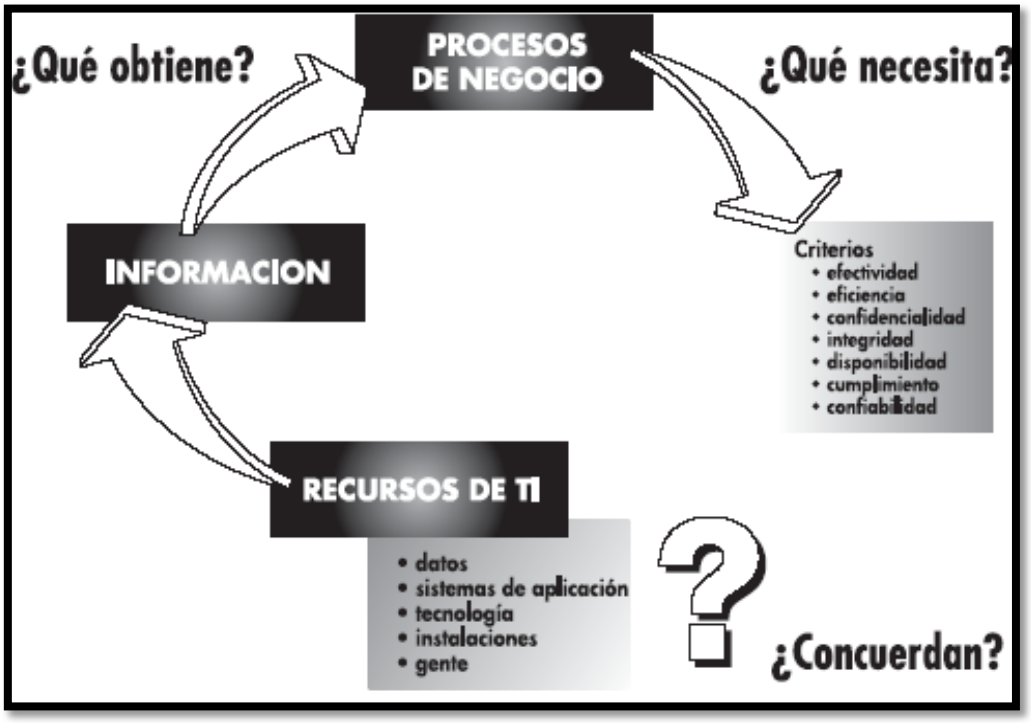

Figura 3-01 Relación del Marco Referencial con las necesidades de la empresa (Torres & Villegas, [C], 2008)

El centro del Marco Referencial son los objetivos de control clasificados y presentados de manera particular y única por COBIT siendo los objetivos de control de alto nivel sobre los cuales se ha establecido la estructura de la metodología. Se pueden diferenciar tres niveles de actividades en un proceso de TI.

En el nivel más bajo encontramos las actividades y tareas necesarias para alcanzar un resultado medible, las actividades cuentan con un ciclo de vida mientras que las tareas son más discretas. En un nivel intermedio encontramos los procesos, que son un conjunto varias tareas y actividades.

El nivel superior de agrupación son los dominios, los dominios en una estructura organizacional se denominan dominios de responsabilidad y se alinean con el ciclo de vida o el ciclo administrativo de los procesos TI.

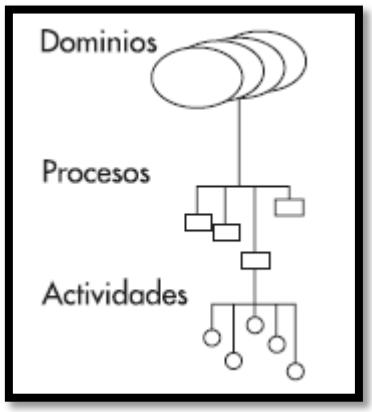

Figura 4-01 Niveles de Actividades de TI
(Torres & Villegas, [C], 2008)

El Marco referencial de COBIT puede ser enfocado desde tres puntos generales: Criterios de Información (Requerimientos del negocio), Recursos de TI, Procesos de TI, estos tres puntos son representados en el cubo de COBIT.

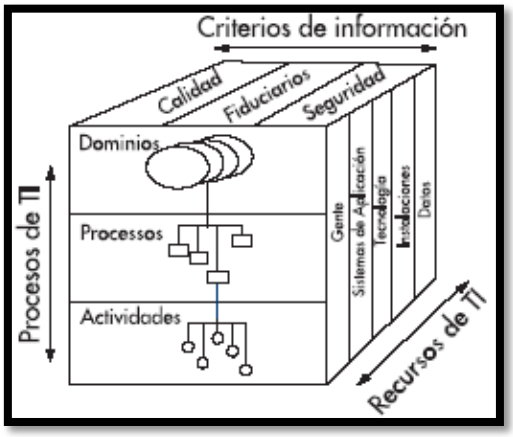

Figura 5-01 Puntos de Enfoque del marco referencial
(Torres & Villegas, [C], 2008)

La Información debe satisfacer para las organizaciones: requerimientos de calidad, seguridad, confiabilidad y disponibilidad. La Gerencia debe balancear el uso de recursos disponibles incluyendo talento humano, instalaciones, hardware y software. Para sustentar esta responsabilidad y lograr sus expectativas, la Gerencia debe establecer un sistema adecuado de control interno.

Este sistema debe dar soporte a los procesos del negocio, ser claro de cómo cada actividad individual de control impacta en los recursos y satisface los requerimientos.

El control interno, que incluye políticas, estructuras organizacionales, prácticas y procedimientos es responsabilidad de la Gerencia.

(Torres & Villegas, [C], 2008)

1.4.3 DOMINIOS

COBIT con un conjunto de 34 Objetivos de Control de alto nivel, uno por cada uno de los Procesos de Tecnología Informática, se agrupan en cuatro Dominios que son los siguientes:

- **Planeamiento y Organización:** Este Dominio cubre la estrategia y las tácticas y le concierne la identificación de la forma en que la tecnología informática puede contribuir mejor al logro de los objetivos del negocio. Más aún, la realización de la visión estratégica necesita planearse, comunicarse y administrarse desde diferentes perspectivas. Finalmente, debe instalarse una organización apropiada así como una infraestructura tecnológica.
- **Adquisición e Implementación:** Para comprender la estrategia de Tecnología Informática, las soluciones de Tecnología Informática necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en el proceso del negocio.
- **Entrega y Soporte:** A este Dominio le concierne la entrega real de los servicios requeridos, que cubre desde las operaciones tradicionales sobre aspectos de seguridad y continuidad hasta el entrenamiento. Para brindar servicios deben instalarse los procesos de soporte necesarios. Este Dominio incluye el procesamiento real de los datos por los sistemas de aplicación, a menudo clasificados como controles de las aplicaciones.

- **Monitoreo y Evaluación:** Todos los procesos de Tecnología Informática necesitan ser evaluados regularmente en el tiempo en su calidad y cumplimiento con los requerimientos de control.

  (Torres & Villegas, [C], 2008)

1.5 ITIL

1.5.1 ORIGEN Y DEFINICIÓN

Es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de información TI de alta calidad. ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

ITIL provee la guía de las "mejores prácticas" sobre todos los aspectos de la administración de servicios "de principio a fin" y cubre todo el espectro de personas, procesos, productos y asociados. ITIL fue diseñada y desarrollada en la década de los ochentas, pero ha sido revisado y actualizado de manera constante para alinearlo con las prácticas más modernas.

Para hacer a ITIL más accesible (y menos costosa) a aquellos que deseen explorarla, uno de los objetivos del proyecto de actualización ITIL versión 2 fue agrupar los libros según unos conjuntos lógicos destinados a tratar los procesos de administración que cada uno cubre. De esta forma, diversos aspectos de los sistemas de TIC, de las aplicaciones y del servicio se presentan en conjuntos temáticos. En el 2007 aparece ITIL V3 que recoge las experiencias de las versiones anteriores y se centra al mismo tiempo en apoyar el negocio base de las empresas e intentar que las mismas puedan conseguir a largo plazo ventajas sobre la competencia mejorando la labor de la organización de TI. La nueva edición ITIL 2011 se publicó a finales de julio de 2011, en esta edición no se añadieron nuevos conceptos sino que se depuro todos los libros de incongruencias en textos y diagramas.

ITIL fue perfeccionada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI.

La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

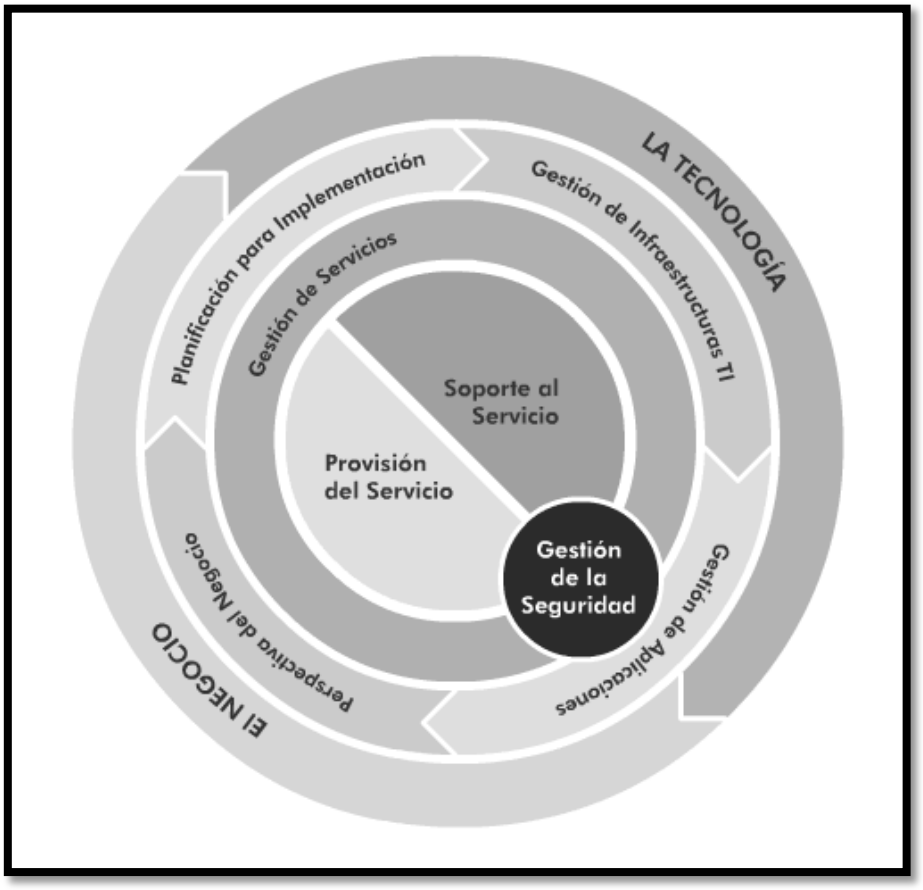

Figura 6-01 ITIL Framework

(OSIATIS)

La Figura 6-01 muestra el ambiente y la estructura dentro de la que fueron creados los módulos. Ilustra la relación que cada uno de los módulos tiene con el negocio y la tecnología. Se puede apreciar cómo el módulo de la Perspectiva del Negocio se encuentra alineado de manera estrecha con el negocio, y el módulo de Gestión de Infraestructura de TI está alineado con la tecnología. Los módulos de Provisión del Servicio y Soporte de Servicio son el núcleo del marco de referencia de procesos.

(OSIATIS)

1.5.2 LIBROS

La revisión reciente ha mejorado la estructura de ITIL y su nuevo alcance, los contenidos y las relaciones entre los diferentes libros son en esencia los siguientes:

- **Entrega de Servicios:** Cubre los procesos requeridos para la planeación y entrega de servicios de TI de calidad y ve a los procesos a un plazo más largo asociado con la mejora de la calidad de los servicios entregados.
- **Soporte de Servicios:** Describe los procesos relacionados con el soporte diario y las actividades de mantenimiento asociadas a la provisión de servicios de TI.
- **Gestión de la Infraestructura de TI:** Cubre todos los aspectos de la administración de infraestructura desde la identificación de los requerimientos del negocio, el proceso de cotización, pruebas, instalación, distribución, operación continua y optimización de los componentes de TI y servicios de TI.
- **Planeación de la Implementación de la Administración de Servicios**: Examina los aspectos y tareas involucradas en la planeación, implementación y mejora de procesos de Administración de Servicios en una organización. También hace referencia a los problemas asociados al Cambio Cultural y Organizacional, el desarrollo de una visión y estrategia y el método de enfoque más apropiado.

- **Administración de Aplicaciones:** Describe cómo administrar las aplicaciones desde las necesidades iníciales del negocio, y durante todas las etapas del ciclo de vida de la aplicación, hasta e inclusive, su retiro. Pone énfasis en asegurar que los proyectos y estrategias de TI estén alineados con las del negocio durante todo el ciclo de vida de la aplicación, para asegurar que el negocio obtiene el mejor valor por su inversión.
- **La Perspectiva del Negocio:** Provee una guía que ayuda al personal de TI a entender cómo puede contribuir a los objetivos del negocio y cómo sus roles y servicios pueden alinearse y aprovecharse de mejor manera para maximizar su contribución.
- **Administración de la Seguridad:** Detalla el proceso de la planeación y administración de un nivel de seguridad definido para la información y los servicios de TI, incluyendo todos los aspectos asociados con la respuesta a incidentes de Seguridad. Incluye también la evaluación y administración de riesgos y vulnerabilidades, y la implementación de contra medidas que se justifiquen en costo.

Para asistir en la implementación de prácticas ITIL, se publicó un libro adicional con guías de implementación (principalmente de la Gestión de Servicios):

- Planeando implementar la Gestión de Servicios.

Adicional a los ocho libros originales, se añadió una guía con recomendaciones para departamentos de TI más pequeños:

- Implementación de ITIL a pequeña escala

(Torres & Villegas, [C], 2008)

CAPÍTULO 2. SITUACIÓN ACTUAL

El entorno financiero es susceptible debido al manejo de dinero e información de clientes que en manos incorrectas pueden ocasionar mucho daño tanto a la entidad como a sus clientes, el control interno es fundamental para determinar procesos que mitiguen cualquier fuga o manejo incorrecto de la información, la tecnología es la herramienta indica para entregar un servicio de calidad y validar que los procesos de control sean efectivos.

Las entidades financieras internacionales y nacionales están en un constante cambio innovando sus servicios para satisfacer a sus clientes externos e internos, hoy aquellos servicios son medidos por su generación de valor, debido a esto tienen que ser evaluados y controlados por una entidad supervisora financiera.

2.1 ENTORNO MACRO

Dentro del entorno macro encontraremos ejemplos de modelos de control interno aplicados en entidades financieras, todos los procesos se rigen a los acuerdos estipulados en Basilea, complementados con metodologías y marcos de referencia tecnológicas.

2.1.1 CONTROL INTERNO EN ENTIDADES FINANCIERAS A NIVEL INTERNACIONAL

La Ley SOX[8] exige a las entidades inscritas en la Bolsa de Valores de Nueva York el establecer, mantener y valorar la efectividad del Sistema de Control Interno para la presentación de reportes financieros.

[8] Sarbanes Oxley

De acuerdo a lo anterior, a partir del año 2006, la Administración en este caso como ejemplo la banca colombiana es responsable por establecer y mantener un adecuado Sistema de Control Interno y periódicamente evaluarlo para concluir sobre su efectividad.

Igualmente, la ley exige que un Auditor Independiente (Revisoría Fiscal), realice la evaluación del Sistema de Control Interno y emita una opción sobre la efectividad del mismo.

Teniendo en cuenta que la ley recomienda el uso del Modelo de Control Interno COSO[9] y que la banca colombiana tomó la decisión de adoptarlo, la evaluación del Sistema de Control Interno se realiza considerando las actividades desarrolladas para el cumplimiento de cada uno de los cinco componentes: Ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y monitoreo.

Las anteriores actividades se pueden desarrollar a nivel de la Entidad (directrices de la alta gerencia y con alcance global para las entidades financieras que demarcan el tono de gobierno) y a nivel de las actividades (acciones realizadas en cada uno de los procesos).

La banca colombiana tomó la decisión de adoptar COBIT[10] como modelo de referencia, a nivel internacional COBIT es el modelo utilizado por los auditores para verificar la adhesión y cumplimiento de los modelos de control interno por parte de cada una de las entidades que son objetos de supervisión y control en términos de los servicios de TI[11].

(GRUPOBANCOLOMBIA)

[9] Committee of Sponsoring Organizations of the Treadway Commission
[10] Control Objectives for Information and related Technology
[11] Tecnologías de la Información

La implementación de COBIT como modelo de referencia permite garantizar el cumplimiento de la ley SOX. Implementar COBIT es una acción proactiva, no sólo en términos de cumplir la legislación sino de implementar acciones de mejoramiento de los procesos y/o servicios de las áreas de tecnología.

La Superintendencia Financiera de Colombia expidió la Circular Externa No. 014 de 2009 por la cual imparte instrucciones relativas a la revisión y adecuación del Sistema de Control Interno de las entidades supervisadas.

Esta circular establece un marco conceptual y normativo para el Sistema de Control Interno como elemento fundamental del Gobierno Corporativo de las entidades supervisadas, basado en modelos ampliamente aceptados a nivel internacional (COSO y COBIT) que contemplan en detalle la noción, contenido y alcance del Sistema de Control Interno.

Específicamente busca que las entidades vigiladas fortalezcan los Sistemas de Control Interno para la apropiada administración de los riesgos a los cuales se ven expuestas en el desarrollo de sus actividades. Así mismo, la Circular Externa 014 de 2009, establece que las entidades financieras vigiladas por esta entidad deberán tomar como referencia en su modelo de Sistema de Control Interno, los siguientes modelos internacionales: COBIT, COSO I, COSO II, Basilea, SOX y estándares de Auditoría Interna.

(GRUPOBANCOLOMBIA)

2.1.2 CASOS REALES DE FALENCIAS ENCONTRADAS EN ATAQUES EFECTUADOS A LA INTEGRIDAD DE LA INFORMACIÓN

Los ataques a la integridad de los datos consisten en la modificación intencional de los datos, sin autorización alguna, en algún momento de su ciclo de vida y comprende las siguientes etapas:

- Introducción, creación y/o adquisición de datos.

- Procesamiento y/o derivación de datos.
- Almacenamiento, replicación y distribución de datos.
- Archivado y recuperación de datos.
- Realización de copias de respaldo y restablecimiento de datos.
- Borrado, eliminación y destrucción de datos.

El fraude es el más antiguo de los métodos destinados a atacar la integridad de los datos, tiene múltiples variantes, las cuales no analizaremos en el presente artículo, excepto para mencionar un caso que, en el año 2008, apareció en la primera plana de los periódicos de todo el mundo: Un empleado de Societe Generale de Francia incurrió en delitos de "abuso de confianza, falsificación y uso no autorizado de los sistemas informáticos del banco", que produjeron pérdidas estimadas en €4900 millones.

A juzgar por la cantidad de publicaciones y conferencias internacionales que abordan el tema del fraude, es probable que este caso siga estando vigente durante algún tiempo. Hace años que las organizaciones que operan tanto en el sector público como en el privado sufren alteraciones en sus sitios web, pero, más allá del eventual perjuicio a la reputación de una empresa, ninguno de los daños ocasionados puede considerarse "catastrófico"

Las bombas lógicas, el software no autorizado que se introduce en un sistema por acción de las personas encargadas de programarlo/mantenerlo, los troyanos y demás virus similares también pueden afectar la integridad de los datos a través de la introducción de modificaciones (por ejemplo, al definir una fórmula incorrecta en una hoja de cálculo) o la encriptación de datos y posterior exigencia de un "rescate" para revelar la clave de desencriptación. En los últimos años se han producido numerosos ataques de características similares a las mencionadas, que afectan principalmente los discos duros de las computadoras personales. Debería esperarse que tarde o temprano se produzcan ataques de este tipo destinados a los servidores. La modificación no autorizada de sistemas operativos (servidores y redes) y/o de software de aplicaciones (como los códigos no documentados), tablas de bases de datos, datos de producción y configuración de infraestructura también se consideran ataques a la integridad de los datos.

Es lógico suponer que los hallazgos de las auditorías de TI incluyen con regularidad las fallas producidas en procesos clave, particularmente en la gestión del acceso privilegiado, la gestión de cambios, la segregación de funciones y la supervisión de registros.

Estas fallas posibilitan la introducción de modificaciones no autorizadas y dificultan su detección (hasta que se produce algún incidente). Otro método de ataque a la integridad de los datos es la interferencia en los sistemas de control de supervisión y adquisición de datos (SCADA, Supervisory Control and Data Acquisition), como los que se utilizan en infraestructuras críticas (suministro de agua, electricidad, etc.) y procesos industriales. A menudo, la función de TI no interviene en la instalación, el funcionamiento ni la gestión de estos sistemas.

El ataque dirigido a plantas de enriquecimiento de uranio en Irán durante el año 2010 había sido planeado con la finalidad de alterar el comportamiento de los sistemas de centrifugación sin que los tableros de control indicaran ninguna anomalía.

Cabe destacar que muchos de estos sistemas de control no están conectados a Internet y que, en el caso de la inyección del software Stuxnet[12], debió realizarse una intervención manual, un hecho que confirma la teoría de que el "hombre" sigue siendo el eslabón más débil de la cadena de aseguramiento/seguridad de la información.

(ISACA)

2.2 ENTORNO MICRO

La evolución de los delitos significa que las entidades financieras deben hacer frecuentes inversiones para blindar sus sistemas, el Ecuador no está exento de estos ataques y en la medida en que una entidad financiera se proteja le dará mayor confianza a su clientes, lo cual se traducirse en una mayor lealtad por parte de ellos.

[12] **Gusano informático que afecta a equipos con Windows, descubierto en junio de 2010**

2.2.1 CONTROL INTERNO EN ENTIDADES FINANCIERAS EN EL ECUADOR

Las entidades financieras cuentan con un área de seguridad informática, y dentro de la Asociación existe un comité de seguridad bancaria que agrupa a todos los jefes de seguridad.

El negocio financiero en este momento tiene un fuerte componente tecnológico y Ecuador no es la excepción. Por lo cual el sistema financiero ecuatoriano debería estar a la par de los sistemas mundiales, que ponen como prioridad máxima de sus negocios la protección contra los ataques cibernéticos.

Los activos más importantes de la institución bancaria son los clientes, por lo tanto está implícita la responsabilidad de cuidar la información que se proporciona a través de sistemas que bloqueen el ataque de hackers o de fraudes informáticos.

Al organismo de control (Superintendencia de Bancos) le toca velar porque los estándares de seguridad de los datos que se manejan en las entidades financieras tengan los más altos niveles.

Ecuador no es que ocupa un sitial importante en el mundo de las inversiones, otros países tienen sistemas más complejos y nuestra banca tendrá que ir evolucionando hacia ellos. Los delitos comunes se incrementan día a día, también ocurre en la parte informática; y aunque el regulador establezca nueva medidas para bloquear el ataque, los ladrones virtuales estudian cada día nuevos mecanismos para evadir esas seguridades.

Con el objeto de asegurar una adecuada planificación y administración de la TI, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos, las mismas se refieren a:

a) Con el objeto de garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

- El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia.
- Un plan funcional de TI alineado con el plan estratégico institucional; y un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos.
- Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos.
- Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación.

b) Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

- Manuales o reglamentos internos, aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de TI.
- Un procedimiento de clasificación y control de activos de tecnología de información, que al menos considere, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes.

c) Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

- Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información.
- Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

d) Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

- Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas.
- Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada.
- Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría.

- Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude.
- Adecuados sistemas de control y autenticación para evitar accesos no autorizados.
- Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos.
- Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores.
- Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida.
- Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información.
- Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información.

e) Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

- Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; entre otros.
- Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado.
- Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios.
- Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

f) Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

- Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados.
- Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución.
- Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción.

- Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

g) Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada, las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

(SBS)

Al momento la ley bursátil se encuentra en debate por la asamblea, en resumen este proyecto de ley consta de 158 artículos e incluye reformas a varias leyes, como la de Mercado de Valores, de Compañías, de las Instituciones del Sistema Financiero, Notarial, de Registro, de Régimen Tributario Interno y la ley para la Equidad Tributaria en el Ecuador; además de reformas a los códigos de Procedimiento Civil y de Comercio.

Esencialmente el desarrollo integral del mercado de valores en el Ecuador, regulando la participación de nuevos inversionistas públicos o privados, que beneficien a las medianas o pequeñas empresas, las cuales podrán acceder a otras fuentes de financiamiento diferentes a las del sector financiero, teniendo este último que mejorar su oferta de créditos incentivando al microempresario con mejores beneficios y asesoramiento para invertir su dinero. Los Bancos en general tienen que invertir en el mercado de valores, dejando inversiones en bolsas del exterior, este tema hasta este momento es un punto de debate, pero en la práctica llevará al País a un manejo transparente de las inversiones.

2.2.2 MODELO COMPARATIVO DEL MANEJO DE CONTROL INTERNO ENTRE EL ECUADOR Y PAÍSES DEL PRIMER MUNDO

En Ecuador las entidades y organismos financieros deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo. Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos.

Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología. No se presentan por parte de la Superintendencia de Bancos y Seguros una normativa o estándar internacional para el manejo del control interno, todos los conceptos del manejo financiero únicamente se fundamentan en el acuerdo de Basilea.

En la región muchos países por falta de una normativa de control interno produjeron la quiebra de bancos. En Ecuador liquidaron 15 de los 30 bancos que operaban, Nicaragua liquidaron 6 de 12 bancos que funcionaban, México los bancos no conceden préstamos, Argentina, Uruguay, Paraguay, Brasil, Perú, Venezuela, Colombia, con problemas de orden económico, social y financiero.

La normativa dirigida al control interno no ha sido formalmente definida por los organismos profesionales nacionales, las organizaciones regionales como la Asociación Interamericana de Contabilidad (AIC) y las instituciones internacionales de profesionales como la Federación Internacional de Contabilidad (IFAC de sus siglas en inglés), que requiere una definición general, que se fundamente en una estructura acordada o consensuada, quizá sobre la base del Informe COSO, adaptada a los requerimientos de la región y potencialmente especificadas a nivel de cada país para el futuro. El enfoque moderno del control interno integrado se fundamenta en los valores y los principios éticos del personal de las organizaciones.

Tanto en el Ecuador como en todos los países que siguen el acuerdo de Basilea el control interno debe aportar un grado de seguridad razonable, en ningún caso la seguridad será total o absoluta, a la dirección superior de la organización, en relación al cumplimiento de la metas y objetivos institucionales.

La estructura del acuerdo de Basilea establece en base a tres pilares fundamentales, donde se han incluido los diferentes métodos de medición de riesgos:

- **Pilar I:** Establece requisitos mínimos de capital
- **Pilar II:** Fomenta la labor supervisora tendente al reforzamiento de la evaluación del riesgo y utilización de las herramientas y procedimientos adecuados para la gestión del riesgo.
- **Pilar III:** Disciplina de mercado. Referida principalmente a la transparencia informativa sobre el riesgo y capital de cada entidad.

En lo concerniente al desarrollo de esta guía metodológica el pilar II es un punto de vista a tomar. Para garantizar la evaluación de riego el acuerdo de Basilea considera los siguientes principios:

- **Principio 1:** Los bancos evaluarán, mediante un proceso integral la cuantía de su capital total en función de su perfil de riesgo y con una estrategia para el mantenimiento de sus niveles de capital. El banco tendrá que demostrar que sus objetivos internos de capital están bien fundamentados y resultan acordes con su perfil general de riesgo y con su actual entorno operativo.

  Las cinco características más importantes de un proceso riguroso de supervisión son:
  - Vigilancia por parte del consejo de administración y de la alta dirección.
  - Evaluación rigurosa del capital
  - Evaluación integral de los riesgos
  - Seguimiento e información y
  - Examen de los controles internos

- **Principio 2:** Las autoridades supervisoras deberán evaluar periódicamente los procesos utilizados por los bancos para determinar la suficiencia de capital, la posición de riesgo de la entidad, los niveles de capital resultantes y la calidad del capital mantenido. Los supervisores deberán también examinar los procesos internos de evaluación de la suficiencia de capital. El examen deberá centrarse en:
  - Calidad de la gestión
  - Control del riesgo
  - El banco no podrá suponer que los supervisores acaban realizando las funciones correspondientes a la dirección de la entidad.

- **Principio 3:** Se espera que los bancos sitúen sus cifras de capital por encima de mínimos establecidos, debido a que deben tratar de cubrir también riesgos por pérdidas inesperadas que no han sido tenidas en cuenta dentro del capital mínimo. Es posible que algunos riesgos, ya sean específicos a determinados bancos o relativos al conjunto de la economía, no estén contemplados en el Pilar I.

- **Principio 4:** La autoridad monetaria del país tratará de impedir que los niveles de capital de cada entidad se sitúen por debajo de los mínimos, lo que haría peligrar la estabilidad no del propio banco sino además la del sistema financiero.

  El supervisor podrá adoptar diferentes medidas, siempre que exista la sospecha que un banco puede infringir los principios rectores, antes mencionados. Entre estas medidas se pueden mencionar:
  - Intensificar la supervisión del banco.
  - Restringir el pago de dividendos.
  - Obligar al banco a preparar y aplicar un plan satisfactorio para restablecer la suficiencia de capital.
  - Exigir al banco la obtención inmediata de capital adicional.

(UBIOBIO)

La seguridad razonable requerida para el cumplimiento de los objetivos de las organizaciones es posible programarla mediante el diseño y aplicación de un sistema de control interno integrado a las operaciones sustantivas de la organización, completándola mediante las evaluaciones periódicas internas y externas del control interno.

Algunas limitaciones que ratifican la característica de seguridad razonable del control interno se fundamentan en los siguientes aspectos:

- Decisiones del personal pueden ser erradas.
- Pueden suceder fallas humanas.

- Controles diseñados que pueden ser burlados por alianza entre dos o más personas que participan en el proceso de la operación.
- Alta dirección que puede eludir los controles internos en todos los casos que los estime conveniente para fines fraudulentos o de interés personal.
- Ausencia de información importante para la toma de decisiones. Sea por ocultamiento de la información o porque los resultados negativos hayan sido maquillados para presentar resultados de la gestión de las finanzas en forma satisfactoria.

En el Ecuador el ente regulador no emite una ley en la cual se exija la implementación de normas o marcos de referencia que ayuden a controlar lo ejecutado en el acuerdo de Basilea, en la siguiente tabla se puede ver una comparación de los marcos de referencia o normas que rigen en otros países.

PAIS	***COSO***	***COBIT***
Ecuador		O
Colombia	X	X
Estados Unidos	X	X

X Normativa obligatoria

O Se aplica pero no es obligatoria

Tabla 1-02 Normativas aplicadas en los Países consultados
(Torres, [A], 2013)

CAPÍTULO 3. TECNOLOGÍAS DE APOYO PARA LA PROTECCIÓN DE LA INFORMACIÓN

Una vez estudiadas las normas y estándares que aseguran el control interno dentro de la organización hay que implementar herramientas complementarias de hardware y software, su fin son fortalecer los controles y el cumplimiento de estos estándares, a continuación se presentan las tecnologías que apoyan la protección de la información.

3.1 SISTEMAS PARA EL CONTROL DE FUGA DE INFORMACIÓN

Las empresas en su día a día manejan una gran cantidad de información confidencial, que en ninguno de los casos debería salir del entorno en el que encuentra ubicada. Nos referimos, por ejemplo, a nóminas, presupuestos, tarjetas de crédito, información de empleados, etc. Muchos datos, reseñas y detalles que, de salir a la luz, comprometerían seriamente la seguridad, tanto de los empleados, como de la propia empresa donde se generan estos documentos.

La evolución del concepto de seguridad nos ha llevado, por consiguiente, hasta la importancia de la prevención de la pérdida de estos datos, algo que se ha convertido en la actualidad en una de las principales preocupaciones de los directores TI[13] de seguridad. Las distintas tecnologías de prevención de fugas de información, hoy conocidas como tecnologías Data Loss Prevention (DLP), se están volviendo en el caballo de batalla del mercado, el epicentro de un concepto de gestión segura optimizada que ha de evitar que toda la información corporativa viaje libremente sin ningún tipo de control. Aquellos fabricantes de referencia en el mercado de la seguridad y con un largo recorrido en la protección de las corporaciones ya están incluyendo en su portfolio soluciones de seguridad basadas en evitar la fuga de información.

[13] Tecnologías de la Información

Estos fabricantes han sido los primeros receptores de la elevada demanda que existe en este ámbito; han sido también, a la par, los primeros concienciados de la importancia de aportar soluciones robustas que atiendan estas necesidades que se dan en entidades de todos los tamaños.

Dentro del abanico de posibilidades que plantea cada fabricante destacan los sistemas de cifrado de disco duro y carpetas, cifrado y control de dispositivos extraíbles como USB, bluetooth, CD/DVD, sistemas de gestión de identidad y acceso a red y sistemas perimetrales capaces de detectar la fuga de información en una barrera de seguridad más externa.

Estamos ante una tecnología emergente, pero con un futuro palpable; una tecnología que está en sus primeros años de vida, pero que en cierta manera podemos decir que todo el mundo estaba ya esperando. Todos podemos entender a la perfección que ninguna organización está en disposición de ver comprometida la protección del flujo de información interno que maneja; que ahí es donde se halla su valor y potencial en donde se cobija el propio compromiso con sus clientes y su integridad. Es por tanto, de fácil predicción que todo aquel sistema o solución tecnológica que refuerce y fortalezca este ámbito gozará de un interés inusitado. Las empresas han pasado los últimos años aprendiendo a combatir el contenido malicioso entrante, como virus, troyanos, spyware y spam. Pero la implementación de firewalls, antivirus y antispyware en el perímetro no han podido combatir una amenaza que ha crecido sigilosamente tanto en importancia como en impacto: “la fuga de datos”.

Quedaron atrás los días en los que la propiedad intelectual y los secretos corporativos se guardaban en cajas fuertes. Casi toda la información corporativa se almacena electrónicamente y es accesible para la mayoría de los empleados. Los dispositivos móviles utilizados para almacenamiento tienen cada día mayor capacidad por lo que la cantidad de datos expuesta es mayor y la pérdida o el robo se dan más fácilmente.

Cuando hablamos de soluciones DLP[14] nos referimos a un conjunto probado de herramientas que proporcionan una monitorización bidireccional del flujo de información, realizando funciones de inspección de contenidos en el tráfico saliente.

Asimismo de forma simultánea estas herramientas pueden efectuar funciones de "higiene perimetral" (antivirus, antispyware, antispam, filtrado de URL,...) en el tráfico de entrada de modo que logran una barrera de seguridad completa desde cualquier punto de vista.

En la actualidad, cada vez más numerosos dispositivos móviles que se usan en las organizaciones pueden exponer una ingente cantidad de datos fuera del perímetro de seguridad que ofrece el entorno de la oficina.

Existe en el mercado una gama de producto específica para solucionar este problema, protegiendo los datos de dispositivos móviles y portátiles mediante el cifrado, convirtiendo dicha información en "inaccesible" para todo aquel sujeto no consentido. Su administración completa de puertos y dispositivos de almacenamiento impide además la copia no autorizada de dicha información.

En definitiva, hoy en día el mercado nos ofrece las herramientas y soluciones necesarias para proteger nuestros datos desde todas las direcciones y frentes, como nunca antes habíamos visto o contemplado, ya no valen las excusas; ahora nuestros datos críticos pueden tener la mejor de las fortalezas, sin ataques y, gracias al avance de las soluciones DLP, sin fugas comprometidas. En resumen DLP es un término de seguridad referente a un sistema que identifica, monitorea y protege datos en uso, datos en movimiento y datos en reposo por medio de mecanismos de inspección, análisis contextual de transacciones (origen, destino, medio, etc...), siendo administrado desde una consola central donde tiene la capacidad de detectar y prevenir uso no autorizado así como transmisión de información confidencial.

(DLP)

[14] **Data Loss Prevention**

Los sistemas basados en DLP mantienen como base los siguientes controles:

- **Cifrado:** Entre sus características destacan el cifrado para portátiles, desktops, servers y dispositivos móviles con la flexibilidad de elegir entre el cifrado de disco completo o de archivos/carpetas. Confianza en la integridad de datos confidenciales cuando se pierde o se roba un dispositivo. Protección Safe Harbor (o sea, pérdida de datos cifrados = no-incidente, que no exige la divulgación pública), esto para empresas norteamericanas o algunas internacionales sujetas a esta norma.

- **Prevención de Pérdida de Datos:** Entre sus características destacan evitar que los usuarios transmitan datos confidenciales, ya sea accidentalmente o intencionalmente. Da visibilidad y control completos del uso y del movimiento de datos confidenciales. Permite que la infraestructura y sus datos se protejan. Protege contra escapes accidentales causados por las tareas cotidianas de los usuarios. Ofrece una gama completa de reacciones prácticas en el momento de la detección de la pérdida de datos confidenciales, tales como:
    - Registro detallado y recopilación de pruebas forenses,
    - Prevención y bloqueo en tiempo real,
    - Notificación a usuarios y administradores,
    - Cuarentena de datos confidenciales.

- **Control de Dispositivos:** Entre sus características destacan monitorear y permitir que sólo los dispositivos autorizados se conecten en el equipo (Laptop, Desktop o Servidores). Restringir y bloquear la posibilidad de conexión de dispositivos no autorizados, tales como teléfonos, memorias USB, tabletas, discos duros externos, etc.

  Fiscaliza el control sobre qué datos se pueden copiar en dispositivos autorizados. Control refinado de datos y dispositivos. Permite conectar únicamente los dispositivos autorizados por la empresa.

Políticas por usuario, grupo o departamento, por ejemplo, permite que el Gerente se conecte con cualquier dispositivo y en cualquier máquina, mientras que otros empleados pueden conectarse sólo con un subconjunto de dispositivos y/o sólo en ciertas máquinas.

Registro detallado a nivel de usuario y dispositivo para las necesidades de auditoría y conformidad. Permite controlar y evitar el uso de la unidad de CD/DVD, salvo para los CDs (o DVDs), que el área de sistemas defina.

Controla la conexión a través de cualquier puerto que tenga el equipo. Incrementa la productividad y disminuye el riesgo, al basar las políticas en marcas, modelos y hasta firmware.

- **Dispositivos USB Cifrados:** Entre sus características destacan la protección para los medios de almacenamiento externos de sus usuarios intensivos. Poder asegurar que los datos confidenciales transportados en medios externos permanezcan continuamente protegidos. Optimización del flujo de trabajo para ahorrar tiempo y dinero utilizando el directorio activo para establecer la correspondencia entre usuarios y dispositivos. Cifrado de los datos en el momento del uso y apertura con contraseña tradicional o biomecánicos, con huella digital.

3.2 NUEVAS TECNOLOGÍAS PARA EL CONTROL DE TARJETAS DE PAGO (CRÉDITO)

El uso de las tarjetas de crédito como medio de pago y los canales a través de los cuales se pueden acceder a realizar consumos es un producto vigente en el mercado y de importancia para las entidades financieras. Sin embargo este sector es blanco de constantes amenazas y/o modalidades de fraude a las que están expuestos los clientes y establecimientos. Así tenemos varios tipos de fraude:

- **Tarjeta Perdida:** Cuando el cliente pierde la tarjeta, quien la encuentra la utiliza fraudulentamente.

- **Tarjeta Robada:** Cuando se produce el robo físico de la tarjeta de crédito para ser utilizada fraudulentamente.
- **Falsificación de Tarjeta:** Cuando se copia la información de la banda magnética de la tarjeta para incluirla en un nuevo plástico con la intención de cometer fraude.
- **Tarjeta No recibida por el Cliente:** Las tarjetas son interceptadas antes de ser recibidas por el cliente para ser utilizadas fraudulentamente.
- **Suplantación de Identidad:** Los consumos son efectuados suplantando la identidad de otra persona a través de canales electrónicos y/o presenciales.

El fraude es variable e impredecible puede atacarnos en cualquier momento podemos detectarlo, analizarlo, vigilarlo, prevenirlo pero nunca detenerlo del todo. Los delincuentes prefieren tarjetas de cupos altos.

Evolución del Fraude:

- Migración de bandas internacionales de delincuentes organizadas y con recursos.
- Tecnología avanzada, económica y disponible.
- Conocimiento de la industria e infraestructura.
- Facilidades de consumos a través Internet sin presencia física del cliente ni del plástico.

Aspectos Generales que ayudan a prevenir el Fraude:

- Conocer adecuadamente los productos con los que se trabaja
- Aplicar los controles establecidos: segregación de funciones, confidencialidad de la información restringida entre otros.
- Mantener control visual sobre la tarjeta de crédito al momento de realizar el consumo.
- Alertar oportunamente eventos que puedan fomentar los consumos indebidos.

La revisión, análisis y seguimiento de transacciones sospechosas se las puede realizar con la herramienta "SENTINEL PREVENTION[15]", que mediante el uso de reglas de monitoreo permite identificar o determinar si una transacción es considerada como sospechosa y/o fraudulenta.

Las reglas están compuestas por varios parámetros que permiten segmentar y crear condiciones para ejecutar el monitoreo, tales como: monto, número de transacciones, tipo de bin, país de origen, giro de comercio entre otros.

Las reglas de monitoreo se dividen en dos grupos:

- Las reglas exigidas como mínimas por las franquicias Mastercard y Visa.
- Las reglas que son creadas por las instituciones financieras en función de las necesidades y experiencias de casos o situaciones que registra el histórico de casos de fraude tanto de clientes como del intercambio de información con otras instituciones financieras (Emisores y/o Adquirentes) del país.

Así también se han definido niveles de riesgo para cada regla a través del "Acuerdo Sentinel", con el fin de establecer la prioridad de atención a las reglas, la prioridad es directamente proporcional al nivel de riesgo, así tenemos: riesgo alto – prioridad alta, riesgo medio – prioridad media y riesgo bajo – prioridad baja.

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (Crédito) (PCI) se desarrollaron 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. Las PCI[16] DSS[17] proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas.

[15] **Es una solución especializada, para la prevención de las pérdidas ocurridas debido al fraude en transacciones con tarjetas de crédito, débito, privadas, en los siguientes canales: puntos de venta, ATM´s, transferencias por internet, pagos a comercios y banca móvil. Enfocada al negocio emisor y al adquirente con una clara diferenciación de las herramientas utilizadas para prevenir el fraude en cada una, con un enfoque en tiempo real, en línea y batch.**

[16] **Industria de Tarjetas de Pago (Crédito)**

[17] **Normas de Seguridad de Datos**

Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas.

Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos. Los requisitos de seguridad de las PCI DSS se aplican a todos los componentes del sistema.

En el contexto de las PCI DSS, los "componentes del sistema" se definen como cualquier componente de red, servidor o aplicación que esté incluida en el entorno de los datos del titular de la tarjeta o que esté conectado a éste.

Los “componentes del sistema” también incluyen cualquier componente de virtualización tales como máquinas virtuales, interruptores/routers virtuales, dispositivos virtuales, aplicaciones/escritorios virtuales.

El entorno de los datos de los titulares de tarjetas consta de personas, procesos y tecnología que almacenan, procesan o transmiten datos de titulares de tarjetas o datos confidenciales de autenticación. Los componentes de la red incluyen, a modo de ejemplo, firewalls, interruptores, routers, puntos de acceso inalámbricos, aplicaciones de la red y otras aplicaciones de seguridad.

Los tipos de servidores incluyen, a modo de ejemplo: web, aplicación, base de datos, autenticación, correo electrónico, proxy, protocolo de tiempo de red (NTP) y servidor de nombre de dominio (DNS). Las aplicaciones incluyen todas las aplicaciones compradas y personalizadas, incluidas las aplicaciones internas y externas (como Internet).

El primer paso de una evaluación de las PCI DSS es determinar con exactitud el alcance de la revisión. Por lo menos una vez al año y antes de la evaluación anual, la entidad evaluada debería confirmar la exactitud del alcance de las PCI DSS al identificar todas las ubicaciones y flujos de datos de titulares de tarjetas y al asegurar que se incluyan en el alcance de las PCI DSS. Para confirmar la exactitud e idoneidad del alcance de las PCI DSS, hay que considerar lo siguiente:

- La entidad evaluada identifica y documenta la existencia de todos los datos de los titulares de tarjetas en su entorno, con la finalidad de verificar que no haya datos de titulares de tarjetas fuera del entorno de los datos de los titulares de tarjetas (CDE) actualmente definido.
- Una vez que se hayan identificado y documentado todas las ubicaciones de los datos de los titulares de tarjetas, la entidad utiliza los resultados para verificar que el alcance de las PCI DSS sea apropiado (por ejemplo, los resultados pueden ser un diagrama o un inventario de ubicaciones de datos de titulares de tarjetas).
- La entidad considera que todos los datos de titulares de tarjetas encontrados están dentro del alcance de la evaluación de las PCI DSS y forman parte del CDE[18], a menos que dichos datos se eliminen o migren/consoliden en el CDE actualmente definido.
- La entidad retiene la documentación que demuestre los resultados y cómo se confirmó el alcance de las PCI DSS para la revisión por parte de los asesores y/o como referencia durante la actividad anual de la siguiente confirmación.

(PCI DSS)

[18] **Entorno de los datos de los titulares de tarjetas**

3.3 HERRAMIENTAS PARA LA PREVENCIÓN DE ATAQUES EN LÍNEA

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todo el personal externo tiene las mismas competencias y responsabilidades en cuanto a Internet en sus campos normales de actividad, de acuerdo con los términos del contrato, y están obligados a cumplir siempre con las Guías Corporativas.

El acceso a Internet se restringe exclusivamente a través de la red la empresa, es decir, por medio de un Firewall[19] incorporado en la misma. No está permitido acceder a Internet vía módem (sea un módem individual o en pool).

El Internet es una herramienta de trabajo, todas las actividades en Internet deben estar en relación con tareas y actividades, exclusivamente para cumplimentar las obligaciones contractuales; los usuarios no deben hacer transferencia de datos de o a Internet. En caso de producirse la necesidad de una transmisión, esta deberá ser realizada por personal de la empresa.

Las amenazas de seguridad en el centro de datos: ataques tradicionales de red, ataques de denegación de servicio en HTTP y DNS y vulnerabilidades en el nivel de aplicación son mitigadas con equipos de última generación en la protección de acceso, en este trabajo de investigación se destaca la empresa F5 con su producto BIG-IP que es un firewall con características innovadoras como:

- **BIG-IP Advanced Firewall Manager (AFM):** Como punto central de la solución firewall para centros de datos de F5, BIG-IP Advanced Firewall Manager es un innovador firewall de red construido sobre arquitectura full-proxy que proporciona una seguridad excepcional. Orientando la seguridad de las aplicaciones en torno a ellas mismas, F5 consigue simplificar la política de gestión del firewall.

[19] **Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos (redes) sobre la base de un conjunto de normas y otros criterios.**

Este modelo de seguridad, centrado en la aplicación, impulsa las capacidades e inteligencia líderes de F5 en la entrega de aplicaciones, mejorando el posicionamiento global de seguridad de las empresas, aligerando la complejidad asociada a la seguridad de la infraestructura de aplicaciones a modelos estáticos como las zonas de cortafuegos tradicionales.

- **BIG-IP Access Policy Manager (APM):** Con soporte para SAML 2.0, F5 ofrece capacidades de single sign-on mejoradas para web, VDI y aplicaciones cliente/servidor con independencia de si se alojan en centros de datos o en la nube. Además, ofrece federación de identidades a través de múltiples productos instalados dentro de una misma organización.

- **BIG-IP Application Security Manager (ASM)**: Incluye nuevas funciones para ayudar a las empresas a fortalecer la seguridad de aplicaciones web y para hacer frente a las cambiantes amenazas. BIG-IP ASM cuenta con soporte para aplicaciones desarrolladas con Google Web Toolkit, con lo que los equipos pueden reforzar las políticas de seguridad de las aplicaciones que utiliza este framework ampliamente adoptado. Además, detecta y mitiga amenazas como clickjacking.

(F5)

Internamente se tiene que controlar el uso de ciertas herramientas que tienen al internet como medio de transmisión de datos, así se tiene que:

- Utilizar el acceso a Internet para debates en tiempo real (Chat) siendo "especialmente peligroso", ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema.
- Visitar páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc… que no sirvan como soporte al objetivo de negocio de la empresa.

- La transferencia de ficheros no relativa a actividades de negocio - en particular la bajada de juegos de ordenador, ficheros de sonido y fotos, gráficos, etc.
- El uso del nombre, símbolo, logotipo o símbolo similar de la empresa en ningún elemento de Internet (correo electrónico, páginas web, etc.) sin el previo consentimiento por escrito de la Gerencia Ejecutiva General.
- Facilitar la accesibilidad desde Internet a ningún tipo de Información Corporativa sin obtener previamente consentimiento por escrito.
- Ocultar o manipular su identidad bajo ninguna circunstancia.

CAPÍTULO 4. DESARROLLO DE LA GUÍA METODOLÓGICA PARA LA GESTIÓN DEL CONTROL INTERNO

La constante evolución dentro del mundo tecnológico invita a que el área de tecnología se adapte pronto a los cambios, sin perder su importancia y brindando a las empresas en este caso del sector financiero, una alta confiabilidad en los servicios entregados, con constante innovación, convirtiéndose en un área estratégica en el entorno institucional. El desarrollo de una Guía Metodológica para la Gestión del Control Interno es el camino para cumplir los objetivos propuestos, los siguientes seis pasos están fundamentados en los marcos de referencia y metodologías descritas en los capítulos anteriores, con ellos se garantiza el éxito en la gestión de tecnología, estos son:

- Planificación e implementación de la gestión del servicio
- Planificación e implementación de nuevos servicios o de servicios modificados
- Procesos de provisión de servicio
- Procesos de relaciones
- Procesos de resolución
- Proceso de control

4.1 PLANIFICACIÓN E IMPLEMENTACIÓN DE LA GESTIÓN DEL SERVICIO

En el proceso de planificación e implementación la metodología PDCA[20] es el cimiento primario para fundamentar el control interno de una entidad financiera en todos los servicios de TI[21] y se describirse del modo siguiente:

[20] Metodología conocida como Planificar-Hacer-Verificar-Actuar (PDCA, del inglés Plan-Do-Check-Act)

[21] Tecnologías de la Información

a) **Planificar:** Determinar los objetivos y los procesos necesarios para proporcionar resultados de acuerdo con las necesidades del cliente y con las políticas de la empresa.
b) **Hacer:** Implementar los procesos.
c) **Verificar:** Evaluar, monitorear los procesos y los servicios contrastándolos con las políticas, los objetivos y los requisitos, e informar sobre los resultados obtenidos a las líneas de control.
d) **Actuar:** Iniciar las acciones necesarias para mejorar continuamente el rendimiento y comportamiento del proceso.

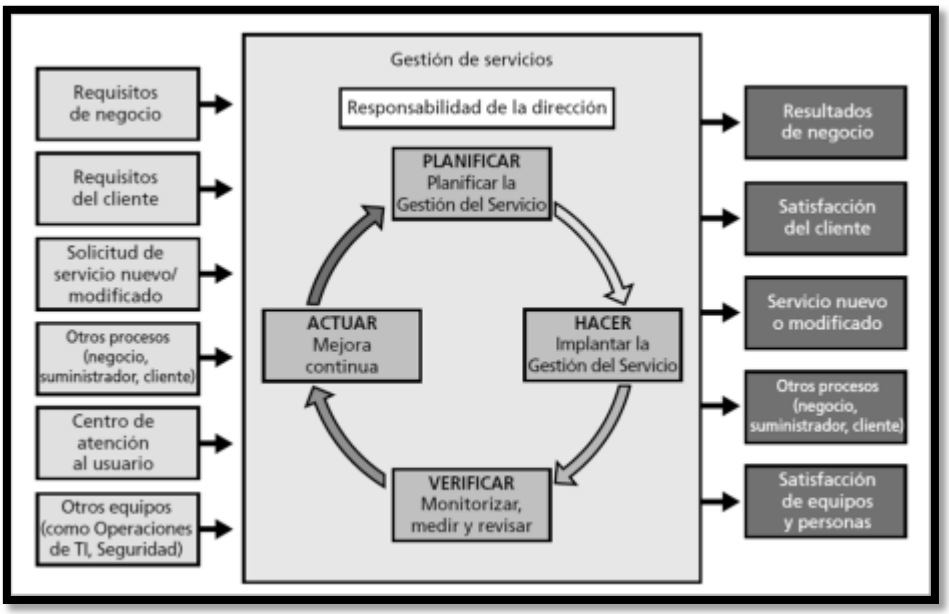

Figura 7-04 Metodología PDCA orientado a TI

(Telefónica, 2010)

La implantación de la gestión del servicio de TI siguiendo el ciclo PDCA aporta entre otros, los beneficios siguientes:

- Permitirá que todas las actividades de transformación de la organización se lleven a cabo de una forma controlada y organizada.

- Los objetivos se fijan en función de la situación de partida, obtenida mediante una evaluación inicial.
- Los proyectos de implementación tiene unos objetivos fijados.
- Se monitorizan y miden los resultados de los proyectos.
- Se establece un plan de mejora continua.
- Se aprovecha la experiencia de otras organizaciones que iniciaron antes el camino.

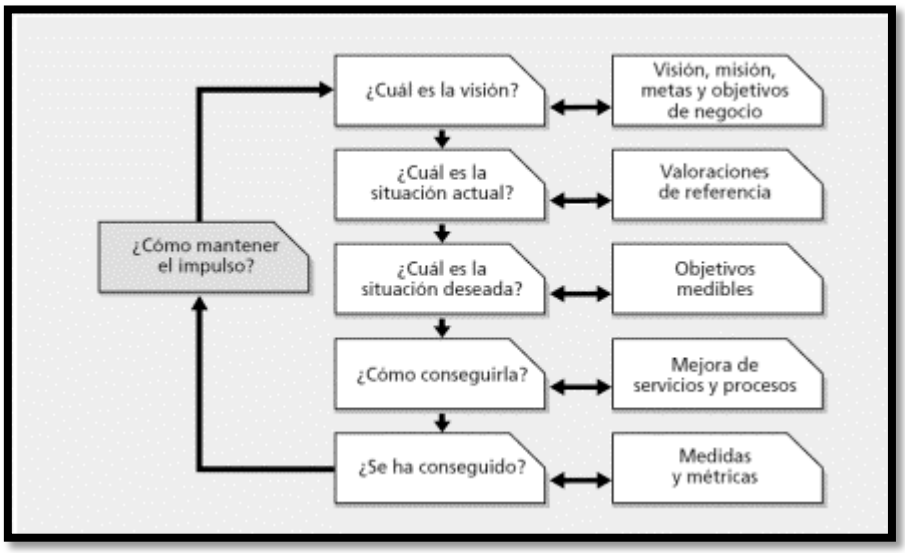

Figura 8-04 Mejora continua

(Torres, [A], 2013)

Es posible establecer las siguientes correspondencias entre estas fases y el ciclo PDCA:

- Planificar – ¿Cuál es la visión? ¿Cuál es la situación actual? ¿Cuál es la situación deseada? (objetivos de negocio de alto nivel, valoraciones, objetivos medibles).
- Hacer – ¿Cómo conseguir la situación deseada? (mejora de procesos).
- Verificar – ¿Cómo comprobar que se han alcanzado los hitos? (medidas y métricas).

- Actuar – ¿Cómo mantener el impulso?

La aplicación de lo descrito en esta sección se la ve a detalle en el anexo I "Resumen Ejecutivo Guía Metodológica para la Gestión del Control Interno".

4.2 PLANIFICACIÓN E IMPLEMENTACIÓN DE NUEVOS SERVICIOS O DE SERVICIOS MODIFICADOS

La misión de entregar nuevos servicios tiene relación con el acuerdo que tengan todas las partes que intervinieron en la planificación, los servicios no solo se componen de código, también utilizan otros componentes como lo son la infraestructura, el personal técnico encargado de la administración y soporte, por ello se debe analizar desde el inicio de la planificación que todos estos actores estén al tanto de sus tareas en cada proceso del ciclo de vida del servicio.

El fundamento de la creación de un nuevo servicio tiene relación con la estrategia de TI, desde aquí se inician las propuestas que darán valor a la gestión tecnológica, la creación de un servicio es como la línea de fábrica de un producto en general, comienza con los requerimientos del negocio (cliente) y termina con los servicios operativos (satisfacción de una necesidad del cliente).

La creación de servicios se ha convertido en un factor clave para lograr el éxito empresarial. El proveedor de TI debe posibilitar un tiempo de entrega de servicios (time-to-market) acorde a las necesidades del cliente, pero también debe contemplar que los costes, la funcionalidad y calidad de los servicios estén ajustados a sus necesidades reales.

Sus responsabilidades principales son las siguientes:

- Responsable de cumplir con lo comprometido con el cliente.
- Controla que el proyecto se constituya cumpliendo con las políticas de TI.
- Hace que otros procesos o áreas realicen lo planificado.

Además, el proceso realiza dos aportaciones fundamentales a la gestión de servicios de TI:

- Organiza todo el ciclo de creación de servicios para que se "fabriquen" en los acordados, con la calidad, costes y funcionalidad pactados.
- Asume la responsabilidad de coordinar a todos los procesos y departamentos de TI para lograr sus objetivos.

Para ello, el ciclo de la provisión de servicios que involucra y gestiona todos los procesos, funciones y áreas de TI implicados. Elabora un plan de trabajo integrado para proveer e implantar el servicio a partir del cual se negocia con el cliente. Una vez que se ha logrado un consenso y acuerdo con el cliente, se aprueba formalmente el plan de proyecto mediante el proceso de gestión del cambio y su órgano de gestión interno, el comité de cambios, en el que están representadas todas las partes implicadas.

Si se tiene un orden en la generación del servicio según lo planificado se logran los siguientes aportes:

- Implementa un ciclo completo de creación y entrega de servicios, desde las necesidades y acuerdos con el cliente hasta su entrega y puesta en funcionamiento operativo.
- Los servicios se crean de una forma eficiente.
- Los servicios se crean en los plazos acordados, velando por las necesidades del negocio en el time-to-market.
- Los servicios de TI se diseñan para satisfacer las necesidades reales del cliente y cumpliendo con la arquitectura y políticas de la entidad financiera.
- Los servicios se crean con la participación de todas las áreas: Desarrollo, Investigación, Producción y Gestión de Servicios.
- Tecnología y sus clientes tienen unas expectativas claras y formalizadas del solicitado.

4.3 PROCESOS DE PROVISIÓN DE SERVICIO

Una vez creado el servicio y puesto con éxito en explotación regular, es necesario desencadenar una serie de actividades que ayuden a garantizar que los servicios cumplen los cometidos pactados con el negocio en términos de: los niveles de servicios, la continuidad, la disponibilidad, los presupuestos, la capacidad y la seguridad.

4.3.1 GESTIÓN DE NIVEL DE SERVICIO

Es el proceso por el cual se definen, negocian y supervisan la calidad de los servicios TI ofrecidos.

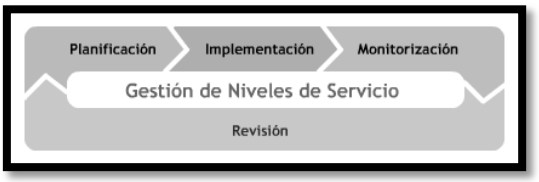

Figura 9-04 Cadena de Valor Gestión Niveles de Servicio

(OSIATIS)

La Gestión de Niveles de Servicio identifica el cumplimiento de políticas, normas y procedimientos que buscan proteger el recurso de la información brindadas en un servicio con un proceso que tiene como fin mantener y mejor la calidad de los servicios de TI mediante una gestión eficiente de los acuerdos de nivel de servicio firmados con los clientes.

La fijación de los objetivos de los servicios mediante parámetros medibles garantiza un alto nivel de control y confianza de que los niveles de servicio acordados se pueden cumplir. Se pueden tener indicadores precisos del esfuerzo que le supone a TI alcanzar en la aplicación de los niveles de servicio.

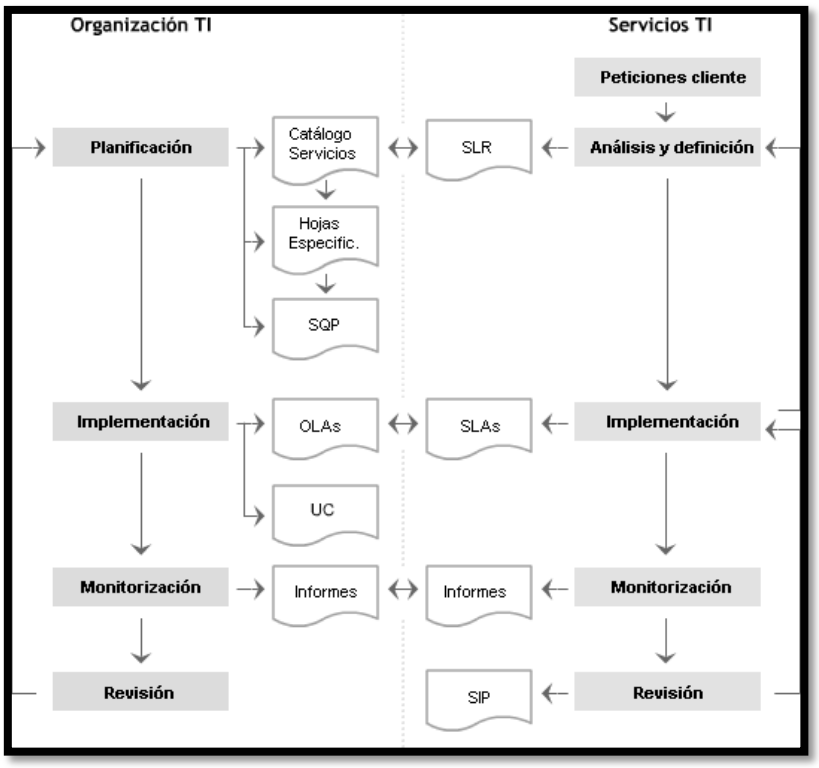

Figura 10-04 Gestión Niveles de Servicio

(OSIATIS)

Conceptos básicos

- **Requisitos de Nivel de Servicio (SLR)**

  Los Requisitos de Nivel de Servicio (SLR) deben recoger información detallada sobre las necesidades del cliente y sus expectativas de rendimiento y nivel de servicios.

  El documento de requisitos de nivel de servicio constituye el elemento base para desarrollar los SLA y posibles acuerdos de nivel de operación correspondientes.

- **Hojas de Especificación**

  Las Hojas de Especificación son, primordialmente, documentos técnicos de ámbito interno que delimitan y precisan los servicios ofrecidos al cliente.

Las Hojas de Especificación deben evaluar los recursos necesarios para ofrecer el servicio requerido con un nivel de calidad suficiente y determinar si es necesario el outsourcing de determinados procesos, sirviendo de documento de base para la elaboración de los acuerdo de nivel de operación y contrato de soporte correspondientes.

- **Plan de Calidad del Servicio (SQP)**

  El Plan de Calidad del Servicio (SQP) debe incorporar toda la información necesaria para posibilitar una gestión eficiente de los niveles de calidad del servicio:

  - Objetivos de cada servicio.
  - Estimación de recursos.
  - Indicadores clave de rendimiento.
  - Procedimientos de monitorización de proveedores.

- **Acuerdo de Nivel de Servicio (SLA)**

  El SLA debe recoger en un lenguaje no técnico, o cuando menos comprensible para el cliente, todos los detalles de los servicios brindados.

  Tras su firma, el SLA debe considerarse el documento de referencia para la relación con el cliente en todo lo que respecta a la provisión de los servicios acordados, por tanto, es imprescindible que contenga claramente definidos los aspectos esenciales del servicio tales como su descripción, disponibilidad, niveles de calidad, tiempos de recuperación, etc.

- **Acuerdo de Nivel de Operación (OLA)**

  El Acuerdo de Nivel de Operación (OLA) es un documento interno de la organización donde se especifican las responsabilidades y compromisos de los diferentes departamentos de la organización TI en la prestación de un determinado servicio.

- **Contrato de Soporte (UC)**

  Un UC es un acuerdo con un proveedor externo para la prestación de servicios no cubiertos por la propia organización TI.

- **Programa de Mejora del Servicio (SIP)**

  El Programa de Mejora del Servicio (SIP) debe recoger tanto medidas correctivas a fallos detectados en los niveles de servicio como propuestas de mejora basadas en el avance de la tecnología.

  El programa de mejora de servicio debe formar parte de la documentación de base para la renovación de los SLA y debe estar internamente a disposición de los gestores de los otros procesos TI.

(OSIATIS)

La gestión de nivel de servicio se organiza en tres actividades primordiales: una enfocada en establecer acuerdos de niveles de servicio con los clientes, otra relacionada a que Tecnología cumpla los compromisos que se estableció en los SLA y, finalmente la que corresponde a la mejora continua del servicio.

El **catálogo del servicio** es el instrumento de relación más importante de Tecnología con sus clientes, ya que en él se recoge el conjunto total de los servicios que la organización de TI provee a sus clientes. El catalogo es una excelente herramienta para que Tecnología cambie su cultura como proveedor de servicios de TI hacia objetivos como:

- Alineamiento con el negocio
- Orientación al cliente
- Calidad de servicio
- Gestión de los servicios

Las características más importantes del catálogo es que constituye el único punto de información sobre la oferta de servicios, de interés tanto para el cliente, como para Tecnología, el catalogo tiene los siguientes propósitos:

- Exponer a los usuarios los servicios existentes de una manera organizada donde se pueden ver las funcionalidades y requisitos de los servicios, esto sirve de base para negociaciones futuras en renovaciones de acuerdos de servicio.
- Organizar los servicios internos de infraestructura por lo general estos no son perceptibles por los usuarios o clientes, pero son necesarios para sustentar cada servicio prestado.
- El catálogo de servicios está enfocado a cualquier cliente que solicite información de los servicios que presta Tecnología.

La estructura que tiene un catálogo de servicios es la siguiente:

1. Definición y objetivos del catálogo de servicios
2. Introducción
3. Categorización de servicios y mapa de servicios
4. Lista y descripción de servicios
5. Glosario
6. Anexos

4.3.2 GESTIÓN DE LA CONTINUIDAD Y DISPONIBILIDAD DEL SERVICIO

Gestión de la Continuidad del Servicio

Para el cumplimiento de esta gestión de acuerdo a las mejores prácticas de la Tecnología de Información se debe cubrir las siguientes fases: Identificación del Riesgo, Valoración del Riesgo, Establecer controles para estos Riesgos y Monitorear el Riesgo y el Cumplimiento de los Controles.

Estos estándares incluyen criterios de control interno de eficacia, eficiencia y cumplimiento, y se los debe revisar y ejecutar en forma permanente e informar sus resultados al Comité de Riesgo Integral verificando que estén alineados a los objetivos de la entidad financiera, el riesgo se presenta debido a desastres naturales u otras fuerzas de causa mayor, evitando consecuencias catastróficas para el negocio.

La estrategia de la Gestión de la Continuidad del Servicio (ITSCM) debe combinar equilibradamente procedimientos:

- Proactivos: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- Reactivos: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

La ITSCM[22] requiere una implicación especial de las personas involucradas, los beneficios sólo se perciben a largo plazo, es costosa y carece de rentabilidad directa. Implementar la ITSCM es como contratar un seguro médico: cuesta dinero, parece inútil mientras uno está sano y desearíamos nunca tener que utilizarlo, pero tarde o temprano nos alegramos de haber sido previsores.

La disponibilidad del servicio

Es un proceso analítico y riguroso de identificación de riesgos que valora y cuantifica la probabilidad de un daño, interrupción de servicio, acceso no autorizado, o mala utilización de la información, producto de una falla de seguridad. Esta valoración es guía para la administración en la toma de decisiones respecto a evaluación de riesgo.

En el marco de establecer una política institucional de seguridad de la información, se ha combinado la utilización de los sistemas, aplicaciones y controles internos para salvaguardar la integridad, autenticidad y confidencialidad de los datos y procesos operativos, esto permite limitar el riesgo en el servicio de ataques internos y externos, así como el riesgo relacionado a la reputación que pueda provenir de brechas de seguridad.

[22] **Gestión de la Continuidad del Servicio**

Los diferentes estados o procesos en los que participan los delegados en mantener la disponibilidad del servicio son:

- **Diseño:** Está a cargo del área de Seguridad de Información en la entidad financiera.
- **Implementación y Ejecución:** Está a cargo del área de Operaciones, Tecnología, Recursos Humanos y Administrativo y Seguridad Corporativa.
- **Hacer cumplir las medidas de seguridad:** Esta función le corresponde a Seguridad de Información a través del monitoreo y a las Jefaturas de las áreas involucradas en su proceso. En forma independiente Auditoría Interna evaluará a través de sus revisiones que las políticas sean adecuadas y que se las cumpla, coordinando con Seguridad de la Información de ser el caso.

"La Gestión de la Disponibilidad es responsable de optimizar y monitorizar los servicios TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo los SLA y todo ello a un coste razonable. La satisfacción del cliente y la rentabilidad de los servicios TI dependen en gran medida de su éxito."

(OSIATIS)

4.3.3 GESTIÓN DE LA CAPACIDAD

La Gestión de la Capacidad tiene como principio que los servicios tengan en todo momento la capacidad necesaria y trabajen con un rendimiento óptimo. Asegurando que el proveedor del servicio (Tecnología), en todo momento, tenga la capacidad suficiente para cubrir la demanda acordada, actual y futura, de las necesidades del negocio.

Entre los beneficios que se tiene con la Gestión de la Capacidad tenemos:

- Conocimiento de la evolución de la actividad del negocio en relación con la utilización de los servicios de TI.

- Gestión adecuada de la capacidad existente, evitando las carencias y también los excesos.
- Un rendimiento óptimo.
- Garantía de que los servicios cumplen con la capacidad requerida en cada momento.
- Ahorro de costes, al tener los recursos ajustados a cada necesidad.
- Prepara el plan de capacidad de Tecnología.
- Predicciones continuas y periódicas basadas en datos de negocios y las que maneja Tecnología.
- Minimiza incidentes por falta de capacidad.

El proceso de gestión de la capacidad debe ser foco de todos los temas relacionados, tanto con la capacidad como con el rendimiento. Las tareas diarias deben realizarse por los recursos técnicos (infraestructura, base de datos, producción, redes, etc…), trabajando en conjunto en las actividades que marca la gestión de la capacidad.

Una correcta gestión en este aspecto reduce las incidencias y degradaciones del servicio por falta de recursos, anticipando las necesidades que pueda tener Tecnología, así trabajar con menos presión y estar innovando constantemente en los servicios prestados.

La gestión de la capacidad enmarca tres ámbitos específicos:

- **La gestión de la capacidad del negocio** – Relacionada a la parte financiera para adquirir y/o cambiar bienes.
- **La gestión de la capacidad de los servicios** – Relacionada a la innovación en los servicios entregados.
- **La gestión de la capacidad de los recursos** – Relacionada netamente al talento humano elaborando una capacitación regular, para que el manejo de los recursos de TI sea el adecuado.

4.3.4 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Es una responsabilidad institucional asumida por la entidad financiera, para lo cual en forma directa o a través del comité de Administración Integral de Riesgos, dará las directrices sobre seguridad de la información, y realizarán las siguientes actividades:

- Revisar y aprobar la política de Seguridad de Información y responsabilidades principales.
- Supervisar y controlar cambios significativos en cuanto a la exposición de los activos de información.
- Revisar los seguimientos de los incidentes en la seguridad de información.
- Aprobar las iniciativas principales para mejorar la seguridad de información.

Por el tamaño y especialización de la actividad, es necesario contar con un Subcomité de Seguridad de la Información, cuyas definiciones se canalizarán a través de la autorizad máxima de Riesgos, siendo miembros permanentes del comité los delegados de Riesgos, Tecnología, Auditoría, Operaciones; Legal, Cumplimiento, Talento Humano y Administrativo (áreas genéricas en una entidad financiera), las demás áreas deberán nombrar un delegado que serán miembros ocasionales de dicho comité. Entre sus principales funciones están:

- Establecer funciones y responsabilidades específicas de seguridad de Información en toda la organización en coordinación con el área de Eficiencia & Productividad de existir.
- Establecer metodologías y procesos específicos para la seguridad de la información, por ejemplo valoración del riesgo y sistema para clasificar la seguridad.
- Establecer y respaldar las iniciativas del área de Seguridad de Información
- Evaluar la adecuación y coordinar la implementación de controles de seguridad de Información específicos para los sistemas o servicios.
- Revisar los incidentes sobre la seguridad de información

- Identificar claramente los activos y procesos de seguridad asociados a cada sistema.
- Nombrar responsables de cada activo o proceso de seguridad y documentar su responsabilidad en coordinación con el área de Eficiencia y Productividad de existir.
- Promover explícitamente el apoyo institucional a la seguridad de información
- Recomendar al Comité de Administración Integral de Riesgos la necesidad cuando se presente, de una asesoría externa especializada en seguridad de Información, la coordinación de la ejecución de esta tarea corresponde al área de Seguridad de Información.

4.4 PROCESOS DE RELACIONES

La gestión de la relación con el negocio permite una mejor alineación continua de TI-Negocio, facilita y formaliza la relación para asegurar que la actividad de TI se enfoca a las necesidades de la entidad financiera.

Establece una disciplina de comunicación que, con un conjunto de documentos, permite mejorar la efectividad de la relación. Los principales medios de formalización que aporta o utiliza este proceso son:

- El catálogo de servicios, que constituye la base para el diálogo.
- Las necesidades del cliente se registran en una hoja de requerimientos del servicio (SLR).
- Se negocia la formación de los compromisos mediante los acuerdos de nivel de servicio (SLA).
- Se mantienen reuniones de seguimiento periódicas del servicio prestado.
- Las quejas del cliente se registran como reclamos.
- Se conoce la opinión del cliente y de los usuarios mediante encuestas y entrevistas.

Beneficios

La gestión de las relaciones con el negocio se asegura de que las actividades llevadas a cabo en la provisión de los servicios contribuyen a los objetivos de negocio del cliente. Entre los beneficios obtenidos destacan:

- Se asegura que el objetivo de TI es la satisfacción del cliente y que éste se mide.
- Saca a TI de su mundo tecnológico para orientarse al negocio.
- Fuerza a TI a trabajar para lo que necesita el negocio.
- Las relaciones con las áreas cliente se gestionan con mayor profesionalidad.
- Los servicios prestados se revisan regularmente con los clientes de TI.
- Se formalizan las reclamaciones.
- Se impulsan acciones de mejora del servicio.

Respondiendo las siguientes inquietudes podrá evaluar que tan fortalecidas se encuentran sus relaciones con la organización:

- ¿Cómo se desempeñan las relaciones entre TI y las áreas de negocio en su organización?
- ¿Cómo se tratan las quejas de los clientes en su empresa?
- ¿Cuál es la frecuencia y contenido principal de las encuestas a las áreas cliente en su organización?

4.5 GESTION DEL PROBLEMA

La misión del proceso de gestión del problema es evitar que se produzcan incidentes repetitivos o nuevos. Este proceso es uno de los más eficaces y que mejores resultados proporciona, pues va buscando y subsanando defectos en los servicios para hacerlos más estables.

Es un proceso de fácil implementación ya que no requiere grandes herramientas, ni la involucraron de todo el personal. Con dos expertos el proceso empieza a dar sus resultados. La gestión del problema se divide principalmente en dos grandes bloques: la gestión reactiva (que comprende el control de problemas y el control de errores) y la gestión proactiva (que busca problemas latentes).

Para conseguir obtener toda la eficiencia del proceso, en sus aspectos reactivos y proactivos, se debe disponer de un proceso de gestión del incidente suficientemente maduro que registre información suficiente para realizar los análisis forenses. El principal resultado de este proceso es la estabilidad de los servicios, con la visibilidad ante el negocio que esto tiene. La reducción de los incidentes produce un efecto positivo en el estrés y carga de trabajo de los equipos de soporte. Además, este proceso es un generador de conocimiento en forma de errores conocidos (que contienen la descripción del problema, la causa raíz y su solución). La gestión del problema no se limita a una mera enumeración de los errores, sino que trabaja en todo el ciclo de vida de la solución, y a lo largo de todo el ciclo de vida del servicio.

Beneficios

Entre las ventajas de adoptar un enfoque formal de gestión del problema se incluyen los siguientes:

- Mejora de la calidad de los servicios de TI. La gestión del problema ayuda a generar un ciclo en el que la calidad de los servicios de TI se incrementa rápidamente.
- Reducción del volumen de incidentes. La gestión del problema contribuyen a reducir el número de incidentes que interrumpen el curso normal del negocio.
- Aporte de soluciones permanentes. Se produce una reducción gradual del número e impacto de problemas y errores, ya que las soluciones son permanentes y no parches provisionales.

- Incremento del conocimiento de la organización. El proceso de gestión del problema genera la base de errores conocidos que permite reutilizar las experiencias previas.
- Mejora del ratio de resoluciones en la primera línea de soporte. El conocimiento generado sobre la resolución de errores permite resolver mayor número de incidentes en la primera línea.

Como una buena práctica se tiene que describir el problema relevante que haya ocurrido en la entidad financiera y sobre él:

- Realizar un diagrama causa-efecto con los errores más frecuentes para un servicio crítico, agrupados según su importancia para el análisis de la causa-raíz.
- En el caso, describir que se hizo mal, que se hizo bien y que cambiaría para que el problema se mitigue.

4.6 PROCESO DE CONTROL

La necesidad de continua evolución de las tecnologías de la información requiere una actividad constante de cambios en las infraestructuras y en los desarrollos para permanecer actualizado y evitar que los servicios se queden obsoletos.

El proceso de gestión del cambio es clave para mantener la estabilidad de los servicios, pues regula y controla toda actuación sobre ellos. El proceso necesita la información de la gestión de la configuración para determinar con precisión el impacto del cambio, y por otra parte, garantiza que la información sobre los servicios modificados permanece actualizada.

El proceso mantiene la fiabilidad de los servicios. Debe velar por que la actividad evolutiva o correctiva de los mismos se realice con un consumo de recursos adecuado, y debe contribuir a la agilidad evolutiva de la organización y al cumplimiento de los plazos de los cambios.

Los principales elementos que intervienen en el proceso son el responsable de cambios, la solicitud de cambio (RFC), el comité de cambio (CAB), la lista de cambios de emergencia y la revisión pos implementación (PIR).

El proceso controla y supervisa tanto la construcción del cambio como su implementación, pero no realiza este trabajo, que lo asumen los equipos técnicos actuando bajo el proceso de la gestión de la entrega.

Beneficios

Los principales beneficios derivados de una correcta gestión del cambio son los siguientes:

- Se reduce el número de incidentes y problemas potencialmente asociados a todo cambio. Por tanto, se reduce el riesgo asociado a los cambios.
- Se reducen los plazos medios en la implantación de los cambios.
- La organización realiza los cambios con más eficiencia
- Se reduce el impacto en el negocio debido a las paradas asociadas a los cambios.
- Se puede retornar a configuraciones estables de manera sencilla y rápida en el caso en el que el cambio tenga un efecto negativo.
- Se reduce el número de operaciones de marcha atrás necesarias.
- Los cambios son mejor aceptados y se evitan "tendencias inmovilistas".
- Se evalúan los verdaderos costes asociados al cambio y, por tanto, es más sencillo valorar el retorno real de la inversión.
- La CMDB y la DSL están correctamente actualizadas, algo imprescindible para la correcta gestión del resto de los procesos de TI.
- Se reducen las actuaciones de emergencia y el trastorno que ocasionan en el trabajo diario.
- Se desarrollan procedimientos de cambio estándar que permiten la rápida actualización de sistemas no críticos.

La creatividad contribuye al cambio realizando estas tareas se la puede incentivar:

- Citar tres ejemplos en su organización de cambios pre-autorizados, de cambios mayores y de cambios de emergencia.
- Por limitación de recursos, escoger solo 3 procesos para implementar en primer lugar. Si uno de ellos es gestión del cambio, ¿Qué otros dos procesos implementaría en su organización?
- ¿Qué aspectos de lo descrito en esta guía no se adaptan bien a su organización? ¿Por qué?

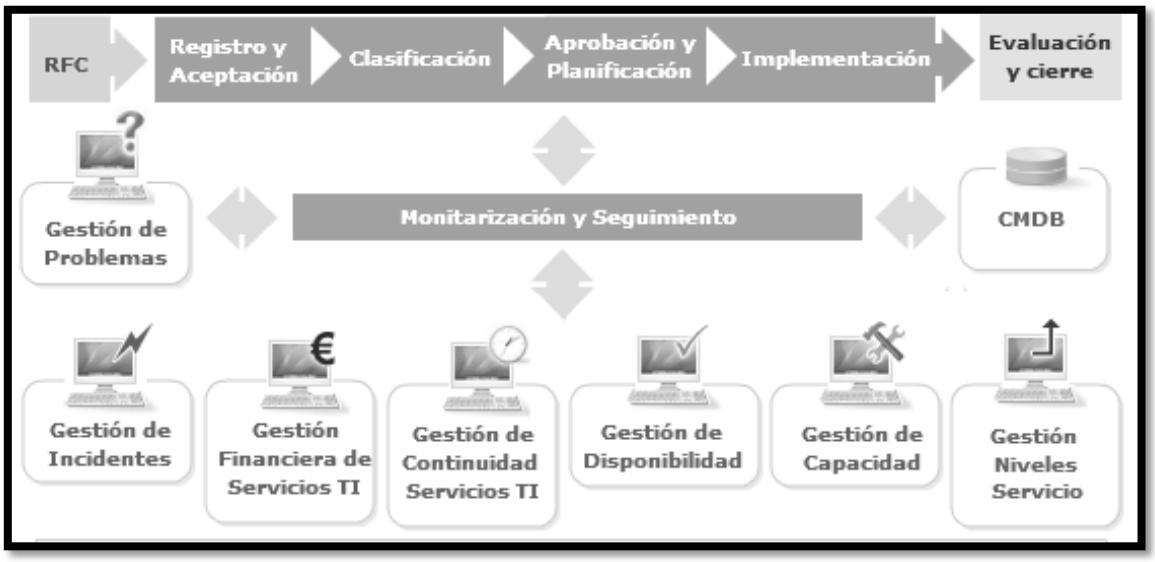

Figura 11-04 Proceso de Control

(OSIATIS)

CAPÍTULO 5. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La guía metodológica fundamenta los procesos de TI expuestos en las normas y marcos de referencia que más se utilizan en el sector financiero, la guía puede servir como fuente de consulta de los profesionales del área de tecnología que deseen optimizar su gestión y busquen asegurar el control interno de los servicios que presta.

2. Los nuevos conocimientos adquiridos en el proceso maestrante contribuyeron a que esta guía se enfoque en ayudar a los profesionales en tecnología en su gestión diaria.

3. La PUCE con esta oferta académica en el área de tecnología está formando profesionales que hoy son cotizados en el entorno laborar y requeridos en empresas que ven en estos recursos una solución para que lideren su visión tecnológica.

4. En lo profesional la guía me ayudó a comprender que existen mejores procesos para la generación de un servicio, este plus en mi gestión se pudo concretar gracias al desarrollo de esta guía.

Recomendaciones

1. En la maestría se tiene que incorporar un módulo internacional para compartir con profesionales de la región las experiencias obtenidas en el transcurso de la etapa curricular.

2. La PUCE tiene que ver su retorno de inversión en incorporar a sus maestrantes titulados para que sean ellos los guías para los nuevos profesionales que asuman este hermoso reto académico.

3. La Guía Metodológica tiene que ser actualizada según aparezcan nuevas innovaciones para la gestión de tecnología.

4. La Superintendencia de Bancos tiene que obligar a todos sus miembros seguir un estándar internacional para la gestión de tecnología, para cumplir esta disposición, se puede usar esta guía metodológica como fuente de consulta.

5. Los profesionales en tecnología o su colegio deben exigir a las entidades de control se sigan normativas que son exitosas en otros países.

ANEXO I. RESUMEN EJECUTIVO GUÍA METODOLÓGICA PARA LA GESTIÓN DEL CONTROL INTERNO

En este anexo se resumen los pasos a seguir para asegurar el control interno en empresas del sector financiero, con un fin didáctico para que su aplicación sea transparente.

1. Planificación e implementación de la gestión del servicio

La implementación de sistemas de gestión del servicio de TI[23] (SGSTI) debe seguir las 4 etapas del ciclo de mejora continua de Deming (PDCA) y estas son:

- **P Plan PLANIFICAR** Planificar la gestión del servicio.
- **D Do HACER** Implementar la gestión del servicio.
- **C Check VERIFICAR** Monitorear, medir y revisar.
- **A Act ACTUAR** Mejora continua**.**

Beneficios

La implantación de la gestión del servicio de TI siguiendo el ciclo PDCA aportara entre otros, los beneficios siguientes:

- Permitirá que todas las actividades de transformación de la organización se lleven a cabo de una forma controlada y organizada.
- Los objetivos se fijan en función de la situación de partida, obtenida mediante una evaluación inicial.
- Los proyectos de implementación tiene unos objetivos fijados.
- Se monitorizan y miden los resultados de los proyectos.
- Se establece un plan de mejora continua.

[23] **Tecnologías de la Información**

- Se aprovecha la experiencia de otras organizaciones que iniciaron antes el camino.

Técnicas asociadas al PDCA

En la parte PLAN se puede estructurar en:

- Descripción del problema:
  - Diagramas de afinidad.
- Recopilación de datos:
  - Matrices.
  - Diagramas de control.
- Análisis de datos:
  - Histogramas.
- Formulación de las causas:
  - Diagramas de causa-efecto.
  - Diagrama de relaciones.
  - Diagramas de flujo.
- Elaboración de hipótesis y comprobación de hipótesis:
  - Histogramas.
  - Nubes de puntos.
- Identificar las causas raíz:
  - Diagramas de causa-efecto.
  - Pareto.
- Propuesta de acciones:
  - Diagrama de árbol.
- Evaluación y selección de acciones:
  - Matrices.
- Identificación de métricas:
  - Diagramas de tendencias.
  - Histogramas.

- Planificación de las acciones:
  - Diagramas de flechas.
  - Diagrama de Gantt.

En la etapa DO se puede realizar:

- Ejecución de las acciones planificadas en la fase de plan.
- Ejecución de las mediciones oportunas para establecer una línea base.
- Ejercer un seguimiento de la ejecución del plan.
- Recopilación de la información necesaria para la toma de decisiones antes de la fase CHECK.

En la etapa CHECK:

- Ejercer un seguimiento de las acciones implementadas.
- Analizar los resultados.
- Evaluación de las mejoras.
- Planificar la estandarización de las mejoras si procede.
- Tener en cuenta la posible resistencia de la organización al cambio.
- Recopilar la información necesaria para tomar la decisión de estandarizar o no.

En la etapa ACT:

- Supone establecer la nueva forma de hacer las cosas que elimina las causas de los problemas que se quería resolver.
- Documentar la nueva manera de hacer las cosas.
- Informar a todas las partes implicadas de los nuevos métodos de trabajo.
- Proporcionar formación sobre la nueva forma de hacer las cosas.
- Establecer los nuevos mecanismos de control para asegurar que la nueva forma de hacer las cosas subsiste en la empresa.

Para afianzar la comprensión de este proceso, se sugiere que responda a las siguientes preguntas:

- ¿Cómo se aplica el ciclo PDCA en su organización?
- ¿Cuál es la secuencia de la implantación de los procesos que más se adecua a su caso particular?
- En función de su experiencia, ¿Qué otras recomendaciones de implementación añadiría al proceso PDCA?

2. Planificación e implementación de nuevos servicios o de servicios modificados

La creación de servicios se ha convertido en un factor clave para lograr el éxito empresarial. El proveedor de TI debe posibilitar un tiempo de entrega de servicios (time-to-market) acorde a las necesidades del cliente, pero también debe contemplar que los costes, la funcionalidad y calidad de los servicios estén ajustados a sus necesidades reales.

Sus responsabilidades principales son las siguientes:

- Responsable de cumplir con lo comprometido con el cliente.
- Controla que el proyecto se constituya cumpliendo con las políticas de TI.
- Hace que otros procesos o áreas realicen lo planificado.

Además, el proceso realiza dos aportaciones fundamentales a la gestión de servicios de TI:

- Organiza todo el ciclo de creación de servicios para que se "fabriquen" en los acordados, con la calidad, costes y funcionalidad pactados.
- Asume la responsabilidad de coordinar a todos los procesos y departamentos de TI para lograr sus objetivos.

Para ello, articula un ciclo de la provisión de servicios que involucra y gestiona todos los procesos, funciones y áreas de TI implicados. Elabora un plan de trabajo integrado para proveer e implantar el servicio a partir del cual se negocia con el cliente.

Una vez que se ha logrado un consenso y acuerdo con el cliente, se aprueba formalmente el plan de proyecto mediante el proceso de gestión del cambio y su órgano de gestión interno, el comité de cambios, en el que están representadas todas las partes implicadas.

Resumen del ciclo de fabricación de un servicio de TI

a. Identificar las necesidades del cliente y proponer servicios TI que satisfagan dichas necesidades.

b. Documentar los requisitos que debe cumplir el servicio solicitado por el cliente. El resultado de esta actividad: Requisitos de nivel de servicio (SLR).

c. Realizar un análisis de viabilidad (si procede).

d. Elaborar las especificaciones técnicas del servicio.

e. Elaborar la propuesta de servicio incluyendo la propuesta de SLA final. Solo se tratan los aspectos de cliente y en términos de negocio.

f. Elaborar el plan de proyecto del servicio con todos los procesos y departamentos TI implicados.

g. Revisión de acuerdos internos (OLA) y externos (UC).

h. Crear RFC y presentar a gestión de cambio para su aprobación, formalización y compromiso de realización de todas las partes implicadas.

i. Inclusión del proyecto en la planificación de cambios (FSC), a partir de la cual se gestiona cualquier cambio, propio o provocado por otros motivos, de forma integrada y normalizada.

j. Control del proceso de fabricación del servicio realizado por cada uno de los intervinientes.

k. Aprobación de la implantación del servicio.

l. Gestión de la entrega del servicio al cliente y revisión pos implantación.

m. Comprobación resultados de la implantación del servicio comparando los resultados reales obtenidos con los planificados.

n. Comunicación de resultados.

o. Cierre de la petición.

Este proceso de planificación e implementación es el punto central sobre el que se sustenta la coordinación dentro del proveedor de servicios TI para la creación y evolución de los servicios a los clientes. Esta actividad la realiza con la colaboración de múltiples intervinientes coordinándolos en la búsqueda de encontrar el equilibrio correcto entre la demanda del cliente, la provisión del servicio, el coste de los mismos y la satisfacción del cliente.

Para finalizar, es importante destacar que este proceso es complejo y soporta múltiples relaciones, por lo que el uso de las herramientas adecuadas es un punto que no se debe descuidar. La disponibilidad de herramientas específicas (catálogo de servicios actualizado, formularios de recolección de requerimientos y especificaciones SLR, modelos de SLA/OLA/UC, un sistema de gestión documental, etc…) pueden ser el elemento clave para el éxito de este proceso y, por tanto, para el éxito de TI en la provisión de servicios nuevos o modificados.

Beneficios

La planificación e implementación de servicios nuevos o de servicios modificados posibilita una mayor confianza en la relación TI-Negocio, y un incremento de la satisfacción de los clientes, gracias a la transparencia y claridad de las propuestas de los servicios que se van a proveer e implantar, ya que están realizadas con el compromiso de todas las partes implicadas y alineadas con las necesidades de negocio planteadas por el cliente.

También contribuyen a mejorar esta relación la fiabilidad que proporciona la planificación integrada de todas las áreas y procesos TI intervinientes que permite asegurar que una petición es viable, que la relación calidad-precio es adecuada, que está alineada con la estrategia de negocio y técnica. También contribuye a agilizar y asegurar el time-to-market de provisión de soluciones, minimizando los riesgos relacionados con el cumplimiento de plazos y costes asociados.

Los principales beneficios que se obtienen al implementar este proceso son:

- Los servicios TI se diseñan para satisfacer las necesidades reales del cliente.
- La relación con el cliente se basa en "servicios" que TI proporciona, y en el lenguaje y términos del negocio.
- Se atienden las demandas del negocio convirtiéndolas en servicios, de acuerdo con la estrategia y los presupuestos.
- La organización de TI y sus clientes tienen unas expectativas claras y consistentes del servicio solicitado a TI.
- Gestión formalizada de los requisitos del cliente, en su propio lenguaje.
- Control del ciclo completo, e integrado, de creación y modificación de los servicios, desde la perspectiva de las necesidades y acuerdos con el cliente, hasta su entrega y puesta en funcionamiento operativo.
- La organización del proveedor de TI tiene una visión integrada de los que el cliente espera de ellos y dirige sus esfuerzos a las áreas y compromisos clave para el negocio.
- Aseguramiento de calidad del servicio acorde a lo estipulado con el cliente.

- Mejora del cumplimiento de los plazos de entrega de servicios, nuevos o evolucionados, al cliente.
- Gestión de los costes del proyecto acordes a lo estipulado con del cliente.
- Controla que el servicio se ha realizado siguiendo las políticas y estándares de la organización TI, lo que facilita su posterior evolución de forma eficiente.

Para afianzar la comprensión del proceso, se sugiere que contestar las siguientes preguntas:

- ¿Cuál es la operativa habitual para la creación de servicios TI en su organización?
- ¿Cómo se validan las propuestas de nuevos servicios?
- ¿Qué mejoras incorporaría al proceso propuesto?

3. Procesos de provisión de servicio

Gestión de nivel de servicio

El proceso de gestión de nivel de servicio es clave para cumplir con las expectativas de los clientes de TI, manteniendo y mejorando la estabilidad de los servicios ya que regula y controla toda la cadena de aseguramiento de los acuerdos de nivel de servicio firmados con los clientes.

El proceso mantiene la calidad y fiabilidad de los servicios, velando, tanto por ella creación de SLA fiables y acordes con las necesidades del negocio, como por el control y mejora reactiva/proactiva que permiten mejorar la calidad de la presentación de los servicios de TI. Este proceso trabaja en estrecha colaboración con los procesos y con las áreas técnicas.

Los principales elementos que componen el proceso son: el responsable del proceso, el catálogo de servicios, los SLA los OLA, los UC y los programas de mejora del servicio (SIP).

Beneficios

La mejora en la calidad y la reducción de las interrupciones del servicio, que aporta una efectiva gestión de nivel de servicio, permite la obtención de ahorros económicos significativos. Por un lado, el cliente puede realizar sus funciones de negocio de forma predecible y minimizar el impacto negativo en sus actividades mediante el cumplimiento de los acuerdos de servicio establecidos y la planificación de paradas de mantenimiento del servicio, y por otro, la organización TI gastara mucho menos tiempo y esfuerzo al tener menos incumplimientos de SLA que resolver.

Entre los beneficios de la gestión de nivel de servicio se pueden destacar:

- La prestación del servicio TI se diseña para satisfacer los requerimientos del servicio de los clientes.
- Permite mejorar las relaciones con los clientes.
- Las dos partes firmantes del SLA tienen una visión clara de sus funciones y responsabilidades, evitando posibles omisiones o malentendidos.
- Se tienen objetivos específicos y acordados, con los que se puede comparar y medir la calidad del servicio; "si no aspira a nada, probablemente eso sea lo que consiga".
- Permite centrar el esfuerzo en TI en los servicios clave para el negocio.
- La monitorización de los servicios facilita la identificación de áreas de debilidad, permitiendo emprender las acciones resolutivas que sean necesarias, mejorando así la calidad de los futuros servicios.
- El seguimiento realizado por este proceso permite identificar fallos en los servicios motivados por acciones de los usuarios, pudiendo definir acciones de mejora, como por ejemplo, la formación.
- La actividad de gestión de nivel de servicio refuerza la gestión y relación con las áreas internas de TI y con los proveedores externos gracias a su integración en la cadena de aseguramiento de los SLA de los clientes, "todos tienen un objetivo en común".

- Los SLA constituyen el elemento básico para poder realizar la facturación de los servicios TI a los clientes según los niveles de servicio requeridos.

Para asegurar una correcta aplicación de la gestión de nivel de servicio se tiene que tener bien claras las respuestas de las siguientes interrogantes:

- ¿Cuál es la estructura del catálogo de servicios de su organización de TI?
- ¿Cuál es la estructura de los SLA de su organización?
- ¿Cómo están estructuradas internamente las unidades o grupos de su departamento de TI de cara a la realización de OLA?

Gestión de la disponibilidad y de la continuidad

Parte de principios muy similares de alineación con las necesidades del negocio y de creación de planes, para posteriormente divergir en dos disciplinas diferenciadas. La primera es la disponibilidad que se convertirá en el astro rey de los servicios. El porcentaje de la disponibilidad será la obsesión de todo responsable. La segunda, la gestión de la continuidad, "juega a los dados" con el azar y el futuro de la empresa, proponiendo a la dirección importantes inversiones para garantizar la supervivencia, e intentando sustraer presupuesto de las actividades operativas.

Una vez implantados los planes, la gestión de la disponibilidad estará continuamente en boca de todos, mientras que la gestión de la continuidad se convertirá en ese profeta que muchas veces predica en el desierto.

La gestión de la disponibilidad tiene por objetivo que se alcancen los máximos niveles de disponibilidad posibles (dentro de las requeridas por el negocio), o por lo menos los niveles pactados siempre moviéndose dentro del ámbito presupuestario asignado, La gestión de la disponibilidad trabaja para alcanzar los siguientes resultados:

- Tasas de disponibilidad y tiempos de respuesta acordes con lo pactado con el negocio y, al menos, que sean similares a las de las empresas de la competencia.
- Definición de las directrices de diseño para la disponibilidad. Diseño de arquitecturas de disponibilidad.
- Tipificación de los servicios en función de su criticidad para el negocio.
- Generación y revisión del plan de disponibilidad.
- Planificación y control de componentes de la infraestructura y de los servicios, para asegurar el cumplimiento de las necesidades de disponibilidad actuales y futuras.
- Análisis de las situaciones de no disponibilidad del servicio, con el fin de identificar mejoras.
- Mejorar la disponibilidad de la infraestructura.
- Controlar que los cambios cumplen con unos niveles de disponibilidad adecuados y fiables.

La gestión de la disponibilidad y la continuidad deben estar presentes desde el momento en que se decide crear un servicio. Para ello, es necesaria una perfecta sintonía tanto con gestión de nivel de servicio, como con el proceso de creación de nuevos servicios o modificación de los existentes.

La gestión de la continuidad de TI se centra en garantizar que, después de una contingencia severa, la empresa seguirá teniendo los servicios que necesita en el plazo acordado. Proporciona los siguientes resultados:

- Identificación de los riesgos que la organización está afrontando, en términos de probabilidad e impacto. La identificación y priorización de los procesos clave de la organización.
- Evaluación del impacto que tendrían las interrupciones en el negocio y fijas los objetivos del negocio en lo referente a los recursos de TI.
- Formulación de la estrategia de continuidad de negocio coherente con los objetivos y prioridades de negocio.

- Realización del plan de continuidad de TI, junto con todos los procedimientos o planes de recuperación asociados.
- Contratación de pólizas de seguros adecuadas para mitigar la exposición a pérdidas económicas.
- Implantación de las contramedidas de reducción del riesgo y de las soluciones de continuidad.
- Personal concienciado y entrenado para actuar en el caso de un desastre.

Beneficios

Los principales beneficios son la obtención de una correcta disponibilidad y tiempo de respuesta de los servicios, y una mejora significativa en la garantía de continuidad de los servicios de TI.

En cuanto a la gestión de la disponibilidad, los beneficios se resumen en:

- El negocio utiliza unos servicios con unos niveles de disponibilidad y tiempo de respuesta adecuados a sus necesidades.
- Los servicios se diseñan sobre una arquitectura planificada para ofrecer la disponibilidad deseada.
- Los cambios se prueban para verificar el cumplimiento de los criterios de disponibilidad.
- Se identifican los incumplimientos y se investiga su causa.
- Los niveles de disponibilidad se monitorizan continuamente y se mejoran donde sea necesario.
- Se detecta la incapacidad de determinados suministradores para satisfacer los requisitos de servicio.
- Se salvan fallos evitables en los servicios.

Los beneficios aportados por la gestión de la continuidad son:

- Se conoce y se tienen acordados, con el negocio, las necesidades de continuidad de los servicios de TI, en función de las necesidades de continuidad de las funciones del negocio.

- Se dispone de un plan de continuidad de TI que aglutina todo lo necesario para definir, implantar y actuar.
- Se analizan las situaciones que pueden poner en peligro la continuidad de los servicios, para identificar acciones que controlen esos riesgos, así como, para identificar acciones de mejora. Se gestionan los riesgos para que la organización pueda seguir funcionando, al menos, al nivel mínimo predeterminado.
- Se reduce el riesgo a un nivel aceptable y se planifica la recuperación de los servicios de TI. Por tanto, se puede esperar una reducción de la prima de seguros, una mejora de la imagen de la empresa, etc.
- Las soluciones de replicación remota, consolidación y virtualización, que muchas veces son necesarias, aportan mejoras en la robustez de las infraestructuras y ahorros en la gestión de una planta más uniforme.

Las siguientes preguntas tienen que ser contestadas para saber que se está haciendo una adecuada gestión de la continuidad:

- ¿Cuáles con los principales riesgos a los que está expuesto los servicios de TI en su organización?
- ¿Cuáles son las funciones vitales en su negocio?
- ¿Qué impacto tendría en su negocio una indisponibilidad de una hora de los servicios de TI más críticos (bien por falla interna o por desastre)?

Gestión de la capacidad

La gestión de la capacidad es un proceso que comprende un amplio abanico de especialidades diferentes, desde el entendimiento de la evolución del negocio, hasta las funciones más técnicas de ajuste de las aplicaciones y de las plataformas para conseguir un rendimiento óptimo.

El proceso se revitaliza con la realización del plan de capacidad y sus revisiones periódicas, lo que le obliga a estar al tanto de las tendencias del negocio y sus variaciones en la utilización de los servicios, estar al día de la evolución tecnológica y de la situación económica de la empresa.

La gestión de la capacidad se estructura en tres subprocesos o áreas actividad:

- *La gestión de la capacidad del negocio*: que traslada las necesidades y planes del negocio en requisitos para los servicios y las infraestructuras, con el fin de asegurar que los futuros requerimientos del negocio se puedan cumplir.
- *La gestión de la capacidad de los servicios*: está centrado en la gestión, control y predicción del rendimiento extremo a extremo de los servicios para cumplimiento de los requisitos del servicio y los acuerdos pactados de nivel de servicio.
- *La gestión de la capacidad de los recursos*: cuyo objetivo es la gestión y el control de los recursos de TI, y especialmente de los más esenciales para que presten el mejor rendimiento posible.

En estas tres áreas se realizan el siguiente conjunto de actividades:

- La elaboración del plan de capacidad, que sincroniza a toda la organización en las previsiones de recursos necesarios para satisfacer la evolución de las demandas del negocio.
- El ciclo de mejora de la capacidad y rendimiento garantiza que se están revisando estos parámetros de forma continua. Se inicia en la monitorización, sigue con el análisis de los datos, para identificar las necesidades de ajuste de aplicaciones y de infraestructuras, para realizar posteriormente la implementación de las mejoras a través del proceso de cambios.
- Influir en la utilización de los servicios y consumo de recursos es otra de las facetas que desarrolla el proceso. Despliega las condiciones (comunicación, facturación, etc.) para que el uso transcurra por la senda prevista.

- Se realiza el modelado de los servicios, con el fin de tener una previsión de su comportamiento en situaciones de carga pico.
- El dimensionado de aplicaciones en las fases tempranas de su concepción, permitirá anticipar las necesidades de infraestructuras.
- Realiza los informes de capacidad y rendimiento de los servicios y los recursos.
- Crea y administra la base de datos de capacidad (CDB), que centraliza la información de monitorización de la capacidad y del rendimiento.
- Como en el resto de los procesos, se supervisa a sí mismo y se mejora.
- El proceso de gestión de la capacidad es el proceso "tacaño" por excelencia, velando por la optimización y evitando derroches. Por ello, año tras año, se irá viendo como la gestión de la capacidad va cobrando mayor relevancia en un mundo que requiere ajustar al máximo el consumo de recursos materiales y energéticos.

Beneficios

La gestión de la capacidad es un proceso de previsión que permite anticipar las necesidades y gestionar la dotación de fondos para conseguirlos. Por tanto, tiene una vertiente importante en la planificación económica.

También lucha contra el despilfarro en la compra o utilización de los recursos, ajustando la demanda a las infraestructuras necesarias. En su faceta técnica pura, se centra en conseguir un rendimiento óptimo de los servicios, realizando el ajuste fino de las aplicaciones y de las plataformas.

Los principales beneficios esperados con la implantación de este proceso son los siguientes:

- Se conocen anticipadamente las necesidades de recursos.
- Se pueden agrupar y racionalizar las compras
- El dialogo con el negocio permite identificar los perfiles de utilización de los servicios y reconducir el consumo que se hace de ellos por parte de los usuarios.

- Se controlan los gastos imprevistos por nuevos proyectos o por necesidades de compras urgentes.
- La optimización de recursos, la revisión de la utilización de licencias, la gestión de la obsolescencia del parte de equipamiento y la retirada de recursos no utilizados, pueden generar importantes ahorros.
- La mejora del rendimiento y la optimización es una garantía para la estabilidad de los servicios y la utilización óptima de los recursos.
- La monitorización permitirá seguir el consumo de capacidad (por ejemplo, el consumo energético) y el rendimiento.
- El ciclo de mejora de la capacidad asegura que las instalaciones están siendo revisadas y mejoradas continuamente.

Por tanto, el proceso de gestión de la capacidad aporta predicción en las necesidades, con los beneficios que trae consigo la anticipación.

Es un proceso de ajuste corrección de los excesos, tanto en el uso como en la dotación de equipamiento. Además, es un proceso técnico en el que se afina el funcionamiento de la maquinaria de TI. Aportará un mejor control de los costes en las plataformas y una mayor estabilidad en las mismas.

Cuando conteste estas interrogantes se dará cuenta si su gestión de capacidad en la adecuada:

- ¿Cuál es el contenido del plan de capacidad de su organización?
- ¿Cómo se realizan las pruebas de rendimiento de las aplicaciones?
- Cite las dos mejores prácticas de su entidad financiera relativas al proceso de capacidad.

Gestión de la seguridad de la información

El incremento continuo de las amenazas hace que la seguridad de la información sea cada vez un aspecto más crítico en las empresas. La red Internet es el cauce por el que llegan la mayoría de ellas. Si las amenazas han aumentado por esta vía, las vulnerabilidades también: la conectividad desde cualquier lugar, la proliferación de aparatos tecnológicos en el mercado de consumo en la empresa, la gran capacidad de los dispositivos móviles en la empresa, etc.

La seguridad se ha convertido en los cimientos sobre los que se sustenta la información de la empresa, cimientos que hay que cuidar continuamente para que no pierdan su solidez.

El marco normativo internacional pone foco en la gestión de la seguridad aportando un conjunto de requisitos y buenas prácticas que ayudan a las empresas a enfocar su implantación. Resulta esencial utilizar la normativa existente. ISO 27001 aporta un conjunto de actividades y buenos controles para mejorar la seguridad, mientras que la ISO 20000 integra la gestión de la seguridad con el resto de los procesos de gestión de TI.

La implementación de la gestión de la seguridad de TI se articula en torno a un proceso específico, que permite controlar la seguridad en la empresa y sus riesgos asociados. Este proceso gestiona el mantenimiento de unos niveles de seguridad adecuados, tanto en la presentación de los servicios de TI, como para el control de los activos de información de la organización.

Los principales elementos de la gestión de la seguridad son:

- La política de seguridad.
- El responsable de seguridad.
- El comité de seguridad.
- La evaluación de riesgos.
- Los objetivos de control y los controles.
- La declaración de riesgos o declaración de aplicabilidad.
- El plan de tratamiento de riesgos.

- La gestión de incidentes de seguridad.
- Los registros de seguridad.

Beneficios

Entre los beneficios más relevantes que proporciona la gestión de la seguridad de la información destacan los siguientes:

- Protege y aumenta la robustez y seguridad de los sistemas de información, realizando un tratamiento adecuado de los riesgos, reduciendo el riesgo de sustracción o perdida de información esencial.
- Proporciona confianza a todas las partes. A la dirección porque sus activos están mejor protegidos, al mercado porque son más robustos los sistemas, y al departamento de TI porque le permite cumplir las exigencias de la dirección.
- Asegura que los incidentes de seguridad de la información son correctamente gestionados, reduciendo su impacto en el negocio.
- Establece auditorias de seguridad con regularidad, que comprueban la adecuación de las medidas de seguridad implantadas.
- Aporta información a la dirección sobre el estado de seguridad de la empresa u organización, de cara a adoptar las medidas que se consideren oportunas.
- Fortalecimiento de la imagen ante el mercado y confianza de los clientes en una organización que apuesta por la seguridad de la Información.
- Ahorro de costes por evitar incidentes de seguridad, en primas de seguros, por sanciones derivadas de incumplimientos legales, etc.

Las siguientes inquietudes nacen cuando se piensa en evaluar la gestión de la seguridad de la información:

- ¿Cómo se realiza la gestión de la seguridad de la información en su empresa?
- ¿Está la dirección de su empresa implicada en la gestión de la seguridad de la información?

- ¿La gestión de la seguridad se trata en su organización como un ámbito independiente o de forma integrada con los otros procesos de gestión de los servicios de TI?

4. Procesos de relaciones

La gestión de la relación con el negocio permite una mejor alineación continua de TI-Negocio, facilita y formaliza la relación para asegurar que la actividad de TI se enfoca a las necesidades de la empresa.

5. Gestión del Problema

La misión del proceso de gestión del problema es evitar que se produzcan incidentes repetitivos o nuevos. Este proceso es uno de los más eficaces y que mejores resultados proporciona, pues va buscando y subsanando defectos en los servicios para hacerlos más estables.

Es un proceso de fácil implementación ya que no requiere grandes herramientas, ni la involucraron de todo el personal. Con dos expertos el proceso empieza a dar sus resultados. La gestión del problema se divide principalmente en dos grandes bloques: la gestión reactiva (que comprende el control de problemas y el control de errores) y la gestión proactiva (que busca problemas latentes).

6. Proceso de control

La necesidad de continua evolución de las tecnologías de la información requiere una actividad constante de cambios en las infraestructuras y en los desarrollos para permanecer actualizado y evitar que los servicios se queden obsoletos.

El proceso de gestión del cambio es clave para mantener la estabilidad de los servicios, pues regula y controla toda actuación sobre ellos.

El proceso necesita la información de la gestión de la configuración para determinar con precisión el impacto del cambio, y por otra parte, garantiza que la información sobre los servicios modificados permanece actualizada.

El proceso mantiene la fiabilidad de los servicios. Debe velar por que la actividad evolutiva o correctiva de los mismos se realice con un consumo de recursos adecuado, y debe contribuir a la agilidad evolutiva de la organización y al cumplimiento de los plazos de los cambios.

BIBLIOGRAFÍA Y REFERENCIAS

BORRMART. (s.f.). Obtenido de http://www.borrmart.es/articulo_redseguridad.php?id=2078

BURODEANALISIS. (s.f.). Obtenido de http://www.burodeanalisis.com/2011/08/08/robos-electronicos-alertan-sobre-fragilidad-en-ecuador/

COSO. (s.f.). Obtenido de http://www.coso.org

DLP. (s.f.). Obtenido de http://m.b5z.net/i/u/6113204/f/Est%20DLP/Presentacion_DLP.pdf

GOBERNABILIDAD. (s.f.). Obtenido de http://www.gobernabilidad.cl/documentos/martinez.pps

GRUPOBANCOLOMBIA. (s.f.). Obtenido de http://www.grupobancolombia.com/webCorporativa/gobierno/pdf/informeSistemaControlInterno.pdf

GRUPOBANCOLOMBIA. (s.f.). Obtenido de http://www.grupobancolombia.com/webCorporativa/gobierno/buenGobierno/sistemaControlInterno.asp

IDG. (s.f.). Obtenido de http://www.idg.es/iworld/articulo.asp?id=152376

ISACA. (s.f.). Obtenido de http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

ISACAMTY. (s.f.). Obtenido de http://www.isacamty.org.mx/archivo/Evento%20Anual%202010.pdf

KASPERSKY. (s.f.). Obtenido de http://latam.kaspersky.com/sobre-kaspersky/centro-de-prensa/blog-de-kaspersky/troyanos-brasil

Mantilla, S. (2013). [D]. *Auditoría del control interno*. Colombia: ECOE EDICIONES.

NETWORKWORLD. (s.f.). Obtenido de http://www.networkworld.es/Prevencion-de-intrusiones_Como-desplegar-sistemas-IPS/seccion-/articulo-190083

OSIATIS. (s.f.). Obtenido de http://itil.osiatis.es/

PCI DSS. (s.f.). Obtenido de http://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/pci_dss_v2-0.pdF

REPOSITORIO UASB. (s.f.). Obtenido de http://repositorio.uasb.edu.ec/bitstream/10644/2415/1/T0358-MBA-Silva-An%C3%A1lisis.pdf

REVISTAVANGUARDIA. (s.f.). Obtenido de http://www.revistavanguardia.com/index.php?option=com_content&view=article&id=204&Itemid=216

SBS. (s.f.). Obtenido de http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=7&vp_tip=2

SCRIBD. (s.f.). Obtenido de http://es.scribd.com/doc/39934738/Metodos-y-tecnicas-para-la evaluaciondecontrol-interno

Telefónica. (2010). [B]. *Guía completa de aplicación para la gestión de los servicios de tecnologías de la información*. España: AENOR.

Torres, G. (2013). [A]. *Desarrollo de una guía metodológica para la gestión de tecnología que asegure el control interno en empresas del sector financiero*. Ecuador: PUCE.

Torres, G., & Villegas, F. (2008). [C]. *Evaluación y Auditoria del Sistema de Información de la Escuela Politécnica del Ejército: Dominio, Evaluación y Monitoreo*. Ecuador: ESPE.

UNAP. (s.f.). Obtenido de http://www.unap.cl/~setcheve/cobit/CobiT-106_1.gif