ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMÁTICA

III PROMOCIÓN

PROYECTO

TEMA

"AUDITORÍA AL DESARROLLO DE APLICACIONES DE UNA ENTIDAD FINANCIERA "

AUTORES

Ing. Leonor Quinchango C.

AÑO

2011

AGRADECIMIENTO

A Dios, a mis padres que desde cielo me bendicen y a la empresa donde me permitieron realizar este trabajo.

Contenido

Tablas y Gráficos

Tablas

CAPITULO I

1. INTRODUCCION

En la Actualidad los Sistemas Informáticos constituyen una herramienta bastante poderosa para la mejora de rendimiento de toda organización empresarial. Por tal motivo el uso adecuado de una metodología para el desarrollo de aplicaciones, especifica qué es lo que se debe construir, permite dirigir y planear las tareas de lo que se desarrolla, como también proporciona criterios para hacer seguimiento y medir productos y actividades. Adicionalmente simplifica el mantenimiento de la aplicación, el control de la calidad del producto, y la reutilización de componentes de software.

En consideración a los requerimientos de tecnologías de la información y a la necesidad de racionalizar y optimizar el uso de los recursos, se aprovechó esta necesidad y se planteó realizar un estudio mediante una auditoria al desarrollo de las aplicaciones que mantiene la organización, por tal motivo este documento es el resultado de un análisis y evaluación de los métodos y proceso común para el desarrollo de aplicaciones, junto con los marcos de trabajo y normas básicas de documentación que deben aplicarse. Durante la ejecución de las actividades relacionadas con el desarrollo de software en su ciclo de vida completo se utilizó metodologías y normas expuestas para la evaluación de las etapas del ciclo de desarrollo de los proyectos de software.

1.1 Objetivo

La Auditoría Informática, es un punto clave en este documento, debido a que, si bien es cierto, ayuda a detectar errores y señalar fallas en determinadas áreas o procesos, su objetivo está orientado a revisar y evaluar los métodos y procedimientos usados para el desarrollo de aplicaciones y su ciclo de vida de la organización con el objetivo de lograr una utilización de recursos y metodologías más eficientes que servirá para una adecuada toma de decisiones.

1.2 Alcance

La auditoría realizada comprende al periodo del primer semestre del presente año, aplicada a la Empresa Financiera Credicard S.A en la División de Tecnología y Desarrollo – Departamento de Desarrollo. El alcance de esta auditoría abarca:

- Revisión de Procedimientos, organización de archivos, estándares de programación, controles, utilización de los sistemas, gestión de proyectos
- Evaluación de avance, control de cambios.
- Evaluación de la etapa del desarrollo y prueba de la aplicación.
- Control de procesos y ejecuciones de programas críticos.
- Satisfacción de usuarios

CAPITULO 2

2. ENFOQUE A UTILIZAR

2.1 Marco Conceptual

Hace casi 500 años, Maquiavelo dijo: ... no hay nada más difícil de llevar a cabo, más peligroso de realizar o de éxito más incierto que tomar el liderazgo en la introducción de un nuevo orden de cosas». Durante los Últimos 50 años, los sistemas basados en computadora han introducido un nuevo orden. Aunque la tecnología ha conseguido grandes avances desde que habló Maquiavelo, sus palabras siguen sonando a verdad.

Las compañías destinan con frecuencia, significativos recursos de tecnología de información (personas, aplicaciones, instalaciones, tecnologías, etc.) para el desarrollo, adquisición y mantenimiento de sistemas de aplicaciones que son críticos para el funcionamiento efectivo de los procesos clave del negocio. Estos sistemas a la vez controlan a menudo activos de información críticos y deben ser considerados un activo que necesita ser administrado y controlado de manera efectiva. Los procesos de TI, para gestionar/ administrar y controlar estos recursos de TI, y otras actividades semejantes, son parte de un proceso del ciclo de vida, con etapas definidas aplicables al desarrollo, implementación, mantenimiento y eliminación de las aplicaciones del negocio. El proceso de implementación para aplicaciones de negocios, comúnmente conocido como un SDLC[1], empieza

[1]SDLC: System Development life cycle

cuando una aplicación individual es iniciada como un resultado de una o más de las situaciones siguientes:

- ✓ Una nueva oportunidad que se relaciona con un proceso de negocio nuevo o ya existente
- ✓ Un problema que se relaciona con un proceso existente de negocio
- ✓ Una nueva oportunidad que permitirá a la organización obtener ventajas de la tecnología
- ✓ Un problema con la tecnología existente.

Todas estas situaciones están estrechamente vinculadas con impulsores clave de negocio. Los impulsores clave de negocio, en este contexto, pueden definirse como los atributos de una función de negocios que impulsan y la implementación de esta función de negocio, para alcanzar las metas estratégicas de negocio de la compañía.

Las aplicaciones de negocio, deben iniciarse usando procedimientos o actividades bien definidos como parte de un proceso definido para comunicar las necesidades de negocio a la gerencia. Estos procedimientos a menudo requieren, documentación detallada que identifique la necesidad o el problema, que especifique la solución que se desea y que relacione los beneficios potenciales para la organización. Se deben identificar todos los factores internos y externos afectados por el problema y su impacto en la corporación.

Un riesgo de cualquier proyecto de desarrollo de software es el hecho de que el resultado final no cumpla con todos los requerimientos, Algunos problemas de traducción surgen cuando se definen inicialmente lo requerimientos para los productos

provisiones. El ***modelo cascada*** (Waterfall) y las variantes del modelo, por lo general implican un enfoque de verificación del ciclo de vida que segura que los errores potenciales sean corregidos lo antes posible y no hasta la prueba final de aceptación. El modelo de verificación y validación, llamado a veces ***el modelo V***, también hace énfasis en la relación entre las etapas del desarrollo y los niveles de prueba (Figura 1). La prueba más granular, ocurre inmediatamente después de que los programas han sido escritos. Siguiendo este modelo, la prueba se realizad para validar el diseño detallado. La prueba del sistema se relaciona con la especificación arquitectónica del sistema, mientras que la prueba de aceptación del usuario final se refiere a los requerimientos.

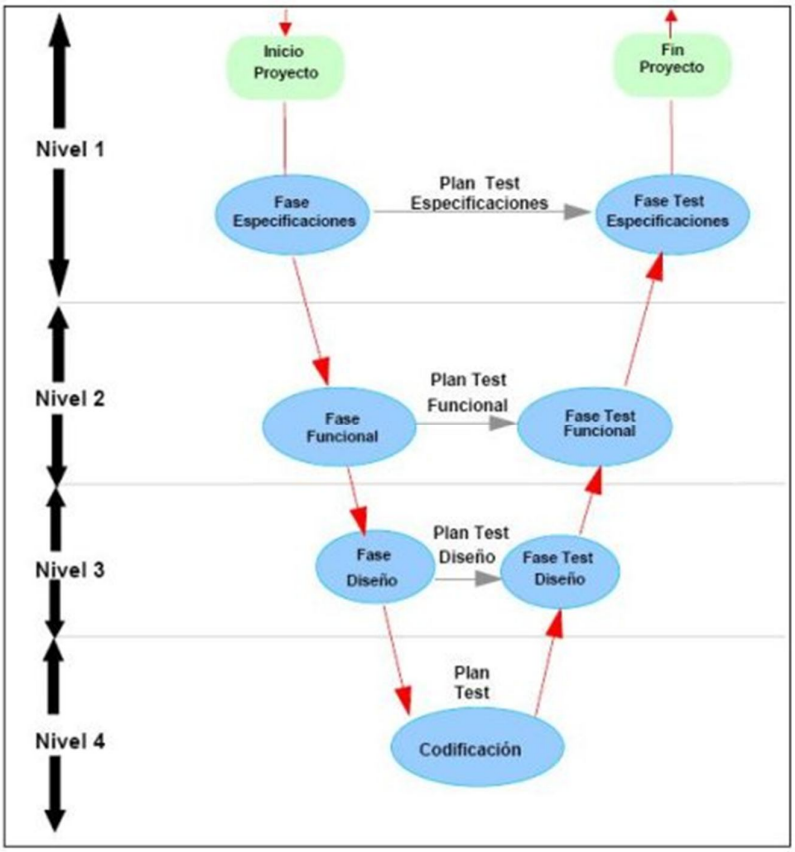


Grafico #1: Modelo V

Cualquier sistema de aplicación de negocio desarrollado, caerá en alguna de las siguientes categorías: centrada en la organización (Sistema de información Gerencial [Management Information System – MIS]. ERP, gestión de relaciones con clientes [Customer Relashionship Management - CRM], gestión de la cadena de suministros [SCM], etc.)y centrada en el usuario final. Las aplicaciones orientadas/centradas de la organización continúan utilizando el método tradicional SDLC, mientras las aplicaciones orientadas/centradas en el usuario final utilizan métodos alternos de desarrollo. El objetivo de una aplicación orientada a la organización es recolectar, integrar, almacenar, archivar y compartir información a los usuarios del negocio y diversas funciones aplicables de soporte con base a la necesidad de saber. De ese modo, los datos de venta están disponibles para los contadores, la administración, los departamentos de pago de impuestos, etc. El cumplimiento de obligaciones tributarias (pago de impuestos) es resuelto a través del uso de aplicaciones orientadas a la organización. El objetivo de una aplicación centrada en el usuario final, es proveer diferentes vistas de los datos para la optimización de su desempeño. Esto incluye técnicas de DSS y sistemas geográficos de información (GIS), etc. La mayoría de estas aplicaciones son desarrolladas usando métodos alternos de desarrollo.

Un objetivo de décadas ha sido el encontrar procesos y metodologías, que sean sistemáticas, predecibles y repetibles, a fin de mejorar la productividad en el desarrollo y la calidad del producto software. La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones, determinando así las etapas del desarrollo de un sistemas.

A través de los años, el desarrollo de una aplicación de negocio se ha realizado en gran medida, por medio del uso de las etapas tradicionales del ciclo de vida del desarrollo de sistemas (SDLC), también referido como la técnica de cascada, este enfoque del ciclo de vida es el más antiguo y el más ampliamente utilizado para desarrollar aplicaciones del negocio. Este enfoque se basa en un enfoque secuencial y sistemático de desarrollo de software (en gran medida de aplicaciones de negocio) que comienza con un estudio de factibilidad y continúa con la definición de los requerimientos, el diseño, desarrollo e implementación. Esta serie de pasos o de etapas tienen definidas metas y actividades, responsabilidades, resultados esperados y fechas de cumplimiento.

Este enfoque funciona mejor cuando se estima que los requerimientos de un proyecto serán estables y bien definidos. Esto facilita la determinación de la arquitectura de un sistema de manera relativamente anticipada durante la actividad de desarrollo. Otro tipo de enfoque de desarrollo de software es el enfoque iterativo, según el cual los requerimientos del negocio se desarrollan y prueban en iteraciones hasta que toda la aplicación sea diseñada, construida y probada. Este enfoque es útil en aplicaciones WEB en las cuales los prototipos de pantallas son necesarios para ayudar a complementar los requerimientos y el diseño.

2.2 Justificación

Aunque cualquier departamento o área de una organización es susceptible de ser auditado, hay una serie de circunstancias que

hacen especialmente importante al área de desarrollo, y por tanto también de auditoría, frente a otras funciones o áreas dentro del departamento de informática:

- ✓ Los avances en tecnologías de las computadoras han hecho que actualmente el desafío más importante y el principal reto sea la ***calidad del software***.

- ✓ El gasto destinado a software es cada vez superior al que se dedica al hardware.

- ✓ El software como producto es muy difícil de validar. Un mayor control en el proceso de desarrollo incrementa la calidad del mismo y disminuye los costos de mantenimiento.

- ✓ El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual denota la inexistencia o mal funcionamiento de los controles en este proceso.

- ✓ Las aplicaciones informáticas, que son el producto principal obtenido al final del desarrollo, pasan a ser la herramienta de trabajo principal de las áreas informatizadas, convirtiéndose en un factor esencial para la gestión y la toma de decisiones.

En 1998, los datos de la industria del software indicaron que el 26% de proyectos de software fallaron completamente y que el 46% experimentaron un desbordamiento en la planificación
Y en el coste. Aunque la proporción de éxito para los proyectos de software ha mejorado un poco, nuestra proporción de fracaso de proyecto permanece más alto del que debería ser.

En 2006 del total de los proyectos de TI monitoreados, **sólo el 29%** lo logró a tiempo y en costo, los costos promedio se **excedieron 56%** y en promedio tomó **84% más de tiempo** para completarse[2].

Considerando la realidad de los proyectos según los estudios se ha determinado:

- 15% de los proyectos fracasan y son cancelados totalmente
- 51% no cumplen sus objetivos
- 42% en promedio por encima del presupuesto
- 82% no cumplen el cronograma
- US $55.000 millones perdidos en proyectos sólo en USA
- US $17.000 millones en sobrecostos

Las circunstancias por la que los proyectos en el desarrollo de sistemas fracasan:

- Falta de comprensión del problema, visión ligera del alcance
- Problemas tecnológicos y con proveedores
- Problemas de comunicación y trabajo en equipo
- Problemas de liderazgo
- Problemas metodológicos. Falta de un proceso de administración de proyectos.

La auditoría en su revisión del ciclo de vida del desarrollo de Aplicaciones, adquisición o mantenimiento, es:

- ✓ identificar, analizar y evaluar, requerimientos del usuario, riesgos, exposiciones a ellos y los controles en aplicaciones

[2] Fuente: Over due and over budget, over and over again" The Economist, june 11th 2007

específicas durante la fase de desarrollo, adquisición o mantenimiento de las aplicaciones.

- ✓ Determinar los componentes, objetivos y requerimientos principales de los usuarios de la aplicación e identificar las áreas que exigen controles al hacer entrevistas con miembros claves del proyecto.
- ✓ Determinar y clasificar los principales riesgos y exposición a riesgos de la aplicación, para permitir controles por medio de discusiones con miembros del equipo del proyecto.

- ✓ Identificar los controles para minimizar los riesgos y exposiciones a riesgos de la aplicación por referencia a fuentes confiables y por medio de discusiones con miembros del equipo del proyecto.

- ✓ Asesorar al equipo del proyecto respecto del diseño de la aplicación y la implantación de controles al evaluar los controles disponibles y al participar en discusiones con miembros del equipo del proyecto.

- ✓ Monitorear el proceso de desarrollo, mantenimiento o adquisición de las aplicaciones para asegurarse de que se implantan los controles, se satisfacen los requerimientos de los usuarios y se sigue la metodología más adecuada en cada caso, esto permite asegurarse que las aplicaciones son eficaces y eficientes, al realizar reuniones periódicas con miembros del equipo del proyecto y al hacer exámenes de la documentación y los productos en sus diversas etapas.

2.3 Aspectos Metodológicos

Los aspectos metodológicos aplicados en esta auditoría se lo realizó en base a las guías de aplicaciones de ITAF de ISACA y el marco de trabajo COBIT Versión 4.1.

A continuación encontraremos la descripción de dichas metodologías:

2.3.1Guía de aplicaciones de ITAF de ISACA

ITAF se centra en el material de ISACA, así como los contenidos y orientaciones elaboradas por la IT Governance Institute ® (ITGITM) y otras organizaciones, y, como tal, proporciona una fuente única a través del cual los profesionales de auditoría pueden buscar la guía, las políticas de investigación y los procedimientos, obtener evidencia de auditoría y los programas de garantía, y elaborar informes eficaces.

- ✓ Proporciona una guía sobre la auditoría de diseño, realización e informes de las TI y las asignaciones de seguridad.
- ✓ Define los términos y conceptos propios de TI la garantía.
- ✓ Establece las normas que se ocupan de las funciones de TI de auditoría y profesionales y responsabilidades, conocimientos y habilidades, y la diligencia, la realización y los requisitos de información.

Organización del Marco de Aseguramiento de TI

ITAF se compone de los elementos, como se muestra en la gráfico 2. Estos incluyen tres categorías de normas generales, el rendimiento y la presentación de informes, así como las directrices y herramientas y técnicas:

- **Estándares Generales.**-Son las guías sobre los principios con el que TI garantice un operador profesional. Se aplican a la conducta de todas las tareas, y frente a la Auditoría de TI y la garantiza la ética, objetividad así como los conocimientos, competencias y habilidades.
- **Estándares de Desempeño:** De acuerdo con la realización de la tarea, tales como planificación y supervisión, determinación del alcance, riesgo y materialidad, la movilización de recursos, evidencia de la supervisión y gestión de asignaciones, de auditoría y aseguramiento, y la del ejercicio de su juicio profesional y el debido cuidado. Normas Internacionales de Información Dirección de los tipos de informes, medios de comunicación y la información comunicada.
- **Guía:** Proporcionar al auditor de TI, dirección durante la ejecución de la auditoría, con tres categorías, las normas, directrices se centran en los diferentes enfoques de auditoría, metodologías, herramientas y técnicas, y materiales relacionados para ayudar en la planificación, ejecución, evaluación, pruebas e informes en los procesos de TI, controles. Estas directrices también ayudan a aclarar la relación entre actividades empresariales, y las realizadas por IT.

➢ **Herramientas y Técnicas:** Proporciona información específica sobre las diversas metodologías, herramientas y plantillas, y proporciona una dirección en su aplicación y utilización de poner en práctica la información contenida.

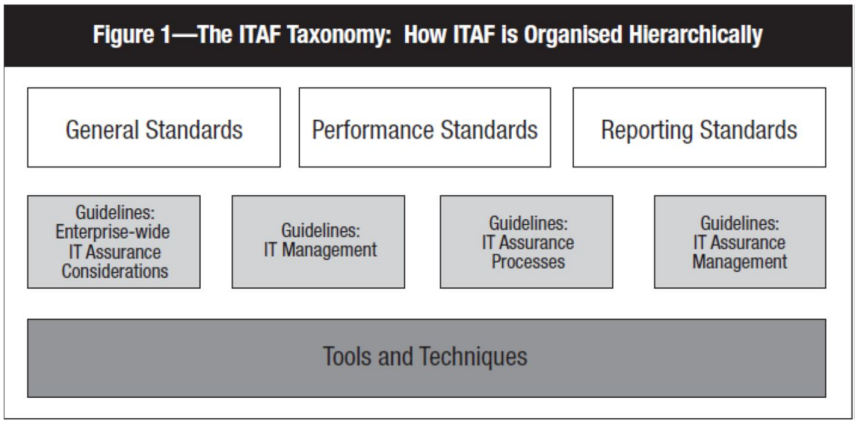


Grafico # 2 ITAF

Auditoria y Aseguramiento de Procesos.

Esta sección enfoca la auditoría mediante metodologías y técnicas. Proporciona al auditor de TI información sobre las prácticas comunes, problemas, preocupaciones y dificultades con el empleo de diversos procedimientos de auditoría y aseguramiento, una orientación sobre cómo planificar y llevar a cabo la actividad para asegurar el éxito. El auditor de TI debe reconocer y valorar el papel de TI en la empresa, y las relaciones que existen entre los departamentos de TI y las operaciones empresariales y de gestión.

La siguiente tabla representa un desglose de la sección 3600. Se identifican posibles áreas para el desarrollo de directrices de ISACA, proporciona información sobre el alcance y el contenido de la guía, y la lista de los recursos existentes relevantes de ISACA y algunas técnicas ilustrativas a considerar.

3600 – IT Auditoria y Aseguramiento de Procesos. (Cont.)	
IT Procesos	**ISACA Recursos**
3657|**Auditoría de estrategias alternativas de desarrollo de software**	
En esta sección se presenta la auditoría de TI y seguridad profesionales a las estrategias de desarrollo diferente y no tradicional de software. A la vista de la creciente complejidad de sistemas, desarrolladores de software han creado estrategias alternativas para reducir el desarrollo y mantenimiento tiempo y costes, y mejorar la calidad del software producido. Estas nuevas técnicas pueden complementar, modificar o sustituir los procesos tradicionales de SDLC. La introducción de portales, servicios web, software orientado a servicios, Unified Modeling Language (UML), etc, son factores clave en la necesidad de adoptar nuevas los controles internos. Esta guía presenta diversas estrategias y las direcciones de su adecuada utilización, fortalezas y debilidades, y las consideraciones especiales de auditoría. También se ofrece una comparación con las estrategias más tradicionales.	• **G14** Revisión a los Sistemas de Aplicación. • **G23** Sistema de Desarrollo de Ciclo de vida (SDLC). • **COBIT:** - P01 Definir un Plan Estratégico de TI. - P04. Definir los Procesos, Organización y Relaciones de TI. - P05 Administrar la Inversión de TI. - P06 Comunicar las aspiraciones y la Dirección de la Gerencia. - P07. Administrar los recursos Humanos de TI - P08 Administrar la calidad. - P09 Evaluar y Administrar los riesgos de TI - P10 Administrar Proyectos - AI1 Identificar soluciones automatizadas - AI2 Adquirir y mantener aplicación de software. - AI3 Adquirir y mantener infraestructura tecnológica. - AI4 Facilitar operación y el uso - EA5 Adquirir recursos de TI. - AI6 Administrar los cambios. - DS1 Definir y gestionar los niveles de servicio. - DS2 Administrar servicios de terceros - DS3 Administrar desempeño y capacidad. - DS4 Garantizar la continuidad del servicio. - DS5 Garantizar la continuidad de los sistemas. - DS7 Educar y entrenar a los usuarios. - DS10 Administración de problemas. - DS13 Administrar las operaciones.

Tabla # 1 Auditoria y Aseguramiento de Procesos

2.3.2 Marco de Trabajo COBIT 4.1

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de Tecnología Informática.

COBIT está basado en los Objetivos de Control existentes de la information Systems Audit and Control Foundation (ISACF) mejorados con los estándares internacionales existentes y emergentes técnicos, profesionales, regulatorios y específicos de la industria. Los Objetivos de Control resultantes, aplicables y aceptados en forma generalizada, han sido desarrollados para ser aplicados a los sistemas de información de toda la empresa.

El término "*generalmente aplicable y aceptado*" es explícitamente utilizado en el mismo sentido que los Principios Contables Generalmente Aceptados (GAAP). Para los propósitos del proyecto, "buenas prácticas" significan el consenso de los expertos.

➢ Contenido

Las organizaciones deben satisfacer con su información, como por todos sus activos, los requerimientos de calidad, información financiera y seguridad. La Dirección debe balancear el uso de recursos disponibles incluyendo gente, instalaciones, tecnología, sistemas aplicativos y datos. Para sustentar esta responsabilidad, así como para lograr sus expectativas, la dirección debe establecer un sistema adecuado de control interno. Tal sistema o estructura debe soportar los procesos del negocio y debe ser claro sobre cómo cada actividad individual de control impacta en los recursos y satisface los requerimientos. El control, que incluye políticas,

estructuras organizacionales, prácticas y procedimientos es responsabilidad de la dirección. Un Objetivo de Control es una declaración del resultado deseado o propósito a lograr al implementar procedimientos específicos de control dentro de una actividad de Tecnología Informática.

La orientación hacia los negocios es el tema principal de COBIT. La Estructura es en respuesta a la necesidad de un sistema de control interno en Tecnología Informática. Está diseñado no sólo para ser empleado por los usuarios y los auditores, sino también, y más importante, como un amplio "checklist" para los propietarios del proceso del negocio. Cada vez más, la práctica de los negocios, involucra una completa facultad en los propietarios de los procesos del negocio, de forma tal, que tienen responsabilidad total sobre todos los aspectos del proceso del negocio. En particular, esto incluye la provisión de controles adecuados. La Estructura COBIT provee una herramienta para el propietario del proceso del negocio que facilita el descargo de su responsabilidad. La estructura comienza con una premisa simple y pragmática:

- **Orientado a Procesos**

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

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos

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

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco de COBIT, estos dominios, como se muestra en la Figura 8, se llaman:

- **Planear y Organizar (PO)** – Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS).
- **Adquirir e Implementar (AI)** – Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS)** – Recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y Evaluar (ME)**-Monitorear todos los procesos para asegurar que se sigue la dirección provista.

Grafico # 3: Los 4 Dominios de COBIT

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

• ¿Están alineadas las estrategias de TI y del negocio?

• ¿La empresa está alcanzando un uso óptimo de sus recursos?

• ¿Entienden todas las personas dentro de la organización los objetivos de TI?

• ¿Se entienden y administran los riesgos de TI?

• ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

• ¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
• ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
• ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
• ¿Los cambios no afectarán a las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos. Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?

- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

A lo largo de estos cuatro dominios, ***COBIT ha identificado 34 procesos de TI*** generalmente usados (ver figura 23 para la lista completa). Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de COBIT. COBIT

proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aun más, se pueden combinar como se necesite por cada empresa.

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

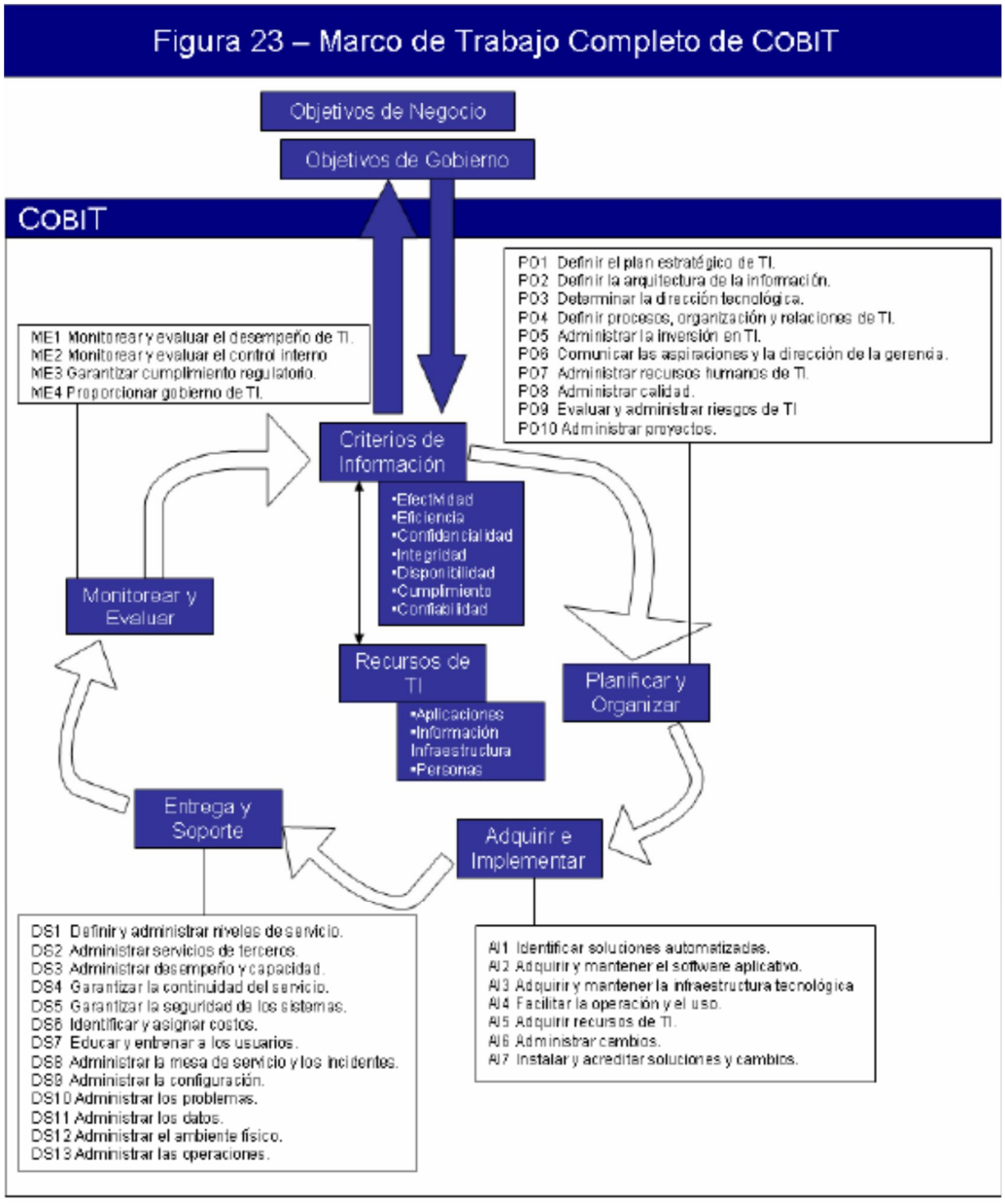


Grafico # 4: Marco de Trabajo completo COBIT

➢ Basado en controles

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

Los procesos requieren controles

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

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Ellos:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.
- La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:
- Seleccionando aquellos aplicables.
- Decidir aquellos que deben implementarse.
- Elegir como implementarlos (frecuencia, extensión, automatización, etc.)

- Aceptar el riesgo de no implementar aquellos que podrían aplicar.

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

➢ CONTROLES DEL NEGOCIO Y DE TI

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

1. ***Al nivel de dirección ejecutiva***, se fijan los objetivos de negocio, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos empresariales para ejecutar la estrategia de la compañía. El enfoque genérico hacia el gobierno y el control se establece por parte del consejo y se comunica a todo lo largo de la empresa. El ambiente de control de TI es guiado por este conjunto de objetivos y políticas de alto nivel.

2. ***Al nivel de procesos de negocio***, se aplican controles para actividades específicas del negocio. La mayoría de los procesos de negocio están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos

de los controles a este nivel estén automatizados. Estos se conocen como controles de las aplicaciones. Sin embargo, algunos controles dentro del proceso de negocios permanecen como procedimientos manuales, como la autorización de transacciones, la separación de funciones y las conciliaciones manuales. Los controles al nivel de procesos de negocio son, por lo tanto, una combinación de controles manuales operados por el negocio, controles de negocio y controles de aplicación automatizados. Ambos son responsabilidad del negocio en cuanto a su definición y administración aunque los controles de aplicación requieren que la función de TI dé soporte a su diseño y desarrollo.

3. ***Para soportar los procesos de negocio***, TI proporciona servicios, por lo general de forma compartida, por varios procesos de negocio, así como procesos operativos y de desarrollo de TI que se proporcionan a toda la empresa, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento). Los controles aplicados a todas las actividades de servicio de TI se conocen como controles generales de TI. La operación formal de estos controles generales es necesaria para que dé confiabilidad a los controles en aplicación. Por ejemplo, una deficiente administración de cambios podría poner en riesgo (por accidente o de forma deliberada) la confiabilidad de los chequeos automáticos de integridad.

➢ CONTROLES GENERALES DE TI Y CONTROLES DE APLICACIÓN

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

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

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

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

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

Por lo tanto, la responsabilidad de los controles de aplicación es una responsabilidad conjunta, fin a fin, entre el negocio y

TI, pero la naturaleza de la responsabilidad cambia de la siguiente manera:

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

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

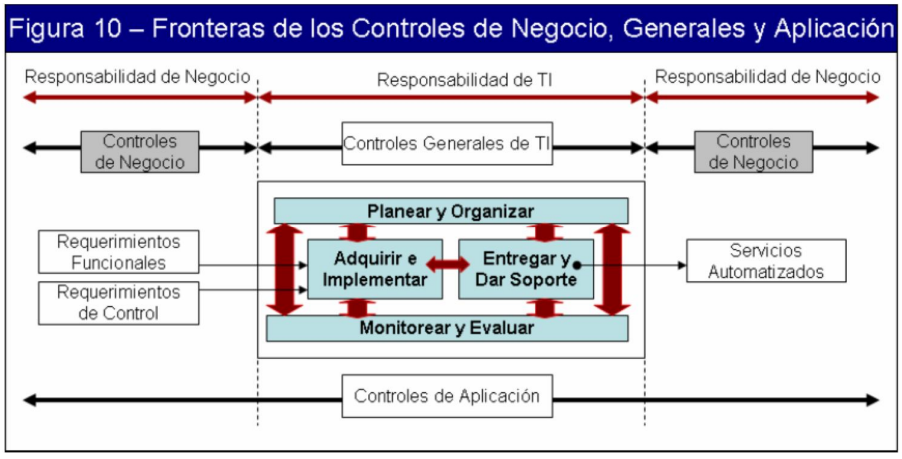


Grafico # 5: Fronteras de los controles

➢ MODELOS DE MADUREZ

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que consideren qué tan bien

se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información. Aunque pocos argumentarían que esto no es algo bueno, se debe considerar el equilibrio del costo beneficio y éstas preguntas relacionadas:

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

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

1. Una medición relativa de dónde se encuentra la empresa

2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

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

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

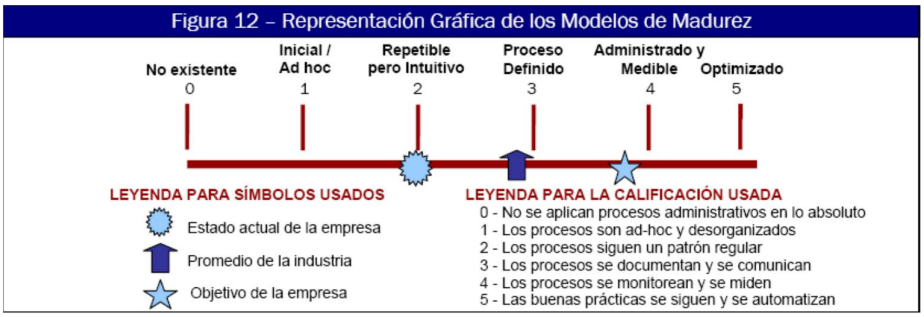
evaluación de la madurez con los modelos de COBIT, a menudo algunas implementaciones estarán en diferentes niveles aunque no esté completa o suficiente. Estas fortalezas pueden apalancarse para seguir mejorando la madurez. Por ejemplo, algunas partes del proceso pueden estar bien definidas, y, aún cuando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

Utilizando los modelos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la gerencia podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa
- El crecimiento requerido entre “como es” y “como será”
- Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método gráfico de presentación (figura 12).

El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la tabla 3.

Grafico # 6: Modelo de Madurez



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

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

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

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

Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a

establecer objetivos donde se requieran. El nivel de madurez correcto estará influenciado por los objetivos de negocio de una empresa, por el ambiente operativo y por las prácticas de la industria. Específicamente, el nivel de madurez en la administración se basará en la dependencia que tenga la empresa en TI, en su sofisticación tecnológica y, lo más importante, en el valor de su información

Tabla1 – Modelo Genérico de Madurez

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

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

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

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

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

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

➢ DESCRIPCION DE LOS PROCESOS:

P08 Planear y Organizar
Administrar la Calidad

P08: Administrar la calidad

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

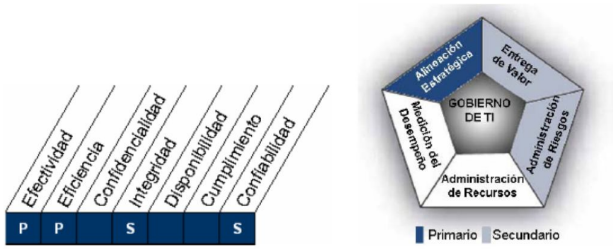


Grafico # 7: Proceso Adm. La Calidad

Control sobre el proceso TI de

Administrar la calidad

Que satisface el requerimiento del negocio de TI para

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

Enfocándose en

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

Se logra con

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

Y se mide con

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

OBJETIVOS DE CONTROL

PO8.1 Sistema de Administración de Calidad

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

PO8.2 Estándares y Prácticas de Calidad

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

PO8.3 Estándares de Desarrollo y de Adquisición

Adoptar y mantener estándares para todo desarrollo y adquisición que siga el ciclo de vida, hasta el último entregable e incluir la aprobación en puntos clave con base en criterios de aceptación acordados. Los temas a considerar incluyen estándares de codificación de software, normas de nomenclatura; formatos de archivos, estándares de diseño para esquemas y diccionario de datos; estándares para la interfaz de usuario; inter-operabilidad; eficiencia de desempeño de sistemas; escalabilidad; estándares para

desarrollo y pruebas; validación contra requerimientos; planes de pruebas; y pruebas unitarias, de regresión y de integración.

PO8.4 Enfoque en el Cliente de TI

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

PO8.5 Mejora Continua

Mantener y comunicar regularmente un plan global de calidad que promueva la mejora continua.

PO8.6 Medición, Monitoreo y Revisión de la Calidad

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

AI2 Adquirir e Implementar
Adquirir y Mantener Software Aplicativo

AI2 Adquirir y Mantener Software Aplicativo

Las aplicaciones deben estar disponibles deben estar disponibles de acuerdo con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad, y el desarrollo y la

configuración en sí de acuerdo a los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas

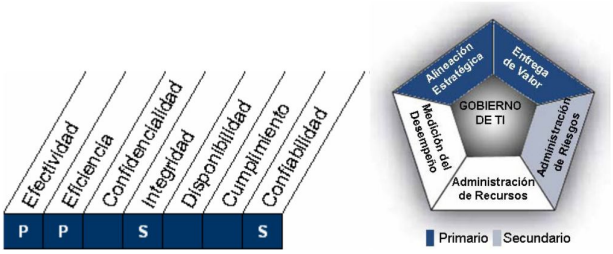


Grafico # 8: Proceso de Adq. y mantener

Que satisface el requerimiento del negocio de TI para

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

Enfocándose en

Garantizar que existe un proceso de desarrollo y confiable

Se logra con

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

Se mide con

- Numero de problemas en producción por producción por aplicación, que causan tiempo periodo significativo

- Porcentaje de usuarios satisfechos con la funcionalidad entregada.

OBJETIVOS DE CONTROL

AI2.1 Diseño de Alto Nivel

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

AI2.2 Diseño Detallado

Preparar el diseño detallado y los requerimientos técnicos del software de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel. Realizar reevaluaciones cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento.

AI2.3 Control y Posibilidad de Auditar las Aplicaciones

Implementar controles de negocio, cuando aplique, en controles de aplicación automatizados tal que en el procesamiento sea exacto, completo, oportuno, autorizado y auditable.

AI2.4 Seguridad y Disponibilidad de las Aplicaciones

Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad

de la información y la tolerancia a riesgos de la organización.

AI2.5 Configuración e implantación de Software Aplicativo Adquirido

Configurar e implementar software de aplicaciones adquiridas para conseguir los objetivos de negocio.

AI2.6 Actualizaciones Importantes en Sistemas Existentes

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

AI2.7 Desarrollo de Software Aplicativo

Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifican y direccionan para el software aplicativo desarrollado por terceros.

AI2.8 Aseguramiento de la Calidad del Software

Desarrollar, Implementar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización

AI2.9 Administración de los Requerimientos de Aplicaciones

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

AI2.10 Mantenimiento de Software Aplicativo

Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software.

AI6 Adquirir e Implementar
Administrar cambios

AI6 Administrar Cambios

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

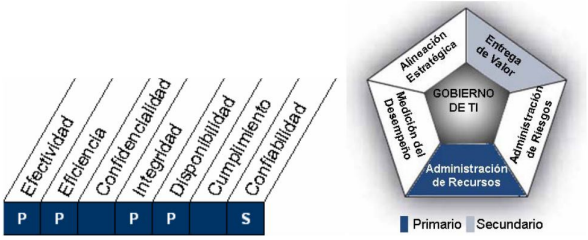


Grafico # 9: Proceso Administración de Cambio

Que satisface el requerimiento del negocio de TI para

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

Enfocándose en

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

Se logra con

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

Y se mide con

El número de interrupciones o errores de datos provocados por especificaciones inexactas o una evaluación de impacto incompleta.

- La repetición de aplicaciones o infraestructura debida a especificaciones de cambio inadecuadas
- El porcentaje de cambios que siguen procesos de control de cambios formales.

OBJETIVOS DE CONTROL

AI6.1 Estándares y procedimientos para Cambios

Establecer procedimientos de administración de cambios formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistemas y servicios, y las plataformas fundamentales.

AI6.2 Evaluación de impacto, Priorización y Autorización

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

AI6.3 Cambios de Emergencia

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

AI6.4 Seguimiento y reporte del Estatus del Cambio

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

AI6.5 Cierre y Documentación del cambio

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

CAPITULO 3

3. MARCO GENERAL DE LA INSTITUCIÓN

Credicard S.A. es una empresa emisora y administradora de tarjetas de Crédito - Pago servicios del tarjetahabiente y procesamiento Operativo a Terceros.

Hace 30 años varios inversionistas junto con un Banco determinado, constituyeron la primera empresa emisora y administradora de tarjetas de crédito del Ecuador, misma que nació con el nombre de Unicredit. Luego de 14 años de exitoso desempeño, su razón social cambió a MasterCard del Ecuador. En el 2003 y fruto de los deseos de seguir desarrollando el mercado de medios de pago en el Ecuador, se da su última transformación a Credicard S.A., incorporando la administración de la marca Visa.

En los años 90 consolidamos nuestra estructura, penetramos mucho más el mercado y durante los últimos años administramos con éxito la crisis bancaria incorporando la marca Visa.

3.1 Misión

De acuerdo con su misión, Credicard ofrece los mejores servicios financieros de medios de pago. Gracias a nuestro talento humano e infraestructura tecnológica tenemos la capacidad de operar eficientemente y brindar el mejor servicio para nuestros clientes, optimizando la rentabilidad y beneficiando a empleados, accionistas y la sociedad.

Los clientes de Credicard son: tarjeta-habientes, comercios afiliados y los bancos encargados de emitir los productos que ofrece la empresa.

3.2 Visión Estratégica

"Todo ecuatoriano sujeto de crédito usando una Credicard"

3.3 Estructura Institucional

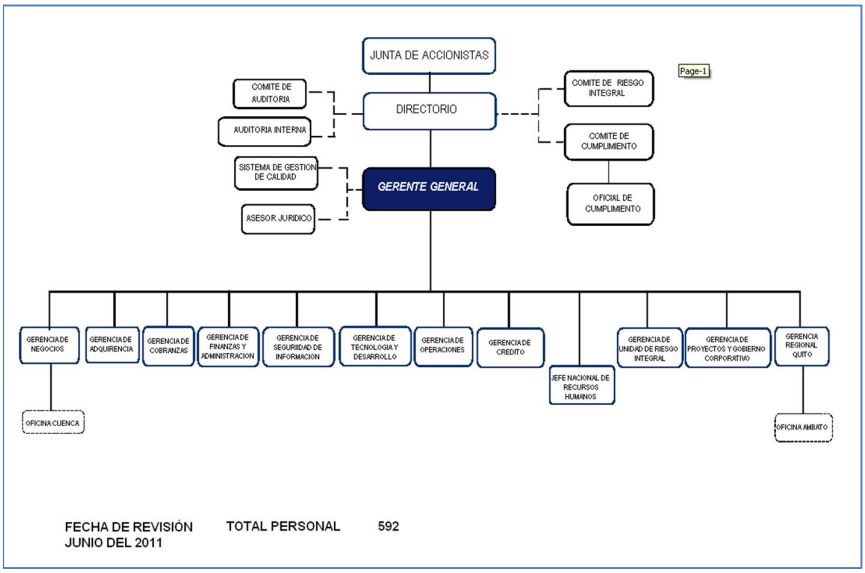


Grafico #10: Estructura Organizacional

3.4 Estructura de la División de Tecnología & desarrollo

La División de Tecnología y desarrollo está conformada por 5 áreas, cada una con sus funciones y responsabilidades.

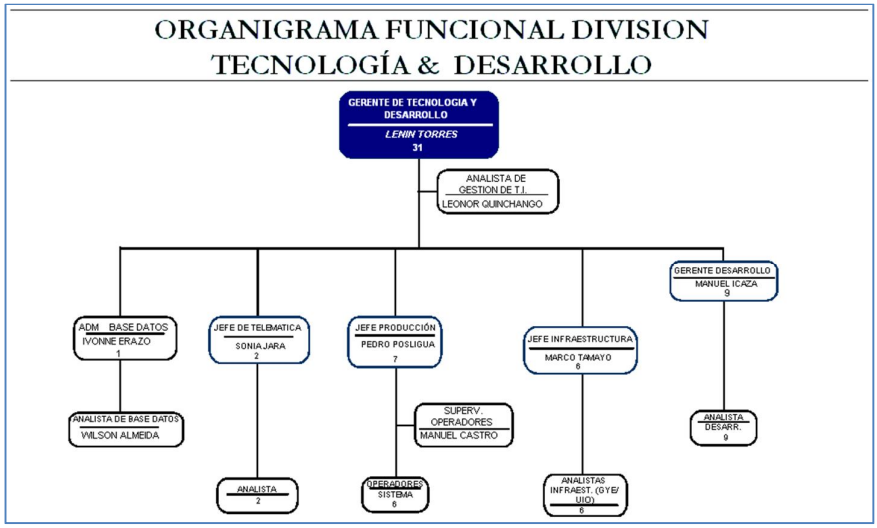


Grafico # 11: Estructura División T &D

3.5 Misión de la División de Tecnología & Desarrollo

Brindar servicios y soluciones, basados en tecnología, promover su óptima utilización de forma que ayude a los usuarios a realizar sus actividades eficientemente y por consecuencia a la empresa a cumplir con sus objetivos y requerimientos de tipo legal y regulatorio, apoyando el mejoramiento continuo de los procesos en beneficio de los clientes externos e internos.

3.6 Funciones Principales de la División de Tecnología & Desarrollo

Producción:

- Políticas para la operación del Centro de Cómputo de la empresa.

- Procesamiento de los datos en el Centro de Cómputo, garantizando información exacta y oportuna a los usuarios internos y externo de la empresa.
- Optimización de la operación de los sistemas operativos, con el objetivo de mantener siempre en funcionamiento los recursos críticos de la producción.
- Planificación y el Presupuesto de las necesidades de crecimiento en la capacidad de procesamiento de las transacciones de la empresa.

Infraestructura:

- La adquisición de equipos, contratación de enlaces e instalación de herramientas (hardware y software), para poner a disposición de los usuarios las herramientas adecuadas para el desarrollo de sus funciones.
- Los estudios necesarios para el correcto diseño de la red.

Desarrollo:

- Establecer estrategias, lineamientos de políticas y procedimientos necesarios para el desarrollo e implementación eficaz de los productos tecnológicos requeridos.

- Controlar la eficiencia y calidad de los sistemas desarrollados según las estrategias del negocio.
- Desarrollar e implementar nuevas aplicaciones o realizar modificaciones a las existentes.
- Disminuir las cargas operativas mediante el uso de la tecnología.

Base de Datos

- Administrar la estructura de la Base de Datos.
- Establecer técnicas adecuadas que garanticen la protección e integridad de los datos.

- Definir estándares y procedimientos de control que garanticen la correcta captura, procesamiento y presentación de los datos, controlar el cumplimiento de los mismos.

Telemática

- Coordinar con el Jefe de Telemática la planificación y ejecución de las actividades para los mantenimientos mensuales del Switch Transaccional.

- Coordinar con el Jefe de Telemática para establecer políticas, niveles y procedimientos de monitoreo del Switch, que permitan salvaguardar la información y la correcta utilización de los sistemas.

- Verificar conjuntamente con Jefe de Telemática la coordinación y supervisión al Proveedor del Switch.

- Establecer necesidades de Crecimiento en la capacidad de procesamiento del Switch Transaccional.

3.7 Información del Área Auditada

Credicard cuenta con un sistema central de aplicaciones que se conoce como el Modelo de Negocio “Tarjeta de Crédito”, el cual reside en la plataforma iSeries y contiene los modelos de

datos MCREDIT1[3] y MCREDIT2 sobre el motor de bases de datos DB2. Los datos de estas bases son únicamente accesibles a través de los programas y aplicaciones que desarrolla el Área de Desarrollo.

Los requerimientos que el departamento de desarrollo atiende implican creaciones de nuevas aplicaciones de negocios, modificaciones, mejora y justes a las ya existentes, que soliciten para las plataformas iSeries, PLEX y BAT (Business Advantage Technology).

Se establecen como herramientas estándares de desarrollo de aplicaciones en Credicard, dependiendo de la plataforma, las siguientes:

- ✓ Para ambientes iSeries (Host): AllFusion 2E
- ✓ Para ambientes Windows y Host: AllFusion Plex y Visual Basic 6.X (Cliente/Servidor)
- ✓ Para ambientes Windows y SQL-Server: MS PUNTO.NET

3.7.1 Herramienta usada en la organización

AllFusion 2E

AllFusion 2E (anteriormente llamado Advantage 2E para iSeries 400) es un poderoso ambiente de desarrollo para el iSeries 400 que ayuda a los equipos de desarrollo a entregar rápida y eficientemente aplicaciones de negocios a sus usuarios. Desde modelos, AllFusion 2E crea todo el código, base de datos, ayuda en línea y todos aquellos objetos

[3]Por motivos de confidencialidad los nombres de los modelos de datos han sido cambiados

necesarios en la construcción de aplicaciones de acuerdo al requerimiento del negocio.

AllFusion 2E es una herramienta de desarrollo de aplicaciones que permite, desarrollar, implementar y mantener aplicaciones de software de manera más eficiente, rigurosa, y permitir que los métodos de tercera generación sean efectivos. Utilizando 2E AllFusion, se puede crear programas sin tener que saber idioma de programación.

Los principios de diseño AllFusion utiliza 2E se aplican en todo el ciclo de vida de desarrollo de aplicaciones, incluyendo todos las tareas necesarios para iniciar, completar y mantener una aplicación 2E.AllFusion es compatible con estructura basada en datos con el enfoque de desarrollo de aplicaciones ayudan a eliminar la ciclo de vida. AllFusion 2E y se describen las especificaciones de aplicaciones que reflejan las necesidades de los usuarios. Después de los requisitos son representados por el modelo de diseño y acordado por los usuarios, las otras tareas del ciclo de vida utilizan esta información para asegurar el desarrollo eficaz de la solicitud.

AllFusion 2E incorpora una serie de metodologías estándar de la industria en el desarrollo de aplicaciones tales como el modelado entidad-relación y el diseño basado en objetos. Aunque AllFusion 2E es una herramienta de modelado y las especificaciones, el producto final no es sólo un diseño, es un sistema de aplicación 2E.AllFusion separa el proceso de diseño de la aplicación. Además de la claridad en el desarrollo, se beneficiará de las siguientes maneras:

- Cambios en la especificación se puede aplicar de forma automática a través del diseño de la aplicación.
- Las mejoras o modificaciones a la aplicación se pueden realizar independientemente de la especificación.

El mismo diseño se puede utilizar para implementar aplicaciones para varios sistemas operativos y entornos de uso AllFusion 2E, recibirá los siguientes beneficios:

- Fácil diseño de aplicaciones que están más cerca de sus necesidades de usuario final de Apoyo en el diseño de aplicaciones de mayor calidad.
- Crear aplicaciones que sean fáciles de mantener Aplicaciones de forma independiente de la lengua en la que se les apliquen.
- Desarrollar sistemas que hacen un uso efectivo de la arquitectura para los que van dirigidos.
- Le permiten diseñar y generar aplicaciones varias veces más rápido que los métodos tradicionales

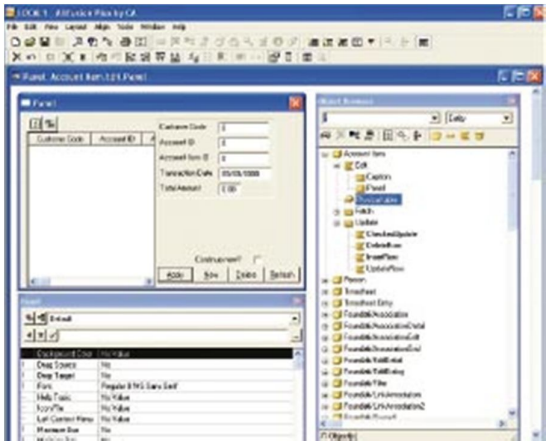
Plex: Desarrollo y generación desde modelos

Plex es una herramienta 4GL, en el mercado desde 1994. Nacida como segunda etapa de **2E**, en la época en que el diseño orientado a objetos comenzaba su segunda generación de investigaciones. Enlaza con la primera generación de herramientas 4GL a través de sus vínculos con 2E, y fue precursora de los productos que hoy

proliferan en las arquitecturas de diseño conducido por modelo. Fue creada con la idea de basarse en un repositorio común de definiciones, un concepto que fue un antecedente del uso del xml como medio de intercambio de modelos. Las empresas que participaron sucesivamente en su desarrollo (primero Synon, luego Sterling, y finalmente Computer Associates) fueron miembros activos de distintas iniciativas que contribuyeron a delinear el estado actual del diseño por modelos: el concepto mencionado de repositorio único, el UML, el concepto de patrones de diseño.

Plex adoptó parcialmente estas características, en una evolución que admite distintas vías para lograr el objetivo del desarrollo de aplicaciones por modelos.

Plex genera código sin errores, procesamiento distribuido, y creación automática de códigos y bases de datos – DB2/400, SQL Server, Oracle, MySQL entre otras.



Plex se enfoca en el ciclo de vida del software y maneja las siguientes características;

- ✓ Manejo de Versiones
- ✓ El impacto de los cambios
- ✓ El uso de metacódigo
- ✓ Patrones de Diseño
- ✓ Patrones Web
- ✓ Las APIs
- ✓ Uso de Componentes
- ✓ La integración de aplicaciones heterogéneas en la empresa
- ✓ Problemas y Soluciones
- ✓ Recursos externos auxiliares

Con todas estas características Plex logra:

- ✓ Independencia de la plataforma a la que está destinado
- ✓ Robustez del modelo de datos
- ✓ Identificación interna única de cada objeto, y visión instantánea de cada cambio en todo el modelo
- ✓ Herencia empleada a nivel del modelo
- ✓ Aplicación de Patrones de diseño, apoyado en un repositorio pre-hecho
- ✓ Capacidad de administrar modificaciones, resolviendo el impacto del cambio con precisión
- ✓ Capacidad de integrar código del usuario sin riesgo de sobre escritura
- ✓ Aplicación integrada de Configuración y Versionamiento
- ✓ Manejo sólido del trabajo de equipos
- ✓ Flexibilidad para manejar modelos de aplicaciones complejas (Variantes y Versiones)
- ✓ Adopción rápida de cambios tecnológicos
- ✓ Libertad para emplear distintas filosofías de diseño

3.7.2 Metodología usada para el Desarrollo y Mantenimiento de Aplicaciones

De acuerdo a la revisión de los procesos y procedimientos establecidos, actualmente Credicard en su desarrollo de aplicaciones mantienen las etapas tradicionales del ciclo de vida del desarrollo (SDLC) que se muestran en la gráfica, este enfoque se basa en un enfoque secuencial y sistemático de desarrollo de software que comienza con un estudio de factibilidad y continúa con la definición de los requerimientos, el diseño, desarrollo e implementación. Esta serie de pasos o de etapas tienen definidas metas y actividades, responsabilidades, resultados esperados y fechas de cumplimiento.

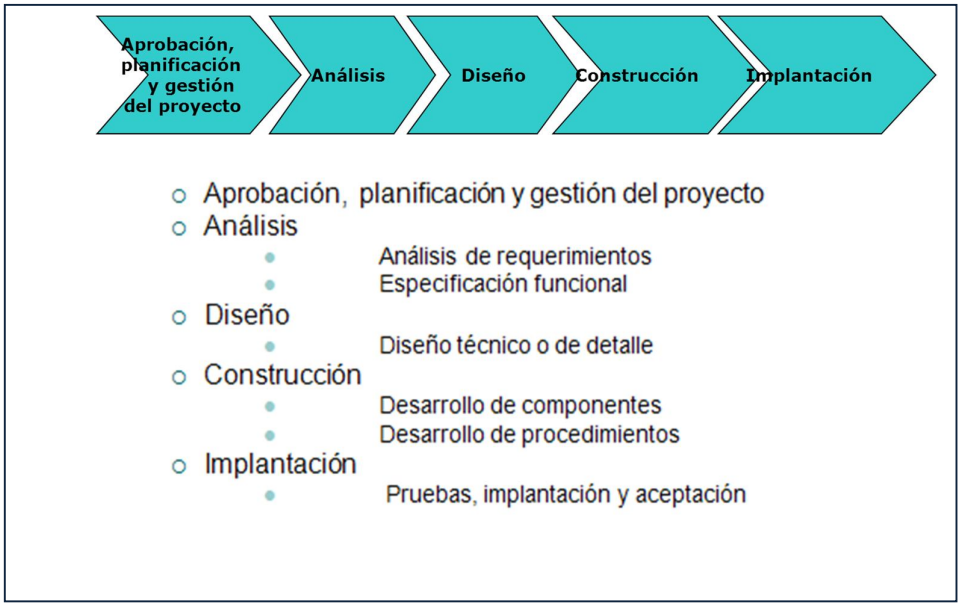


Gráfico # 12: Etapas del Desarrollo de un sistema

CAPITULO 4

4. PROPUESTA DE LA AUDITORIA

4.1 Propuesta

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar. Para decidir el nivel correcto, la gerencia debe preguntarse: ¿Hasta dónde debemos ir?, y ¿está el costo justificado por el beneficio? , aprovechando esta necesidad se ha propuesto al Gerente de Desarrollo evaluar los métodos y procedimientos usados en el desarrollo de las aplicaciones y su ciclo de vida como también medir productos y actividades que simplifiquen el mantenimiento de las aplicaciones, el control de la calidad del producto y la reutilización de componentes de software.

4.2 Cronograma de Trabajo

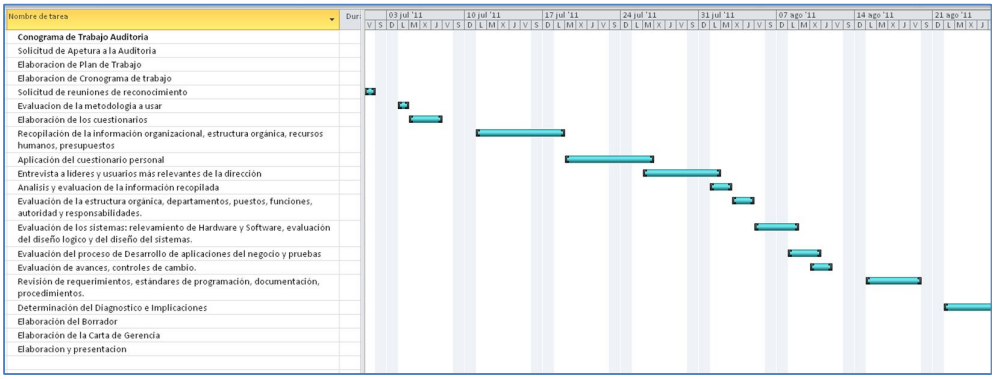


Gráfico # 13: Cronograma de Trabajo

4.3 Plan de Auditoría

PROGRAMA DE AUDITORIA			
EMPRESA		**FECHA**	
FASE	**ACTIVIDAD**	**HORAS ESTIMADAS**	**ENCARGADO**
I	**VISITA PRELIMIAR** ✓ Solicitud de Manuales y Documentaciones ✓ Elaboración de los cuestionarios ✓ Recopilación de la información organizacional, estructura orgánica, recursos humanos, presupuestos**.**	**3Días**	**L.Q.**
II	**DESARROLLO DE LA AUDITORIA** ✓ Aplicación del cuestionario personal ✓ Entrevista a líderes y usuarios más relevantes de la dirección ✓ Evaluación de la estructura orgánica, departamentos, puestos, funciones, autoridad y responsabilidades. ✓ Evaluación del proceso de Desarrollo de aplicaciones del negocio y pruebas ✓ Evaluación de avances, controles de cambio. ✓ Revisión de requerimientos, estándares de programación, documentación, procedimientos.	**30Días**	**L.Q.**
III	**REVISION Y PRE-INFORME** ✓ Revisión de los papeles de trabajo ✓ Determinación del Diagnostico e Implicaciones ✓ Elaboración de la Carta de Gerencia ✓ Elaboración del Borrador	**6 Días**	**L.Q.**
IV	**INFORME** ✓ Elaboración y presentación del informe	**3 Días**	**L.Q.**

Tabla 3: Programa de Auditoria

CAPITULO 5

5. DESARROLLOY EJECUCIÓN DE LA AUDITORIA

5.1 Carta de inicio de Auditoria

El presente plan contiene el detalle de los controles que se revisaran para mejorar los procedimientos al Desarrollo de Aplicaciones y los controles informáticos internos, de *Credicard S. A,* con corte al 30 de Junio de 2011.

De acuerdo con normas de auditoría generalmente aceptadas, y según acordamos con ustedes, se efectuó una revisión de la metodología aplicada en los desarrollos de aplicaciones de la Compañía, pero sólo hasta donde consideramos necesario con el propósito de tener una base para determinar la confianza que se puede depositar en el mismo al determinar la naturaleza, oportunidad y extensión de las pruebas de auditoría de con corte al 30 de Junio de 2011.

Por consiguiente, nuestra revisión no abarca todos los procedimientos y técnicas de control y no se llevó a cabo con el propósito de hacer recomendaciones detalladas o evaluar si los controles de la Compañía son adecuados para prevenir y detectar todos los errores e irregularidades. A este respecto, debe reconocerse que debido a las limitaciones inherentes a cualquier estructura de control interno, pueden ocurrir errores e irregularidades y no ser detectados. Además, la proyección de cualquier evaluación de la estructura a períodos futuros está

sujeta al riesgo de que los procedimientos puedan volverse inadecuados debido a cambios en las condiciones existentes o que se deteriore el grado de cumplimiento con los procedimientos establecidos.

5.2 Programa de Auditoria

5.2.1 Identificación de Objetivos de control usadas en la auditoría basada en COBIT 4.1

Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos, para esta Auditoría al Desarrollo de Aplicaciones se identificaron los siguientes objetivos de control.

- ✓ PO8 Administrar la Calidad
- ✓ AI2 Adquirir y mantener software aplicativo
- ✓ AI6 Administración de cambios

Área de Control	Objetivos de Control
P08 Administrar la Calidad	P08.2 Estándares y prácticas de calidad (SDLC) P08.3 Estándares de desarrollo y de adquisición (SLDC)
AI2 Adquirir y mantener el software aplicativo	A.I2.1 Diseño de alto nivel
	AI2.2 Diseño detallado
	AI2.5 Configuración e implementación de software aplicativo adquirido
	AI2.6. Actualizaciones importantes en sistemas existentes
	AI2.7 Desarrollo de Software aplicativo
	AI2.8 Aseguramiento de la Calidad del Software
	AI2.10 Mantenimiento de Software aplicativo

AI6 Administración de cambios	AI6.1 Estándares y procedimientos de cambios
	AI6.2 Evaluación de impacto, priorización y autorización
	AI6.3 Cambios de Emergencia
	AI6.4 Seguimientos y reporte de estatus de cambio
	AI6.5 Cierre y documentación del cambio

Tabla # 4 Matriz de Control

5.2.2 Personal Entrevistado

Para llevar a efecto la presente auditoria se realizó reuniones y entrevistas sobre el entendimiento del negocio, de los procesos, y las actividades que realizan para llevar a cabo el desarrollo de una aplicación en fase desarrollo y desarrollados, entre los entrevistados están:

ENTREVISTA	CARGO
Proceso de desarrollo de Aplicaciones:	Gerente de Desarrollo
Lógica de Programación	Analista de Desarrollo
Administración de librerías, tablas, acceso a archivos, modelos de Objetos:	Administrador Bases de Datos
Revisión de Documentación de proyectos	Analistas de Procesos y Desarrollo

Tabla # 5: Personas Entrevistadas

Por la buena imagen que tiene el departamento de desarrollo, no hubo dificultades en levantar la información.

5.2.3 Documentos a solicitar

Para la verificación y análisis de la auditoria en cuestión se solicitaron los siguientes documentos:(Ver Anexo 1)

- ✓ Políticas, estándares, normas y procedimientos.
- ✓ Organigrama y manual de funciones.
- ✓ Manuales de sistemas.

- ✓ Registros
- ✓ Archivos
- ✓ Requerimientos de Usuarios

5.2.4 Técnicas

La auditoría ha sido basada en técnicas de revisión, análisis y visualización:

- ✓ En reuniones con las áreas involucradas en el desarrollo
- ✓ Visualización del Panorama: verificación de las funciones, seguridad de los equipos, etc.
- ✓ Verificación de documentos de desarrollos de aplicativos en fase desarrollo y desarrollados.
- ✓ Análisis de los Requerimientos de Usuarios.
- ✓ Revisión de documentación de los desarrollos en sus diferentes etapas.

5.3 Ejecución de la Auditoria

5.3.1 Verificación de controles

P08. Administración de la calidad del Software

Objetivos.-

Medir la calidad de los procesos y estándares de desarrollo.

Alcance.-

Alcanzar mejora continua con una administración de calidad en los desarrollos de aplicaciones que de valor al negocio.

Objetivos de control

1. Estándares y prácticas de calidad (SDLC)
2. Estándares de desarrollo y de adquisición (SLDC)

Procedimiento

1. **Entrevistas:**
   - Gerente de Desarrollo
   - Líderes de Proyectos
   - Administrador de la calidad de la Organización

2. **Obteniendo soportes**
   - Políticas y Procedimientos relacionados con el aseguramiento de la calidad, el ciclo de vida del desarrollo de sistemas y la documentación de sistemas.

- Actas de revisiones a la metodología del ciclo de vida del desarrollo de sistemas

3. Evaluación de controles

- Existe un plan de calidad de la función de servicios de información: Que tome como base el plan general de calidad de la organización y los planes a corto y largo plazo de tecnología de información.
- Se tiene implantada una metodología de desarrollo de sistemas de información (SLDC) soportada por herramientas de ayuda.
- Requiere el mantenimiento de documentación detallada de programación y de sistemas (por ejemplo, diagramas de flujo, diagramas de flujo de datos, narrativas escritas de programación, etc.), y que dichos requerimientos hayan sido comunicados a todo el personal involucrado
- Evaluar la calidad de la documentación de la aplicación de operaciones. (Esto debe incluir diagramas de flujo de trabajo y sistema de entrada y las descripciones de salida, frecuencia de trabajo y la secuencia de operación, reinicie el trabajo / los procedimientos de recuperación, los requisitos de archivo de copia de seguridad y los procedimientos, los mensajes de error y técnicas de la conciliación, procedimientos de distribución de informes, instrucciones de captura de datos).

4. Probando que

La metodología del ciclo de vida de desarrollo de sistemas asegura apropiadamente:

- Controles suficientes durante el proceso de desarrollo para sistemas y tecnologías nuevas
- Comunicación con todos los empleados apropiados involucrados en el desarrollo y mantenimiento de sistemas
- se utilizan procedimientos para los cambios tecnológicos
- Se utilizan procedimientos para asegurar la aceptación y aprobación de los usuarios
- La adecuación de los acuerdos de terceras partes como implementadores
- Los usuarios comprenden los controles y requerimientos de la metodología del ciclo de vida del desarrollo de sistemas.
- Los mecanismos de control de cambios dentro de la metodología del ciclo de vida del desarrollo de sistemas permiten el llevar a cabo cambios a la metodología y que ésta es un documento "vivo"
- El registro de las revisiones y modificaciones a la metodología del ciclo de vida del desarrollo de sistemas de la organización refleja los nuevos sistemas y tecnologías considerados actualmente y esperados en el futuro

- Los resultados completos de las pruebas de programas y sistemas (incluyendo resultados de pruebas en paralelo/piloto) son revisados y retenidos para pruebas futuras
- Existe un proceso para resolver problemas encontrados durante la pruebas.
- Se ha llevado a cabo una revisión post-implementación por parte del personal de aseguramiento de la calidad
- Los representantes del departamento usuario involucrados en los proyectos de desarrollo de sistemas están satisfechos con el uso actual de la metodología.
- Se requiere el llevar a cabo una revisión de aseguramiento de la calidad subsecuente al término de todas las pruebas del sistema y de la revisión y aprobación de los resultados de las pruebas.
- Se llevan a cabo revisiones post-implementación, que los resultados son comunicados a la Presidencia y que se requieren planes de acción para las áreas de implementación con necesidad de mejoras.
- Los resultados de las mediciones de las metas de calidad, existen y se trabaja con ellos.

I2. Desarrollo y Mantenimiento de Aplicaciones

Objetivos.-

Evaluar metodología de clico de vida de los sistemas que permitan la disponibilidad de los sistemas de acuerdo a los requerimientos del negocio

Alcance.-

Cubre el diseño de las aplicaciones, la inclusión apropiada de los aplicativos, y el desarrollo y la configuración de acuerdo a los estándares.

Objetivos de control

1. Diseño de alto nivel
2. Diseño detallado
3. Configuración e implementación de software aplicativo adquirido
4. Actualizaciones importantes en sistemas existentes
5. Desarrollo de Software aplicativo
6. Aseguramiento de la Calidad del Software
7. Mantenimiento de Software aplicativo

Procedimiento

1. **Entrevistas:**
    - Gerente de Desarrollo
    - Analistas de Desarrollo
    - Administrador de Bases de datos

2. **Obteniendo soportes**
    - Políticas y Procedimientos organizacionales relacionados con la metodología del ciclo de vida de desarrollo de sistemas.
    - Objetivos y planes a corto y largo plazo de tecnología de información
    - Documentación seleccionada del proyecto, incluyendo aprobaciones de diseños, definición de requerimientos de archivo, especificaciones de programas, diseño de recopilación de datos fuente, definición de requerimientos de entrada, interface usuario, definición de requerimientos de procesamiento, plan de pruebas y resultados del software de aplicación, materiales de soporte y referencia para usuarios y reevaluación del diseño del sistema.
    - Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de documentación
    - Procedimientos formales para la operación del Sistema de Gestión de Bases de datos (SGBD), creación de tablas, vistas, etc.

3. **Evaluación de controles**
    - Existe implantada una metodología de desarrollo de sistemas de información (SLDC) soportada por herramientas de ayuda.
    - Existe bitácora de control de aplicaciones
    - Existe un mecanismo de evaluación del versionamiento que permita el control de mismo.

- Existen definiciones claras de requerimientos funcionales y técnicos que cubran el alcance de todos los cambios requeridos en el sistema.
- Se preparan especificaciones detalladas de programas para cada proyecto de desarrollo o modificación de información, y que estas especificaciones concuerdan con las especificaciones del diseño del sistema
- Existen mecanismos adecuados para la definición y documentación de los requerimientos de entrada para cada proyecto nuevo de desarrollo o modificación de sistemas
- Se especifican mecanismos adecuados para asegurar los requerimientos de seguridad y control internos para cada proyecto nuevo de desarrollo o modificación de sistemas

4. Probando que:

- Se especifican mecanismos adecuados para asegurar los requerimientos de seguridad y control internos para cada proyecto nuevo de desarrollo o modificación de sistemas

- La metodología del ciclo de vida de desarrollo de sistemas asegura que existe un proceso que considera apropiadamente todos los aspectos de diseño de sistemas (por ejemplo, entrada, procesamiento, salida, controles internos, seguridad, recuperación en caso de desastre, tiempo de respuesta, reportes, control de cambios, etc.)

- Los usuarios clave de los sistemas están involucrados en el proceso del diseño del sistema
- Los cambios mayores a los sistemas existentes aseguran que éstos han sido desarrollados utilizando una metodología de ciclo de vida de desarrollo de sistemas similar a la utilizada para el desarrollo de nuevos sistemas
- Existen los procedimientos de aprobación del diseño para asegurar que la programación del sistema no se inicie hasta que se hayan obtenido las aprobaciones correspondientes
- Los requerimientos de archivo y la documentación del sistema, así como el diccionario de datos, son consistentes con los estándares
- Las especificaciones de programación concuerdan con las especificaciones del diseño del sistema
- Existen las especificaciones del diseño de la interface usuario - máquina
- Se documenten las interfaces internas y externas
- Los requerimientos de procesamiento forman parte de las especificaciones del diseño
- Los requerimientos de seguridad y control interno forman parte de las especificaciones del diseño
- Las especificaciones de diseño de los requerimientos de controles de aplicación garantizan la precisión, suficiencia,

oportunidad y autorización de las entradas y las salidas

- El funcionario de seguridad está involucrado activamente en el proceso de diseño, desarrollo e implementación del proyecto del nuevo sistema o de modificación del sistema
- El diseño del sistema determina si se han cuantificado las mejoras de disponibilidad/confiabilidad en términos de tiempo y de procedimientos más eficientes en comparación con métodos anteriores, en caso de aplicar
- Las provisiones de programas de aplicación verifican rutinariamente las tareas llevadas a cabo por el software para asegurar la integridad de los datos
- Existen estándares de pruebas establecidos
- Existe un plan de pruebas del proyecto y un proceso de aprobación del usuario
- El proceso para escalar los problemas del help desk incluye el seguimiento, monitoreo y reporte de tales problemas a la administración de la función de servicios de información apropiada
- Se requiere la existencia de mecanismos para actualizar la documentación de los usuarios
- Existe la comunicación sobre los cambios a la documentación de los usuarios

AI6. Manejo de Cambios

Objetivos.-

Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores

Alcance.-

Un sistema de administración que permita el análisis de implementación y seguimientos de todos los cabios requeridos.

Objetivos de control

1. Estándares y procedimientos de cambios
2. Evaluación del Impacto, priorización y autorización
3. Cambios de Emergencia
4. Seguimientos y reporte de estatus de cambio
5. Cierre y documentación del cambio

Procedimiento

1. **Entrevistas:**
   - Gerente de Desarrollo
   - Líderes de Proyectos

2. **Obteniendo soportes**
   - Políticas y Procedimientos organizacionales relacionados con: Planeación de sistemas de información, control de cambios, seguridad y ciclo de vida de desarrollo de sistemas.
   - Política y procedimientos de la función de servicios de sistemas de información relacionada con: Metodología del ciclo de

vida de desarrollo de sistemas, estándares de seguridad. Aseguramiento independiente de la calidad, implementación, distribución, mantenimiento, cambios de emergencia, liberación de software y control de versiones del sistema.

- Plan de desarrollo de aplicaciones
- Formato de bitácora de requerimientos de control de cambios
- Contratos con proveedores relacionados con servicios de desarrollo de aplicaciones.

3. Evaluación de controles

- Existe y se utiliza una metodología para priorizar los requerimientos de cambios al sistema.
- Se consideran procedimientos de cambios de emergencia en los manuales de operaciones.
- El control de cambio es un procedimiento formal tanto para los usuarios como para los grupos de desarrollo.
- La bitácora de control de cambios asegura que todos los cambios mostrados fueron resueltos.
- El usuario está satisfecho con el resultado de los cambios solicitados – calendarización y costos.
- Para una selección de cambios en la bitácora de control de cambios:
  - El cambio trajo como resultado modificaciones en los programas y operaciones

- Los cambios hayan sido llevados a cabo como fueron documentados
- La documentación actual refleja el ambiente modificado

- El proceso de cambios es monitoreado en cuanto a mejoras en el conocimiento, efectividad en el tiempo de respuesta y satisfacción del usuario con respecto al proceso

4. **Probando que:**

- Para una muestra de cambios, la administración ha aprobado los siguientes puntos:
  - ✓ solicitud de cambios
  - ✓ especificación del cambio
  - ✓ acceso al programa fuente
  - ✓ finalización del cambio por parte del programador
  - ✓ solicitud para mover el programa fuente al ambiente de prueba
  - ✓ finalización de pruebas de aceptación
  - ✓ solicitud de compilación y paso a producción
  - ✓ determinación y aceptación del impacto general y específico
  - ✓ desarrollo de un proceso de distribución

- La revisión del control de cambios en cuanto a la inclusión de:
  - ✓ fecha del cambio solicitado
  - ✓ persona(s) que lo solicitan
  - ✓ solicitud aprobada de cambios
  - ✓ aprobación del cambio realizado - función de servicios de información
  - ✓ aprobación del cambio realizado – usuarios
  - ✓ fecha de actualización de documentación

- ✓ fecha de paso a producción
- ✓ aprobación del cambio por parte de aseguramiento de la calidad
- ✓ aceptación por parte de operaciones

- Los tipos de análisis de cambios realizados al sistema para la identificación de tendencias
- Existen procedimientos de entradas y salidas ("check in/checkout) para cambios
- Todos los cambios en la bitácora fueron resueltos a satisfacción de los usuarios y que no se llevaron a cabo cambios que no hayan sido registrados en la bitácora
- Los usuarios tienen consciencia y conocimiento de la necesidad de procedimientos formales de control de cambios
- El proceso de reforzamiento del personal asegura el cumplimiento de los procedimientos de control de cambios

5.3.2 Obtención de Soporte y papeles de Trabajo.

Entre los principales manuales obtenidos en la presente auditoría 2011 constan:

- ✓ Manual de procedimientos de Desarrollo y Mantenimiento.
- ✓ Instructivo de la Metodología Tecnológica para el Desarrollo de Proyectos.
- ✓ Instructivo de Versionamientos de funciones y de Fuentes de Objeto

- ✓ Manual de Procedimientos de Producción
- ✓ Manual de Procedimientos de Requerimientos para Sistemas
- ✓ Manual de Procedimientos para el Manejo de Desarrollo y Cambios de las Aplicaciones del Sistema
- ✓ Solicitud de Requerimientos por muestreo

5.3.3 Matriz de Riesgos

Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo.

Por tanto se ha aplicado parámetros de medición del riesgo para la evaluación de esta auditoría, descritos a continuación:

Metricas de Medicion	
Alto	Impacta la estabilidad o seguridad del negocio
Medio	Tiempo que tardaria en restablecer el negocio
Bajo	No afecta a la continuidad del Negocio

MATRIZ DE RIESGO

Área	Area	Proceso	Código	Responsable	Hallasgo	Nivel Riesgo	Riego
Desarrollo	Tecnología	Adm. De calidad del Software	DESTEC001	Gerente de Desarrollo	Metodología que cubre todas las fases del desarrollo y sea adaptable a distintos tipos de proyectos.	B	Que no se aseguramiento la calidad en el ciclo de vida del desarrollo de sistemas y la documentación de sistemas.
Desarrollo	Tecnología	Adm. De calidad del Software	DESTEC002	Gerente de Desarrollo	Registro y control de todos los proyectos fracasados o en stand by	B	Que se Generen errores recurrente sobre estos proyectos
Desarrollo	Tecnología	Adm. De calidad del Software	DESTEC003	Gerente de Desarrollo	Falta de evidencia de analisis funcional para los desarrollos realizados	B	No se implementes adecuadamente los proyectos o requerimientos
Desarrollo	Tecnología	Desarrollo y Mantenimento de aplicaciones	DESTEC004	Gerente de Desarrollo	Por cada cambio y/o modificaciòn que se vaya a realizar existe un analisis de impacto en el modelo de datos y sus afectaciones ?	A	Ocurran errores graves que conlleven a cambios emergentes concurrentes
Desarrollo	Tecnología	Desarrollo y Mantenimento de aplicaciones	DESTEC005	Gerente de Desarrollo	Controles sin evidencia de cumplimiento	B	No se cumplan con los cronogrmas de implementacion de proyectos
Desarrollo	Tecnología	Desarrollo y Mantenimento de aplicaciones	DESTEC006	Gerente de Desarrollo	Medicion de indicadores	B	No se midan apropiadamente el rendimiento del personal
Desarrollo	Tecnología	Desarrollo y Mantenimento de aplicaciones	DESTEC007	Gerente de Desarrollo	Por cada cambio y/o modificaciòn quese vaya a realizar existe un analisis y documentación de impacto en el modelo de datos y sus afectaciones	M	Que no se contemplen todos los escenarios que impacten el modelo la documentación para hacer seguimientos en posibles errores.
Desarrollo	Tecnología	Desarrollo y Mantenimento de aplicaciones	DESTEC008	Administrador de base de datos	Existen mecanismos adecuados para la definición y documentación de los requerimientos de entrada para cada proyecto nuevo de desarrollo o modificación de sistemas	B	Que no se documente proyectos en ambiente WEB
Desarrollo	Tecnología	Desarrollo y Mantenimento de aplicaciones	DESTEC009	Administrador de base de datos	Falta de procesos claves para garantizar el buen desempeño de las aplicaciones, bases de datos	A	Que no de detecten a tiempo saturación transaccional
Desarrollo	Tecnología	Manejo de Cambios	DESTEC010	Administrador de base de datos	Falta de aprobacion en los cambios de aplicaciones por otras, y las solicitudes de nuevas aplicaciones	M	Que se realicen cambios o modificaciones inapropiadas
Desarrollo	Tecnología	Manejo de Cambios	DESTEC011	Administrador de base de datos/Gerente de desarrollo	Falta de analisis de impacto funcional para los reversos y optimizaciones de programas	M	Que afecten la degradación del modelo del negocio
Desarrollo	Tecnología	Manejo de Cambios	DESTEC012	Administrador de base de datos/Gerente de desarrollo	Niveles de aprobación no adecuados para el desarrollo o cambios de programas	B	Que el Analista de Bases de Datos apruebe requerimientos no relacionados a sus funciones

CAPITULO 6

6. INFORME DE AUDITORIA

6.1 Resumen de Informe de Auditoria

En este capítulo se presenta un resumen del informe producto de la evaluación de controles de la metodología usada en el desarrollo de las aplicaciones y su ciclo de vida de los sistemas (SDLC), la información obtenida durante el proceso de auditora ha sido suministrada por los propios involucrados en la organización correspondiente al primer semestre del 2001. La revisión no abarcó todos los procedimientos y técnicas de control, al respecto, debe reconocerse que debido a las limitaciones inherentes a cualquier estructura de control interno, pueden ocurrir errores e irregularidades y no ser detectados

Administración de la calidad del Software

Observaciones

De nuestra evaluación a la administración de de la calidad del Software para los aplicativos STC, BAT, WEB se observó lo siguiente:

A. Se pudo evidenciar que para los Desarrollo de Aplicaciones en ambiente WEB no existen procedimientos de estándar de programación documentados y soportes de las mismas, incumpliendo la política descrita en el mismo Manual de Desarrollo, Proceso de programación, pruebas y ajustes técnicos de requerimientos que indica: " En el aspecto de programación, el analista de desarrollo debe seguir las reglas de sintaxis de documentación que encontrara en los programas y utilizará los estándares ya establecidos tanto para programas de consulta, así como para reportes y aplicaciones transaccionales según lo descrito en el Instructivo de Estándar para el desarrollo de aplicaciones.."

B. No se evidencio el análisis funcional, modelo conceptual, definición de rutinas, tablas, cambios al modelo de datos, etc. de las aplicaciones y programas que serán modificadas para un proyecto o requerimiento. Según lo descrito en el Proceso de diseño de las aplicaciones, estructuras y funcionalidad de los requerimientos y/o proyectos.

C. De acuerdo a lo consultado durante el año 2011 no existe evidencia de que se haya ejecutado las reuniones trimestrales del comité de Proyectos y requerimientos como lo indica el instructivo de la Metodología para el desarrollo de Proyectos

actualizado 21/Diciembre/2010 " cada tres meses se reúnen los miembros del comité de Proyectos y requerimientos, el mismo que está conformado por la Gerencia General y las gerencias de cada área, a fin de asignar la prioridad a cada uno de los proyectos que estén alineados con la estrategia de la empresa."

Riesgos

- ✓ La falta de una metodología aplicada que involucre a todos los desarrollos de aplicaciones proporciona una escasez de resultados óptimos en la calidad de software.
- ✓ No exista documentación de los programas y/o sistemas, en donde ésta sea inadecuada o no esté actualizada.

Recomendaciones

En base a lo expuesto recomendados los siguientes puntos de mejora:

A. Diseñar y documentar estándares para el desarrollo de todas las aplicaciones incluyendo el ambiente WEB que sigan el ciclo de vida de los sistemas.
B. Formalizar documentación en Fase de desarrollo de aplicaciones (Diseño conceptual, Diseño Funcional, diagramas de flujos, datos de entradas, etc.) que permitirán mantener una visión del diseño general y cambios a los modelo de datos de todas las plataformas.
C. Cumplir con las políticas establecidas en los manuales.

Comentarios de la Gerencia:

Desarrollo y Mantenimiento de Aplicaciones

Observación:

De la evaluación de requerimientos y proyectos ejecutados en el primer semestre del 2011 se encontraron las siguientes novedades

A. De una muestra tomada de 53 requerimientos, se encontraron que3 de estos requerimientos no cuentan con la firma del Analista de Proyectos y procesos a pesar que en el capítulo III del "Manual de Procedimientos para el manejo de desarrollos y cambios de las aplicaciones del sistema" actualizado el 13-06-11 se menciona lo siguiente: " El Analista de Proyectos y Procesos, procede a elaborar el acta de certificación en donde se consignarán las firmas de los usuarios líderes del proyecto, el Analista de Proyectos y Procesos y del departamento de Desarrollo, que estuvieron involucrados en las pruebas de certificación de la opción y/o aplicación."

Nº Req.	Fecha Puesta Producción
13763,	28/04/2011
14137	12/05/2011
14148	19/06/2011

B. Dentro del proceso del ciclo de vida de los sistemas no se pudo evidenciar documentación formal de análisis de impacto funcional aun cuando en el Manual de Procedimiento de Desarrollo y mantenimiento actualizado en 13/Jun/11, Proceso de Análisis de Requerimientos indica "El analista de desarrollo asignado realiza el análisis de impacto y las necesidades de cambio en las estructuras de datos, así como del diccionario de datos vs el modelo de negocio del sistema.".
C. El único soporte evidenciado en relación al análisis de impacto fue, en el Formulario de Pases a Producción indicando en un check box Si tiene impacto o No, de las cuales se encontraron que no todos los formularios cumplen con indicar este análisis.

	Análisis de Impacto		
Muestreo	SIN	CON	No Definido
53	36	4	13

D. Durante la revisión de los requerimientos ingresados por los mantenimientos a las aplicaciones, no se encontraron registros de los requerimientos detallados en la tabla siguiente.

Requerimiento	Descripción Formulario	Usuario Ingreso	Fecha Ingreso
12092	Mantenimiento y Desarrollo Otras Plataformas	gye\mcvill	01/10/2010
12859	Mantenimiento y Desarrollo Otras Plataformas	gye\rpalac	04/01/2011
14320	Mantenimiento y Desarrollo Otras Plataformas	gye\rpalac	31/05/2011

E. Según lo descrito en el manual de Desarrollo y Mantenimiento de aplicaciones, Procedo e optimización y/o cambios Emergentes dice: "Si, el requerimiento es emergente, el Analista de Desarrollo solicita el usuario de contingencia de acuerdo a lo descrito en el Proceso de Perfil de Usuario de Contingencia, del Manual de Procedimientos de Producción, ***para realizar los pases*** en el caso de ser necesario en el ***ambiente de Producción***." Incumpliendo la política de seguridad de la compañía basada en la norma PCI/DSS descrita: "El personal de desarrollo no debe ni puede realizar tareas o funciones del área de Producción. De manera inversa el personal de producción no debe ni puede realizar tareas del área de Desarrollo."

F. No se encontró descrito proceso de mantenimiento y monitoreo de bases de datos SQL, indicando si se realiza ajustes, optimización de rendimiento, monitoreo de contadores de rendimiento, bloqueos de memoria, etc. Procesos claves para poder garantizar el buen desempeño de las aplicaciones.

G. Uso de datos reales en el ambiente de desarrollo

Se analizó una muestra de 3 archivos utilizados para realizar pruebas en el ambiente de desarrollo y detectamos en cada uno de ellos números de tarjeta y cédula reales. Por lo tanto, se incumplen normas de PCI, las políticas de seguridad de la Compañía y el manual de procedimientos del área de Desarrollo.

Archivo	Descripción del archivo	Cantidad de números de tarjeta reales encontrados	Cantidad de números de cédula reales encontrados
BTTYREP	Histórico de transacciones	197	199,589
DSAJREP	Tarjetas emitidas	6	77,370
DSANREP	Saldos	6	66,077

H. Controles sin evidencia de su cumplimiento

Existen controles que según el Manual de Procedimientos de Desarrollo y Mantenimiento deben ser realizados por el Gerente del área; sin embargo, no observamos evidencia del cumplimiento de los mismos. Cabe señalar que algunos de dichos controles están presentes en la matriz de riesgos como controles mitigantes a eventos de riesgo alto.

Proceso	Control según el manual de procedimientos
Análisis de requerimientos	Durante toda la etapa de análisis, el Gerente de Desarrollo realiza continuos seguimientos de control a los Analistas de Sistemas, Desarrolladores y/o Proveedores.
Programación, pruebas y ajustes técnicos	El Gerente de Desarrollo y Mantenimiento realiza verificaciones continuas al cronograma de desarrollo y al cumplimiento de actividades de programación.
Monitoreo de aplicaciones	Durante toda la etapa de monitoreo, el Gerente de Desarrollo verifica la ejecución y atención de las observaciones planteadas.

Riesgos

- ✓ Análisis de impacto no evaluados pueden ocasionar errores graves que conlleven a cambios emergentes concurrentes.
- ✓ Errores funcionales en la operación del aplicativo y no de acuerdo a requerimientos de los usuarios.
- ✓ Perdida de seguimiento a los cambios en aplicaciones por soporte de documentación inexistentes.

Recomendaciones:

A. Mantener debidamente documentada, revisada y formalmente aprobada el registro de aceptación de todos los participantes en

cada una de las fases de pases a producción.

B. Cumplir con lo descrito en los procesos, documentar los análisis de impacto para todos los requerimientos o proyectos que sean tratados a nivel de desarrollo de todas las plataformas.
C. Generar documentación que evidencie el cumplimiento de los controles establecidos en el manual de procedimientos.
D. Implementar mecanismos de control y pistas de auditorías de todas las actividades realizadas por el usuario contingencia las misma que debe ser monitoreado por un responsable.
E. Implementar procesos de mantenimientos y monitoreo a las bases de datos SQL
F. Cumplir lo señalado en los manuales de la Compañía respecto a la prohibición de utilizar datos reales en el ambiente de desarrollo, especialmente números de tarjeta.
G. Implementar un control que analice por muestreo los archivos utilizados en el ambiente de desarrollo con la finalidad de comprobar que no existen datos reales en ellos. Este control podría incorporarse a la lista de revisiones periódicas que realiza el Oficial de Seguridad Lógica.
H. Generar documentación que evidencie el cumplimiento de los controles establecidos en el manual de procedimientos.

Comentarios de la Gerencia:

Manejo de Cambios

Observaciones:

De nuestra evaluación a los Manejo de Cambios a los aplicativos se observó lo siguiente:

A. El requerimiento 12161 ingresado en Junio del 2010 por el Gerente de Desarrollo y puesto a producción en 7/Ene/2011 fue aprobado para la ejecución del desarrollo y certificación del usuario por una la misma persona, el Gerente de Desarrollo. La certificación del usuario debe realizada por la persona que va a usar la herramienta u opción implementada.

B. En las actualizaciones de objetos en bases de datos para plataformas SQL-server no se evidenció el análisis de impacto que el DBA-SQL debe realizar para los cambios o actualizaciones en el modelo de datos como lo indicado en el Manual de Procedimientos de Bases de datos, actualizado 23/Diciembre/2010 del Proceso de Actualización de objetos de bases de datos dice: " El DBA-SQL realiza adicionalmente un análisis de impacto para medir el esfuerzo que implicaría crear o modificar las estructuras solicitadas si fuera el caso"

C. Se pudo evidenciar dentro de los requerimientos ingresados por intranet para los diferentes tratamientos en desarrollo de las diferentes plataformas, que 10 requerimientos de ellos han sido aproados por el DBA-SQL para la ejecución del desarrollo no contemplando en ningún proceso descrito en los manuales existentes de desarrollo el nivel de jerarquía para aprobar requerimientos del área de desarrollo.

Requerimiento	Descripcion Formulario	Estado	Usuario Autorizador	Fecha Ultima Aprobacion
12092	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	24/03/2011
12440	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	24/03/2011
12859	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	11/01/2011
13162	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	10/05/2011
13191	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	03/05/2011
13269	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	24/03/2011
14320	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	15/06/2011
14321	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	15/07/2011
14678	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	13/07/2011
14804	Mantenimiento y Desarrollo Otras Plataformas	PU	gye\walmeida	26/07/2011

D. Reversos de Pases a Producción

No se evidenció el respectivo análisis de impacto funcional en los soportes de Solicitud de Procesos especiales como lo indica el Manual de Procedimiento de Desarrollo y mantenimiento que dice: “Todo reverso debe mantener un previo análisis de impacto por los Analistas de Desarrollo, Gerencia de Desarrollo y/o Administradora de Base de Datos” y de acuerdo a la Norma de seguridad de la compañía basada en PCI dice: Todo desarrollo o cambio en las aplicaciones de Credicard S.A. debe incluir un análisis de impacto o incidencia en el negocio, en la base y en los usuarios, el análisis será aprobado de La Gerencia de Tecnología & Desarrollo o su delegado.

E. Se encontraron 22 formularios sin la respectiva aprobación de un superior para la ejecución de los cambios en producción, incumpliendo la política descrita en el Manual de Procedimiento de Desarrollo que dice:” Todo reverso debe ser registrado en el formulario “Solicitud de Procesos Especiales” manteniendo la debida aprobación de la Gerencia de Desarrollo y/o Administrador de Bases de datos y Jefe de Producción.”

F. De una muestra tomada 50 formularios, se encontraron 8 formularios de Solicitudes de procesos especiales solicitados por el Administrador de bases de datos para algún reverso de Pases a Producción, siendo estos formularios aprobados por la misma DBA, lo que estaría siendo juez y parte en los cambios y controles realizados en producción.

G. Se evidencio en las Solicitudes de Procesos especiales la falta de datos en los campos Fecha y Hora de ejecución de los reversos de pases a producción y sin adjuntos de impresión de

log con evidencia de la ejecución exitosa del reverso, ocasionando la pérdida de control de seguimiento sobre los cambios realizados.

Riesgos:

- ✓ La ausencia de controles de cambios puede ocasionar que modificaciones no autorizadas en las aplicaciones se ejecuten.
- ✓ Segregación de funciones mal definidas.

Recomendaciones:

A. Las certificaciones de los cambios en aplicaciones, programas deben ser certificados y evaluados por el usuario que vaya a utilizar la herramienta o aplicación.
B. Para los cambios o actualizaciones en el modelo de SQL – server realizar el análisis de impacto funcional y/o operacional según lo descrito en su manual de administración de bases de datos.
C. Revisar la segregación de funciones entre el DBA-SQL y desarrolladores.
D. Formalizar el respectivo análisis de impacto para los reversos de pases a producción.
E. Regularizar las debidas aprobaciones antes de ser ejecutados los pases o cambios en producción.
F. Los reversos de pases a producción deben ser aprobados por el Gerente del área de desarrollo.
G. Llenar fielmente los campos de fecha y hora de los reversos realizados en producción para que no se pierda el control de los cambios realizados en el sistema.

Comentarios de la Gerencia:

ANEXOS

Information Systems Audit and Control Association
www.isaca.org

GenericApplicationReview

AUDIT PROGRAM
&
INTERNAL CONTROL QUESTIONNAIRE

The Information Systems Audit and Control Association

With more than 23,000 members in over 100 countries, the Information Systems Audit and Control **Association**® (ISACA™) is a recognized global leader in IT governance, control and assurance. Founded in 1969, ISACA sponsors international conferences, administers the globally respected CISA® (Certified Information Systems Auditor™) designation earned by more than 25,000 professionals worldwide, and develops globally applicable information systems (IS) auditing and control standards. An affiliated **foundation** undertakes the leading-edge research in support of the profession. The **IT Governance Institute**, established by the association and foundation in 1998, is designed to be a "think tank" offering presentations at both ISACA and non-ISACA conferences, publications and electronic resources for greater understanding of the roles and relationship between IT and enterprise governance.

Purpose of These Audit Programs and Internal Control Questionnaires

One of the goals of ISACA's Education Board is to ensure that educational products developed by ISACA support member and industry information needs. Responding to member requests for useful audit programs, the Education Board has recently released audit programs and internal control questionnaires on various topics for member use through the member-only web site and K-NET. These products are intended to provide a basis for audit work.

E-business audit programs and internal control questionnaires were developed from material recently released in ISACA's *e-Commerce Security Technical Reference Series*. These technical reference guides were developed by Deloitte &Touche and ISACA's Research Board and are recommended for use with these audit programs and internal control questionnaires.

Audit programs and internal questionnaires on other subjects were developed by ISACA volunteers and reviewed and edited by the Education Board. The Education Board cautions users not to consider these audit programs and internal control questionnaires to be all-inclusive or applicable to all organizations. They should be used as a starting point to build upon based on an organization's constraints, policies, practices and operational environment.

Disclaimer

The topics developed for these Audit Programs and Internal Control Questionnaires have been prepared for the professional development of ISACA members and others in the IS Audit and Control community. Although we trust that they will be useful for that purpose, ISACA cannot warrant that the use of this material would be adequate to dischargethe legal or professional liability of members in the conduct of their practices.

September 2001

Generic Application Review
Audit Program and ICQ

Get Preliminary Information	***Procedure Step:*** Determine personnel responsible		*Comments:*
	Details/Test: • Determine which IT specialist and which primary users are responsible for the oversight of this application.		

Get Preliminary Information	***Procedure Step:*** Research Vendor on-line		*Comments:*
	Details/Test: • Research the vendor and the application on-line. - Note any generic or specific problems.		

Get Preliminary Information	***Procedure Step:*** Technical/Information Systems		*Comments:*

	Details/Test: • Determine what hardware is used to run the system. - Classify the system as micro, LAN, client/server or mainframe based. • Determine what operating system is used to control the environment, and what tracking mechanisms are in use. • Determine if the software was purchased or developed in-house. - When it was developed and what modifications have been made since the initial development? • If the software was purchased, determine if any vendor warranties are still in force. - Determine if the vendor is financially sound and if the software is held in escrow. • If the software was developed in-house, verify that the software was developed and updated based on a sound systems development methodology. • Identify the programming languages used in the application. - Determine who is responsible for normal and abnormal maintenance. - If responsibility is in-house, determine if the IS department has programming staff knowledgeable in these programming languages. • Determine whether the system processes data on-line, by batch or in combination. - Identify the types of data files used in processing (database, sequential files, disk, tape). • Identify the primary transaction, master and reference files used in processing, and where they come from (data entry, automatic transfer, polling, etc). • Determine how the IS department controls and secures access to the application programs and data. - Identify the access facility to control basic sign-on and any others such as database task definitions, file and record restrictions, biometrics, etc. • Determine if passwords are entered in such a way that they are not displayed. - Are they supplemented by biometrics, tokens, etc.? • Evaluate the quality of the programmer application documentation. (This should include system and program flowcharts, decision tables, file layouts, data element definitions, narratives, source program listings, record of changes. The documentation should also indicate on which platform the various portions of the system operate). • Evaluate the quality of the application operations documentation. (This should include job and system flowcharts, input and output descriptions, job frequency and sequence of operation, job restart/recovery procedures, file backup requirements and procedures, error messages and reconciliation techniques, report distribution procedures, data capture instructions). • Determine if backup copies of application program and operations documentation are stored off-site. • Determine if the IS department monitors processing flows to verify application programs run according to schedule.

Generic Application Review
Audit Program and ICQ

Get Preliminary Information	***Procedure Step:*** End-Users		*Comments:*
	Details/Test: • Determine if the organization practices data ownership. - If so, identify and interview the data owners to determine if they understand their roles and responsibilities. - Evaluate whether user access coincides with assigned responsibility. • Interview a sample of end-user managers to determine end-user management attitudes regarding the quality and effectiveness of the system. • Determine from end-user management what they perceive to be the risks, exposures and limitations associated with the system. • Determine the number of end-users working with the system, their locations and responsibilities associated with the system. - Obtain an organization chart for these positions and people. • Determine if this application generates data for legal or regulatory agencies. - If so, pay extra attention to these transactions. • Evaluate the quality of end-user documentation (This should include description of the system, description of source documents and procedures for their preparation, job submission procedures, control procedures, error identification and correction procedures, description of output reports and their use). • Identify the application training available for end-users. - Evaluate this training to determine if it is adequate, current and available for new people. - Determine how much training has actually been provided. • Determine if end-user activity is adequately supervised.		

Get Preliminary Information	***Procedure Step:*** System Interfaces		*Comments:*
	Details/Test: • Detail what happens when other applications interface (manually or electronically) with this application. - Document what is received from and what is sent to these other applications. • Determine how end-users verify or establish assurances that interfaces are providing complete, accurate and authorized data.		

Generic Application Review
Audit Program and ICQ

Get Preliminary Information	***Procedure Step:*** File Handling		*Comments:*
	Details/Test: • Determine the retention periods for the various key application data files. - Evaluate if the retention periods satisfy management reporting, IRS reporting, other legal and internal accounting requirements. • Determine if end-user management and data owners are aware of the retention periods of the various key application data files, and if these managers are satisfied with the length of retention. Determine whether actual retention is consistent with requirements.		

Get Preliminary Information	***Procedure Step:*** Backup and Recovery		*Comments:*
	Details/Test: • Identify the key system files and evaluate whether the files are appropriate. - Determine how often key files are backed up. - Determine if copies of these backup files are stored at a suitable off-site facility. • Verify that the off-site backup file storage facilities are secure. • Determine if application recovery plans exist (both technical and end-user) for restoring from short-term and long-term interruption of computer processing. - Verify that these plans address both technical restoration needs and alternative end-user processing procedures. • Determine if these application recovery plans have been tested in the last year. - Evaluate the results. • Establish how long the organization could comfortably function and avoid significant financial loss if the computerized aspects of this application failed. - Verify that restart/recovery and disaster recovery plans provide for restoring this application in the time needed to avoid significant financial loss. - Evaluate alternative plans should the application not be able to be restored in time. • Determine if the IS department has established data file and record retention periods. - Determine if these retention periods are reasonable for backup, disaster/recovery and audit purposes. • Verify that restart/recovery plans from short-term computer interruptions include the ability to identify the status of all processing to the point of application failure to establish a cutoff for transaction re-entry.		

Get Preliminary Information	***Procedure Step:*** Identify all subsystems		*Comments:*
	Details/Test: • Identify all subsystems associated with this application.		

Generic Application Review
Audit Program and ICQ

Application Generic Controls	***Procedure Step:*** Data Origin	***Objective:*** To determine that controls over the preparation, collection, and processing of source documents ensure the accuracy, completeness, and timeliness of data before they reach the application.	*Comments:*
	Details/Test: • Review the source document(s) and determine that the document design contributes to the accuracy and efficiency of the input. Identify any cost beneficial improvements in source documents and related forms. • Determine that source document(s) are retained for an effective period of time.		

Application Generic Controls	***Procedure Step:*** Data Input	***Objective:*** To determine that manual and automated controls over data entry (batch or online), data validation, error identification and reporting, and error correction and reentry are effective to ensure that data are completely and accurately entered into the application.	*Comments:*
	Details/Test: • Determine that data entry procedures and controls are effective to ensure complete and accurate input of data. • Determine that online edit routines identify inaccurate data as early as possible and prevent the entry of invalid/duplicate/out of period data into the system. • Determine that invalid data is properly rejected during subsequent processing of data input. • Review transactions and determine that the screens are effective and useful. • Determine that controls over correcting errors are effective and that errors are corrected and resubmitted on a timely basis. Identify any cost beneficial improvements in error correction procedures.		

Generic Application Review
Audit Program and ICQ

Application Generic Controls	***Procedure Step:*** Processing	***Objective:*** To determine that controls over application programs and related computer operations ensure the accuracy, completeness, and timeliness of data during batch or real time processing.	*Comments:*
	Details/Test: • Determine that job documentation is accurate and effective for proper scheduling and restart/recovery. • Review user and IT data control procedures relating to job scheduling to ensure that jobs are run in the correct sequence, and that no data is inappropriately added, changes or lost during processing. • Review the IT problem reports to identify problems relating to the application system. - Determine that production problems are identified and resolved on a timely basis. - Determine if any significant problems are not reflected on the problem reports and follow up as required.		

Application Generic Controls	***Procedure Step:*** Storage and Retrieval	***Objective:*** To determine that controls over file handling, file access, and backup and recovery are effective to ensure the completeness and accuracy of data during the process of data storage and retrieval.	*Comments:*
	Details/Test: • Determine that effective backup and recovery procedures have been established and properly tested and that critical system files and programs are stored at an offsite location.		

Generic Application Review
Audit Program and ICQ

Application Generic Controls	***Procedure Step:*** Output	***Objective:*** To determine that controls over balancing and reconciliation, distribution of output, handling of negotiable documents, and output retention are effective to ensure that output is accurate and distributed to authorized personnel on a timely basis.	*Comments:*
	Details/Test: • Review output distribution to determine that output is distributed on a timely basis only to authorized personnel and that restricted output is properly labeled. • Review user balancing and reconciliation procedures to ensure that out of balance conditions are resolved on a timely basis. • Review reports generated with users and determine their necessity and usefulness. - Determine if any reports could be eliminated or if any additional reports could be beneficial. - Determine that reports are retained for proper periods of time. • Review controls over handling of negotiable documents if any.		

Application Generic Controls	***Procedure Step:*** Review change control		*Comments:*
	Details/Test: • Determine program change requests are documented in writing, that users assist in developing test data, review test results, and approve all program changes in writing prior to being placed into production. • Review controls over changes to user developed programs (if these programs perform significant processing).		

Application Generic Controls	***Procedure Step:*** Measure user satisfaction		*Comments:*
	Details/Test: • Survey a sample of users to determine the degree of user satisfaction with the system.		

Detalle de Información Requerida para la Auditoría al Desarrollo de Aplicaciones
31 de Junio del 2011

No.	Descripción	Responsable

No.	INFORMACION DE TECNOLOGIA – DESARROLLO	
1	Organigrama funcional actualizado del área de Tecnología del Grupo debidamente aprobado.	
2	Descripción de las funciones y responsabilidades que ejercen los integrantes del área así como el nivel de reporte de los mismos.	
3	Descripción del sistema bancario instalado cubriendo los siguientes aspectos: Detallar: Nombre, proveedor, versión del mismo y los módulos que lo conforman. la plataforma de desarrollo, bases de datos y producción utilizada para las aplicaciones más críticas, así como la existencia de otras plataformas paralelas para la utilización del aplicativo a nivel de Internet. Número de licencias instaladas a nivel de servidores y de estaciones de trabajo.	
4	Detalle de inventario de software instalado en equipos (incluir el software utilizado para el desarrollo de sistemas y las licencias adquiridas para servidores), el que debe incluir: Nombre y tipo de software Versión Descripción de los módulos y opciones Número de licencias instaladas de cada software	
5	Detalle de los procedimientos del área de sistemas relacionados con: Cambios a programas y versiones de sistemas, así como nuevos desarrollos. Procedimientos relacionados al manejo de: Programas Fuentes Programas Objetos Versiones de Ejecutables Directorio de Pruebas Pases de desarrollo a pruebas Pases de pruebas a Producción Autorizaciones sobre las Bases de Datos. Procedimientos que maneja el banco al respecto de este punto.	
6	Detalle de los procesos Batch a nivel de cada aplicativo incluyendo descripción y procedimientos de control aplicados para cada proceso y nombre del personal responsable de su ejecución.	
7	Copia de contratos vigentes con terceros por concepto de prestación de servicios de: Prestación de servicios de desarrollo	
8	Descripción de los pasos que sigue el personal de tecnología con respecto a las autorizaciones de pases a producción como resultado de trabajos realizados en:	

Detalle de Información Requerida para la Auditoría al Desarrollo de Aplicaciones
31 de Junio del 2011

No.	Descripción	Responsable
	Cambios a estructuras (Tablas de Sistemas) Creación de nuevas estructuras Control de las estructuras definidas en ambiente de desarrollo Detallar el personal responsable que interactúa en las definiciones, autorizaciones y ejecución de los puntos anteriores.	
9	Documento de Plan de Aseguramiento de la Calidad del Software (SQAP)	
10	Detalle de los cambios más significativos realizados a los sistemas y nuevos desarrollos durante el año 2010 (seguimiento) y 2011.	
11	Detalle de los proyectos a corto y mediano plazo que se encuentran vigentes o para implementación. Describir el nombre del proyecto y su función.	

Verificación de Controles

Empresa			
Area Auditada		Fecha:	
Auditado:		Página #:	

Numeral	Descripción	Sí	No	Comentarios
	Entorno Organizacional			
1	¿Existe el documento que contiene las funciones que son competencia del área de desarrollo, esta aprobado por la dirección de sistemas y se respeta?	x		Manual de Funciones de Div. De Tecnologia y Desarrollo
2	Se mantiene segregación de funciones de empleados	x		
3	Existe un procedimiento de aprobación de nuevos proyectos?	x		Existe un flujo de aprobaciones
	Adminstración de la Calidad			
4	¿Se tiene implantada una metodología de desarrollo de sistemas de información (SLDC) soportada por herramientas de ayuda?	x		Si mantienen una estructura de metodologia pero no automatizada
5	¿La metodología (SLDC) cubre todas las fases del desarrollo y es adaptable a distintos tipos de proyectos?		x	Para proyectos en ambiente WEB no mantienen estandares
6	Cuando fue la ultima vez que se actualiazò la metodologia (SLDC)			
7	¿La metodología y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y a la organización del área de desarrollo?	X		se apoyan en la metodologa de proyectos
8	¿Se registran y controlan todos los proyectos fracasados o en stand by?		x	A nivel de sistemas no se los mide, sino a nivel de estrategias de negocio
	Adquirir y mantener el software aplicativo			
9	Cuando existe la necesidad de una nueva aplicación o desarrollo, se realiza una revisión de factibilidad tecnologica y recurso humano ?	X		Existe un comité de requerimientos
10	Existen definiciones claras de requerimientos funcionales y tecnicos que cubran el alcance de todos los cambios requeridos en el sistema.	x		Documento de Definicion del Requerimiento # Los reque. Funcionales no estan documentados
11	Proporciona un documento inicial de definición del proyecto que incluya estatus claros sobre la naturaleza y alcance del proyecto	X		
12	¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuario o guías de instalación pueden ser modificados o creados, si fuese necesario	x		De acuerdo a la necesidad
13	Considera que es adecuado el numero de personal que labora en la empresa	x		
14	Por cada cambio y/o modificaciòn quese vaya a realizar existe un analisis de impacto en el modelo de datos y sus afectaciones ?	x		Si lo realizan pero no existe documentación formal
15	Existen mecanismos adecuados para la definición y documentación de los requerimientos de entrada para cada proyecto nuevo de desarrollo o modificación de sistemas	x		
16	Éxiste un Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de documentación		x	
17	Existe algún procedimiento, Bitácora de creación, modificación o eliminación de tablas, Vistas, o campos de las BD en Desarrollo y Producción	x		Para el STC:EL control lo mantienen en la misma aplicación, existe un procedimiento y formulario para la creacion de tablas, vistas o campos en el modelo de negocio. Para los SQL Server no existe una bitacora, unicamente se manejan con los documentos de soportes no secuenciados.
18	¿Existe un catalogo de las aplicaciones disponible en el área?	x		

Verificación de Controles

Empresa	Procesadora de Tarjetas de Credito		
Area Auditada	Desarrollo	Fecha:	
Auditado:	Gerente de Desarrollo	Página #:	

Numeral	Descripción	Sí	No	Comentarios
19	Existe un control de aplicaciones que se encuentran en uso y se les da el debido manejo.		x	En la aplicación mismo controlan el uso de la misma
20	¿Existen procedimientos formales para la operación del Sistema de Gestion de Bases de datos (SGBD) ?	x		
22	¿Se tiene un responsable del SGBD?	x		ADM - Iseries ADM-SQL
23	Se mantiene un registro permanente (Bitácora) de las nuevas aplicaciones modificadas e identificadas por cada proyecto?	x		
24	¿Se reflejan el software codificado tal como se diseñó en la documentación?		x	Existe una documentacion que es propia de la aplicación, y no todos los desarrolladores documentan sus desarrollos
25	Se preparan especificaciones detalladas de programas para cada proyecto de desarrollo o modificación de información, y que estas especificaciones concuerdan con las especificaciones del diseño del sistema		x	No para todos los casos.
	Se especifican mecanismos adecuados para asegurar los requerimientos de seguridad y control internos para cada proyecto nuevo de desarrollo o modificación de sistemas		x	
13	Se deja de realizar alguna actividad por falta de personal		x	
26	Existe un mecanismo de evaluación del versionamiento que permita el control de mismo.	x		La herramienta controla este proceso
Administración de cambios				
27	Existe un procedimiento formal de aceptación de cambios propuestos a los sistemas de procesamiento de información?	x		
28	Se consideran procedimientos de cambios de emergencia en los manuales de operaciones.	x		Aplican formularios de control
29	Existe un responsable en caso de falla de los sistemas o aplicaciones	x		Analistas de desarrollo por modulos
30	Los cambios a los sistemas de procesamiento de información son comunicados a todas las personas relevantes?	x		Gerentes, lideres de proyecto, usuarios
31	Existe personal con autoridad sufuciente que es el que aprueba los cambios en las aplicaciones por otras, y las solicitudes de nuevas aplicaciones	x		
Instalar y acreditar soluciones y cambios				
32	Se realizan pruebas de calidad para garantizar eficacia en la puesta a Producciòn los sistemas nuevos, o cambios realizados.	x		
33	Los sistemas de ambiente de pruebas emulan los ambientes operacionales con la suficiente precisión?	x		
34	Existe evaluacion del usuario de las aplicaciones modificadas	x		
35	¿Se cumplen las especificaciones de la documentación del usuario del software?	x		
36	Como se mide el rendimiento de las aplicaciones y bases de datos puestas en producciòn (Web, stacion)	x		Mantienen indicadores con las franquicias, para los ambientes web realizan monitoreo al rendimiento de las bases
37	Se realiza el monitoreo de las mejoras realizadas en el sistema, cuanto tiempo y como son tratadas.	x		

Verificación de Controles

Empresa	Procesadora de Tarjetas de Credito		
Area Auditada	Desarrollo	Fecha:	
Auditado:	Gerente de Desarrollo	Página #:	

Numeral	Descripción	Sí	No	Comentarios
38	La Transferecia de conocimiento al usuario final se realiza por cada aplicación modificada, realizada	x		
39	¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?	x		