Banco Popular y de Desarrollo Comunal

Dirección Tecnología de Información

Proceso Control Operativo

Informe de Cierre de Gestión al 31 de julio 2010

Autor: Jorge Mayorga Castillo

Versión: 1.0
Agosto, 2010

Tabla de Contenidos

1. Antecedentes

En este apartado se presentan los objetivos, organización y funciones del Proceso Control Operativo, esto con el propósito de que sean tomados en consideración delimitar el alcance de este informe.

1.1 Objetivo

Realizar las funciones generales asociadas a la administración de las diferentes contrataciones externas que requiere el Banco, en materia tecnológica, una función centralizada para el manejo de la seguridad operativa y seguimiento de las directrices, normativas y políticas asociadas a la seguridad informática.

Servir de enlace con las Entidades o áreas reguladoras “SUGEF, Auditorías Externas, Auditoría Interna” y será el área responsable para la implantación del Modelo de Control (COBIT).

Comunicar los objetivos de servicio, políticas y procedimientos, etc., aprobados y soportados por la administración.

Adquirir, mantener y motivar una fuerza de trabajo competente para la creación y suministro de los servicios de TI para el negocio.

Crear y mantener un marco de administración de riesgos. Documentando un nivel de común acuerdo para los riesgos de TI, las estrategias de mitigación y los riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización acusado por un evento no planeado deberá ser identificado, analizado y determinado. Las estrategias de mitigación del riesgo deben ser adoptadas para minimizar el riesgo residual para un nivel aceptable. El resultado de la determinación debe ser entendible para los usuarios permitiendo alinear los riesgos en un nivel aceptable de tolerancia.

Establecer un programa de control interno eficaz para la supervisión de los requerimientos de TI. Este proceso incluye la supervisión y la divulgación de las excepciones de control, de los resultados de autoevaluaciones y de las revisiones de entes externos. Proporcionando aseguramiento con respecto a operaciones eficaces y eficientes de conformidad con leyes y regulaciones aplicables.

Establecer un proceso independiente de revisión para asegurar conformidad con leyes y regulaciones.

1.2 Objetivos específicos

- Proporcionar mecanismos de control mediante normativas (metodologías; instrumentos, estándares, procedimientos y otros mecanismos de control de calidad) los cuales aseguren la operatividad de las plataformas tecnológicas del Banco.

- *Coordinar la recepción de eventos dentro de la Dirección, con el fin de que éstos reciban un servicio eficiente y efectivo.*

- Controlar los procesos de cambios dados por adición de nuevos elementos, retiros, “upgrades” o modificaciones en el ambiente de Tecnología de Información.

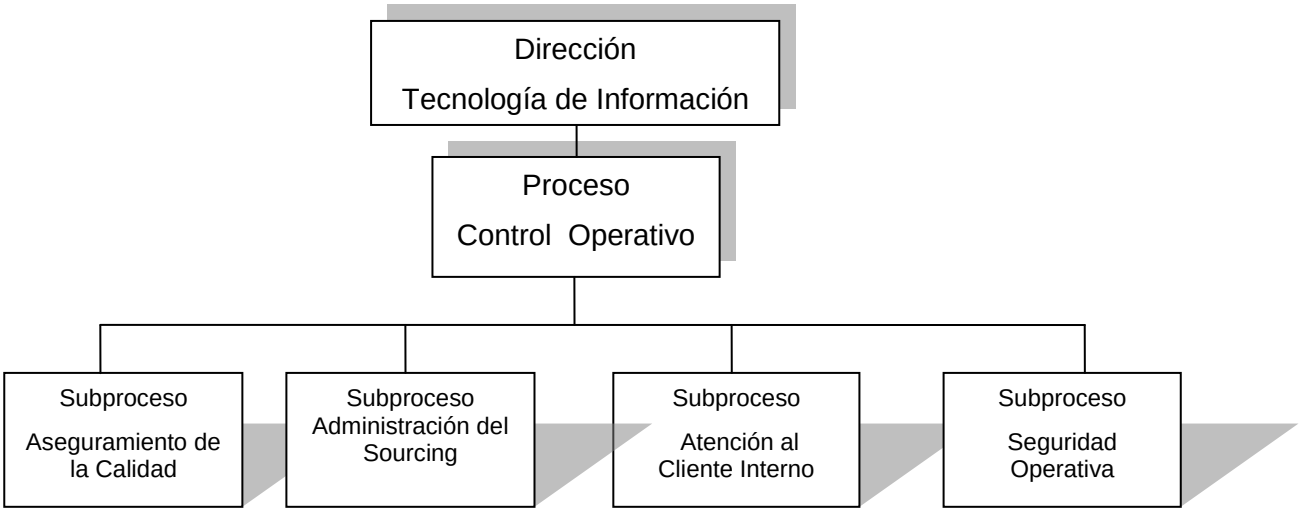
- Vigilar la operatividad de la red de telecomunicaciones del Banco Popular, con la finalidad de mantener la interconexión de la red así como la conectividad a la Internet, a fin de dar un servicio ágil, seguro y oportuno a los clientes y usuarios de la Institución.

- Ejercer el control y seguimiento del presupuesto y de los diferentes procesos de licitación relacionados con Tecnología de Información, con el fin de lograr que se cuente con los recursos necesarios en forma oportuna para apoyar las labores de todas las dependencias del Macro Proceso.

- Planear, coordinar y administrar los servicios de Seguridad de la Información en la organización con el fin de garantizar una seguridad razonable en todas las operaciones realizadas, a través del establecimientos de procesos, normas, reglas, políticas y estándares que aseguren una adecuada protección de los recursos informáticos.

- Garantizar que se cumplan los objetivos del Plan Anual Operativo.

1.3 Estructura Funcional



1.4 Funciones del área

El Proceso Control Operativo debe cumplir las siguientes funciones, de manera que el adecuado cumplimiento de éstos asegure a la Dirección de Tecnología de Información y al Banco el alcance de los objetivos propuestos, en apego a las normativas internas y externas, y leyes vigentes.

Las siguientes funciones fueron tomadas y adaptadas del modelo COBIT, el cual contiene las mejores prácticas de control en Tecnología de Información.

Marco del proceso de TI

Definir un marco del proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye una estructura de procesos de TI y sus relaciones (por Ej.: del proceso de administrar brechas y sobreponer funciones), dueños del producto, madurez, niveles de servicio, mejoras, aceptación, puntos de calidad y planes para archivarlo. El marco provee integración entre los procesos que son específicos de TI, administración del portafolio de la empresa, procesos del negocio y procesos de cambio del negocio. El marco de los procesos de TI deberá ser integrado en un sistema de manejo de la calidad y al marco de control interno.

Comité del manejo de TI

Participar activamente en un comité del manejo de TI (o su equivalente) compuesto por ejecutivos, el negocio y administradores de TI para:

• Determinar la priorización de los programas de inversión permitidos para TI en línea con las estrategias del negocio y las prioridades

• Dar seguimiento a los proyectos y resolver conflictos de recursos

• Monitorear los niveles de servicio y el mantenimiento de las mejoras

Responsabilidad de Aseguramiento de la Calidad

Asignar responsabilidad para la función de aseguramiento de la calidad y proveer a los sistemas de garantía de calidad apropiados, controles y experiencia en comunicaciones. El lugar organizacional, las responsabilidades y el tamaño del grupo de aseguramiento de la calidad deben satisfacer los requerimientos de la organización.

Responsabilidad en cuanto a riesgos, seguridad y aceptación

Definir y asignar roles críticos para administrar los riesgos de TI incluyendo la responsabilidad específica de la seguridad de la información, seguridad física y lógica.

Establecer riesgos y responsables de la administración de la Seguridad a nivel organizacional. Como parte de la administración de las responsabilidades de la seguridad puede ser necesario asignar diferentes niveles de seguridad. Obtener las directrices de cualquier riesgo, así como del riesgo residual de TI.

Datos y propietarios de sistemas

Proveer al negocio con procedimientos y herramientas que permitan asignar responsabilidades de propietarios de la información y de los sistemas de información. Los dueños deben tomar decisiones acerca de la clasificación de la información, los sistemas y protegerlos de acuerdo a esta clasificación.

Políticas de TI y ambiente de control

Definir los elementos de un ambiente de control para TI, alineado con el estilo y funcionamiento de la empresa. Estos elementos incluyen expectativas/requisitos con respecto a la entrega del valor de las inversiones de TI, riesgo, integridad, los valores éticos, capacidad del personal y responsabilidad. El ambiente del control se basa en una cultura que apoye el valor mientras que maneja riesgos significativos, anima la cooperación y el trabajo en equipo cruzado, promueve conformidad y la mejora de proceso continua y maneje desviaciones de proceso.

Riesgos empresariales de TI y marco interno de control

Desarrollar y mantener un marco que establezca los riesgos y el control interno para entregar valor mientras que protege los recursos y los sistemas. El marco deberá estar integrado con los procesos de TI y el sistema de administración de la calidad, y se complementa con los objetivos del negocio. Debe estar dirigido al éxito de la entrega del valor mientras que reduce

al mínimo riesgos a los activos de la información con medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la recuperación oportuna de los activos del negocio.

Administración de políticas de TI

Desarrollar y mantener un conjunto de políticas para soportar la estrategia del negocio. Estas políticas deberán incluir políticas de pruebas, roles y responsabilidades, procesos de excepción, aceptación, conformidad y referencias a procedimientos, estándares y guías. Las políticas deberán estar direccionadas a tópicos como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia deberá ser confirmada y aprobada regularmente.

Políticas de involucramiento

Asegurarse que las políticas de TI involucren a todo el personal relevante, de manera que estén cubiertos los desarrolladores, que son una parte integral de las operaciones de la empresa. El método de implantación debe direccionar los recursos y las necesidades e implicaciones del conocimiento.

Comunicando los objetivos y la dirección de TI

Asegurarse de que el conocimiento y entendimiento del negocio, así como de los objetivos de TI y la dirección estén comunicados a través de la empresa. La información comunicada debe abarcar una misión claramente articulada, objetivos del servicio, seguridad, controles internos, calidad, código de ética/conducta, políticas y procedimientos, etc., y será incluida dentro de un programa continuo de la comunicación, apoyado por la dirección en acciones y palabras. La dirección debe dar atención específica para comunicar la conciencia de la seguridad y el mensaje de que seguridad es responsabilidad de cada uno.

Reclutamiento y retención del personal

Asegurarse que el proceso de reclutamiento de personal de TI está de acuerdo con todas las políticas y procedimientos del personal de la organización (por ejemplo: emplear, ambiente de trabajo positivo y orientación). La administración del proceso de implementación debe asegurarse que la organización tiene un apropiado desarrollo de la fuerza de trabajo de TI y que tiene las habilidades necesarias para alcanzar las metas de la organización.

Competencias del personal

Verificar regularmente que el personal tiene las competencias que satisfacen sus roles sobre la base de la educación, entrenamiento y/o experiencia. Definir los requerimientos de la competencia del Core de TI y verificar que son mantenidas usando programas de calificación y certificación apropiadas.

Roles del personal

Definir, monitorear y supervisar roles, responsabilidades y marcos de compensación para el personal, incluyendo lo requerido para adherir políticas y procedimientos, así como el código de ética y prácticas profesionales. Los términos y las condiciones para emplear deben crear en el empleado la responsabilidad de la seguridad de la información, el control interno y cumplimientos regulatorios. El nivel de supervisión debe estar de acuerdo con la sensibilización del puesto y el grado de responsabilidad asignada.

Entrenamiento del personal

Proveer al empleado de TI la orientación apropiada para mantener su conocimiento, habilidades, capacidades, controles internos y conocimiento de la seguridad en el nivel requerido para alcanzar las metas de la organización.

Dependencia sobre individuos

Minimizar la exposición de dependencias críticas sobre individuos clave capturando el conocimiento por medio de Documentación, compartiendo el conocimiento, planes de sucesión y personal de respaldo.

Identificación de eventos

Identificar cualquier evento (amenaza y vulnerabilidad) con un impacto potencial sobre las metas u operaciones de la empresa, incluyendo el negocio, regulatorios, legales, tecnológicos, socios de negocio, recurso humano y aspectos operacionales. Determinar la naturaleza del impacto— positivo, negativo o ambos—y mantener esta información.

Determinando riesgos

Determinar sobre una base recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad y el impacto asociado con riesgos inherentes y residuales deben ser determinados individualmente por categoría y sobre un portafolio base.

Respuesta al riesgo

Identificar un propietario del riesgo y un propietario de proceso afectado, desarrollar y mantener una respuesta al riesgo para asegurar el control del costo-beneficio y medidas de seguridad que atenúen la exposición al riesgo sobre la base de la continuidad. La respuesta al riesgo debe identificar estrategias de riesgo tales como evitar, reducir, compartir y aceptar. Al desarrollar la respuesta se deben considerar los costos y beneficios, seleccionar respuestas que consideren costos y beneficios y responder a los riesgos residuales obligados con los niveles de riesgos tolerancia definidos.

Mantenimiento y monitoreo del plan de acción de riesgos

Priorizar y planear las actividades de control de todos los niveles para implementar la identificación de respuestas al riesgo necesarias, incluir identificación de costos, beneficios y responsabilidad para ejecución. Aprobar búsqueda para acciones recomendadas y aceptación de cualquier riesgo residual, el asegurar acciones confiables son propiedad del dueño del proceso afectado. Monitorear la ejecución de los planes, reportes y cualquier desviación son funciones del administrador.

Monitoreo del marco de control interno

Supervisar continuamente el ambiente del control de TI y el marco. Usando las mejores prácticas de la industria y benchmarking para mejorar el ambiente del control de TI y para controlar el marco.

Control de excepciones

Registrar la información con respecto a todas las excepciones del control y el análisis de la causa subyacente y a la acción correctiva. Debe decidirse qué excepciones se comunican al individuo responsable de la función y qué excepciones deben ser extendidas. Se es responsable también de informar a otras áreas afectadas.

Aseguramiento de Control Interno

Obtener, si es necesario, revisiones independientes. Tales revisiones pueden ser realizadas por el cumplimiento corporativo o, a petición de la gerencia, por la auditoría interna o por auditores y consultores externos o por organismos de certificación. Verificar las calificaciones de los individuos que realizaban la intervención, por ejemplo: certificación de los sistemas de información AuditorTM (CISA®), deben ser aseguradas.

Control interno de terceras partes

Determinar el estado de los controles internos de cada proveedor de servicio externo. Confirmar que los proveedores de servicio externos cumplan con los requisitos legales y reguladores, y obligaciones contractuales. Esto se puede prever con la intervención de tercera persona u obtener de una revisión por la función de la auditoria y los resultados de otras auditorias.

Acciones correctivas

Identificar y emprender las acciones correctivas basadas en la supervisión, y el reporte de control. Esto incluye la supervisión y el reporte con:

- Revisión, negociación y establecimiento de las respuestas de la administración
- Asignación de la responsabilidad de la corrección
- Rastreo de los resultados de las acciones comprometidas

Autoevaluación

Evaluar la eficacia de los controles internos de la administración de los procesos de TI, las políticas y los contratos con un programa continuo de la autovaloración.

Supervisar Controles Internos

Monitorear y divulgar la eficacia de los controles internos sobre el área por medio de la revisión incluyendo, por ejemplo, la conformidad con las políticas y los estándares, seguridad de la información, controles de cambio y los controles establecidos en acuerdos de niveles de servicio.

Identificación de leyes y regulaciones que tienen impacto en TI

Definir e implementar un proceso que asegure la identificación oportuna de requerimientos legales, contractuales y políticas relacionados con la información, el servicio informativo entrega-incluyendo terceras partes- y la organización de TI, los procesos y la infraestructura. Considerar las leyes y las regulaciones para el comercio electrónico, flujos de datos, privacidad, controles internos, reportes financieros, las regulaciones específicas de la industria, propiedad y copyright intelectual, y salud y seguridad.

Optimización de respuesta a requerimientos regulatorios

Repasar y optimizar las políticas, los estándares y los procedimientos de TI para asegurarse de que los requisitos legales y reguladores están cubiertos eficientemente.

Evaluación de conformidad con requerimientos regulatorios

Evaluar eficientemente la conformidad de TI con las políticas, estándares y procedimientos, incluyendo los requisitos legales y reguladores, basados en negocio, la administración del gobierno de TI y la operación de controles internos.

Aseguramiento positivo de cumplimiento

Definir e implementar procedimientos para obtener y divulgar el aseguramiento positivo de cumplimiento y, definir cuando sea necesario, que las acciones correctivas sean tomadas por el dueño de proceso responsable sobre una base oportuna para tratar cualquier brecha de cumplimiento. Integrar los informes de TI progreso y estado de cumplimiento con salida similar a otras funciones del negocio.

Administración de riesgos

Trabajar con la Dirección para definir los riesgos de TI. Comunicar los riesgos del área y convenirlo en plan de la administración de riesgo. Tomar las responsabilidades de la

administración de riesgo, asegurándose de que TI determine y divulgue regularmente los riesgos relacionados. Cerciorarse de que la administración de TI siga en las exposiciones del riesgo, poniendo atención especial a las faltas del área y las debilidades del control y descuido internos, y a su impacto real y potencial del negocio. La posición del riesgo de TI debe ser transparente a todos los dueños de productos.

En forma general se presenta un desglose de las funciones que el Proceso Control Operativo debe realizar y que concuerdan con las actividades a realizar en todas las áreas operativas:

Cumplimiento de normativa vigente:

Los funcionarios son responsables de cumplir y hacer cumplir todas las políticas, así como las normas de control interno emitidas tanto por la Dirección como por el Banco Popular.

Adicionalmente, se deberá realizar cualquier otra función que sea asignada por el Proceso o Dirección.

2. Informe de cumplimiento de los Objetivos del Proceso

2.1 Presupuesto y Contratación Administrativa de Recursos de TI

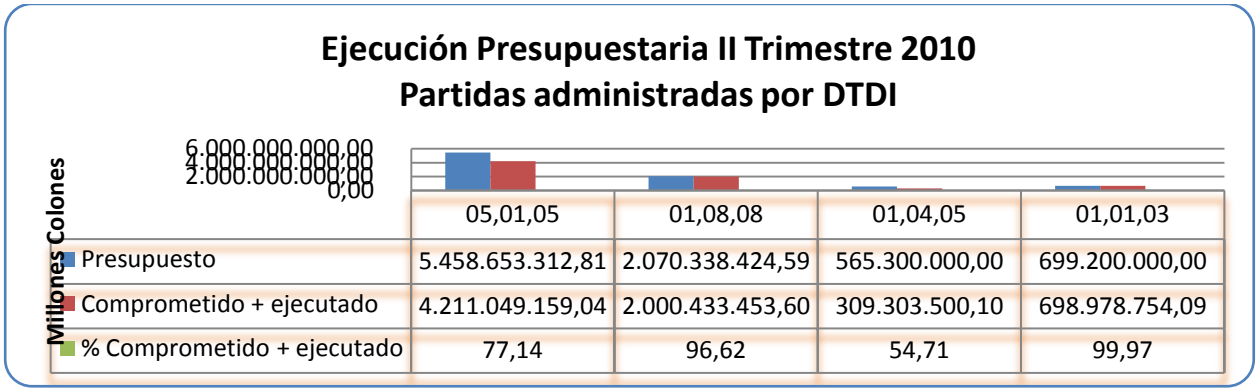
El control a la ejecución de los procesos de adquisición, relativos a la tecnología, que se llevan a cabo en el Banco, se encuentran agrupadas en las cuentas presupuestarias siguientes:

- 5.01.05 Equipo y Programas de Cómputo
- 1.08.08 Mantenimiento Equipo de Cómputo y Sistemas
- 1.04.05 Desarrollo de Sistemas Informáticos
- 1.01.03 Alquiler Equipo de Cómputo

Por lo que la consolidación, emisión, seguimiento y control del presupuesto de dichas partidas se lleva a cabo en la Dirección de TI, específicamente en el Subproceso de Administración del Sourciong, la cual depende directamente del Proceso Control Operativo.

A continuación se presente un corte al 30/06/2010 de la ejecución presupuestaria para dichas partidas:

Ejecución Presupuestaria al segundo trimestre 2010				
Partida	Presupuesto	Comprometido + ejecutado	% Comprometido + ejecutado	Disponible
05,01,05	5.458.653.312,81	4.211.049.159,04	77,14	1.247.604.153,77
01,08,08	2.070.338.424,59	2.000.433.453,60	96,62	69.904.970,99
01,04,05	565.300.000,00	309.303.500,10	54,71	255.996.499,90
01,01,03	699.200.000,00	698.978.754,09	99,97	221.245,91



Al respecto se puede indicar que, de la partida 5-01-05 se ha comprometido y ejecutado un 77,14% este resultado se deriva del compromiso de contratos que se pagan por esta partida y de todos aquellos requerimientos de equipo de cómputo para los cuales se ha generado la solicitud de compra respectiva, importante señalar que se ha realizado cesión de recursos por ¢ 13.665 millones. Respecto a la partida 01.08.08 se obtiene un compromiso más ejecución de 96,62%; como resultado de la reserva en contratos para atender las erogaciones que se derivan de estos, de igual forma para nuevos compromisos que se encuentran en trámite de adquisición., en esta partida se inyectaron ¢ 300 millones vía modificación para atender necesidades no previstas en la formulación ordinaria.

Complementariamente, el Subproceso de Administración del Sourcing controla los procesos de compra relativos a las partidas indicadas, dichos procesos se encuentran en el status que muestra la siguiente tabla:

El siguiente cuadro contiene el movimiento por estado asociado a la adquisición de bienes y servicios con cierre al mes de junio del 2010.

Estado	Suma De Monto ¢	total Estado	Periodo-Año
29 Ejecución	1.737.268.000,00	23	2009
31 Infructuosa	363.348.698,00	9	2009
32 Anulada	1.162.406.179,00	13	2009
	3.263.022.877,00	**45**	
10 Recepción de Ofertas	365.844.167,65	2	2010
15 Criterio Técnico Área Usuaria	51.199.901,00	2	2010
2 Revisión cartel	1.197.946.322,00	3	2010
21 Vº Bº Legal Informe recomendación	186.547.505,00	3	2010
22 Aprobación Comisión	449.137.360,00	5	2010
28 Refrendo CGR	46.740.000,00	1	2010
29 Ejecución	1.408.467.655,00	7	2010
30 Desierta	16.479.360,00	1	2010
31 Infructuosa	1.402.501,00	1	2010
32 Anulada	254.696.561,31	1	2010
6 Validar el Cartel Área Usuaria	252.772.876,00	4	2010
	4.231.234.208,96	**30**	

El siguiente cuadro representa el movimiento por tipo de concurso y periodo asociado, de lo cual al cierre del mes de junio se ha realizado la gestión para un total de 30 concursos que suman un importe total de ¢ 4.231.234.208,96

Tipo	Suma De Monto ¢	Total tipo	Pdo
LPUB	1.840.548.867,00	11	2009
LABR	1.299.726.083,00	22	2009
CDIRE	75.138.472,00	5	2009
CDIR	47.609.455,00	7	2009
	3.263.022.877,00	**45**	
LREG	7.950.623,00	1	2010
LPUB	1.747.091.472,00	7	2010

LABR	1.173.724.720,31	15	2010
CDIRE	1.275.408.013,65	4	2010
CDIR	27.059.380,00	3	2010
	4.231.234.208,96	**30**	

2.2 Seguridad Informática

En relación con la seguridad informática, tal como se ha mostrado en el organigrama del Proceso, a éste le reporta el Subproceso de Seguridad Operativa Informática, cuyo objetivo es:

> Planear, coordinar y administrar los servicios de Seguridad de la Información en la organización con el fin de garantizar una seguridad razonable en todas las operaciones realizadas, a través del establecimientos de procesos, normas, reglas, políticas y estándares que aseguren una adecuada protección de los recursos informáticos.

Actualmente, como resultado del trabajo de este Subproceso, el Banco Popular cuenta como una de sus ventajas competitivas, el hecho de disponer de una plataforma tecnológica con altos niveles de seguridad informática. Esto por la implementación de esquemas de control de acceso lógico superiores a la competencia en la página Web del Banco. La tecnología implementada es conocida como PKI, Infraestructura de Llave Pública, por sus siglas en inglés, la cual se ha habilitado para el uso a lo interno del Banco, lo cual la firma física podrá ser sustituida por un mecanismo de firma digital, lo cual dará un gran potencial a la organización para el ahorro en la documentación escrita.

Un aspecto relevante en la gestión del SSOI es la administración de la infraestructura de la red Microsoft del Banco, la cual es la que provee la usabilidad a todos los usuarios de la red de datos. Siendo esta una plataforma de alto impacto, se ha realizado lo requerido para la instalación y configuración del ambiente de de contingencia en el sitio alterno del Banco, con lo cual se está proporcionando la posibilidad de que en caso de un evento que interrumpa el servicio, éste podrá ser restablecido en el sitio alterno, de forma limitada, para 600 usuarios.

Con relación a la cobertura contra software malicioso (malware) el avance logrado corresponde a un 99%, con lo cual se cumple con la meta y nivel de servicio establecidos. Dicho logro se puede resumir en el indicador de desempeño que se muestra en la siguiente tabla:

Nivel Objetivo			99%		
Tipo de Equipo	**Equipos con Cobertura (*)**	**Total de Equipos**	**% Cobertura actual**	**% Cobertura corte anterior**	**Diferencia**
Servidores	259	266	99%	97%	2%
Pc´s	3594	3894	99%	92%	7%

En esta misma línea, se está con una cobertura del 60% la actualización a la versión 6 del antivirus, el restante, 40% se encuentran en versión 5, lo cual no representa riesgos.

Cabe indicar que como aspectos adicionales a los planteados a los objetivos de este Subproceso, también se han analizado, instalado y probado nuevos servicios, los cuales se indican a continuación:

Servicio de OCS, relativo a comunicaciones unificadas, el cual estuvo disponible por 6 meses para 50 funcionarios con excelentes resultados. Para proseguir con su utilización se hace requerido adquirir las licencias y asignarle los servidores.

Servicio de acceso de correo electrónico a través del teléfono celular: este servicio se ha implementado de forma exitosa para 25 usuarios. No obstante, para una mayor cobertura de usuarios se hace requerido reforzar la infraestructura y establecer la documentación operativa del servicio.

2.3 Entidades o áreas reguladoras

En lo referente al objetivo de servir como enlace de TI con las Entidades o áreas reguladoras “SUGEF, Auditorías Externas, Auditoría Interna”, se indica que:

Se coordinó durante los años 2008 y 2009 la revisión de auditoría independiente sobre los estados financieros del Banco, llevada a cabo por el despacho Lara Eduarte, S.A. Cuyo estado de recomendaciones se resumen en el siguiente cuadro:

Recomendaciones Auditoría Externa-Lara Eduarte				
Año	Cumplida	Proceso	Pendiente	Total
2009			3	3
2008	3	2		5
2007	1			1
Total	4	2	3	9

En la siguiente tabla se muestra el estatus de las recomendaciones de Auditoría Interna en las diferentes áreas adscritas a la Dirección de TI:

Área de TI	Cumplidas	Pendientes	En Proceso	Por Validar	Total Recomendaciones
Dirección Tecnología Información	21	8			29
Proceso Control Operativo	4				4
Proceso Desarrollo	17				17
Proceso Operación de Producción	10				10
Subp. Administración del Sourcing	3				3
Subp. Administración y Desarrollo Proyectos	11				11
Subp. Aseguramiento de la Calidad	10	5		1	16
Subp. Atención Cliente Interno	5	1			6
Subp. Desarrollo Sistemas	2				2
Subp. Investigación Tecnológica	5				5
Subp. Mantenimiento Sistemas	1				1
Subp. Seguridad Operativa Informática	7		2		9
Subproceso de Cómputo	28	4	4		36
Subproceso Redes y Telecomunicaciones	6	1	1		8
Subproceso Soporte Técnico	15	6	1		22
Total	**145**	**25**	**8**	**1**	**179**

2.4 Políticas y Procedimientos

Referente a las políticas y procedimientos, este Proceso se apoya en el área de Aseguramiento de la Calidad para dar control de actualización a los mismos y disponer de un único contacto con la Dirección de Desarrollo Humano, para este objetivo. Por lo tanto, se puede indicar que en lo relativo a las políticas de TI, se ha dispuesto lo siguiente:

a. Políticas de TI, de acatamiento institucional, estás son incluidas en el Capítulo 27 del Manual de Políticas y Procedimientos Institucionales, su modificación requerirá que la Gerencia General eleve los cambios al CTI de Junta Directiva.
b. Directrices de TI, corresponde con temas de acatamiento técnico específico de TI, por lo tanto su aprobación estará a cargo del Comité Interno de TI, CITI.

Con relación a los procedimientos de TI, en las siguientes tablas se muestra el nivel de actualización por corte trimestral para el 2010:

Primer Trimestre 2010

Subproceso Aseguramiento de la Calidad

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
8	1	Recepción, registro y destrucción de medios de Software	5-0-0-1-25	4	febrero	I	5 de enero 2010 por correo	PCO-029-2010 el 17 de febrero

Subproceso Atención al Cliente Interno

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
12	1	Comunicación para caídas de sistemas por falla Local y/o General	5-0-0-1-88	1	Marzo	2009	5 de enero 2010 por correo	PCO-029-2010 el 17 de febrero
13	2	Creación de accesos en ambiente producción para Subprocesos de TI.	5-0-0-1-39	5	Febrero	2009	5 de enero 2010 por correo	
14	3	Inclusión, Exclusión de Opident en SAXO, SIPO y Banca	5-0-0-1-42	4	Febrero	2009	5 de enero 2010 por correo	
15	4	Registro de incidentes con los Módulos de Seguridad	5-0-0-1-44	5	Febrero	2009	5 de enero 2010 por correo	
16	5	Reporte de Hardware de Cajeros Automáticos (Contrato GBM)	5-0-0-1-45	5	Febrero	2009	5 de enero 2010 por correo	
17	6	Solicitud para Trámites Especiales	5-0-0-1-46	5	Febrero	2009	5 de enero 2010 por correo	
18	7	Supervisión de reportes en SIEBEL	5-0-0-1-35	5	Febrero	2009	5 de enero 2010 por correo	
19	8	Trámite para la apertura de nuevas oficinas y cambio de código de agencia	5-0-0-1-36	5	Febrero	2009	5 de enero 2010 por correo	

Subproceso Administración del Sourcing

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
	1	Administración y fiscalización de contratos		1	Febrero		19 de enero 2010 por correo	Validado PCO-019 el 3 de Febrero
	2	Administración y control de la gestión de abastecimiento de bienes y servicios relacionados con recursos tecnológicos		1	Febrero		19 de enero 2010 por correo	

Subproceso Computo

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
30	1	Cierre diario y mensual de sistemas que residen en el IBM S390	5-0-0-1-54	4	marzo	I	5 de enero 2010 por correo	PCO-029-2010, 17 de feb
31	2	Ejecución de IPL para el equipo IBM 390 y el AS 400	5-0-0-1-56	4	marzo	I	5 de enero 2010 por correo	Validado PCO-019-2010
32	3	Intercambio y Respaldo de Datos Convenio UCR	5-0-0-1-51	4	marzo	I	5 de enero 2010 por correo	
33	4	Monitoreo de Cajeros Automáticos	5-0-0-1-57	5	marzo	I	5 de enero 2010 por correo	
34	5	Monitoreo de los enlaces comerciales	5-0-0-1-50	5	marzo	I	5 de enero 2010 por correo	PCO-029-2010, 17 de feb
35	6	Trámites especiales en Cómputo	5-0-0-1-19	3	marzo	I	5 de enero 2010 por correo	

Subproceso Redes y Telecomunicaciones

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
39	1	Solicitud de enlaces de comunicaciones	5-0-0-1-65	5	Febrero	I	5 de enero 2010 por correo	Validado PCO-019-2010
40	2	Atención de fallas en equipos de comunicación	5-0-0-1-64	5	Febrero	I	5 de enero 2010 por correo	
41	3	Atención de reportes en redes	5-0-0-1-81	3	Febrero	I	5 de enero 2010 por correo	

Segundo Trimestre 2010

Subproceso Investigación Tecnológica

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
5	1	Solicitud de nuevas investigaciones para Software y Hardware	5-0-0-1-69	3	abril	II	9 de marzo por correo	PCO-051-2010

Subproceso Aseguramiento de la Calidad

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
9	2	Cambios a Sistemas de Información	5-0-0-1-86	1	mayo	II	9 de marzo por correo	No tiene cambios
10	3	Cambios a Componentes de Infraestructura Tencológica	5-0-0-1-93	1	abril	II	9 de marzo por correo	No tiene cambios

Subproceso Atención al Cliente Interno

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
20	9	Creación, modificación, control de usuarios y dispositivos de impresión en el Sistema SISCARD	5-0-0-1-83	2	Mayo	2009	9 de marzo por correo	se envía por correo falta oficio
21	10	Creación, modificación, exclusión, suspensión de accesos a usuarios (AS/400, Top Secret, Banca, SIPO, Ahorro a Plazo, Opident)	5-0-0-1-40	7	Junio	2009	9 de marzo por correo	
22	11	Mantenimiento de Cuentas de red, correo electrónico Internet e Intranet, virus y antivirus	5-0-0-1-76	4	Mayo	2009	9 de marzo por correo	PCO-051-2010

Proceso Operación de la Producción

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
28	1	Monitoreo, control y corrección de fallas en el módulo de seguridad Visa	5-0-0-1-43	4	Abril	II	9 de marzo por correo	No tiene cambios
		Instructivo Solicitud de acceso a CODISA						

Subproceso Redes y Telecomunicaciones

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
42	4	Utilización y Preinstalación de Equipos	5-0-0-1-13	4	Mayo	II	9 de marzo por correo	No tiene cambios
		Reparación de equipo de cómputo						PCO-051-2010

Subproceso Soporte técnico

# TI	# área	Actividad	Código	Versión	Mes	Trimestre	Fecha envío a áreas	Fecha y oficio envío a GNR
47	1	Definición de archivos, transacciones y programas en pruebas y producción	5-0-0-1-73	3	Mayo	II	9 de marzo por correo	PCO-051-2010
48	2	Instalación y revisión de servidores de aplicaciones en Áreas de Negocios	5-0-0-1-68	3	Mayo	II	9 de marzo por correo	
49	3	Pases a Producción ambiente IBM/390	5-0-0-1-79	2	Mayo	II	9 de marzo por correo	PCO-051-2010

2.5 Servicios de TI

En lo referente al desarrollo de servicios, el PCO ha presentado una propuesta de catálogo de servicios, que se considera un punto de partida para iniciar una implementación al mediano plazo de la gestión de TI basada en servicios. La siguiente tabla es un extracto de la plantilla denominada Catálogo de Servicios de TI:

Catálogo de Servicios de TI

Versión: 1.0

Junio 2010

Código	Nombre del servicio	Dueño del servicio	Administrador del servicio
STI-L1-1	Redes y Conectividad	Subproceso de Redes y Telecomunicaciones	Subproceso de Redes y Telecomunicaciones
STI-L1-2	Sistemas de información en producción y canales	Subproceso Soporte Técnico	Subproceso Soporte Técnico
STI-L1-3	Asignación de equipo a usuario final	Subproceso de Redes y Telecomunicaciones	Subproceso de Redes y Telecomunicaciones
STI-L1-4	Mantenimiento y reparación del hardware y software de equipo usuario final	Subproceso de Redes y Telecomunicaciones	Subproceso de Redes y Telecomunicaciones
STI-L1-5	Procesos Batch	Subproceso de Cómputo	Subproceso de Cómputo
STI-L1-6	Emisión y distribución de informes relativos a datos de sistemas de información.	Subproceso de Cómputo	Subproceso de Cómputo
STI-L1-7	Almacenamiento y respaldo de datos	Subproceso de Cómputo	Subproceso de Cómputo
STI-L1-8	Servicio de navegación en Internet	Subproceso Seguridad Operativa Informática	Subproceso Seguridad Operativa Informática
STI-L1-9	Servicio de correo electrónico	Subproceso Seguridad Operativa Informática	Subproceso Seguridad Operativa Informática
STI-L1-10	Servicio de antivirus y AntiSPAM	Subproceso Seguridad Operativa Informática	Subproceso Seguridad Operativa Informática
STI-L1-11	Certificados digitales	Subproceso Seguridad Operativa Informática (desde punto de vista de infraestructura)	Subproceso Seguridad Operativa Informática
STI-L1-12	Servicio de identidad y autenticación en la red	Subproceso Seguridad Operativa Informática	Subproceso Seguridad Operativa Informática
STI-L1-13	Licenciamiento de software	Subproceso Aseguramiento de la calidad	Subproceso Aseguramiento de la calidad
STI-L1-14	Asesoría en adquisición de recursos tecnológicos	Subproceso Administración del Sourcing	Subproceso Administración del Sourcing
STI-L1-15	Atención y canalización de requerimientos de usuario.	Subproceso Atención al Cliente Interno	Subproceso Atención al Cliente Interno
STI-L1-16	Atención y canalización de requerimientos e incidentes	Subproceso Atención al Cliente Interno	Subproceso Atención al Cliente Interno
STI-L1-17	Mantenimiento de sistemas de información	CAPSI	Subproceso Desarrollo de Sistemas
STI-L1-18	Desarrollo y/o adaptación de Sistemas de información	Subproceso Desarrollo de Sistemas	Subproceso Desarrollo de Sistemas
STI-L1-19	Servicio de Confección de Estudio de Mercado y Factibilidad técnica de iniciativas del negocio y áreas de apoyo	Subproceso Administración del Sourcing. Todas las áreas del Banco Popular durante la confección del Presupuesto	Subproceso Investigación Tecnológica
STI-L1-20	Servicio de Intranet	Subproceso Desarrollo de Sistemas	Subproceso Desarrollo de Sistemas

2.6 Gestión de Riesgos de TI

Hasta el 2008, la Dirección de TI disponía de una metodología particular de riesgos, la cual había sido emitida por el Proceso Control Operativo y se venía aplicando consistentemente dos veces al año. No obstante, a pesar que dicha metodología había sido emitida fundamentada en normas internacionales, tales como el AS/NZS 4360 y COBIT, los resultados no eran homologados por la Unidad Técnica de la Gestión (UTEG), lo que obligaba a la Dirección de TI reprocesar las evaluaciones de riesgos basada en la herramienta SERO y control interno.

Es por ello, que a partir del 2009, evitando el indicado reproceso, se adopta el modelo de evaluación de riesgos y control interno vigente en el Banco, cuyos resultados se resumen a continuación:

Resultados Riesgo Operativo 2009

Áreas	Nota
Dirección Tecnología de Información	6,19
Proceso Desarrollo	6,33
Subproceso Adm y Desarrollo de Proyectos (Set-09)	7
Subproceso Investigación Tecnológica (Mar-09)	7
Subproceso Desarrollo de Sistemas (Oct-08)	5
Proceso Operación de la Producción	5,5
Subproceso Mantenimiento de Sistemas (Oct-08)	4
Subproceso Cómputo (Mayo-09)	7
Subproceso Soporte Técnico (Jun-08)	7
Subproceso Redes y Telecomunicaciones (Oct-08)	4
Proceso Control Operativo	6,75
Subproceso Aseguramiento de Calidad (Mayo-09)	7
Subproceso Administración del Sourcing (Nov-08)	9
Subproceso Seguridad Operativa Informática (Jul-08)	3
Subproceso Atención al Cliente Interno (Jul-08)	8

Resumen de resultados Control Interno 2009

AREA	CALIFICACIÓN	NIVEL
Dirección Tecnología de Información	0%	Excelente
Proceso Control Operativo	0%	Excelente
Proceso Desarrollo	0%	Excelente
Proceso Operación de Producción	0%	Excelente
Subproceso Investigación Tecnológica	1%	Excelente
Subproceso Desarrollo Sistemas	1%	Excelente
Subproceso Administración y Desarrollo de Proyectos	2%	Excelente
Subproceso Administración del Sourcing	0%	Excelente
Subproceso Atención al Cliente Interno	0%	Excelente
Subproceso Seguridad Operativa Informática	0%	Excelente
Subproceso Aseguramiento de la Calidad	2%	Excelente
Subproceso Mantenimiento de Sistemas	2%	Excelente
Subproceso Cómputo	3%	Excelente
Subproceso Redes y Telecomunicaciones	1%	Excelente
Subproceso Soporte Técnico	0%	Excelente

Los resultados específicos del Proceso Control Operativo y sus áreas adscritas para el año 2008 fue el que se muestra en la siguiente tabla:

Proceso Control Operativo	15411	1100	7,00%	Satisfactorio
63-Subp. Aseguram. Calidad	5526	523	9,00%	Satisfactorio
69-Subp. Administ. Sourcing	3923	348	9,00%	Satisfactorio
70-Sup. Segur. Oper. Informát.	3671	126	3,00%	Excelente
71-Subp. Aten. Cliente Interno	2291	103	4,00%	Excelente

2.7 Autoevaluaciones de TI

En lo referente a la SUGEF, durante el 2008 y 2009 se coordinó las autoevaluaciones de TI relativas al acuerdo SUGEF 24-00, cuyos resultados se transcriben a continuación, no omito indicar que dichos resultados fueron avalados por la Auditoría Interna:

Resultados Autoevaluación SUGEF 2009

Área de evaluación	Calificación 2008	Estado 2008	Calificación 2009	Aporte	Asignado 2009	Estado 2009
Administración del Área de Tecnología de Información	95,83	Normal	95,83	14	13,42	Normal
Seguridad Lógica y Acceso a Datos	87,5	Normal	87,50	14	12,25	Normal
Seguridad Física	100	Normal	100,00	12	12,00	Normal
Sistemas de Información	91,67	Normal	91,67	12	11,00	Normal
Software y Bases de Datos	87,5	Normal	87,50	12	10,50	Normal
Hardware, Redes y Comunicaciones	100	Normal	100,00	11	11,00	Normal
Continuidad de las Operaciones	77,5	Irregularidad 1	77,50	11	8,53	Irregularidad 1
Servicios Financieros por Internet	95	Normal	95,00	7	6,65	Normal
Descentralización de Procesamiento en el Exterior	-	N/A	-			N/A
	91,77		**91,77**	**93**	**85,34**	

Resultados Autoevaluación SUGEF 2008

Área de evaluación	Calificación 2007	Estado 2007	Calificación 2008	Aporte	Asignado 2008	Estado 2008
Administración del Área de Tecnología de Información	100	Normal	95,83	14	13,42	Normal
Seguridad Lógica y Acceso a Datos	87,5	Normal	87,5	14	12,25	Normal
Seguridad Física	87,5	Normal	100	12	12,00	Normal
Sistemas de Información	83,33	Irregularidad 1	91,67	12	11,00	Normal
Software y Bases de Datos	87,5	Normal	87,5	12	10,50	Normal
Hardware, Redes y Comunicaciones	100	Normal	100	11	11,00	Normal
Continuidad de las	77,5	Irregularidad	77,5	11	8,53	Irregularidad

Operaciones		1				1
Servicios Financieros por Internet	90	Normal	95	7	6,65	Normal
Descentralización de Procesamiento en el Exterior	-	N/A	-			N/A
	89,33		**91,77**	**93**	**85,34**	

Con relación a las principales actividades realizadas, a partir de la entrada en vigencia del Reglamento para la Gestión de TI, denominado Acuerdo SUGEF 14-09, se pueden resumir como sigue:

- Con el propósito de que esta normativa se divulgara al más alto nivel, se presentó ante la Comisión de Planeamiento Estratégico Informático, de Junta Directiva Nacional, los alcances del Acuerdo SUGEF 14-09.

- En cumplimiento de dicho Reglamento, en el mes de mayo del 2009, se aprueban por parte de la Junta Directiva Nacional, las modificaciones a las funciones, conformación, denominación y plan de trabajo de la Comisión indicada en el punto anterior. Esto en línea con los artículos 7 y 8 del referido Reglamento.

- La Gerencia General designó a la Dirección de TI para que asuma un rol de liderazgo en la planificación y coordinación de las acciones requeridas para la implementación del Reglamento. Por lo tanto, el PCO coordinó a lo interno de TI las siguientes acciones:
    - Basados en estudios previos, situación vigente y nueva regulación, se seleccionaron preliminarmente los procesos COBIT más relevantes para el Banco y que eventualmente integrarían el marco de gestión de TI.
    - Priorización de los procesos seleccionados, con el propósito de utilizar esta variable como elemento de planificación.
    - Evaluación de la situación actual de los procesos seleccionados.
    - Determinación de la brecha con respecto al modelo de evaluación de la SUGEF 14-09, aplicando como modelo de autoevaluación las matrices incluidas en los Lineamientos Generales de la 14-09, comunicadas en SUGEF 839-2009.
    - Determinación y asignación a los dueños de procesos de los planes de acción aplicables.
    - Conformación de un equipo de trabajo para el establecimiento de los requisitos documentales de la norma. Para ello, se adopta el modelo documental definido para el Core System y consistente en la documentación descriptiva del proceso y documentos

complementarios denominados instructivos de trabajo, fase en la que actualmente se encuentra en desarrollo.

- En relación con la contratación de una auditoría externa para la aplicación de la evaluación independiente, en procura de dar cumplimiento con el Capítulo III del Reglamento, por lo cual, se ha previsto el monto requerido en el presupuesto ordinario 2010 de la Dirección de Tecnología de Información. El cartel ha sido confeccionado y el mismo ha sido publicado. No obstante, se están cursando modificaciones al mismo, de tal forma que se incluya un comunicado de la SUGEF indicando que dentro del alcance de la evaluación se deberá incluir al proveedor ATH, lo cual se prevé incrementará de manera importante el monto presupuestado.

- Durante el 2009 se elaboró el Documento Perfil Tecnológico, requerido en dicha Normativa en el artículo 10, siendo enviando por primera vez a la SUGEF durante el mes de octubre pasado. Actualmente, también fundamentados en lo establecido por dicho ente supervisor, nos encontramos coordinando esfuerzos para la actualización y remisión del Perfil Tecnológico del Banco del 2010, proceso que debe ejecutarse cada año durante los primeros diez días hábiles del mes de junio, según Artículo 10 del Reglamento.

- En el mes de junio del 2009 y conforme se establece en el artículo 6 se definió el Marco para la Gestión de TI, mismo que fue revisado en la Comisión de Tecnología de Información, en sesión No. 16-2009 y aprobado en acuerdo No. CTI-ACD-072-2009, posteriormente fue elevado a Junta Directiva Nacional para su aprobación: Acuerdo No 947 de Sesión Ordinaria No. 4707, celebrada el jueves 22 de octubre del 2009.

- Actualmente se está coordinando la aplicación de la autoevaluación prevista en el acuerdo SUGEF 24-00, no obstante, considerando el modelo COBIT 4.0. Por lo tanto, no será aplicada el anterior método de evaluación, significando con ello que es altamente probable que el nivel de cumplimiento decaiga significativamente, al incorporarse un nuevo modelo de evaluación.

Con relación al proceso de implementación de las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República, éste fue iniciado durante el inicios del 2008 y fue concluido al 31 de Julio del 2009 de forma satisfactoria. Cabe destacar que se cumplió con el cronograma establecido para dicha tarea, sin embargo en algunos casos se definieron planes de acción que contribuirían a alcanzar la meta establecida al inicio de la implementación de cada norma que consistía en alcanzar el nivel de madurez 3 Definido según las mejores prácticas COBIT para la Gobernabilidad de TI.

En el oficio DTDI-469-2009 se envía la Gerencia del Banco el Informe de acuerdo a las Normas Técnicas para la Gestión y Control de las Tecnologías y publicadas en La Gaceta., según ese estudio se obtiene:

Parámetros de evaluación	Valor del parámetro	Q Normas	Puntos obtenidos	Distribución
Cumple	1	19	19	61%
Cumple Parcialmente Alto	0,75	6	4,5	15%
Cumple Parcialmente	0,50	1	0,5	2%
Cumple Parcialmente Bajo	0,35	5	1,75	6%
Total de Normas		**31**		
Puntaje total esperado		**31**		
Puntaje total obtenido			**25,75**	
Calificación final				**83%**

Como se observa 19 normas cumplen satisfactoriamente, según los criterios aplicados, las doce normas restantes presentan algún margen de brecha, por lo que requieren de esfuerzos adicionales para lograr el nivel acordado. En los siguientes cuadros se observan los resultados por cada norma:

Punto de la Norma	Estado
1.1. Marco Estratégico de TI	Cumple
2.5. Administración de Recursos Financieros	Cumple
3.4. Contratación de Terceros para la Implementación y Mantenimiento de Software e Infraestructura	Cumple
5.2. Seguimiento y Evaluación del Control Interno en TI	Cumple
5.3. Participación de la Auditoria Interna	Cumple
1.4.3. Seguridad Física y Ambiental	Cumple
1.5. Gestión de Proyectos	Cumple
1.6. Decisiones sobre asuntos Estratégicos de TI	Cumple
2.4. Independencia y Recurso Humano de la Función de TI	Cumple
4.6. Administración de servicios Prestados por Terceros	Cumple
1.2. Gestión de la Calidad	Cumple
1.7. Cumplimiento de Obligaciones relacionadas con la Gestión de TI	Cumple
3.2. Implementación de Software	Cumple
4.4. Atención de Requerimientos de los Usuarios de TI	Cumple
5.1. Seguimiento de los Proceso de TI	Cumple
1.4.4. Seguridad en las Operaciones y Comunicaciones	Cumple
2.1. Planificación de las Tecnologías de Información	Cumple
1.4.5. Control de Accesos	Cumple
4.3. Administración de los Datos	Cumple

Punto de la Norma	Estado
1.3. Gestión de Riesgos	Cumple Parcialmente Alto
1.4.2. Compromiso del Personal con la Seguridad de la Información	Cumple Parcialmente Alto
4.5. Manejo de Incidentes	Cumple Parcialmente Alto
1.4.6. Seguridad en la Implementación y Mantenimiento de Software e Infraestructura Tecnológica	Cumple Parcialmente Alto
3.1. Consideraciones Generales de la Implementación de TI	Cumple Parcialmente Alto
1.4.7. Continuidad de los Servicios de TI (alcance parcial)	Cumple Parcialmente Alto

Punto de la Norma	Estado
4.2. Administración y Operación de la Plataforma Tecnológica	Cumple Parcialmente

Punto de la Norma	Estado
2.3. Infraestructura Tecnológica	Cumple Parcialmente Bajo
1.4.1. Implementación de un Marco de Seguridad de la Información	Cumple Parcialmente Bajo
3.3. Implementación de Infraestructura Tecnológica	Cumple Parcialmente Bajo
2.2. Modelo de Arquitectura de Información	Cumple Parcialmente Bajo
4.1. Definición y Administración de Acuerdos de Servicio	Cumple Parcialmente Bajo

2.8 Plan Estratégico de TI del Conglomerado

Una de las funciones asignadas al Proceso Control Operativo, corresponde con la coordinación de la emisión, actualización, seguimiento e informes del Plan Estratégico de TI del Conglomerado, por lo tanto en este punto se informa de la situación del Proceso Definir un Plan Estratégico de Tecnología de Información del Conglomerado Banco Popular, según la Directriz de TI que se transcribe a continuación:

DITI-PO1-01 Plan estratégico de TI	
Responsable(s)	Dirección de Tecnología de Información
Afecta a	Dirección de Tecnología de Información
Enunciado	Anualmente o cuando sea requerido en caso que se presenten cambios que requieren su actualización se hará una revisión del Plan Estratégico de Tecnología de Información del Conglomerado, procurando que se encuentre alineado con los cambios en los objetivos, metas o estratégicas institucionales y a partir de los insumos de todas las áreas de Tecnología de Información del Conglomerado. Se centraliza la actualización en el Subproceso Aseguramiento de la Calidad.

El Plan Estratégico de Tecnología de Información del Conglomerado Banco Popular 2009-2012 vigente, fue actualizado debido a modificaciones realizadas al PEC, enviadas por Gestión Estratégica mediante oficio PGE-711-2009, las cuales se realizaron según acuerdo de Junta Directiva Nacional N° 913, sesión JDN-4704, éstas modificaciones del PETICO fueron aprobadas por el Proceso de Gestión Estratégica en oficio PGE-783-2009, el 13 de noviembre de 2009, fueron avaladas por la Comisión de Tecnología de Información, el 16 de diciembre de 2009, en CTI-ACD#086-2009 y por último aprobado por JDN en sesión JDN-4724, acuerdo N° 058, de 21 de enero de 2010.

Sin embargo, mediante oficio PGE-125-2010 el Proceso de Gestión Estratégica solicita sean incluidos el Análisis de riesgos del Petico, la Dirección lo envía en el oficio DTDI-253-2010 el 19 de mayo de 2010 y es avalado por Proceso de Gestión Estratégica en el oficio PGE-321-2010 y por el Proceso de Administración del Riesgo en PAR-361-2010. Se envía a Gerencia en el DTDI-318-2010 el 29 de junio, es visto por la Comisión de Tecnología de Información y envía el 21 de julio a Junta Directiva para que sea avalada.

A la fecha de este informe, el documento del PETICO presentado en enero de este año, requiere ser aprobado por la JDN, al respecto hemos dado el seguimiento desde que se presentó en enero a Gestión Estratégica, luego fue aprobado por dicha área y enviado a Gerencia General para ser aprobado por JDN, sin embargo, sufrió una serie de consultas que requirieron atención de TI y en estos momentos se está a la espera de la respuesta por parte de Gestión de Riesgos. Se adjunta el cuadro de seguimiento de los oficios:

	Fecha	Oficio	De:	Hacia:	Asunto:
1	6 de enero de 2010	DTI-008-2010	TI	Gestión Estratégica	envió seguimiento PETICO
2	14 de enero de 2010	PGE-035-2010	Gestión Estratégica	TI	observaciones al seguimiento del PETICO
3	18 de enero de 2010	DTI-035-2010	TI	Gestión Estratégica	respuesta a observaciones del seguimiento del PETICO
4	21 de enero de 2010	PGE-051-2010	Gestión Estratégica	TI	validación seguimiento del PETICO
5	21 de enero de 2010	DTI-066-2010	TI	Gerencia General Corporativa	envio seguimiento PETICO
			Gerencia General Corporativa	Comité de Tecnología de Información	
			Comité de Tecnología de Información	Junta Directiva Nacional	
	23 de febrero de 2010	JDN-4732-165	Manuel Rivera	Comisión de Tecnología de Información	Devolver cuadro de cumplimiento del PETICO
	9 de febrero de 2010	DTDI-170-2010	TI	Comisión de Tecnología de Información	Explicación sobre acuerdo de JDN-4732,acd165 sobre comentarios auditor interno
	30 de abril de 2010	JDN-4741-297	Martín Alfaro	TI	Solicita atención de las recomendaciones de orden estratégico
	4 de mayo de 2010	CTI-ACD-029-2010	Comisión de Tecnología de Información	TI	Dar por recibido 170 y solicita para el 22 de mayo presentación del informe de seguimiento. Presentar en un mes indicadores
			Presentación		
	27 de mayo de 2010	DTDI-262-2010	TI	Gerencia General Corporativa	Respuesta a JDN-4741-297
	2 de julio de 2010	JDN-4769-639	Junta Directiva Nacional	Gerencia General Corporativa	ampliación plazo al 15 de julio de acuerdo JDN-4741-297

2.8.1 Procesos internos asociados con el PETICO

A efectos de estandarizar y coordinar adecuadamente los procesos asociados con el PETICO, fue coordinado con el Proceso de Gestión Estratégica los siguientes documentos:

- *Procedimiento de Formulación, actualización, evaluación y seguimiento de planes estratégicos del Conglomerado Financiero BPDC*: Este procedimiento explica los pasos para formular, actualizar, evaluar y dar seguimiento a los planes estratégicos del Banco, inicia con el PEC que es la base para los demás planes, continua con el envío a las áreas del PEC para que éstas modifiquen los planes (en caso necesario) alineados al PEC, explica la parte de aprobaciones y concluye con la divulgación por el área dueña del Plan.

- *Metodología de Formulación, actualización, evaluación y seguimiento de planes estratégicos del Conglomerado Financiero BPDC:* La metodología inicia con la formulación, donde se establece la definición del grupo de trabajo dependiendo de cada Plan, sigue con la información requerida, elaboración del cronograma y pasa a explicar que se debe incluir en situación actual (análisis del entorno, Análisis de riesgos, Análisis FODA), continua con la razón de ser (misión, visión, estrategia general), luego de esto entra en la parte de Planeamiento Estratégico (objetivos, indicadores, metas, unidades de medida, estrategias y supuestos), para esta etapa Gestión Estratégica ha definido un estándar en Excel, una hoja por objetivo donde se tome en cuenta estos puntos.

  Debe continuarse con la Viabilidad financiera punto que TI no cumple por el momento. Luego hay que llevar a cabo el análisis de la estructura organizativa.

  La metodología como punto 2 se refiere a la actualización del Plan, punto 3 la evaluación, en esta parte hace referencia a que en:

  > *"Plan estratégico de Tecnología de Información del Conglomerado: el Proceso Control Operativo o el área que la Dirección de Tecnología de Información designe será el responsable de coordinar con las áreas de Tecnología de Información de las Sociedades Anónimas y las demás dependencias del Banco para efectuar la evaluación."*

  Luego vienen las consideraciones para la evaluación, el seguimiento y por último la aprobación, comunicación y divulgación.

  Esta metodología fue remitida inicialmente con una serie de observaciones por parte de Tecnología de Información en el oficio DTDI-199-2010 el 12 de abril, entre las cuales está:

  > *"2. Considerando que el Plan Estratégico de TI debe ser construido sobre la base de los requerimientos generales que plantea el negocio en el PEC, surge la duda*

del cómo las sociedades anónimas deben interactuar internamente para que a partir de su particular plan estratégico sea emitido el plan de TI, el cual se incorporará en el PETICO. Por ello se considera importante el que éstos temas sean desarrollados con claridad en la metodología.

Esta medida permite asegurar que al emitirse y actualizarse el plan estratégico de TI particular de cada sociedad, se asegure el adecuado alineamiento con el plan estratégico (de negocio) de dicha sociedad y que éstos a su vez se encuentren alineados al PEC."

El Proceso Gestión Estratégica contesta en el oficio PGE-195-2010 que puede cumplir con los demás puntos pero que éste lo estarían realizando luego ya que requiere de mayor coordinación y más tiempo y que deben cumplir con la recomendación de auditoría sobre la metodología, por lo que estamos en espera de que se comience a trabajar en este punto.

Tecnología de Información contesta en el DTDI-236-2010 del 3 de mayo que aceptábamos la metodología con la condición de que se modificara lo antes posible.

En estos momentos sabemos que esta Metodología no ha sido divulgada por parte de Gestión Estratégica quienes son los responsables de ésta.

La responsabilidad de la Dirección de TI, se encuentra asignada en el acuerdo de Junta Directiva Nacional 4739, que indica:

"El informe del Plan Estratégico Informático es responsabilidad de Tecnología de Información, es de periodicidad anual, se presenta la primera semana de febrero al Comité de Planeamiento Estratégico."

Este acuerdo debe ser tomado en cuenta al hacer el cronograma del seguimiento del PETICO.

- Procedimiento de presentación de informes ante la Junta Directiva Nacional: Este procedimiento indica que la Unidad Técnica de Evaluación de la Gestión recuerda a los encargados de los informes la presentación de éstos, lo importante de este procedimiento es que debe entregarse en forma digital.

- Plan de trabajo para la definición, actualización o seguimiento del PETICO: Como parte de la mejora de procesos en TI, debía realizarse el plan de trabajo para formular,

actualizar y dar seguimiento al PETICO, por lo que fue necesario hacer un Plan de Trabajo, el cual avaló auditoria.

A continuación se presentan las actividades tomadas en cuenta de acuerdo a la metodología y una breve explicación de cada una.

La responsabilidad de definir o actualizar el Plan Estratégico es de la Dirección de Tecnología de Información, quién se apoyará en el Proceso Control Operativo, con apoyo de todas las áreas de TI, especialmente de Aseguramiento de la Calidad.

Se deberá establecer un equipo de trabajo, el cual podrá estar constituido al menos por:

- Liderado por el Director de Tecnología de Información o la persona que él designe
- 1 persona de TI de Popular Valores y SAFI
- 1 persona de TI de Popular Pensiones
- 2 personas del grupo de Arquitectura
- El coordinador de Control Operativo
- 1 Gestor de Calidad

Con el propósito de agilizar la comunicación se hará uso intensivo del correo electrónico y minimizar reuniones generales, para hacer énfasis en específicas.

Todo el proceso comienza con un análisis de la situación actual, que produce el modelo funcional imperante en el banco. En este paso se evalúa de manera general el entendimiento de la estrategia de negocios, la eficiencia de los procesos operativos y la aceptación de TI en la organización.

Se revisan las necesidades de los negocios, o sea la revisión del establecimiento de la estrategia de negocios (el proceso de planeación se basa en una transformación de dichas estrategias), se da la comunicación con las áreas sobre el inicio del proceso de formulación del Plan Estratégico de TI. Se presenta la documentación base (especialmente el PEC y la metodología).

La fase siguiente, relacionada con la creación de un modelo de la organización, inicia con un análisis del entorno, análisis de riesgo, análisis FODA y una evaluación de los sistemas existentes (funcionalidad, estabilidad, complejidad). Se define o revisa la razón de ser de TI (misión, visión, estrategia general, valores, actitudes corporativas y principios éticos).

Se entra en la parte más importante que es el Planeamiento Estratégico, aquí se definen los objetivos, los indicadores, las metas y las estrategias. Se llena la matriz y se ponen los supuestos.

Es aquí donde se ponen los requerimientos de TI necesarios para mejorar la eficiencia y la productividad, así como cumplir con los requerimientos de las áreas del banco.

Con base en los objetivos, metas y estrategias se definen los planes tácticos, que soportarán el Plan Estratégico para TI se han definido los planes tácticos de: Seguridad, Infraestructura Tecnológica, Mantenimiento de la infraestructura y el de capacidad y desempeño.

Una vez que estos planes estén aprobados y alineados al PETICO se hace el Plan de adquisiciones y el plan de inversiones (la diferencia es el plazo)

Posteriormente, se debe revisar la estructura de la organización, que especifica puestos, perfiles, habilidades, conceptualizaciones de las áreas, roles, funciones, etcétera, necesarios para administrar TI.

A partir de aquí se pasa para aprobación y una vez aprobado se divulga.

En cuanto al seguimiento la mecánica es diferente puesto que es verificar el cumplimiento del Plan Estratégico, lo primero es comunicar a las sociedades anónimas el inicio del seguimiento ya que éstas requieren más tiempo.

Las matrices de seguimiento ya están definidas, por lo que hay que llenarlas y buscar la información de respaldo.

Lo mismo debe hacerse con los planes tácticos, darles seguimiento al mismo tiempo que al PETICO.

En cuanto a la recopilación de información en TI, la mayoría se encuentra en los informes de labores de las áreas dentro del site de TI, solo es necesario solicitar muy pocos puntos por lo que se realiza por correo electrónico.

Una vez listo el informe se inicia con las revisiones y aprobaciones y por último la divulgación.

2.8.2 Avance del Plan Estratégico (PETICO)

El avance de cada una de las metas se consideró de acuerdo al esfuerzo ejecutado versus el tiempo transcurrido, de manera que al medir la meta dé cómo resultado el porcentaje de cumplimiento esperado.

Para el primer semestre de 2010, se estima el avance del Plan Estratégico del Conglomerado, en un 93,15% en promedio según el siguiente detalle:

Objetivos Estratégicos	Indicadores / meta	Meta 2010	Logros 2010					
			Banco Popular		Popular Pensiones		SAFI y Valores	
			Valor	Peso	Valor	Peso	Valor	Peso
1. Plataforma tecnológica	1	100%	100%	**7,58**	100%	**12,50%**	100%	**8,75%**
	2	99%	99,73%	**8,33**	100,00%	**12,50%**	99,59%	**12,50%**
	3	0%	NA	**NA**	NA	**NA**	NA	**NA**
2. Core System	1	100%	100%	**4,17**	NA	**NA**	NA	**NA**
	2	100%	100%	**4,17**	NA		NA	
	3	5	100%	**4,17**	NA		NA	
	4	100%	100%	**4,17**	NA		NA	
	5	0%	NA	**NA**	NA		NA	
3. Servicios informáticos	1	>= 90%	90%	**3,87**	100%	**25,00%**	94.5	**8,33%**
	2	>= 90%	96,45	**4,17**	NA	**NA**	96	**8,33%**
	3	100%	100%	**4,17**	NA		100%	**8,33%**
	4	100%	100%	**4,17**	NA		NA	**NA**
4. Normativa aplicable a TI	1	Normal	Normal	**5,56**	Excelente	**6,25%**	Normal	**8,34%**
	2	<= 10%	6,19%	**5,56**	Satisfactorio	**6,25%**	8,00%	**8,33%**
	3	Satisfactorio	Excelente	**5,56**	Satisfactorio	**6,25%**	Satisfactorio	**8,33%**
	4	100%	100%	**NA**	100%	**6,25%**	100%	**NA**
5. Procesos internos de TI	1	100%	100%	**8,34**	NA	**NA**	NA	**NA**
	2	100%	100%	**8,33**	NA		NA	
	3	0%	NA	**NA**	NA		NA	
6. Competencias técnicas y profesionales del factor humano	1	>= 90%	74,33%	**12,39**	100,00%	**6,50%**	100,00%	**19,50%**
	2	0%	NA	**NA**	NA	**NA**	NA	**NA**
	3	0%	NA	**NA**	100,00%	**12,50%**	NA	**NA**
Calificación Total				**94,70**		**94,00**		**90,75**

Ver informe: Informe semestral de seguimiento del PETICO Junio-2010, remitido a la Dirección de TI en oficio POP-115-2010.

2.9 Resultados administrativos del PCO

En lo referente al cumplimiento de las metas del PAO, se puede indicar que el porcentaje es bastante satisfactorio, siendo que el último corte, al 30/06/2010 se había alcanzado un 99.5% de cumplimiento, como puede ser observado en el siguiente cuadro resumen:

Área	Metas Totales	Metas I Trimestre	Metas II Trimestre	Metas Cumplidas I Trimestre	Metas Cumplidas II Trimestre	Metas En Proceso II Trimestre
Proceso Control Operativo	7	1	1	1	1	0
Subproceso Aseguramiento Calidad	10	4	4	4	4	0
Subproceso Atención al Cliente	8	3	3	2,98	2,95	0,05
Subproceso Administración del Sourcing	9	1	2	1	2	0
Subproceso Seguridad Operativa Informática	8	1	1	1	1	0
Totales	42	10	11	9,98	10,95	0,05
Grado de Cumplimiento al II Trimestre	**99,55%**					

Otro de los resultados importantes del Proceso, corresponde con los resultados de la evaluación del cliente interno, el cual en promedio se alcanza el nivel meta. No obstante, el Subproceso de Aseguramiento de la Calidad alcanza una calificación del 88%, situación que ameritó que se le exigiera planes de acción en procura de mejorar este resultado. Los resultados de la última evaluación del cliente interno se resumen en el siguiente cuadro:

Resultado de evaluaciones de Cliente Interno
A Diciembre 2009

Proceso Control Operativo	**92**
Subproceso Aseguramiento de Calidad	88
Subproceso Administración del Sourcing	94
Subproceso Seguridad Operativa Informática	93
Subproceso Atención al Cliente Interno	93

3. Aspectos Adicionales a Considerar

En esta sección se incluyen aspectos relevantes que es requerido se brinde seguimiento, dado que los mismos fueron iniciados por lo tanto se encuentran en proceso. Así como indicar otros aspectos que podrían incidir en los resultados de las áreas adscritas:

3.1 Proceso Control Operativo

- Se ha iniciado el proceso de autoevaluación de SUGEF, esto basado en el modelo COBIT, según lo exigido por dicho ente. El mayor riesgo asociado a esta actividad es que corresponde con el cambio de modelo de evaluación, por lo tanto sería la primera vez que éste se aplica. En este sentido se decidió utilizar las matrices de evaluación propuestas por la SUGEF para realizar la auditoría externa. Lo cual conlleva a retos importantes, dado que requiere una coordinación mayor con otras áreas del Banco pero externas a TI, lo cual también se presume de riesgo.

3.2 Subproceso Atención al Cliente Interno

- En el SACI, actualmente se está siguiendo un proceso de sustitución de la herramienta conocida como SIEBEL, la cual es la base para registrar, controlar e informar a cerca de la atención de casos en TI. Dicha herramienta, ha cumplido su ciclo de vida por lo que renovarla resulta sumamente oneroso y la misma no satisface las prácticas de ITIL. Por lo tanto, se inició con un proceso de presupuestación y adquisición de una herramienta que la reemplazara, con un presupuesto de US$200.000 que debería ser reforzado con un monto similar para la asesoría. Paralelamente, se obtuvo el visto bueno por parte de Microsoft para realizar un plan piloto con el objetivo de conocer las funcionalidades del software System Center Service Manager. Los resultados de dicha prueba y la estimación de costos fueron satisfactorios, al punto que se decidió autorizar su adquisición e implementación.

  Para ello será requerido iniciar un proceso de contratación de una empresa que implemente, asesore y capacite los funcionarios involucrados. Esta actividad se considera un proyecto de TI por lo tanto, se ha solicitado la participación de las diferentes áreas involucradas.

- Dada la pérdida de personal del SACI, actualmente dicha área se ha reforzado con personal de la empresa el Orbe, situación que permite una sustitución de los funcionarios con categoría 15, no obstante, por los niveles de acceso y el conocimiento requerido no vemos conveniente ceder a un tercero las responsabilidades de los de categoría 17, por lo que estos son funcionarios de planta del Banco.

Las estadísticas del área muestran una disminución significativa en la productividad de los funcionarios de ésta área, asociables al esquema de horarios rotativos, producto de la eliminación del horario 3X4, entre otros. Razón por la cual la jefatura de ésta área implementó equipos de especialización, que permitieran un esquema de atención más ágil. Asimismo, dicha jefatura ha iniciado un plan para incrementar las estadísticas de productividad con el objetivo de identificar y mejorar puntos débiles.

- Con relación al Proyecto Core System, ésta área se considera de alta importancia logística, dado que será el punto de atención de los usuarios durante la puesta en producción y subsecuentemente, por lo tanto se ha solicitado al Core que tome en cuenta a esta área en los planes de implementación.

3.3 Subproceso de Seguridad Operativa Informática

- De esta área se encuentra pendiente la migración del Exchange a la versión 2007, con lo cual se obtendrán una serie de ventajas adicionales en la comunicación organizacional.

- Por otra parte, ésta área tiene un rol fundamental para la emisión de la estrategia del diseño, desarrollo e implementación del nuevo sitio web para T24.

- Un aspecto importante a considerar es que se deberá realizar un análisis de las funciones de soporte que actualmente desarrolla el SSOI, con el propósito que se juzgue la viabilidad que algunas sean trasladadas a las áreas correspondientes de Operación de la Producción, esto en aras de procurar un mayor énfasis en las labores de seguridad informáticas.

3.4 Subproceso Aseguramiento de la Calidad

- Como parte de los aspectos requeridos para la planificación, desarrollo e implementación de la herramienta Service Manager, mencionada en el punto correspondiente al SACI, será necesario realizar un replanteamiento de las funciones referentes a los procesos de cambios y configuración que actualmente ejecuta el SAC. De tal forma que se reenfoque en la verificación del cumplimiento de los procesos que conforman el “Marco de TI”, en línea con el Reglamento SUGEF 14-09.

- Un aspecto importante que requerirá pronta resolución es la negativa de la Contraloría respecto a nuestra solicitud de iniciar negociaciones con Microsoft para la renovación del Enterprise Agreement. Situación que pone en riesgo la infraestructura Microsoft actual del Banco. A este respecto, se le ha solicitado al Lic. Jorge Alfaro que desarrolle un estudio comparativo de software alternativo a las soluciones Microsoft, cuyo licenciamiento el Banco procura renovar. Dicho estudio deberá incluir costos de adquisición, implementación, incluyendo capacitación y mantenimiento. Se fue enfático en indicar que este estudio debe ser

presentado ante la CGR con el tiempo suficiente para que dicho ente realice su análisis y emita un criterio, previo a la finalización del contrato vigente, sea 31/10/2010.

3.5 Subproceso Administración del Sourcing

- Durante el último año ésta área ha sido afectada por la merma de recursos, no obstante, hoy en día se le ha devuelto al número de funcionarios que le permiten el cumplimiento de las funciones actuales.

- Actualmente se encuentra en ejecución el plan institucional para la emisión del presupuesto 2011, por lo tanto, esta área se encuentra avocada a su cumplimiento.