ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE CIENCIAS ADMINISTRATIVAS

IDENTIFICACIÓN DE LOS FACTORES Y EVENTOS DE RIESGO OPERATIVO DENTRO DEL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES BASADO EN COBIT 5.0 EN INSTITUCIONES FINANCIERAS PÚBLICAS, CASO BANCO DEL ESTADO

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SISTEMAS DE GESTIÓN INTEGRADOS

ING. SAÚL ALEJANDRO CÓRDOVA QUILODRÁN
saulitocordova@hotmail.com

Director: ING. GIOVANNI PAULO D'AMBROSIO VERDESOTO
giovanni.dambrosio@epn.edu.ec

2014

DECLARACIÓN

Yo, Saúl Alejandro Córdova Quilodrán, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

ING. SAÚL ALEJANDRO CÓRDOVA QUILODRÁN

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Saúl Alejandro Córdova Quilodrán, bajo mi supervisión.

ING. GIOVANNI D'AMBROSIO VERDESOTO
DIRECTOR

AGRADECIMIENTOS

Agradezco a la Escuela Politécnica Nacional, por haber sido una institución de excelencia con una plantilla de profesores de altísimo nivel que me entregaron conocimientos y experiencias para superarme personal y profesionalmente.

Agradezco al Banco del Estado, especialmente a la Dirección de Gestión de la Calidad, Dirección de Sistemas de Información y a la Dirección de Riesgo Operativo, por brindarme todas las facilidades del caso para el desarrollo del presente proyecto y por apoyarme con los conocimientos propios del negocio.

Finalmente, agradezco a mis compañeros de curso con quienes compartimos momentos inolvidables que jamás se borrarán de mi memoria.

DEDICATORIA

La presente investigación la dedico a mi familia por haber sido un magnífico equipo a lo largo de nuestras vidas en conjunto; a mi hijo Nicolás, por ser uno de los pilares fundamentales y principal razón de mi vida; a mi esposa Andrea, por ser un apoyo incondicional y una de las promotoras para emprender el presente trabajo; a mi querida madre, por haberme enseñado todos los principios éticos y morales; y a mi padre, por ser un ejemplo para mi superación personal y profesional

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

La presente investigación tiene como objetivo general la Identificación de los factores y eventos de riesgo operativo dentro del proceso de Gestión De Tecnologías de Información y Comunicaciones basado en COBIT 5.0 en el Banco del Estado, entendiéndose como factor de riesgo a la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos, mientras que un evento se entiende como el hecho que puede derivar en pérdidas financieras para la institución controlada.

La estructura de la investigación se la ha dividido en 5 capítulos como se detallan a continuación:

1 Introducción: en esta sección se plantea un panorama general del Banco del Estado, puntualizando aspectos relacionados a su historia, planificación estratégica y principales productos y servicios financieros. Adicionalmente se describe el plan de la investigación.
2 Marco teórico: en esta sección se realiza una descripción acerca de metodologías para modelamiento de procesos, identificación de riesgos y la explicación del contenido del marco de referencia COBIT 5.0
3 Metodología: en esta sección se explica los mecanismos de aplicación de ARIS PLATFORM, con los modelos integrados para una gestión por procesos con enfoque de riesgos, así como las herramientas para levantamiento de información.
4 Discusión y resultados: en esta sección, presentan los resultados del levantamiento de procesos y la identificación de riesgos en el marco de referencia COBIT 5.0 de forma integrada, como base para la medición, diseño de controles y monitoreo de los resultados.
5 Conclusiones y Recomendaciones: en esta sección se evidencia el cumplimiento de los objetivos específicos así como posibles cursos de acción futuros a seguir

Palabras clave: COBIT 5.0, Gestión de Riesgo Operativo, Gestión de Tecnologías de Información y Comunicación.

ABSTRACT

This research has the as a main objective the Identification of factors and events of operational risk in TI Management process based on COBIT 5.0 case Banco del Estado, understood as a risk factor for primary cause or origin of an operational risk event. The factors are the processes, people, TI and external events, while an event is understood as that which may result in financial loss to the audited entity.

The structure of the research has been divided into 5 chapters as detailed below:

1 Introduction: This section presents an overview of Banco del Estado, pointing out aspects of its history, strategic planning and major products and financial services.
2 Background: This section provides a description of methodologies for process modeling, risk identification and explanation about contents of COBIT 5.0 framework.
3 Methodology: In this section the implementation mechanisms of ARIS PLATFORM, with integrated models for process management approach to risk, as well as tools for gathering information is explained.
4 Discussion and results: This section presents the results of the survey process and the identification of risks in the COBIT 5.0 framework seamlessly as a basis for measurement, control design and monitoring of results.
5 Conclusions and Recommendations : This section fulfilling the specific objectives and possible future courses of action to follow evidence

Keywords: COBIT 5.0, Operational Risk Management, TI Management.

.

1 INTRODUCCIÓN

1.1 HISTORIA DE LA INSTITUCIÓN

El nombre actual del “Banco del Estado”, nace con la promulgación de la Ley de Régimen Monetario y Banco del Estado, publicada en el Registro Oficial – Suplemento N° 930, de 7 de mayo de 1992. Sin embargo su nombre no data de la misma fecha de su creación; fue mediante Decreto Ley que se expidió la Ley estatutaria del “Banco de Desarrollo del Ecuador” - BEDE- el 6 de agosto de 1979, fecha desde la cual comienza su funcionamiento como persona jurídica autónoma de derecho privado con finalidad social y pública. Esta Ley, promulgada apenas cuatro días antes del retorno a la democracia en nuestro país, viabilizó la operación de una institución que ya había sido creada mediante Decreto Supremo del 17 de septiembre de 1976 (Banco del Estado, 2012a).

En los considerandos de la Ley de creación, el Consejo Supremo de Gobierno de entonces estableció la necesidad “que el Estado ecuatoriano cuente con una institución financiera que concentre, coordine y distribuya los recursos destinados al financiamiento de proyectos prioritarios de desarrollo del sector público y facilite la aplicación de una sana estrategia de inversión; dentro del marco de los objetivos de desarrollo económico que propugna el Gobierno Nacional”.

Hay que anotar que la incorporación del Ecuador al modelo de sustitución de importaciones implicó que nuestro país estableciera una serie de instituciones públicas que tenían como objetivo propiciar el desarrollo nacional. Así, la creación de instituciones como el BEDE, ahora Banco del Estado, fue un reflejo de la mentalidad desarrollista vigente en aquella época.

Esta orientación desarrollista del Estado puede ser claramente observada en el artículo segundo de la Ley Estatutaria la Ley Estatutaria del Banco de Desarrollo del Ecuador S.A., expedida en 1979, la cual establece que “El objetivo del BEDE es financiar programas, proyectos, obras y servicios del sector público, tales como

Ministerios, Municipios, Consejos Provinciales, etc., que se relacionen con el desarrollo económico nacional".

En este cuerpo legal se establecía, además, que el Directorio estaría integrado por el Ministro de Finanzas, el Presidente de la Junta Nacional de Planificación, el Gerente General del Banco Central, un representante de los organismos regionales de desarrollo, un representante de los organismos seccionales y, como vocales consejeros, el Gerente General y el Subsecretario de Crédito Público. De hecho, la creación misma del BEDE fue una suerte de continuación o institucionalización del Fondo Nacional de Desarrollo (FONADE), establecido en marzo de 1976 y cuyo funcionamiento, inclusive físico, estaba íntimamente relacionado con el Ministerio de Finanzas. Esta institución administraba el fondo establecido para "financiar a través de la concesión de créditos reembolsables a las Municipalidades la ejecución de proyectos de inversión que contribuyan al desarrollo económico y social del país, en sectores considerados como prioritarios por la Junta Nacional de Planificación y que cuenten con los estudios técnicos pertinentes".

Han pasado más de 34 años desde entonces, tiempo en el que el Banco del Estado se ha consolidado institucional y financieramente para convertirse en la entidad líder en el financiamiento de la obra de los gobiernos autónomos descentralizados, brindando servicios financieros y no financieros en las mejores condiciones para sus clientes (Banco del Estado, 2012b).

1.2 PLANIFICACIÓN ESTRATÉGICA INSTITUCIONAL

La planificación estratégica institucional, actualmente tiene un periodo de vigencia 2013 – 2016 y contempla los elementos que se describen en los siguientes numerales.

1.2.1 Misión

La misión del Banco del Estado se ha definido de la siguiente manera:

“Impulsar, acorde a las políticas de Estado, el desarrollo sostenible con equidad social y regional, promoviendo la competitividad territorial, mediante la oferta de soluciones financieras y servicios de asistencia técnica, para mejorar la calidad de vida de la población” (Banco del Estado, 2012a).

Como se puede apreciar en la misión, el eje fundamental se basa en el componente social, alineado a Ley de Régimen Monetario y del Banco del Estado, cuya última actualización se registra el lunes 5 de Octubre del 2009, Suplemento Registro Oficial - Nro. 40, lo que hace de esta, una institución estratégica dentro del sector público para el financiamiento de proyectos para el acceso a mejores condiciones de vida.

1.2.2 Visión

“Consolidarse como un banco de desarrollo referente de excelencia en el financiamiento de la inversión pública” (Banco del Estado, 2012a).

La visión del Banco del Estado, tiene un enfoque prioritario a generar un posicioneamiento de excelencia. Sin embargo, no se puede identificar claramente los factores de excelencia, y consecuentemente, su medición resulta difícil de ejecutar. Adicionalmente, y con la reciente adopción de la competencia en materia de Vivienda de Interés Social, también se fomenta la inversión privada, con enfoque hacia el bienestar de la población, por lo que se requiere una actualización de la misma incluyendo este línea de negocio estratégico al portafolio de productos de la institución.

1.2.3 Objetivos estratégicos

Los objetivos estratégicos del Banco del Estado, se alinean a cuatro perspectivas que son: 1) Accionistas, Clientes y Comunidad, 2) Financiera, 3) Capital Humano y 4) Procesos Internos. Éstos se muestran en la Figura Nro. 1:

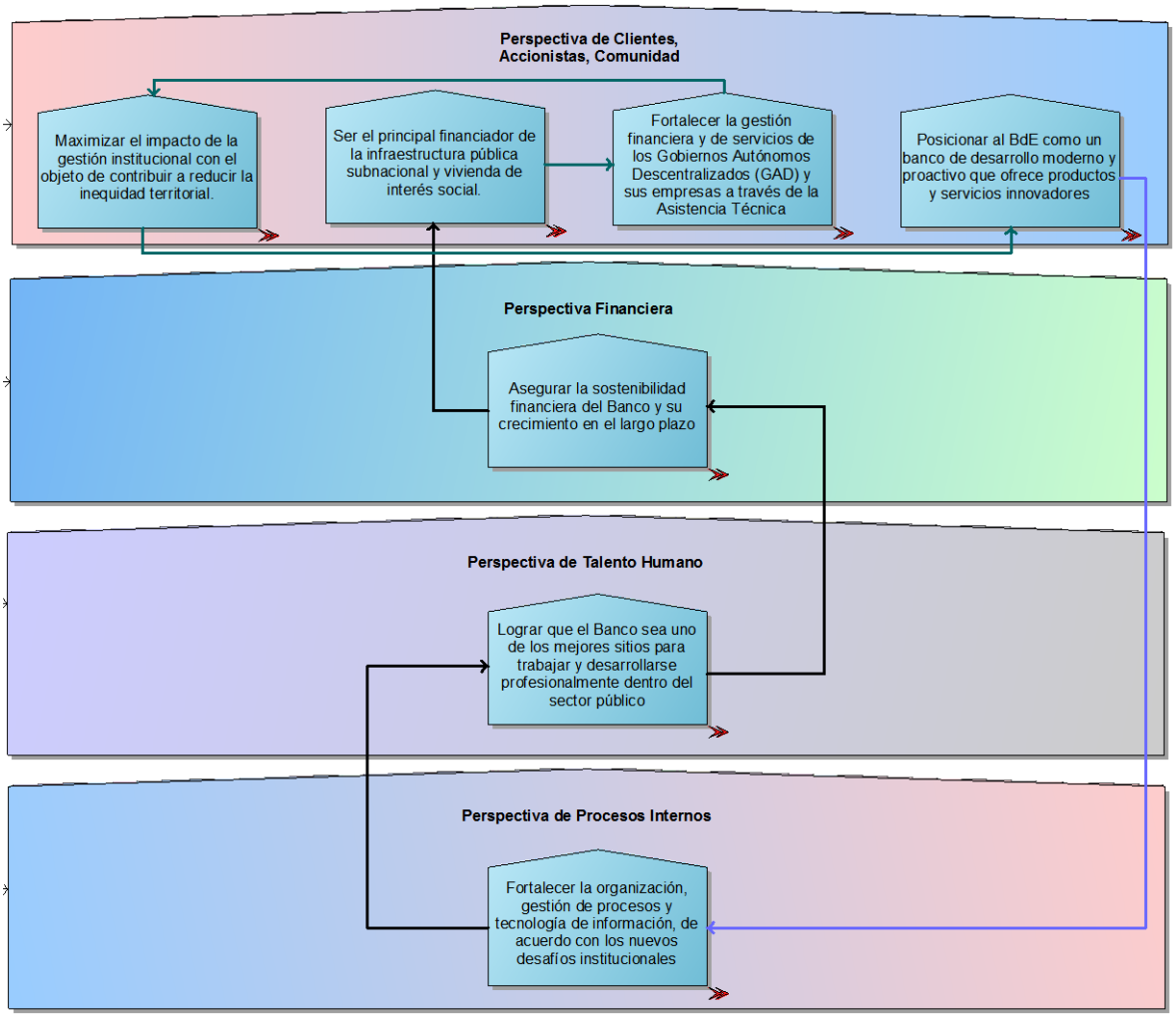


Figura No. 1 Objetivos Estratégicos del Banco del Estado
(Banco del Estado, 2012a)

Haciendo un análisis de los objetivos estratégicos, se puede aseverar que cada uno de ellos tiene un cierto grado de alineamiento hacia la visión, donde ya se incluyen los aspectos relacionados al elemento de Vivienda de Interés Social. Cabe mencionar que cada uno de estos objetivos estratégicos, cuenta con objetivos operativos de menor nivel, los que se pueden encontrar en el Anexo A.

Cabe mencionar que los objetivos estratégicos y objetivos operativos cumplen con el objeto social para el cual el Banco del Estado fue creado, los cuales se resumen a continuación:

- Financiar programas, proyectos, obras, servicios a cargo de los organismos o entidades del sector público
- Financiar en las formas previstas en la ley, actividades privadas.
- Proporcionar asistencia técnica, económica, financiera, legal o administrativa a las entidades y organismos precedentes.
- Administrar los fondos provenientes de créditos externos contratados por el Gobierno Nacional para los programas y proyectos de desarrollo económico y social.
- Financiar proyectos de desarrollo para los sectores productivos y privados en las formas previstas en la ley.
- Financiar la provisión de servicios públicos de responsabilidad del Estado.

Fuente: (Banco del Estado, 2012a)

1.3 ESTRUCTURA ORGANIZACIONAL

Dentro del año 2013, se realizó la respectiva reforma Integral al Estatuto Orgánico de Gestión Organizacional por Procesos del Banco del Estado. Mediante oficio No. 4572-MRL-FI-2013-EDT de 16 de agosto del 2013, el Ministerio de Relaciones Laborales emitió dictamen favorable al proyecto en mención, al amparo de lo establecido en el artículo 51 de la Ley Orgánica de Servicio Público, artículo 136 de su Reglamento General de aplicación y Disposición General Primera de la Norma Técnica de Reglamentos o Estatutos Orgánicos de Gestión Organizacional por Procesos.

Con este antecedente, la estructura organizacional del Banco del Estado quedó diseñada de como se muestra en la Figura Nro. 2:

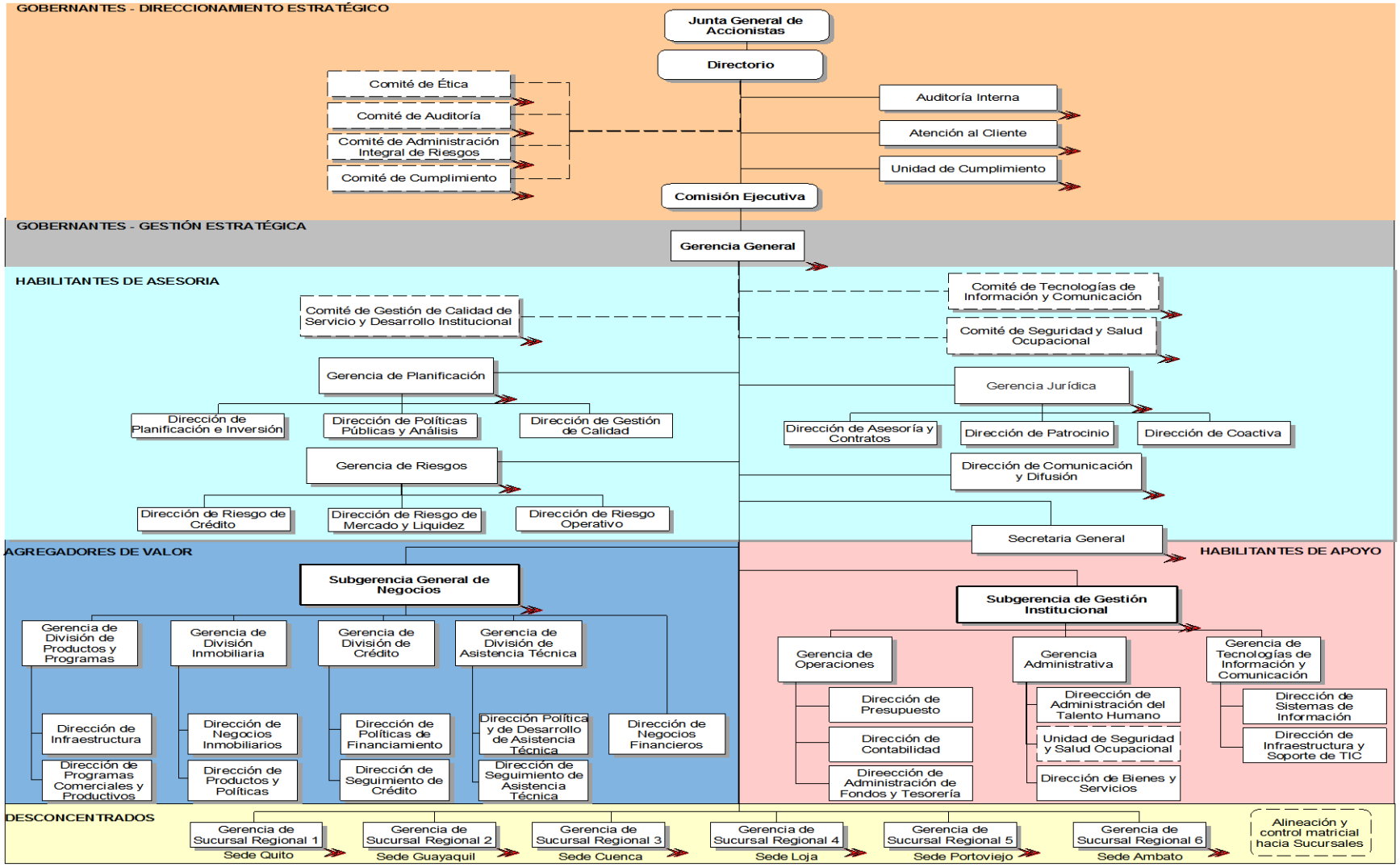


Figura No. 2 Estructura organizacional
(Banco del Estado, 2012a)

Los principales cambios que se suscitaron con la reforma integral se detallan a continuación:

- Se redefine la cadena de valor institucional a través de un esquema gráfico que hace más explícito los procesos que conforman el giro del negocio institucional y sus componentes de asesoría y apoyo. Con base en la nueva cadena de valor se plantea también un nuevo mapa de procesos y los ajustes necesarios en la estructura orgánica.
- En cumplimiento de la normativa específica y vigente, se crean los Comités de Ética, de Tecnologías de Información y Comunicación, y el de Seguridad y Salud Ocupacional.
- Se renombra el Comité de Riesgos por Comité de Administración Integral de Riesgos con el objetivo de denotar el alcance total de esta Gestión, como es, el Riesgo de Mercado, el Riesgo de Crédito, el Riesgo de Liquidez y el Riesgo Operativo adoptado según las Normas de Basilea II.
- La Gerencia de Desarrollo Local y sus Direcciones, son sustituidas por la Gerencia de División Inmobiliaria y sus dos Direcciones: Negocios Inmobiliarios y de Productos y Políticas, lo cual no implica creaciones presupuestarias adicionales.
- Se crea la Dirección de Coactivas para ejecutar los procesos judiciales que permitan hacer efectivo el cobro de las obligaciones vencidas de los clientes del Banco, en particular aquellas resultantes de nuevas competencias en materia de vivienda de interés social.
- Se crea la Gerencia de Tecnologías de Información y Comunicación, en cumplimiento a las recomendaciones de la Superintendencia de Bancos y Seguros sustentadas en el oficio No INF-DNIF1-SAIFQ5-2008-00260 donde señala: “Esto garantizará la oportunidad e independencia del área de tecnología de información…”. Esta creación involucró un cambio en el modelo de gestión de este proceso bajo un esquema alineado a COBIT 5.0, lo que es el objeto de estudio de la presente investigación.
- Se crea la Dirección de Infraestructura y Soporte de TIC, área especializada en el manejo y soporte técnico de los recursos tecnológicos,

incluyendo la operación del centro de cómputo, redes y telecomunicaciones, cuyos procesos y servicios logran una mayor eficacia al ser gestionados de forma interdependiente y complementaria a la Dirección de Sistemas de Información.

- Se crea la Gerencia Administrativa en lugar de la Gerencia de Talento Humano convirtiéndose esta última en una Dirección administrada por dicha gerencia.
- En la estructura tipo de la Sucursales Regionales se suprime como Unidad Administrativa, el área de Comunicación y Difusión, cuyos procesos y productos son asignados a la Coordinación de Gestión Institucional, como proceso desconcentrado.
- Se incluye la Unidad de Atención al Cliente, para dar cumplimiento a lo establecido en la Codificación de Resoluciones de la Junta Bancaria, LIBRO I, Título XIV, CAPÍTULO V.- De la protección al usuario financiero, de los servicios de información y atención de reclamos (JB-2013-2393 de 22 de enero del 2013), sin que la misma implique la creación de un puesto del Nivel Jerárquico Superior.
- Conforme al Plan Estratégico 2013-2016, la Estructura Organizacional planteada guarda concordancia con los objetivos estratégicos desarrollados para cada una de las perspectivas.

1.4 PRODUCTOS Y SERVICIOS

Dentro del portafolio de productos financieros que el Banco del Estado ha puesto a disposición del sector público y privado, se puede realizar una categorización en dos grandes líneas de financiamiento de pre inversión e inversión en:

- Inversión Pública
- Vivienda de Interés Social

Adicionalmente se ha creado los servicios de Asistencia Técnica, que representa la preventa del financiamiento, con la finalidad de mejorar las capacidades

técnicas y financieras de los clientes del Banco del Estado, previo a la solicitud de financiamiento.

1.4.1 Crédito de inversión pública

El crédito de inversión pública, está dirigido a entidades del sector público (Empresas Públicas y Gobiernos Autónomos Descentralizados) para el mejoramiento de la calidad dentro del ámbito de su competencia, agrupando las líneas de financiamiento en los siguientes programas principales:

a) PROVERDE

El Programa de Recuperación de Espacios de Convivencia Ciudadana Orientados a la Sustentabilidad Ambiental para el Buen Vivir, - denominado PROVERDE- tiene como objetivo promover a los Gobiernos Autónomos Descentralizados (GAD) al desarrollo sustentable de sus territorios. Por medio de esta iniciativa, el BdE financia proyectos para mejorar la calidad ambiental, la preservación de recursos naturales y la generación de áreas de convivencia entre el ser humano y los ecosistemas (Banco del Estado, 2012c).

Cumpliendo este objetivo, PROVERDE se divide en dos componentes. El primero constituido en un “Fondo de Financiamiento de Proyectos” conformado por incentivos de financiamiento, créditos y recursos no reembolsables. Y el segundo, un fondo concursable anual, orientado a institucionalizar el “Premio Verde Banco del Estado”, que es entregado como un reconocimiento a los GAD que presenten prácticas verdes innovadoras.

b) GESTIÓN PATRIMONIAL

Gestión Patrimonial busca contribuir al financiamiento de proyectos integrales de conservación y dinamización de los patrimonios de los Gobiernos Autónomos Descentralizados en todo Ecuador. Cuenta con el apoyo técnico-financiero del

Ministerio de Cultura y Patrimonio, del Instituto Nacional de Patrimonio Cultural y del Banco del Estado (Banco del Estado, 2012c).

El programa financia proyectos dirigidos a recuperar, rehabilitar y construir obras de infraestructura que permitan mitigar los impactos, por causas naturales o antrópicas, y a establecer nuevos usos para los inmuebles recuperados.

c) EQUIPAMIENTO URBANO Y COMERCIAL

El Programa financia proyectos de equipamientos urbanos comerciales como centros de faenamiento, terminales terrestres, cementerios, estacionamientos y mercados públicos. El objetivo es mejorar la calidad de vida de la población en los distintos Gobiernos Autónomos Descentralizados.

Asimismo, impulsa oportunidades económicas en los territorios con modelos de gestión que garanticen la calidad de los servicios, la sostenibilidad del proyecto y la generación de recursos para la municipalidad a partir de los flujos del negocio.

d) PROINDEPOR

El objetivo es ejecutar proyectos de pre inversión e inversión. El primero realiza estudios técnicos, económicos, financieros, ambientales, participación comunitaria y gestión del servicio que permitan obtener rentabilidad socioeconómica. El segundo, financia obras de mejoramiento, rehabilitación, terminación, complementación, restauración, entre otras de infraestructura deportiva (Banco del Estado, 2012c).

e) PROSANEAMIENTO

El Programa de Saneamiento Ambiental Nacional, “PROSANEAMIENTO”, es la integración de los programas mediante los cuales el Banco del Estado financia

proyectos de los sectores de agua potable, saneamiento y gestión de desechos sólidos (Banco del Estado, 2012c).

Tales sectores han sido señalados como prioritarios por el Gobierno Nacional, que a su vez se ha comprometido a invertir los recursos necesarios para cerrar la brecha de cobertura, de tal manera que llegue al 95% en cada servicio, hasta el año 2017.

1.4.2 Vivienda de interés social (VIS)

El programa está dirigido a promotores inmobiliarios públicos y privados, combinando un componente no reembolsable, correspondiente a bonos de la vivienda, y un componente reembolsable de financiamiento para el desarrollo de proyectos VIS en áreas urbanas consolidadas a lo largo del territorio nacional.

El programa de financiamiento inmobiliario del Banco del Estado, PROHABITAT-VIVIENDA, se encuentra dentro del nuevo esquema de intervención pública para crear incentivos a la vivienda de interés social, que busca disminuir el costo de vivienda para los grupos de menores ingresos mediante subsidios y generando nuevos instrumentos de financiamiento para que el mercado de vivienda sea compatible con el perfil socioeconómico de los hogares de menores ingresos (Banco del Estado, 2012c).

De esta manera, articulándose con el bono de la vivienda, e incorporando otros incentivos financieros, el programa tiene como objetivo viabilizar y efectivizar la alta demanda de vivienda de interés social.

1.4.3 Servicios de asistencia técnica

Asistencia Técnica constituye un producto estratégico que el Banco del Estado brinda a sus clientes, mediante el diseño e implementación de programas y productos, los que se enriquecen continuamente en base al proceso proactivo

generado entre el Banco y sus clientes; así como también, a los nuevos retos que debe afrontar la gestión pública (Banco del Estado, 2012c).

Este servicio se divide en tres grandes grupos que son:

a) Programas de corresponsabilidad

a. Contribución especial de mejoras: Consiste en generar incentivos para que los GAD mejoren sus ingresos propios a través de la recaudación de la Contribución Especial de Mejoras (CEM), que es un tributo cuyo objeto "es el beneficio real o presuntivo proporcionado a las propiedades inmuebles urbanas por la construcción de cualquier obra pública" (Art. 569 COOTAD).
b. Cartera vencida: El Banco mediante el producto cartera vencida, propone directrices claras para el mejoramiento de recursos propios que instan a los GAD a cumplir con su responsabilidad de cobro.
c. Patentes y activos totales: Asistencia Técnica junto a los GAD elaboran e implementan planes de trabajo tendientes a mejorar la aplicación de los impuestos por Patentes y Activos Totales, estos tributos recaen en las actividades comerciales, industriales y financieras que se llevan a cabo en los distintos municipios. Así se fomenta el involucramiento en la gestión pública de todos los actores que forman parte del territorio.

b) Asistencia técnica para vivienda de interés social

Para contribuir a garantizar el derecho al hábitat y a una vivienda digna de las personas de escasos recursos económicos, el programa de Asistencia Técnica para Vivienda de Interés Social (PATVIS) busca que las entidades involucradas en el proceso, implementen normativas y herramientas técnicas acordes a sus características y realidades, propongan procedimientos simplificados que permitan mejorar los procesos actuales con criterios de eficiencia, fomenten la

participación de promotores públicos y privados en la ejecución de proyectos de Vivienda de Interés Social en los territorios, a la vez de generar espacios de aprendizaje, intercambio y réplica de mejores prácticas, que será fundamental en este proceso (Banco del Estado, 2012c).

c) Gestión de servicios

Asistencia técnica a través del asesoramiento directo o la contratación de servicios especializados de empresas públicas o privadas con altos estándares de eficiencia impulsa a los GAD Municipales y a sus Empresas Públicas a mejorar la gestión administrativa, financiera, comercial y operacional de los servicios de agua potable, saneamiento y desechos sólidos, aplicando la metodología "Aprender – Haciendo" con participación directa del personal del GAD o Empresa, a fin de desarrollar destrezas y habilidades en dichos funcionarios, lo que permitirá que exista una transferencia real de tecnología y la generación de capacidades locales.

1.5 ESTADÍSTICAS CREDITICIAS

Para realizar un análisis apropiado de las estadísticas crediticias, se ha tomado en consideración el periodo 2007 – 2013, debido a la continuidad del régimen del Gobierno del Ec. Rafael Correa Delgado, evidenciando cierta estabilidad en lo que al negocio financiero del Banco del Estado concierne.

1.5.1 Evolución de las aprobaciones

Las aprobaciones, son los montos que corresponden a los créditos que ya tienen la decisión gerencial o resolución de directorio, para su ejecución. Cabe mencionar que los valores que se presentan a continuación son montos consolidados de las 6 sucursales regionales que actualmente posee el Banco del Estado:

	2007	2008	2009	2010	2011	2012	2013
ASIGNADO	121.279.342	586.206.250	313.459.333	673.449.352	667.925.782	454.046.382	493.544.705

Figura No. 3 Estadísticas de aprobaciones periodo 2007 – 2013
(Banco del Estado, 2012a)

Como se observa en la Figura No. 3, existe un comportamiento variable en la evolución de las aprobaciones, con los picos más altos en los años 2010 y 2011. Esto se debe a que en estos periodos existieron fuentes de financiamiento provenientes de Fondos en Administración, además del mejoramiento del cupo de endeudamiento gracias a la Ley de Distribución del 15% a Gobiernos Seccionales. Estos organismos deben poner en ejecución, preferentemente, con cargo a este Fondo, planes o proyectos destinados al mejoramiento del nivel de vida de los sectores de menor desarrollo.

1.5.2 Evolución de los desembolsos

Los desembolsos, corresponden a las entregas de recursos que se realizan a los clientes del Banco, para la ejecución de sus proyectos. A igual que el caso anterior, los valores que se presentan son consolidados de las 6 sucursales regionales que el Banco del Estado actualmente posee y estos son:

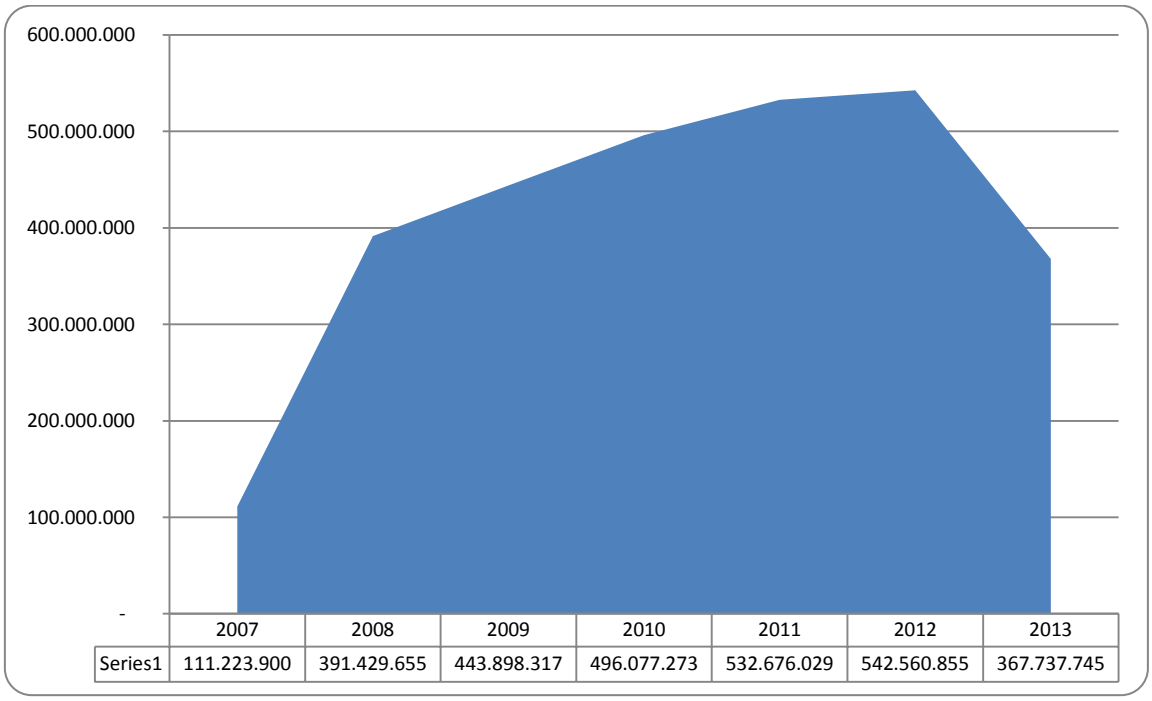


Figura No. 4 Estadísticas de desembolsos periodo 2007 – 2013
(Banco del Estado, 2012a)

Al igual que en el caso anterior, en la Figura No. 4 se observa la misma tendencia variable con los picos en los años 2010 y 2011. Cabe mencionar adicionalmente, que el comportamiento de los desembolsos, obedece a los criterios de la planificación institucional, estructurado en base al Plan Anual de Inversiones y a la disponibilidad presupuestaria para la entrega de recursos.

1.5.3 Productos por segmento de mercado

Tras años de trayectoria en el financiamiento de proyectos para inversión pública, sin duda alguna, el producto que se cataloga como la línea de negocio estrella, son los créditos para agua potable, alcantarillado y residuos sólidos, los que se encuentran catalogados dentro del programa PROSANEAMIENTO, con el 15% del total de los créditos vigentes dentro del segmento del 70% de Gobiernos Autónomos Descentralizados Municipales, dadas las competencias establecidas en el Código Orgánico de Organización Territorial, Autonomías y Descentralización (COOTAD). Dadas las condiciones actuales del Banco del

Estado, se presenta la Figura No. 5 en donde se ilustran los productos financieros por segmento de mercado:

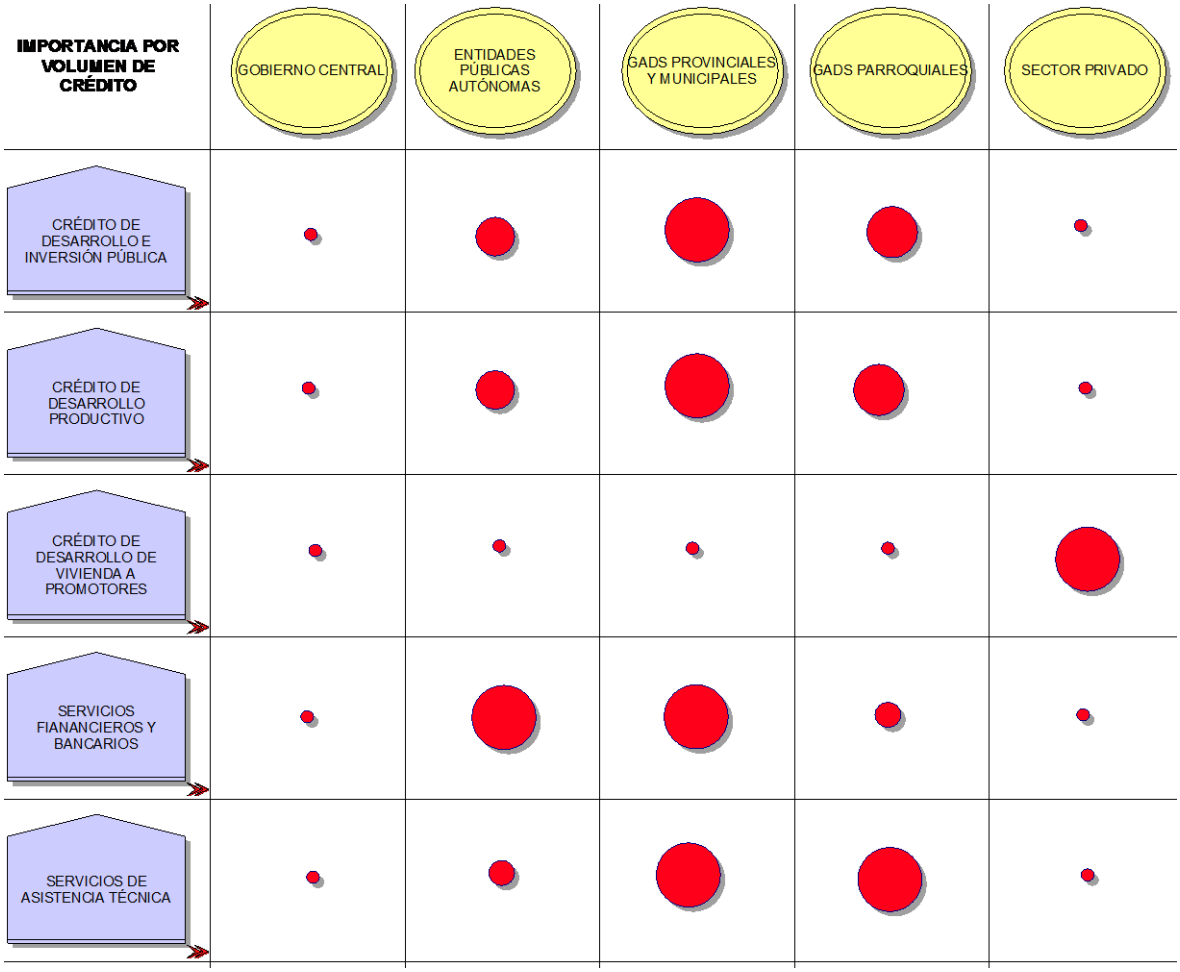


Figura No. 5 Productos por segmento de mercado
(Banco del Estado, 2012a)

Como se aprecia en la Figura No. 5, claramente se observa que los principales clientes del Banco del Estado son los Gobiernos Autónomos Descentralizados Municipales en todas las líneas de negocio, con excepción del Crédito de Vivienda de Interés Social, cuyo pilar fundamental de operación, se centra en el sector privado.

Toda esta sólida operación financiera, se debe en gran medida, al soporte que el proceso de Gestión de Tecnologías de Información y Comunicación, ofrece como soporte para el Proceso de Gestión del Financiamiento.

1.6 DISEÑO DE LA INVESTIGACIÓN

1.6.1 Planteamiento del Problema

El Banco del Estado es una institución financiera pública que se encarga de otorgar soluciones financieras y servicios de asistencia técnica para el mejoramiento de la calidad de vida de los ciudadanos ecuatorianos. Para el año 2012, la institución desembolsó USD 542.594.157 a 221 GAD´S a nivel nacional (Banco del Estado, 2012a) con una focalización del crédito hacia el desarrollo múltiple, educación y cultura, equipamiento urbano, fortalecimiento institucional, medio ambiente, desastres naturales, riego, control de inundaciones, saneamiento ambiental turismo y vialidad.

Todo este esfuerzo, se ve canalizado a través del constante y continuo mejoramiento del proceso de crédito, el cual, en la actualidad se encuentra automatizado dentro de la herramienta BPMS, lo que ha ayudado a ejercer un adecuado control del proceso, en términos de tiempo y carga de trabajo.

En la actualidad, la Dirección de Riesgo Operativo, que forma parte dentro de la Gerencia de Riesgos, ha desarrollado un Plan de Contingencia para garantizar la continuidad del proceso de crédito, obteniendo como resultado, el mapeo de riesgos del mismo, la medición del nivel de probabilidades de ocurrencia, y el respectivo Plan de Continuidad debidamente probado, pero no ha considerado un factor muy importante que es el recurso que mantiene operativo a dicho proceso, como lo es el proceso de Gestión de Tecnologías de Información y Comunicaciones.

Por un lado, la normativa de la Superintendencia de Bancos y Seguros, exige a todas las instituciones financieras que dispongan de un Plan de Continuidad en sus procesos críticos como parte de la Gestión de Riesgo Operativo del Negocio (Superintendencia de Bancos y Seguros del Ecuador, 2005), y por otro, las Normas de Basilea II, plantean que deben identificar factores y eventos de riesgo

dentro de los procesos, basado en cuatro ejes que son: procesos, personas, riesgos de TIC y eventos externos (Bassel Comittee on Bankin Supervision, 2006). En ambos casos, no se está cumpliendo con la normativa para el proceso de Gestión de Tecnologías de Información.

1.6.2 Formulación y Sistematización del Problema

1.6.2.1 *Formulación*

¿Cuáles son los factores y eventos de riesgo operativo dentro del proceso de Gestión De Tecnologías de Información y Comunicaciones basado en COBIT 5.0 en el Banco del Estado?

1.6.2.2 *Sistematización*

- ¿Cuáles son las herramientas metodológicas y tecnológicas apropiadas para la identificación de riesgos en procesos?
- ¿Cuál es el detalle de actividades del Marco de Referencia COBIT 5.0 aplicado al Banco del Estado dentro del Proceso de Gestión de Tecnologías de Información y Comunicaciones?
- ¿Cuáles son los factores y eventos de riesgo que enfrenta el Marco de Referencia COBIT 5.0 aplicado al Banco del Estado, dentro del Proceso de Gestión de Tecnologías de Información y Comunicaciones?

1.6.3 Objetivos de la Investigación

1.6.3.1 *Objetivo General*

Identificar los factores y eventos de riesgo operativo dentro del proceso de Gestión De Tecnologías de Información y Comunicaciones basado en COBIT 5.0 en el Banco del Estado.

1.6.3.2 *Objetivos Específicos*

- Identificar la metodología para el levantamiento de procesos y riesgos para su modelado de manera integrada.
- Mapear los procesos de TI a nivel de actividades, en base al Marco de Referencia COBIT 5.0 a nivel de actividades, como base para el levantamiento de riesgos.
- Identificar los riesgos operativos en el proceso de Gestión de Tecnologías de Información asociados al Marco de Referencia COBIT 5.0.

1.6.4 Justificación del Proyecto

El presente estudio tiene como finalidad el establecimiento de una metodología estándar para el diseño y modelado de los procesos y riesgos del Banco del Estado en la herramienta ARIS PLATFORM, así como establecer pautas generales para la adecuada administración y organización de dichos procesos. De este modo, los usuarios modeladores podrán utilizar este estudio como una guía para documentar los procesos en ARIS de manera uniforme y estandarizada.

Cabe destacar que la herramienta ARIS PLATFORM, contiene una variedad de modelos que pueden ser adaptados según las necesidades de cada organización, trabajo que aún no ha sido realizado por las áreas de Calidad y Riesgos dentro de la Institución, debido a la reciente adquisición de esta herramienta tecnológica.

En otro ámbito del conocimiento, la aplicación del Marco de Referencia COBIT 5.0, publicado por la compañía ISACA en el año 2013, tiene como principal objetivo garantizar la seguridad de las empresas mejorando la gestión de TI y el cumplimiento de riesgos relacionados. En este sentido, cabe mencionar que este marco de referencia aún no está siendo aplicado en ninguna Institución Financiera Pública del Ecuador, teniendo el mayor avance en la Corporación Financiera Nacional, que ha llegado implementar COBIT 4.0. (ISACA, 2013). Por estas razones, el Banco del Estado ha sido pionero en implementar estas prácticas de gestión de TI, faltando únicamente el correspondiente mapeo de procesos y

levantamiento de riesgos para cumplir con todos los requerimientos legales y prácticas de gestión vanguardistas.

Dentro de las próximas versiones de COBIT, se espera se expidan certificaciones relacionadas con la aplicación del Marco de Referencia, para lo cual, con la presente investigación, ya se dejan sentadas las bases hasta que esto ocurra.

1.6.5 Hipótesis

Los factores y eventos de riesgos que se identificarán dentro del Proceso de Gestión de Tecnologías de Información y Comunicaciones con base a COBIT 5.0 se encuentran concentrados en la categoría de “procesos”.

2 MARCO TEÓRICO

2.1 METODOLOGÍAS PARA EL MODELAMIENTO DE PROCESOS

2.1.1 Modelamiento de procesos en notación BPMN

BPMN (Business Process Modeling Notation) es una notación gráfica creada para proveer un lenguaje unificado de acepción mundial, utilizada para la especificación de procesos de negocio (…) (BizAgi, 2009)

Utilizando la metodología de modelamiento BPMN, es posible crear un modelo de proceso, con un enfoque a la automatización, es decir, se emplea una iconografía que facilita la parametrización de las actividades y de las reglas de negocio.

Entre las principales ventajas que presenta este esquema de modelamiento se pueden citar los siguientes:

- Provee una notación única y consistente.
- Facilita la automatización.
- Se requiere de menos conocimientos de programación para la automatización de un proceso.

Entre las principales desventajas que presenta este esquema de modelamiento se pueden citar las siguientes:

- La nomenclatura puede ocasionar confusión en el usuario.
- Fracaso en la implementación del BPM cuando una organización tiene bajo nivel de madurez en el conocimiento de sus procesos.
- No asocia los riesgos implícitos del proceso.

El diagrama de procesos en notación BPMN se utiliza principalmente para modelar modelos de proceso. Los elementos de modelación más importantes son las actividades, los eventos y los gateways (nodos de flujo), así como los flujos de

secuencia entre todos ellos. Para agregar más información al proceso pueden agregarse otras estructuras de modelación, como por ejemplo, objetos de datos o artefactos. (Software AG, 2013).

La Figura No. 6 presenta un diagrama de flujo en notación BPMN:

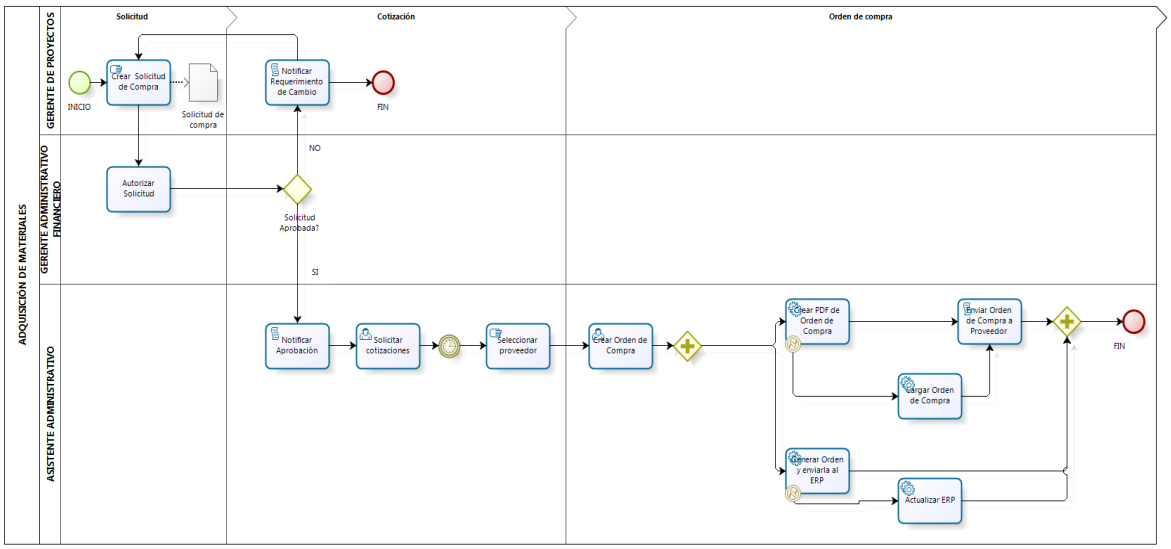


Figura No. 6 Diagrama en notación BPMN
(BizAgi, 2009)

2.1.2 Modelamiento de procesos en CPE (Cadena de Procesos Basadas en Eventos)

Con ayuda de cadenas de proceso controladas por eventos (CPE) se representan la organización y el desarrollo de los procesos que tienen lugar dentro de la empresa, es decir se representa la interconexión entre los objetos de la vista de datos, de la vista de funciones y de la vista organizacional (Software AG, 2013).

El orden de procesamiento de las funciones en el contexto de procesos empresariales se representa mediante cadenas de procesos. Para cada función pueden modelarse los eventos iniciales y finales. Los eventos son tanto desencadenadores como resultados de funciones (Software AG, 2013).

El cambio de estado de un objeto de información puede referirse a la primera aparición de dicho objeto (como por ejemplo: Llegada la consulta del cliente) o a

un cambio de estado registrado en una ocurrencia de atributo (por ejemplo: Rechazada la oferta). Debido a que los objetos de información y los atributos son descritos en la vista de datos de ARIS, la representación controlada por eventos de cadenas de proceso es una unión entre la vista de datos y la de funciones y, por lo tanto, está asignada a la vista de control. Los eventos presentan una forma hexagonal.

El nombre del evento debe contener el objeto de información (Pedido) y también el cambio de estado de dicho objeto de información (Entrada). Ya que los eventos definen la condición o el estado necesarios para iniciar una función y la condición o el estado necesarios para concluir dicha función, los nodos iniciales y finales de una CPE son siempre eventos.

De un mismo evento pueden salir varias funciones al mismo tiempo, del mismo modo una función puede tener como resultado varios eventos. Para representar estas ramificaciones y bucles de procesamiento en una CPE se utiliza una regla en forma de círculo. Este tipo de unión representado por reglas no es sólo gráfico, sino mucho más la relación lógica entre los distintos objetos.

La Figura No. 7 presenta un ejemplo de diagrama en notación CPE.

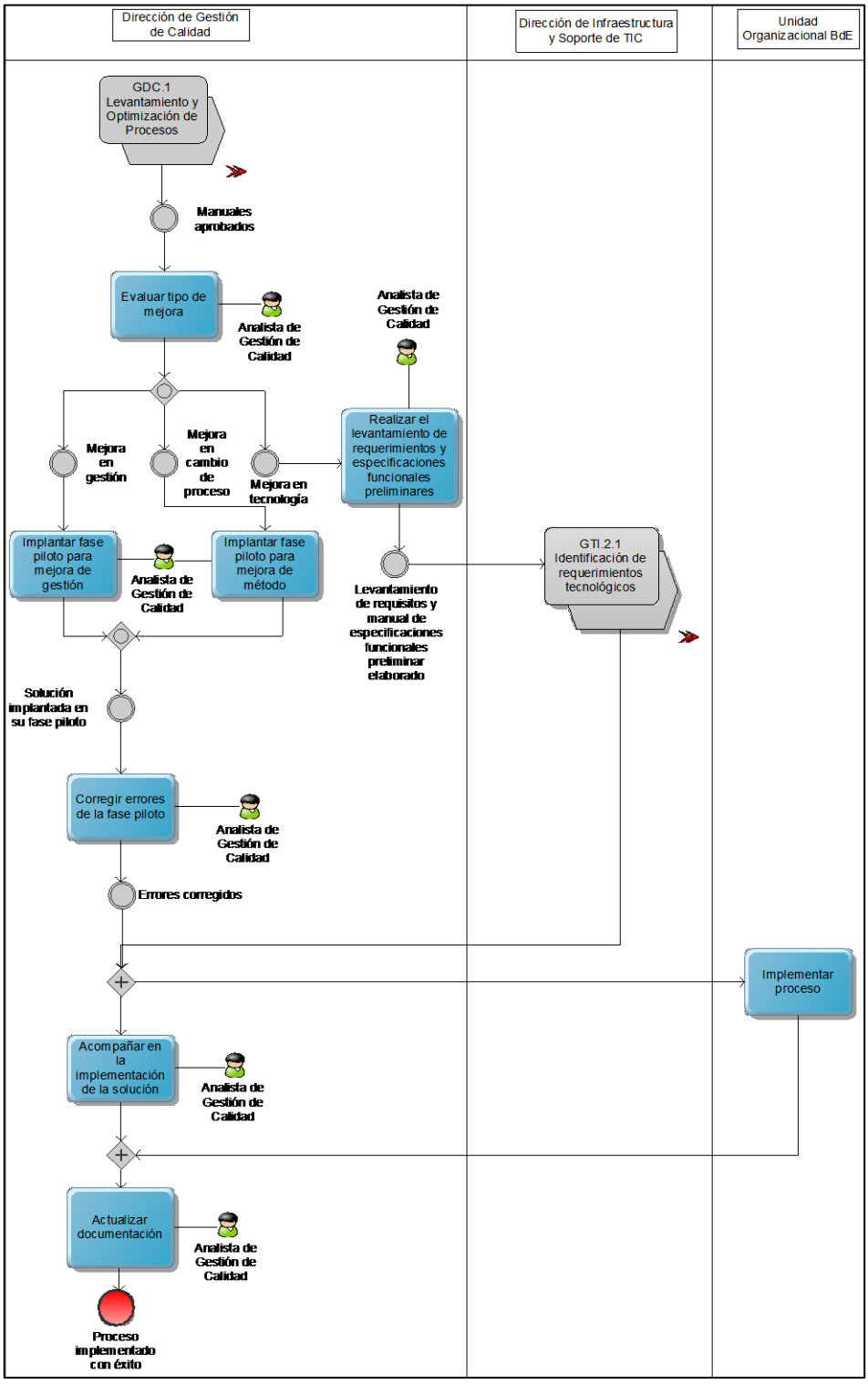


Figura No. 7 Diagrama de flujo en notación CPE
(Software AG, 2013)

2.1.3 Análisis comparativo entre las notaciones BPMN y CPE

Haciendo un análisis comparativo integral, se puede concluir que la notación CPE, es el paso preliminar antes de llegar a la automatización de procesos. Esta notación proporciona información más entendible para el usuario, ya que identifica claramente los eventos intermedios que activan las actividades, convirtiéndose en una poderosa herramienta previa a la migración a la notación BPMN.

Finalmente, al interactuar más amigablemente con el usuario, permite generar oportunidades de mejora con mayor facilidad, al identificar partes críticas dentro del proceso de una manera rápida y sencilla.

2.2 MARCO LEGAL DEL RIESGO OPERATIVO EN EL BANCO DEL ESTADO

El Artículo 5 de la Resolución JB-2005-834, relacionada al Riesgo Operativo dice: *En el marco de la administración integral de riesgos, establecido en la sección II "Administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", las instituciones controladas incluirán el proceso para administrar el riesgo operativo como un riesgo específico, el cual, si no es administrado adecuadamente puede afectar el logro de los objetivos de estabilidad a largo plazo y la continuidad del negocio.*

El diseño del proceso de administración de riesgo operativo deberá permitir a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias. (Superintendencia de Bancos y Seguros del Ecuador, 2005).

Según esta norma, se observa que la gestión de riesgos es obligatoria para todas las instituciones controladas por la Superintendencia de Bancos y Seguros del Ecuador.

Internamente, el Banco del Estado también cuenta con normativa específica como es el Manual de Políticas y Procedimientos para la Gestión del Plan de Continuidad de Negocio con sus respectivos reglamentos en donde se establece un marco para su administración mediante la creación de la infraestructura y la cultura organizacional adecuada permitiendo la aplicación de un método sistémico para identificar, analizar, evaluar, monitorear, controlar y comunicar las amenazas y riesgos a los que está expuesto el proceso de crédito. Con este trabajo se identificarán los insumos para complementar dicho plan, en lo que se refiere al apoyo de TI, para dicho proceso.

2.3 IDENTIFICACIÓN DE FACTORES Y EVENTOS DE RIESGO

Según el Artículo 2 de la Norma Técnica de Gestión del Riesgo Operativo, define a un factor y a un evento de riesgo de la siguiente manera:

Evento de riesgo operativo.- Es el hecho que puede derivar en pérdidas financieras para la institución controlada; (Superintendencia de Bancos y Seguros del Ecuador, 2005)

Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos; (Superintendencia de Bancos y Seguros del Ecuador, 2005)

Definiendo los factores los diferentes factores de riesgo operativo, se puede establecer las siguientes conceptualizaciones:

Riesgo de personas: Comprende la probabilidad de pérdidas asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente desfavorable, falta de especificaciones claras en la contratación de personal, entre otros factores (Dirección de Riesgo Operativo del Banco del Estado, 2013).

Procesos: Identifica las posibles pérdidas relacionadas con el diseño inapropiado de los procesos críticos, o con las políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia, el desarrollo deficiente de las operaciones y servicio o suspensión temporal de los mismos (Dirección de Riesgo Operativo del Banco del Estado, 2013).

Tecnología de información: Incluye la posibilidad de pérdidas financieras derivadas del uso inadecuado de sistemas de información y tecnologías relacionadas, que puedan afectar el desarrollo y servicios que presta la institución al atentar contra la confidencialidad (Dirección de Riesgo Operativo del Banco del Estado, 2013).

Eventos externos: Comprende la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la institución que pueden alterar el desarrollo de sus actividades, así por ejemplo, fallas en los servicios públicos, desastres naturales, atentados, actos delictivos, o fallas en los servicios prestados por terceros (Dirección de Riesgo Operativo del Banco del Estado, 2013).

Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos (Superintendencia de Bancos y Seguros del Ecuador, 2005).

Los tipos de eventos son los siguientes:

- Fraude interno;
- Fraude externo;
- Prácticas laborales y seguridad del ambiente de trabajo;
- Prácticas relacionadas con los clientes, los productos y el negocio;
- Daños a los activos físicos;
- Interrupción del negocio por fallas en la tecnología de información; y,

- Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Fuente: (Bassel Comittee on Bankin Supervision, 2006)

Los eventos de riesgo operativo y las fallas o insuficiencias necesitan ser identificados en relación con los factores de este riesgo a través de una metodología formal (Anexo B), debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (Scorecard), bases de datos u otras.

Dentro del proceso de identificación al que se refiere lo anteriormente citado, las instituciones deben adicionalmente determinar de manera puntual las fallas o insuficiencias de orden legal, de tal manera que les proporcione una visión clara sobre su exposición al riesgo legal, debiendo tener como referencia para el efecto los tipos de evento de riesgo operativo antes indicado.

2.4 EL MARCO DE REFERENCIA COBIT 5.0

2.4.1 Definición de COBIT

COBIT 5 es un marco de referencia para el gobierno y la gestión de TI en las organizaciones. La versión 5.0 incorpora las últimas ideas relacionadas con la gobernanza empresarial y técnicas de gestión, proporcionando principios globalmente aceptados mediante la integración de otros grandes marcos como son: Val IT de ISACA, Biblioteca de Infraestructura de Tecnologías de Información (ITIL ®) y las normas relacionadas de la Organización Internacional de Estandarización (ISO) (ISACA, 2013).

2.4.2 Familia de productos de COBIT

La versión 5.0 de COBIT, se divide en 4 publicaciones que se describen en la Figura No. 8:

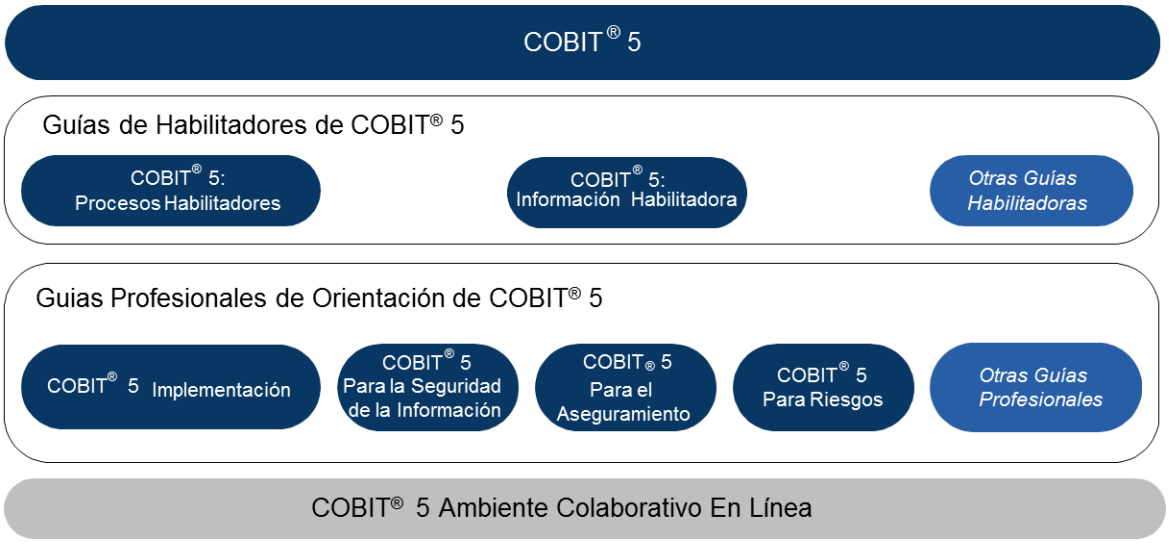


Figura No. 8 Familia de productos de COBIT 5.0
(ISACA, 2013)

Entre los principales productos se describen los siguientes:

- COBIT 5.0 Framework (Información habilitadora): Este producto presenta una síntesis del marco de referencia a manera de resumen ejecutivo para los usuarios de la herramienta.
- COBIT 5.0 Enabling Processes (Procesos habilitadores): Este producto contiene el marco de referencia a nivel de detalle de los 37 procesos que lo conforman, divididos en 5 dominios.
- COBIT 5.0 for Risk IT (Para riesgo): Este producto tiene un enfoque hacia la gestión de riesgo operativo de TI, con sus respectivos mecanismos de identificación y control.
- COBIT 5.0 Online: Es un reemplazo a la versión 4.1 que permite a los usuarios mantener una conexión interactiva y en línea.

2.4.3 Principios de COBIT

El marco de referencia de COBIT 5.0, se basa en cinco principios que se enuncian en la Figura No.9:

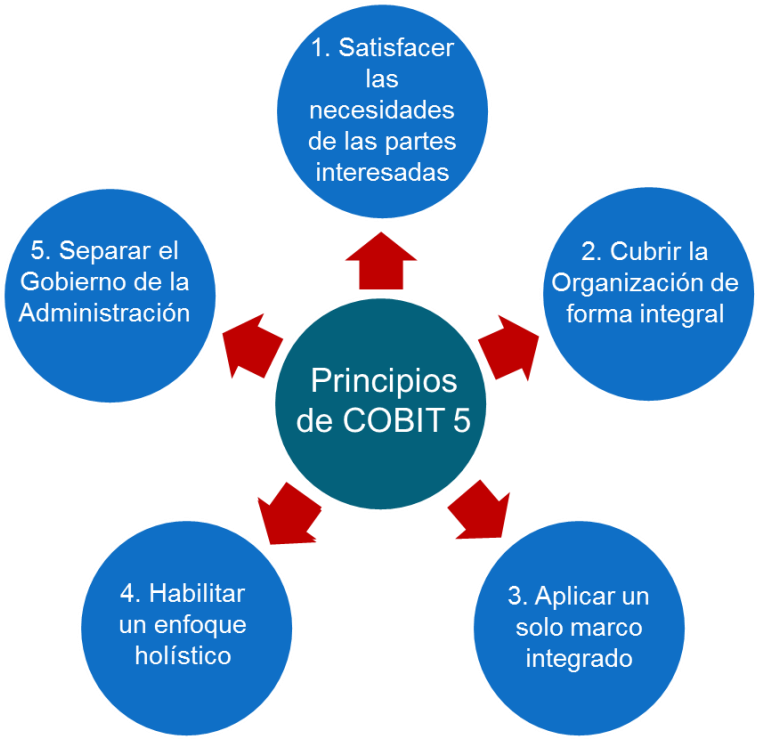


Figura No. 9 Los 5 principios de COBIT
(ISACA, 2013)

- **Principio 1: Satisfacer las necesidades de las partes interesadas**

Las organizaciones tienen muchas partes interesadas y crear valor significa cosas diferentes y a veces conflictivas para cada una de ellas. Las necesidades de las partes interesadas deben ser transformadas en una estrategia accionable para la organización (ISACA, 2013).

- **Principio 2: Cubrir la organización de forma integral:**

COBIT 5 se concentra en el gobierno y la administración de la tecnología de la información relacionados desde una perspectiva integral a nivel de toda la organización, es decir que no solamente se concentra en la “Función de la TI”,

sino trata la tecnología de la información y relacionadas como activos que necesitan ser manejados como cualquier otro activo, por todos en la organización (ISACA, 2013).

- **Principio 3: Aplicar un único marco integrado**

COBIT 5 está alineado con los últimos marcos y normas relevantes usadas por las organizaciones:

  - A nivel corporativo: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
  - Relacionado con TI y gestión de proyectos: ISO/IEC 38500, ITIL, la serie ISO/IEC 27000, TOGAF, PMBOK/PRINCE2, CMMI

Fuente: (ISACA, 2013)

- **Principio 4: Habilitar un enfoque holístico**

Los habilitadores de COBIT 5 son factores que, individual y colectivamente, influyen sobre el funcionamiento del gobierno y administración de la TI corporativa. Estos factores son impulsados por las metas en cascada (numeral 2.4.4), desde el más alto nivel hasta llegar al despliegue de sus procesos (ISACA, 2013).

Estos habilitadores se clasifican en siete categorías como se muestran en la Figura No. 10:

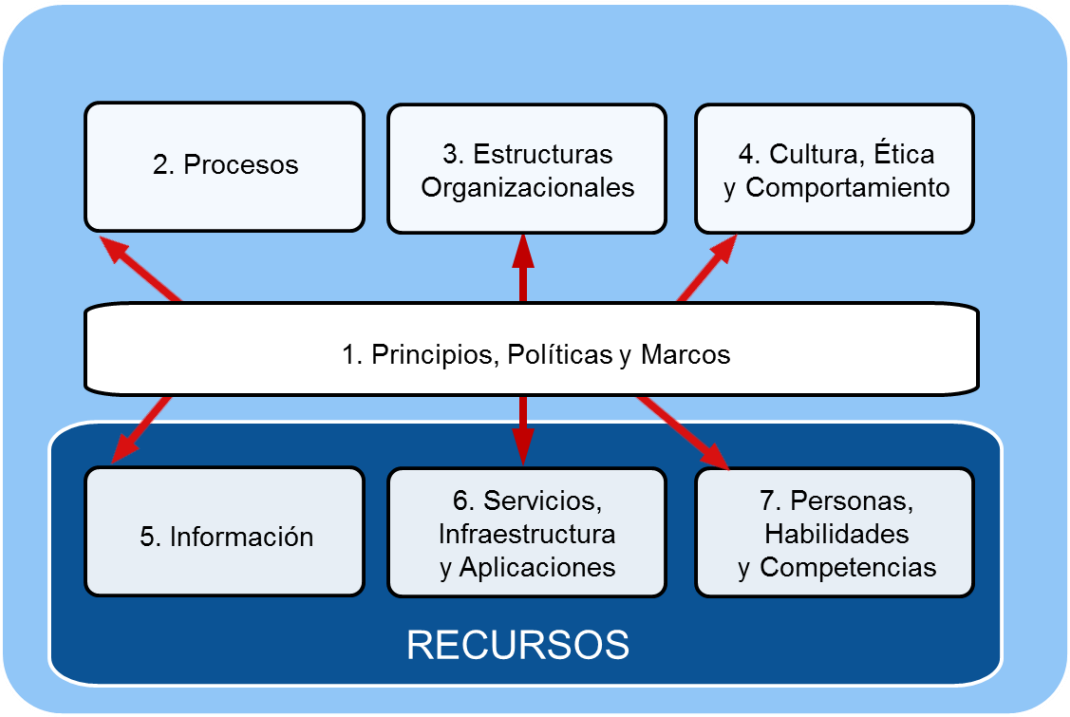


Figura No. 10 Habilitadores de COBIT 5.0 desde un enfoque holístico
(ISACA, 2013)

- **Principio 5: Separar el gobierno de la administración**

COBIT 5.0, hace una discriminación muy marcada de lo que se refiere a las funciones del gobierno y de la administración.

El Gobierno asegura que se evalúen las necesidades de las partes interesadas, así como las condiciones y opciones, para determinar los objetivos corporativos balanceados acordados a lograr, fijando directrices al establecer prioridades y tomar decisiones, además de monitorear el desempeño de su cumplimiento.

La administración planifica, construye, ejecuta y monitorea las actividades conforme a las directrices fijadas por el ente de Gobierno para lograr los objetivos de la Compañía.

COBIT 5 no es obligatorio, pero propone que las organizaciones implementen los procesos de gobierno y administración de tal manera que las áreas claves queden cubiertas, tal como se muestra en la Figura No. 11:

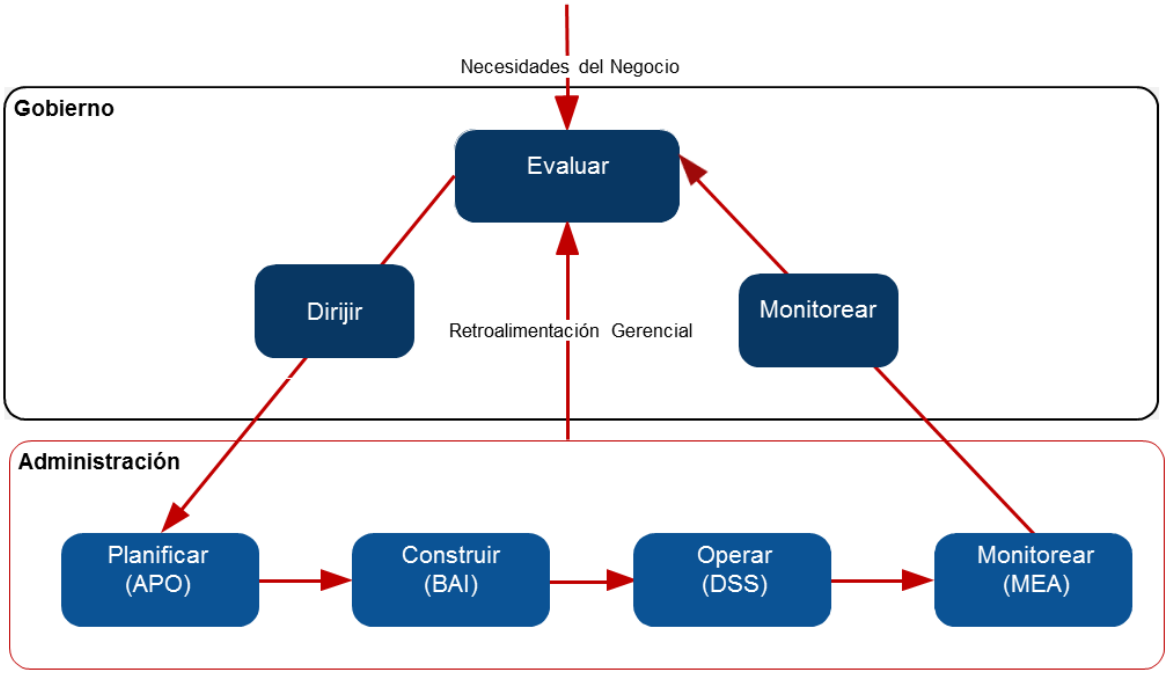


Figura No. 11 Esquema de separación del gobierno y la administración
(ISACA, 2013)

2.4.4 Modelo de objetivos de cascada

Los objetivos en cascada de COBIT 5.0, transforman las necesidades de las partes interesadas en metas específicas, prácticas y personalizadas de acuerdo al giro de negocio de cada organización. La Figura No. 12, muestra el esquema de cascada propuesto por este marco de referencia:

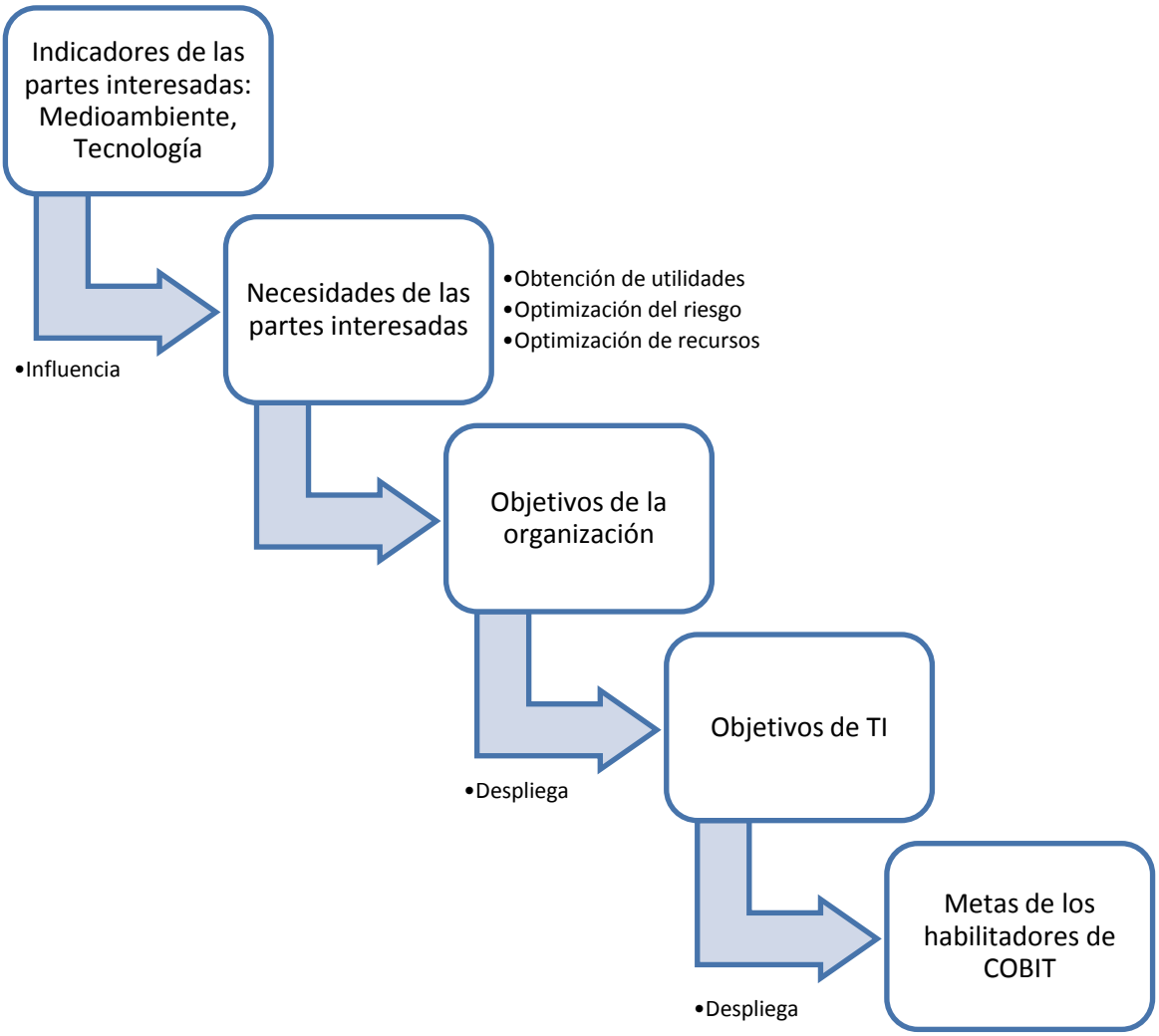


Figura No. 12 Objetivos de cascada de COBIT 5.0
(ISACA, 2013)

Este despliegue, asegura el alineamiento estratégico de todos los objetivos y metas de TI, hacia los objetivos de la organización, definiendo las prioridades para mejoramiento, implementación y aseguramiento del gobierno corporativo de TI, basado en los objetivos estratégicos y riesgos relacionados.

2.4.5 Modelo de procesos de COBIT

El modelo de referencia de procesos de COBIT 5 subdivide las actividades y prácticas de la Organización relacionadas con la TI en dos áreas principales como son el Gobierno y Administración, tal como se muestra en la Figura No. 13:

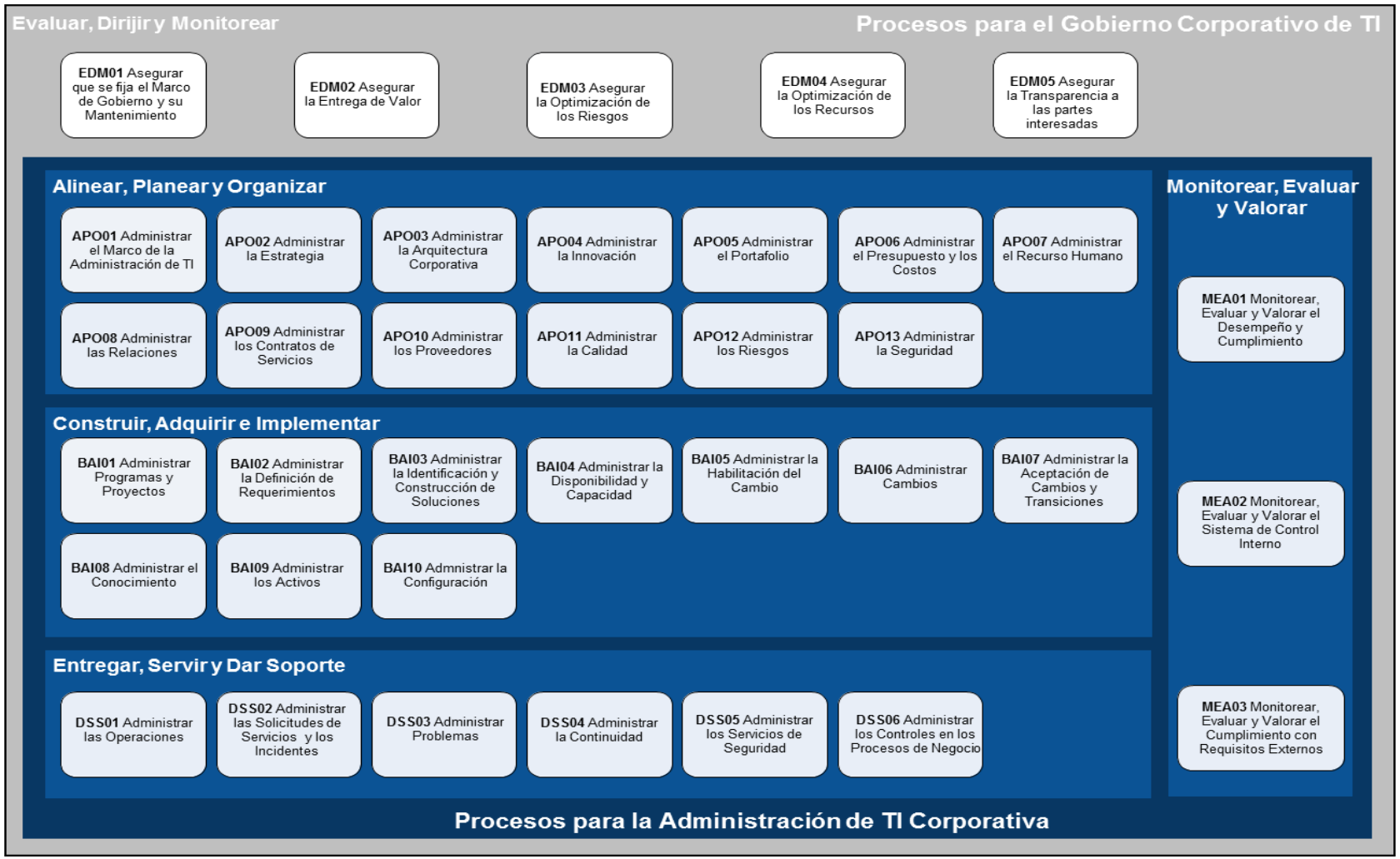


Figura No. 13 Modelo de procesos de COBIT 5.0
(ISACA, 2013)

Dentro de los objetivos de cada grupo de procesos aplicados al caso de estudio, se podrían establecer los siguientes:

1. ***Planificación y Organización de TI:*** Diseñar las directrices estratégicas de la Gestión de las Tecnologías de Información y Comunicación para el cumplimiento del Plan Estratégico.
2. ***Construcción, Adquisición e Implementación de TI:*** Desarrollar soluciones tecnológicas y de comunicaciones que optimicen la consecución de los objetivos estratégicos.
3. ***Entrega de servicio y soporte técnico para las TI:*** Entregar un servicio y soporte técnico de calidad para mantener la infraestructura y aplicativos tecnológicos de la institución garantizando su operación permanente con un enfoque de apoyo hacia la consecución de los objetivos estratégicos.
4. ***Monitoreo y evaluación de TI:*** Monitorear y evaluar los servicios de TI y de la planificación operativa de la unidad con un enfoque hacia el mejoramiento continuo y calidad de servicio hacia el cliente interno.

2.5 APLICACIÓN DE ISO/IEC 27000 AL PROCESO DE GESTIÓN DE LAS SEGURIDADES DE TI

Dentro de la familia de ISO 27000, existen cuatro normas que sirven de base para el diseño e implementación de un Sistema de Gestión de Seguridad Informática, y estas son:

- ISO/IEC 27001:2013: Requerimientos de la norma.
- ISO/IEC 27002:2013: Código de prácticas para los controles de seguridad de la información.
- ISO/IEC 27003:2010: Guía para la implementación del sistema de administración de seguridad de la información.
- ISO/IEC 27004:2009 Medidas para el sistema de administración de seguridad de la información.

Fuente: (International Standard Organization, 2013a)

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo (International Standard Organization, 2013b).

Cada cláusula contiene un número de categorías de seguridad principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

a) Política de Seguridad (1);
b) Organización de la Seguridad de la Información (2);
c) Gestión de Activos (2);
d) Seguridad de Recursos Humanos (3);
e) Seguridad Física y Ambiental (2);
f) Gestión de Comunicaciones y Operaciones (10);
g) Control de Acceso (7);
h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6);
i) Gestión de Incidentes de Seguridad de la Información (2);
j) Gestión de la Continuidad Comercial (1);
k) Conformidad (3).

Fuente: (International Standard Organization, 2013b)

Cabe mencionar que COBIT 5.0, al ser un marco de referencia constituido por los requisitos de ISO 27000 dentro de su modelo de gestión, entre otros, los incluye dentro de los dominios de Construcción, Adquisición e Implementación y Entrega de Servicio y Soporte Técnico, manera integrada tal como se puede apreciar en la Figura No. 14.

Este estándar internacional se alinea perfectamente con el ciclo de ISO 9001:2008, y con ISO 14001:2004 para dar soporte de una manera integrada con

los sistemas de gestión relacionados. Por lo tanto, un sistema de gestión adecuadamente diseñado puede satisfacer todos los requerimientos de estos estándares. En el Anexo C, se muestra la tabla de correspondencias entre ISO 27001, ISO 14001 e ISO 9001.

2.6 APLICACIÓN DE ISO/IEC 15504 AL PROCESO DE MONITOREO Y EVALUACIÓN DE LOS SERVICIOS DE TI

La norma ISO/IEC 15504 proporciona un marco de trabajo para la evaluación de los procesos y establece los requisitos mínimos para realizar una evaluación de forma consistente. Actualmente esta norma está estructurada en siete partes incluyendo la parte en la que se centra este artículo, la “Parte 7: evaluación de la madurez de una organización”, tal como se muestra en la Figura No. 14:

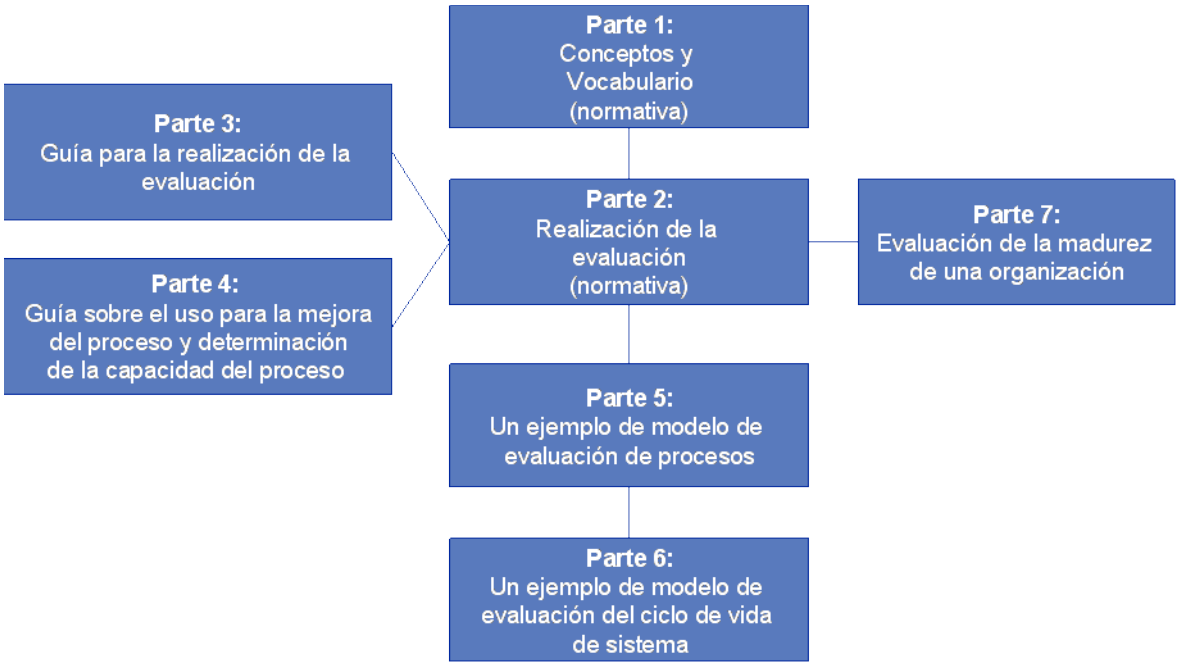


Figura No. 14 Estructura de la norma ISO/IEC 15504
(International Standard Organization, 2013c)

COBIT 5.0, integra los requisitos de esta norma en el dominio de Monitoreo y Evaluación de TI, tal como se observa en la Figura No. 14.

El modelo de procesos de referencia que utiliza ISO/IEC 15504-7, propio de la industria del software, es la norma ISO/IEC 12207.

La norma ISO/IEC 15504-7 establece 6 niveles de madurez para clasificar a las organizaciones, tal y como se muestra en la Figura No. 16

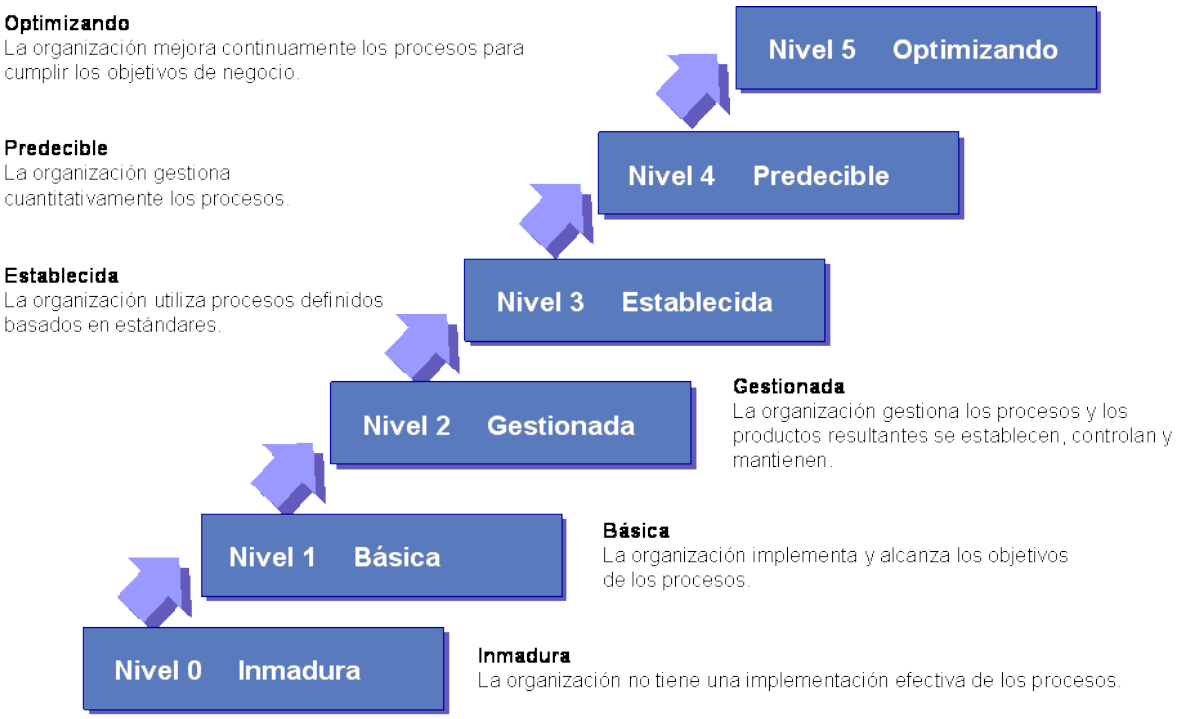


Figura No. 15 Niveles de madurez según ISO IEC/15504 - 7 (INTERNATIONAL STANDARD ORGANIZATION, 2013c)

Para que una organización pueda alcanzar un nivel de madurez debe evaluarse frente a la norma ISO/IEC 15504. Existen 3 clases de evaluaciones, clase 1, clase 2 y clase 3. Estas dos últimas se corresponden con evaluaciones internas y no ofrecen una certificación oficial, a diferencia de la clase 1 que es una evaluación más exhaustiva y rigurosa que permite alcanzar una puntuación oficial.

ISO/IEC 15504-7 es una oportunidad para que las organizaciones puedan obtener una certificación internacional. El modelo referente en la actualidad, CMMI[1], es un

[1] Integración de modelos de madurez de capacidades o Capability maturity model integration (CMMI)

estándar de facto, de uso internacional pero no avalado por una organización internacional como ISO.

Asimismo, con la publicación de esta norma las organizaciones desarrolladores de software utilizarán las buenas prácticas de un modelo de procesos de referencia más adaptado a sus necesidades, ya que ISO/IEC 12207 es más específico en ingeniería del software que el modelo CMMI-DEV[2].

[2] Integración de modelos de madurez de capacidades para el desarrollo o Capability Maturity Model integration for Development (CMMI-DEV)

3 METODOLOGÍA

3.1 APLICACIÓN DE LA HERRAMIENTA ARIS PLATFORM

La herramienta ARIS PLATFORM, en su integralidad contiene varias características que permiten diseñar, documentar, analizar, optimizar y comunicar los procesos para lograr la excelencia organizacional. Las características de ARIS PLATFORM se describen en la Tabla No. 1.

CARACTERÍSTICA	DESCRIPCIÓN
Documentación de procesos	Documentación de la arquitectura empresarial, alineamiento a la estrategia corporativa, procesos de negocio y TI.
Análisis	Análisis costo beneficio, control de versionamiento, consultas, documentación de la historia de cambios y optimización de los tiempos de proceso
Repositorio	Repositorio para información del negocio.
Publicación	Información de los procesos compartida con roles flexibles a través de la web.
Reportería	Evaluación de procesos en términos de calidad, uso de recursos, y resultados de los indicadores para su optimización.
Simulación	Análisis de los procesos de negocio a través del análisis de escenarios (what if).
Model-to-Execute	Transformación de los modelos de procesos de ARIS hacia la plataforma de webMethods Business Process Management Suite (BPMS).
Conexión con SAP®	Links directos para sistemas SAP, especialmente para SAP® Solution Manager, asegurando que los procesos definidos se reflejen en el entorno de sistemas asegurando un mejor implementación.
Pruebas de diseño	Gráficos de diseño para pruebas de caso basados en los procesos existentes.
Gobernanza	Administración de procesos en BPMS (webMethods).

Tabla No. 1 Características de ARIS PLATFORM
(Software AG, 2013)

Para el caso de la presente investigación, se utilizaron las características de documentación y análisis de procesos, para cumplir con los objetivos propuestos. Los resultados serán publicados dentro de la herramienta ARIS BUSINESS PUBLISHER.

Cabe mencionar que la herramienta ARIS PLATFORM, contiene una amplia variedad de modelos que deben ser instrumentados de acuerdo a las necesidades de cada organización, en virtud de lo cual, se parametrizó el filtro metodológico de ARIS para la utilización de los modelos necesarios en el desarrollo de esta investigación tal como se explica en el numeral 3.2.

3.2 DEFINICIÓN DE LOS MAPAS Y MODELOS A UTILIZAR

Dentro de la gama de modelos existente, se ha optado por utilizar aquellos que se describen a continuación:

Los modelos o mapas seleccionados, de acuerdo a las necesidades del Banco del Estado, y discutidas entre los miembros de la Dirección de Gestión de la Calidad para la documentación de sus procesos son los siguientes:

a. Modelo de Introducción (Modelo de estructuración)
b. Mapa de Procesos (Diagrama de Cadena de valor añadido)
c. Riesgos (Diagrama de Riesgos)
d. Flujogramas (CPE visualizado en columnas)
e. IDEF0 (CPE adaptado a IDEF0)

Fuente: (Software AG, 2013)

3.3 ICONOGRAFÍA DE PROCESOS, APLICATIVOS Y ORGANIZACIÓN

3.3.1 Modelo de estructuración

El diagrama de estructuración (Figura No. 16) se utiliza para describir a la organización y su composición. En la parte superior por lo general se detalla la estrategia organizacional de la empresa, normativa aplicable y riesgos, en la parte izquierda se detallan los productos por segmento de mercado, en la parte derecha se detallan los productos y servicios y en la parte inferior se detallan la estructura y los sistemas de información. La parte central es donde se definen los Procesos que interactúan con los demás elementos.

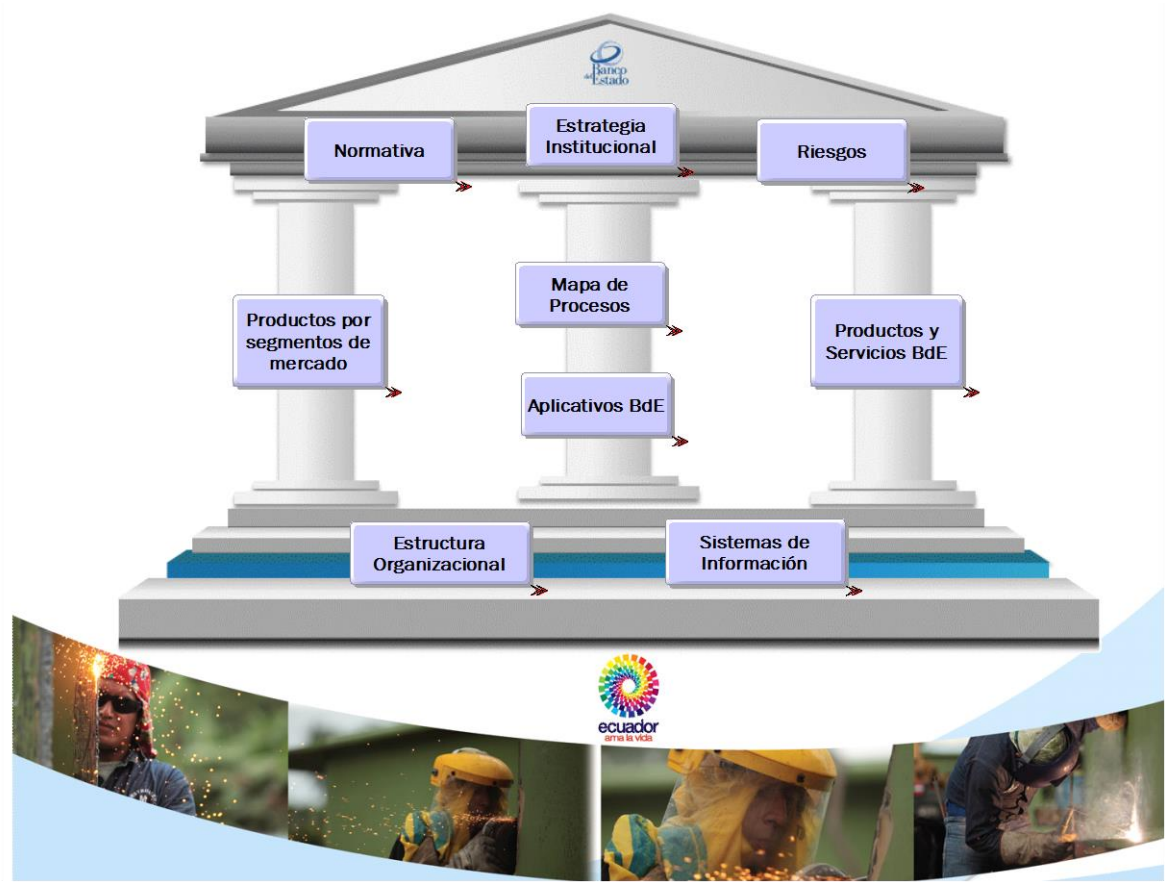


Figura No. 16 Modelo de estructuración
(Software AG, 2013)

3.3.2 Mapa de Procesos (Diagrama de cadena de valor añadido)

El Mapa de Procesos (Figura No. 17) es la representación gráfica de los procesos que ejecuta el Banco del Estado, reflejando su secuencia e interacciones, e identificando a la vez las entradas y resultados de los procesos y sus clientes.

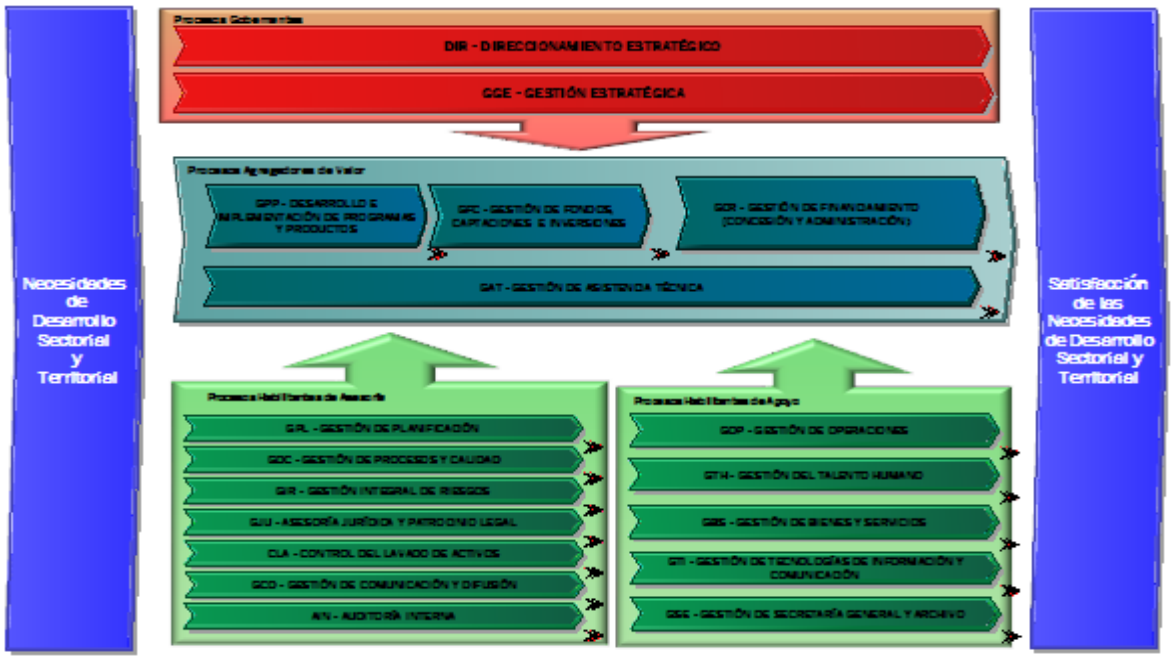


Figura No. 17 Mapa de Procesos del Banco del Estado
(Software AG, 2013)

3.3.3 Riesgos (Diagrama de Riesgos)

El modelo de riesgos se utiliza para clasificar los riesgos en jerarquías, según las Normas de Basilea II. Estos pueden asignarse a distintas categorías de riesgos y estas a su vez pueden depender las unas de las otras.

El modelo de riesgos según las normas de BASILEA II se establece como se muestra en la Figura No. 18:

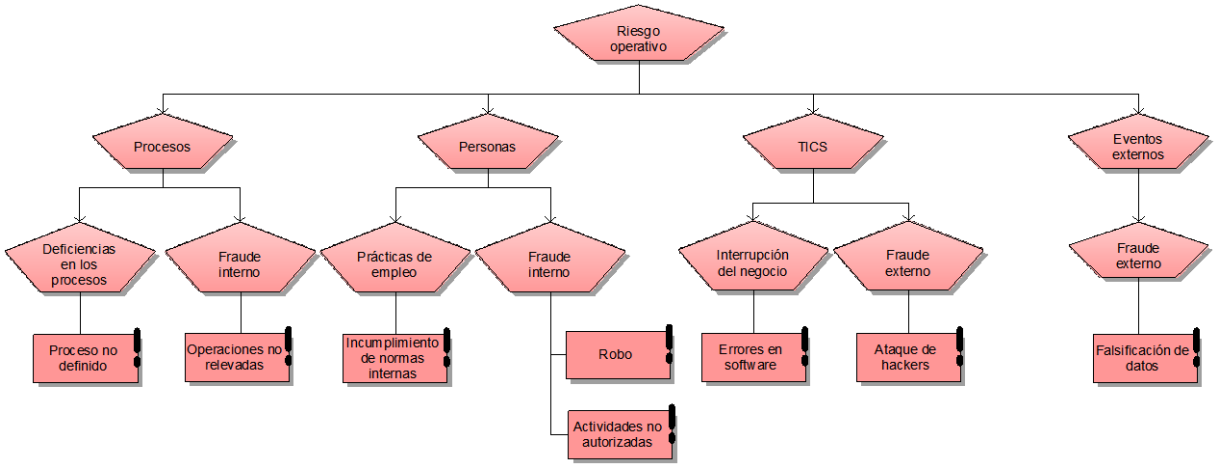


Figura No. 18 Modelo de riesgos según BASILEA II
(Bassel Comittee on Bankin Supervision, 2006)

3.3.4 Flujogramas (CPE visualizado en columnas)

Es la representación gráfica de los flujos de las actividades y eventos que componen los procesos. Las actividades son la unidad de menor nivel de acción en un proceso, por lo cual ya no se descompone en elementos más pequeños. El detalle de la utilización de estos modelos se los describió en el numeral 2.1.2 dentro de las definiciones del Marco Teórico.

3.3.5 IDEF0 (CPE adaptado a IDEF0)

Este mapa se utiliza para hacer un resumen general de los principales recursos asociados a la ejecución de cada proceso o actividad (Organizaciones, Informáticos y Datos), así como las entradas (insumos) y salidas (productos y servicios). También se pueden asociar métricas (KPI), políticas, controles, riesgos, entre otros. ARIS, al no contar con un modelo preestablecido para generar diagramas en notación IDEF0, se adaptó el modelo CPE de acuerdo a las condiciones para la identificación de entradas, salidas, controles y mecanismos.

La Figura No. 19 muestra la representación de este diagrama:

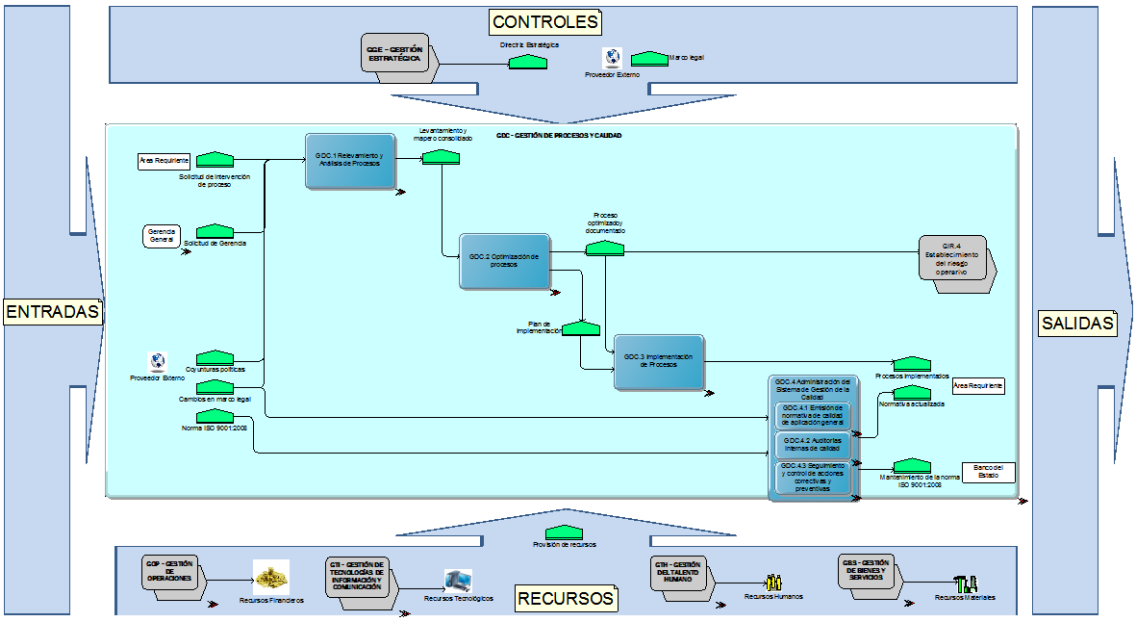


Figura No. 19 Diagrama IDEF0
(Software AG, 2013)

3.4 DEFINICIÓN DE REGLAS GENERALES PARA EL MODELAMIENTO DE PROCESOS EN CPE

3.4.1 Orientación del modelado de procesos

La orientación de los modelos CPE, que son los mapas de procesos y procedimientos debe ser de arriba hacia abajo (Top-Down). Siempre los eventos de entrada van por arriba del proceso o actividad y los eventos de salida van por debajo de estos.

Sólo los mapas de Cadena de Valor y los mapas de procesos (donde se emplea el modelo Diagrama de Cadena de Valor Añadido) la orientación es de izquierda a derecha, colocando los procesos estratégicos por encima de los procesos de negocio y los procesos soporte por debajo de los mismos.

3.4.2 Inicio de mapas de procesos y procedimientos

Los mapas de procesos y procedimientos comienzan siempre con uno o más eventos. Si estos provienen de otros procesos debe anteponerse la interfaz de proceso correspondiente con el nombre del proceso, como indica la Figura No. 20:

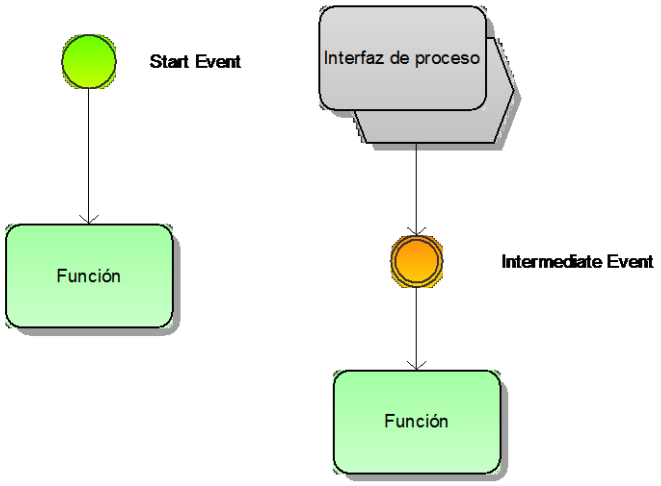


Figura No. 20 Inicio de procesos y procedimientos
(Software AG, 2013)

3.4.3 Fin de mapas de procesos y procedimientos

Del mismo modo, los mapas de procesos y procedimientos finalizan siempre con uno o más eventos. Si estos derivan en otros procesos debe colocarse a continuación la interfaz de proceso correspondiente con el nombre del proceso.

El evento final de un procedimiento será con un objeto de tipo Evento, con color Rojo, como indica la Figura No. 21:

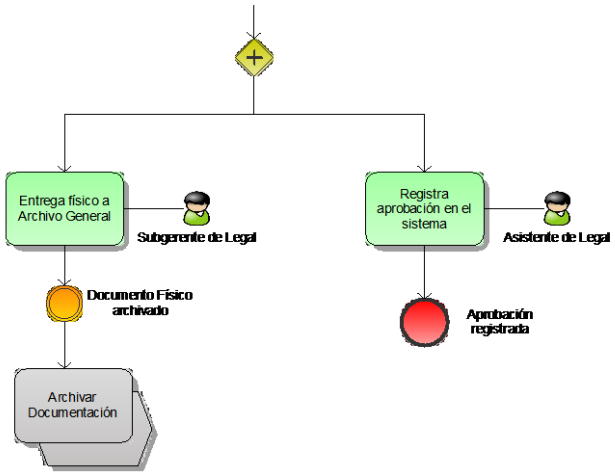


Figura No. 21 Finalización de procesos y procedimientos
(Software AG, 2013)

3.4.4 Uso de eventos

Los símbolos de eventos son utilizados para iniciar y finalizar un proceso o una actividad, o un conjunto de estas últimas. Los eventos iniciales y finales tienen sus propios símbolos, mientras que los eventos intermedios o para procesos de interface utilizan el símbolo de círculo con doble circunferencia.

El nombre del evento sigue la fórmula: Objeto + Verbo en Pasado Participio, por ejemplo: Factura Pagada.

En las conexiones entre procesos o tareas generalmente debe interponerse un evento. Se debe recordar que un proceso tiene al menos un evento que lo origina y debe generar al menos un evento como producto final. Por otro lado, en el caso de un procedimiento si es posible que existan una sucesión de actividades hasta finalizar con un evento, como muestra la Figura No. 22:

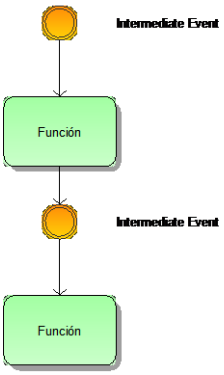


Figura No. 22 Uso de los eventos
(Software AG, 2013)

3.4.5 Uso de conectores lógicos

Cuando se desea conectar dos o más eventos con un proceso o una actividad, siempre se debe utilizar un conector lógico según la relación que se quiera representar, como muestra la Figura No. 23:

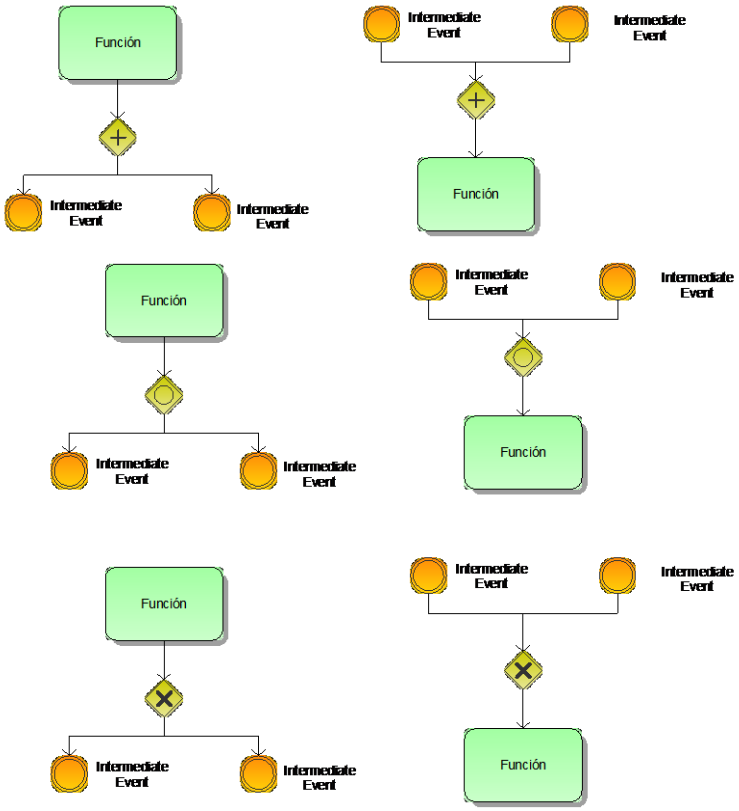


Figura No. 23 Uso de los conectores lógicos de eventos a actividades
(Software AG, 2013)

Del mismo modo, cuando se desea conectar dos o más procesos o actividades con un evento, éstos siempre deben llevar un conector lógico según la relación se quiera representar, como muestra la Figura No. 24.

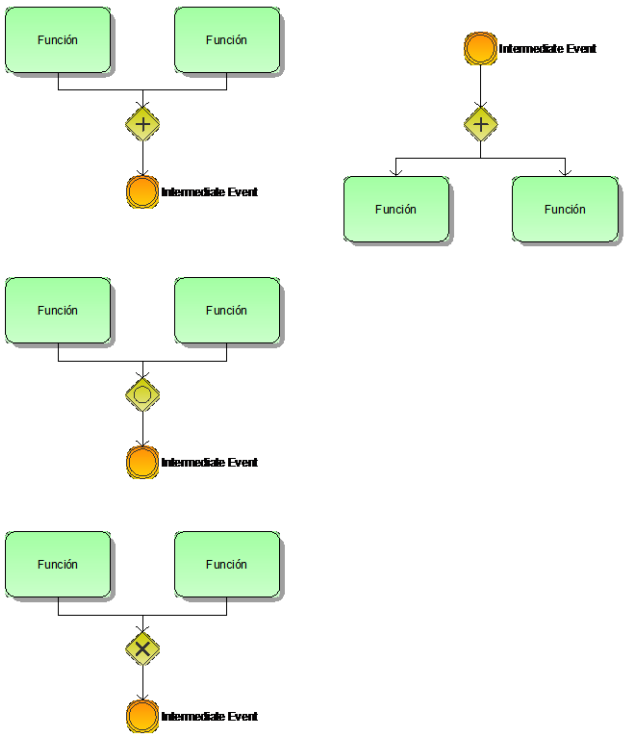


Figura No. 24 Uso de los conectores lógicos de actividades a eventos (Software AG, 2013)

Nunca se debe utilizar conectores lógicos para conectar eventos entre sí, ni actividades o procesos entre sí. El o los evento(s) origina(n) tareas o tarea(s), los que generan evento(s), siempre relacionados a través de los conectores lógicos cuando se presenta más de una rama u alternativa.

Nunca se debe utilizar el conector O ó XOR después de un evento, porque los eventos no deciden, son las personas que ejecutan las tareas las que son responsables de las mismas.

Si dos ramas o caminos se vuelven a cerrar en algún momento del proceso, generalmente deberá cerrarse utilizando el mismo conector con el cual se abrieron (la excepción sería la regla anterior).

3.4.6 Uso de actividades

Como convención las actividades se nombrarán utilizando verbos en infinitivo, por ejemplo: Recibir orden de compra de cliente.

No es correcto utilizar la letra “y” entre dos verbos en el nombre de una actividad. Si ello sucede es que estamos hablando de dos actividades separadas y deben representarse como tal.

Si de una actividad se desprenden dos actividades que se realizan en simultáneo, es necesario que se genere un evento intermedio y luego se utilice el conector lógico Y. Hay que recordar que por regla de uso de los conectores lógicos, estos nunca pueden utilizarse para conectar actividades entre sí.

3.4.7 Denominación de procesos

Para la denominación de procesos macro y procesos se sugiere que sean sustantivos, por ejemplo: “Concesión de Financiamiento”

3.4.8 Asociación de archivos externos a objetos en la herramienta de modelamiento

Para asociar archivos externos, se debe ir a los atributos del objeto e insertar los links en el los Atributos de Sistema. Allí deben ingresarse el link del documento y el título del ejecutable, como muestra la Figura No. 25.

Una vez ingresados el atributo de sistema, este puede ser visualizados en el costado superior derecho del objeto (utilizando la opción Formato/Representación).

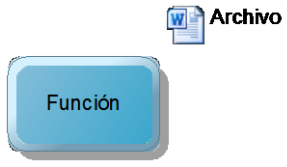


Figura No. 25 Asociación de objetos
(Software AG, 2013)

ARIS permite insertar hasta 4 links o archivos ejecutables como máximo por objeto o modelo.

3.4.9 Representación de la integración entre procesos

Para integrar los procesos se utiliza el símbolo de Interface de Procesos. Una forma de hacerlo es realizar una copia de ocurrencia del objeto o buscarlo en el modelo a través de la ventana de navegación y arrastrarlo hasta el área de modelado. Una vez insertado en el área de modelado, se deberá cambiar el símbolo al de interface de proceso utilizando la opción Formato / Representación / Apariencia del Objeto, como muestra la Figura No. 26:

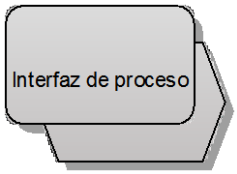


Figura No. 26 Símbolo de Interface de Procesos
(Software AG, 2013)

El símbolo de interface de proceso se utiliza para representar las relaciones entre procesos o procedimientos. La forma como se inicia y termina un proceso o procedimiento se encuentra al inicio de esta sección (Inicio y Fin de Mapas de Procesos y Procedimientos).

De este modo, el evento final que active el nuevo proceso a través del símbolo de interface, deberá ser utilizado como evento inicial en nuevo proceso mencionado, tal como se indica en la Figura No. 27:

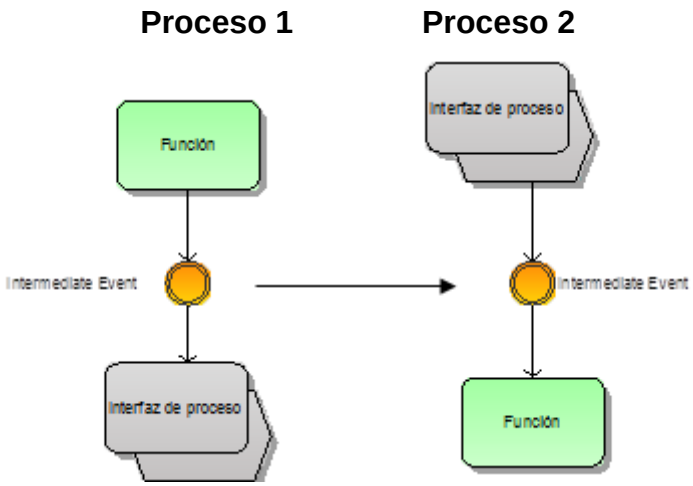


Figura No. 27 Reglas para el Interface de Procesos
(Software AG, 2013)

3.4.10 Uso de copia de ocurrencia y copia de definición

Se utiliza copia de ocurrencia, cuando lo que se quiere es reutilizar un objeto existente y que cualquier cambio que se haga al mismo, se quiere que quede reflejado en todos los mapas donde se esté utilizando ese objeto.

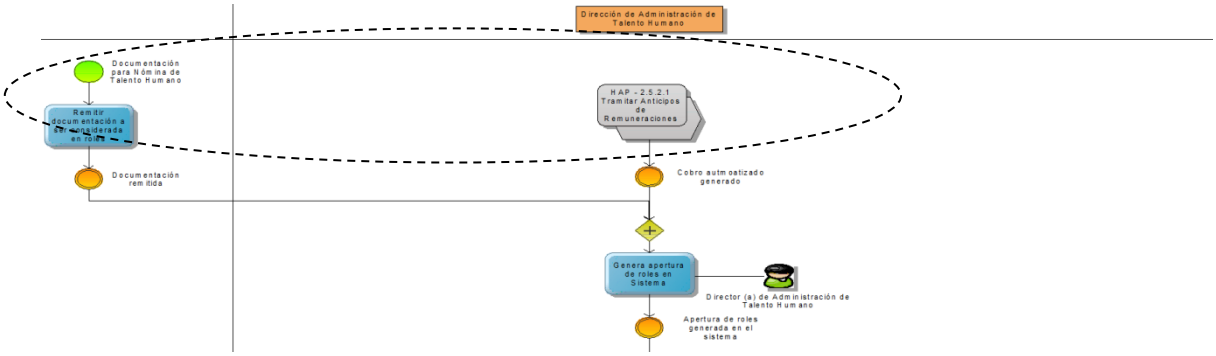
La copia de definición es cuando se quiere crear un nuevo objeto que contenga los mismos atributos que el original. En este caso es conveniente utilizar nombres de objetos diferentes para evitar confusiones.

Cuando se crean modelos que son variantes de otros, conviene que las actividades que son comunes tengan como referencia el mismo objeto. En este caso lo que debe entenderse es que se están modelando procesos y por lo tanto debe despojárselo de las cuestiones propias de implementación.

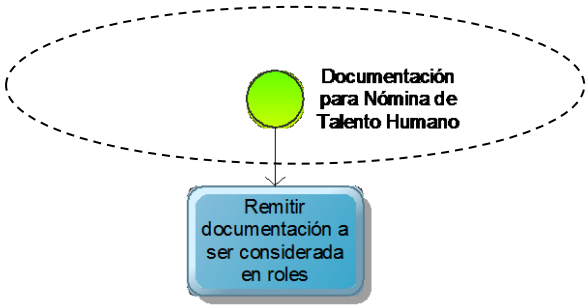
3.5 DEFINICIÓN DE NORMAS ESPECÍFICAS PARA EL MODELADO DE FLUJOGRAMAS EN CPE

Las normas específicas para el modelado de procesos, se enuncian a continuación:

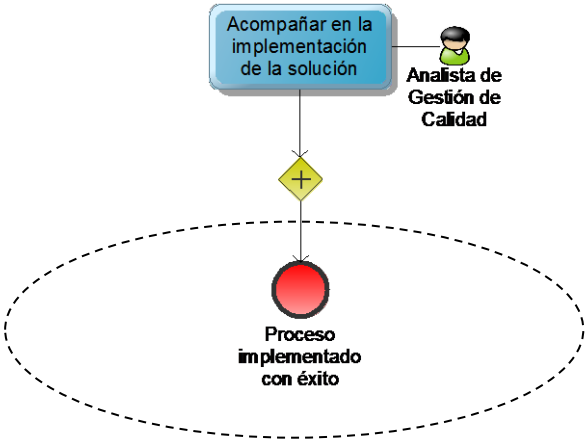
1. Se deberá identificar claramente el o los disparadores del proceso, ya sea desde una o varias actividades, o desde la interfaz de otro proceso, como se ilustra a continuación:



2. El evento de inicio, deberá contener claramente, la identificación del evento inicial, tal como se indica a continuación:

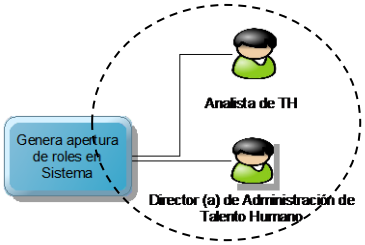


3. El evento de fin debe coincidir con el producto que se entrega en el proceso, el cual debe ser escrito a un costado de la gráfica, como se indica a continuación:



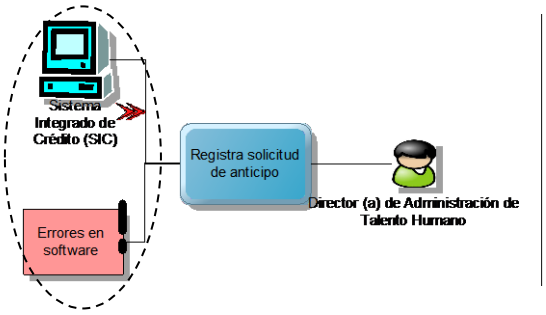
4. En cada actividad relacionada a la ejecución por parte de una unidad organizacional del Banco del Estado, se deberá colocar el cargo del ejecutor de dicha actividad, al lado derecho de la gráfica de las mismas, tal como se indica a continuación:

5. En el caso de existir varios cargos ejecutores de la actividad, se identificarán con igual número de gráficos para cada uno de ellos, tal como se indica a continuación:

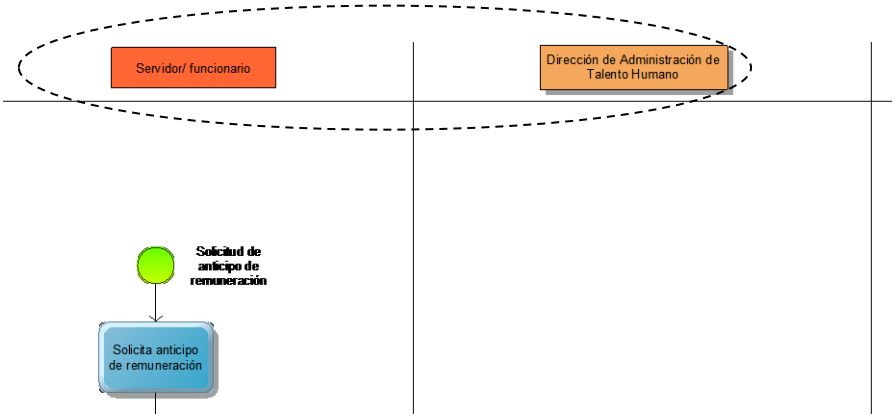


6. En cada actividad que requiera de operación dentro de un sistema transaccional del Banco del Estado, se deberá colocar el ícono del sistema empleado en de dicha actividad, al lado izquierdo de la gráfica de las mismas, tal como se indica a continuación:

7. En cada actividad que identifique un riesgo, se deberá colocar el ícono del mismo en dicha actividad, al lado izquierdo de la gráfica de las mismas, tal como se indica a continuación:



8. La identificación de los pools deberá contener, las unidades organizacionales internas, roles, o las entidades externas que intervienen el proceso, como se indica a continuación:



3.6 DISEÑO DE LAS HERRAMIENTAS DE LEVANTAMIENTO DE PROCESOS

Para el levantamiento de información en base al marco de referencia COBIT 5.0 se utilizó una ficha de levantamiento de procesos, la que consta de dos pestañas. La primera en donde se encuentra la caracterización básica del proceso, mientras que la segunda contiene el detalle del proceso a nivel de actividades, conjuntamente con el análisis de valor agregado. Esta última información se levanta aprovechando el trabajo de campo para el mejoramiento continuo. La Tabla No. 2 y Tabla No. 3 muestran las fichas a utilizar con su respectiva explicación.

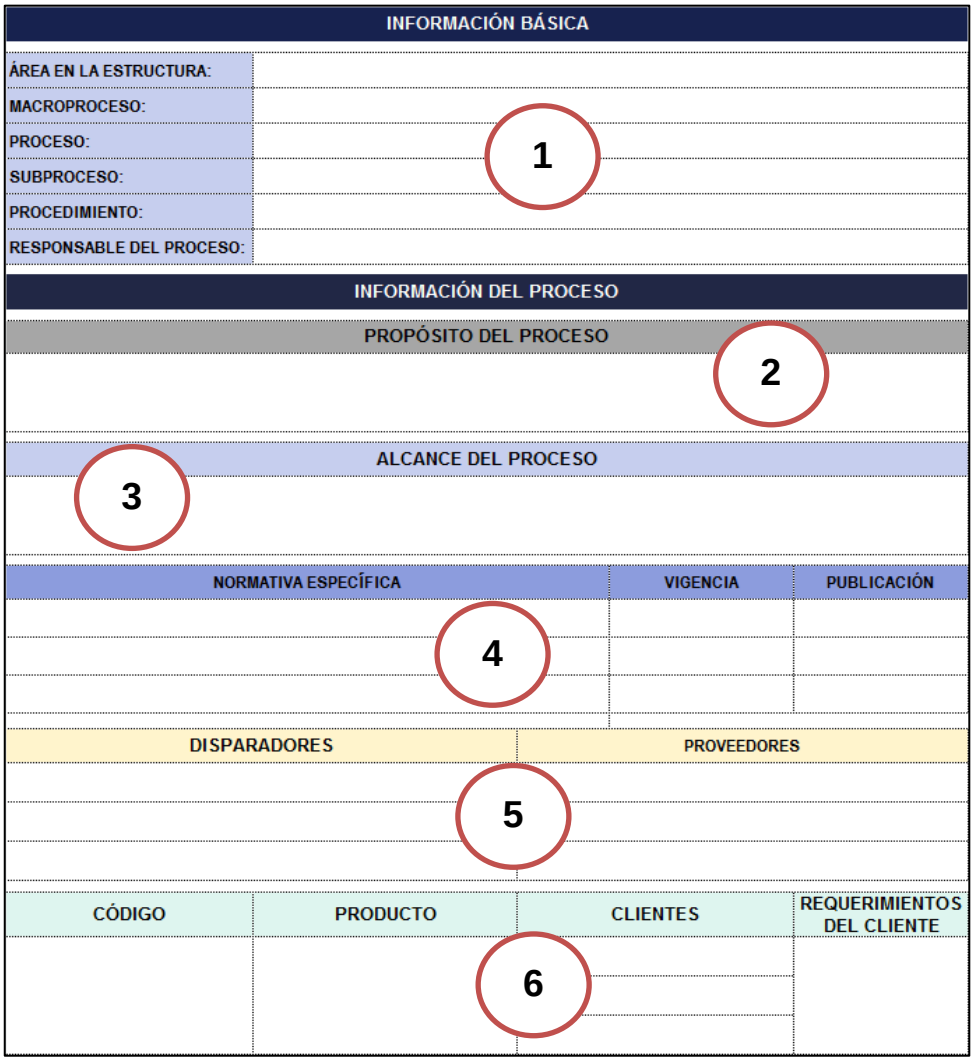


Tabla No. 2 Formulario de caracterización del proceso
(Secretaría Nacional de la Administración Pública, 2013)

- *Área Nro. 1:* En esta área se puede encontrar la información de la jerarquización del proceso, así como el responsable de su ejecución[3].
- *Área Nro. 2:* Esta área está destinada para colocar el objetivo del proceso cumpliendo las características de la metodología "SMART"[4].
- *Área Nro. 3:* En esta área se coloca el alcance del proceso, es decir su inicio y su fin, además de su aplicabilidad dentro de matriz y sucursales.

[3] Según la herramienta RACI Chart, este responsable es el equivalente al Accountable, es decir el que cumple con el rol de aprobación.
[4] S = Específico, M = Medible, A = Asignables, R = Realistas, T = Tiempo determinado

- *Área Nro. 4:* Esta área sirve para identificar los controles normativos, en la que se debe identificar la vigencia (fecha en que la normativa es aplicable) y publicación (fecha en que la norma se publicó en Registro Oficial).
- *Área Nro. 5:* Esta área sirve para caracterizar las entradas del proceso, en términos de insumos que requiere el mismo para convertirse en productos. Además se identifican qué procesos proveen de esos insumos.
- *Área Nro. 6:* En esta área se identifican los productos que generan los procesos, entendiéndose como tales a las salidas finales que sirven de insumos para otros procesos.

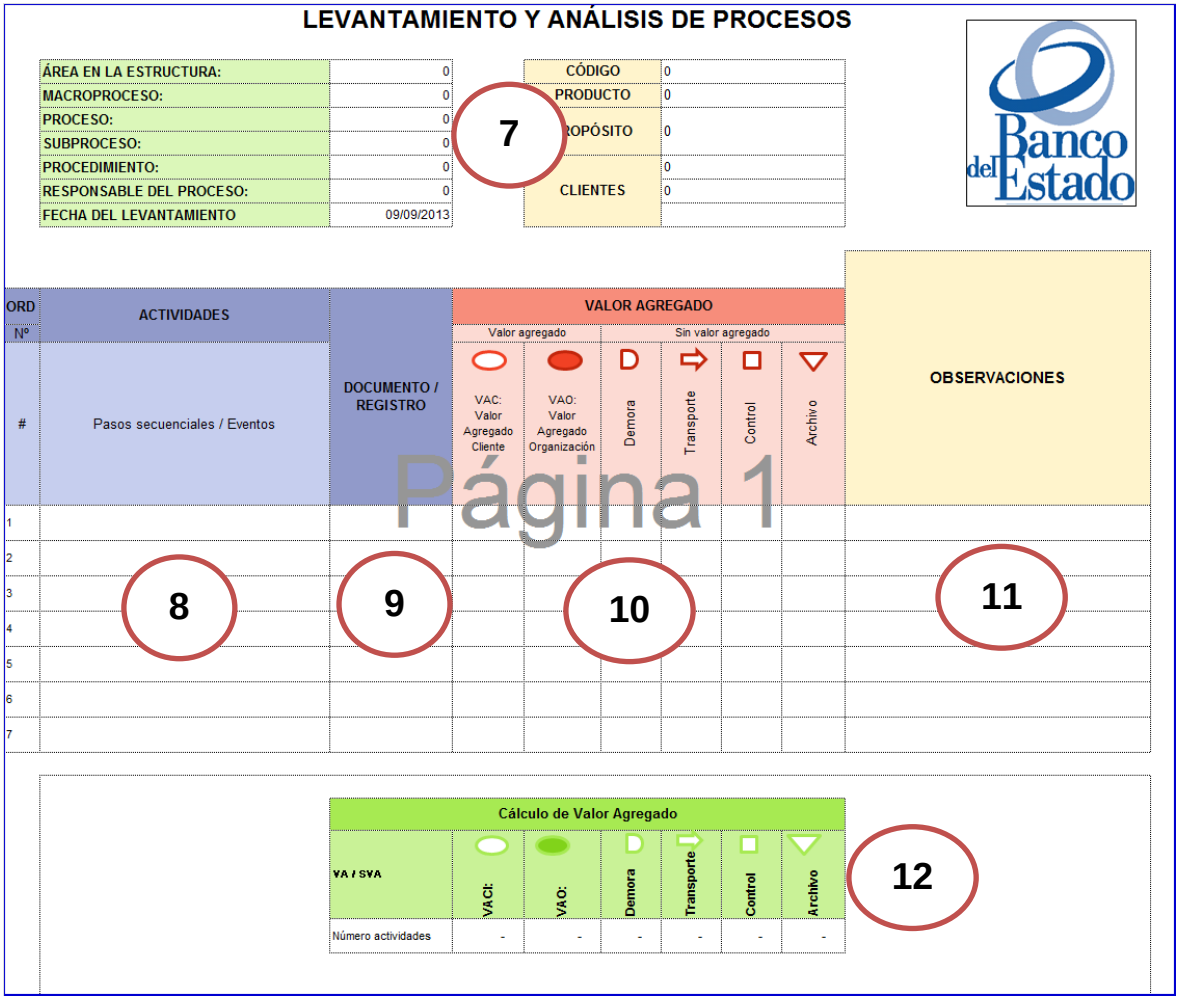


Tabla No. 3 Formulario para levantamiento del proceso
(Secretaría Nacional de la Administración Pública, 2013)

- *Área Nro. 7:* Ésta área es la transcripción de la información anteriormente descrita, para identificar el encabezado de la ficha de levantamiento del proceso.
- *Área Nro. 8:* En esta área se colocan las actividades en forma secuencial como base para la flujodiagramación del proceso.
- *Área Nro. 9:* Ésta área está destinada para la identificación de documentos o registros, con lo cual también se puede analizar situaciones potenciales de riesgo.
- *Área Nro. 10:* En esta área se realiza un análisis de valor agregado, aprovechando el levantamiento como base para el mejoramiento continuo.
- *Área Nro. 11:* Ésta área está destinada para colocar cualquier aclaración respecto a la actividad identificada, lo que facilita la flujo diagramación.
- *Área Nro. 11:* En esta área se presenta el resumen en número de actividades del análisis del valor agregado.

Esta herramienta de levantamiento se aplicará en un primer taller con el objetivo de documentar el proceso para su posterior validación.

3.7 DISEÑO DE LAS HERRAMIENTAS DE LEVANTAMIENTO DE RIESGOS

Para el levantamiento de riesgos, se utilizó un formulario que alimenta una base de datos. Este esquema ayudará a realizar la medición cualitativa y cuantitativa de los riesgos identificados en futuros estudios. A continuación se presenta el modelo de formulario que se utilizó en el levantamiento de riesgos.

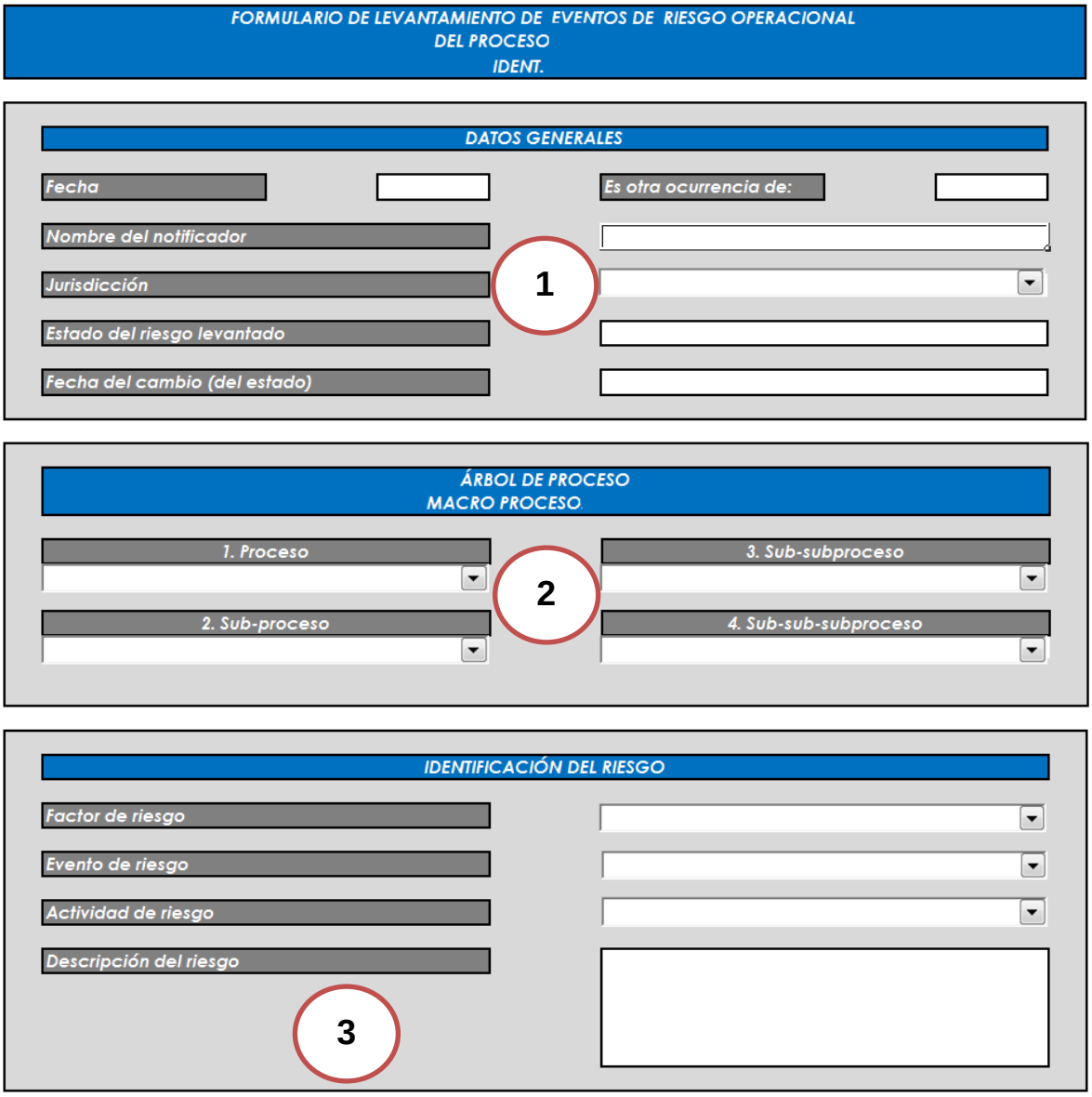


Tabla No. 4 Formulario para el levantamiento de riesgos
(Dirección de Riesgo Operativo del Banco del Estado, 2013)

- *Área Nro. 1:* Esta área está destinada para la identificación de la información general del riesgo levantado, con la finalidad de proporcionar información dentro de la fase de medición.
- *Área Nro. 2:* En esta área se puede encontrar la información de la jerarquización del proceso, con el fin de encontrar su procedencia y dominio de COBIT 5.0 al que pertenece la situación de riesgo.

- *Área Nro. 3:* En esta área se colocan los riesgos identificados desde el factor y evento (según Basilea II) hasta llegar a la actividad específica y su descripción.

Esta herramienta se aplicó luego de tener depurado el levantamiento del proceso, en cuyo caso, las actividades y caracterización de los mismos se ingresaron como campos validados en el formulario de levantamiento de riesgos.

4 RESULTADOS Y DISCUSIONES

4.1 IDENTIFICACIÓN DEL MAPA DE PROCESOS

El mapa de procesos del Banco del Estado, se clasifica en tres categorías según la Norma Técnica de Administración por Procesos, Registro Oficial Nº 895, miércoles 20 de febrero de 2013, como se muestra en las Figuras No. 28, 29 y 30

- Procesos gobernantes.

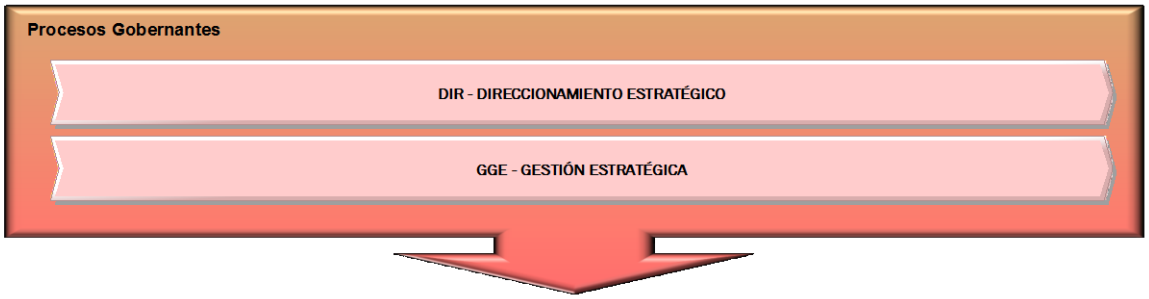


Figura No. 28 Procesos Gobernantes

- Procesos sustantivos o generadores de valor

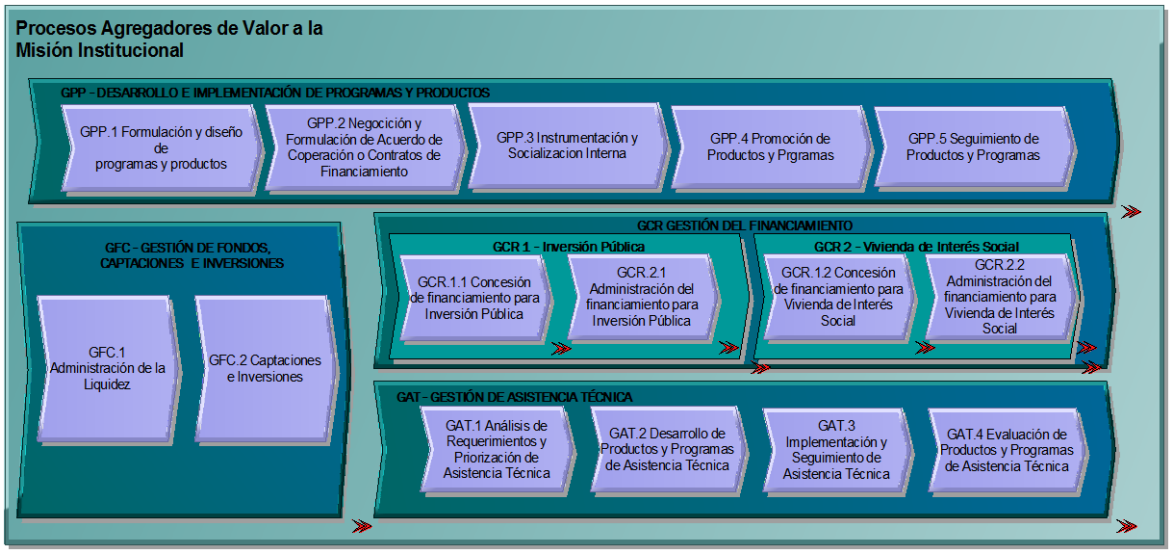


Figura No. 29 Procesos Sustantivos

- Procesos adjetivos, que su vez se dividen en habilitantes de apoyo y habilitante de asesoría

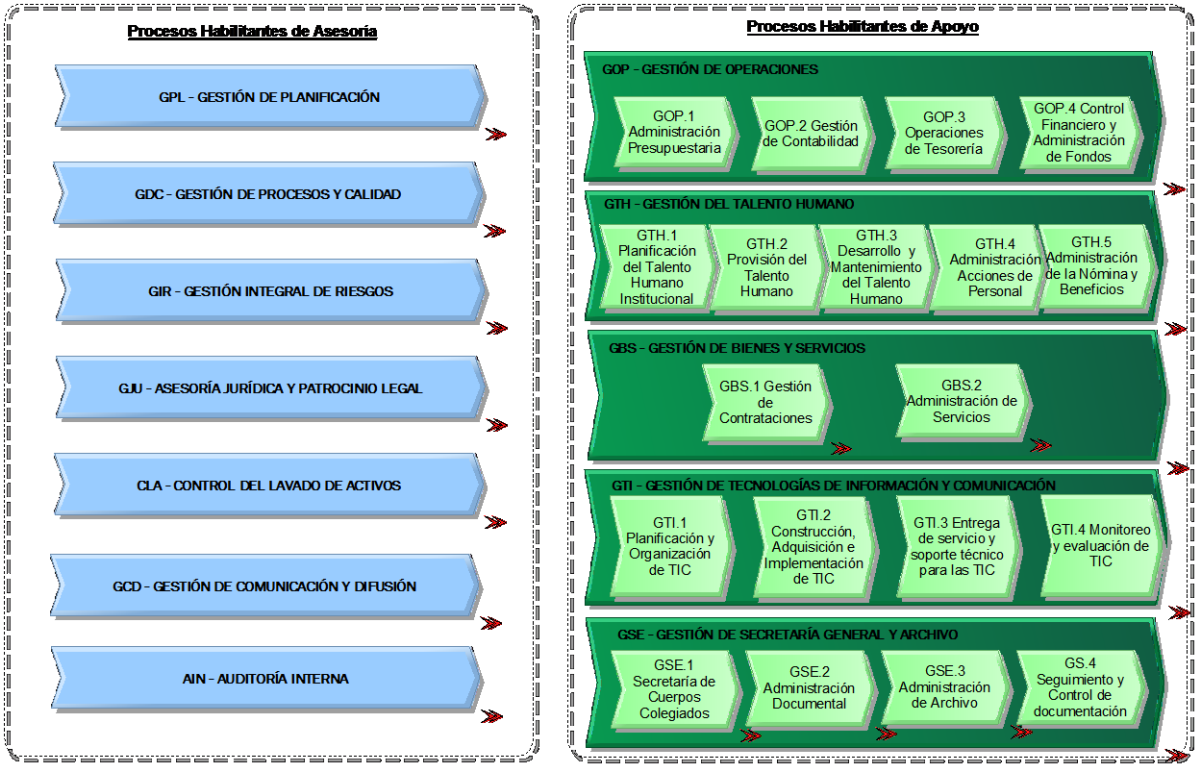


Figura No. 30 Procesos Adjetivos

Para un mejor entendimiento de los procesos del Banco del Estado, cada uno de ellos tiene asociado un objetivo el que está alineado a los objetivos estratégicos institucionales, para lo cual, se presenta la Tabla No. 5 para un mejor entendimiento de la labor que cumple cada proceso dentro del sistema de gestión por procesos de la institución.

Cabe mencionar que la estructura de procesos que se presenta en la Tabla No. 5 está vigente según Resolución de Directorio 2013-DIR-053, publicada en la Edición Especial No. 56-A, Registro Oficial de martes 8 de octubre de 2013.

PROCESO	OBJETIVO
DIR – Direccionamiento Estratégico	Ejercer la administración superior del Banco del Estado, generando las disposiciones y directrices para su adecuado funcionamiento.
GGE – Gestión Estratégica	Planificar, dirigir y evaluar las actividades del negocio y la administración interna del Banco, contribuyendo al cumplimiento de los objetivos institucionales.
GPP – Desarrollo e Implementación de Programas y Productos	Desarrollar productos y programas de financiamiento que articulen los requerimientos sectoriales y territoriales con los lineamientos de políticas, estrategias públicas e instrumentos de planificación.
GFC – Gestión de Fondos, Captaciones e Inversiones	Desarrollar y ejecutar estrategias, productos e instrumentos de negocios financieros que aseguren disponibilidad de recursos para las operaciones del Banco del Estado, invirtiendo los excedentes en procura de generar rendimientos en el marco de la normativa vigente.
GCR – Gestión del Financiamiento	Promover, desarrollar e implementar productos y proyectos de inversión pública y de negocios inmobiliarios acordes con las políticas públicas, en el marco del Plan Nacional de Desarrollo, asegurando niveles aceptables de riesgo.
GPL – Gestión de Planificación	Articular, controlar y evaluar la Planificación Estratégica, de Inversiones y Operativa, así como la Gestión de la Calidad del Banco del Estado, en concordancia con las políticas públicas nacionales, sectoriales y territoriales, con el objeto de orientar el financiamiento y otros servicios que ofrece la Institución hacia el cumplimiento de los objetivos determinados en el Plan Nacional de Desarrollo.
GDC – Gestión de Procesos y Calidad	Administrar el Sistema de Gestión de la Calidad promoviendo la eficiencia en los procesos, la alineación estratégica de las áreas, la mejora continua y una cultura organizacional basada en el servicio al cliente.
GIR – Gestión Integral de Riesgos	Administrar la gestión integral de riesgos a través de identificar, medir, controlar, mitigar, monitorear y reportar los riesgos asumidos por la Institución en sus operaciones, mediante el desarrollo de metodologías y la aplicación de políticas o directrices necesarias, con la finalidad de proteger el margen financiero y el valor económico del Banco del Estado.
GJU – Asesoría Jurídica y Patrocinio Legal	Asesorar en materia legal y jurídica orientando a la alta administración hacia la correcta toma de decisiones, emitiendo así también, los respectivos informes sobre la viabilidad legal de los actos que genera la Institución, además de patrocinar la defensa judicial y extrajudicial del Banco del Estado, en caso de litigios.
CLA – Control del Lavado de Activos	Cumplir y hacer cumplir los requerimientos de la Unidad de Análisis Financiero UAF; Superintendencia de Bancos y procedimientos y controles establecidos para prevenir el lavado de activos y financiamiento de delitos.

PROCESO	OBJETIVO
GCD – Gestión de Comunicación y Difusión	Difundir a través de los distintos medios y estrategias de comunicación, las actividades y compromisos que el Banco del Estado desarrolla y cumple, generando en la opinión pública un conocimiento claro, preciso y positivo de su misión, visión, objetivos y gestiones institucionales.
AIN – Auditoría Interna	Verificar el cumplimiento de normas, políticas, emanadas por las autoridades, principalmente en lo relacionado a normativa de control interno.
GOP – Gestión de Operaciones	Administrar los procesos operacionales que soportan el giro del negocio institucional, afianzando tiempos de respuesta óptimos y un eficiente uso de los recursos financieros del Banco del Estado.
GTH – Gestión del Talento Humano	Administrar los subsistemas y procesos de gestión de talento humano, fortaleciendo y potencializando las competencias del personal para un desempeño óptimo de sus funciones en armonía con un adecuado clima organizacional.
GBS – Gestión de Bienes y Servicios	Garantizar la provisión oportuna de los recursos materiales, equipos, bienes, obras y servicios, incluidos los de consultoría, necesarios para el cumplimiento de los objetivos institucionales.
GTI – Gestión de Tecnologías de Información y Comunicación	Asegurar la provisión oportuna de sistemas de información y servicios de telecomunicaciones necesarios para la consecución de los objetivos institucionales, garantizando su disponibilidad, integridad y confiabilidad.
GSE – Gestión de Secretaría general y Archivo	Administrar la documentación oficial del Banco del Estado y dar fe de la misma, brindando el soporte necesario a la gestión de los órganos de gobierno y de la administración superior, para el cumplimiento de sus funciones y objetivos dentro del ámbito de su competencia.

Tabla No. 5 Matriz de Procesos - Objetivos

4.2 DESPLIEGUE DEL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

El despliegue del proceso de Gestión de Tecnologías de Información y Comunicación, funciona con base al Marco de Referencia COBIT 5.0, desde la aprobación de la Reforma Integral al Estatuto de Gestión Organizacional por Procesos, cuya primera documentación, parte de la presente investigación para el respectivo levantamiento de riesgos. Con este producto, se podrá realizar las respectivas mediciones e implementación de controles para mejoramiento del alcance del actual Plan de Continuidad de Negocio (PCN), cuyo alcance es

únicamente para el proceso de Gestión del Financiamiento en ambiente de contingencia. El despliegue del proceso es el siguiente:

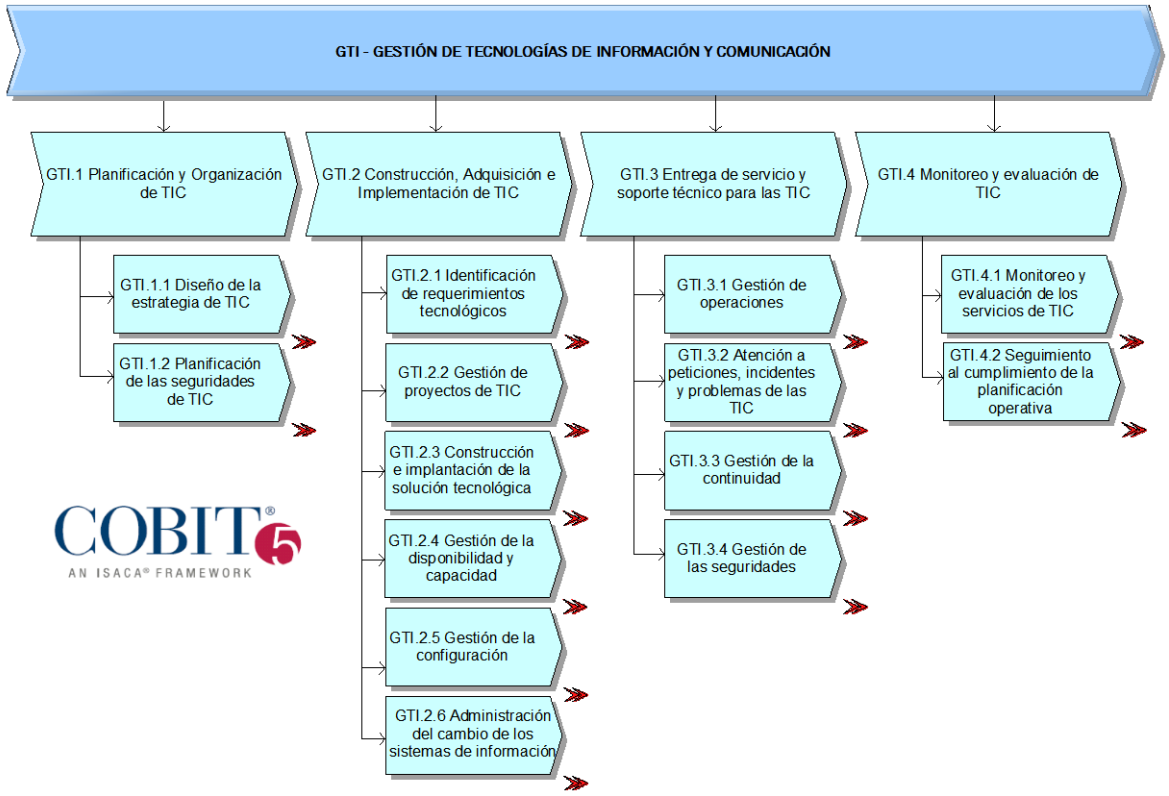


Figura No. 31 Despliegue del proceso de Gestión de Tecnologías de Información y Comunicaciones basado en COBIT 5.0

Al hacer un análisis comparativo, entre el marco de referencia y los procesos documentados, existen procesos que no se encuentran en la misma, debido a las siguientes razones:

- Fusión de procesos en uno solo.
- Aplicación del marco de referencia de acuerdo a la normativa legal vigente (Normas de Control Interno de Contraloría General del Estado y Estatuto Orgánico de Gestión Organizacional por Procesos)
- Aplicación del marco de referencia de acuerdo a la prioridad en relación al alineamiento de los procesos a los objetivos estratégicos del Banco del Estado.

4.3 CARACTERIZACIÓN DEL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La caracterización del proceso, tal como se explicó en el numeral 3.3.5, corresponde a un modelo desarrollado en base a los fundamentos de BPWIN, y adaptado desde un CPE hasta un IDEF 0. El nivel de caracterización utilizado es a nivel de proceso identificando los elementos críticos en entradas, salidas, controles y mecanismos para hacer lo más entendible posible el concepto de ICOM.

La caracterización tiene un nivel de detalle más profundo en las hojas de caracterización de proceso, las que se pueden apreciar en el Anexo D.

Cabe destacar que el Proceso de Gestión de Tecnologías de Información y Comunicación, tiene sus principales interfaces a nivel de entradas con los siguientes procesos:

- Gestión de Planificación: para el respectivo alineamiento estratégico hacia el nivel superior de la organización:
- Gestión de Procesos y Calidad: para la recepción de requerimientos de especificaciones funcionales en temas de automatización de procesos, ya sea dentro de BPMS, o a nivel transaccional.

Adicionalmente, este proceso, por medio de la caracterización, denota un alto nivel de servicio con el cliente interno principalmente en lo referente a lo relacionado con los productos de construcción, adquisición e implementación de soluciones tecnológicas y con la entrega de servicio y soporte técnico, aspectos incluidos dentro del marco de referencia COBIT 5.0. La Figura No. 32 presenta la caracterización del proceso en mención:

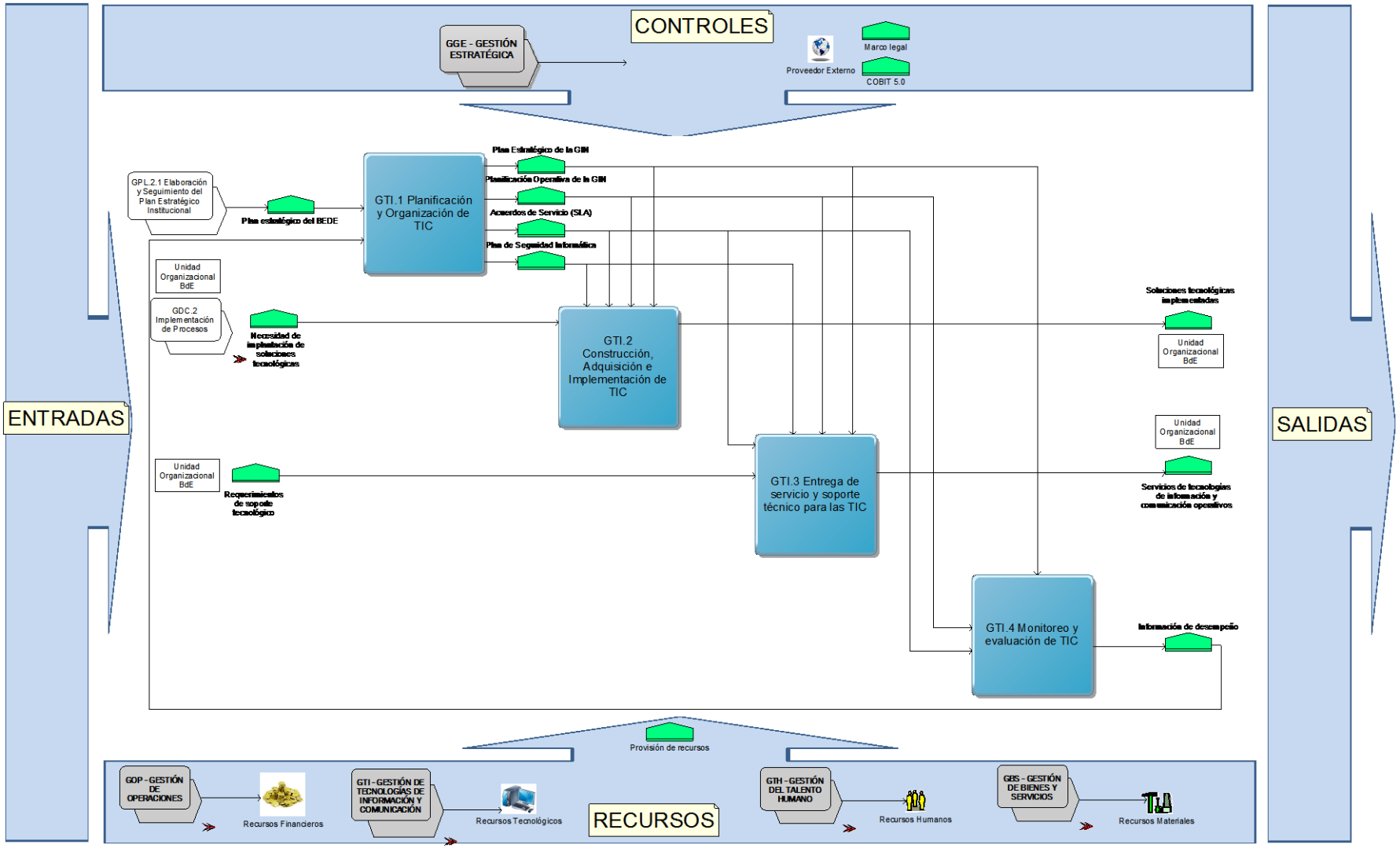


Figura No. 32 Caracterización del proceso de Gestión de Tecnologías de Información y Comunicaciones

4.4 MAPEO DE PROCESOS E IDENTIFICACIÓN DE RIESGOS

Para el mapeo de procesos, se aplicó la herramienta de levantamiento descrita en el numeral 3.6, y para el levantamiento de riesgos, se aplicó la herramienta descrita en el numeral 3.7

Con la información levantada se construyó un modelo mixto para identificar procesos y riesgos en un mismo diagrama, el cual, a través de matrices comparativas, permiten realizar análisis cruzados.

Cabe destacar que el levantamiento de procesos, es una situación AS-IS, es decir tal como está funcionando en la actualidad, mientras que los riesgos, son situaciones que ya han ocurrido en el pasado, o que podrían ocurrir en el futuro para su posterior medición e implementación de controles. Para la diferenciación de estas dos situaciones de riesgo, se identificará la probabilidad de ocurrencia, es decir, que si es alta, media o baja, lo que servirá de base para futuros estudios en la medición de riesgo. Finalmente la descripción de actividades del proceso se encuentra en el Anexo E.

4.4.1 Planificación y Organización de TI

Para comprender el resultado de la cadena de valor actual, en relación al marco de referencia COBIT 5.0, se presenta la Figura No. 33 asociando ambos elementos. Como parte de la estrategia de TI, están todos los elementos, con excepción de la Planificación de las seguridades, ya que por alineamiento estratégico, se está planificando la implementación de ISO/IEC 27001:2013.

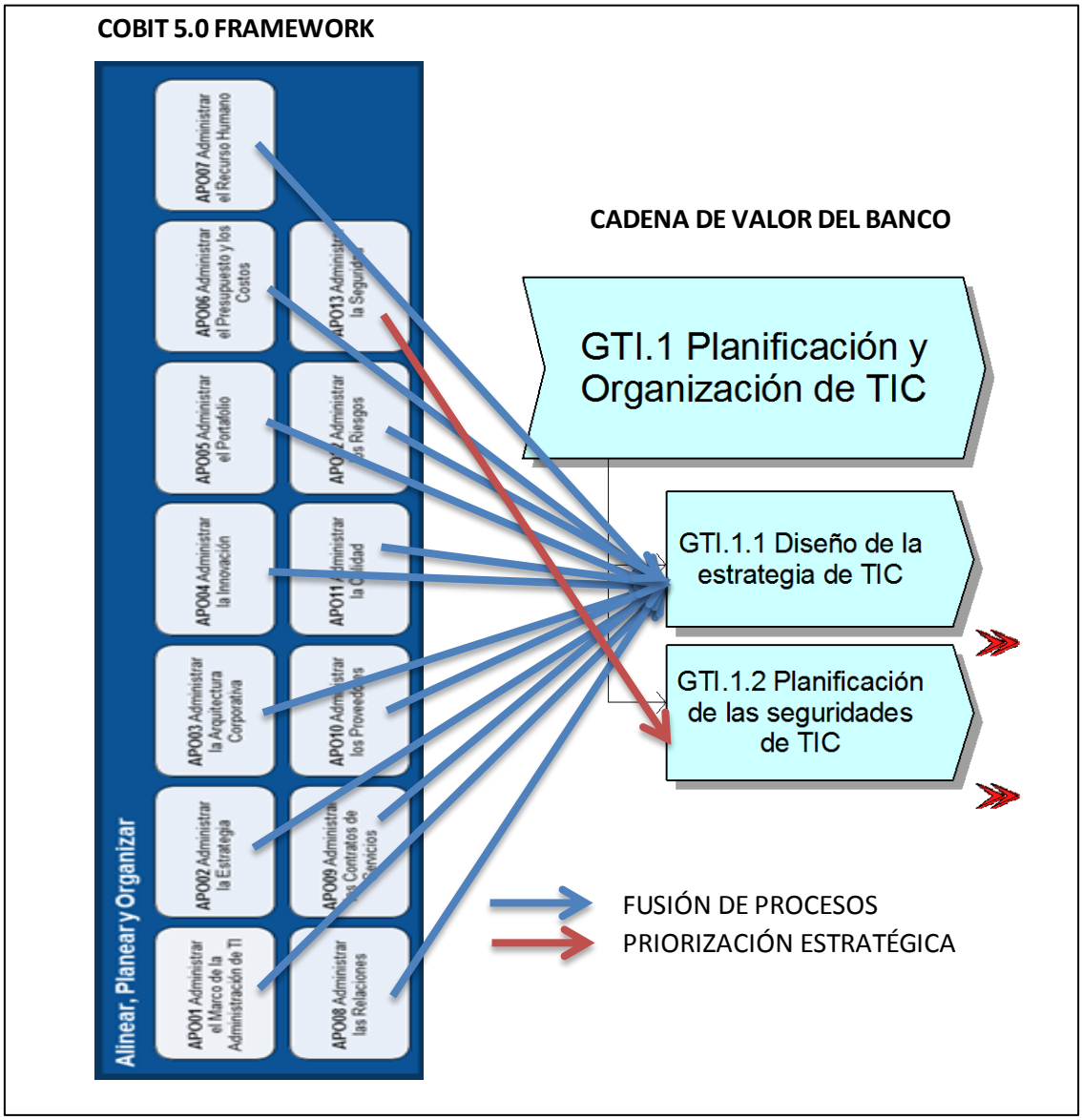
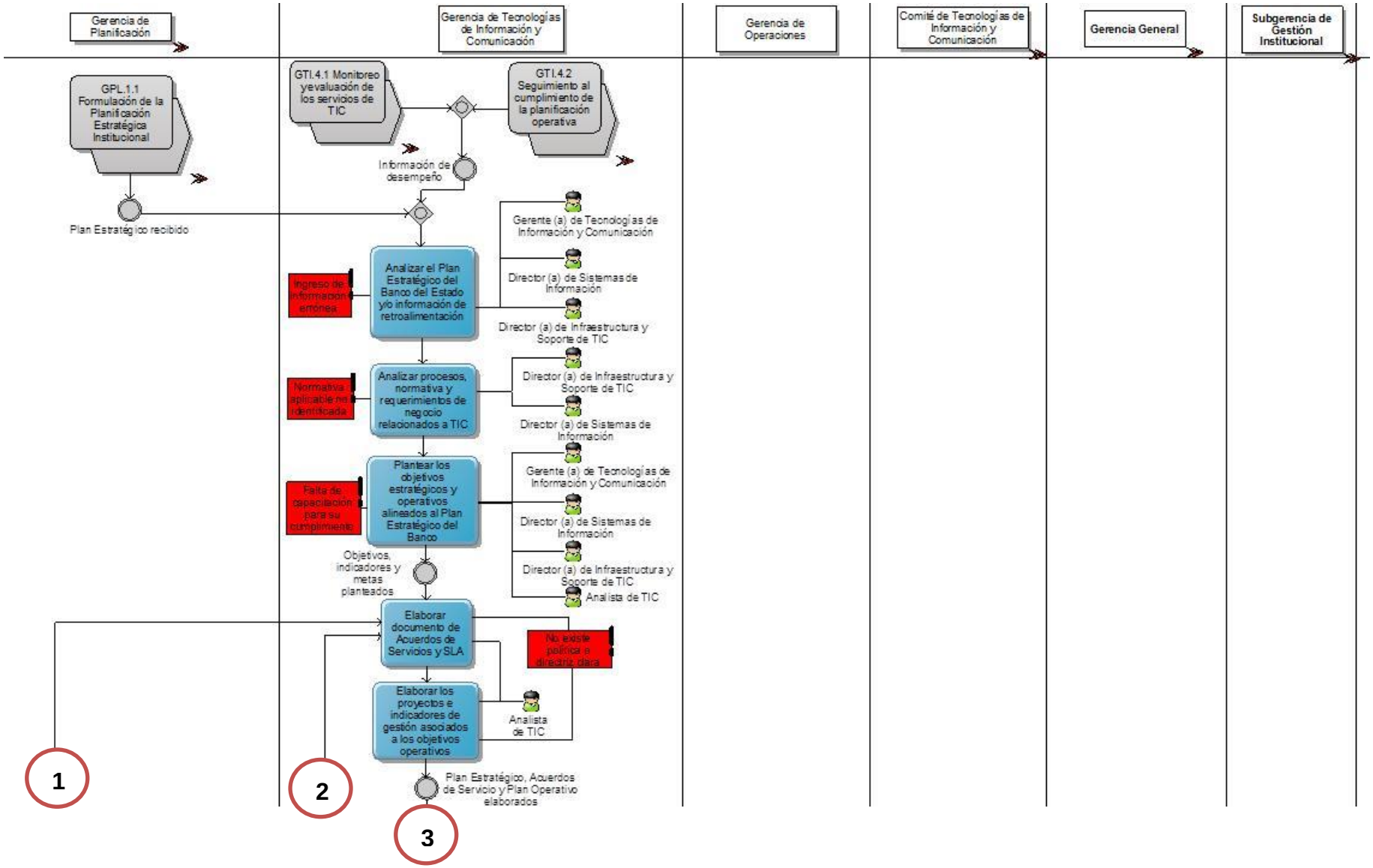
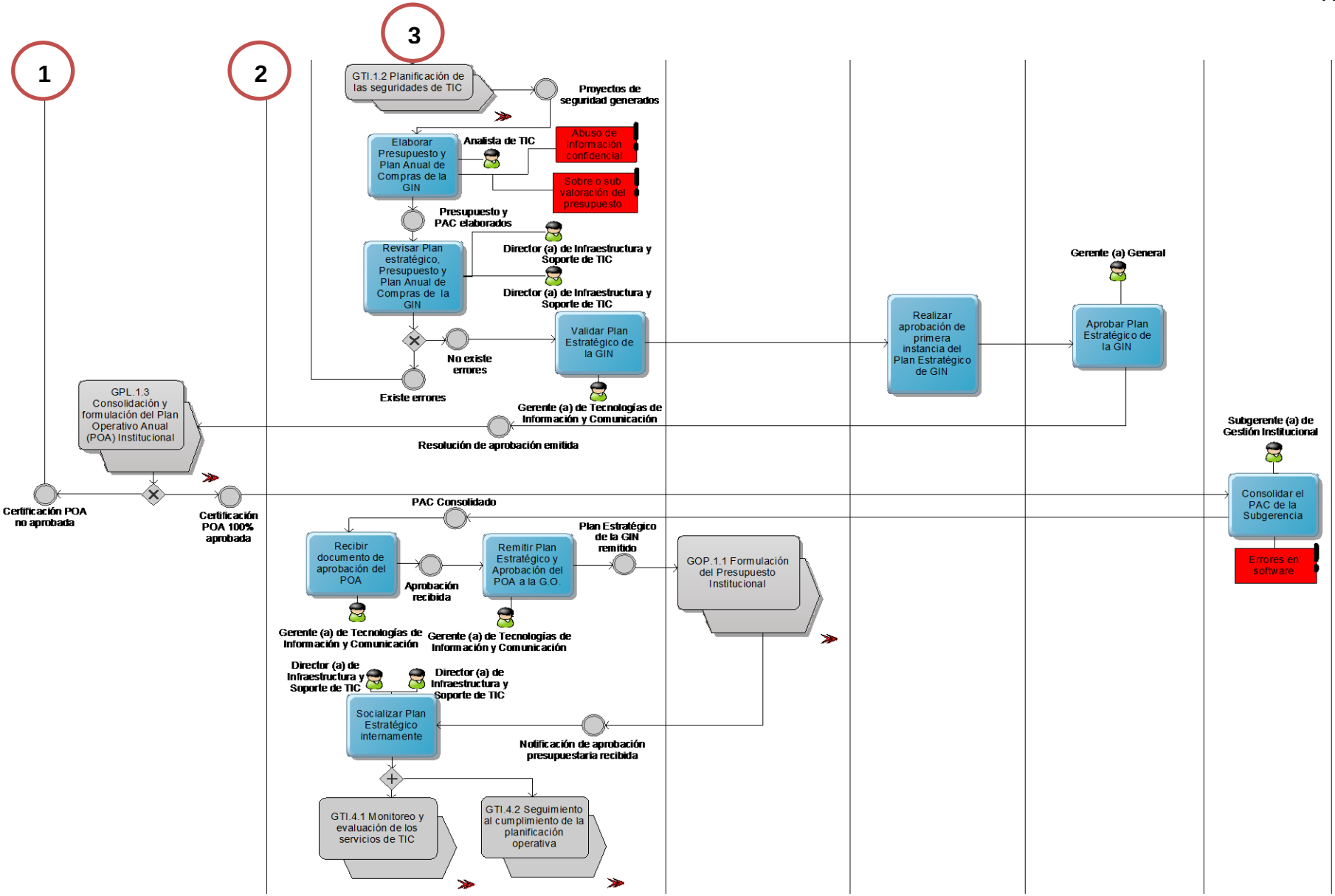


Figura No. 33 Relación COBIT 5.0 con el Dominio APO aplicado al BdE

4.4.1.1 *Diseño de la estrategia de TIC*

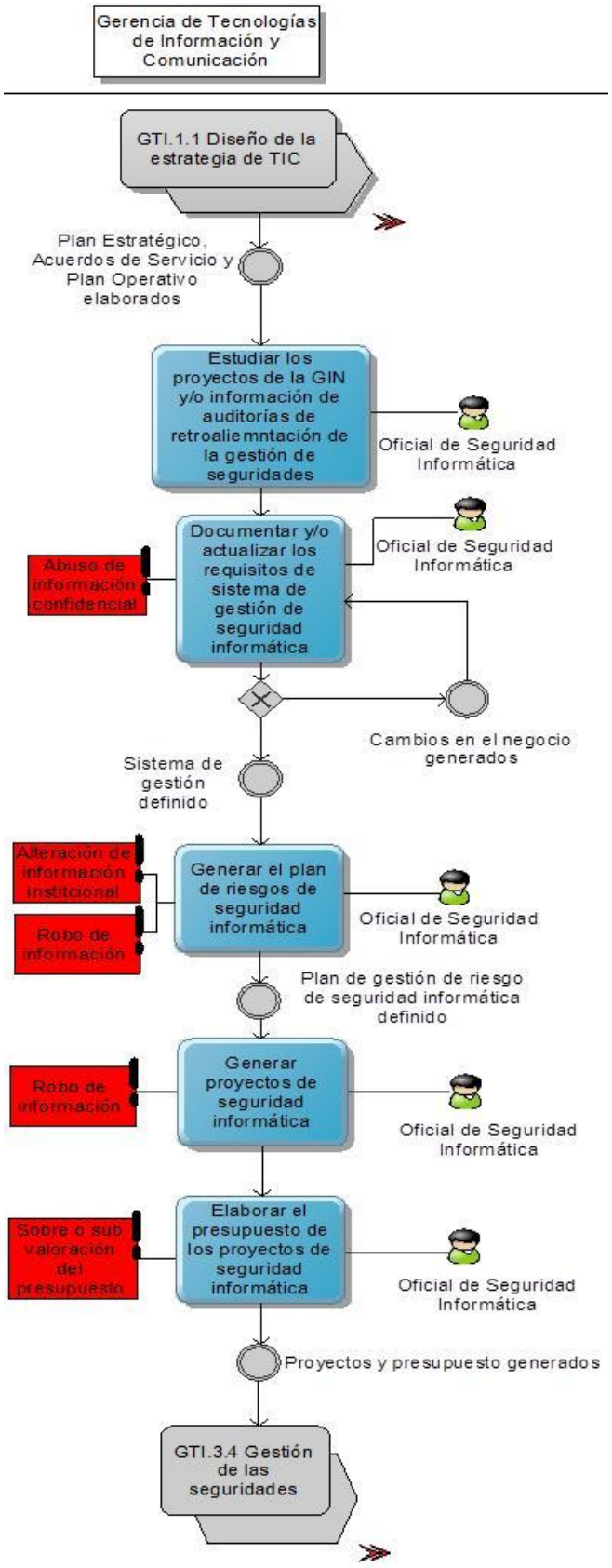



1
2
3
GTI.1.2 Planificación de las seguridades de TIC
Proyectos de seguridad generados
Elaborar Presupuesto y Plan Anual de Compras de la GIN
Analista de TIC
Abuso de información confidencial
Sobre o sub valoración del presupuesto
Presupuesto y PAC elaborados
Revisar Plan estratégico, Presupuesto y Plan Anual de Compras de la GIN
Director (a) de Infraestructura y Soporte de TIC
Director (a) de Infraestructura y Soporte de TIC
Validar Plan Estratégico de la GIN
No existe errores
Existe errores
Gerente (a) de Tecnologías de Información y Comunicación
Realizar aprobación de primera instancia del Plan Estratégico de GIN
Gerente (a) General
Aprobar Plan Estratégico de la GIN
GPL.1.3 Consolidación y formulación del Plan Operativo Anual (POA) Institucional
Resolución de aprobación emitida
Subgerente (a) de Gestión Institucional
Consolidar el PAC de la Subgerencia
Errores en software
Certificación POA no aprobada
Certificación POA 100% aprobada
PAC Consolidado
Recibir documento de aprobación del POA
Aprobación recibida
Remitir Plan Estratégico y Aprobación del POA a la G.O.
Plan Estratégico de la GIN remitido
GOP.1.1 Formulación del Presupuesto Institucional
Gerente (a) de Tecnologías de Información y Comunicación
Gerente (a) de Tecnologías de Información y Comunicación
Director (a) de Infraestructura y Soporte de TIC
Director (a) de Infraestructura y Soporte de TIC
Socializar Plan Estratégico internamente
Notificación de aprobación presupuestaria recibida
GTI.4.1 Monitoreo y evaluación de los servicios de TIC
GTI.4.2 Seguimiento al cumplimiento de la planificación operativa

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Analizar el Plan Estratégico del Banco del Estado y/o información de retroalimentación	Personas	Fraude interno (Personas)	Ingreso de información errónea	La información de los indicadores es cargada manualmente y arroja resultados erróneos	ALTA
Analizar procesos, normativa y requerimientos de negocio relacionados a TIC	Procesos	Deficiencias en los procesos	Normativa aplicable no identificada	La normativa respecto al EGSI no fue considerada	MEDIA
Plantear los objetivos estratégicos y operativos alineados al Plan Estratégico del Banco	Procesos	Deficiencias en los procesos	Falta de capacitación para su cumplimiento	Los objetivos de la Gerencia Informática no se alinearon a los Objetivos de alto nivel	BAJA
Elaborar documento de Acuerdos de Servicios y SLA	Procesos	Deficiencias en los procesos	No existe política o directriz clara	Los acuerdos de servicio no han tenido una directriz clara para su elaboración	MEDIA
Elaborar los proyectos e indicadores de gestión asociados a los objetivos operativos	Procesos	Deficiencias en los procesos	No existe política o directriz clara	Los indicadores de gestión o han tenido una directriz clara para su planteamiento y medición	MEDIA
Elaborar Presupuesto y Plan Anual de Compras de la GIN	Procesos	Deficiencias en los procesos	Sobre o sub valoración del presupuesto	El presupuesto planificado no alcanzó para la ejecución de todos los proyectos	BAJA
	Personas	Fraude interno (Personas)	Abuso de información confidencial	El presupuesto fue formulado para beneficiar a ciertos proveedores no calificados	ALTA
Consolidar el PAC de la Subgerencia	TICS	Interrupción del negocio	Errores de software	El sistema arroja errores en la consolidación del PAC	ALTA

Tabla No. 6 Identificación de riesgos por actividad (GTI.1.1)

4.4.1.2 *Planificación de las seguridades de TI*



ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Documentar y/o actualizar los requisitos de sistema de gestión de seguridad informática	Personas	Fraude interno (Personas)	Abuso de información confidencial	La actualización de la documentación se dio con intereses personales perjudicando a terceros	ALTA
Generar el plan de riesgos de seguridad informática	Personas	Fraude interno (Personas)	Alteración de información institucional	La información documentada no coincidía con los planificado e implementado	MEDIA
	Personas	Fraude interno (Personas)	Robo de información	La información establecida en el plan de riesgos fue robada y entregada a terceros	ALTA
Generar proyectos de seguridad informática	Personas	Fraude interno (Personas)	Robo de información	La información establecida en los proyectos de seguridad fue robada y entregada a terceros	MEDIA
Elaborar el presupuesto de los proyectos de seguridad informática	Procesos	Deficiencias en los procesos	Sobre o sub valoración del presupuesto	El presupuesto planificado no alcanzó para la ejecución de todos los proyectos	ALTA

Tabla No. 7 Identificación de riesgos por actividad (GTI.1.2)

4.4.2 Construcción, Adquisición e Implementación de TI

Para comprender el resultado de la cadena de valor actual, en relación al marco de referencia COBIT 5.0, se presenta la Figura No. 34 asociando ambos elementos. En este dominio, los procesos de construcción, adquisición e implementación de TI, en su mayoría tienen una relación uno a uno debido a la importancia que estos generan dentro del modelo de gestión. Adicionalmente, existe un proceso de gestión de activos que aparece dentro del modelo, el cual está normado dentro del marco legal referente a la administración de los activos en instituciones públicas, en las normas de control interno de Contraloría General del Estado, Ley Orgánica del Sistema Nacional de Contratación Pública y su

Reglamento y en el Reglamento Sustitutivo de Administración de Bienes en el Sector Público. Todos estos procesos pertenecen a la Dirección de Bienes y Servicios del Banco del Estado.

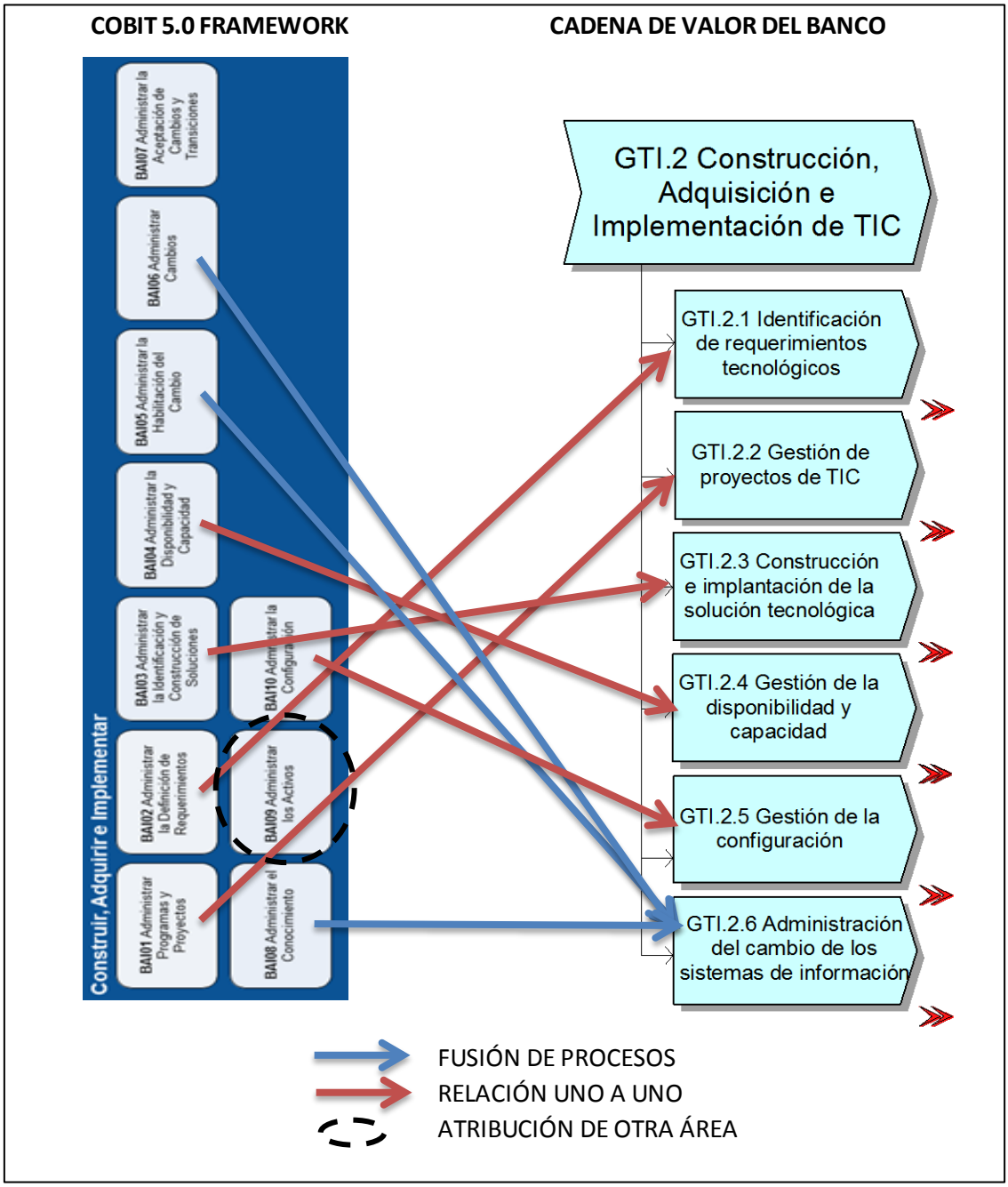
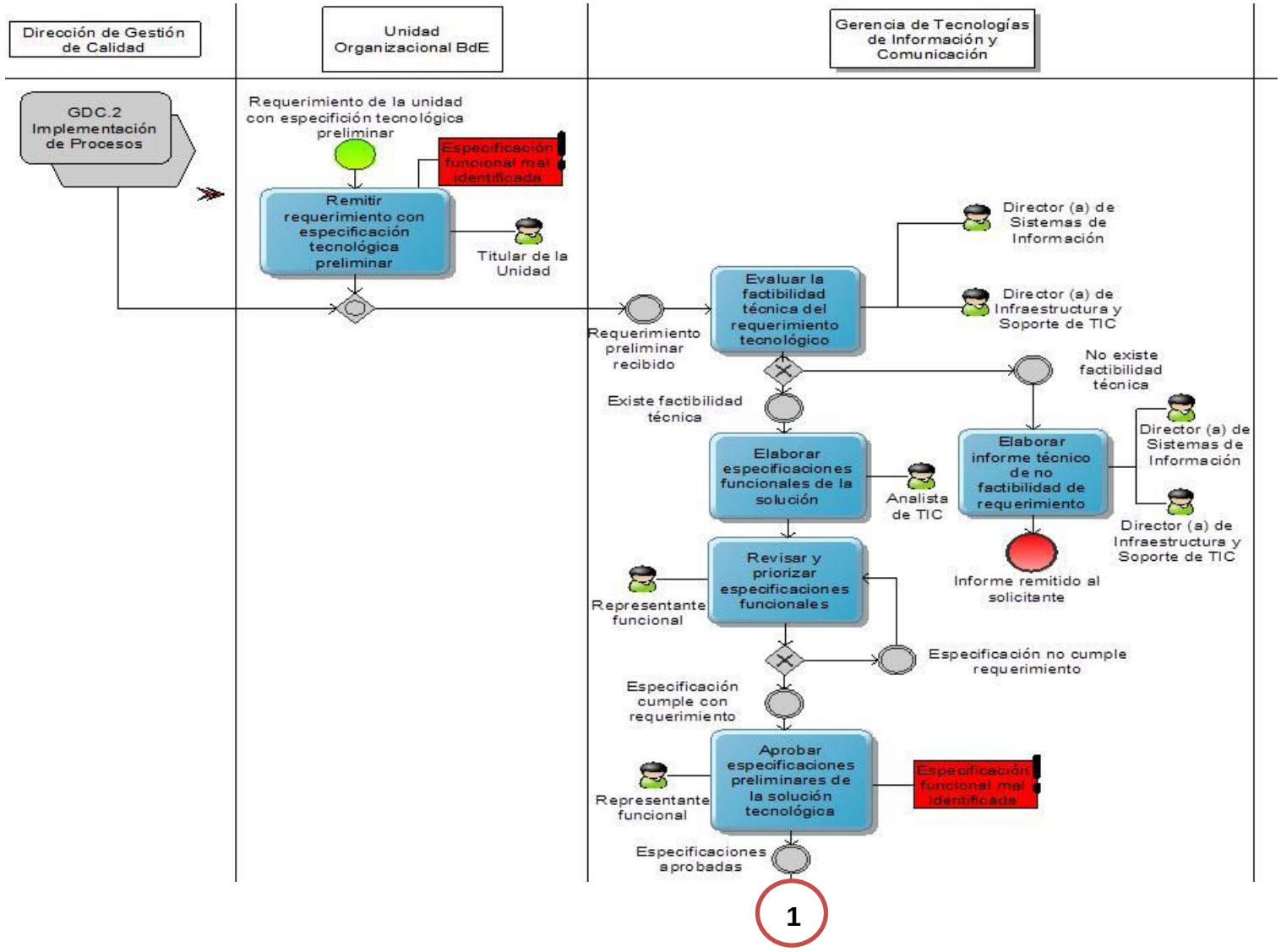
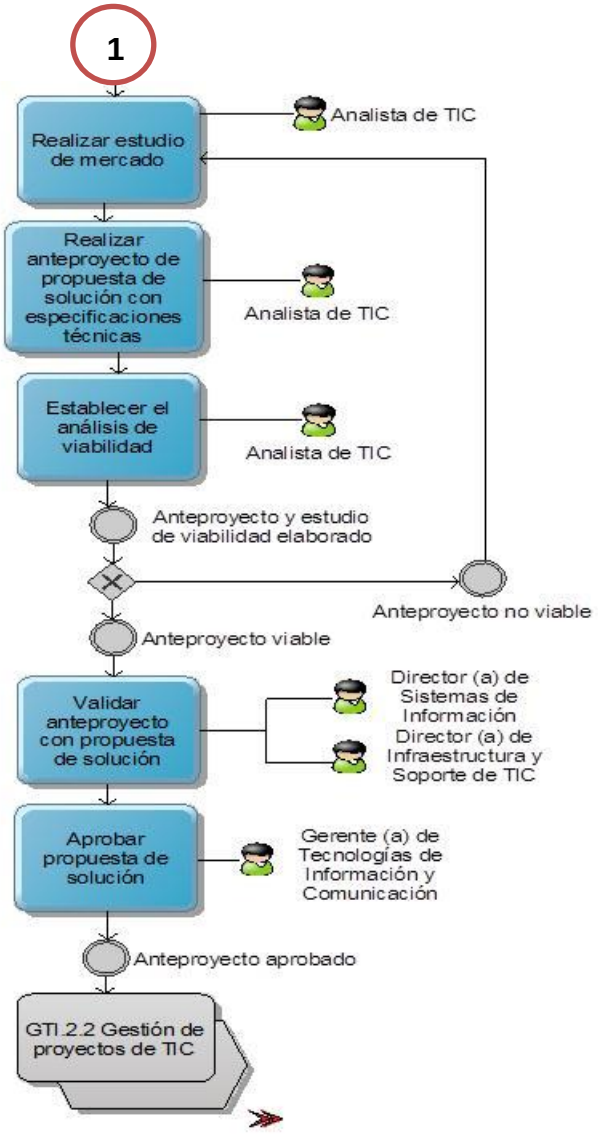


Figura No. 34 Relación COBIT 5.0 con el Dominio CAI aplicado al BdE

4.4.2.1 *Identificación de requerimientos tecnológicos*

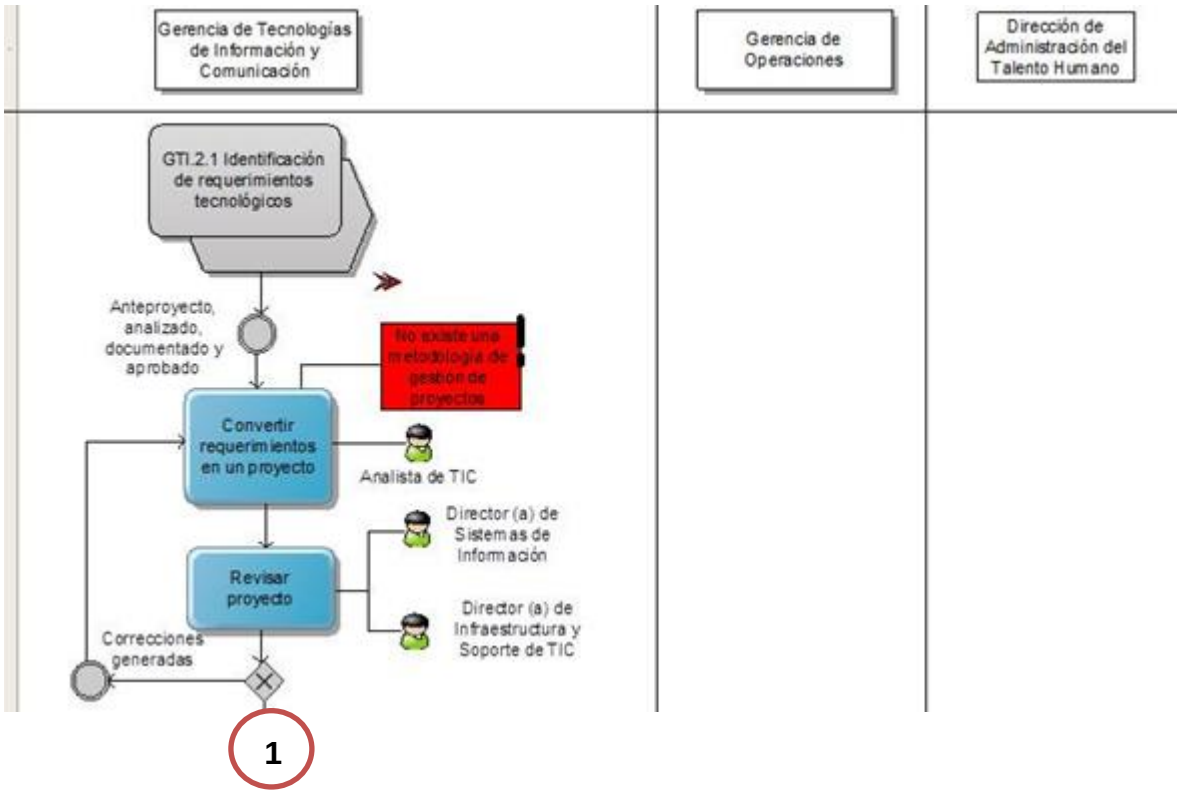


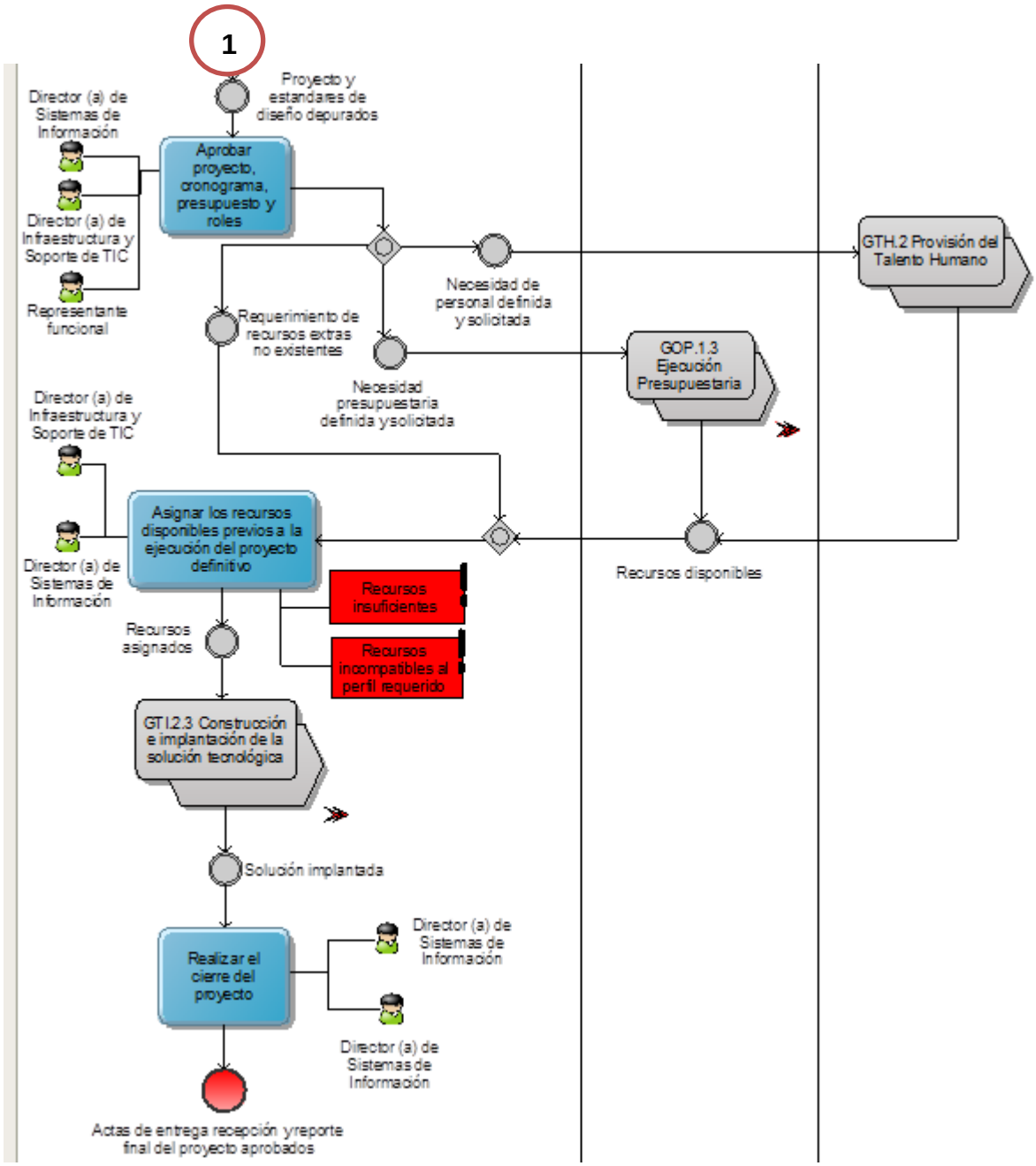

1
Realizar estudio de mercado
Analista de TIC
Realizar anteproyecto de propuesta de solución con especificaciones técnicas
Analista de TIC
Establecer el análisis de viabilidad
Analista de TIC
Anteproyecto y estudio de viabilidad elaborado
Anteproyecto no viable
Anteproyecto viable
Validar anteproyecto con propuesta de solución
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Aprobar propuesta de solución
Gerente (a) de Tecnologías de Información y Comunicación
Anteproyecto aprobado
GTI.2.2 Gestión de proyectos de TIC

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Remitir requerimiento con especificación tecnológica preliminar	Procesos	Deficiencias en los procesos	Especificación funcional mal identificada	No se toma en cuenta las especificaciones funcionales desde el enfoque del usuario	ALTA
Remitir requerimiento con especificación tecnológica preliminar	Procesos	Deficiencias en los procesos	Especificación funcional mal identificada	Al momento de la aprobación, no corresponde la especificación funcional real	BAJA

Tabla No. 8 Identificación de riesgos por actividad (GTI.2.1)

4.4.2.2 *Gestión de proyectos de TIC*



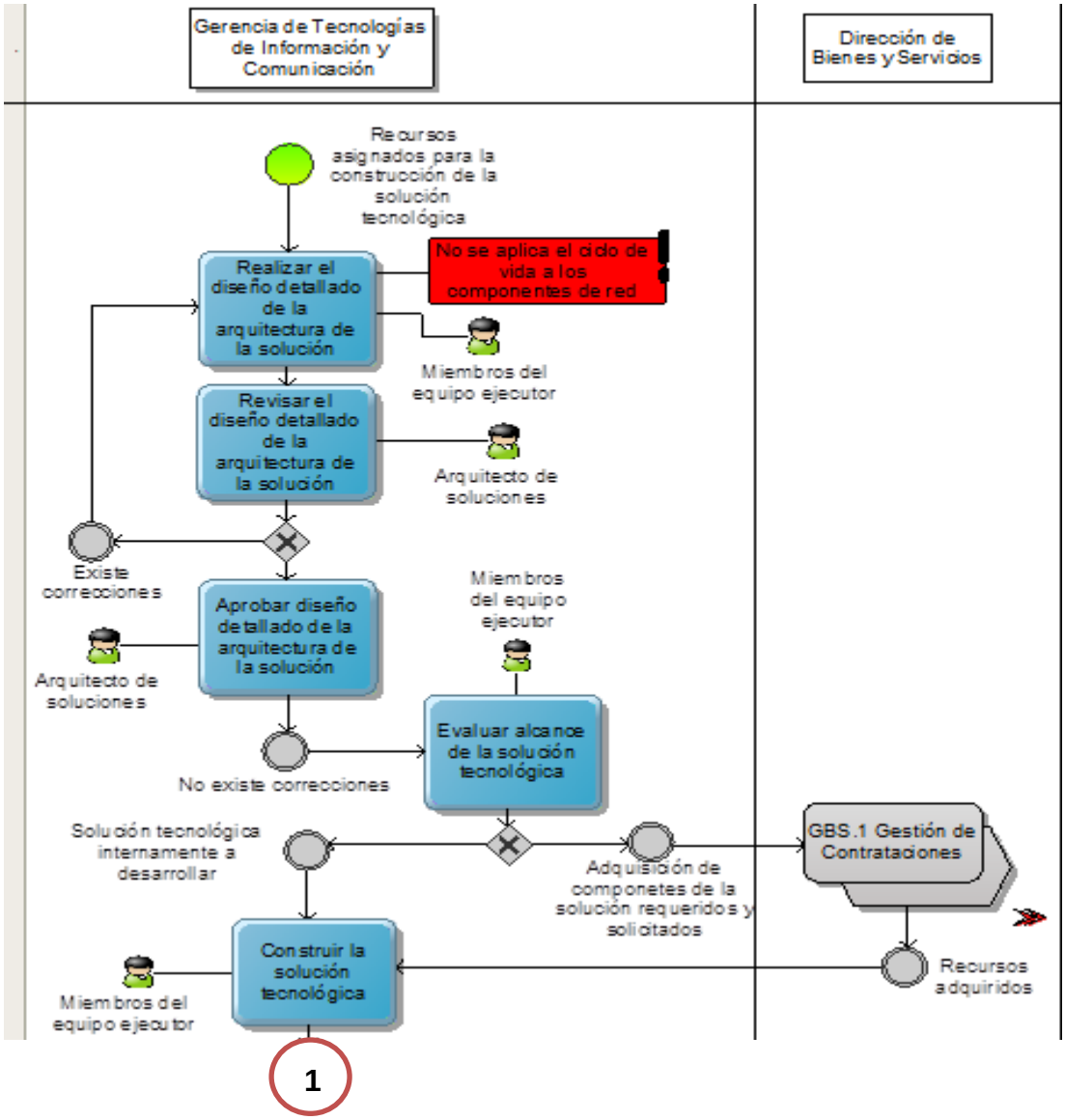


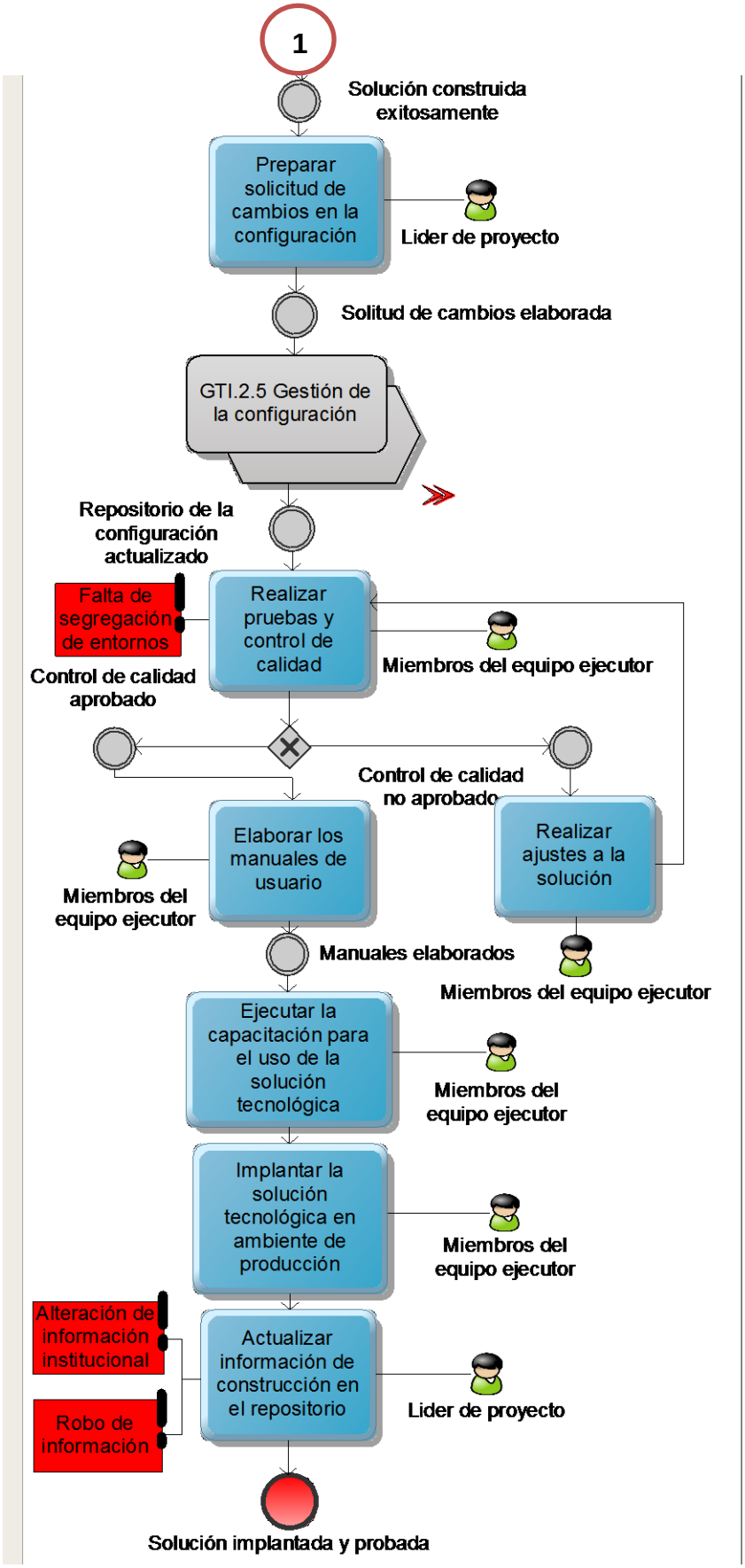
ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Convertir requerimientos en un proyecto	Procesos	Deficiencias en los procesos	No existe una metodología de gestión de proyectos	No se identifican todas las restricciones del proyecto en las áreas de conocimiento	ALTA

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Asignar los recursos disponibles previos a la ejecución del proyecto definitivo	Procesos	Deficiencias en los procesos	Recursos insuficientes	No se cuenta con el personal y los recursos para el éxito del proyecto	MEDIA
Asignar los recursos disponibles previos a la ejecución del proyecto definitivo	Personas	Fraude interno (Personas)	Recursos incompatibles al perfil requerido	Los perfiles no se ajustan a los requerimientos del proyecto	BAJA

Tabla No. 9 Identificación de riesgos por actividad (GTI.2.2)

4.4.2.3 *Construcción e implantación de la solución tecnológica*

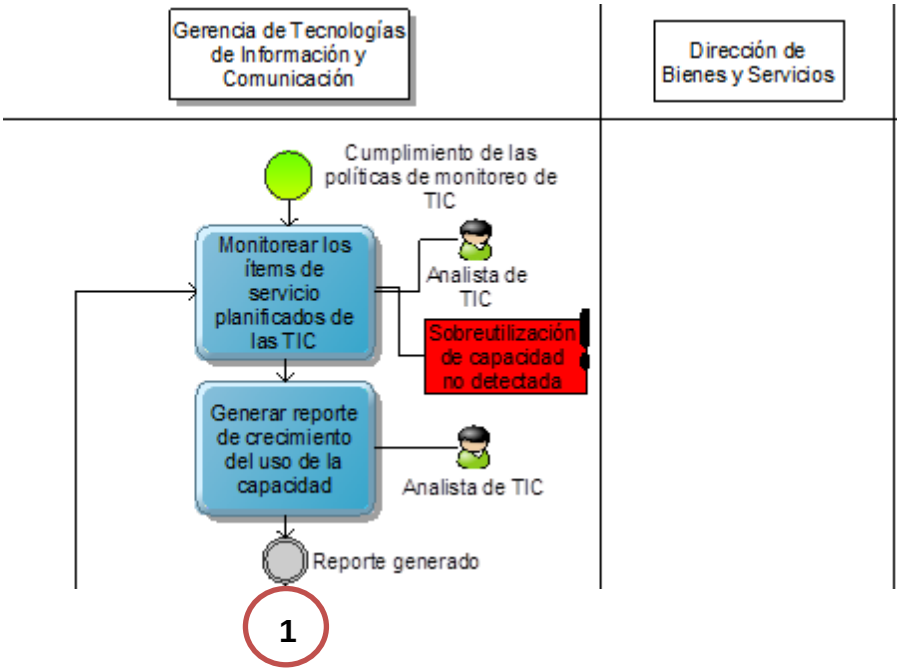


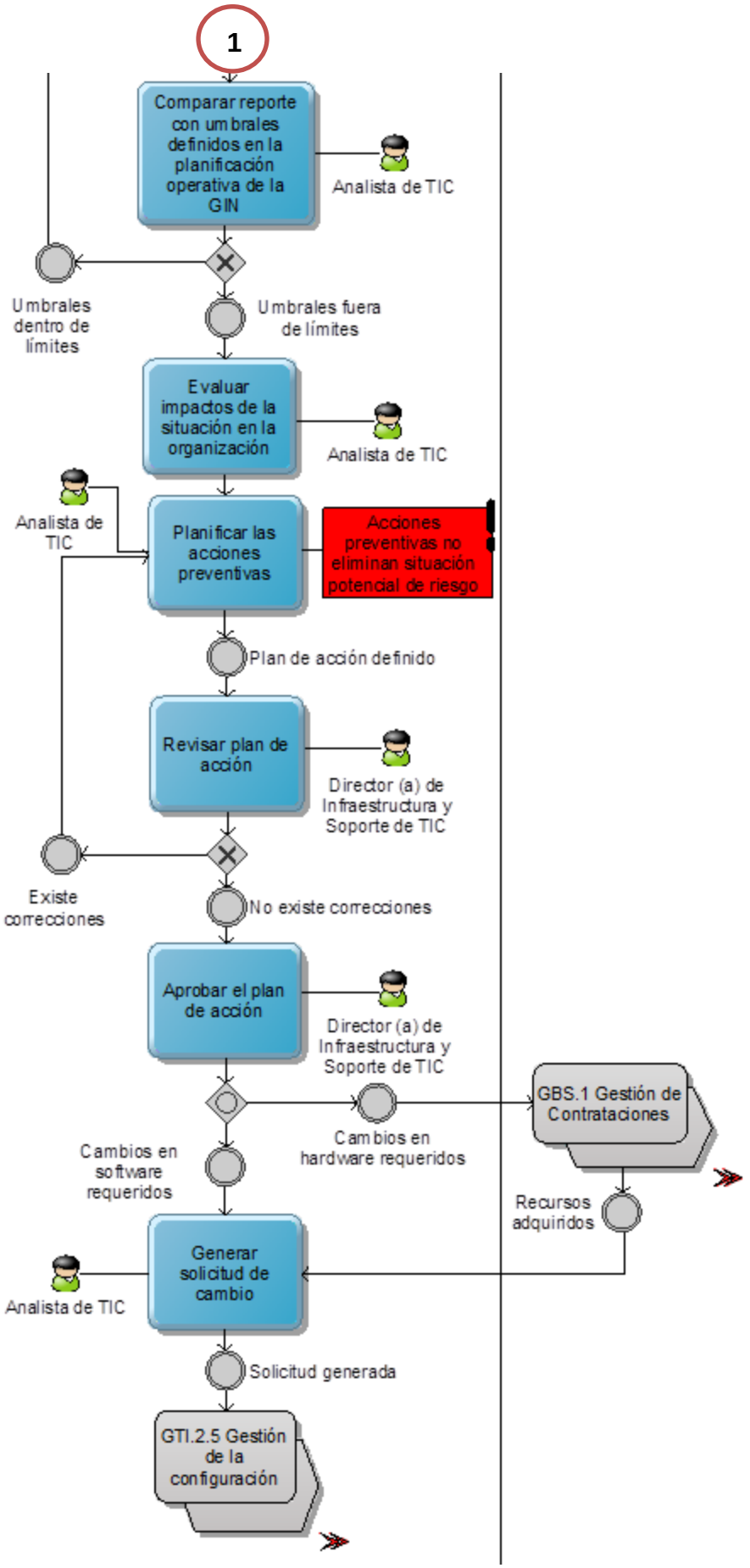

1
Solución construida exitosamente
Preparar solicitud de cambios en la configuración
Lider de proyecto
Solitud de cambios elaborada
GTI.2.5 Gestión de la configuración
Repositorio de la configuración actualizado
Falta de segregación de entornos
Realizar pruebas y control de calidad
Miembros del equipo ejecutor
Control de calidad aprobado
Control de calidad no aprobado
Elaborar los manuales de usuario
Realizar ajustes a la solución
Miembros del equipo ejecutor
Manuales elaborados
Miembros del equipo ejecutor
Ejecutar la capacitación para el uso de la solución tecnológica
Miembros del equipo ejecutor
Implantar la solución tecnológica en ambiente de producción
Miembros del equipo ejecutor
Alteración de información institucional
Robo de información
Actualizar información de construcción en el repositorio
Lider de proyecto
Solución implantada y probada

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Realizar el diseño detallado de la arquitectura de la solución	TICS	Interrupción del negocio	No se aplica el ciclo de vida a los componentes de red	Para el diseño de bases de datos se utiliza (DTS DE SQL2000) sin soporte técnico por Microsoft	ALTA
Realizar pruebas y control de calidad	TICS	Interrupción del negocio	Falta de segregación de entornos	En los entornos de desarrollo y prueba se utilicen los datos de producción sin enmascararlos, razón por la cual se dificulta en garantizar la confidencialidad	MEDIA
Actualizar información de construcción en el repositorio	Personas	Fraude interno (Personas)	Alteración de información institucional	El repositorio no tiene las seguridades suficientes de acceso a la información	MEDIA
Actualizar información de construcción en el repositorio	Personas	Fraude interno (Personas)	Robo de información	Existe un riesgo potencial de robo de información sujeta a sigilo bancario	MEDIA

Tabla No. 10 Identificación de riesgos por actividad (GTI.2.3)

4.4.2.4 *Gestión de la disponibilidad y capacidad*

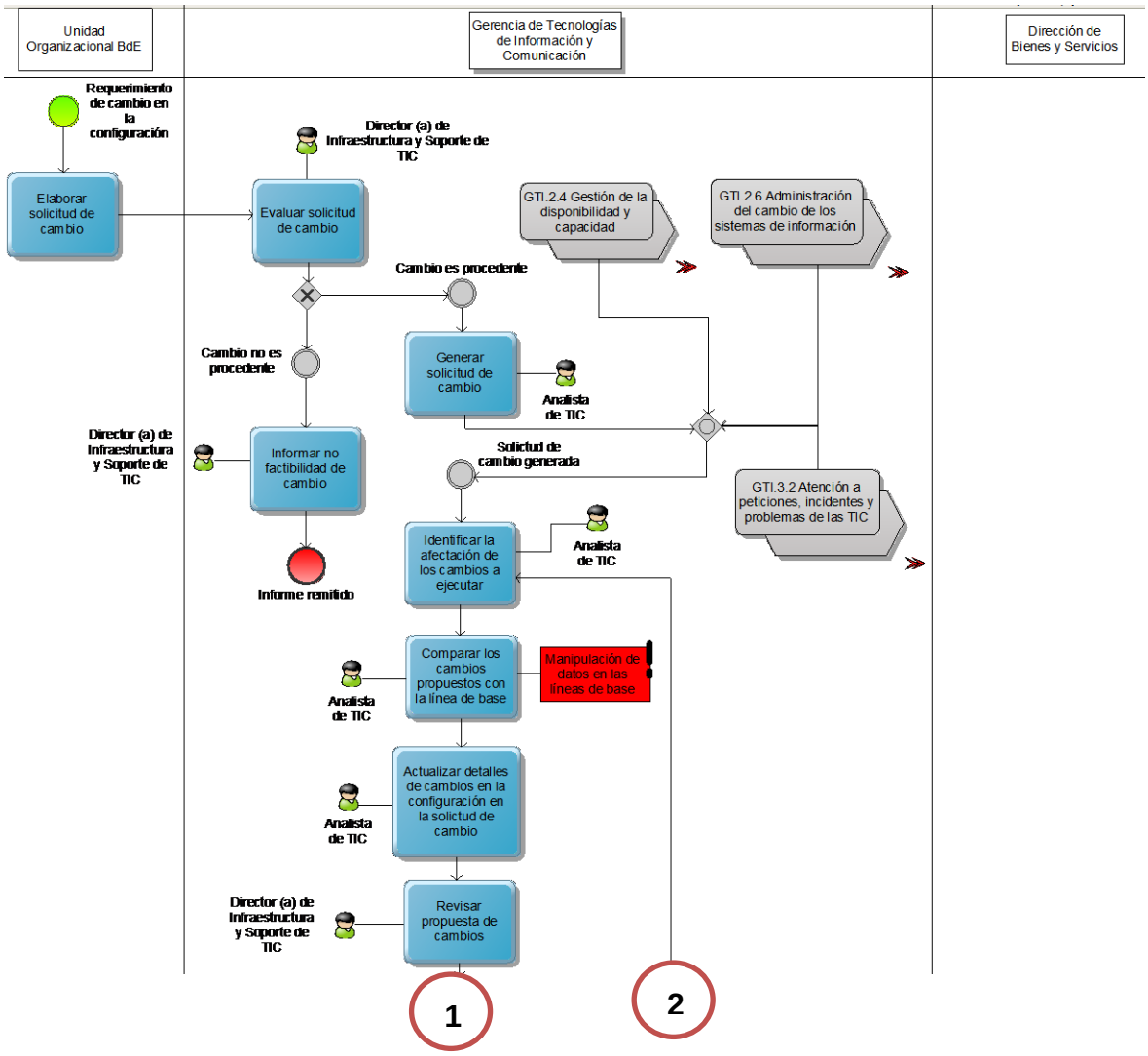


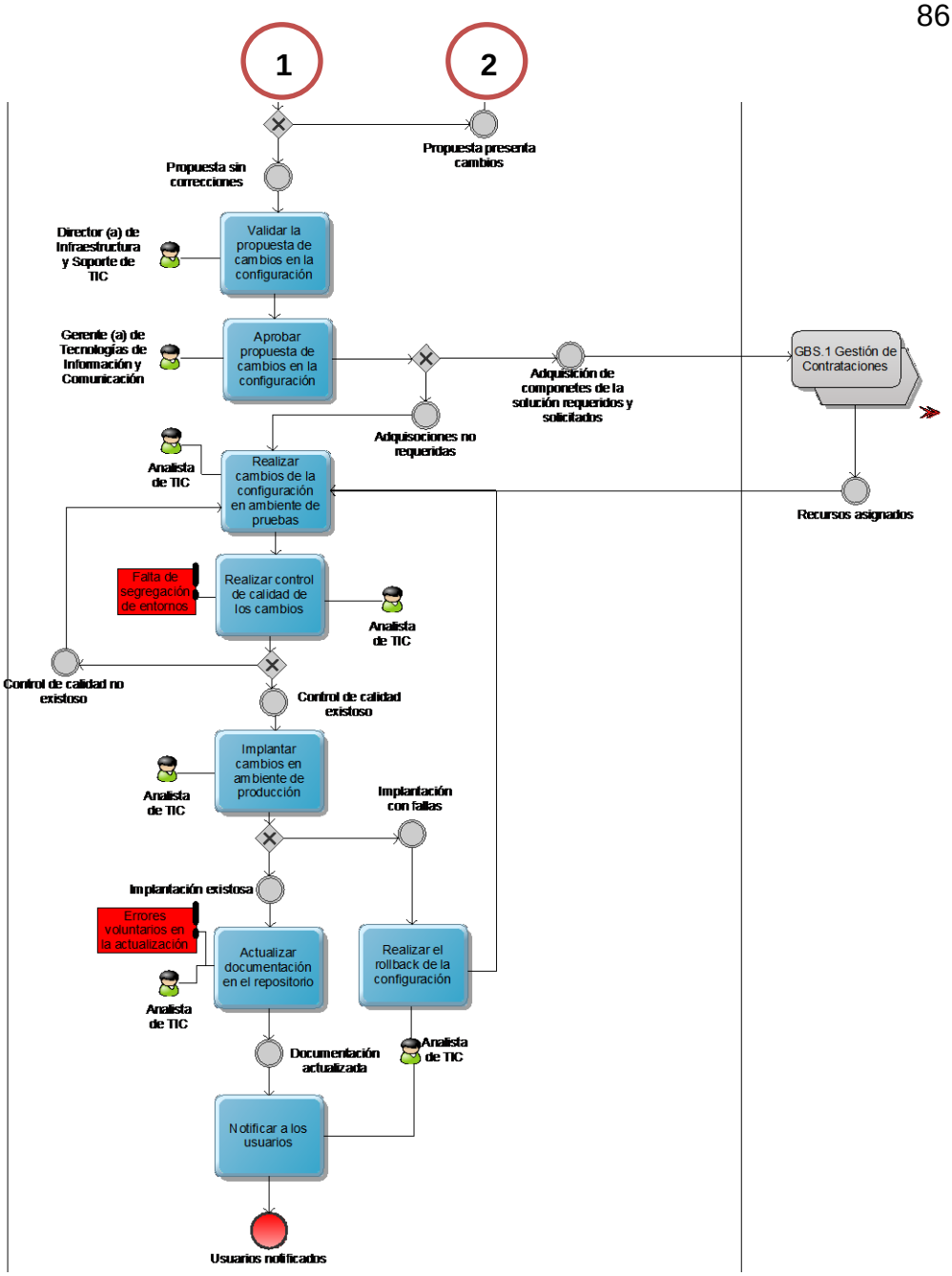

1
Comparar reporte con umbrales definidos en la planificación operativa de la GIN
Analista de TIC
Umbrales dentro de límites
Umbrales fuera de límites
Evaluar impactos de la situación en la organización
Analista de TIC
Analista de TIC
Planificar las acciones preventivas
Acciones preventivas no eliminan situación potencial de riesgo
Plan de acción definido
Revisar plan de acción
Director (a) de Infraestructura y Soporte de TIC
Existe correcciones
No existe correcciones
Aprobar el plan de acción
Director (a) de Infraestructura y Soporte de TIC
GBS.1 Gestión de Contrataciones
Cambios en hardware requeridos
Cambios en software requeridos
Recursos adquiridos
Generar solicitud de cambio
Analista de TIC
Solicitud generada
GTI.2.5 Gestión de la configuración

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Monitorear los ítems de servicio planificados de las TIC	TICS	Interrupción del negocio	Sobreutilización de capacidad no detectada	La capacidad de la capacidad del servidor de correo electrónico no fue detectada colapsando el servicio	ALTA
Planificar las acciones preventivas	Procesos	Deficiencias en los procesos	Acciones preventivas no eliminan situación potencial de riesgo	Los planes preventivos no eliminan la situación potencial de riesgo causando esfuerzo innecesario	MEDIA

Tabla No. 11 Identificación de riesgos por actividad (GTI.2.4)

4.4.2.5 *Gestión de la configuración*



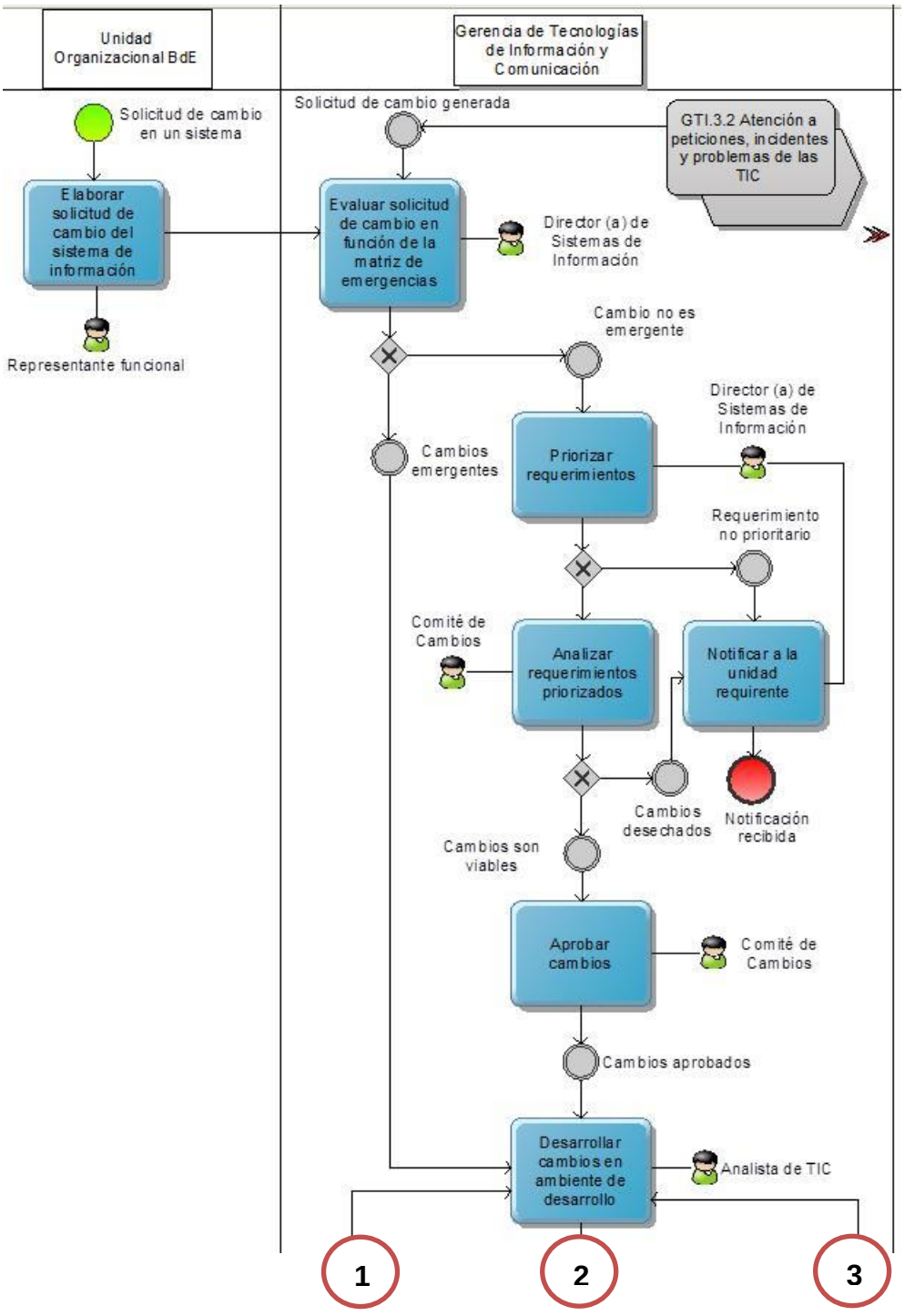


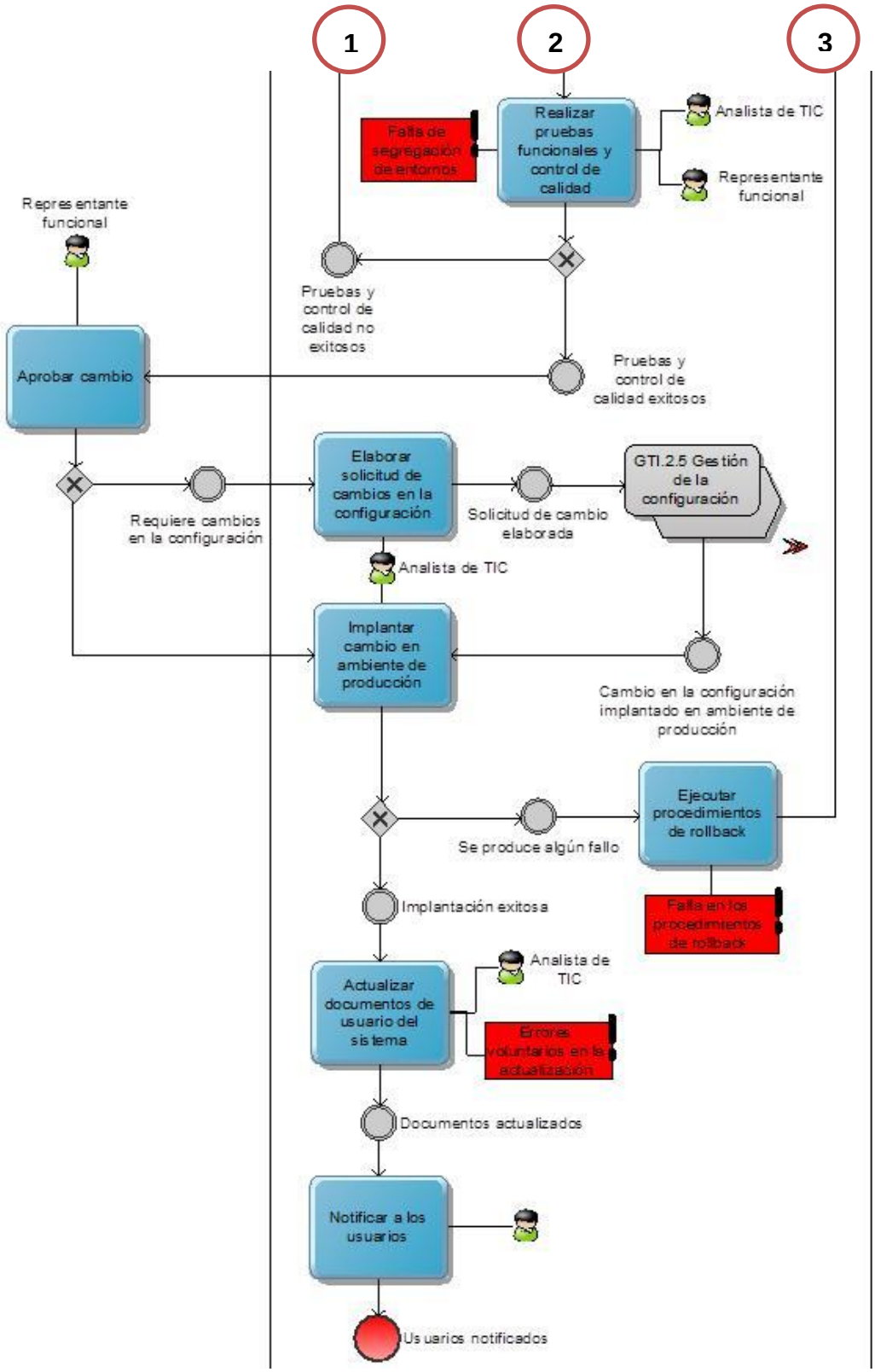
ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Comparar los cambios propuestos con la línea de base	TICS	Interrupción del negocio	Manipulación de datos en las líneas de base	Los datos han sido cambiados sin autorización en las líneas de base	MEDIA
Realizar control de calidad de los cambios	TICS	Interrupción del negocio	Falta de segregación de entornos	En los entornos de desarrollo y prueba se utilicen los datos de producción sin enmascararlos	ALTA

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Actualizar documentación en el repositorio	Personas	Fraude interno (Personas)	Errores voluntarios en la actualización	Se actualiza la información de los documentos deliberadamente equivocada	BAJA

Tabla No. 12 Identificación de riesgos por actividad (GTI.2.5)

4.4.2.6 *Administración del cambio de los sistemas de información*




1
2
3
Falla de segregación de entornos
Realizar pruebas funcionales y control de calidad
Analista de TIC
Representante funcional
Representante funcional
Pruebas y control de calidad no exitosos
Aprobar cambio
Pruebas y control de calidad exitosos
Elaborar solicitud de cambios en la configuración
GTI.2.5 Gestión de la configuración
Requiere cambios en la configuración
Solicitud de cambio elaborada
Analista de TIC
Implantar cambio en ambiente de producción
Cambio en la configuración implantado en ambiente de producción
Ejecutar procedimientos de rollback
Se produce algún fallo
Implantación exitosa
Falla en los procedimientos de rollback
Analista de TIC
Actualizar documentos de usuario del sistema
Errores voluntarios en la actualización
Documentos actualizados
Notificar a los usuarios
Usuarios notificados

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	FRECUENCIA ANUAL
Realizar pruebas funcionales y control de calidad	TICS	Interrupción del negocio	Falta de segregación de entornos	En los entornos de desarrollo y prueba se utilicen los datos de producción sin enmascararlos	ALTA
Ejecutar procedimientos de rollback	Procesos	Deficiencias en los procesos	Falla en los procedimientos de rollback	Los procedimientos de rollback no han sido probados para el regreso a la normalidad	BAJA
Actualizar documentos de usuario del sistema	TICS	Interrupción del negocio	Falta de segregación de entornos	En los entornos de desarrollo y prueba se utilicen los datos de producción sin enmascararlos	ALTA

Tabla No. 13 Identificación de riesgos por actividad (GTI.2.6)

4.4.3 Entrega de Servicio y Soporte Técnico de TI

Para comprender el resultado de la cadena de valor actual, en relación al marco de referencia COBIT 5.0, se presenta la Figura No. 35 asociando ambos elementos. Este dominio para el caso de instituciones públicas, cuenta el nuevo Esquema Gubernamental de Seguridad de la Información publicado en el Segundo Suplemento, Registro Oficial Nº 88 del miércoles 25 de septiembre de 2013, en donde se establecen todos los lineamientos relacionados con la seguridad de la información bajo un esquema NTE INEN-ISO/IEC 27000. Por otro lado, este dominio asegura la operación de las tecnologías de información en la continuidad del negocio.

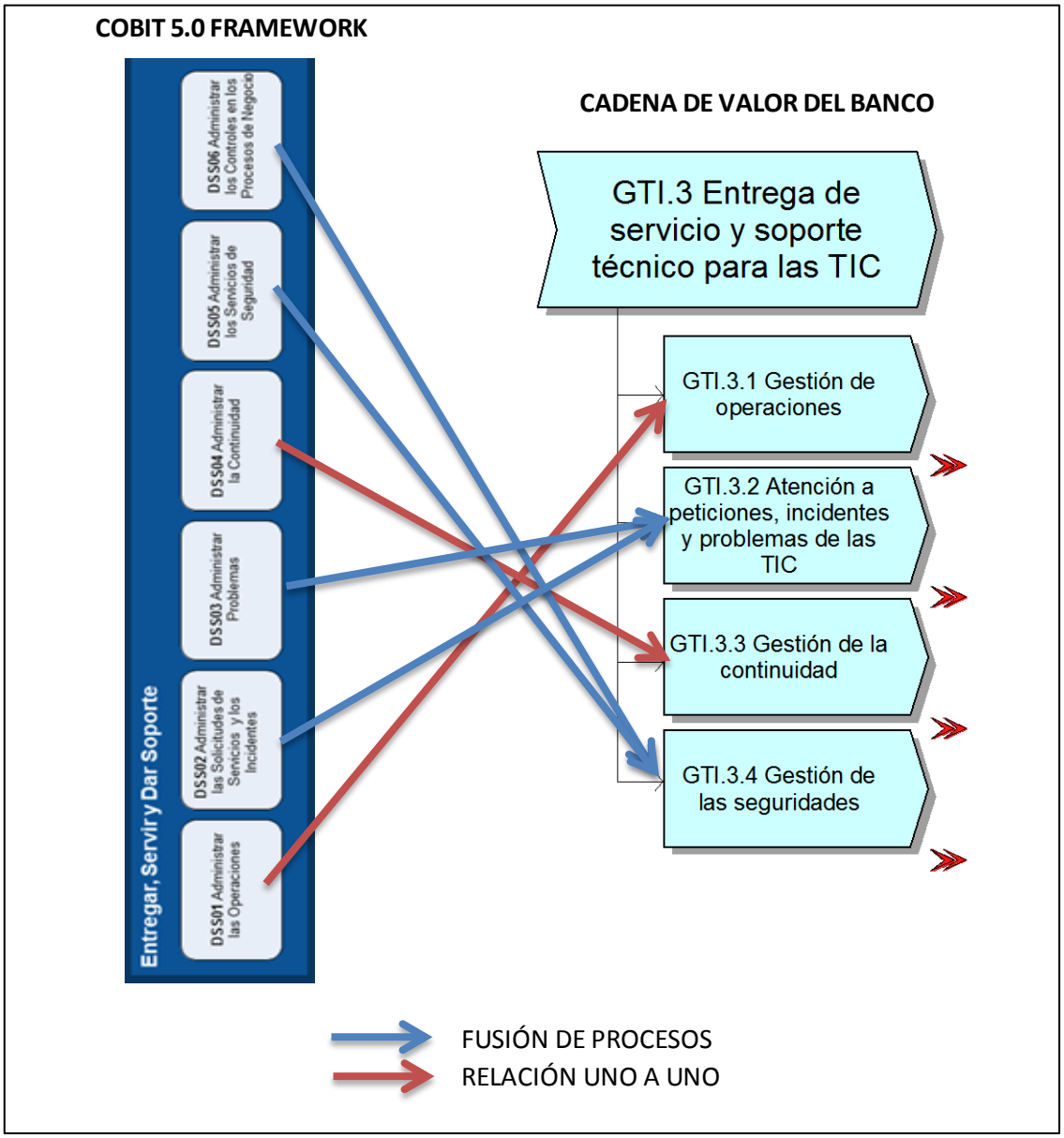
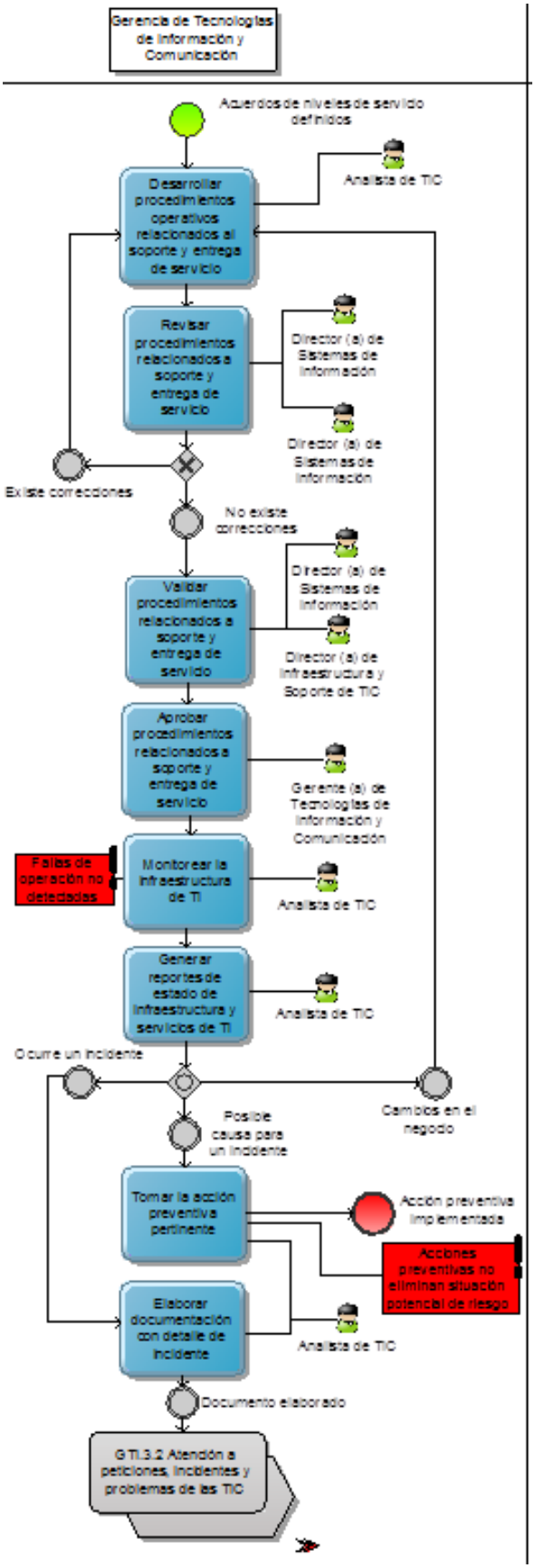


Figura No. 35 Relación COBIT 5.0 con el Dominio DSS aplicado al BdE

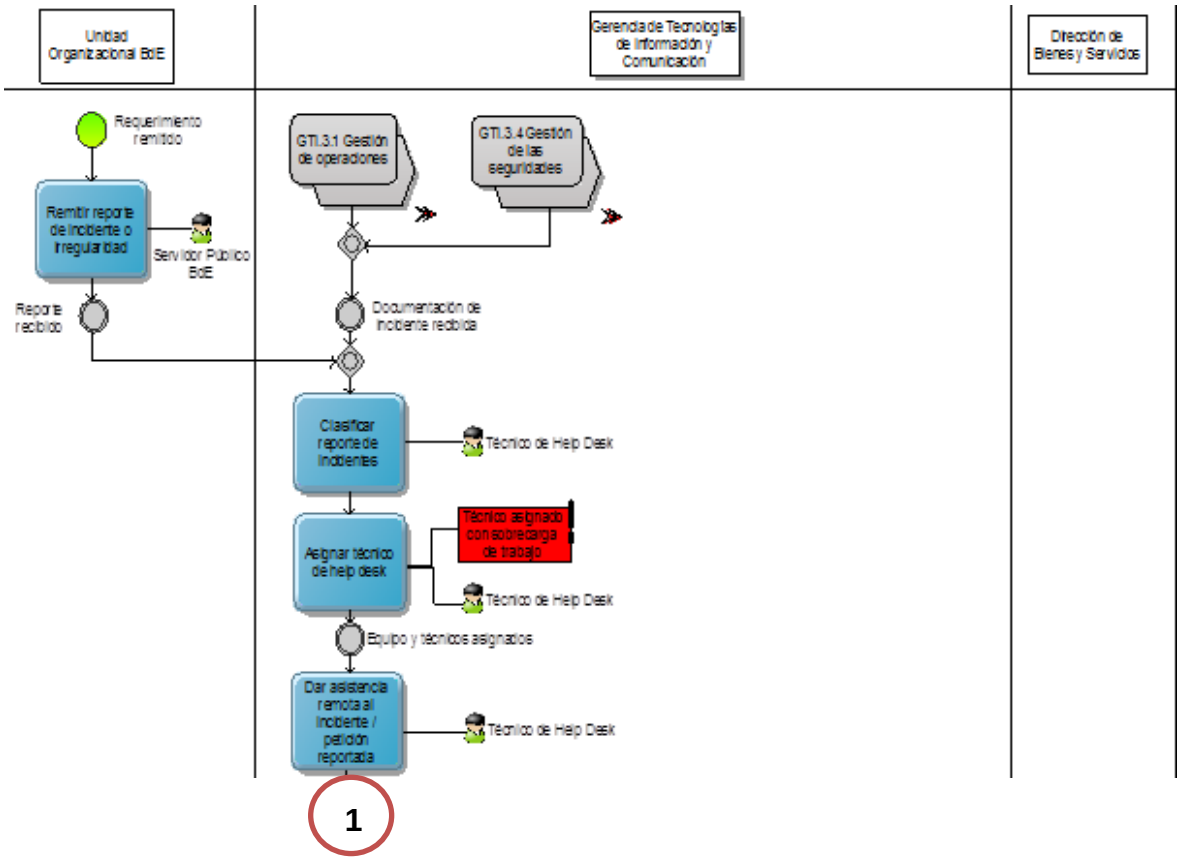
4.4.3.1 *Gestión de operaciones*

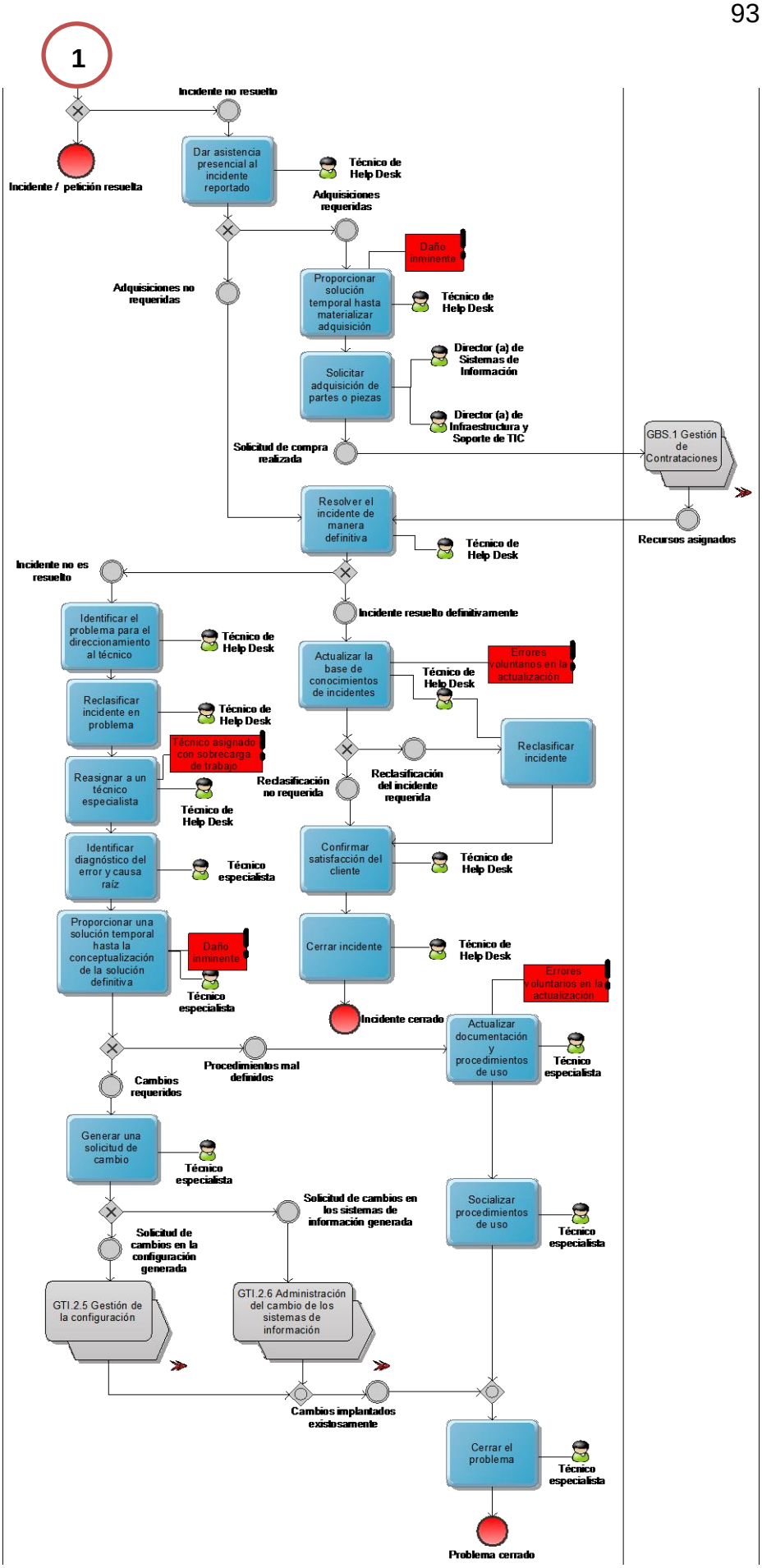


ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Monitorear la infraestructura de TI	TICS	Interrupción del negocio	Fallas de operación no detectadas	Fallas en los niveles de servicio establecidos en los SLA podrían no ser detectados	BAJA
Tomar la acción preventiva pertinente	Procesos	Deficiencias en los procesos	Acciones preventivas no eliminan situación potencial de riesgo	Los planes preventivos no eliminan la situación potencial de riesgo causando esfuerzo innecesario	MEDIA

Tabla No. 14 Identificación de riesgos por actividad (GTI.3.1)

4.4.3.2 *Atención a peticiones, incidentes y problemas de las TIC*

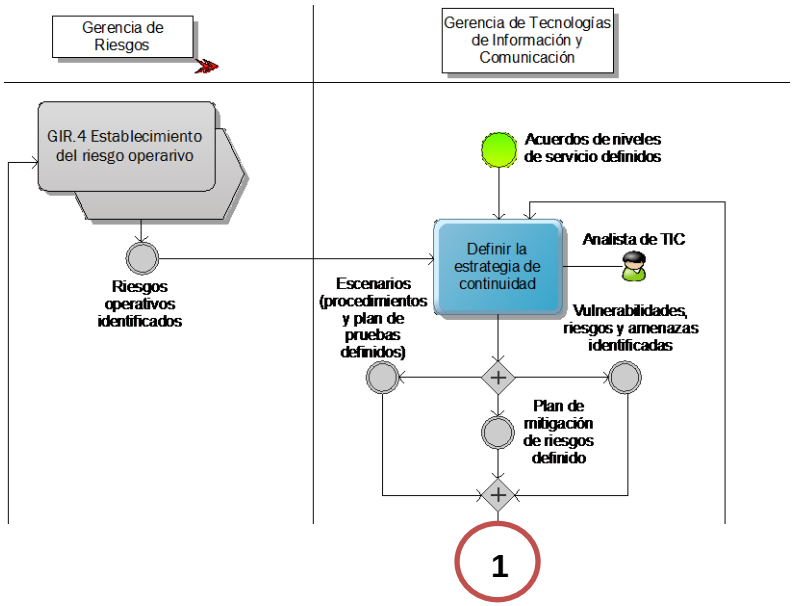


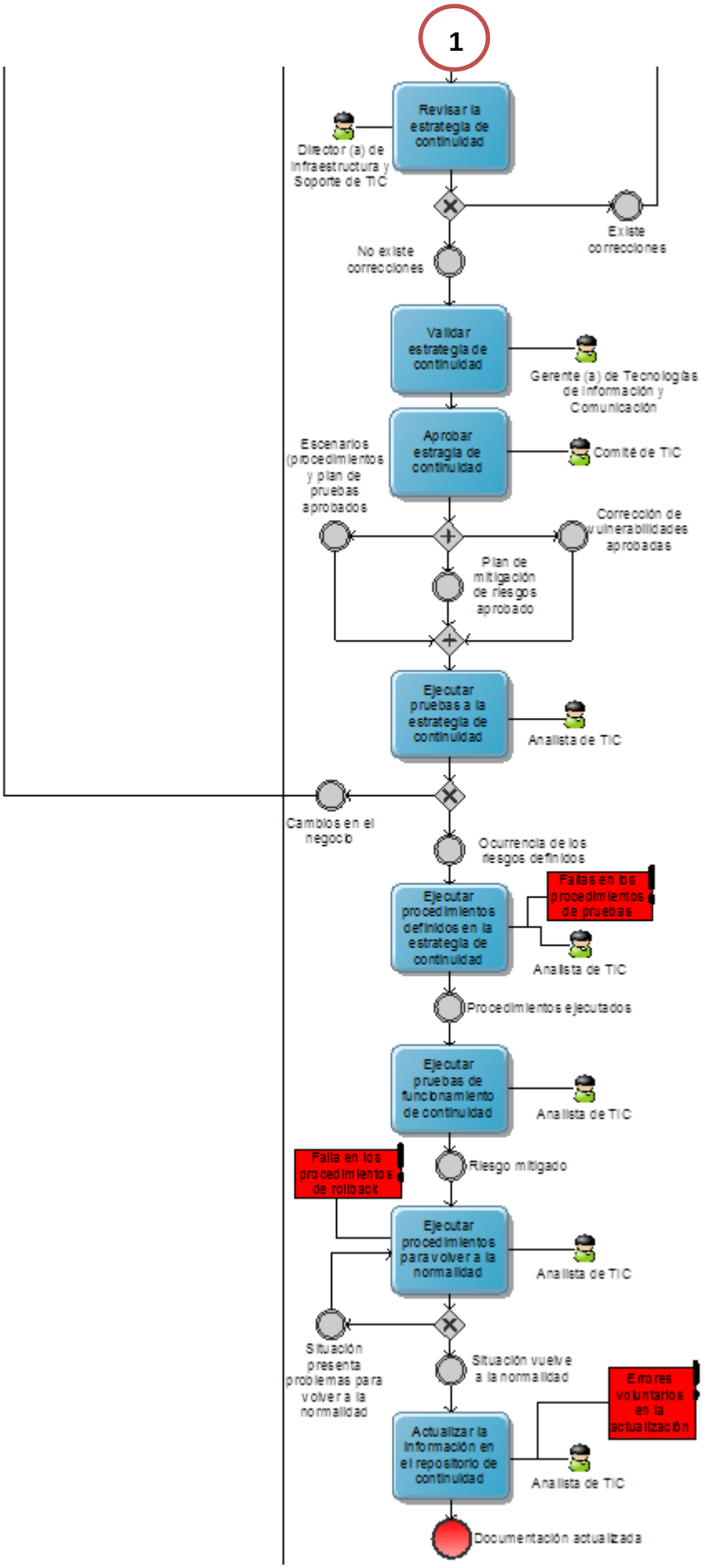

1
Incidente no resuelto
Incidente / petición resuelta
Dar asistencia presencial al incidente reportado
Técnico de Help Desk
Adquisiciones requeridas
Daño inminente
Adquisiciones no requeridas
Proporcionar solución temporal hasta materializar adquisición
Técnico de Help Desk
Solicitar adquisición de partes o piezas
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Solicitud de compra realizada
GBS.1 Gestión de Contrataciones
Recursos asignados
Resolver el incidente de manera definitiva
Técnico de Help Desk
Incidente no es resuelto
Incidente resuelto definitivamente
Identificar el problema para el direccionamiento al técnico
Técnico de Help Desk
Actualizar la base de conocimientos de incidentes
Errores voluntarios en la actualización
Técnico de Help Desk
Reclasificar incidente en problema
Técnico de Help Desk
Técnico asignado con sobrecarga de trabajo
Reasignar a un técnico especialista
Técnico de Help Desk
Reclasificación no requerida
Reclasificación del incidente requerida
Reclasificar incidente
Identificar diagnóstico del error y causa raíz
Técnico especialista
Confirmar satisfacción del cliente
Técnico de Help Desk
Proporcionar una solución temporal hasta la conceptualización de la solución definitiva
Daño inminente
Técnico especialista
Cerrar incidente
Técnico de Help Desk
Incidente cerrado
Errores voluntarios en la actualización
Actualizar documentación y procedimientos de uso
Técnico especialista
Procedimientos mal definidos
Cambios requeridos
Generar una solicitud de cambio
Técnico especialista
Solicitud de cambios en los sistemas de información generada
Socializar procedimientos de uso
Técnico especialista
Solicitud de cambios en la configuración generada
GTI.2.5 Gestión de la configuración
GTI.2.6 Administración del cambio de los sistemas de información
Cambios implantados exitosamente
Cerrar el problema
Técnico especialista
Problema cerrado

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Asignar técnico de Help Desk	Procesos	Deficiencias en los procesos	Técnico asignado con sobrecarga de trabajo	No se cuenta con una base técnica para asignar a los técnicos en base a la carga de trabajo	MEDIA
Proporcionar solución temporal hasta materializar adquisición	TICS	Interrupción del negocio	Daño inminente	La solución temporal puede causar daños en la infraestructura tecnológica	ALTA
Actualizar la base de conocimientos de incidentes	Personas	Fraude interno (Personas)	Errores voluntarios en la actualización	Se actualiza la información de los documentos deliberadamente equivocada	BAJA
Reasignar a un técnico especialista	Procesos	Deficiencias en los procesos	Técnico asignado con sobrecarga de trabajo	No se cuenta con una base técnica para asignar a los técnicos en base a la carga de trabajo	MEDIA
Proporcionar una solución temporal hasta la conceptualización de la solución definitiva	TICS	Interrupción del negocio	Daño inminente	La solución temporal puede causar daños en la infraestructura tecnológica	ALTA
Actualizar documentación y procedimientos de uso	Personas	Fraude interno (Personas)	Errores voluntarios en la actualización	Se actualiza la información de los documentos deliberadamente equivocada	BAJA

Tabla No. 15 Identificación de riesgos por actividad (GTI.3.2)

4.4.3.3 *Gestión de continuidad*

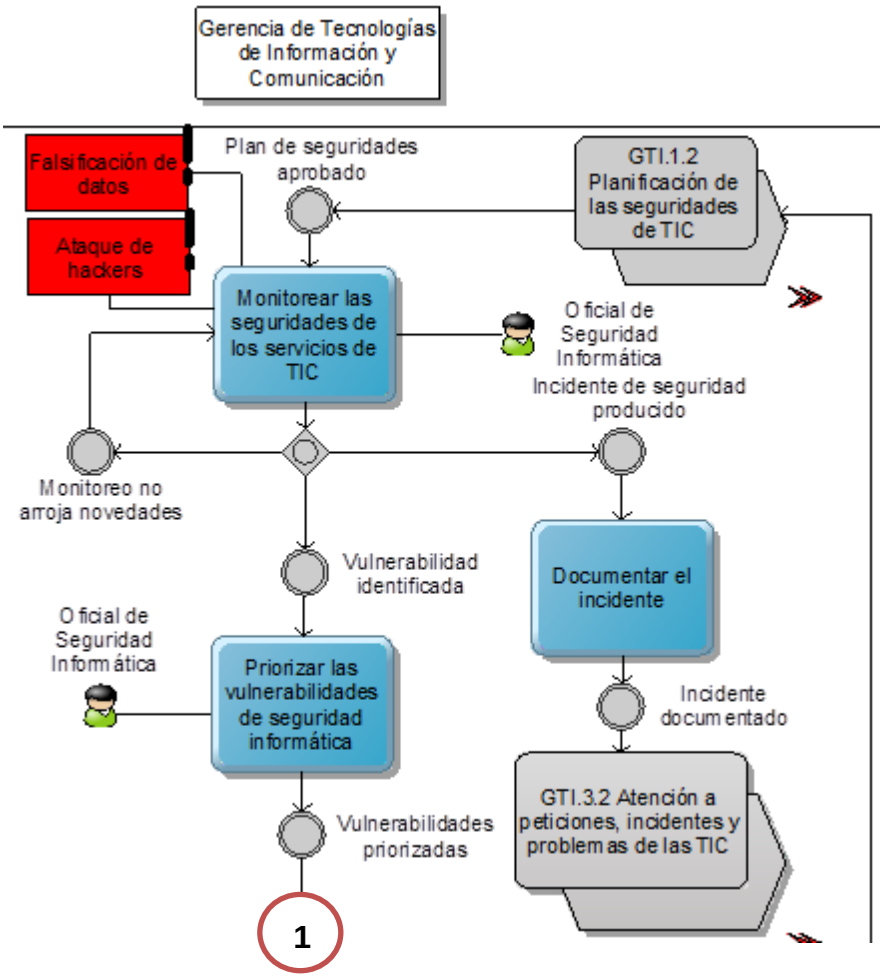


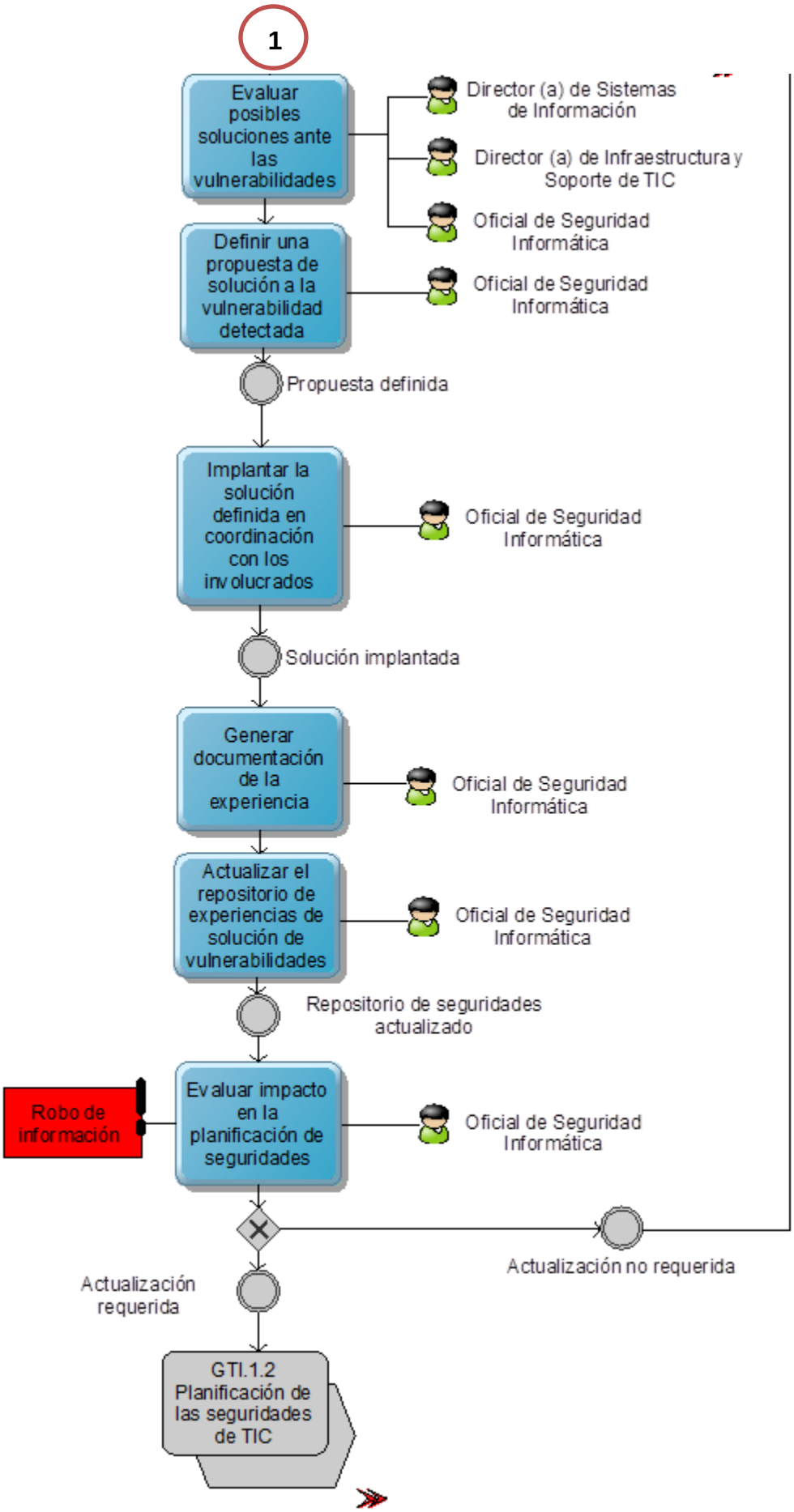

1
Revisar la estrategia de continuidad
Director (a) de Infraestructura y Soporte de TIC
Existe correcciones
No existe correcciones
Validar estrategia de continuidad
Gerente (a) de Tecnologías de Información y Comunicación
Aprobar estragia de continuidad
Comité de TIC
Escenarios (procedimientos y plan de pruebas aprobados
Corrección de vulnerabilidades aprobadas
Plan de mitigación de riesgos aprobado
Ejecutar pruebas a la estrategia de continuidad
Analista de TIC
Cambios en el negocio
Ocurrencia de los riesgos definidos
Ejecutar procedimientos definidos en la estrategia de continuidad
Fallas en los procedimientos de pruebas
Analista de TIC
Procedimientos ejecutados
Ejecutar pruebas de funcionamiento de continuidad
Analista de TIC
Falla en los procedimientos de rollback
Riesgo mitigado
Ejecutar procedimientos para volver a la normalidad
Analista de TIC
Situación presenta problemas para volver a la normalidad
Situación vuelve a la normalidad
Errores voluntarios en la actualización
Actualizar la información en el repositorio de continuidad
Analista de TIC
Documentación actualizada

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Ejecutar procedimientos definidos en la estrategia de continuidad	Procesos	Deficiencias en los procesos	Fallas en los procedimientos de pruebas	Los procedimientos de prueba no cuentan con estándares para su correcta ejecución	ALTA
Ejecutar procedimientos para volver a la normalidad	Procesos	Deficiencias en los procesos	Falla en los procedimientos de rollback	Los procedimientos de rollback no han sido probados para el regreso a la normalidad	ALTA
Actualizar la información en el repositorio de continuidad	Personas	Fraude interno (Personas)	Errores voluntarios en la actualización	Se actualiza la información de los documentos deliberadamente equivocada	MEDIA

Tabla No. 16 Identificación de riesgos por actividad (GTI.3.3)

4.4.3.4 *Gestión de las seguridades*




1
Evaluar posibles soluciones ante las vulnerabilidades
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Oficial de Seguridad Informática
Definir una propuesta de solución a la vulnerabilidad detectada
Oficial de Seguridad Informática
Propuesta definida
Implantar la solución definida en coordinación con los involucrados
Oficial de Seguridad Informática
Solución implantada
Generar documentación de la experiencia
Oficial de Seguridad Informática
Actualizar el repositorio de experiencias de solución de vulnerabilidades
Oficial de Seguridad Informática
Repositorio de seguridades actualizado
Robo de información
Evaluar impacto en la planificación de seguridades
Oficial de Seguridad Informática
Actualización no requerida
Actualización requerida
GTI.1.2 Planificación de las seguridades de TIC

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Monitorear las seguridades de los servicios de TIC	TICS	Fraude externo (TIC)	Ataque de hackers	La información confidencial podría ser vulnerada mediante ataques DDOS	ALTA
Monitorear las seguridades de los servicios de TIC	Eventos Externos	Fraude externo (EE)	Falsificación de datos	Se podrían crear datos falsos de manera externa	ALTA
Evaluar impacto en la planificación de seguridades	Personas	Fraude interno (Personas)	Robo de información	Se podría robar la información confidencial de las seguridades y ser entregada a terceros	ALTA

Tabla No. 17 Identificación de riesgos por actividad (GTI.3.4)

4.4.4 Monitoreo y Control de TI

Para comprender el resultado de la cadena de valor actual, en relación al marco de referencia COBIT 5.0, se presenta la Figura No. 35 asociando ambos elementos. Este dominio se relaciona con la norma ISO/IEC 15504, la que proporciona un marco de trabajo para la evaluación de los procesos y establece los requisitos mínimos para realizar una evaluación de forma consistente, tal como se describió el numeral 2.6 del Marco Teórico.

Cabe mencionar que los tres procesos que componen este dominio, dentro de la cadena de valor del proceso de Gestión de Tecnologías de Información, se han fusionado en uno solo, y se ha creado un proceso adicional que tiene que ver con la evaluación de la planificación operativa anual, con la directrices de la Norma Técnica del Gobierno por Resultados (GPR).

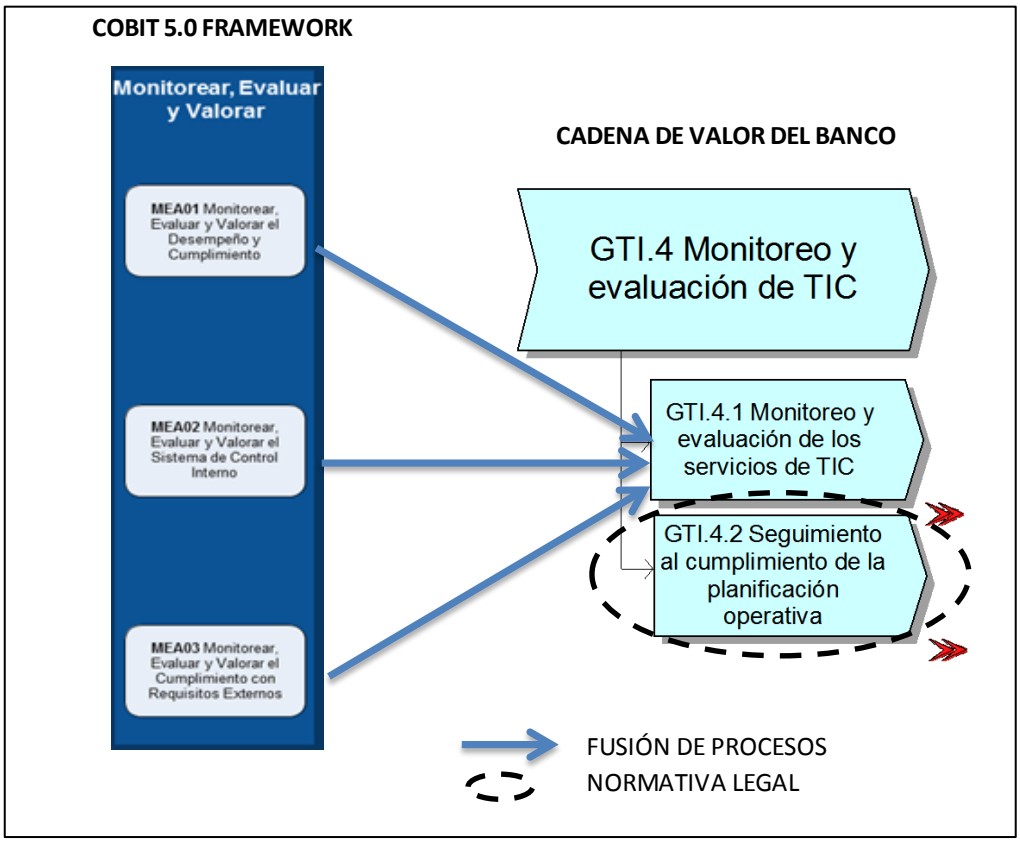
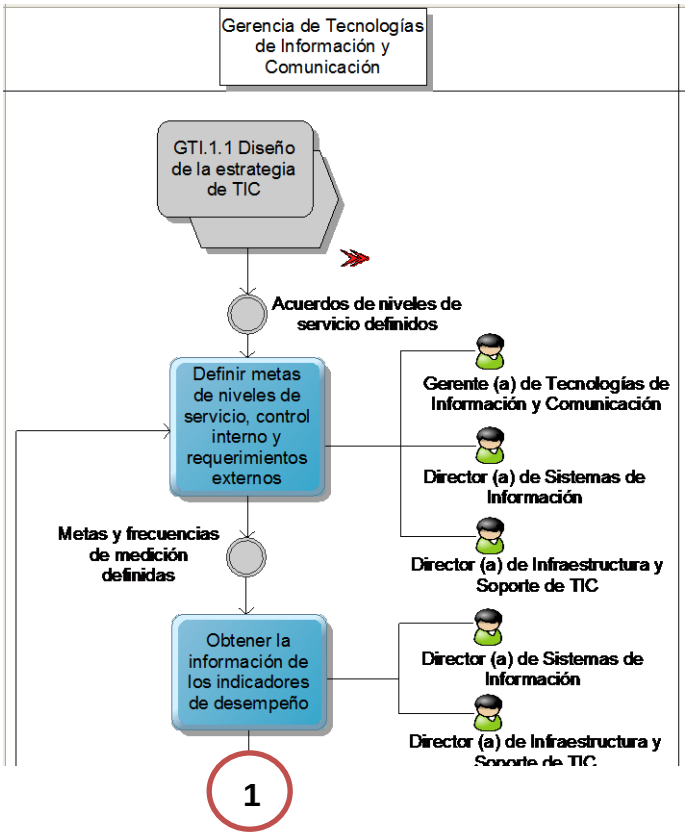
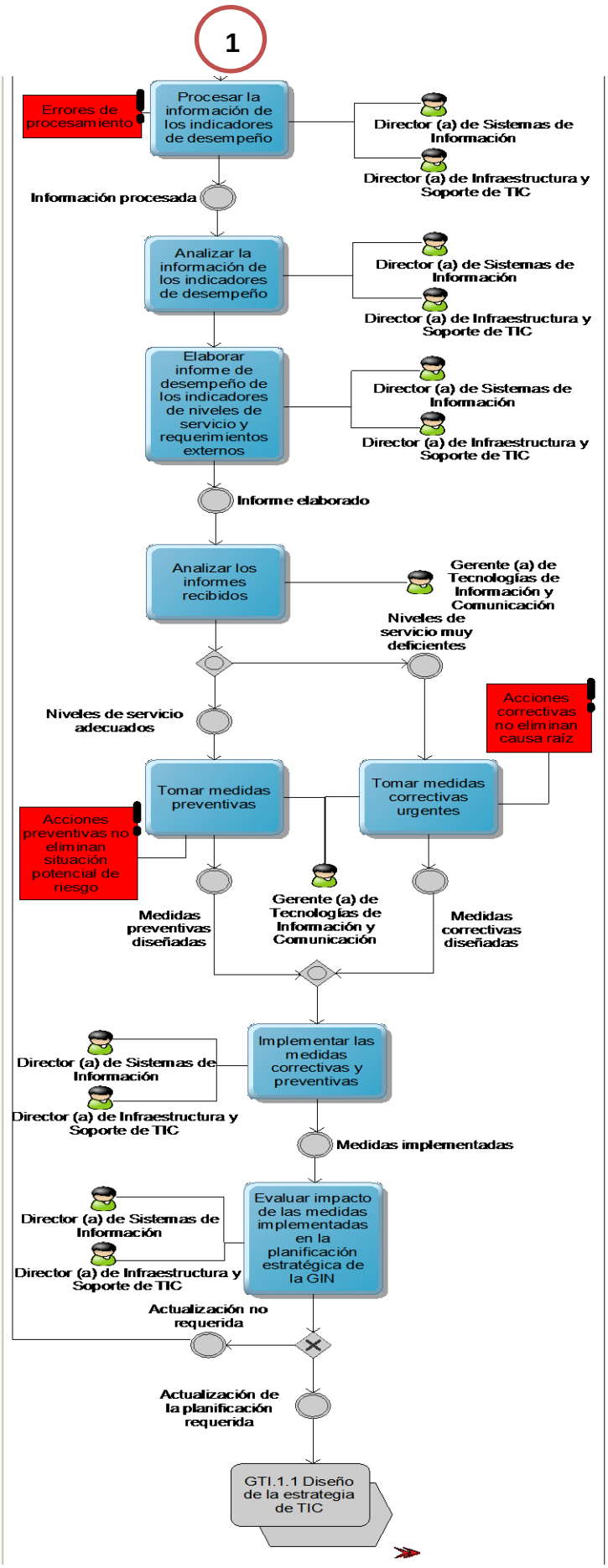


Figura No. 36 Relación COBIT 5.0 con el Dominio MAE aplicado al BdE

4.4.4.1 *Monitoreo y evaluación de los servicios de TIC*

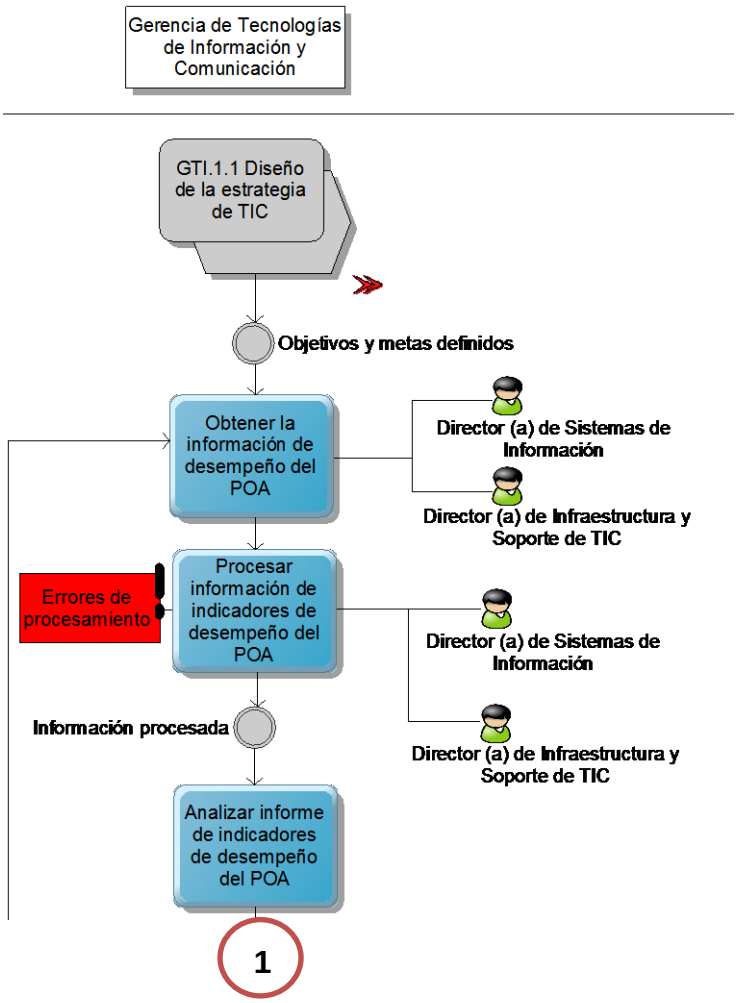


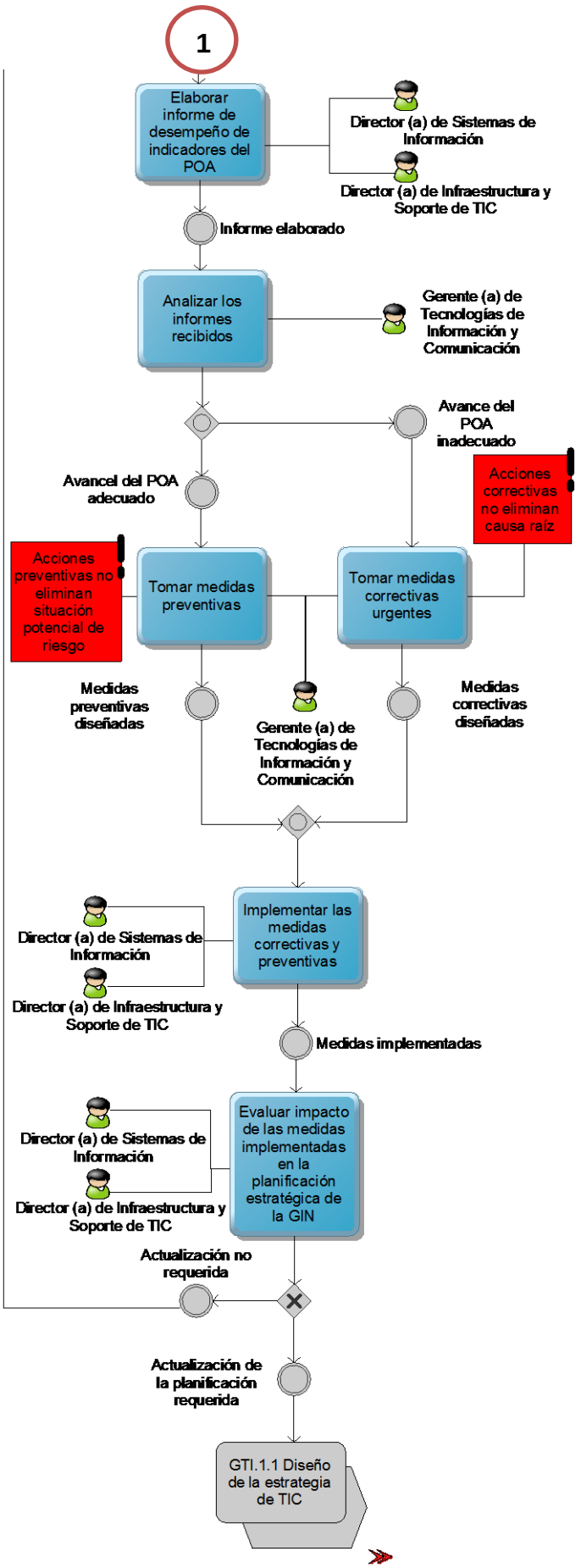

1
Errores de procesamiento
Procesar la información de los indicadores de desempeño
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Información procesada
Analizar la información de los indicadores de desempeño
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Elaborar informe de desempeño de los indicadores de niveles de servicio y requerimientos externos
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Informe elaborado
Analizar los informes recibidos
Gerente (a) de Tecnologías de Información y Comunicación
Niveles de servicio muy deficientes
Niveles de servicio adecuados
Acciones correctivas no eliminan causa raíz
Tomar medidas preventivas
Tomar medidas correctivas urgentes
Acciones preventivas no eliminan situación potencial de riesgo
Gerente (a) de Tecnologías de Información y Comunicación
Medidas preventivas diseñadas
Medidas correctivas diseñadas
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Implementar las medidas correctivas y preventivas
Medidas implementadas
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Evaluar impacto de las medidas implementadas en la planificación estratégica de la GIN
Actualización no requerida
Actualización de la planificación requerida
GTI.1.1 Diseño de la estrategia de TIC

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Procesar la información de los indicadores de desempeño	Personas	Fraude interno (Personas)	Errores de procesamiento	La información ingresada para el cálculo de indicadores es manual pudiendo existir errores	MEDIA
Tomar medidas preventivas	Procesos	Deficiencias en los procesos	Acciones preventivas no eliminan situación potencial de riesgo	Los planes preventivos no eliminan la situación potencial de riesgo causando esfuerzo innecesario	MEDIA
Tomar medidas correctivas urgentes	Procesos	Deficiencias en los procesos	Acciones correctivas no eliminan causa raíz	Los planes correctivos no eliminan la causa raíz del riesgo	MEDIA

Tabla No. 18 Identificación de riesgos por actividad (GTI.4.1)

4.4.4.2 *Seguimiento al cumplimiento de la planificación operativa anual*




1
Elaborar informe de desempeño de indicadores del POA
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Informe elaborado
Analizar los informes recibidos
Gerente (a) de Tecnologías de Información y Comunicación
Avance del POA inadecuado
Acciones correctivas no eliminan causa raíz
Avancel del POA adecuado
Acciones preventivas no eliminan situación potencial de riesgo
Tomar medidas preventivas
Tomar medidas correctivas urgentes
Medidas preventivas diseñadas
Gerente (a) de Tecnologías de Información y Comunicación
Medidas correctivas diseñadas
Implementar las medidas correctivas y preventivas
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Medidas implementadas
Evaluar impacto de las medidas implementadas en la planificación estratégica de la GIN
Director (a) de Sistemas de Información
Director (a) de Infraestructura y Soporte de TIC
Actualización no requerida
Actualización de la planificación requerida
GTI.1.1 Diseño de la estrategia de TIC

ACTIVIDAD RELACIONADA	FACTOR DE RIESGO	EVENTO DE RIESGO	ACTIVIDAD DE RIESGO	DESCRIPCIÓN DE RIESGO	PROB. DE OCUR.
Procesar la información de los indicadores de desempeño del POA	Personas	Fraude interno (Personas)	Errores de procesamiento	La información ingresada para el cálculo de indicadores es manual pudiendo existir errores	MEDIA
Tomar medidas preventivas	Procesos	Deficiencias en los procesos	Acciones preventivas no eliminan situación potencial de riesgo	Los planes preventivos no eliminan la situación potencial de riesgo causando esfuerzo innecesario	MEDIA
Tomar medidas correctivas urgentes	Procesos	Deficiencias en los procesos	Acciones correctivas no eliminan causa raíz	Los planes correctivos no eliminan la causa raíz del riesgo	MEDIA

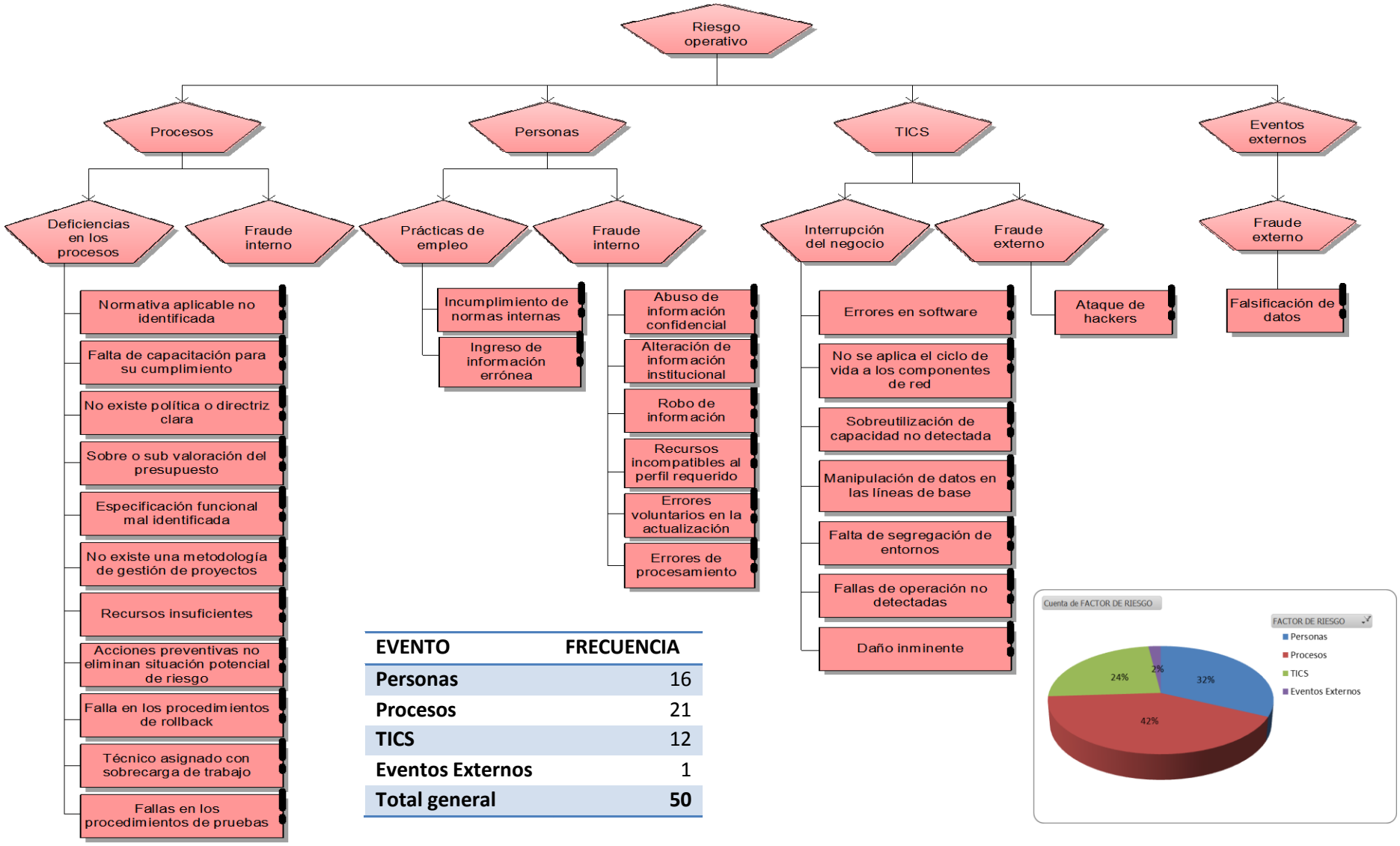
Tabla No. 19 Identificación de riesgos por actividad (GTI.4.2)

4.5 DISCUSIÓN DE RESULTADOS

4.5.1 Diagrama de riesgos

El diagrama de riesgos se utiliza para clasificar los riesgos en jerarquías según la Resolución JB-2005-834, relacionada con la Gestión del Riesgo Operativo. Los riesgos identificados en el trabajo de campo, relacionados a las actividades de cada proceso, se clasificaron en las cuatro categorías, que representan los factores de riesgo, las que a su vez, poseen subcategorías que representan los eventos de riesgo.

Con la base de esta identificación de riesgos, el siguiente paso para futuras investigaciones es la realización de la medición cualitativa para su priorización, y posteriormente, la medición cuantitativa para evaluar la probabilidad de ocurrencia con el impacto económico, a fin de garantizar la continuidad del negocio. Esta medición servirá de base para el diseño de controles e implementación de los mismos, en donde se evidencien situaciones potenciales de riesgo de alto impacto. La Figura No. 37 muestra el diagrama de riesgos resumen.



EVENTO	FRECUENCIA
Personas	16
Procesos	21
TICS	12
Eventos Externos	1
Total general	**50**

Figura No. 37 Diagrama de riesgos del proceso de Gestión de Tecnologías de Información y Comunicación

El diagrama de riesgos muestra cada uno de las actividades de riesgo presente en los distintos procesos. La Figura No. 37 muestra la frecuencia total de las actividades de riesgos sin importar si repiten en los diferentes procesos, concluyendo que existen los siguientes riesgos comunes, cuya frecuencia es mayor a uno:

ACTIVIDAD DE RIESGO	FRECUENCIA
Abuso de información confidencial	2
Acciones correctivas no eliminan causa raíz	2
Acciones preventivas no eliminan situación potencial de riesgo	4
Alteración de información institucional	2
Daño inminente	2
Errores de procesamiento	2
Errores voluntarios en la actualización	4
Especificación funcional mal identificada	2
Falla en los procedimientos de rollback	2
Falta de segregación de entornos	4
No existe política o directriz clara	2
Robo de información	4
Sobre o sub valoración del presupuesto	2
Técnico asignado con sobrecarga de trabajo	2
Total general	**36**

Tabla No. 20 Riesgos comunes

Existen cuatro actividades de riesgo que se consideran como las más comunes, cuyo diseño e implementación de controles, impactarían en cada uno de los subprocesos en los que aparecen.

Con este análisis, se acepta la hipótesis planteada: "*Los factores y eventos de riesgos que se identificarán dentro del Proceso de Gestión de Tecnologías de Información y Comunicaciones con base a COBIT 5.0 se encuentran concentrados en la categoría del factor de procesos"* con un 42% de actividades de riesgo contenidas dentro de esta categoría.

4.5.2 Análisis de riesgos por procesos

Del trabajo de campo, se identificaron un total de 50 actividades de riesgos, agrupados en los cuatro dominios de COBIT 5.0, tal como se muestra a continuación:

DOMINIO	FRECUENCIA
GTI.1 Planificación y Organización de TIC	13
GTI.2 Construcción, Adquisición e Implementación de TIC	17
GTI.3 Entrega de servicio y soporte técnico para las TIC	14
GTI.4 Monitoreo y evaluación de TIC	6
Total general	50

Tabla No. 21 Resumen de riesgos por proceso

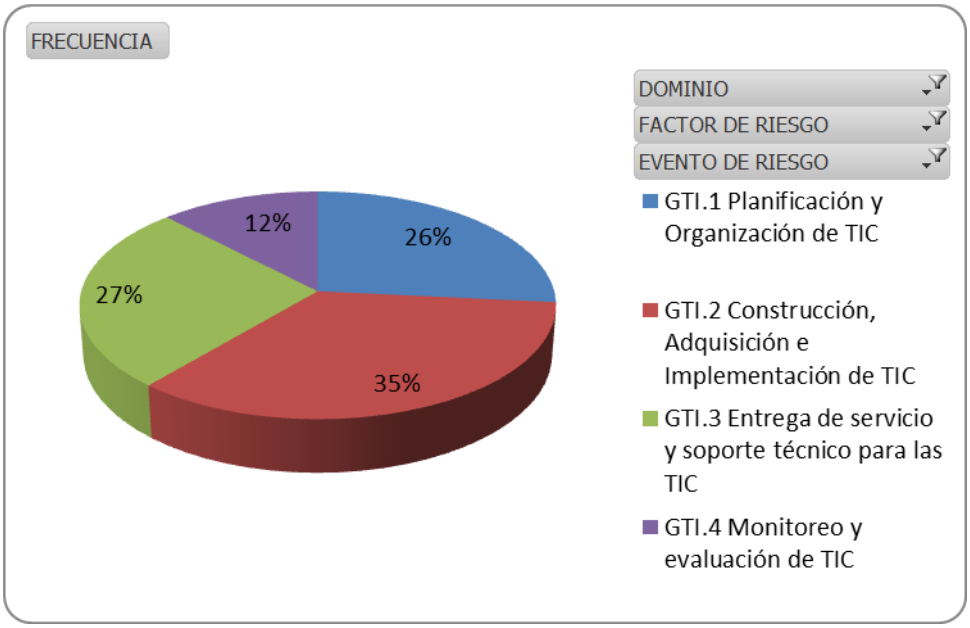


Figura No. 38 Estructura de riesgos por proceso

De los procesos analizados, el proceso con mayor número de actividades de riesgo es GTI.2 Construcción, Adquisición e Implementación de TIC. Esto se debe a que es un proceso que contiene seis subprocesos, además de ser un área de gestión crítica para la administración de las tecnologías de información.

El dominio de Planificación y Organización de TIC, presenta la siguiente estructura de riesgos por factor:

DOMINIO / FACTOR DE RIESGO	FRECUENCIA
GTI.1 Planificación y Organización de TIC	13
Personas	6
Procesos	6
TICS	1
Total General	**13**

Tabla No. 22 Estructura de riesgos Dominio Planificación y Organización de TIC

Como se observa en la Tabla No. 22, la tendencia de actividades de riesgo hacia el factor de procesos se mantiene, siendo este el más importante en este dominio.

El dominio de Construcción, Adquisición e Implementación de TIC, presenta la siguiente estructura de riesgos por factor:

DOMINIO / FACTOR DE RIESGO	FRECUENCIA
GTI.2 Construcción, Adquisición e Implementación de TIC	**17**
Personas	4
Procesos	6
TICS	7
Total General	**17**

Tabla No. 23 Estructura de riesgos Dominio Construcción, Adquisición e Implementación de TIC

Como se observa en la Tabla No. 23, la tendencia de actividades de riesgo hacia el factor de procesos se mantiene, siendo este el más importante en este dominio.

El dominio de Entrega de Servicio y Soporte Técnico para las TIC, presenta la siguiente estructura de riesgos por factor:

DOMINIO / FACTOR DE RIESGO	FRECUENCIA
GTI.3 Entrega de servicio y soporte técnico para las TIC	**14**
Eventos Externos	1
Personas	4
Procesos	5
TICS	4
Total General	**14**

Tabla No. 24 Estructura de riesgos Dominio Entrega de Servicio y Soporte Técnico para las TIC

Como se observa en la Tabla No. 24, la tendencia de actividades de riesgo hacia el factor de procesos se mantiene, siendo este el más importante en este dominio.

El dominio de Monitoreo y Evaluación de TIC, presenta la siguiente estructura de riesgos por factor:

DOMINIO / FACTOR DE RIESGO	FRECUENCIA
GTI.4 Monitoreo y evaluación de TIC	**6**
Personas	2
Procesos	4
Total General	**6**

Tabla No. 25 Estructura de riesgos Dominio Monitoreo y evaluación de TIC

Como se observa en la Tabla No. 25, la tendencia de actividades de riesgo hacia el factor de procesos se mantiene, siendo este el más importante en este dominio.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En esta investigación se ha podido identificar los factores y eventos de riesgo operativo de TI con base en el Marco de Referencia COBIT 5.0, relacionados con la capacidad de este proceso para garantizar la continuidad del negocio en situaciones de contingencia, concluyendo que el factor de procesos según las Normas de Basilea II, es el que mayor actividades en riesgo posee con un 42% del total, mientras que el evento con mayor actividades de riesgo dentro del factor antes citado es deficiencia en los procesos, probando la hipótesis planteada inicialmente.

- La metodología aplicada para la documentación de procesos se enmarcó dentro de los estándares de ARIS PLATFORM, cuyas licencias de propiedad del Banco del Estado, sirvieron para el desarrollo de la presente investigación, para lo cual, dentro del filtro metodológico se utilizaron los siguientes modelos:
    a. Modelo de Introducción (Modelo de estructuración)
    b. Mapa de Procesos (Diagrama de Cadena de valor añadido)
    c. Riesgos agrupados en factores y eventos según BASILEA II (Diagrama de Riesgos)
    d. Flujogramas con integración a eventos de riesgo (CPE visualizado en columnas)
    e. IDEF0 para la identificación de ICOM[5] (CPE adaptado a IDEF0)

- Tras el mapeo del proceso de Gestión de Tecnologías de Información y Comunicación, se pudo evidenciar que a través de sus cuatro dominios, el Banco del Estado está haciendo los mejores esfuerzos para: mantener información de calidad para apoyar las decisiones del negocio, generar un

[5] I = Inputs o Entradas, C = Controles, O = Outputs o Salidas, y M = Mechanisms o Recursos.

valor comercial de las inversiones habilitadas por la Tecnología de la Información (TI), es decir, lograr metas estratégicas y mejoras al negocio mediante el uso eficaz e innovador de la TI; lograr una excelencia operativa mediante la aplicación eficiente y fiable de la tecnología; mantener el riesgo relacionado con TI a niveles aceptables; optimizar el costo de la tecnología y los servicios de TI.

- Del trabajo de campo, se identificaron un total de 50 actividades de riesgos, agrupados en cuatro dominios de COBIT 5.0 concluyendo que el proceso con mayor número de actividades de riesgo es GTI.2 Construcción, Adquisición e Implementación de TIC debido a que es un proceso que contiene seis subprocesos, además de ser un área de gestión crítica para la administración de las tecnologías de información. Cabe mencionar que este dominio contiene la mayor cantidad de actividades de riesgo en el factor TICS, con un 41%, debido a que este es el principal apoyo tecnológico para el desarrollo de soluciones tecnológicas, principalmente en el diseño de nuevos sistemas de información.

5.2 RECOMENDACIONES

- Se recomienda designar oficialmente mediante notificación de la Dirección de Administración de Talento Humano a gestores de riesgo operativo que desempeñen sus funciones dentro de los procesos de Gestión de Tecnologías de Información y Comunicaciones a fin de mantener actualizados los factores y eventos de riesgo operativo de TI con base en el Marco de Referencia COBIT 5.0 para su posterior medición cualitativa y/o cuantitativa, priorización e implementación de controles en cumplimiento de la Resolución JB-2005-834. Estos gestores deberán ser capacitados por la Dirección de Riesgo Operativo en la metodología de levantamiento de riesgos, y por la Dirección de Gestión de Calidad para el uso de la herramienta de Administración de Procesos y Riesgos del Banco del Estado.

- Se considera una excelente alternativa, migrar las licencias actuales de ARIS PLATFORM 7.0 a ARIS PLATFORM 9.6, ya que es una versión que tiene mejoras en la administración de procesos con un enfoque a riesgos tales como:
    a. Los usuarios pueden conectarse, comunicarse y colaborar para mejorar los procesos e identificación de riesgos a través de las redes sociales como FACEBOOK y TWITER.
    b. Los usuarios pueden visualizar, crear, analizar y mejorar el contenido de proceso e identificación de sus riesgos asociados en sus dispositivos móviles
    c. Los usuarios pueden almacenar sus procesos, formatos y mediciones de riesgos asociados con tecnología en la nube.

- Para realizar un ciclo de mejora continua en los esfuerzos realizados por el Banco del Estado en relación a COBIT 5.0, se recomienda la implementación de los indicadores de desempeño de este marco de referencia de manera priorizada, con la finalidad de obtener un cuadro de monitoreo de procesos asociados a los indicadores claves de riesgo, lo que deberán ser incluidos en el Plan de Continuidad del Negocio.

- Se recomienda utilizar los hallazgos de esta investigación para continuar con la medición cualitativa y/o cuantitativa, diseño de los controles que minimicen el impacto de los riesgos, y finalmente, su monitoreo y control para la medición del riesgo residual.

REFERENCIAS

Banco del Estado. (2012a). *Informe de Rendición de Cuentas 2012* (p. 145). Quito.

Banco del Estado. (2012b). Historia. Retrieved December 17, 2013, from http://www.bancoestado.com/index.php/2013-09-20-20-58-22/historia

Banco del Estado. (2012c). Banco del Estado - República del Ecuador. Retrieved December 17, 2013, from http://www.bancoestado.com/

Bassel Comittee on Bankin Supervision. (2006). *Normas de Basilea II* (Segunda Ed., p. 347). Basel: Bank for International Settlements.

BizAgi. (2009). Bizagi Process Modeler User's Guide. Retrieved August 26, 2013, from http://help.bizagi.com/processmodeler/es/

Dirección de Riesgo Operativo del Banco del Estado. (2013). *Plan de Continuidad del Negocio* (p. 160). Quito.

International Standard Organization. (2013a). ISO 27001 - Information security management. Retrieved from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Standard Organization. (2013b). NTC ISO/IEC 27001. Suiza.

International Standard Organization. (2013c). NTC ISO/IEC 15504. Suiza.

ISACA. (2013). *Enabling Processes*. (ISACA, Ed.) (Quinta Edi., p. 230). Illinois.

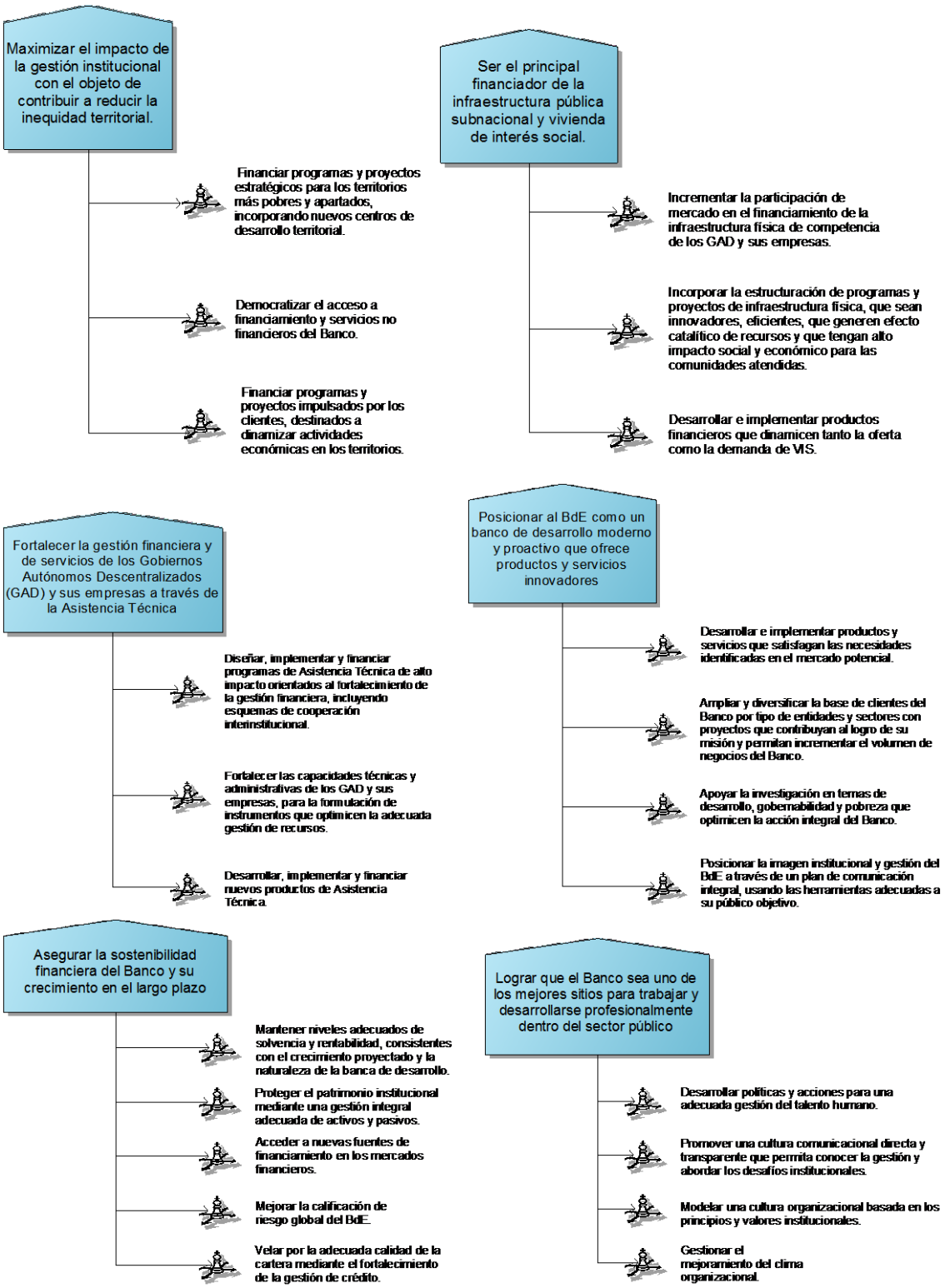
Software AG. (2013). ARIS PLATFORM. Munich: Software AG. Retrieved from www.softwareag.com

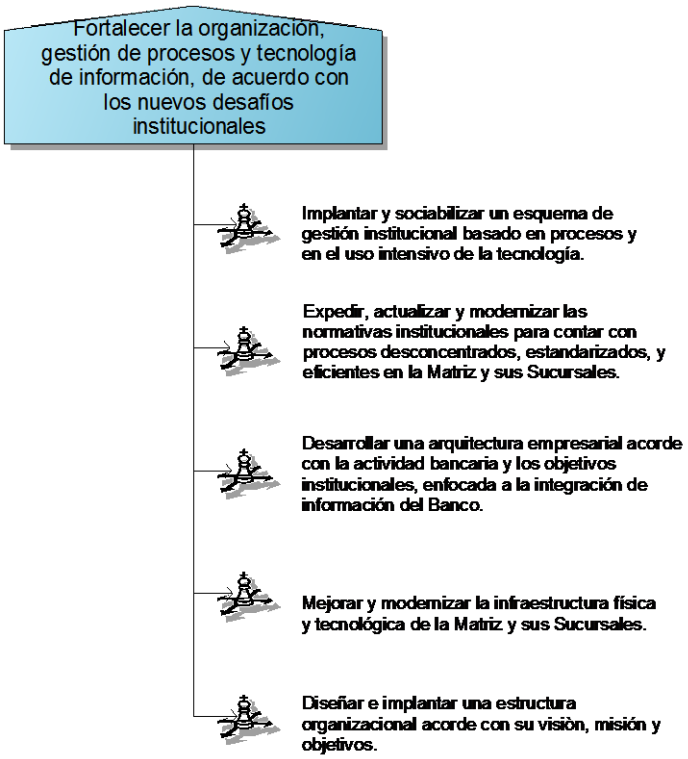
Superintendencia de Bancos y Seguros del Ecuador. Norma Técnica de Gestión del Riesgo Operativo (2005).

Secretaría Nacional de la Administración Pública. Norma Técnica de Administración por Procesos (2013).

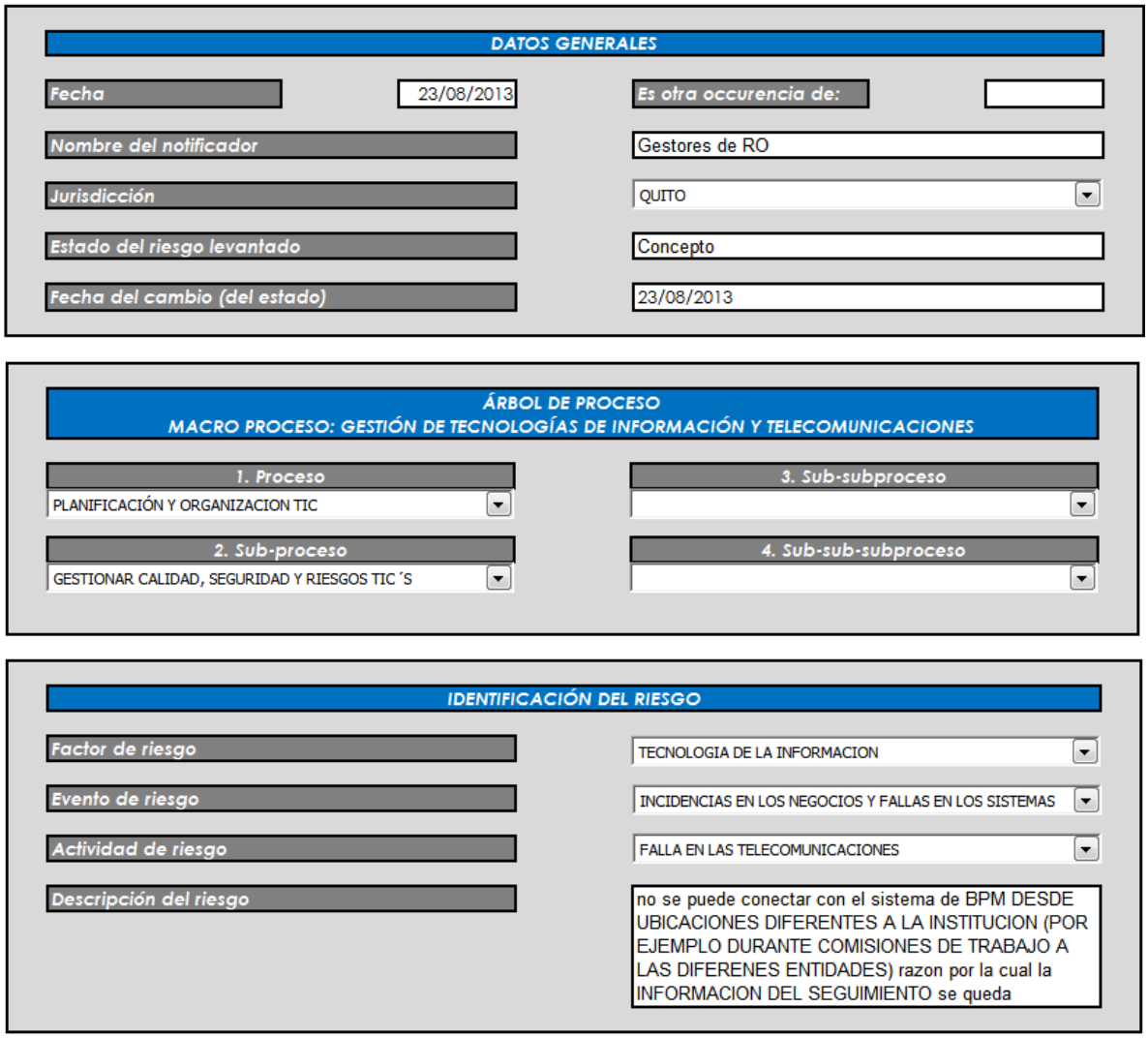
ANEXOS

ANEXO A – Objetivos operativos de menor nivel




Fortalecer la organización, gestión de procesos y tecnología de información, de acuerdo con los nuevos desafíos institucionales
Implantar y sociabilizar un esquema de gestión institucional basado en procesos y en el uso intensivo de la tecnología.
Expedir, actualizar y modernizar las normativas institucionales para contar con procesos desconcentrados, estandarizados, y eficientes en la Matriz y sus Sucursales.
Desarrollar una arquitectura empresarial acorde con la actividad bancaria y los objetivos institucionales, enfocada a la integración de información del Banco.
Mejorar y modernizar la infraestructura física y tecnológica de la Matriz y sus Sucursales.
Diseñar e implantar una estructura organizacional acorde con su visiòn, misión y objetivos.

ANEXO B – Herramienta para el levantamiento de riesgos



DATOS GENERALES

Fecha	23/08/2013	Es otra occurencia de:	
Nombre del notificador		Gestores de RO	
Jurisdicción		QUITO	
Estado del riesgo levantado		Concepto	
Fecha del cambio (del estado)		23/08/2013	

ÁRBOL DE PROCESO
MACRO PROCESO: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y TELECOMUNICACIONES

1. Proceso: PLANIFICACIÓN Y ORGANIZACION TIC	3. Sub-subproceso:
2. Sub-proceso: GESTIONAR CALIDAD, SEGURIDAD Y RIESGOS TIC ´S	4. Sub-sub-subproceso:

IDENTIFICACIÓN DEL RIESGO

Factor de riesgo	TECNOLOGIA DE LA INFORMACION
Evento de riesgo	INCIDENCIAS EN LOS NEGOCIOS Y FALLAS EN LOS SISTEMAS
Actividad de riesgo	FALLA EN LAS TELECOMUNICACIONES
Descripción del riesgo	no se puede conectar con el sistema de BPM DESDE UBICACIONES DIFERENTES A LA INSTITUCION (POR EJEMPLO DURANTE COMISIONES DE TRABAJO A LAS DIFERENES ENTIDADES) razon por la cual la INFORMACION DEL SEGUIMIENTO se queda

ANEXO C Tabla de correspondencias entre SGSI, SGC y SGA

ISO 27001:2013	ISO 9001:2008	IS0 14001:2004
0 Introducción 0.1 Generalidades 0.2 Enfoque a procesos 0.3 Compatibilidad con otros sistemas	0 Introducción 0.1 Generalidades 0.2 Enfoque a procesos 0.3 Relación con ISO 9004 0.4 Compatibilidad con otros sistemas de gestión	0 Introducción
1 Alcance 1.1 General 1.2 Aplicación	1 Alcance 1.1 General 1.2 Aplicación	1 Alcance 1.1 General 1.2 Aplicación
2 Referencias normativas	2 Referencias normativas	2 Referencias normativas
3 Términos y definiciones	3 Términos y definiciones	3 Términos y definiciones
4 Sistema de Gestión de Seguridad de la Información 4.1 Requerimientos generales 4.2 Establecer y manejar el SGSI 4.2.1 Establecer el SGSI 4.2.2 Implementar y operar el SGSI 4.2.3 Monitorear y evaluar el SGSI 4.2.4 Mantener y mejorar el SGSI 4.3 Requerimientos de documentación 4.3.1 Generalidades 4.3.2 Control de documentos 4.3.3 Control de registros	4 Sistema de Gestión de Seguridad de la Información 4.1 Requerimientos generales 8.2.3 Seguimiento y medición de los procesos 8.2.4 Seguimiento y medición del producto 4.2 Requerimientos de documentación 4.2.1 Generalidades 4.2.2 Manual de Calidad 4.2.3 Control de documentos 4.2.4 Control de registros	4 Sistema de Gestión de Seguridad de la Información 4.1 Requerimientos generales 4.3 Implementación y operación 4.5.1 Seguimiento y medición 4.4.5 Control de documentos 4.5.4 Control de registros
5 Compromiso de la alta dirección 5.1 Política de seguridad de la información 5.2 Gestión de los recursos 5.2.1 Provisión de recursos 5.2.2 Capacitación, conocimiento y capacidad	5 Responsabilidad de la dirección 5.1 Compromiso de la dirección 5.2 Enfoque al cliente 5.3 Política de calidad 5.4 Planificación 5.5 Responsabilidad, autoridad y comunicación 6 Gestión de los recursos 6.1 Provisión de recursos 6.2 Recursos humanos 6.3 Infraestructura 6.4 Ambiente de trabajo	4.2 Planificación 4.3 Política ambiental 4.4.1 Recursos, funciones, responsabilidad y autoridad 4.4.2 Competencia, formación y toma de conciencia
6 Auditoría interna	8.2.2 Auditoría interna	4.5.5 Auditoría interna

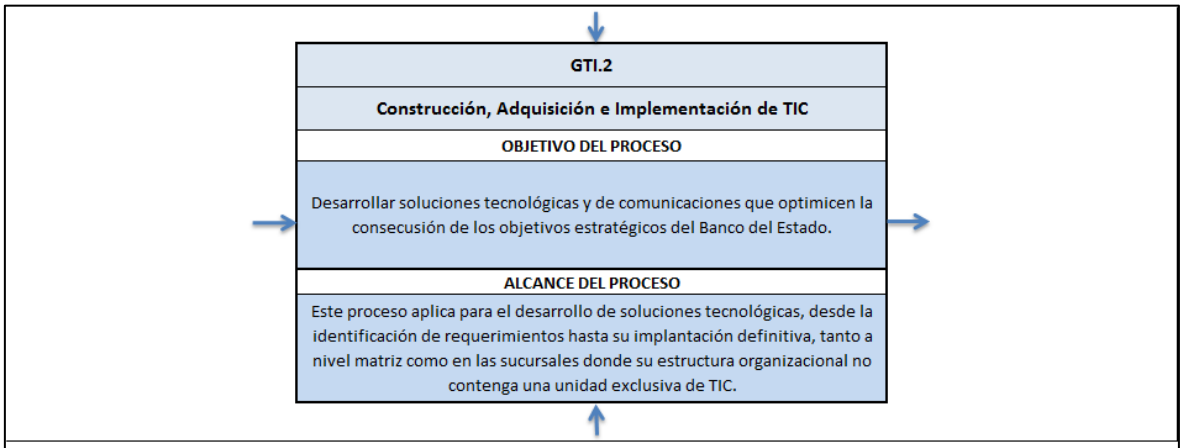
ISO 27001:2013	ISO 9001:2008	IS0 14001:2004
7 Revisión por la dirección 7.1 Generalidades 7.2 Información para la revisión 7.3 Resultados de la revisión	5.6 Revisión por la dirección 5.6.1 Generalidades 5.6.2 Información para la revisión 5.6.3 Resultados de la revisión	4.6 Revisión por la dirección
8 Mejoramiento del SGSI 8.1 Mejoramiento continuo 8.2 Acción correctiva 8.3 Acción preventiva	8.5 Mejoramiento del SGSI 8.5.1 Mejoramiento continuo 8.5.2 Acción correctiva 8.5.3 Acción preventiva	4.5.3 Investigación de incidentes, no conformidades y acciones correctivas

ANEXO D – Hojas de Caracterización del proceso

GTI.1
Planificación y Organización de TIC
OBJETIVO DEL PROCESO
Diseñar las directrices estratégicas de la Gestión de las Tecnologías de Información y Comunicación para el el cumplimiento del Plan Estratégico del Banco del Estado.
ALCANCE DEL PROCESO
Este proceso aplica a la elaboración del Plan Estratégico de la Gestión de las Tecnologías de Información y Comunicación tanto a nivel matriz como a nivel de sucursales. Inicia desde el análisis del Plan Estratégico del Banco del Estado, hasta la Socialización del Plan Estratégico de la Gestión de las Tecnologías de Información y Comunicación.

ENTRADAS	PROVEEDORES INTERNOS (PROCESO DE REFERENCIA)	SALIDAS	CLIENTES INTERNOS (PROCESO DE REFERENCIA)
Plan Estratégico del Banco del Estado	GPL.2.1 Elaboración y Seguimiento del Plan Estratégico Institucional	Plan Estratégico de la GIN	GTI.2 Construcción, Adquisición e Implementación de TIC, GTI.3 Entrega de servicio y soporte técnico para las TIC, GTI.4. Monitoreo y evaluación de TIC
Información de desempeño	GTI.4. Monitoreo y evaluación de TIC	Planificación Operativa de la GIN	GTI.2 Construcción, Adquisición e Implementación de TIC, GTI.3 Entrega de servicio y soporte técnico para las TIC, GTI.4. Monitoreo y evaluación de TIC
Directrices Estratégicas	GGE - DIRECCIONAMIENTO ESTRATÉGICO	Acuerdos de Servicio (SLA)	GTI.2 Construcción, Adquisición e Implementación de TIC, GTI.3 Entrega de servicio y soporte técnico para las TIC, GTI.4. Monitoreo y evaluación de TIC
		Plan de Seguridad Informática	GTI.2 Construcción, Adquisición e Implementación de TIC, GTI.3 Entrega de servicio y soporte técnico para las TIC, GTI.4. Monitoreo y evaluación de TIC
ENTRADAS	**PROVEEDORES EXTERNOS**	**SALIDAS**	**CLIENTES EXTERNOS**

CONTROLES	PROCESO DE REFERENCIA	RECURSOS	PROCESO DE REFERENCIA
Información de retroalimentación del Sistema de Indicadores de Gestión	GTI.4. Monitoreo y evaluación de TIC	HUMANOS	GTH - GESTIÓN DEL TALENTO HUMANO
Manual de Políticas de Seguridad Informática	Interno	TECNOLÓGICOS	GTI: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
		MATERIALES	GBS - GESTIÓN DE BIENES Y SERVICIOS
		FINANCIEROS	GOP - GESTIÓN DE OPERACIONES
CONTROLES	**PROVEEDORES EXTERNOS**	**RECURSOS**	**PROVEEDORES EXTERNOS**
Normas de Contraloría General del Estado, Acuerdo CG-039	Contraloría General del Estado		
Gestión de Riesgo Operativo de la Junta Bancaria, Resolución JB-834	Junta Bancaria		
COBIT 5.0	ISACA		



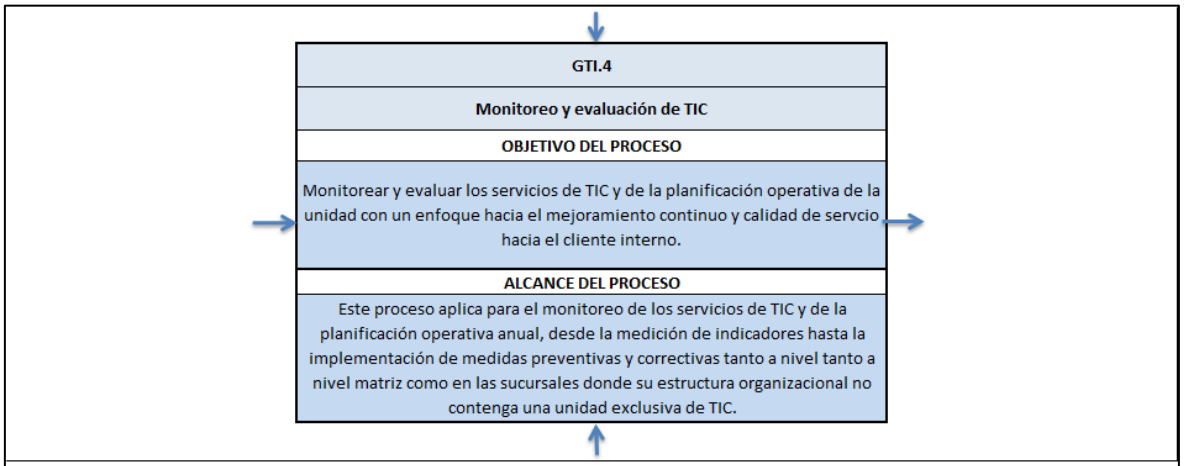
ENTRADAS	PROVEEDORES INTERNOS (PROCESO DE REFERENCIA)	SALIDAS	CLIENTES INTERNOS (PROCESO DE REFERENCIA)
Necesidad de Implantación de necesidades tecnológicas	Unidades del Banco, GDC.3 Implementación de Procesos	Soluciones Tecnológicas implementadas	Unidades del Banco
ENTRADAS	**PROVEEDORES EXTERNOS**	**SALIDAS**	**CLIENTES EXTERNOS**

CONTROLES	PROCESO DE REFERENCIA	RECURSOS	PROCESO DE REFERENCIA
Plan Estratégico de la GIN	GTI.1 Planificación y Organización de TIC	HUMANOS	GTH - GESTIÓN DEL TALENTO HUMANO
Planificación Operativa de la GIN	GTI.1 Planificación y Organización de TIC	TECNOLÓGICOS	GTI: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
Acuerdos de Servicio (SLA)	GTI.1 Planificación y Organización de TIC	MATERIALES	GBS - GESTIÓN DE BIENES Y SERVICIOS
Plan de Seguridad Informática	GTI.1 Planificación y Organización de TIC	FINANCIEROS	GOP - GESTIÓN DE OPERACIONES
Directrices Estratégicas	GGE - DIRECCIONAMIENTO ESTRATÉGICO		
Manual de Políticas de Seguridad Informática	Interno		
CONTROLES	**PROVEEDORES EXTERNOS**	**RECURSOS**	**PROVEEDORES EXTERNOS**
Normas de Contraloría General del Estado, Acuerdo CG-039	Contraloría General del Estado		
Gestión de Riesgo Operativo de la Junta Bancaria, Resolución JB-834	Junta Bancaria		
Gobierno por Resultados	Presidencia de la República		
COBIT 5.0	ISACA		

GTI.3
Entrega de servicio y soporte técnico para las TIC
OBJETIVO DEL PROCESO
Entregar un servicio y soporte técnico de calidad para mantener la infraestructura tecnológica y aplicativos tecnológicos de la institución garantizando su operación permanente con un enfoque de apoyo hacia la consecusión de los objetivos estratégicos
ALCANCE DEL PROCESO
Este proceso aplica desde el monitoreo de las operaciones de los servicios de TIC, hasta la implementación de las seguridades, tanto a nivel tanto a nivel matriz como en las sucursales donde su estructura organizacional no contenga una unidad exclusiva de TIC.

ENTRADAS	PROVEEDORES INTERNOS (PROCESO DE REFERENCIA)	SALIDAS	CLIENTES INTERNOS (PROCESO DE REFERENCIA)
Requerimientos de soporte tecnológico	Unidades del Banco	Servicios de tecnologías de información y comunicación operativos	Unidades del Banco
Acuerdos de Servicio (SLA)	GTI.1 Planificación y Organización de TIC		
ENTRADAS	**PROVEEDORES EXTERNOS**	**SALIDAS**	**CLIENTES EXTERNOS**

CONTROLES	PROCESO DE REFERENCIA	RECURSOS	PROCESO DE REFERENCIA
Plan Estratégico de la GIN	GTI.1 Planificación y Organización de TIC	HUMANOS	GTH - GESTIÓN DEL TALENTO HUMANO
Planificación Operativa de la GIN	GTI.1 Planificación y Organización de TIC	TECNOLÓGICOS	GTI: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
Plan de Seguridad Informática	GTI.1 Planificación y Organización de TIC	MATERIALES	GBS - GESTIÓN DE BIENES Y SERVICIOS
Directrices Estratégicas	GGE - DIRECCIONAMIENTO ESTRATÉGICO	FINANCIEROS	GOP - GESTIÓN DE OPERACIONES
Manual de Políticas de Seguridad Informática	Interno		
CONTROLES	**PROVEEDORES EXTERNOS**	**RECURSOS**	**PROVEEDORES EXTERNOS**
Normas de Contraloría General del Estado, Acuerdo CG-039	Contraloría General del Estado		
Gestión de Riesgo Operativo de la Junta Bancaria, Resolución JB-834	Junta Bancaria		
Gobierno por Resultados	Presidencia de la República		
COBIT 5.0	ISACA		



ENTRADAS	PROVEEDORES INTERNOS (PROCESO DE REFERENCIA)	SALIDAS	CLIENTES INTERNOS (PROCESO DE REFERENCIA)
Planificación Operativa de la GIN	GTI.1 Planificación y Organización de TIC	Información de desempeño	GTI.1 Planificación y Organización de TIC
Acuerdos de Servicio (SLA)	GTI.1 Planificación y Organización de TIC		
ENTRADAS	**PROVEEDORES EXTERNOS**	**SALIDAS**	**CLIENTES EXTERNOS**

CONTROLES	PROCESO DE REFERENCIA	RECURSOS	PROCESO DE REFERENCIA
Plan Estratégico del Banco del Estado	GPL.2.1 Elaboración y Seguimiento del Plan Estratégico Institucional	HUMANOS	GTH - GESTIÓN DEL TALENTO HUMANO
Directrices Estratégicas	GGE - DIRECCIONAMIENTO ESTRATÉGICO	TECNOLÓGICOS	GTI: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
		MATERIALES	GBS - GESTIÓN DE BIENES Y SERVICIOS
		FINANCIEROS	GOP - GESTIÓN DE OPERACIONES
CONTROLES	**PROVEEDORES EXTERNOS**	**RECURSOS**	**PROVEEDORES EXTERNOS**
Normas de Contraloría General del Estado, Acuerdo CG-039	Contraloría General del Estado		
Gestión de Riesgo Operativo de la Junta Bancaria, Resolución JB-834	Junta Bancaria		
COBIT 5.0	ISACA		

ANEXO E Descripción de actividades

GTI.1.1 DISEÑO DE LA ESTRATEGIA DE TIC

ACTIVIDAD	DESCRIPCIÓN
Analizar el Plan Estratégico del Banco del Estado y/o información de retroalimentación	Cada año, la Gerencia de Planificación debe remitir el Plan estratégico del Banco del Estado a la Gerencia de Tecnologías de Información y Comunicación, para su posterior estudio y análisis. En el caso de la información proveniente de los procesos de Monitoreo y Evaluación, se procederá a la aplicación de este proceso cuando el resultado de esta, arroje una necesidad de actualizar el Plan Estratégico Operativo de la GIN. Esta decisión la deberá tomar el responsable del proceso de Monitoreo y Evaluación en conjunto con las autoridades del área.
Analizar procesos, normativa y requerimientos de negocio relacionados a TIC	Para la consecución de esta actividad, es necesario identificar la situación actual de procesos e infraestructura tecnológica, marco legal vigente y requerimientos de sistemas del Banco del Estado, para su traslado al Plan Estratégico de TIC.
Plantear los objetivos estratégicos y operativos alineados al Plan Estratégico del Banco	Cada uno de los objetivos propuestos, deberán estar alineados a los Objetivos Estratégicos del Banco del Estado, además que deben guardar una relación causa efecto, para establecer las prioridades. Adicionalmente, es necesario que en esta fase, se planteen los indicadores de gestión con sus respectivas metas, como insumos para el proceso de Monitoreo y Evaluación. Los objetivos deben estar enfocados, al menos, en los siguientes puntos: • Gestión de la Arquitectura empresarial • Gestión de Innovación • Gestión del Talento Humano de TIC. • Gestión de las Relaciones • Gestión con los Proveedores • Gestión de la Calidad • Gestión del Riesgo • Objetivos de Control Interno
Elaborar documento de Acuerdos de Servicios y SLA	El documento de Acuerdos de Servicio, se lo debe elaborar en formato GTI.R1
Elaborar los proyectos e indicadores de gestión asociados a los objetivos operativos	Los proyectos de que corresponden a cada objetivo, deben identificar claramente sus actividades, con los respectivos responsables. Se recomienda el uso de herramientas como MS – Proyect. Para los proyectos se debe utilizar el formato GTI.R2
Elaborar Presupuesto y Plan Anual de Compras de la GIN	Cada uno de los proyectos debe tener el sustento económico para su presupuestación incluida la consolidación del presupuesto de seguridad informática. El resumen de este se lo debe elaborar en el formato GTI.R2
Revisar Plan estratégico, Presupuesto y Plan Anual de Compras de la GIN	Con todos los productos, como son, Plan Estratégico, Acuerdos de Servicio, y Planificación Operativa Anual representada a través de los proyectos, se realiza la respectiva revisión para corrección de posibles errores.
Validar plan Estratégico de la GIN	Cuando los el Plan Estratégico, Acuerdos de Servicio y Planificación Operativa Anual hayan pasado por el filtro de los Directores de Área, se procede a la firma autorizada por parte del responsable del área de Tecnologías de Información y Comunicación para su validación previa a su aprobación por parte del Comité de Tecnologías de Información y Comunicación.

ACTIVIDAD	DESCRIPCIÓN
Realizar aprobación de primera instancia del Plan Estratégico de GIN	El del Comité de Tecnologías de Información y Comunicación se reúne para discutir la aprobación del Plan Estratégico Operativo de la GIN y viabilizar su aprobación por parte de la Gerencia General.
Aprobar Plan Estratégico de la GIN	La Gerencia General da la aprobación final del Plan Estratégico de la GIN.
Consolidar el PAC de la Subgerencia	La Subgerencia de Gestión Institucional consolida el PAC de las unidades a su cargo.
Recibir documento de aprobación del POA	Una vez que el Plan Estratégico de la unidad de TIC, haya pasado por el filtro de planificación, se anexa al documento la certificación del POA para la obtención de recursos financieros.
Remitir Plan Estratégico y Aprobación del POA a la G.O.	Se envía el documento de aprobación del POA a la Gerencia de Operaciones para la obtención de Recursos Financieros y obtención de la Certificación Presupuestaria.
Socializar Plan Estratégico internamente	Una vez que ya se hayan comprometido los recursos, Se debe socializar el plan a todos los integrantes del área para su conocimiento.

GTI.1.2 PLANIFICACIÓN DE LAS SEGURIDADES DE TIC

ACTIVIDAD	DESCRIPCIÓN
Estudiar los proyectos de la GIN	Una vez que el direccionamiento estratégico de la GIN se encuentre claramente definido, se analizan los proyectos y los informes de auditoría para el diseño y/o actualización del Sistema de Gestión de Seguridad Informática.
Documentar y/o actualizar los requisitos de sistema de gestión de seguridad informática	El Sistema de Gestión de Seguridad Informática debe establecer claramente los requisitos de documentación del Sistema de Gestión de Seguridad Informática seleccionado, con su respectivo manual y su plan de auditorías internas y externas para el cumplimiento de los requisitos.
Generar el plan de riesgos de seguridad informática	El plan de riesgos debe contemplar todos los posibles escenarios que podrían vulnerar las seguridades informáticas, así como los planes de mitigación de los mismos.
Generar proyectos de seguridad informática	Los proyectos de que corresponden a cada objetivo de seguridad, deben identificar claramente sus actividades, con los respectivos responsables. Se recomienda el uso de herramientas como MS – Proyect. Para los proyectos se debe utilizar el formato GTI.R2
Elaborar el presupuesto de los proyectos de seguridad informática	Cada uno de los proyectos debe tener el sustento económico para su presupuestación. El resumen de este se lo debe elaborar en el formato GTI.R2

GTI.2.1 IDENTIFICACIÓN DE REQUERIMENTOS TECNOLÓGICOS

ACTIVIDAD	DESCRIPCIÓN
Remitir requerimiento con especificación tecnológica preliminar	El requerimiento proveniente de las unidades funcionales debe contener claramente las necesidades tecnológicas de la unidad. Aquellos requerimientos que vengan de la Dirección de Gestión de la Calidad deben ser recibidos a través del Manual de Especificaciones Funcionales en formato GDC.R11. Cuando un requerimiento tecnológico afecte la cadena de valor o sea el producto de una optimización de procesos, se lo debe canalizar a través de la Dirección de Gestión de Calidad, caso contrario, podrá ser atendido directamente a través de la Gerencia Informática. Las especificaciones funcionales se refieren a mejoramientos en sistemas de información, mientras que las especificaciones técnicas se refieren a mejoramientos en la infraestructura tecnológica.
Evaluar la factibilidad técnica del requerimiento tecnológico	La factibilidad para generar una solución tecnológica debe alinearse al Plan Estratégico de la Institución.
Elaborar informe de no factibilidad	El informe técnico redacta con el sustento técnico de todos los elementos anteriores, y se difunde a través del sistema de gestión documental institucional. Se utiliza el formato GTI.R4.
Elaborar las especificaciones tecnológicas	Las especificaciones funcionales detalladas se las debe elaborar en formato GTI.R3.
Revisar y priorizar especificaciones tecnológicas	La priorización de las especificaciones funcionales preliminares se las debe realizar en función de las necesidades más importantes de la organización.
Aprobar especificaciones tecnológicas	Finalmente el dueño del proceso debe aprobar la especificación tecnológica definitiva.
Realizar estudio de mercado	Una vez que el requerimiento tecnológico sea claramente entendido, se debe realizar un estudio de mercado para evaluar la disponibilidad en herramientas desarrolladas o en opciones para desarrollo con la finalidad de entender los aspectos técnicos y presupuestarios de la mencionada solución.
Realizar anteproyecto de propuesta de solución con especificaciones técnicas	El anteproyecto debe contener el diagnóstico preliminar, estudio de mercado, análisis de factibilidad técnica, operativa, legal y definición de especificaciones tecnológicas priorizadas, con sus respectivas conclusiones y recomendaciones. Se debe utilizar el formato GTI.R5, el cual incluye el análisis de viabilidad para el siguiente paso. En el caso de desarrollo de soluciones dentro del BPMS, se deberá establecer claramente las especificaciones de integración.
Establecer el análisis de viabilidad	El análisis de viabilidad para generar la solución tecnológica, debe visibilizarse desde el punto de vista económico financiero.
Validar anteproyecto con propuesta de solución	Una vez que el proyecto cumpla con los requisitos de alineamiento hacia la Planificación Estratégica, especificaciones funcionales priorizadas, estudio de mercado favorable, análisis de factibilidad técnica, operativa, legal y financiero viable, se procede a la validación del anteproyecto previa a su aprobación por parte de la Gerencia Informática.

GTI.2.2: GESTIÓN DE PROYECTOS DE TIC

ACTIVIDAD	DESCRIPCIÓN
Convertir requerimientos en un proyecto	Con base a identificación de requerimientos tecnológicos, se realiza un proyecto, el cual consiste en generar la idea que da origen a un proyecto de implementación de la solución tecnológica. El proyecto se lo debe elaborar en formato GTI.R6, el cual establece las siguientes la gestión en las siguientes áreas de conocimiento: • Gestión de Integración • Gestión del Alcance • Gestión del Tiempo • Gestión de Costos • Gestión de Calidad • Gestión de Recursos Humanos • Gestión de las Comunicaciones • Gestión de Riesgo • Gestión de las Adquisiciones • Gestión de Interesados
Revisar proyecto	El proyecto es revisado a fin de validar que todo se encuentre alineado a la planificación operativa de la institución.
Definir roles, cronograma y recursos	Una vez que se ha autorizado el inicio del proyecto, se plantea el cronograma y recursos necesarios para la implementación de la solución tecnológica. En caso de que se requiera, recursos financieros, humanos o materiales, se procederá a hacer la respectiva solicitud a la unidad administrativa correspondiente.
Asignar los recursos disponibles previos a la ejecución del proyecto definitivo	Una vez que los recursos se encuentran disponibles, en esta etapa se debe asignar los recursos para su utilización.
Realizar el cierre del proyecto	En esta etapa se encuentra toda la elaboración de entregables, incluyendo el reporte final del proyecto aceptado.

GTI.2.3: CONSTRUCCIÓN E IMPLANTACIÓN DE LA SOLUCIÓN TECNOLÓGICA

ACTIVIDAD	DESCRIPCIÓN
Realizar el diseño detallado de la arquitectura de la solución	La arquitectura detallada de la solución corresponde al diseño tecnológico detallado de las especificaciones técnicas elaboradas conjuntamente con el anteproyecto. En esta etapa es necesario detallar los componentes de hardware y/o software que formará parte de la solución tecnológica de forma detallada.
Revisar el diseño detallado de los componentes	La revisión se enfoca en establecer si la propuesta cumple con la arquitectura tecnológica del Banco del Estado.
Aprobar diseño detallado de la arquitectura de la solución	Si la propuesta de solución se alinea con la infraestructura tecnológica del Banco del Estado, se procede a su aprobación.
Evaluar alcance de la solución tecnológica	Para la generación de un curso de acción adecuado, se procede a definir si se trata de un desarrollo interno o de una solución tecnológica que se genere un proceso de contratación.

ACTIVIDAD	DESCRIPCIÓN
Construir la solución tecnológica	La construcción de la solución tecnológica se ejecuta de acuerdo al diseño detallado definido en la arquitectura de la solución, sea este un desarrollo interno, externo o mejoramiento de la infraestructura tecnológica.
Preparar solicitud de cambios en la configuración	Para el inicio de pruebas, es necesario modificar la configuración actual, tanto de los servicios de TIC, como de los ítems del hardware, para lo cual, se requiere de la respectiva solicitud de cambio en formato GTI.R7
Realizar pruebas y control de calidad	El control de calidad debe enfocarse a las pruebas de la solución tecnológica dentro de escenarios controlados que permitan demostrar la funcionalidad total del sistema.
Realizar ajustes a la solución	Si la solución no cumple con las pruebas de calidad dentro de los escenarios controlados, se procede a hacer los respectivos cambios.
Elaborar los manuales de usuario	Una vez que la solución haya pasado las pruebas de calidad, se emiten los manuales de usuario de la solución tecnológica, a fin de garantizar su buen uso.
Ejecutar la capacitación para el uso de la solución tecnológica	Las capacitaciones de deben impartir a los usuarios directos de la solución tecnológica. En caso de que el universo sea muy grande, se seleccionará una muestra representativa y se obligará la réplica por parte de los beneficiarios de la capacitación hacia los compañeros.
Implantar la solución tecnológica en ambiente de producción	Finalmente la solución se pone a disposición de los beneficiarios.
Actualizar documentación en el repositorio	Cuando la solución tecnológica ha sido implantada exitosamente, se procede a actualizar el versionamiento vigente, dentro del repositorio de Tecnologías de Información y Comunicación.

GTI.2.4: GESTIÓN DE DISPONIBILIDAD Y CAPACIDAD

ACTIVIDAD	DESCRIPCIÓN
Monitorear los ítems de servicio planificados de las TIC	Cada inicio de periodo, la Gerencia Informática debe planificar los ítems de servicio que serán monitoreados en función de su criticidad para la continuidad del negocio. Este monitoreo se realizará de forma de regular de tal manera que permita identificar novedades antes de que estas ocurran.
Generar reporte de crecimiento del uso de la capacidad	La generación del reporte consiste en la elaboración de estadísticas que permitan evaluar el comportamiento histórico de la utilización de la capacidad en el tiempo. Se recomienda la presentación de gráficas de barras o dispersión, las cuales permitan hacer proyecciones estadísticas.
Comparar reporte con umbrales definidos en la planificación operativa de la GIN	Una vez que se ha generado el reporte, es necesaria la elaboración de un análisis comparativo que permita definir si la situación actual de uso de la capacidad, se encuentra dentro de los umbrales definidos dentro del manual de políticas de uso de la capacidad establecido por la Gerencia Informática.
Evaluar impactos de la situación en la organización	En caso de, de que se identifique un ítem con un valor de capacidad fuera de los umbrales definidos en el manual de políticas de capacidad, se debe hacer un análisis documentado en el que se establezcan las consecuencias que podrían afectar al Banco del Estado, en caso de no tomar medidas inmediatas. Este análisis deberá ser almacenado dentro del repositorio documental de la Gerencia Informática.

ACTIVIDAD	DESCRIPCIÓN
Planificar las acciones preventivas	La planificación acciones preventivas se lo deberá documentar en formato GTI.R8.
Revisar plan de acción	La revisión del plan de acciones preventivas debe enfocarse desde el punto de vista de viabilidad técnica, operativa legal y económica para dar paso a la generación de solicitud de cambio.
Generar solicitud de cambio	La solicitud de generación de solicitud de cambio se las debe realizar en formato GTI.R7.

GTI.2.5: GESTIÓN DE LA CONFIGURACIÓN

ACTIVIDAD	DESCRIPCIÓN
Elaborar solicitud de cambio	La solicitud de cambio remitida por la unidad requirente debe contener los elementos detallados que son necesarios para el cambio en la configuración de las tecnologías de información y comunicación. Toda solicitud de cambio debe generarse por escrito en formato GTI.R7.
Evaluar solicitud de cambio	La solicitud de cambio debe ser evaluada en relación al presupuesto, y alineamiento estratégico del Banco del Estado.
Informar no factibilidad de cambio	Si la solicitud de cambio, no es aplicable en relación al presupuesto, y alineamiento estratégico del Banco del Estado, se procede a su desaprobación, para lo cual se requiere la respectiva comunicación al originador del requerimiento con las debidas justificaciones técnicas.
Generar solicitud de cambio	Si el cambio es autorizado, se actualiza técnicamente la solicitud de generación de solicitud de cambio, la cual se la debe elaborar en formato GTI.R7.
Identificar la afectación de los cambios a ejecutar	Con la solicitud de cambio, se deben identificar los cambios requeridos tanto en los servicios como en los ítems de TIC, que se deben realizar a nivel detallado.
Comparar los cambios propuestos con la línea de base	La línea de base de las configuraciones, se la puede encontrar en el repositorio de configuraciones del Banco del Estado, para lo cual, es necesario extraer los documentos relacionados a la solicitud de cambio, y compararlos con los requerimientos.
Actualizar detalles de cambios en la configuración en la solicitud de cambio	Una vez que se ha comparado los requerimientos con la línea de base, se realiza las actualizaciones necesarias en la solicitud de cambio desde la perspectiva técnica informática.
Revisar propuesta de cambios	La propuesta debe ser revisada para evaluar la viabilidad técnica, legal y económica de la propuesta de cambio.
Validar la propuesta de cambios en la configuración	Con la solicitud de cambio depurada, la autoridad responsable revisa la propuesta, para su posterior aprobación por parte de la Gerencia Informática.
Aprobar propuesta de cambios en la configuración	Con la aprobación por parte de la Gerencia Informática, se oficializa la autorización para la ejecución del cambio.
Realizar cambios de la configuración en ambiente de pruebas	Los cambios en la configuración se hacen en ambiente de pruebas, sin afectar la funcionalidad de configuración de los usuarios, hasta que no se haya efectuado el control de calidad con resultados totalmente favorables.

ACTIVIDAD	DESCRIPCIÓN
Realizar control de calidad de los cambios	El control de calidad debe enfocarse a las pruebas de cambios en la configuración dentro de escenarios controlados que permitan demostrar la funcionalidad de la modificación.
Implantar cambios en ambiente de producción	Los cambios en la configuración se ponen a disposición de los usuarios.
Actualizar documentación en el repositorio	Cuando los cambios han sido exitosos, se procede a actualizar el versionamiento de la configuración vigente, dentro del repositorio de Tecnologías de Información y Comunicación.
Realizar el rollback de la configuración	En caso de que la implantación en ambiente de producción, genere fallas, se debe recurrir a la configuración anterior de inmediato para no afectar la funcionalidad de los servicios de TIC.
Notificar a los usuarios	Se notifica a los usuarios que el proceso ha culminado con éxito, fundamentalmente en el cambio en la configuración solicitado y la documentación actualizada.

GTI.2.6: ADMINISTRACIÓN DEL CAMBIO DE LOS SISTEMAS DE INFORMACIÓN

ACTIVIDAD	DESCRIPCIÓN
Elaborar solicitud de cambio del sistema de información	La solicitud de cambio de los sistemas de información debe realizarse de manera detallada, de tal forma que sea entendida por los técnicos de la Gerencia Informática. Este pedido se lo debe realizar en formato GTI.R7. Para pasar al siguiente paso se deben acumular las un número adecuado de solicitudes para su evaluación en conjunto.
Evaluar solicitud de cambio en función de la matriz de emergencias	Cada solicitud de cambios que ingrese como requerimiento, debe ser evaluada en función de la matriz de emergencias, para lo cual se debe mantener un plan de actualización de la misma de acuerdo a los requerimientos del Banco del Estado. Para el caso de solicitudes emergentes se procederá directamente con el desarrollo del cambio, sin pasar por ningún nivel de aprobación.
Priorizar requerimientos	En aquellos casos que no sean considerados requerimientos emergentes, es necesario diseñar una matriz de ponderación de factores que permitan identificar aquellos pedidos que requieran ser atendidos antes que otros.
Notificar a la unidad requirente	En caso de que los requerimientos no sean prioritarios para la organización, serán notificados directamente a los representantes funcionales.
Analizar requerimientos priorizados	Con un primer filtro de priorización, El Comité de Cambios analiza los requerimientos para viabilizar su implantación.
Aprobar cambios	Con las conclusiones debidamente documentadas como sustento de las reuniones del Comité de Cambios, se procede a la autorización de los cambios. Las actas serán archivadas como sustento documental.
Desarrollar cambios en ambiente de desarrollo	Los cambios solicitados y aprobados por el Comité de Cambios, son llevados técnicamente a la práctica en ambiente de desarrollo, con la participación activa del representante funcional para la obtención de los resultados deseados.
Realizar pruebas funcionales y control de calidad	Las pruebas y control de calidad, deben enfocarse en el cumplimiento de las funcionalidades solicitadas. En caso de que las pruebas no tengan resultados exitosos, se deberá regresar a la fase de desarrollo hasta que los controles tengan resultados positivos.

ACTIVIDAD	DESCRIPCIÓN
Aprobar cambio	Cuando las pruebas y control de calidad, haya arrojado resultados exitosos, se debe suscribir un acta de aprobación en donde obligatoriamente deben firmar, el representante funcional, el Director de Sistemas de Información y el Técnico responsable del desarrollo del cambio, dejando constancia de que el producto fue desarrollado y recibido a entera satisfacción del requirente.
Elaborar solicitud de cambios en la configuración	En caso de que el cambio solicitado, genere un cambio en la configuración, se debe elaborar la respectiva solicitud de cambio, para generar una modificación en la configuración, la que se enlaza al proceso GTI.2.5 Gestión de la configuración.
Implantar cambio en ambiente de producción	Con base a la configuración apropiada se procede a implantar solución en ambiente de producción.
Ejecutar procedimientos de rollback	En caso de que el cambio genere problemas para su implantación en ambiente de producción, se aplica los procedimientos de rollback, y se regresa al ambiente de desarrollo hasta que el cambio de pueda implantar con éxito.
Actualizar documentos de usuario del sistema	Cuando el cambio solicitado se encuentre en ambiente de producción sin problemas, se procede a la actualización de la documentación de los sistemas de información, los cuales sirven como manuales de usuarios para su utilización por parte de los beneficiarios.
Notificar a los usuarios	Se notifica a los usuarios que el proceso ha culminado con éxito, fundamentalmente en el cambio del sistema solicitado y la documentación actualizada.

GTI.3.1: GESTIÓN DE OPERACIONES

ACTIVIDAD	DESCRIPCIÓN
Desarrollar procedimientos operativos relacionados al soporte y entrega de servicio	Para el desarrollo y mantenimiento de procedimientos operativos es necesario el diseño de un cronograma de actividades de monitoreo de las operaciones de los servicios ofrecidos por el área de TI. Además estos procedimientos deben contemplar la extracción de respaldos de los registros operativos de acuerdo a las estrategias y políticas establecidas.
Revisar procedimientos relacionados a soporte y entrega de servicio	Una vez que los procedimientos operativos se encuentran adecuadamente diseñados, se procede a su revisión en búsqueda de posibles ajustes, que podrían darse en un enfoque hacia el mejoramiento.
Validar procedimientos relacionados a soporte y entrega de servicio	Cuando todos los ajustes se encuentran realizados, se procede a su validación para su aprobación por parte de la Gerencia Informática
Aprobar procedimientos relacionados a soporte y entrega de servicio	Con la firma autorizada de la gerencia informática se oficializa la vigencia de los procedimientos operativos.
Monitorear la infraestructura de TI interna y tercerizada	El monitoreo corresponde a la ejecución de los procedimientos operativos, y debe ser una actividad constante que permita identificar, posibles causas que conlleven a incidentes. Los servicios que deben ser monitoreados son: • LAN

ACTIVIDAD	DESCRIPCIÓN
	• WAN • WIRELESS • INTERNET • INTRANET • ANCHO DE BANDA • LDAP • CORREO • TELEFONÍA IP • VIDEO CONFERENCIA • SPI – SPL • CGWB • IMPRESIÓN • FOTOCOPIADO • BPMN • BDO
Generar reportes de estado de infraestructura y servicios de TI	La generación del reporte consiste en obtención de respaldos de registros (LOGS) que permitan evaluar la operatividad de un servicio informático.
Tomar la acción preventiva pertinente	En caso de detectarse alguna anomalía, se debe tomar la acción preventiva correspondiente. Su documentación se la realizará en formato GTI.R8.
Elaborar documentación con detalle de incidente	El detalle del incidente debe ser documentado en formato GTI.R9

GTI.3.2: ATENCIÓN A PETICIONES, INCIDENTES Y PROBLEMAS DE LAS TIC

ACTIVIDAD	DESCRIPCIÓN
Remitir reporte de incidente o irregularidad	Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, el mismo Centro de Servicios o el soporte técnico. Se recomienda que el reporte del incidente se lo realice en formato GTI.R9, a través del Sistema de Mesas Ayuda GLPI. Si este llega vía telefónica, el responsable de esta actividad deberá realizar el registro en el respectivo formato dentro del sistema.
Clasificar reporte de incidentes	El proceso de clasificación debe implementar, al menos, los siguientes pasos: • **Categorización**: se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su resolución. Se identifican los servicios afectados por el incidente. • **Establecimiento del nivel de prioridad**: dependiendo del impacto y la urgencia se determina, según criterios prestablecidos, un nivel de prioridad. • **Asignación de recursos**: si el **Centro de Servicios** no puede resolver el incidente en primera instancia designara al personal de soporte técnico responsable de su resolución (segundo nivel). • **Monitorización del estado y tiempo de respuesta esperado**: se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al SLA correspondiente y la prioridad.

ACTIVIDAD	DESCRIPCIÓN
Asignar técnico de help desk	Una vez que el registro y clasificación del incidente, se procede a la designación de un técnico para la solución del mismo.
Dar asistencia remota al incidente reportado	La asistencia remota consiste en la búsqueda de una solución al incidente, sin necesidad de acudir al lugar del usuario, por lo que puede ser vía telefónica o vía escritorio remoto.
Dar asistencia presencial al incidente reportado	En caso de que el incidente no se solucione vía asistencia remota, el técnico asignado debe acudir presencialmente para implementar la solución.
Proporcionar solución temporal hasta materializar adquisición	Si la solución requiere disparar una adquisición, se debe dar una solución temporal que permita resolver el incidente hasta materializar la compra de una parte o pieza.
Solicitar adquisición de partes o piezas	Con el requerimiento de compra, se procede a la compra de las partes o piezas.
Resolver el incidente de manera definitiva	Con la parte o pieza adquirida, o simplemente, tras la asistencia presencial al incidente reportado, se examina el incidente con ayuda recomendada de la Base de Conocimientos para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.
Actualizar la base de conocimientos de incidentes	Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las correspondientes bases de datos para que los agentes implicados dispongan de cumplida información sobre el estado del mismo, además de disponer de información que pueda ser replicada para incidentes similares.
Reclasificar incidente	Si el incidente resuelto, se atribuye a diferentes causas y categorizaciones establecidas en la actividad de registro y clasificación, se procede a la reclasificación del mismo para la actualización de su estado.
Confirmar satisfacción del cliente	Cuando el incidente ha sido resuelto, se indaga al requirente, si está conforme con la solución implementada, a través de la medición de su satisfacción del servicio.
Cerrar incidente	Con el caso resuelto, se cierra el incidente y se ordena la información en las respectivas bases de conocimiento.
Identificar el problema para el direccionamiento al técnico	En caso de que no se encuentre una solución al incidente, se procede al análisis de las posibles causas para la reasignación de un técnico especialista. Si la incidencia fuera recurrente y no se encuentra una solución definitiva al mismo se deberá informar igualmente a la Gestión de Problemas para el estudio detallado de las causas subyacentes.
Reclasificar incidente en problema	Si la resolución del incidente se escapa de las posibilidades del Centro de Servicios, se procede a realizar una reclasificación del mismo para categorizarlo como problema. El registro de problemas es, en principio, similar al de los incidentes aunque el énfasis debe hacerse no en los detalles específicos de los incidentes asociados sino más bien en su naturaleza y posible impacto. El registro debe incorporar, entre otras, información sobre: • Los CIs implicados. • Causas del problema. • Síntomas asociados. • Soluciones temporales. • Servicios involucrados. • Niveles de prioridad, urgencia e impacto. • Estado: activo, error conocido, cerrado.

ACTIVIDAD	DESCRIPCIÓN
Reasignar a un técnico especialista	Una vez que el registro y reclasificación del incidente se transformó en problema, se procede a la designación de un técnico especialista para la solución del mismo.
Identificar diagnóstico del error y causa raíz	Los objetivos principales del proceso de análisis y diagnóstico son: • Determinar las causas del problema. • Proporcionar soluciones temporales a la Gestión de Incidencias para minimizar el impacto del problema hasta que se implementen los cambios necesarios que lo resuelvan definitivamente. Es esencial tener en cuenta que no siempre el origen del problema es un error de hardware o software. Es frecuente que el problema esté causado por: • Errores de procedimiento. • Documentación incorrecta. • Falta de coordinación entre diferentes áreas. Es también posible que la causa del problema sea un bug bien conocido de alguna de las aplicaciones utilizadas. Por lo tanto, es conveniente establecer contacto directo con el entorno de desarrollo, en caso de aplicaciones desarrolladas "en la casa", o investigar en Internet información sobre errores conocidos aplicables al problema en cuestión.
Proporcionar una solución temporal hasta la conceptualización de la solución definitiva	El registro de los errores conocidos es de vital importancia para la Gestión de Incidencias, pues debe llevar asociado, siempre que esto sea posible, algún tipo de solución temporal (también llamada workaround) que permita minimizar el impacto de los incidentes asociados.
Generar una solicitud de cambio	La solicitud de cambio de los sistemas de información o de la configuración, debe realizarse de manera detallada, de tal forma que sea entendida por los técnicos de la Gerencia Informática. Este pedido se lo debe realizar en formato GTI.R7.
Actualizar documentación y procedimientos de uso	En caso de que el problema sea atribuido a documentación desactualizada, es necesaria la modificación de la misma para la aplicación de los procedimientos correctamente.
Socializar procedimientos de uso	Con la documentación actualizada, se socializa el uso de la misma a los usuarios.
Cerrar el problema	Antes de dar el problema por resuelto y cambiar su estado a “cerrado” se debe analizar el resultado de la implementación de la RFC elevado a la Gestión de Cambios (PIR). Si los resultados de esta PIR son los deseados y se pueden cerrar todos los incidentes relacionados con este problema, se considera concluido el proceso y se emiten los informes correspondientes. Por último, es indispensable actualizar la Base de Datos de Errores Conocidos (KEDB) para futuras ocasiones. Adicionalmente, en el caso de problemas de carácter grave, todo el proceso se somete a una Revisión de Problemas Graves para prevenir la reaparición del problema.

GTI.3.3: GESTIÓN DE LA CONTINUIDAD

ACTIVIDAD	DESCRIPCIÓN
Definir la estrategia de continuidad	La estrategia de continuidad, debe establecerse en base al levantamiento de riesgos operativos y debe definir fundamentalmente los siguientes aspectos: • Identificación de vulnerabilidades, amenazas y riesgos. • Plan de mitigación de riesgos y corrección de vulnerabilidades • Escenarios (Procedimientos y Plan de Pruebas)
Revisar la estrategia de continuidad	Una vez que la estrategia de continuidad se ha definido, se procede a la revisión previa a la validación final.
Validar la estrategia de continuidad	La validación final se da con la firma de la Gerencia Informática, previa a su aprobación por parte del Comité de TIC.
Aprobar estrategia de continuidad	Con la aprobación del Comité de TIC, se oficializa la vigencia de la estrategia de continuidad para el periodo definido.
Ejecutar pruebas a la estrategia de continuidad	De los tres elementos fundamentales de la estrategia de continuidad, se procede a realizar pruebas reales para garantizar el funcionamiento de los escenarios previstos, vulnerabilidades y plan de mitigación de riesgos ante una posible situación que pueda alterar la continuidad del negocio.
Ejecutar pruebas de funcionamiento de continuidad	Las pruebas de funcionamiento de continuidad consisten verificar que todos los servicios de TIC, se encuentren activos. En caso de que los servicios no se levanten automáticamente, se procede al levantamiento manual, o en su defecto al contacto inmediato con el proveedor de los servicios.
Ejecutar procedimientos definidos en la estrategia de continuidad	En caso de una situación de riesgo se materialice, es necesario seguir los procedimientos establecidos en el plan de contingencia, para garantizar la continuidad del negocio.
Ejecutar procedimientos para volver a la normalidad	Una vez que la situación de riesgo ha sido controlada, es necesario seguir los procedimientos establecidos en el plan de contingencia, para volver a la normalidad, es decir, a la situación previa a la materialización del riesgo identificado.
Actualizar documentación en el repositorio	Una vez que la situación ha vuelto a la normalidad, es necesaria la documentación del evento para garantizar que los eventos ocurridos sirvan de experiencia ante posibles de situación de riesgo similares.

GTI.3.4 GESTIÓN DE LAS SEGURIDADES

ACTIVIDAD	DESCRIPCIÓN
Monitorear las seguridades de los servicios de TIC	El monitoreo de las seguridades de TIC debe enfocarse, al menos en los siguientes aspectos: • Protección de los servicios contra código malicioso. • Identificación de posibles vulnerabilidades en las redes (LAN y WAN) y conectividad. • Seguridad de identidad de usuarios y accesos lógicos. • Seguridad a los accesos físicos de los activos de TI. • Seguridad de documentos sensibles y dispositivos de salida. • Seguridad de la infraestructura de TI.
Documentar el incidente	El detalle del incidente debe ser documentado en formato GTI.R9

ACTIVIDAD	DESCRIPCIÓN
Priorizar las vulnerabilidades de seguridad informática	La priorización de vulnerabilidades, se debe efectuar de acuerdo a la sensibilidad respecto a los objetivos del negocio, desde el punto de vista de continuidad.
Evaluar posibles soluciones ante las vulnerabilidades	La evaluación de las soluciones ante las vulnerabilidades detectadas, se la debe realizar interna y externamente, a fin de mantener el vanguardismo en temas de seguridad informática.
Definir una propuesta de solución a la vulnerabilidad detectada	La solución a la vulnerabilidad, debe considerar todos los aspectos técnicos, económicos y plan de implementación para su aplicación.
Implantar la solución definida en coordinación con los involucrados	La solución se debe implantar inmediatamente para evitar que la vulnerabilidad se transforme en incidente.
Generar documentación de la experiencia	Cuando la implantación ha sido exitosa, se procede a actualizar la base de conocimientos, dentro del repositorio de Tecnologías de Información y Comunicación, para su posible réplica ante situaciones de similares características.
Actualizar el repositorio de experiencias de solución de vulnerabilidades	Durante todo el monitoreo e implementación de las soluciones para mitigación de vulnerabilidades, se debe actualizar la información almacenada en las correspondientes bases de datos para que los agentes implicados dispongan de cumplida información sobre el estado del mismo, además de disponer de información que pueda ser replicada para incidentes similares.
Evaluar impacto en la planificación de seguridades	En caso de que las soluciones implementadas generen un cambio sustancial en la planificación estratégica de las seguridades, es necesaria su actualización y modificación.

GTI.4.1: MONITOREO DE LOS SERVICIOS DE TIC

ACTIVIDAD	DESCRIPCIÓN
Definir metas de niveles de servicio, control interno y requerimientos externos	Con base a los acuerdos de servicio, objetivos de control interno y requerimientos externos, se fijan las metas de cada uno los indicadores de desempeño, a fin de evaluar el rendimiento de estos tres ámbitos de gestión. Las metas deben ser cuantificables y fácilmente alcanzables para lo que se sugiere que sean definidas bajo metodologías participativas con los involucrados.
Obtener la información de los indicadores de desempeño	Aplicando la metodología definida para el levantamiento de indicadores, se realiza la toma de medidas de manera objetiva en los formatos que la GIN defina para este fin.
Procesar la información de los indicadores de desempeño	La información de los indicadores se procesa a manera de cuadro de mando integral, con la finalidad de obtener información acerca del cumplimiento de metas.
Analizar la información de los indicadores de desempeño	Los indicadores de desempeño son analizados y son comparados con las metas propuestas, a fin de identificar las brechas de cumplimiento.
Elaborar informe de desempeño de los indicadores de niveles de servicio y requerimientos externos	El informe debe contener al menos, los siguientes elementos: • Antecedentes • Metodología para el levantamiento y procesamiento de la información. • Análisis comparativo de los indicadores con las metas. • Causas de no cumplimiento de metas. • Conclusiones y recomendaciones

ACTIVIDAD	DESCRIPCIÓN
Analizar los informes recibidos	Con el informe de evaluación de los indicadores de desempeño, se analizan los posibles cursos de acción que podrían tomarse para el mejoramiento de los servicios de TIC, cumplimiento de los objetivos de control requerimientos externos.
Tomar medidas preventivas	Las acciones preventivas se anticipan a la causa, y pretenden eliminarla antes de su existencia. Evitan los problemas identificando los riesgos. Cualquier acción que disminuya un riesgo es una acción preventiva. El registro y seguimiento de acciones preventivas y correctivas se lo debe realizar en formato GTI.R8.
Tomar medidas correctivas urgentes	Una acción correctiva es aquella que se lleva s a cabo para eliminar la causa de un problema. El registro y seguimiento de acciones preventivas y correctivas se lo debe realizar en formato GTI.R8.
Implementar las medidas correctivas y preventivas	Una vez que las acciones preventivas y correctivas han sido planteadas, se deben implementarlas. Para esto se requiere de la supervisión de las direcciones de TI, para garantizar su correcta aplicación. El registro y seguimiento de acciones preventivas y correctivas se lo debe realizar en formato GTI.R8.
Evaluar impacto de las medidas implementadas en la planificación estratégica de la GIN	En caso de las acciones preventivas y/o correctivas, causen un gran impacto en la planificación estratégica de la GIN, se procede a la aplicación del proceso de diseño de estrategia de TIC.

GTI.4.2: SEGUIMIENTO AL CUMPLIMIENTO DE LA PLANIFICACIÓN OPERATIVA

ACTIVIDAD	DESCRIPCIÓN
Obtener la información de desempeño del POA	Aplicando la metodología definida para el levantamiento de indicadores, se realiza la toma de medidas de manera objetiva en los formatos que la GIN defina para el monitoreo del cumplimiento del POA.
Procesar información de indicadores de desempeño del POA	La información de los indicadores se procesa a manera de cuadro de mando integral, con la finalidad de obtener información acerca del cumplimiento de metas del POA.
Analizar informe de indicadores de desempeño del POA	Los indicadores de desempeño son analizados y son comparados con las metas propuestas, a fin de identificar las brechas de cumplimiento del POA.
Elaborar informe de desempeño de indicadores del POA	El informe debe contener al menos, los siguientes elementos: • Antecedentes • Metodología para el levantamiento y procesamiento de la información. • Análisis comparativo de los indicadores con las metas. • Causas de no cumplimiento de metas. • Conclusiones y recomendaciones
Tomar medidas preventivas	Con el informe de evaluación de los indicadores de desempeño, se analizan los posibles cursos de acción que podrían tomarse para el mejoramiento de los servicios de TIC, cumplimiento de los objetivos de control requerimientos externos.
Tomar medidas correctivas urgentes	Las acciones preventivas se anticipan a la causa, y pretenden eliminarla antes de su existencia. Evitan los problemas identificando los riesgos. Cualquier acción que disminuya un riesgo es una acción preventiva. El registro y seguimiento de acciones preventivas y correctivas se lo debe realizar en formato GTI.R8.

ACTIVIDAD	DESCRIPCIÓN
Implementar las medidas correctivas y preventivas	Una acción correctiva es aquella que se lleva s a cabo para eliminar la causa de un problema. El registro y seguimiento de acciones preventivas y correctivas se lo debe realizar en formato GTI.R8.
Evaluar impacto de las medidas implementadas en la planificación estratégica de la GIN	Una vez que las acciones preventivas y correctivas han sido planteadas, se deben implementarlas. Para esto se requiere de la supervisión de las direcciones de TI, para garantizar su correcta aplicación. El registro y seguimiento de acciones preventivas y correctivas se lo debe realizar en formato GTI.R8.