ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS

PROPUESTA DE GESTIÓN DE LAS TIC'S EN LA SENAMI, UTILIZANDO LAS MEJORES PRÁCTICAS Y ESTÁNDARES INTERNACIONALES.

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER (MSc.) EN GESTION DE LAS COMUNICACIONES Y TECNOLOGIAS DE INFORMACION

ING. DIEGO XAVIER CASTRILLÓN VILLAGOMEZ
diego_castrillon@yahoo.com
ING. ANGEL HERIBERNAN MORENO MUÑOZ
moreno_angel@hotmail.com
DIRECTOR: ING. MSC. GUSTAVO SAMANIEGO
gustavo.samaniego@epn.edu.ec

Quito, Agosto 2009

DECLARACIÓN

Nosotros Diego Castrillón y Angel Moreno, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Ing. Diego Castrillón **Ing. Angel Moreno**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diego Castrillón y Angel Moreno, bajo mi supervisión.

Ing. Msc. Gustavo Samaniego
DIRECTOR DE PROYECTO

DEDICATORIA

A mi esposa Silvia, que siempre está apoyándome en mis retos profesionales quiero darte las gracias de todo corazón por haberme tenido paciencia con el tiempo que dedique a esta Maestría y no lo pase contigo, por tantas noches que me esperaste para irnos juntos a casa con nuestros pequeños hijos, no me queda más que darte las gracias y decirte que te amo con todo mi corazón y mi ser.

A mis hijos amados Erick y Maierly por haberme dado ese tiempo tan valioso que pude haberlo compartido con ellos, se los agradezco y se los repondré siempre apoyándolos con mi mayor esfuerzo.

Con todo mi Amor.
Angel Moreno.

DEDICATORIA

A mi Madre, esposa e hijos por ser los pilares fundamentales de mi existencia.

Gracias,

Diego X. Castrillón V.

INDICE

CAPITULO 1. ..... **8**

SITUACIÓN ACTUAL DE LAS TIC'S EN LA SENAMI. **8**

1.1 INTRODUCCIÓN 8
1.2 ESTRUCTURA ORGÁNICA INSTITUCIONAL 9
1.2.1 MISIÓN *9*
1.2.2 VISIÓN *9*
1.2.3 OBJETIVOS ESTRATÉGICOS *10*
1.2.4 OBJETIVO FUNDAMENTAL *11*
1.2.5 OBJETIVO GENERAL INSTITUCIONAL *11*
1.2.6 OBJETIVOS ESPECÍFICOS INSTITUCIONALES *11*
1.2.7 ANÁLISIS FODA *12*
1.2.7.1 Fortalezas 12
1.2.7.2 Oportunidades 12
1.2.7.3 Debilidades 12
1.2.7.4 Amenazas 13
1.3 ESTRUCTURA BÁSICA ALINEADA A LA MISIÓN. 13
1.3.1 PROCESOS GOBERNANTES. *13*
1.3.2 PROCESOS AGREGADORES DE VALOR. *13*
1.3.3 PROCESOS HABILITANTES. *14*
1.3.3.1 Procesos habilitantes de asesoría. 14
1.3.3.2 Procesos habilitantes de apoyo 14
1.3.3.3 Procesos desconcentrados 14
1.4 CADENA DE VALOR. 15
1.5 MAPA DE PROCESOS 15
1.6 ESTRUCTURA ORGÁNICA 16
1.7 ESTRUCTURA DE LAS SUBSECRETARIAS REGIONALES 16
1.8 PROYECTOS EMBLEMÁTICOS DE LA SENAMI 17
1.8.1 PLAN BIENVENID@S A CASA: PARA UN REGRESO VOLUNTARIO, DIGNO Y SOSTENIBLE. *17*
1.8.2 FACILIDAD PARA EL TRASLADO DE MENAJE DE CASA Y EQUIPO DE TRABAJO BIENVENID@S A CASA. *17*
1.8.3 FONDO PARA EL RETORNO DIGNO Y SOSTENIBLE "FONDO EL CUCAYO" *18*
1.8.4 FORES FORTALECIMIENTO ORGANIZACIONAL Y CONSTRUCCIÓN DE REDES SOCIALES EN EL HECHO MIGRATORIO *18*
1.8.5 SENAMI MÓVIL. CARAVANAS CULTURALES DE SENSIBILIZACIÓN Y DIGNIFICACIÓN DEL HECHO MIGRATORIO. *18*
1.8.6 CASAS ECUATORIANAS *18*
1.8.7 PASAPORTE UNIVERSAL *19*
1.8.8 ECUADOR MÍRAME CON OTROS OJOS *19*
1.8.9 PLATAFORMA VIRTUAL MIGRANTE ECUATORIANO www.migranteecuatoriano.gov.ec 19
1.8.10 MI CASA. BONO DE VIVIENDA PARA PERSONAS MIGRANTES. *20*
1.8.11 BANCO DEL MIGRANTE. PROYECTO EN CONSTRUCCIÓN. *20*
1.9 VISIÓN GENERAL Y PROPÓSITO DE LAS TIC'S 20
1.10 SISTEMAS INFORMÁTICOS (SI) ACTUALES 21
1.10.1 HARDWARE *21*
1.10.2 SOFTWARE *21*
1.10.3 APLICACIONES. *22*
1.10.4 BASE DE DATOS *22*
1.10.5 REDES Y COMUNICACIONES. *22*
1.10.6 INTERNET BANDA ANCHA *23*
1.10.7 RECURSOS HUMANOS *25*
1.11 SISTEMAS DE INFORMACION A LOS PROCESOS INTERNOS Y EXTERNOS DE LA INSTITUCION 25
1.11.1 APOYO A LOS PROCESOS INTERNOS *25*
1.11.2 APOYO A LOS PROCESOS EXTERNOS *26*
1.11.3 LIMITACIONES ACTUALES DE LOS SI *26*
1.11.4 ESTRATEGIA Y ESTRUCTURA DE GESTIÓN DE LOS SI *26*

CAPITULO 2. ..... **28**

DETERMINACIÓN DE LAS MEJORES PRÁCTICAS Y ESTÁNDARES INTERNACIONALES PARA LA GESTIÓN DE LAS TIC'S. **28**

2.1 COBIT 29
2.1.1 ÁREAS FOCALES DEL GOBIERNO DE TI *29*
2.1.1.1 Alineación estratégica. 30
2.1.1.2 Entrega de valor. 30
2.1.1.3 Administración de recursos. 30
2.1.1.4 Administración de riesgos. 30
2.1.1.5 Medición del desempeño. 31
2.1.2 INTERRELACIONES DE LOS COMPONENTES DE COBIT *31*
2.1.3 MARCO GENERAL DE TRABAJO DE COBIT *32*
2.1.3.1 Orientado al negocio 32
2.1.3.2 Criterios de Información de COBIT 32
2.1.3.2.1 Metas de negocio y de TI 33
2.1.3.2.2 Recursos de TI 34
2.1.3.2.3 Procesos orientados 35
2.1.3.2.4 Basado en Controles 36
2.1.3.2.5 Generadores de mediciones 36
2.1.3.2.6 Modelos de Madurez 36
2.1.3.2.7 Medición del desempeño. 38
2.1.4 EL MODELO DEL MARCO DE TRABAJO COBIT *40*
2.2 ITIL 43
2.2.1 BENEFICIOS DE LA GESTIÓN DE SERVICIOS DE TI *44*
2.2.2 GESTIÓN DE SERVICIOS ITIL *45*
2.3 ISO 20.000 45
2.3.1 ISO 20.000 Y SU RELACIÓN CON ITIL *46*

CAPITULO 3. ..... **48**

PROPUESTA DE GESTIÓN DE LAS TIC'S EN LA SENAMI **48**

3.1 PROCESO DE GESTIÓN TECNOLÓGICA 48
3.1.1 OBJETIVO. *48*
3.1.2 POLÍTICAS GENERALES. *48*
3.1.3 DEFINICIONES. *48*
3.1.4 ESTRUCTURA. *49*
3.2 SUBPROCESO: GESTIÓN ESTRATÉGICA TECNOLÓGICA 50
3.2.1 OBJETIVO. *50*
3.2.2 PRODUCTOS. *50*
3.2.3 POLÍTICAS. *50*
3.2.4 PROCEDIMIENTOS *51*
3.2.5 DOCUMENTOS *51*
3.2.6 INDICADORES DE DESEMPEÑO DEL SUBPROCESO *53*
3.3 SUBPROCESO: ADMINISTRACIÓN DE APLICACIONES 55
3.3.1 DEFINICIÓN *55*
3.3.2 ALCANCE. *55*
3.3.3 REFERENCIAS *56*
3.3.4 POLÍTICAS. *56*
3.3.5 PROCEDIMIENTOS *57*
3.3.6 DOCUMENTOS *57*
3.3.7 INDICADORES DE DESEMPEÑO DEL SUBPROCESO *59*
3.4 SUBPROCESO: ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA 59
3.4.1 OBJETIVO. *59*
3.4.2 PRODUCTOS. *60*
3.4.3 POLÍTICAS. *60*
3.4.3.1 Subproceso Administración de Hardware 61
3.4.3.1.1 Procedimiento 61
3.4.3.1.2 Documentos 61
3.4.3.1.3 Indicadores de Desempeño del Subproceso 63
3.4.3.2 Subproceso Administración de Software base y Aplicativos 64
3.4.3.2.1 Procedimiento 64

3.4.3.2.2 Documentos ... 64
3.4.3.2.3 Indicadores de Desempeño del Subproceso ... 65
3.4.3.3 Subproceso Administración de Seguridades ... 66
3.4.3.3.1 Procedimiento ... 66
3.4.3.3.2 Documentos ... 67
3.4.3.3.3 Indicadores de Desempeño del Subproceso ... 68
3.4.3.4 Subproceso Soporte a Usuarios ... 68
3.4.3.4.1 Objetivo ... 68
3.4.3.4.2 Políticas ... 69
3.4.3.4.3 Procedimiento ... 69
3.4.3.4.4 Documentos ... 69
3.4.3.4.5 Indicadores de Desempeño del Subproceso ... 70
3.5 SUBPROCESO: ADMINISTRACIÓN DE REDES Y COMUNICACIONES ... 71
3.5.1 OBJETIVO ... *71*
3.5.2 POLÍTICAS ... *71*
3.5.3 PROCEDIMIENTO ... *71*
3.5.4 DOCUMENTOS ... *71*
3.5.5 INDICADORES DE DESEMPEÑO DEL SUBPROCESO ... *73*
3.6 RECURSOS HUMANOS ... 74
3.6.1 CARGO: DIRECTOR DE GESTIÓN TECNOLÓGICA. ... *74*
3.6.1.1 Definición del cargo, roles y responsabilidades: ... 74
3.6.1.2 Requisitos que el Cargo Exige: ... 75
3.6.1.3 Competencias requeridas para los cargo tipo ... 75
3.6.1.4 Funciones y Responsabilidades del Cargo ... 75
3.6.2 CARGO: TÉCNICO DE SOFTWARE. ... *77*
3.6.2.1 Definición del cargo, roles y responsabilidades: ... 77
3.6.2.2 Requisitos que el Cargo Exige: ... 77
3.6.2.3 Competencias requeridas para los cargo tipo ... 77
3.6.2.4 Funciones y Responsabilidades del Cargo ... 77
3.6.3 CARGO: TÉCNICO DE HARDWARE. ... *81*
3.6.3.1 Definición del cargo, roles y responsabilidades: ... 81
3.6.3.2 Requisitos que el Cargo Exige: ... 81
3.6.3.3 Competencias requeridas para los cargo tipo ... 82
3.6.3.4 Funciones y Responsabilidades del Cargo ... 82
3.7 RECOMENDACIÓN DE HERRAMIENTAS OPEN SOURCE PARA AUTOMATIZAR LA GESTIÓN DE LAS TIC'S. ... 83
3.7.1 HERRAMIENTAS OPEN SOURCE ... *83*

CAPITULO 4. ... **86**

CONCLUSIONES Y RECOMENDACIONES ... **86**

4.1 CONCLUSIONES ... 86
4.2 RECOMENDACIONES ... 87

BIBLIOGRAFÍA ... **89**

ANEXOS ... **91**

ANEXO A. RESUMEN DOMINIOS Y ACTIVIDADES DE COBIT. ... **92**

ANEXO B. PROCEDIMIENTO SUBPROCESO GESTIÓN ESTRATÉGICA TECNOLÓGICA ... **145**

ANEXO C. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE APLICACIONES ... **148**

ANEXO D. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE HARDWARE ... **152**

ANEXO E. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE SW BASE Y APLICATIVOS ... **155**

ANEXO F. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE SEGURIDADES ... **158**

ANEXO G. PROCEDIMIENTO. SUBPROCESO. SOPORTE A USUARIOS ... **162**

ANEXO H. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE REDES Y COMUNICACIONES ... **165**

CAPITULO 1.

SITUACIÓN ACTUAL DE LAS TIC'S EN LA SENAMI.

1.1 INTRODUCCIÓN

La Secretaría Nacional del Migrante SENAMI tiene casi dos años de funcionamiento durante este tiempo han pasado dos administraciones la primera que duro aproximadamente seis meses y la segunda hasta la presente fecha.

En el área tecnológica se han implementado varios servicios a partir de Enero del 2008, desde la implementación de las nuevas oficinas hasta la implementación de varios proyectos en la Unidad de Gestión Tecnológica y los otros departamentos.

Debido al acelerado crecimiento que ha tenido la institución en función del sin numero de requerimientos de nuestros compatriotas emigrantes la Unidad de Gestión Tecnológica ha ido creciendo en funciones y responsabilidades sin un adecuado control, regularización y documentación que permita tener un adecuado Gobierno de TIC's dentro de la SENAMI lo que ha originado el no contar con estándares y procedimientos adecuados para tener una adecuada gestión de las TIC's en la institución.

En función de estos inconvenientes presentados se observa la necesidad de contar con una propuesta de Gestión de las TIC's en la SENAMI, utilizando las mejores prácticas y estándares internacionales.

Para esto se han desarrollado tres encuestas sobre los de servicios que brinda el departamento de Gestión informática de la SENAMI para todos los usuarios internos y externos.

1. Calidad de soporte técnico informático en la institución

2. Requerimientos informáticos en los diferentes departamentos
3. Necesidades en el departamento de Gestión Informática

Los resultados de dichas encuestas nos demuestran que la calidad de servicio del soporte informático en la institución es medio es decir se la debe mejorar; que existen muchos requerimientos en todos los departamentos, tanto de hardware así como de software. Los funcionarios de la Gestión Informática ven la necesidad de contar con una mayor jerarquización de la unidad ya que sus actividades y funciones son transversales para toda la organización.

1.2 ESTRUCTURA ORGÁNICA INSTITUCIONAL

La estructura organizacional de la SENAMI se sustenta en la misión y objetivos institucionales:

1.2.1 MISIÓN

La Secretaría Nacional del Migrante (SENAMI) coordina y ejecuta la política migratoria integral del Estado Ecuatoriano, brindando una atención integral a las personas emigrantes, contribuyendo al aumento de sus capacidades y potencialidades y velando por la salvaguarda de sus derechos fundamentales. Son elementos fundamentales de esta política el diálogo permanente y constructivo con los actores institucionales y sociales del hecho migratorio, así como su proyección en los foros internacionales como parte de la acción exterior del Estado.

1.2.2 VISIÓN

Para que la movilidad y la permanencia en y a través de los territorios sean vividas como verdaderas expresiones de libertad para las personas, quedando garantizados sus derechos fundamentales y acompañadas sus necesidades y expectativas en sus proyectos de vida.

Para que las migraciones desplieguen todo su potencial para el desarrollo humano, político, económico y cultural en las sociedades de origen y de destino.

Para que los pueblos avancen hacia prácticas y políticas efectivas de integración y de convivencia que hagan posible el ejercicio de una plena y real ciudadanía universal y que sean liberados de la discriminación, la xenofobia y el racismo.

Para que los distintos problemas derivados de los procesos de movilidad humana forzada sean mitigados y se generen soluciones eficaces adaptadas a las diferentes situaciones de vulnerabilidad de las personas.

SLOGAN.- “Estamos arreglando la casa para que vuelvan” Tod@s somos migrantes.

1.2.3 OBJETIVOS ESTRATÉGICOS

Coordinar directamente con la Presidencia de la Republica, la ejecución de las políticas migratorias encaminadas al desarrollo humano de todos sus actores;

Promover y coordinar de una manera oportuna con todos los actores e instituciones, ya sean estos públicos y privados, vinculados con el tema migratorio a nivel de país.

Propiciar el respeto de la persona y sus derechos aplicando los convenios internacionales y adecuando a ellos la normativa nacional, con sus respectivos reglamentos.

Convertir la migración en el factor para el desarrollo integral del país, con total respeto a los derechos humanos de los actores y el cumplimiento de sus deberes legales.

Transformar la migración ecuatoriana en un elemento positivo para el intercambio cultural y el desarrollo compartido entre Ecuador y el país de destino partiendo del bienestar del emigrante y su familia.

Fomentar el conocimiento de la realidad migratoria en su dimensión integral con sus múltiples causas y efectos potenciando los factores positivos que contribuyen a la construcción del proyecto país.

1.2.4 OBJETIVO FUNDAMENTAL

Definición y ejecución de las políticas migratorias encaminadas al desarrollo humano de todos sus actores, que servirá de enlace en las acciones de atención, protección y desarrollo del migrante, conforme a los objetivos del estado ecuatoriano.

1.2.5 OBJETIVO GENERAL INSTITUCIONAL

Establecer y ejecutar políticas, planes, programas y proyectos participativos que permitan mejorar las condiciones de vida de los migrantes, sus familias y su entorno.

1.2.6 OBJETIVOS ESPECÍFICOS INSTITUCIONALES

- Crear y fortalecer las políticas migratorias y convenios de cooperación en defensa de los derechos humanos en América latina y el mundo.
- Definir políticas participativas para establecer planes, programas y proyectos de inversión y autogestión financiera en el Ecuador en áreas sociales, culturales y económicas.
- Establecer y promover convenios para el financiamiento de planes, programas y proyectos de la SENAMI.
- Promover la regularización migratoria, la reagrupación familiar y/o el retorno planificado del migrante y su familia para fortalecer el núcleo familiar.
- Facilitar el proceso de formación y fortalecimiento de organizaciones integradas por migrantes para fortalecer la identidad del migrante y su familia a través de la apropiación social o pertenencia del patrimonio ecuatoriano.

1.2.7 ANÁLISIS FODA

1.2.7.1 Fortalezas

- Potencial humano capacitado.
- Institución nueva no esta contaminada.
- Independencia y autonomía Administrativa.
- Funcionarios migrantes y con experiencia en este ámbito.
- Definición y ejecución de políticas migratorias.
- Fondo del migrante.
- Gente joven con nuevas ideas.
- Capacidad de liderazgo.
- Actitud positiva.

1.2.7.2 Oportunidades

- Apoyo del Sr. Presidente.
- Relaciones interinstitucionales e internacionales.
- Proyección a ministerio.
- Traspaso de competencias de otros ministerios y de Cancillería.
- Modelo de desarrollo institucional.
- Posición estratégica con otros ministerios.
- Elevada población de migrantes no atendidos.
- Valiosa oportunidad de Posicionar un modelo de liderazgo latinoamericano en política migratoria.
- Fortalecimiento institucional por medio de la asamblea.
- Creación oportuna de la institución.
- Nuevas políticas latinoamericanas de integración.

1.2.7.3 Debilidades

- No disponer mecanismos de control contra la corrupción.
- Falta de información sistematizada sobre procesos migratorios.
- No existencia de reglamentos y manuales de procedimientos en la actualidad.
- No existencia de procesos definidos y sistemas de logística inadecuada.

- Equipo humano por seleccionar.
- Rumores y cuentos.
- Falta de coordinación interna.
- Falta de difusión de las actividades realizadas por los funcionarios.

1.2.7.4 Amenazas

- Interés sectorial en el manejo de temas migratorios.
- Celos interinstitucionales: Cancillería, Ministerio de Gobierno, Defensoría del Pueblo.
- Falta de puntos de apoyo en el exterior.
- Falta de financiamiento a mediano plazo.
- Falta de marco jurídico en tema migratorio nacional e internacional.
- Falta de coordinación en la normativa migratoria nacional.
- Falta de contacto con organizaciones gubernamentales y no gubernamentales.
- Redes de tráfico de migrantes (coyoterismo).
- Dependencia de las políticas de gobiernos extranjeros.

1.3 ESTRUCTURA BÁSICA ALINEADA A LA MISIÓN.

La SENAMI, para el cumplimiento de su misión y responsabilidades, gestiona procesos internos y está conformada por:

1.3.1 PROCESOS GOBERNANTES.

- Direccionamiento Estratégico De La Definición Y Ejecución De Las Políticas Migratorias.

- Gestión Estratégica De La Definición Y Ejecución De Las Políticas Migratorias.

1.3.2 PROCESOS AGREGADORES DE VALOR.

- Gestión de Atención y Protección al Migrante
- Gestión de Desarrollo del Migrante

- Gestión de Evaluación y Seguimiento de Planes, Programas, y Proyectos del Migrante.

1.3.3 PROCESOS HABILITANTES.

1.3.3.1 Procesos habilitantes de asesoría.

- Gestión de Asesoría Jurídica
- Gestión de Auditoria Interna
- Planificación Institucional
- Comunicación Social

1.3.3.2 Procesos habilitantes de apoyo

- Gestión Administrativa
- Gestión Financiera
- Gestión de Recursos Humanos
- Gestión Informática

1.3.3.3 Procesos desconcentrados

Gestión técnica para la implementación de las políticas migratorias (subsecretarias regionales del austro y del litoral).

1.4 CADENA DE VALOR.

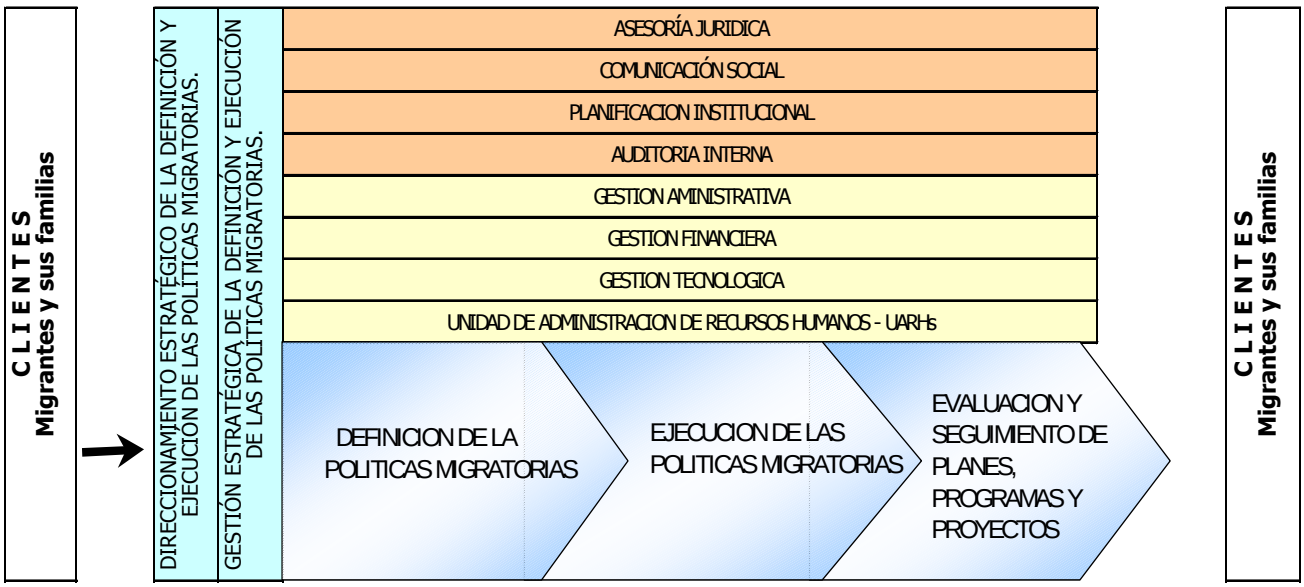


Figura. 1

1.5 MAPA DE PROCESOS

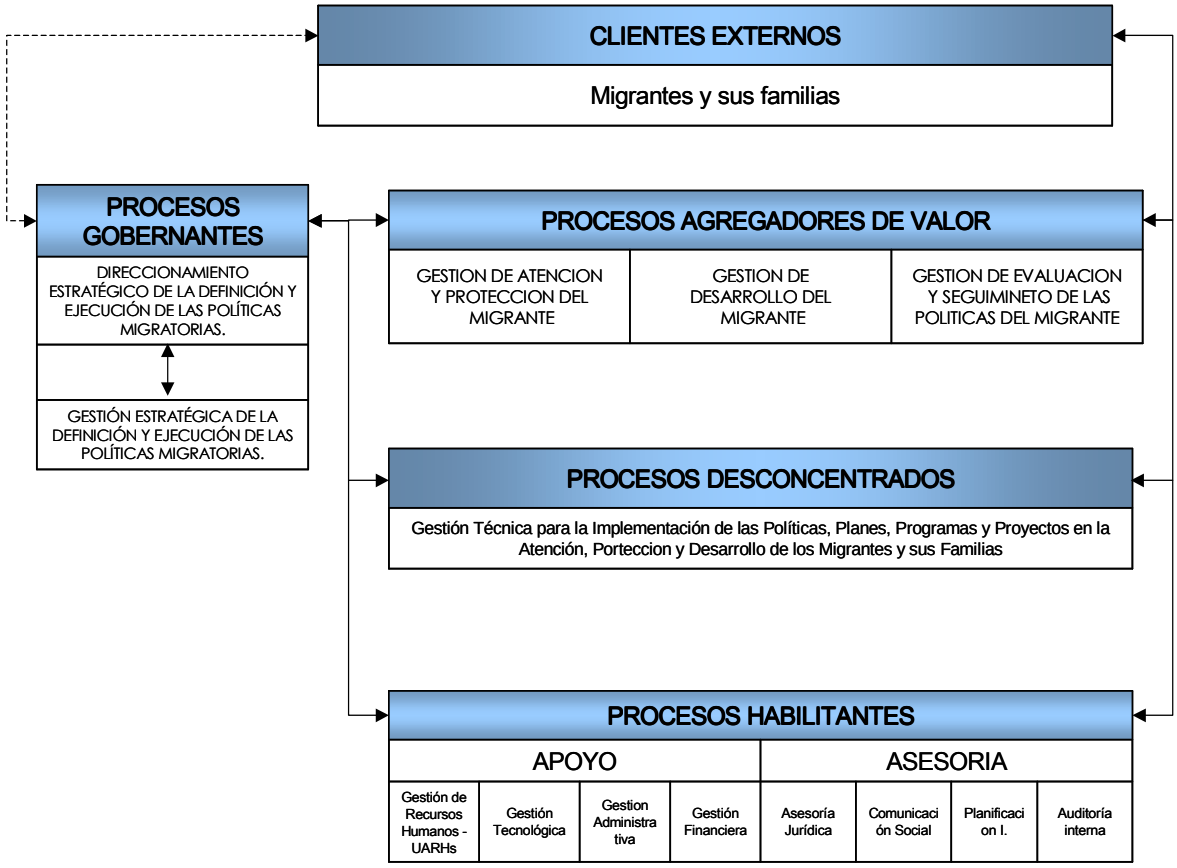


Figura. 2

1.6 ESTRUCTURA ORGÁNICA

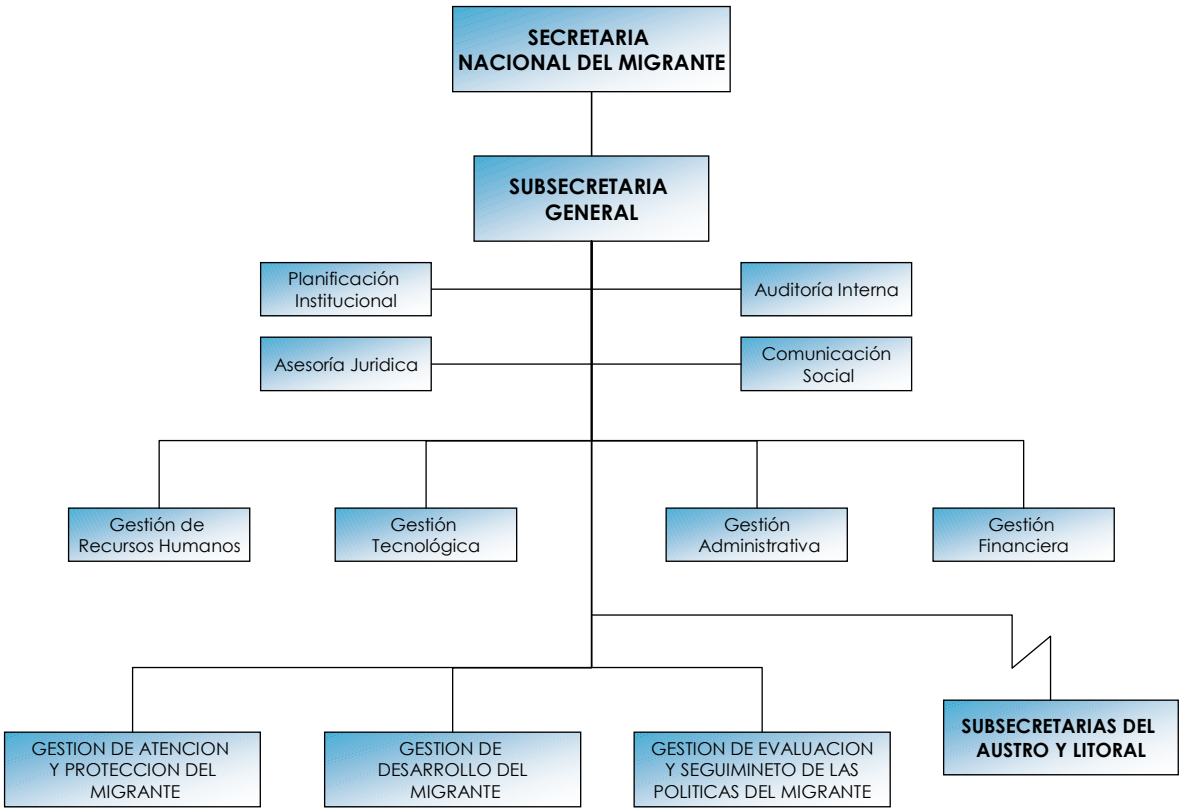


Figura. 3

1.7 ESTRUCTURA DE LAS SUBSECRETARIAS REGIONALES

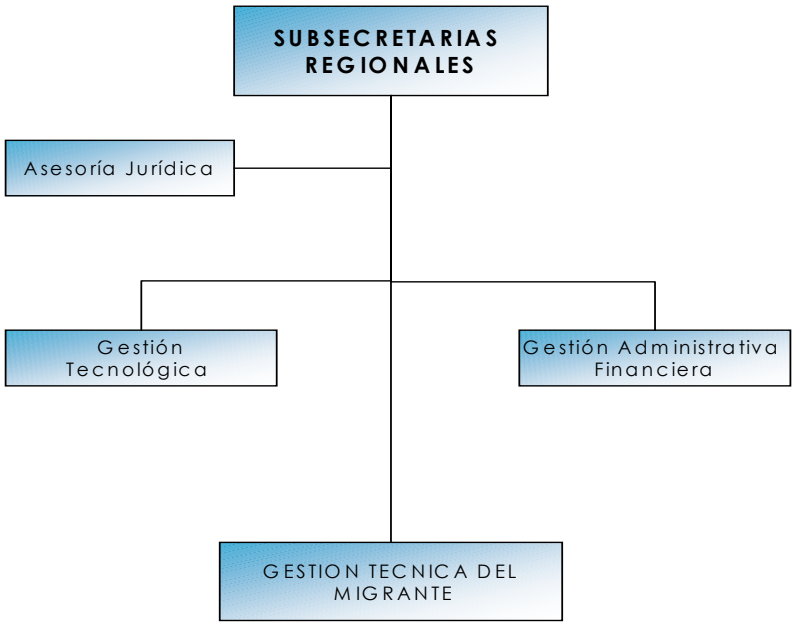


Figura 4.

1.8 PROYECTOS EMBLEMÁTICOS DE LA SENAMI

1.8.1 PLAN BIENVENID@S A CASA: PARA UN REGRESO VOLUNTARIO, DIGNO Y SOSTENIBLE.

Se defiende un regreso entendido en sentido amplio: una vuelta a casa que no implica necesariamente el regreso físico sino, de forma más general, el fortalecimiento de los lazos afectivos, culturales, sociales y económicos de nuestros emigrantes para con su país de origen y al mismo tiempo, la recuperación para el Ecuador de las capacidades y talentos de estos millones de compatriotas, que vienen contribuyendo en la distancia con su esfuerzo al progreso de nuestra sociedad. Este plan lo integran un conjunto de 3 programas (Vínculos, Incentivos productivos; y Acompañamiento al regreso físico) que apoyan y acompañan a las personas ecuatorianas que se encuentran en el exterior, así como aquellas que han decidido regresar a su país o se han visto obligadas a hacerlo. Trabajamos en coordinación con todos los Ministerios del Estado y otras instituciones públicas y privadas, para que las condiciones para un regreso voluntario, digno y sostenible de nuestros emigrantes se fortalezcan desde una política de Estado.

1.8.2 FACILIDAD PARA EL TRASLADO DE MENAJE DE CASA Y EQUIPO DE TRABAJO BIENVENID@S A CASA.

El Gobierno Nacional y la SENAMI han impulsado la reforma al Reglamento a la Ley Orgánica de Aduanas, y e coordinación con la CAE han introducido una serie de facilidades para el traslado del menaje de casa y el equipo de trabajo, que incluyen la exoneración de tasas aduaneras y la simplificación de los trámites. Mediante esta medida, se pretende contribuir a mejorar las condiciones generales de cara al ejercicio del derecho al retorno que tiene toda persona migrante.

1.8.3 FONDO PARA EL RETORNO DIGNO Y SOSTENIBLE “FONDO EL CUCAYO“

El Fondo El Cucayo es un proyecto que ofrece a nuestros compatriotas emigrantes una asesoría técnica especializada para la creación de negocios productivos propios, familiares o asociativos. Así mismo, facilita capital semilla a los mejores proyectos empresariales seleccionados mediante concurso. El programa va dirigido a migrantes que han retornado al país desde el mes de enero de 2007, o que prevean hacerlo en el corto plazo o que hayan permanecido en el exterior por lo menos un año, sin interrupciones mayores a 60 días.

1.8.4 FORES FORTALECIMIENTO ORGANIZACIONAL Y CONSTRUCCIÓN DE REDES SOCIALES EN EL HECHO MIGRATORIO

Es un proyecto para fortalecer los lazos de familiaridad, afectividad y sentido de pertenencia a través de la sensibilización y ejercicio de derechos de la población que ha migrado y sus familias y la ejecución de propuestas para su propio desarrollo.

1.8.5 SENAMI MÓVIL. CARAVANAS CULTURALES DE SENSIBILIZACIÓN Y DIGNIFICACIÓN DEL HECHO MIGRATORIO.

El proyecto cultural Campaña de Sensibilización y Dignificación del hecho Migratorio, consiste en una caravana móvil que recorrerá varias ciudades y pueblos del país y de los principales países de destino ecuatorianas y ecuatorianos. La caravana utiliza el arte como lengua de expresión y divulgación integral y humanista de la migración que tiene el Estado ecuatoriano. Nuestro escenario rodante llegará a todos con teatro, fotografía, radio teatro, video y foros.

1.8.6 CASAS ECUATORIANAS

Espacio de acogida y asesoría a personas migrantes que están viviendo en el exterior, en donde pueden encontrar: Una guía para arreglar situaciones legales; de asesoría en inversiones, emprendimientos en el lugar de destino y en su país de origen; acompañamiento y apoyo a la recuperación de la identidad, la cultura e

inserción en el sistema educativo; escucha y acompañamiento en sus problemas psico-sociales y de violación a los derechos humanos, provocados por las nuevas enfermedades del estrés, el odio racial, la xenofobia, entre otros.

1.8.7 PASAPORTE UNIVERSAL

El pasaporte universal simboliza la orientación fundamental de la política migratoria integral impulsada desde el nuevo Ecuador, que aspira a contribuir al avance gradual de la Humanidad hacia el ideal de una ciudadanía universal en el largo plazo, y hacia la consecución en el mediano plazo, de una ciudadanía de residencia, y no de nacionalidad, que garantice los plenos derechos para las personas migrantes. Este desafío que afronta el Ecuador es tanto mayor cuanto que la actual tendencia de las políticas migratorias en el mundo tiende clara y dramáticamente hacia un endurecimiento con tintes discriminatorios, criminalizantes y represivo-disuasivos, que atentan contra los derechos de millones de personas en movilidad en todo el Mundo.

1.8.8 ECUADOR MÍRAME CON OTROS OJOS

Ecuador mírame con otros ojos es una campaña de comunicación orientada a la sensibilización de la población del litoral ecuatoriano sobre la realidad migratoria, sus dimensiones, sus implicaciones y sus potencialidades. El objetivo principal es fortalecer los vínculos afectivos, sociales y culturales entre las personas migrantes y sus familias residentes en el litoral y, así mismo, fomentar una actitud de respeto hacia el ecuatoriano que regresa al país para facilitar su plena y efectiva reintegración en nuestra sociedad.

1.8.9 PLATAFORMA VIRTUAL MIGRANTE ECUATORIANO www.migranteecuatoriano.gov.ec

Migranteecuatoriano es el espacio virtual de encuentro de las personas migrantes con su país, su familia, su gente, su cultura, dónde también se informa de los planes, programas y proyectos de la Secretaria Nacional del Migrante SENAMI. Esto lo logramos mediante el uso de las nuevas tecnologías de información y comunicaciones, tales como redes sociales virtuales, televisión on-line, video-

conferencias y telecentros disponibles en nuestras Casas Ecuatorianas en el Exterior y en nuestras Casas del Migrante en Ecuador.

1.8.10 MI CASA. BONO DE VIVIENDA PARA PERSONAS MIGRANTES.

El bono de la vivienda para las personas migrantes y sus familias surge como una respuesta de las demandas de aquellos y aquellas compatriotas que prevén un regreso al Ecuador y que no poseen los medios para contar con una vivienda digna. Siendo el acceso a la vivienda un derecho promovido por la Revolución Ciudadana y consagrado en la Nueva Constitución, esta facilidad se ofrece sólo para personas de escasos recursos, como contribución a su derecho a ejercer un regreso a la patria en las mejores condiciones posibles.

1.8.11 BANCO DEL MIGRANTE. PROYECTO EN CONSTRUCCIÓN.

El Banco del Migrante (BdM) es una institución financiera pública orientada a mejorar la calidad de vida y los servicios ofrecidos a los y las ecuatorianos migrantes. Provee servicios financieros y no financieros orientados cubrir las necesidades personales, familiares y empresariales de la persona migrante, impulsa y fortalece la integración económica y financiera entre la persona migrante, su familia y lugar de origen. Para ello, cuentan con el soporte de redes de servicios financieros y no financieros, locales y extra locales, un portafolio de servicios diferenciado, diversificado, innovador y competitivo, y una estructura organizativa liviana, ágil y flexible, apoyada de manera significativa en la tecnología.

1.9 VISIÓN GENERAL Y PROPÓSITO DE LAS TIC’S

El uso de las TIC's Tecnologías de Información y Comunicación, principalmente con el uso de Internet, está brindado un nuevo paradigma de comunicaciones a los migrantes y sus familiares en todo el mundo. Con el uso de la tecnología se han eliminan las fronteras y distancias pudiendo mantener una comunicación instantánea y oportuna con nuestros familiares fuera del Ecuador.

Es por estas razones entre otras que la institución esta empeñada en impulsar el uso eficiente de las tecnologías de información y comunicación en el soporte y apoyo a nuestros migrantes que se encuentran en los diferentes países del mundo, así como también en la implementación de procesos internos eficientes de atención a los mismos.

Por tal motivo el propósito del presente análisis es consolidar la infraestructura tecnológica tanto de hardware, software, comunicaciones, y recurso humano con el que cuenta el Departamento de Gestión Tecnológica con la finalidad de brindar los servicios necesarios tanto para el usuario interno como externo para facilitar la atención al migrante, presentación, evaluación y seguimiento de proyectos, y otros sistemas necesarios para el buen funcionamiento de la institución.

1.10 SISTEMAS INFORMÁTICOS (SI) ACTUALES

Principales sistemas que existen y su capacidad actual: HW, SW, Comunicaciones

1.10.1 HARDWARE

La SENAMI actualmente cuenta con una infraestructura tecnológica robusta con servidores, comunicaciones y estaciones de trabajo.

La SENAMI cuenta con:

- 150 PC's de última tecnología
- 150 UPS personales
- 20 laptos,
- 20 impresoras compartidas
- 10 Proyectores

1.10.2 SOFTWARE

A nivel de estaciones de trabajo se cuenta con:

- Ubuntu.
- Windows XP.
- Microsoft Office 2003.

- Internet Explorer 6.1
- Open Office
- Firefox
- PDF 995 (convertidor de PDF)
- Winrar (compresor de archivos)
- Software de impresoras

1.10.3 APLICACIONES.

Se cuenta con Microsoft Office 2003 como herramienta de escritorio, instalado en todas las PC's de la institución.
Suite de antivirus F-Secure, con actualización en línea conectándose al servidor de Antivirus de la institución, el cual actualiza vía Internet las últimas versiones de los motores de escaneo.
Silec Pro. - Lexis, soporte para la Asesoría Jurídica.
Utilitarios como Winzip, Acrobat Reader, Winrar, PDF995.

1.10.4 BASE DE DATOS

La SENAMI cuenta con bases de datos documentales en Postgresql, bases de datos relaciónales Access, MySQL

1.10.5 REDES Y COMUNICACIONES.

La institución cuenta con una red de cableado estructurado categoría 6, con 150 puntos interconectados en la ciudad de Quito en la oficina matriz en la Av. Eloy Alfaro N29-50 y 9 de Octubre.
Cableado estructurado categoría 5e con 30 puntos en la ciudad de Guayaquil.
Cableado estructurado categoría 5e con 40 puntos en la ciudad de Cuenca.
Cableado estructurado categoría 6 con 30 puntos en la ciudad de Quito en la oficina de la Colón y 10 de Agosto.
Cableado estructurado categoría 6 con 150 puntos en la ciudad de Quito en la oficina matriz Eloy Alfaro y 9 de Octubre.
Se encuentran interconectadas la ciudad de Quito Guayaquil y Cuenca con enlaces de datos dedicados.
Se encuentra implementada telefonía IP, con Open Source Asterisk.

Los equipos de comunicación son los siguientes:

- 1 Switch 3Com 4500 10/100/1000 (12 p).
- 3 Switch 3Com 4500 10/100/1000(48 p).
- 2 Gateways de 4 líneas telefónicas cada uno.
- 1 Transceiver de Fibra Óptica.
- 6 Switch 3Com 5500 10/100/1000 (48 p).
- 4 Modem inalámbricos para conexión a Internet.

1.10.6 INTERNET BANDA ANCHA

Enlace dedicado de fibra óptica de 3 Mbps para datos y 3 Mbps para Internet el cual es distribuido a las oficinas de la casa matriz, oficina de la Colón, Cuenca y Guayaquil.

Se cuenta con el servicio de Internet inalámbrico con módems USB para 6 usuarios directivos.

Como podemos observar en la Figura 5, se encuentra detallada toda la red que utiliza la SENAMI (año 2009).

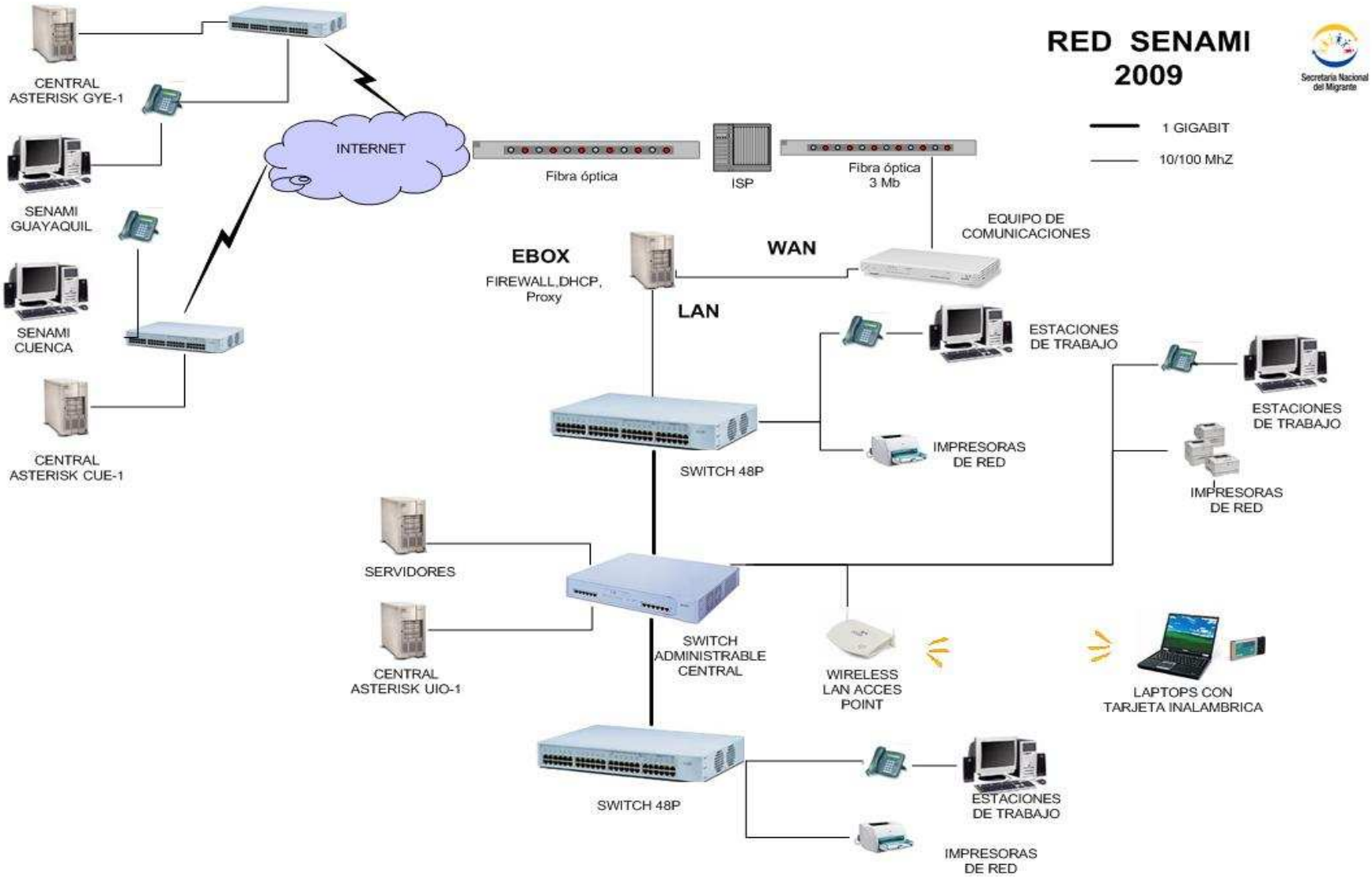

RED SENAMI
2009
Secretaría Nacional del Migrante
1 GIGABIT
10/100 MhZ
CENTRAL
ASTERISK GYE-1
INTERNET
Fibra óptica
ISP
Fibra óptica
3 Mb
SENAMI
GUAYAQUIL
EQUIPO DE
COMUNICACIONES
EBOX
FIREWALL,DHCP,
Proxy
WAN
LAN
SENAMI
CUENCA
ESTACIONES
DE TRABAJO
ESTACIONES
DE TRABAJO
CENTRAL
ASTERISK CUE-1
SWITCH 48P
IMPRESORAS
DE RED
IMPRESORAS
DE RED
SERVIDORES
SWITCH
ADMINISTRABLE
CENTRAL
CENTRAL
ASTERISK UIO-1
WIRELESS
LAN ACCES
POINT
LAPTOPS CON
TARJETA INALAMBRICA
SWITCH 48P
ESTACIONES
DE TRABAJO
IMPRESORAS
DE RED

Figura 5

1.10.7 RECURSOS HUMANOS

El Departamento de Gestión Tecnológica dispone actualmente de 3 Ingenieros de Sistemas, de los cuales uno hace como líder de tecnología. Los tres técnicos realizan varias funciones relacionadas con el Departamento.

1.11 SISTEMAS DE INFORMACION A LOS PROCESOS INTERNOS Y EXTERNOS DE LA INSTITUCION

Se iniciado el proceso de implementación de varios sistemas con los cuales todos los usuarios podrán realizar sus actividades de una manera mucho más eficiente.

1.11.1 APOYO A LOS PROCESOS INTERNOS

Se cuenta con un sistema de Gestión Documental, que actualmente se encuentra en fase de implementación, el cual se encuentra en los Servidores de la Subsecretaría de Informática de acuerdo a los estándares establecidos por ésta.

Existe un Sistema de Gestión de proyectos, que actualmente se encuentra en fase de implementación, el cual se encuentra en el hosting brindado por la empresa adjudicada.

Estos sistemas han sido desarrollados en Open Source con la finalidad de dar cumplimiento al mandato presidencial de usar herramientas Open Source.

Existe una aplicación desarrollada en Access con el fin de tener un control de los inventarios y suministros de la institución, también existe otra para el control de casos atendidos en repatriación de cadáveres.

Además se cuenta con una hoja electrónica donde se registran los casos atendidos por atención al migrante.

1.11.2 APOYO A LOS PROCESOS EXTERNOS

Se cuenta con la página Web: www.senami.org, donde se brinda información de la institución y los diferentes proyectos de apoyo que se implementaran.

Se utiliza el Sistema de Gestión Financiera (e-SIGEF) como herramienta de gestión financiera a nivel gubernamental a través de Internet.

Existe el Sistema Nacional de Inversión Pública (SNIP), del Ministerio de Economía y Finanzas y el Sistema Publico Remuneraciones (SIPREM).

Se utilizara el Sistema de Pagos Interbancarios (SPI) como herramienta de pagos del Banco Central a través de Internet.

1.11.3 LIMITACIONES ACTUALES DE LOS SI

A continuación se indican algunas limitaciones actuales de los SI:

- Falta de posicionamiento de la unidad de Gestión Informática dentro de la organización.
- No se cuenta con el espacio físico adecuado para el Centro de Cómputo de la SENAMI.
- No se tiene el personal mínimo necesario dentro de la unidad de Gestión Informática.
- Espacio físico actual del Centro de computo y oficinas de funcionarios.

1.11.4 ESTRATEGIA Y ESTRUCTURA DE GESTIÓN DE LOS SI

La estrategia y estructura organizacional de los Sistemas de Información (SI) se basa en tener un centro de cómputo en donde se encuentran los servidores centrales de la institución con los cuales se brinda las facilidades y servicios a todos los usuarios, rack de comunicaciones donde se encuentren los equipos de comunicación de la institución, además se tiene como principal objetivo de la

SENAMI el usar e implementar sistemas operativos Open Source a nivel de Servidores, estaciones de trabajo y herramientas de escritorio.

Es necesario implementar el centro de cómputo de la institución, el que debe cumplir con ciertos estándares y seguridades necesarias, tales como acceso restringido, extintor de incendios, respaldos, etc.

Una estrategia a implementar es el uso de una Intranet institucional a través de la cual se tenga acceso a todos los servicios institucionales a ser implementados tales como correo, chat institucional, foros, repositorio de información, entre otros.

Una vez implantada la infraestructura tecnológica de la institución debemos continuar con los desarrollos de los sistemas prioritarios de la institución o a su vez adquirirlos.
El portal de la SENAMI se encuentra actualmente alojado en un servidor externo de hosting en Los Ángeles, esta desarrollado en Open Source con la herramienta Joomla.

CAPITULO 2.

DETERMINACIÓN DE LAS MEJORES PRÁCTICAS Y ESTÁNDARES INTERNACIONALES PARA LA GESTIÓN DE LAS TIC'S.

Para muchas empresas, la información y la tecnología que las soportan representan sus más valiosos activos, aunque con frecuencia son poco entendidos. Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

La necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados a TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del gobierno de la empresa. El valor, el riesgo y el control constituyen la esencia del gobierno de TI

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que la TI de la empresa sostiene y extiende las estrategias y objetivos organizacionales.

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI de la empresa sirva como base a los objetivos del negocio. De esta manera, el gobierno de TI facilita que la empresa aproveche al máximo su información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte al del Control interno.

Las organizaciones deben satisfacer la calidad, los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para la TI y decidir qué tipo de gobierno y de control debe aplicar.

2.1 COBIT

(Control Objectives for Information and related Technology)

(COBIT) brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

2.1.1 ÁREAS FOCALES DEL GOBIERNO DE TI

Las áreas focales de gobierno de TI describen los tópicos en los que la dirección ejecutiva requiere poner atención para gobernar la TI en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI. COBIT brinda un modelo de procesos genéricos que representa todos los procesos que normalmente se encuentran en las funciones de TI, ofreciendo un modelo de referencia común entendible para los gerentes operacionales de IT y del negocio. (Figura. 6)

Figura. 6 Áreas focales del Gobierno de TI.

2.1.1.1 Alineación estratégica.

Se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

2.1.1.2 Entrega de valor.

Se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de TI.

2.1.1.3 Administración de recursos.

Se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI:, aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.

2.1.1.4 Administración de riesgos.

Requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del deseo de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

2.1.1.5 Medición del desempeño.

Rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas que se puedan medir más allá del registro convencional.

2.1.2 INTERRELACIONES DE LOS COMPONENTES DE COBIT

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. (Figura. 7)

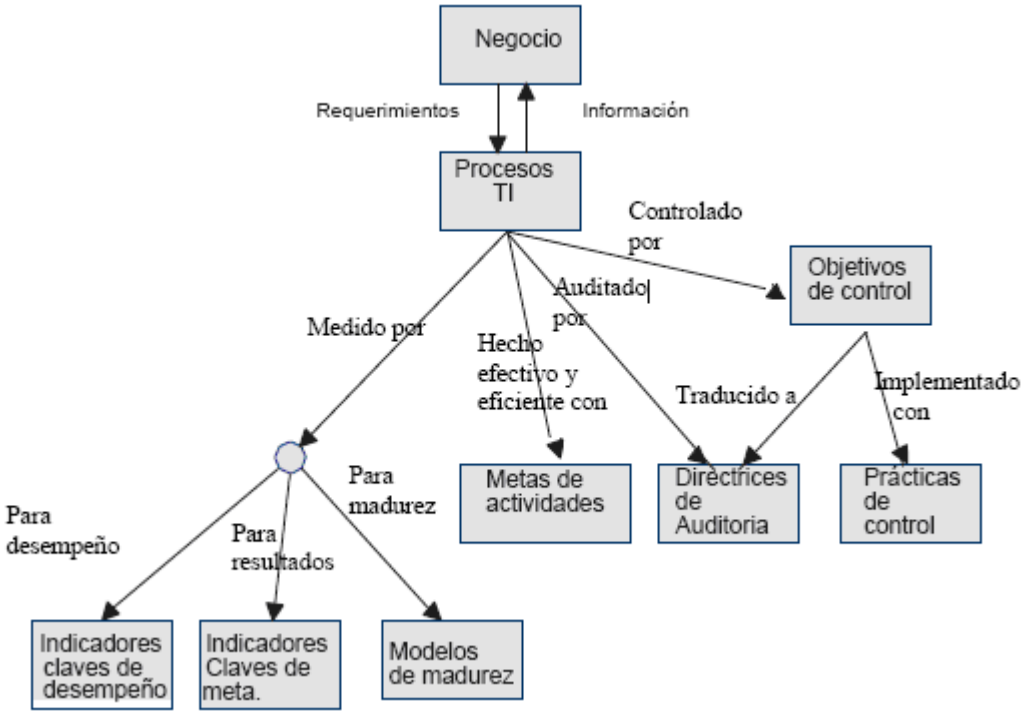


Figura. 7 Interrelaciones de los componentes de COBIT

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre la TI incluyen:

- Mejor alineación, con base en su enfoque de negocios.
- Una visión, entendible para la gerencia, de lo que hace TI.
- Propiedad y responsabilidades claras, con base en su orientación a procesos.
- Aceptación general de terceros y reguladores.
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común.
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI.

2.1.3 MARCO GENERAL DE TRABAJO DE COBIT

2.1.3.1 Orientado al negocio

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los propietarios de los procesos de negocio.

2.1.3.2 Criterios de Información de COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

1. Metas de negocio y de TI.
2. Recursos de TI.
3. Procesos orientados.
4. Basado en Controles.
5. Generadores de mediciones.
6. Modelos de Madurez.
7. Medición del desempeño.

2.1.3.2.1 Metas de negocio y de TI

Mientras que los criterios de información proporcionan un método genérico para definir los requerimientos del negocio, la definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas. Cada empresa usuaria de TI, habilita las iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI.

Si se pretende que la TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio (el cliente) y un claro entendimiento para TI, de cómo y qué debe entregar (el proveedor). La Figura 8 ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos para su uso de iniciativas facilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de la TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar de forma exitosa la parte que le corresponde a TI de la estrategia empresarial. Todos estos objetivos se deben expresar en términos de negocios significativos para el cliente, y esto, combinado con una alineación efectiva de la jerarquía de objetivos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio.

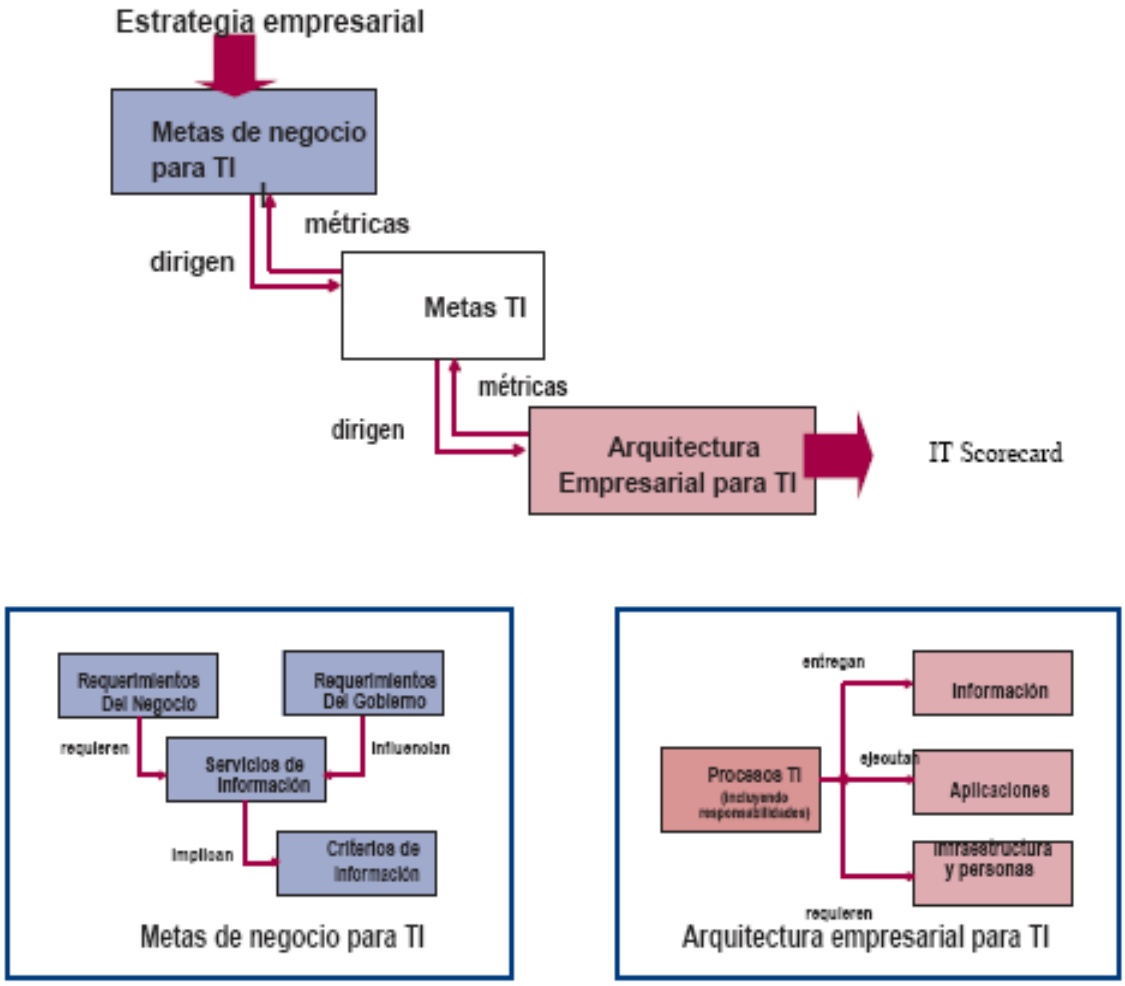


Figura. 8. Definiendo metas de TI y arquitectura empresarial para TI

2.1.3.2.2 Recursos de TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI. (Figura. 9).

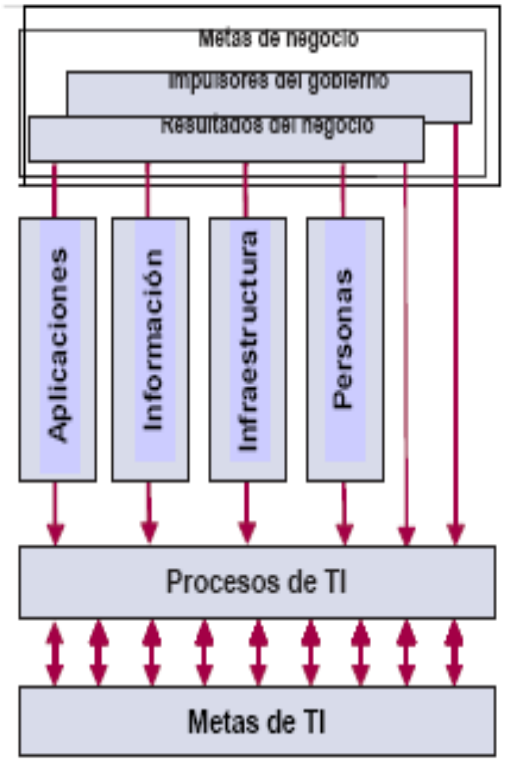


Figura. 9 Administración de los recursos de TI para garantizar las metas de TI

2.1.3.2.3 Procesos orientados

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

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir en el **Anexo A**.

2.1.3.2.4 Basado en Controles

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

2.1.3.2.5 Generadores de mediciones

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa.

La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora.

2.1.3.2.6 Modelos de Madurez

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que se considere qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información.

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método gráfico de presentación (Figura. 10).

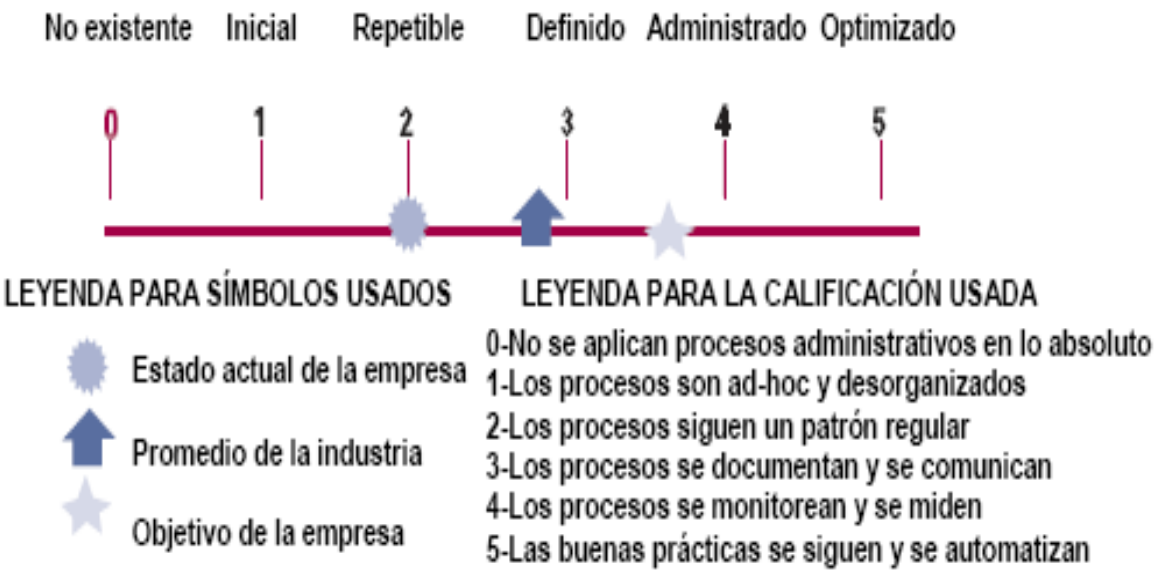


Figura. 10 Representación gráfica de los modelos de madurez

La capacidad, el desempeño y el control son dimensiones de la madurez de un proceso. (Figura. 11).

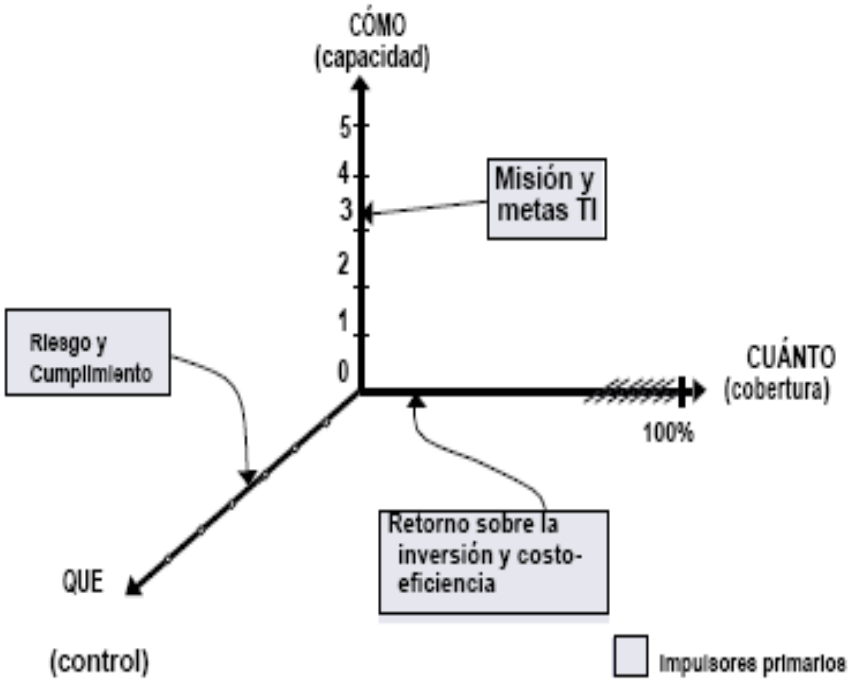


Figura. 11 Las tres dimensiones de la madurez

2.1.3.2.7 Medición del desempeño.

Las métricas y las metas se definen en COBIT a tres niveles:

- Las metas y métricas de TI que definen lo que el negocio espera de TI (lo que el negocio usaría para medir a TI).
- Metas y métricas de procesos que definen lo que el proceso de TI debe generar para dar soporte a los objetivos de TI (cómo sería medido el propietario del proceso de TI).
- Métricas de desempeño de los procesos (miden qué tan bien se desempeña el proceso para indicar si es probable alcanzar las metas).

Los indicadores clave de metas (KGI) definen mediciones para informar a la gerencia—después del hecho—si un proceso TI alcanzó sus requerimientos de negocio, y se expresan por lo general en términos de criterios de información:

- Disponibilidad de información necesaria para dar soporte a las necesidades del negocio.
- Ausencia de riesgos de integridad y de confidencialidad.
- Rentabilidad de procesos y operaciones.
- Confirmación de confiabilidad, efectividad y cumplimiento.

Los indicadores clave de desempeño (KPI) definen mediciones que determinan qué tan bien se está desempeñando el proceso de TI para alcanzar la meta. Son los indicadores principales que indican si será factible lograr una meta o no, y son buenos indicadores de las capacidades, prácticas y habilidades. Miden las metas de las actividades, las cuales son las acciones que el propietario del proceso debe seguir para lograr un efectivo desempeño del proceso.

Las métricas efectivas deben tener las siguientes características:

- Una alta proporción entendimiento-esfuerzo (esto es, el entendimiento del desempeño y del logro de las metas en contraste con el esfuerzo de lograrlos).
- Deben ser comparables internamente (esto es, un porcentaje en contraste con una base o números en el tiempo).

- Deben ser comparables externamente sin tomar en cuenta el tamaño de la empresa o la industria.
- Es mejor tener pocas métricas (quizá una sola muy buena que pueda ser influenciada por distintos medios) que una lista más larga de menor calidad.
- Debe ser fácil de medir y no se debe confundir con las metas.

La figura. 12 ilustra la relación entre los procesos, TI y las metas del negocio, y entre las diferentes métricas, con ejemplo tomados de DS5 Garantizar la seguridad de los sistemas.

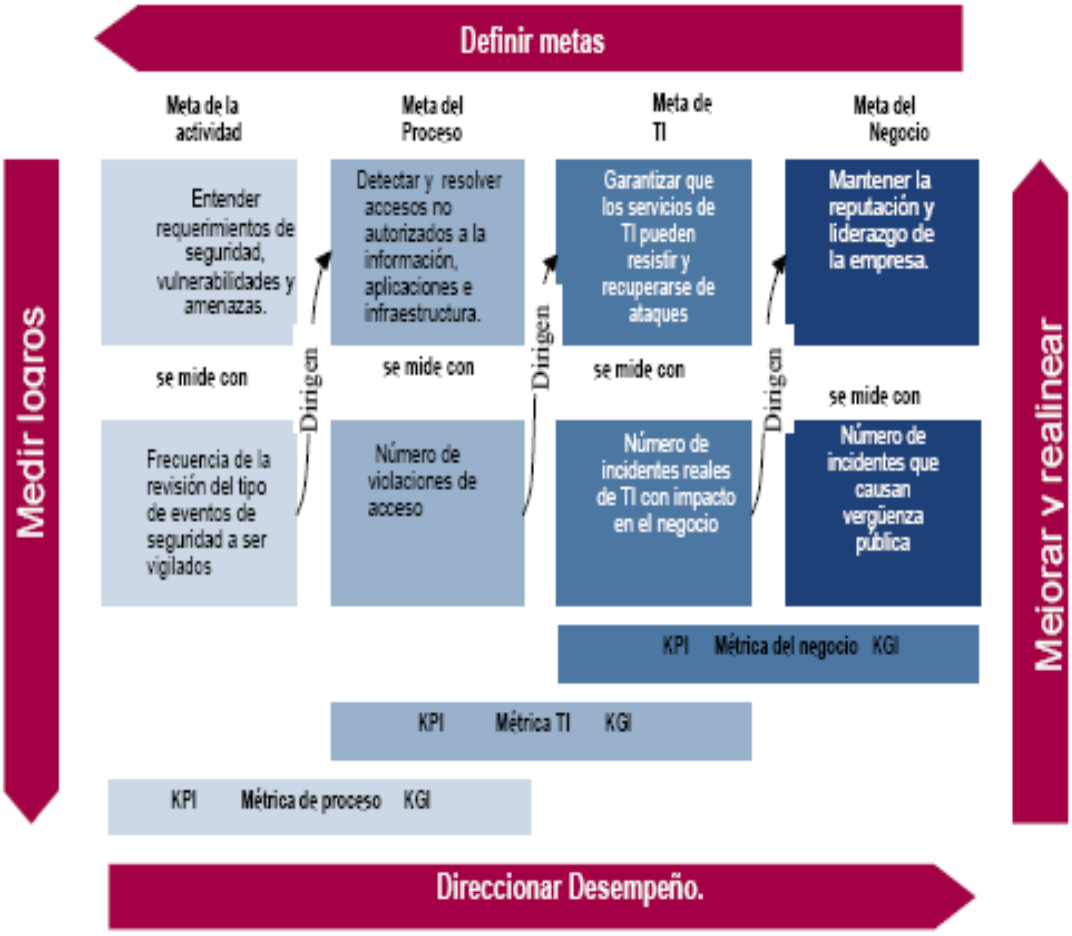


Figura. 12 Relación entre proceso, metas y métricas (DS5)

2.1.4 EL MODELO DEL MARCO DE TRABAJO COBIT

El marco de trabajo COBIT, por lo tanto, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicio de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las métricas KGI y KPI de COBIT. (Figura. 13).

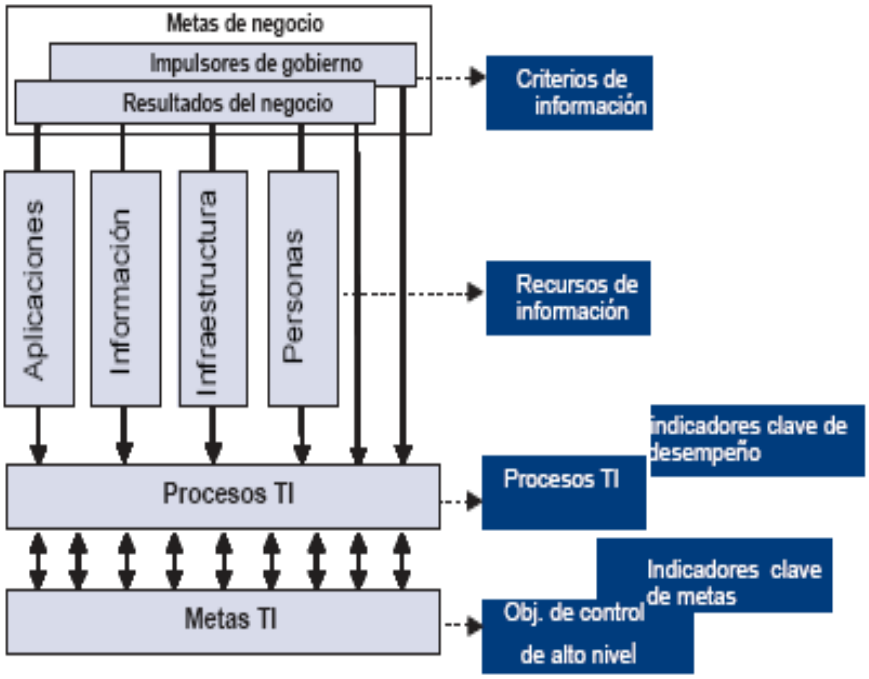


Figura. 13 Administración, control, alineación y monitoreo COBIT

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT (Figura. 14)

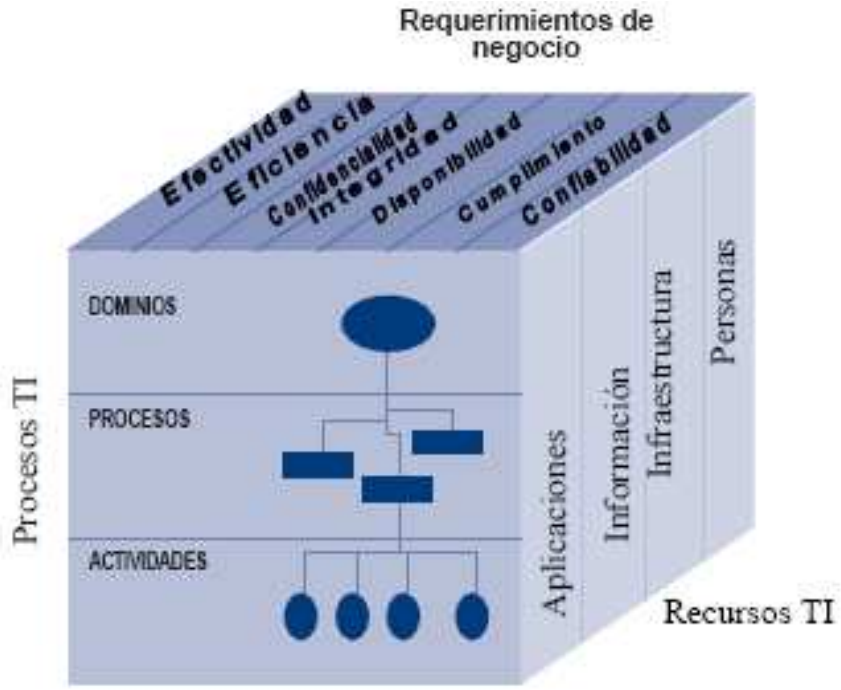


Figura. 14 El cubo COBIT

En detalle, el marco de trabajo general COBIT se muestra gráficamente en la figura 15, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

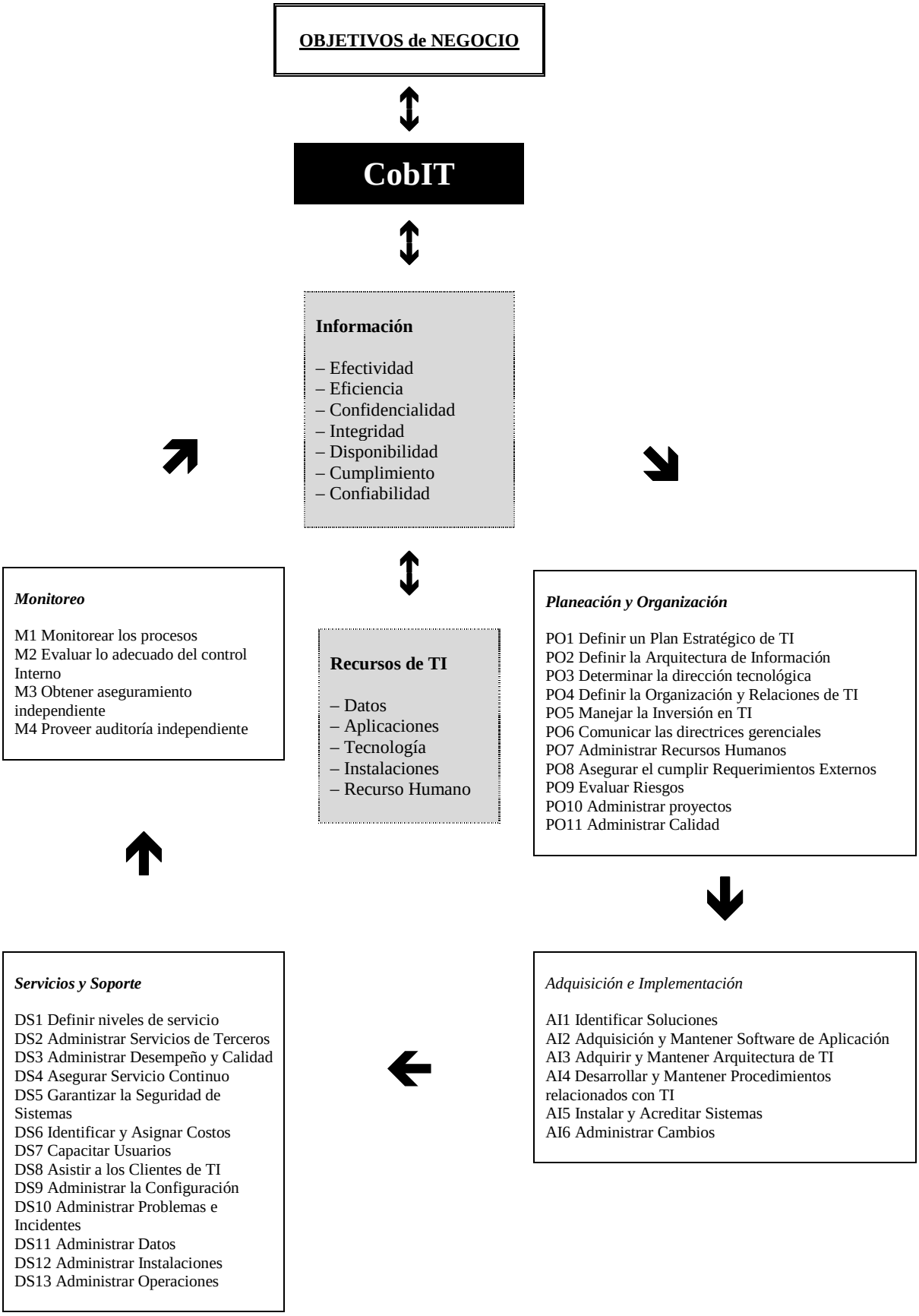


Figura.15 Marco de Trabajo General de COBIT

2.2 ITIL

(IT Infrastructure Library)

ITIL (IT Infrastructure Library) es el marco de procesos de Gestión de Servicios de TI más aceptado. ITIL proporciona un conjunto de mejores prácticas, extraídas de organismos punteros del sector público y privado a nivel internacional, que han sido recogidas por la Oficina Gubernativa de Comercio Británica (OGC, Office of Goverment Comerce).

Este framework (o marco de procesos) es utilizado por cientos de organizaciones en el mundo y ha sido desarrollado reconociendo la dependencia creciente que tienen éstas en la tecnología para alcanzar sus objetivos.

En la actualidad, las empresas están haciendo frente a una enorme presión dirigida hacia la reducción de costes, a una fortísima competencia, a unos recursos cada vez más escasos y a continuos cambios en la manera de operar.

En este contexto, la excesiva complejidad de los sistemas y de su explotación se debe eliminar, convirtiendo una posible debilidad en una fortaleza que dé paso a una nueva ventaja competitiva.

En la empresa actual, los resultados de negocio suelen estar ligados al uso de las Tecnologías de la Información. La coordinación de estas tecnologías a través de todos los eslabones de la cadena de valor existente, ha pasado a ser una condición necesaria para alcanzar el éxito. Los beneficios obtenidos de los procesos de Prestación de Servicios garantizan esta coordinación a largo plazo (Figura. 16)

Figura. 16. Visión empresa

2.2.1 BENEFICIOS DE LA GESTIÓN DE SERVICIOS DE TI

- Maximizar la calidad del servicio apoyando al negocio de una manera fiable.
- Visión clara de la capacidad del departamento de TI.
- Información precisa de qué cambios producirán más beneficios.
- Mayor adaptabilidad de TI al negocio.
- Maximizar la satisfacción en el trabajo mediante una mayor comprensión de las expectativas y capacidades del servicio.
- Aumentar la satisfacción del cliente como proveedores de servicios.
- Minimizar el tiempo del ciclo de cambios y mejorar los resultados de las métricas.
- Toma de decisión en base a indicadores de TI y de negocio.

2.2.2 GESTIÓN DE SERVICIOS ITIL

Los procesos de Gestión de Servicios son el corazón de ITIL, y pueden subdividirse en dos áreas bien diferenciadas.

El Soporte a los Servicios generalmente se concentra en las operaciones cotidianas, así como en dar soporte a los servicios de TI. En cambio, la Prestación de Servicios se ocupa de la planificación a largo plazo y del perfeccionamiento de la provisión de estos servicios. (Figura.17)

Soporte a los Servicios	Prestacion de Servicios
Service Desk *	
Gestión de las Incidencias	Gestión de Nivel de Servicio
Gestión de Problemas	Gestión Financiera para Servicios de TI
Gestión de la Configuración	Gestión de la Capacidad
Gestión de Cambios	Gestión de la Continuidad
Gestión de Versiones	Gestión de la Disponibilidad

Figura. 17 Gestión de Servicios ITIL

2.3 ISO 20.000

La nueva norma se basa en la norma británica BS 15000 y está estrechamente ligada al modelo ITIL® (IT Infrastructure Library). La ISO 20.000 es un código que proporciona las bases para medir y validar el éxito de una organización a la hora de implementar las buenas prácticas definidas por ITIL. Las compañías que cumplan o se estén preparando (Figura. 18)

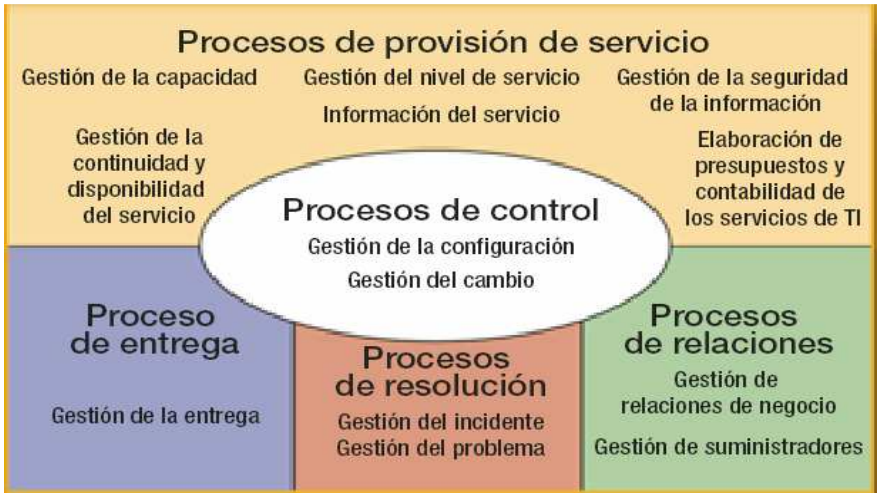


Figura. 18. Procesos de gestión de servicios de la norma ISO 20.000

2.3.1 ISO 20.000 Y SU RELACIÓN CON ITIL

ISO 20000 está alineado con el marco de trabajo de la Biblioteca de Infraestructura de TI (ITIL) definido en los volúmenes de Soporte de Servicio (2000) y provisión de Servicio (2001). ITIL es un conjunto de mejores prácticas, mientras que ISO 20000 es un conjunto formal de especificaciones cuyo cumplimiento debería ser perseguido por los proveedores de servicio: ser capaces de proveer servicios de alta calidad.

Aplicar las mejores prácticas de la Biblioteca de Infraestructura de TI ayudará al proveedor de servicio a alcanzar la calidad en la gestión de servicio requerida por ISO 20000. (Figura. 19).

Figura. 19 ISO 20.000 y su relación con ITIL

Del Análisis y estudio realizado creemos que la Dirección de Gestión Tecnológica debe enmarcarse con los estándares de las mejores prácticas, es decir el Gobierno de TI con COBIT y los procesos de Gestión de Servicios con ITIL.

CAPITULO 3.

PROPUESTA DE GESTIÓN DE LAS TIC'S EN LA SENAMI

La presente propuesta de gestión de las TIC's en la SENAMI se fundamenta en los dos principales modelos de Gestión en TIC's que son ITIL y COBIT.

3.1 PROCESO DE GESTIÓN TECNOLÓGICA

3.1.1 OBJETIVO.

Administrar, apoyar y proveer de servicios y productos tecnológicos informáticos a los usuarios internos y externos de la SENAMI, con oportunidad, seguridad, eficiencia y eficacia.

3.1.2 POLÍTICAS GENERALES.

- Disponibilidad del personal informático a cualquier hora y por cualquier medio.
- Capacitación constante a todo el personal de la institución en las TICS.
- Asesorar a los demás unidades en temas relacionados con las Tecnologías de la Información y Comunicación.

3.1.3 DEFINICIONES.

Tecnologías de la Información y Comunicación TICs	La constituyen en forma general todo el software, hardware, personal y servicios relacionados con el procesamiento de la información.
Aplicativo	Software especializado en automatizar una o varias funciones de un negocio, generalmente construido sobre una plataforma de base de datos.
Intranet	Aplicación de la plataforma de Internet para manejar información en el contexto interno de la empresa únicamente.

Performance	Rendimiento. Velocidad de ejecución o tiempo de respuesta de una aplicación o servicio de información.
Contingencia	Situación fortuita que atenta contra la continuidad de la operación de una empresa.

3.1.4 ESTRUCTURA.

El proceso de Gestión Tecnológica estará conformado por cuatro subprocesos: (Figura 20. Estructura Gestión Tecnológica)

- Gestión Estratégica Tecnológica,
- Administración de Aplicaciones,
- Administración de Redes y Comunicaciones
- Administración de Infraestructura Tecnológica.

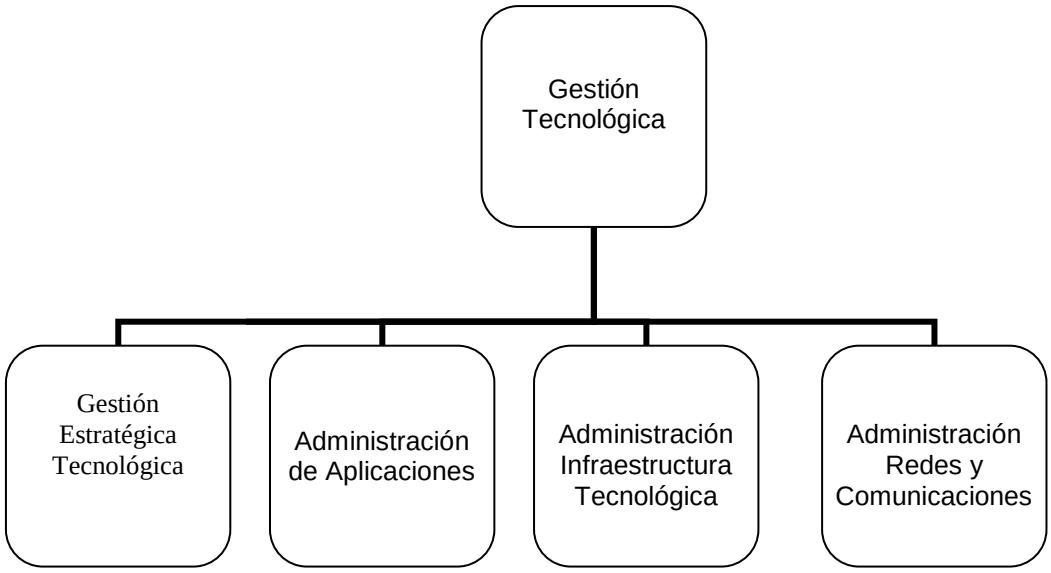


Figura 20. Estructura Gestión Tecnológica

3.2 SUBPROCESO: GESTIÓN ESTRATÉGICA TECNOLÓGICA

3.2.1 OBJETIVO.

Desarrollar e implementar planes, políticas, estándares y procedimientos que guiarán las actividades de TIC.

3.2.2 PRODUCTOS.

- Plan Estratégico Informático global a mediano y largo plazo.
- Definición de Metodologías que normarán los diferentes procesos.
- Planes Operativos para la Unidad de Tecnología.
- Administración de Proyectos
- Seguridades Físicas
- Plan de Contingencias para la organización.
- Plan de Manejo de Riesgos
- Auditoria Informática

3.2.3 POLÍTICAS

- Actualización de las tendencias tecnológicas en el área Informática.
- Aplicar nuevas tecnologías en la institución.
- Apoyar iniciativas tecnológicas internas de las otras unidades departamentales.
- Administrar proyectos tecnológicos.
- Contar con el aval de las altas autoridades para los diferentes proyectos tecnológicos.
- Contar con un Plan Estratégico alineado con los objetivos estratégicos de la institución.
- Difundir toda política y procedimiento a toda la institución.
- Controlar el cumplimiento de las políticas y procedimientos.
- Ejecutar auditorias anuales de cumplimiento de políticas y procedimientos en toda la institución.
- Generar recomendaciones para mejorar la gestión tecnológica dentro de la institución.

- Revisar y actualizar anualmente las políticas y procedimientos.

3.2.4 PROCEDIMIENTOS

Diagrama de Flujo **(Anexo B)**

3.2.5 DOCUMENTOS

Nombre	Código	Llenado / elaborado por	Destinatario	Archivo Activo	Archivo Pasivo
Plan Estratégico Tecnológico	GT001	Director de GT (Gestión Tecnológica)	Subsecretario General Archivo de Sistemas Informáticos	1 año	2 años
Cartera de Proyectos	GT002	Director de GT	Subsecretario General Técnicos de Hardware/ Software Archivo de Sistemas Informáticos	1 año	2 años
Solicitud de aprobación de proyecto	GT003	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	1 año	--
Plan de Contingencias	GT004	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	Período de Vigencia	1 año

Documentación de seguimiento de proyectos	GT005	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	Período de Vigencia	1 año
Informe anual de actividades	GT006	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Plan de mejoras a los servicios	GT007	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Solicitud de auditoria externa	GT008	Director de GT	Auditor externo Archivo de Sistemas Informáticos	1 año	1 año
Documentación de auditoria	GT009	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Notificación de incumplimiento	GT010	Director de GT	Subsecretario General Cliente interno Archivo de Sistemas Informáticos	1 año	1 año

Política	GT011	Director de GT	Archivo de Sistemas Informáticos	Período de Vigencia	1 año
Procedimiento	GT012	Director de GT	Archivo de Sistemas Informáticos	Período de Vigencia	1 año
Documentación de metodología	GT013	Director de GT	Archivo de Sistemas Informáticos	Vigencia	1 año
Notificación de negación de proyecto	GT014	Subsecretario General/ Comité ejecutivo	Director de GT Archivo de Sistemas Informáticos	1 año	1 año
Notificación de aprobación de proyecto	GT015	Subsecretario General/ Comité ejecutivo	Director de GT. Archivo de Sistemas Informáticos	1 año	1 año

3.2.6 INDICADORES DE DESEMPEÑO DEL SUBPROCESO

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Número de proyectos propuestos	Establece la cantidad de nuevos proyectos propuestos en un período de tiempo.	Productividad	Número de nuevos proyectos propuestos en el período de tiempo medido.	Documentación de nuevos proyectos	Director de GT	Anual
Porcentaje	Establece la	Productivi	(Número de	Document	Director de	Anual

de nuevos productos o proyectos implementados	efectividad en la implantación de proyectos.	dad	proyectos implementados/ Número total de proyectos propuestos en el período) *100	ación de proyectos propuestos (cartera de proyectos). Documentación de proyectos en ejecución y ejecutados.	GT	
Costo de Tecnología por empleado	Establece el esfuerzo económico que representa para la institución la tecnología de información por cada empleado.	Calidad	Costo anual de HW, SW, comunicaciones y personal de Sistemas / Número de empleados de la SENAMI	Cuentas contables de gastos de TI, Información de Recursos Humanos	Director de GT	Anual
Costo total de tecnología de información	Establece el porcentaje que representa el costo de	Calidad	Costo anual de HW, SW, comunicaciones y personal de Sistemas /	Cuentas contables de gastos de TI y de operación	Director de GT	Anual

frente al costo total de operación	tecnología de información frente a los costos totales de operación de la institución.		Costo total de operación	.		
Porcentaje de técnicos de sistemas sobre staff total	Establece el porcentaje que representa el número de empleados del área de Servicios Informáticos frente al total de empleados de la Institución.	Calidad	(Número de empleados de Servicios Informáticos / Número de empleados totales) * 100	Información de Recursos Humanos de la SENAMI	Director de GT	Anual

3.3 SUBPROCESO: ADMINISTRACIÓN DE APLICACIONES

3.3.1 DEFINICIÓN

Subproceso en el que se desarrollan, implantan y mantienen aplicativos, incluyendo pruebas, capacitación y generación de documentación. Incluye la selección y customización de aplicativos requeridos por la organización, que sean adquiridos de proveedores externos.

3.3.2 ALCANCE

Aplica desde la detección o recepción de requerimiento hasta la firma del acta de entrega-recepción.

3.3.3 REFERENCIAS

- Plan Estratégico Tecnológico.
- Reporte de Cumplimiento e Incumplimiento.
- Políticas, Procedimientos y Metodologías.
- Presupuesto Institucional.

3.3.4 POLÍTICAS

- Todo requerimiento deberá ser canalizado a través de Soporte a Usuarios.
- El Director de GT y el Jefe del área correspondiente, deben aprobar todas las solicitudes de cambio a aplicativos, excepto las relacionadas con errores de los aplicativos.
- El Jefe del área afectada debe evaluar que las solicitudes de cambio tengan una causa justificable para el proceso y el Director de GT debe determinar si el requerimiento es técnicamente factible.
- Los requerimientos de aplicativos podrán ser atendidos ya sea mediante un desarrollo propio o mediante la selección de una solución ya desarrollada adecuada para la Institución.
- Para el caso del desarrollo propio de un aplicativo, deberá designarse un equipo de usuarios el mismo que aprobará las diferentes etapas durante la implementación de la solución.
- Para la selección de aplicativos ya desarrollados se deberá iniciar un proyecto de selección formal. El proyecto deberá contar con la participación de un equipo compuesto por el coordinador del área beneficiaria, el Director de Información y un grupo de los futuros usuarios del sistema.
- Para garantizar la calidad de un aplicativo, sea este desarrollado en casa o adquirido a empresas externas, se deberá crear un equipo de pruebas que incluirá a los principales usuarios del producto. El equipo de pruebas tendrá la potestad de aceptar o rechazar, mediante actas de entrega – recepción, la solución provista de acuerdo a una evaluación de cumplimiento de sus requerimientos.

- Todo aplicativo desarrollado en la Institución deberá estar soportado por la documentación pertinente para cada etapa de ejecución del proyecto.
- En forma previa a la aceptación de un sistema adquirido a terceros, se deberá recibir a conformidad toda la documentación técnica y de usuario.
- En forma previa a la aceptación de un sistema se deberán haber cumplido todas las horas de capacitación pactadas a satisfacción de los usuarios beneficiarios.
- La finalización de un proyecto se formalizará a través de una “acta de entrega - recepción de aplicación o requerimiento” que establecerá la conformidad del usuario en cuanto a la funcionalidad de la aplicación.

3.3.5 PROCEDIMIENTOS

Diagrama de Flujo (**Anexo C**)

3.3.6 DOCUMENTOS

Nombre	Código	Llenado por	Destinatario	Archivo Activo	Archivo Pasivo
Notificación de negación de requerimiento	GT025	Subsecretario General	Técnico de Software Director de GT	1 año	1 año
Propuesta técnica y económica	GT036	Técnico de Software	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Documentación de análisis	GT037	Técnico de Software	Cliente interno Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Documentación de diseño	GT038	Técnico de Software	Cliente interno Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Documentación de la aplicación	GT039	Técnico de Software	Cliente interno Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Plan de	GT040	Equipo de	Director de GT	1 año	---

pruebas		pruebas	Archivo de Sistemas Informáticos	luego de puesta en marcha	
Acta de entrega / recepción de aplicación o ajuste	GT041	Equipo de selección / implantación de aplicaciones	Director de GT Cliente interno Archivo de Sistemas Informáticos	1 año	1 año
Solicitud de aprobación de ajustes	GT042	Proveedor	Cliente interno Archivo de Sistemas Informáticos	1 año	1 año
Acta de aprobación de análisis	GT043	Cliente Interno	Cliente interno Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Acta de aprobación de diseño	GT044	Cliente Interno	Cliente interno Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Cronograma de desarrollo / ajuste de aplicación	GT045	Técnico de Software	Gerente de proyecto Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Notificación de aprobación de requerimiento	GT026	Subsecretario General / Comité ejecutivo	Técnico de Software Director de Información	1 año	1 año
Requerimiento de instalación / actualización de aplicaciones y software base	GT046	Equipo de selección / implantación de aplicaciones	Técnico de Software Archivo de Sistemas Informáticos	1 año	1 año
Cronograma de selección e implantación de aplicación externa	GT047	Equipo de selección / implantación de aplicaciones Proveedor	Proveedor Archivo de Sistemas Informáticos	1 año	1 año
Informe técnico - económico	GT048	Equipo de selección / implantación de aplicaciones	Subsecretario General Archivo de Sistemas Informáticos	Vigencia de la aplicación	1 año
Requerimiento informático	GT027	Técnico de Software	Intranet de SENAMI	1 año	---
Solicitud de creación /	GT024	Técnico de Software	Director de Información	1 año	1 año

ajuste de política o procedimiento			Archivo de Sistemas Informáticos		
Requerimiento de capacitación	GT049	Equipo de selección / implantación de aplicaciones	Analista de RRHH Archivo de Sistemas Informáticos	1 año	1 año

3.3.7 INDICADORES DE DESEMPEÑO DEL SUBPROCESO

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Número de errores de aplicaciones en Producción reportados	Establece la cantidad de errores reportados con relación a las aplicaciones en producción	Calidad	Número de casos reportados a Help Desk relacionados con errores de las aplicaciones en producción	Aplicación de requerimiento informático	Técnico de Software	Anual
Número de errores detectados durante las pruebas de aplicaciones	Establece la calidad del aplicativo probado.	Calidad	Número de errores detectados durante las pruebas de un aplicativo.	Documentación de la ejecución del plan de pruebas	Técnico de Software	Anual

3.4 SUBPROCESO: ADMINISTRACIÓN DE INFRAESTRUCTURA TECNOLÓGICA

3.4.1 OBJETIVO.

Unidad que se encarga de desarrollar la plataforma tecnológica central, que incluye el hardware y el software base para soportar los aplicativos desarrollados o adquiridos por la organización, bajo los lineamientos del plan estratégico informático.

Este proceso consta de los siguientes subprocesos:

Administración de Hardware
Administración de Software Base y Aplicativos
Administración de Seguridades
Soporte a Usuarios (Help Desk)

3.4.2 PRODUCTOS.

Administración de Hardware.
Administración de Sistemas Operativos
Administración de bases de datos u otras plataformas de software
Puesta en producción de aplicativos.
Asignación y control de seguridades lógicas tanto a nivel de red como de sistemas operativos y aplicativos.
Monitoreo y gestión de disponibilidad de los servicios tecnológicos.
Manejo de backups y recuperación de contingencias.

3.4.3 POLÍTICAS

- Disponibilidad de la infraestructura tecnológica.
- Brindar el soporte técnico especializado a toda la institución.
- Contar con el respectivo licenciamiento del software base y aplicativos.
- Contar con un registro actualizado de licencias instaladas.
- Aprobar cualquier cambio que afecte a un servicio o computadoras.
- Controlar el software base y aplicativos en la institución.
- Controlar el acceso al Centro de Cómputo.
- Monitoreo constante de la infraestructura tecnológica a disposición.
- Controlar el acceso de los perfiles de los usuarios.
- Cambiar las contraseñas de los usuarios cada seis meses.
- Cambiar las contraseñas de los servidores y servicios cada año.
- Mantener un registro seguro de las contraseñas de los servicios y servidores.
- Comunicar cualquier manipulación dolosa de los servicios informáticos.
- Controlar que todas las estaciones tengan activadas la protección de pantalla (5 minutos).

- Mantener respaldos de información (backups) con periodicidad diaria, semanal y mensual.
- Mantener un sistema de respaldos de toda la información en la institución.
- Proteger los respaldos guardados en cintas en una caja fuerte de Sistemas y en una caja fuerte de una institución externa contratada.
- Mantener un registro de todos los respaldos de información.
- Contar con un software de protección Antivirus en los servidores y estaciones de trabajo.
- Realizar mantenimientos preventivos de Software y Hardware. Semestral para las estaciones de trabajo y anual para los servidores.

3.4.3.1 Subproceso Administración de Hardware

3.4.3.1.1 Procedimiento

Diagrama de Flujo (**Anexo D**)

3.4.3.1.2 Documentos

Nombre	Código	Llenado por	Destinatario	Archivo Activo	Archivo Pasivo
Plan de proyecto	GT016	Técnico de Hardware	Archivo de Sistemas Informáticos	1 año	1 año
Documentación de seguimiento de proyectos	GT005	Técnico de Hardware	Responsable de proceso Archivo de Sistemas Informáticos	1 año	1 año
Inventario de Hardware	GT017	Técnico de Hardware	Archivo de Sistemas Informáticos	Vigencia del inventario	1 año
Requerimiento de ampliación de capacidades	GT018	Director de GT	Subsecretario General Archivo de Sistemas	1 año	1 año

			Informáticos		
Requerimiento de nuevos recursos	GT019	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Solicitud de aprobación de compras	GT020	Director de GT	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Requerimiento de mantenimiento externo	GT021	Técnico de Hardware	Proveedor externo Archivo de Sistemas Informáticos	1 año	---
Bitácora de mantenimiento	GT022	Técnico de Hardware	Archivo de Sistemas Informáticos	Existencia del equipo	---
Informe mensual de actividades y avance de proyecto	GT023	Técnico de Hardware	Director de GT Archivo de Sistemas Informáticos	1 año	---
Solicitud de creación / ajuste de política o procedimiento	GTC024	Técnico de Hardware	Director de GT Archivo de Sistemas Informáticos	1 año	1 año
Pedido de adquisición	INS010	Director de GT	Subproceso de Compras Archivo de	1 año	1 año

			Sistemas Informáticos		
Notificación de negación de requerimiento	GTC025	Subsecretario General	Director de GT Archivo de Sistemas Informáticos	1 año	1 año
Notificación de aprobación de requerimiento	GTC026	Subsecretario General	Director de GT Archivo de Sistemas Informáticos	1 año	1 año
Requerimiento Informático	GTC027	Técnico de Hardware	Intranet de la SENAMI	1 año	---

3.4.3.1.3 Indicadores de Desempeño del Subproceso

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Porcentaje de disponibilidad de equipos	Establece el nivel de disponibilidad de los equipos del centro de cómputo.	Calidad	((Total de horas que debe estar disponible el equipo - Número de horas de falla del equipo) / Total de horas que debe estar disponible el equipo) *100 Indicador a	Bitácora de disponibilidad de servicios	Técnico de Hardware	Anual

			calcularse para cada servidor provisto por el centro de cómputo.			
Número de fallas de hardware	Establece el número de fallas de hardware reportadas o descubiertas en el período de tiempo.	Calidad	Número total de fallas de Hardware en el período de tiempo.	Aplicación de Requerimiento Informático	Técnico de Hardware	Anual

3.4.3.2 Subproceso Administración de Software base y Aplicativos

3.4.3.2.1 Procedimiento

Diagrama de Flujo (**Anexo E**)

3.4.3.2.2 Documentos

Nombre	Código	Llenado por	Destinatario	Archivo Activo	Archivo Pasivo
Plan de proyecto	GT016	Técnico de Software	Archivo de Sistemas Informáticos	1 año	1 año
Documentación de seguimiento de proyecto	GT005	Técnico de Software	Responsable de proceso Archivo de Sistemas Informáticos	Vigencia del proyecto	1 año
Informe de	GT028	Técnico de	Director de GT	Vigencia	1 año

monitoreo		Software	Archivo de Sistemas Informáticos	del proyecto	
Requerimiento de ajuste de política o procedimiento	GT024	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	---
Requerimiento de soporte	GT029	Técnico de Software	Proveedor externo Archivo de Sistemas Informáticos	1 año	---
Inventario de Software	GT030	Técnico de Software	Archivo de Sistemas Informáticos	Vigencia	1 año
Informe mensual	GT031	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	1 año
Requerimiento informático	GT027	Técnico de Software	Intranet de la SENAMI	1 año	---

3.4.3.2.3 Indicadores de Desempeño del Subproceso

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Número de fallas debido a la puesta en producción de	Establece la calidad del trabajo de ajuste y puesta en producción de	Calidad	Número total de fallas producidas como producto de la	Aplicación de Requerimiento Informático	Técnico de Software	Anual

actualización de aplicaciones	mejoras o actualización de versiones de los aplicativos en producción.		actualización de aplicaciones.			
Disponibilidad de las aplicaciones críticas	Establece el porcentaje de disponibilidad de las aplicaciones críticas frente al tiempo total que se espera esté disponible.	Calidad	((Tiempo total de disponibilidad esperado – Tiempo fuera de servicio) / Tiempo total de disponibilidad esperado) * 100 Se debe generar un indicador para cada aplicación crítica.	Bitácora de disponibilidad de servicios	Técnico de Software	Anual

3.4.3.3 Subproceso Administración de Seguridades

3.4.3.3.1 Procedimiento

Diagrama de Flujo (**Anexo F**)

3.4.3.3.2 Documentos

Nombre	Código	Llenado por	Destinatario	Archivo Activo	Archivo Pasivo
Plan de proyecto	GT016	Técnico de Software	Archivo de Sistemas Informáticos	1 año	1 año
Documentación de seguimiento de proyecto	GT005	Técnico de Software	Responsable de proceso Archivo de Sistemas Informáticos	Vigencia del proyecto	1 año
Bitácora de respaldos	GT032	Técnico de Software	Archivo de Sistemas Informáticos	1 año	1 año
Informe de monitoreo	GT033	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	---
Requerimiento de ajuste de política o procedimiento	GT024	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	---
Nota de entrega de medios	GT034	Técnico de Software	Proveedor de caja fuerte externa Archivo de Sistemas Informáticos	1 año	---
Informe mensual	GT031	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	1 año

Informe de solución de contingencia	GT035	Técnico de Software	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Requerimiento informático	GT027	Técnico de Software	Intranet de la SENAMI	1 año	---

3.4.3.3.3 Indicadores de Desempeño del Subproceso

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Número de intentos de violación de seguridades	Establece la exposición detectada con respecto a las seguridades de ingreso a los recursos o servicios.	Calidad	Número de intentos de acceso rechazados en el período de tiempo.	Bitácora de seguridades de Sistema Operativo, de red y de aplicaciones.	Técnico de Software	Anual

3.4.3.4 Subproceso Soporte a Usuarios

3.4.3.4.1 Objetivo.

Subproceso que previene y resuelve problemas de operación y funcionamiento de las soluciones informáticas al servicio de usuarios internos y externos, cumpliendo y midiendo estándares de servicio. Incluye la preparación de las estaciones de trabajo, instalación del software base, aplicaciones cliente y servicios; así como su incorporación física a la red interna, asignación al usuario final y manejo del inventario de estaciones de trabajo.

3.4.3.4.2 Políticas

- Brindar soporte técnico en la jornada de trabajo.
- Solucionar los problemas tecnológicos presentados únicamente si existe el requerimiento por parte del usuario.
- Administrar las cuentas de los usuarios de la institución.
- Gestionar la compra o asignación de recursos informáticos.
- Asignar el mejor mecanismo para solucionar cualquier requerimiento.
- Priorizar la atención de los requerimientos.
- Notificar al usuario sobre la factibilidad y prioridad de un requerimiento.
- Mantener un adecuado control de los equipos informáticos.
- Registrar el movimiento de equipos dentro y fuera de la institución.
- Responsabilizar a los usuarios del equipo informático a su cargo.
- Notificar y Registrar la solución de un requerimiento.

3.4.3.4.3 Procedimiento

Diagrama de Flujo. (**Anexo G**)

3.4.3.4.4 Documentos

Nombre	Código	Llenado por	Destinatario	Archivo Activo	Archivo Pasivo
Requerimiento Informático	GT027	Cliente interno	Intranet de la SENAMI	1 año	---
Requerimiento de soporte	GT053	Director de GT	Proveedor externo Archivo de Sistemas Informáticos	1 año	---
Estadísticas de la gestión de Soporte	GT054	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	1 año

Requerimiento de ajuste a políticas o procedimientos	GT024	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	1 año
Informe trimestral de actividades	GT055	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	1 año

3.4.3.4.5 Indicadores de Desempeño del Subproceso

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Tiempo promedio de solución de requerimiento	Establece el promedio de tiempo en el que se solucionan los requerimientos de soporte	Productividad	Sumatoria (horas para solución de requerimiento) / número de requerimientos.	Aplicación de requerimiento informático	Técnico de software	Anual
Carga de trabajo	Mide el número de requerimientos / técnico que son atendidos por el área	Productividad	Número de requerimientos atendidos/ número de técnicos de sistemas que ejecutan el soporte	Aplicación de requerimiento informático	Técnico de software	Anual

3.5 SUBPROCESO: ADMINISTRACIÓN DE REDES Y COMUNICACIONES

3.5.1 OBJETIVO.

Proceso que se encarga de administrar las redes y comunicaciones. Incluye la tecnología de Internet y la definición de esquemas de seguridad a nivel de redes.

Proceso responsable de planificar, organizar, coordinar y supervisar las actividades de administración de la red LAN y WAN que garantice niveles de funcionamiento óptimo y eficiente.

3.5.2 POLÍTICAS

- Brindar el servicio de redes y comunicaciones en forma constante
- Notificar cualquier actividad de mantenimiento o falla imprevista
- Atender cualquier requerimiento ingresado a través de Soporte a Usuarios.
- Aprobar cualquier cambio que afecte a los servicios de red o comunicaciones.
- Monitorear permanentemente el funcionamiento de los recursos de redes y comunicaciones.
- Optimizar el funcionamiento de los recursos de redes y comunicaciones.

3.5.3 PROCEDIMIENTO

Diagrama de Flujo (**Anexo H)**

3.5.4 DOCUMENTOS

Nombre	Código	Llenado por	Destinatario	Archivo Activo	Archivo Pasivo
Plan de proyecto	GT016	Técnico de Software	Archivo de Sistemas Informáticos	1 año	1 año
Documentación de seguimiento de	GT005	Técnico de Software	Responsable de proceso Archivo de	1 año	1 año

proyecto			Sistemas Informáticos		
Informe mensual	GT031	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	---
Informe de monitoreo/ajuste	GT050	Técnico de Software	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Requerimiento de mantenimiento externo	GT021	Técnico de Software	Proveedor externo Archivo de Sistemas Informáticos	1 año	---
Bitácora de mantenimiento	GT022	Técnico de Software	Archivo de Sistemas Informáticos	1 año	2 años
Diagrama de red	GT051	Técnico de Hardware	Archivo de Sistemas Informáticos	Vigencia	1 año
Informe de monitoreo/ajuste de seguridades	GT052	Técnico de Software	Subsecretario General Archivo de Sistemas Informáticos	1 año	1 año
Solicitud de creación / ajuste de política, procedimiento	GT024	Técnico de Software	Director de GT Archivo de Sistemas Informáticos	1 año	1 año

Requerimiento Informático	GT027	Técnico de Software	Intranet de la SENAMI	1 año	---

3.5.5 INDICADORES DE DESEMPEÑO DEL SUBPROCESO

Nombre del indicador	Descripción	Tipo	Forma de cálculo	Fuente	Responsable de cálculo	Periodicidad
Porcentaje de disponibilidad de servicios de red y comunicaciones	Establece el porcentaje de disponibilidad de los servicios de red y enlaces de comunicaciones.	Calidad	((Número total de horas que debe estar disponible el servicio - Número de horas sin servicio) / Número total de horas que debe estar disponible el servicio) * 100 Se debe obtener un indicador por cada servicio de red o comunicaciones.	Bitácora de disponibilidad de servicios	Técnico de Software	Anual
Número de fallas en	Establece el número de	Calidad	Número total de fallas en	Aplicación de	Técnico de Software	Anual

redes y comunicaciones	fallas en los dispositivos de redes y comunicaciones.		dispositivos de redes y comunicaciones en el período medido.	requerimiento informático		

3.6 RECURSOS HUMANOS

La Dirección de Gestión Tecnológica deberá contar con 3 personas técnicas en el área de sistemas o tecnologías de información, para desempeñar en las funciones de Director de Gestión Tecnológica, Técnico de Software y Técnico de Hardware.

3.6.1 CARGO: DIRECTOR DE GESTIÓN TECNOLÓGICA.

Reporta a: Subsecretaria General
Unidad de pertenencia: Dirección de Gestión Tecnológica

3.6.1.1 Definición del cargo, roles y responsabilidades:

El cargo: Director de Gestión Tecnológica es responsable - ejecutor de los siguientes sub-procesos:

Gestión estratégica de TIC,

Administración de infraestructura tecnológica,

Administración de redes y comunicaciones,

Administración de aplicaciones.

Soporte a usuarios.

Como administrador: planifica, organiza, asigna, coordina, controla y ajusta las diversas actividades alineándolas a la estrategia institucional; interviene pro-activamente en la actualización y mejora de los procesos que le competen; atiende y responde con prontitud a los pedidos específicos de sus superiores.

3.6.1.2 Requisitos que el Cargo Exige:

Titulo Académico: Ingeniería de Sistemas ó similares.

Experiencia requerida externa: 5 años

Experiencia requerida interna: 2 años

Otros: Poseer una maestría con relación al título académico

3.6.1.3 Competencias requeridas para los cargo tipo

Relación interpersonal efectiva

Juicio critico

Capacidad de resolución de problemas

Trabajo en equipo

3.6.1.4 Funciones y Responsabilidades del Cargo

Las principales actividades desarrolladas por este cargo en los procesos de la Cadena de Valor y los procesos de Soporte serán:

Proceso: Gestión Estratégica de T.I.C.

- Recepción de requerimientos y necesidades internas percibidas
- Recepción de necesidades para prestación de servicios.
- Análisis de tendencias tecnológicas y factibilidad técnica de necesidades percibidas
- Planificación / revisión presupuestaria
- Creación o ajuste de Plan Estratégico Tecnológico
- Creación o ajuste de Cartera de Proyectos
- Generación de solicitud de aprobación de proyecto
- Creación o ajuste de Plan de Contingencias
- Ejecución de seguimiento de proyectos
- Planificación de mejora a los servicios
- Elaboración de informe anual
- Creación / actualización de política
- Creación / actualización de procedimiento
- Publicación / diseminación de política, procedimiento o metodología a través de la Intranet

- Generación de solicitud de auditoria externa
- Ejecución de auditoria de cumplimiento de políticas, procedimientos y metodologías
- Generación de notificación de incumplimiento

Proceso: Administración de Infraestructura Tecnológica

Subproceso: Administración de Hardware

- Análisis de capacidades actuales de servidores y estaciones de trabajo
- Generación de justificación y requerimiento de ampliación de capacidades.
- Generación de justificación y requerimiento de nuevos recursos
- Generación de solicitud de aprobación de nuevos recursos
- Generación de pedido de adquisición

Subproceso: Administración de seguridades

- Revisión de plan de contingencias
- Generación de plan de acción

Subproceso: Soporte a Usuarios

- Análisis del requerimiento
- Registro de requerimiento negado
- Notificación a cliente interno de requerimiento negado
- Ruteo de requerimiento para infraestructura
- Ruteo de requerimiento para redes o comunicaciones
- Ruteo de requerimiento para desarrollo de aplicativos
- Generación de requerimiento para soporte externo
- Verificación de solución

Proceso: Administración de Aplicaciones

- Participación en Equipo de Pruebas
- Participación en Equipo de Selección / implantación de aplicaciones
- Aprobación / negación del análisis
- Aprobación / negación del diseño

- Aprobación / negación de ajustes

3.6.2 CARGO: TÉCNICO DE SOFTWARE.

Reporta a: Director de Gestión Tecnológica
Unidad de pertenencia: Dirección de Gestión Tecnológica

3.6.2.1 Definición del cargo, roles y responsabilidades:

El cargo: Técnico de Software es el ejecutor de los siguientes subprocesos: Gestión estratégica de TICs, Administración de infraestructura tecnológica, Parametrización de software, desarrollo y replicación de bases de datos. Es el responsable por la correcta utilización de software Institucional y que todas sus licencias estén al día.

Como técnico – administrador: planifica, organiza, asigna, coordina, controla y ajusta las diversas actividades de su unidad alineándolas a la estrategia de la Gerencia de Servicios Corporativos; interviene pro-activamente en la actualización y mejora de los procesos que le competen; atiende y responde con prontitud a los pedidos específicos de sus superiores.

3.6.2.2 Requisitos que el Cargo Exige:

Titulo Académico: Ingeniería de Sistemas ó similares.
Experiencia requerida externa: 4 años
Experiencia requerida interna: 2 años
Otros: Certificaciones con relación al título académico y funciones que realiza.

3.6.2.3 Competencias requeridas para los cargo tipo

Relación interpersonal efectiva
Expertice técnico

3.6.2.4 Funciones y Responsabilidades del Cargo

Las principales actividades desarrolladas por este cargo en los procesos de la Cadena de Valor y los procesos de Soporte serán:

Proceso: Administración de Infraestructura Tecnológica

Subproceso: Administración de Software Base y aplicativos

- Ejecución de monitoreo de Software base o aplicativos
- Generación de informe
- Ejecución de afinamiento de SW base o aplicativos
- Elaboración de informe mensual
- Generación de requerimiento de ajuste de política o procedimiento
- Recepción de cartera de proyectos
- Recepción de requerimiento
- Ajuste de la planificación del proyecto
- Ejecución del proyecto
- Revisión de políticas de administración de infraestructura
- Generación de requerimiento de soporte
- Configurar o actualizar SW base
- Instalar o actualizar aplicativos
- Registro en inventario de Software
- Registro de Solución

Subproceso: Administración de seguridades

- Elaboración de informe mensual
- Recepción de cartera de proyectos
- Recepción de requerimiento
- Ajuste de la planificación del proyecto
- Ejecución del proyecto
- Revisión de políticas de administración de infraestructura
- Revisión de las políticas de backup y recuperación
- Selección de medios magnéticos
- Ejecución de recuperación
- Preparación y etiquetado de medios magnéticos
- Ejecución de backup según calendario
- Registro en bitácora de respaldos
- Almacenamiento de respaldos en caja fuerte de Gestión de Sistemas

- Envío de medios a caja fuerte externa
- Notificación a Soporte a Cliente internos
- Revisión de Políticas de Seguridad
- Monitoreo de disponibilidad de los servicios y alertas de seguridad
- Ejecución de rutinas de monitoreo de red
- Elaboración de informe de monitoreo
- Ajuste de seguridades
- Generación de requerimiento de ajuste de política o procedimiento
- Revisión del plan de contingencias
- Generación de plan de acción
- Ejecución de plan de acción
- Elaboración de informe
- Creación de perfil de cliente interno
- Modificación de perfil de cliente interno
- Eliminación de perfil de cliente interno
- Revisión de bitácora del antivirus (suite)
- Notificación a cliente interno necesidad de formateo
- Salvado de datos y formateo de máquina
- Instalación de software y restauración de datos
- Registro de Solución

Subproceso: Soporte a Usuarios

- Generación de requerimiento de intranet
- Generación de estadísticas de la gestión de soporte
- Análisis de resultados de soporte
- Generación de requerimiento de ajuste de política o procedimiento
- Generación de informe trimestral de actividades

Proceso: Desarrollo e implantación de aplicativos

- Recepción de cartera de proyectos
- Recepción de requerimiento

- Análisis de factibilidad técnica para desarrollo / mantenimiento / implantación de aplicaciones
- Definición de forma de atención del requerimiento
- Generación de justificación de solución propuesta y requerimiento de aprobación de inversión
- Definición de prioridades, recursos y cronograma para desarrollo / ajuste de aplicaciones
- Generación del análisis
- Generación del diseño
- Construcción
- Definición de prioridades, recursos y cronograma para selección de aplicaciones externas
- Participación en Equipo de Pruebas
- Participación en Equipo de Selección / implantación de aplicaciones
- Aprobación / negación del análisis
- Aprobación / negación del diseño
- Aprobación / negación de ajustes
- Registro de solución
- Generación de requerimiento de ajuste de política o procedimiento o política

Proceso: Administración de redes y comunicaciones

- Recepción de cartera de proyectos
- Recepción de requerimiento
- Ajuste a la planificación del proyecto
- Ejecución del proyecto
- Revisión de políticas de redes y comunicaciones
- Administración de servicios de Internet y redes
- Administración de servicios de Intranet
- Creación / modificación / eliminación de accesos a servicios de red
- Configuración de dispositivos de seguridad de red
- Monitoreo seguridades de red

- Ajuste seguridades de red
- Generación de informe
- Registro de solución
- Monitoreo de los servicios de redes y comunicaciones
- Ajuste de los servicios
- Generación de informe
- Generación de solicitud de mantenimiento para el proveedor
- Ejecución de mantenimiento
- Registro en bitácora de mantenimiento
- Elaboración de informe mensual
- Generación de requerimiento de ajuste de política o procedimiento

3.6.3 CARGO: TÉCNICO DE HARDWARE.

Reporta a: Director de Gestión Tecnológica
Unidad de pertenencia: Dirección de Gestión Tecnológica

3.6.3.1 Definición del cargo, roles y responsabilidades:

El cargo: Técnico de Hardware es el ejecutor de los siguientes subprocesos: Administración de redes y comunicaciones, Desarrollo e implantación de aplicaciones, brinda soporte interno a todos los usuarios de la SENAMI. Responsable por los equipos de Comunicación, telefonía, servidores, impresoras, redes, etc.

Como técnico – administrador: planifica, organiza, asigna, coordina, controla y ajusta las diversas actividades de su unidad alineándolas a la estrategia de la Dirección de Gestión Tecnológica; interviene pro-activamente en la actualización y mejora de los procesos que le competen; atiende y responde con prontitud a los pedidos específicos de sus superiores.

3.6.3.2 Requisitos que el Cargo Exige:

Titulo Académico: Ingeniería de Sistemas ó similares.
Experiencia requerida externa: 4 años
Experiencia requerida interna: 2 años

Otros: Certificaciones con relación al título académico y funciones que realiza.

3.6.3.3 Competencias requeridas para los cargo tipo

Relación interpersonal efectiva

Expertice técnico

3.6.3.4 Funciones y Responsabilidades del Cargo

Las principales actividades desarrolladas por este cargo en los procesos de la Cadena de Valor y los procesos de Soporte son:

Proceso: Administración de Infraestructura Tecnológica

Subproceso: Administración de Hardware

- Elaboración de informe mensual
- Generación de requerimiento de ajuste de política o procedimiento
- Recepción de cartera de proyectos
- Ajuste de la planificación del proyecto
- Ejecución del proyecto
- Revisión de políticas de administración de infraestructura
- Configuración de hardware de servidor
- Configuración de hardware de estación de trabajo
- Registro en inventario de Hardware
- Registro de solución
- Revisión de políticas de administración de infraestructura
- Generación de solicitud de mantenimiento para el proveedor
- Ejecución de mantenimiento
- Registro en bitácora de mantenimiento

Subproceso: Administración de seguridades

- Ejecución de plan de acción
- Elaboración de informe

Subproceso: Soporte a Usuarios

- Generación de requerimiento en Intranet

Proceso: Administración de Aplicaciones

- Participación en Equipo de Pruebas
- Participación en Equipo de Selección / implantación de aplicaciones
- Aprobación / negación del análisis
- Aprobación / negación del diseño
- Aprobación / negación de ajustes

Proceso: Administración de redes y comunicaciones

- Revisión de políticas de administración de redes y comunicaciones
- Determinación de topología y forma de conexión
- Provisión o ajuste de cableado
- Provisión o ajuste de medios de comunicación
- Provisión y configuración de dispositivos de comunicaciones
- Configuración de puntos locales o remotos
- Pruebas y activación
- Generación de documentación

3.7 RECOMENDACIÓN DE HERRAMIENTAS OPEN SOURCE PARA AUTOMATIZAR LA GESTIÓN DE LAS TIC'S.

3.7.1 HERRAMIENTAS OPEN SOURCE.

Intalio es el primer y único Open Source Business Process Plataform. La plataforma de la empresa esta construida en base a las normas del modelador Eclipse STP BPM y Apache ODE motor BPEL, ambos originalmente construido por Intalio. Proporciona todos los componentes necesarios para el diseño, despliegue y gestión de los más complejos procesos de negocio, incluyendo BAM, BRE, ECM, ESB, y Portal.

Jboss jBPM, esta herramienta no esta basada en BPEL, pero tiene soporte para el estándar que parece ser en los BPM, ellos usan JPDL, en resumen en su designer también basado en Eclipse, no usan la nomenclatura BPMN, tal vez eso

los aleja de los estándares empresariales, pero no deja de se una herramienta muy completa y poderosa.

FacturaLUX es software libre de tipo ERP (Enterprise Resource Planning) orientado a la administración, gestión comercial, finanzas y en general a cualquier tipo de aplicación donde se manejen grandes bases de datos y procesos administrativos. Su aplicación abarca desde la gestión financiera y comercial en empresas hasta la adaptación a procesos complejos de producción. GNULinux, Windows, Mac.

BulmaGés es una aplicación modular que pretende cubrir las necesidades de gestión empresarial de cualquier pequeña y mediana empresa dentro del entorno del software libre: Contabilidad - BulmaCont, Facturación - BulmaFact, Terminal Punto de Venta - BTPV y Gestión de Nóminas.

Gesticam una solución libre de gestión de pymes. Contiene módulos de gestión de Compras, Ventas, Empresas, Financiera, Inventario, Productos, Producción, etc.

Fisterra es un proyecto que pretende crear un ERP genérico hecho con software libre. En la actualidad soporta: administración de clientes y pedidos, facturación, gestión de stock y de pagos, punto de venta, funcionamiento distribuido y replicación offline de los datos. La implementación usa Gnome SDK y PostgreSQL (libgda).

Gestor documental docmgr. La gestión documental engloba toda la tecnología y procedimientos que han sido creados para la gestión y el acceso a grandes cantidades de información generada en la empresa. El conocimiento es unos de los activos más valiosos de una organización, por lo que es vital disponer de una correcta gestión de los documentos creados en una empresa, los cuales a menudo se hallan dispersos y en numerosos formatos.

La gestión documental abarca todo el ciclo de los documentos, desde el momento en el que se reciben o se crean hasta el momento en el que son eliminados o conservados, dependiendo de su valor.

CAPITULO 4.

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- COBIT, a través de su marco general, su flexibilidad y versatilidad nos permitió crear y adaptar la presente propuesta de Gestión de TIC's en la SENAMI. La misma se la puede implementar de forma gradual y progresiva de acuerdo a los recursos disponibles y en función de los cambios futuros, de acuerdo a la estrategia empresarial.

- En el futuro, continuaremos viendo el crecimiento de COBIT en sus facetas de administración y dirección de los recursos de tecnología. Aparecerán nuevas herramientas de la familia de productos COBIT y nuevos recursos con los cuales mejorar la administración.

- ITIL, define las mejores prácticas en la gestión de servicios de TI, de los cuales adoptamos los que se aplican a la realidad de la institución, proyectándose a un enfoque orientado a procesos y a la mejora continua.

- Aplicando la propuesta de Gestión de las TIC's en la SENAMI, permitirá a la institución alcanzar la calidad en la gestión de servicio requerida por la ISO20000.

- La presente propuesta permite observar que la institución no cuenta con procesos claros y definidos que permitan mantener un adecuado control de las actividades que se realizan a diario en la Dirección de Gestión Tecnológica por lo que es necesario realizar los cambios respectivos para mejorar su eficiencia y eficacia en el desarrollo de las mismas.

- Del presente trabajo se desprende la obligatoriedad de cumplir las mejores prácticas a fin de llevar un adecuada gestión de los procesos de TI con el fin de que el Departamento de Gestión Tecnológica alcance una posición estratégica dentro de la Organización.

- El Departamento de Gestión Tecnológica debe realizar una campaña de socialización de los productos y herramientas que dispone para el beneficio y facilidad en las labores de los usuarios internos.

- Es vital el mejoramiento continuo y el cumplimiento de las responsabilidades del equipo de TI, para la consecución de los objetivos departamentales e institucionales.

4.2 RECOMENDACIONES

En función del presente propuesta se recomienda:

- Implementar la propuesta de Gestión de las TIC's en la SENAMI utilizando las mejores prácticas y estándares internacionales.

- Modificar la estructura jerárquica actual de la SENAMI cambiando de unidad de gestión tecnológica a Dirección de Gestión Tecnológica con el fin de posicionar a las TIC's como elemento fundamental dentro del Core institucional.

- Aplicar la presente propuesta con el fin de facilitar y agilitar los procesos internos y externos (migrantes y otras organizaciones gubernamentales).

- Crear las partidas presupuestarias necesarias para la contratación del personal propuesto en el presente proyecto.

- Se recomienda generar los diferentes planes a fin de cumplir con la propuesta de Gestión.

- Generar los documentos propuestos en los diferentes procesos con la finalidad de llevar el control e inventario respectivo de los procesos que se llevan adelante dentro de la Dirección de Gestión Tecnología.

- Elaborar un plan de capacitación para el personal técnico y para los usuarios finales, anual en función de las necesidades de la organización.

- Elaborar un Plan Estratégico Institucional en el cual este alineado el Plan Informático de la Dirección de Gestión Tecnológica el cual debe ser actualizado permanentemente previo aprobación de la máxima autoridad, además debe alinearse a la política de gobierno de acuerdo al decreto de uso de Software libre y en constante coordinación con la Subsecretaria de Informática.

- En función del crecimiento de la organización se recomienda incrementar el número de técnicos en el Departamento de Gestión Tecnológica.

BIBLIOGRAFÍA

- IT Governance Institute. Cobit 4.0, Objetivos de Control, Directrices Gerenciales, Modelos de Madurez. Estados Unidos de América. 2005.

- OGC (Office of Govermment Commerce). ITIL Managing IT Services. Best Practice For Service Delivery. Primera Edición. TSO (The Stationary Office). Reino Unido. 2005.

- OGC (Office of Govermment Commerce). ITIL Managing IT Services. Best Practice For Service Support. Primera Edición. TSO (The Stationary Office). Reino Unido. 2005.

- ISO 20000 Ecuador. Introducción ISO 20000 Ecuador. http://www.iso20000.com.ar/intro_ecu.html, 10 de enero de 2009

- ITIL Latinoamérica. ITIL Latinoamérica. http://www.itil.com.ar, 10 de febrero de 2009.

- Blanco Cuaresma Sergi. Itil y ISO 20000, marcos de trabajo para servicios IT. Marble Station. http://www.marblestation.com/?p=646, 14 de febrero de 2009.

- Subsecretaría de Informática. Subsecretaría de Informática, Noticias. http://www.informatica.gov.ec, 15 de marzo de 2009.

- Secretaría Nacional del Migrante. Secretaría Nacional del Migrante. http://www.senami.gov.ec, 17 de marzo de 2009.

- Secretaría Nacional del Migrante. Portal del Migrante Ecuatoriano. http://www.migranteecuatoriano.gov.ec, 27 de marzo de 2009.

- Organización Internacional de Estandarización. Organización Internacional de Estandarización. http://www.iso.org, 26 de marzo de 2009.

- ITIL.org. ITIL.org – ITIL. http://www.itil.org, 27 de abril de 2009.

- Federación Latinoamericano de Bancos FELABAN. Bienvenido a felaban. http://www.felaban.com, 27 de abril de 2009.

- Gobierno de las TIC. Gobierno de las TIC. – Conocimiento Adquirido. http://www.gobiernotic.es, 17 de mayo de 2009.

- ISACA (Information Systems Audit and Control Association). ISACA CAPITULO . http://www.isaca.org.ec, 20 de mayo de 2009.

ANEXOS

ANEXO A. RESUMEN DOMINIOS Y ACTIVIDADES DE COBIT.

DOMINIO P&O (PLANEAR Y ORGANIZAR)

PROCESO PO1. DEFINIR UN PLAN ESTRATÉGICO PARA TI.

La función de los sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información.

Actividad 1. Administración del valor de TI: Objetivo de Control: Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos.

Actividad 2. Alineación de TI con el negocio: Objetivo de Control: Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades.

Actividad 3. Evaluación del desempeño actual: Objetivo de control: Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.

Actividad 4. Plan estratégico de TI: Objetivo de control: Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo la TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales

Actividad 5. Planes tácticos de TI: Objetivo de control: Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por

TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados.

Actividad 6. Administración del portafolio de TI: Objetivo de Control: Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos y específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas.

PROCESO PO2. DEFINIR LA ARQUITECTURA DE INFORMACIÓN.

La función de los sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización.

Actividad 1. Modelo de arquitectura de información empresarial: Objetivo de Control: Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI como se describen en P01.

Actividad 2. Diccionario de datos empresarial y reglas de sintaxis de datos: Objetivo de control: Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización.

Actividad 3. Esquema de clasificación de datos: Objetivo de control: Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa.

Actividad 4. Administración de la integridad: Objetivo de control: Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

PROCESO PO3. DETERMINAR LA DIRECCIÓN TECNOLÓGICA

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un consejo de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación.

Actividad 1. Planeación de la dirección tecnológica: Objetivo de control: Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio.

Actividad 2. Plan de infraestructura tecnológica: Objetivo de Control: Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos.

Actividad 3. Monitoreo de tendencias y regulaciones futuras: Objetivo de control: Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.

Actividad 4. Estándares tecnológicos: Objetivo de control: Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices.

Actividad 5. Consejo de arquitectura: Objetivo de control: Establecer un consejo de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento.

PROCESO PO4. DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI.

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, delegación, autoridad, roles, responsabilidades y supervisión.

Actividad 1. Marco de trabajo del proceso: Objetivo de Control: Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Este marco incluye estructura y relaciones de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas.

Actividad 2. Comité estratégico: Objetivo de Control: Establecer un comité estratégico de TI a nivel del consejo directivo. Este comité garantiza que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las inversiones principales a nombre del consejo directivo.

Actividad 3. Comité directivo (Steering Committee): Objetivo de control: Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para:

- Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa
- Hacer seguimiento al estatus de los proyectos y resolver los conflictos de recursos
- Monitorear los niveles de servicio y las mejoras del servicio

Actividad 4. Ubicación organizacional de la función de TI: Objetivo de Control: Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la

empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.

Actividad 5. **Estructura organizacional: Objetivo de control:** Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implantar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.

Actividad 6. Roles y responsabilidades: Objetivo de control: Definir y comunicar los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad. Crear y actualizar periódicamente la descripción de roles.

Actividad 7. Responsabilidad de aseguramiento de calidad de TI: Objetivo de Control: Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad y proporcionar al grupo de aseguramiento los sistemas de aseguramiento de calidad, los controles y la experiencia para comunicarlos.

Actividad 8. Responsabilidad sobre el riesgo, la seguridad y el cumplimiento: Objetivo de control: Incluir la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel senior apropiado. Definir y asignar roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad específica de la seguridad de la información, la seguridad física y el cumplimiento.

Actividad 9. Propiedad de datos y de sistemas: Objetivo de Control: Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información.

PROCESO PO5. ADMINISTRAR LA INVERSIÓN EN TI

Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto.

Actividad 1. Marco de trabajo para la administración financiera: Objetivo de control: Establecer un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos.

Actividad 2. Prioridades dentro del presupuesto de TI: Objetivo de control: Implantar un proceso de toma de decisiones para dar prioridades a la asignación de recursos a TI para operaciones, proyectos y mantenimiento, para maximizar la contribución de TI a optimizar el retorno del portafolio empresarial de programas de inversión en TI y otros servicios y activos de TI.

Actividad 3. Proceso presupuestal: Objetivo de control: Establecer un proceso para elaborar y administrar un presupuesto que refleje las prioridades establecidas en el portafolio empresarial de programas de inversión en TI, incluyendo los costos recurrentes de operar y mantener la infraestructura actual.

Actividad 4. Administración de costos: Objetivo de Control: Implantar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar.

Actividad 5. Administración de beneficios: Objetivo de control: Implantar un proceso de monitoreo de beneficios. La contribución esperada de TI a los resultados del negocio, ya sea como un componente de programas de inversión en TI o como parte de un soporte operativo regular, se debe identificar, acordar, monitorear y reportar.

PROCESO PO6. COMUNICAR LAS ASPIRACIONES Y LA DIRECCIÓN DE LA GERENCIA.

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implantar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección.

Actividad 1. Ambiente de políticas y de control: Objetivo de control: Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa. Estos elementos incluyen las expectativas / requerimientos respecto a la entrega de valor proveniente de las inversiones en TI, el apetito de riesgo, la integridad, los valores éticos, la competencia del personal, la rendición de cuentas y la responsabilidad.

Actividad 2. Riesgo Corporativo y Marco de Referencia de Control Interno de TI: Objetivo de Control: Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI.

Actividad 3. Administración de políticas para TI: Objetivo de Control: Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices.

Actividad 4. Implantación de políticas de TI: Objetivo de Control: Asegurarse de que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales

Actividad 5. Comunicación de los objetivos y la dirección de TI: Objetivo de Control: Asegurarse de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización.

PROCESO PO7. ADMINISTRAR LOS RECURSOS HUMANOS DE TI

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo prácticas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación.

Actividad 1. Reclutamiento y Retensión del Personal: Objetivo de Control: Asegurarse que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización (ej. contratación, un ambiente positivo de trabajo y orientación).

Actividad 2. Competencias del personal: Objetivo de control: Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

Actividad 3. Asignación de roles: Objetivo de Control: Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requisito de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales

Actividad 4. Entrenamiento del personal de TI: Objetivo de control: Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

Actividad 5. **Dependencia sobre los individuos: Objetivo de Control:** Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

Actividad 6. Procedimientos de Investigación del personal: Objetivo de Control: Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores

Actividad 7. Evaluación del desempeño del empleado: Objetivo de Control: Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

Actividad 8. Cambios y terminación de trabajo: Objetivo de control: Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

PROCESO PO8. ADMINISTRAR LA CALIDAD

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad.

Actividad 1. Sistema de administración de calidad: Objetivo de control: Establecer y mantener un QMS que proporcione un enfoque estándar, formal y

continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades.

Actividad 2. **Estándares y prácticas de calidad: Objetivo de control:** Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización.

Actividad 3. Estándares de desarrollo y de adquisición: Objetivo de control: Adoptar y mantener estándares para todo el desarrollo y adquisición que siguen el ciclo de vida, hasta el último entregable e incluyen la aprobación en puntos clave con base en criterios de aprobación acordados.

Actividad 4. Enfoque en el cliente: Objetivo de control: Garantiza que la administración de calidad se enfoque en los clientes, al determinar sus requerimientos y alinearlos con los estándares y prácticas de TI. Se definen los roles y responsabilidades respecto a la resolución de conflictos entre el usuario/cliente y la organización de TI.

Actividad 5. Mejora continua: Objetivo de Control: Se elabora y comunica un plan global de calidad que promueva la mejora continua, de forma periódica.

Actividad 6. **Medición, monitoreo y revisión de la calidad: Objetivo de control:** Definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

PROCESO PO9. EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar.

Actividad 1. Evaluar y administrar los riesgos de TI: Objetivo de Control: Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización

Actividad 2. **Establecimiento del contexto del riesgo: Objetivo de control:** Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evalúan los riesgos.

Actividad 3. Identificación de eventos: Objetivo de Control: Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto – positivo, negativo o ambos – y dar mantenimiento a esta información.

Actividad 4. Evaluación de riesgos: Objetivo de Control: Evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.

Actividad 5. Respuesta a los riesgos: Identificar los propietarios de los riesgos y a los dueños de procesos afectados, y elaborar y mantener respuestas a los

riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan la exposición a los riesgos de forma continua. La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o aceptar.

Actividad 6. Mantenimiento y monitoreo de un plan de acción de riesgos: Objetivo de control: Asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución.

PROCESO PO10. ADMINISTRAR PROYECTOS

Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversión en TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos. Asegurarse de que los proyectos apoyen los objetivos del programa. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados, y resolver los requerimientos y conflictos de recursos.

Actividad 1. Marco de trabajo para la administración de programas: Objetivo de Control: Mantener el programa de los proyectos, relacionados con el portafolio de programas de inversión en TI, por medio de la identificación, definición, evaluación, otorgamiento de prioridades, selección, inicio, administración y control de los proyectos.

Actividad 2. Marco de trabajo para la administración de proyectos: Objetivo de control: Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido.

Actividad 3. Enfoque de administración de proyectos: Objetivo de control: Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto.

Actividad 4. Compromiso de los interesados: Objetivo de Control: Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversión en TI.

Actividad 5. Estatuto de alcance del proyecto: Objetivo de Control: Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversión en TI.

Actividad 6. Inicio de las fases del proyecto: Objetivo de Control: Asegurarse que el arranque de las etapas importantes del proyecto se apruebe de manera formal y se comunique a todos los interesados. La aprobación de la fase inicial se debe basar en las decisiones de gobierno del programa.

Actividad 7. Plan integrado del proyecto: Objetivo de Control: Establecer un plan integrado para el proyecto, aprobado y formal (que cubra los recursos de negocio y de los sistemas de información) para guiar la ejecución y el control del proyecto a lo largo de la vida del éste.

Actividad 8. Recursos del proyecto: Objetivo de control: Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto.

Actividad 9. Administración de riesgos del proyecto: Objetivo de control: Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el

proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central.

DOMINIO (A&I). ADQUISICIÓN E IMPLEMENTACIÓN

PROCESO AI1. IDENTIFICAR SOLUCIONES AUTOMATIZADAS.

La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de “desarrollar” o “comprar”. Todos estos pasos permiten a las organizaciones minimizar el costo para adquirir e implantar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio

Actividad 1. Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.: Objetivo de Control: Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI.

Actividad 2. Reporte de análisis de riesgos: Objetivo de Control: Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos.

Actividad 3. Estudio de factibilidad y formulación de cursos de acción alternativos: Objetivo de Control: Desarrollar un estudio de factibilidad que examine la posibilidad de implantar los requerimientos. Debe identificar los cursos alternativos de acción para el software, hardware, servicios y habilidades que satisfagan los requerimientos establecidos, tanto funcionales como técnicos, y evaluar la factibilidad tecnológica y económica (costo potencial y análisis de

beneficios) de cada uno de los cursos de acción identificados en el contexto de inversión en TI.

Actividad 4. Requerimientos, decisión de factibilidad y aprobación: El patrocinador del negocio aprueba y autoriza los requisitos de negocio, tanto funcionales como técnicos, y los reportes del estudio de factibilidad en las etapas clave predeterminadas. Cada autorización va después de la terminación de las revisiones de calidad.

PROCESO AI2. ADQUIRIR Y MANTENER SOFTWARE APLICATIVO.

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

Actividad 1. Diseño de alto nivel: Objetivo de Control: Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, tomando en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos.

Actividad 2. Diseño detallado: Objetivo de control: Preparar el diseño detallado y los requerimientos técnicos del software de aplicación. Definir el criterio de aceptación de los requerimientos. Aprobar los requerimientos para garantizar que corresponden al diseño de alto nivel.

Actividad 3. Control y auditabilidad de las aplicaciones: Objetivo de control: Asegurar que los controles del negocio se traduzcan correctamente en controles de aplicación de manera que el procesamiento sea exacto, completo, oportuno, aprobado y auditable.

Actividad 4. Seguridad y disponibilidad de las aplicaciones.: Objetivo de Control: Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, de acuerdo con la clasificación de datos, la arquitectura de seguridad en la información de la organización y el perfil de riesgo.

Actividad 5. Configuración e implantación de software aplicativo adquirido: Objetivo de Control: Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización,

Actividad 6. Actualizaciones importantes en sistemas existentes: Objetivo de Control: Seguir un proceso de desarrollo similar al de desarrollo de sistemas nuevos en el caso que se presenten modificaciones importantes en los sistemas existentes, que resulten en un cambio significativo de los diseños y/o funcionalidad actuales.

Actividad 7. Desarrollo de software aplicativo: Objetivo de Control: Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación y los requerimientos de calidad. Aprobar y autorizar cada etapa clave del proceso de desarrollo de software aplicativo, dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad.

Actividad 8. Aseguramiento de la Calidad del Software: Objetivo de Control: Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización.

Actividad 9. Administración de los requerimientos de aplicaciones: Objetivo de Control: Garantizar que durante el diseño, desarrollo e implantación, se da seguimiento al estatus de los requerimientos particulares (incluyendo todos los

requerimientos rechazados), y que las modificaciones a los requerimientos se aprueban a través de un proceso establecido de administración de cambios.

Actividad 10. Mantenimiento de software aplicativo: Objetivo de Control: Desarrollar una estrategia y un plan para el mantenimiento y liberación de aplicaciones de software. Los asuntos a considerar incluyen liberación planeada y controlada, planeación de recursos, reparación de defectos de programa y corrección de fallas, pequeñas mejoras, mantenimiento de documentación, cambios de emergencia, interdependencia con otras aplicaciones e infraestructura, estrategias de actualización, condiciones contractuales tales como aspectos de soporte y actualizaciones, revisión periódica de acuerdo a las necesidades del negocio, riegos y requerimientos de seguridad.

PROCESO AI3. ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA.

Las organizaciones deben contar con procesos para adquirir, implantar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio.

Actividad 1. Plan de adquisición de infraestructura tecnológica: Objetivo de Control: Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización.

Actividad 2. Protección y disponibilidad del recurso de infraestructura: Objetivo de Control: Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.

Actividad 3. Mantenimiento de la Infraestructura: Objetivo de Control: Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad

Actividad 4. Ambiente de prueba de factibilidad: Objetivo de Control: Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo.

PROCESO AI4. FACILITAR LA OPERACIÓN Y EL USO.

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.

Actividad 1. Plan para soluciones de operación: Objetivo de Control: Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.

Actividad 2. Transferencia de conocimiento a la gerencia del negocio: Objetivo de Control: Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación.

Actividad 3. Transferencia de conocimiento a usuarios finales: Objetivo de Control: Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y al continuo

Actividad 4. Transferencia de conocimiento al personal de operaciones y soporte: Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.

PROCESO AI5. ADQUIRIR RECURSOS DE TI.

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.

Actividad 1. Control de adquisición: Objetivo de Control: Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio.

Actividad 2. Administración de contratos con proveedores: Objetivo de Control: Formular un procedimiento para establecer, modificar y concluir contratos que apliquen a todos los proveedores. El procedimiento debe cubrir, al mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad de propiedad intelectual y de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

Actividad 3. Selección de proveedores: Objetivo de Control: Seleccionar proveedores mediante una práctica justa y formal para garantizar la escogencia del mejor con base en los requerimientos que se han desarrollado con información de proveedores potenciales y acordados entre el cliente y el(los) proveedor(es).

Actividad 4. Adquisición de software: Objetivo de Control: Garantizar que se protegen los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software involucrados en el suministro y uso continuo de software.

Actividad 5. Adquisición de recursos de desarrollo: Objetivo de Control: Garantizar la protección de los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de recursos de desarrollo.

Actividad 6. Adquisición de infraestructura, instalaciones y servicios relacionados: Objetivo de Control: Incluir y hacer cumplir los derechos y obligaciones de todas las partes en los términos contractuales, que comprendan los criterios de aceptación, para la adquisición de infraestructura, instalaciones y servicios relacionados.

PROCESO AI6. ADMINISTRAR CAMBIOS.

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

riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.

Actividad 1. Estándares y procedimientos para cambios: Objetivo de Control: Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.

Actividad 2. Evaluación de impacto, priorización y autorización: Objetivo de Control: Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.

Actividad 3. Cambios de emergencia: Objetivo de Control: Establecer un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia

Actividad 4. Seguimiento y reporte del estatus de cambio: Objetivo de Control: Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

Actividad 5. Cierre y documentación del cambio; Objetivo de Control: Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

PROCESO AI7. INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS.

Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operacionales estén en línea con las expectativas convenidas y con los resultados.

Actividad 1. Entrenamiento: Objetivo de Control: Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.

Actividad 2. Plan de prueba: Objetivo de Control: Establecer un plan de pruebas y obtener la aprobación de las partes relevantes. El plan de pruebas se basa en los estándares de toda la organización y define roles, responsabilidades y criterios de éxito.

Actividad 3. Plan de implantación: Objetivo de Control: Establecer un plan de implantación y obtener la aprobación de las partes relevantes. El plan define el diseño de versiones (release), construcción de paquetes de versiones, procedimientos de implantación / instalación, manejo de incidentes, controles de distribución (incluye herramientas), almacenamiento de software, revisión de la versión y documentación de cambios.

Actividad 4. Ambiente de prueba: Objetivo de Control: Establecer un ambiente de prueba separado para pruebas. Este ambiente debe reflejar el ambiente futuro de operaciones (por ejemplo, seguridad similar, controles internos y cargas de trabajo) para permitir pruebas acertadas

Actividad 5. Conversión de sistema y datos: Objetivo de Control: Garantizar que los métodos de desarrollo de la organización, contemplen para todos los proyectos de desarrollo, implantación o modificación, que todos los elementos

necesarios, tales como hardware, software, datos de transacciones, archivos maestros, respaldos y archivos, interfases con otros sistemas, procedimientos, documentación de sistemas, etc., sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido.

Actividad 6. Prueba de cambios: Objetivo de Control: Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba, por parte de un grupo de prueba independiente (de los constructores) antes de comenzar su uso en el ambiente de operación regular.

Actividad 7. Prueba final de aceptación: Objetivo de Control: Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI.

Actividad 8. Transferencia a producción: Objetivo de Control: Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación. La gerencia debe requerir que se obtenga la autorización del propietario del sistema antes de que se mueva un nuevo sistema a producción y que, antes de que se descontinúe el viejo sistema, el nuevo haya operado exitosamente a través de ciclos de producción diarios, mensuales, trimestrales y de fin de año.

Actividad 9. Liberación de software: Objetivo de Control: Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.

Actividad 10. Distribución del sistema: Objetivo de Control: Establecer procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración. Esto implica controles de integridad; segregación de funciones entre los que construyen, prueban y operan; y adecuadas pistas de auditoria de todas las actividades

Actividad 11. Registro y rastreo de cambios: Objetivo de Control: Automatizar el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.

Actividad 12. **Revisión posterior a la implantación: Objetivo de Control:** Establecer procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.

DOMINO (D&S) ENTREGAR Y DAR SOPORTE

PROCESO DS1. DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO.

Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los participantes sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados.

Actividad 1. Marco de trabajo de la administración de los niveles de servicio: Objetivo de Control: Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las

prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio.

Actividad 2. Definición de servicios: Objetivo de Control: Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios.

Actividad 3. Acuerdos de niveles de servicio: Objetivo de Control: Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI. Esto incluye los compromisos del cliente, los requerimientos de soporte para el servicio, métricas cualitativas y cuantitativas para la medición del servicio firmado por los interesados, en caso de aplicar, los arreglos comerciales y de financiamiento, y los roles y responsabilidades, incluyendo la revisión del SLA. Los puntos a considerar son disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte, planeación de continuidad, seguridad y restricciones de demanda.

Actividad 4. Acuerdos de niveles de operación: Objetivo de Control: Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar el (los) SLA(s) de manera óptima. Los OLAs especifican los procesos técnicos en términos entendibles para el proveedor y pueden soportar diversos SLAs.

Actividad 5. Monitoreo y reporte del cumplimento de los niveles de servicio: Objetivo de Control: Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto.

Actividad 6. Revisión de los acuerdos de niveles de servicio y de los contratos: Objetivo de Control: Revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

PROCESO DS2. ADMINISTRAR LOS SERVICIOS DE TERCEROS.

La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada.

Actividad 1. Identificación de las relaciones con todos los proveedores: Objetivo de Control: Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores.

Actividad 2. Administración de las relaciones con los proveedores: Objetivo de Control: Formalizar el proceso de administración de relaciones con proveedores por cada proveedor. Los responsables de las relaciones deben coordinar a los proveedores y los clientes y asegurar la calidad de las relaciones con base en la confianza y la transparencia (por ejemplo, a través de acuerdos de niveles de servicio).

Actividad 3. Administración de riesgos del proveedor: Objetivos de Control: Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los

estándares universales del negocio de conformidad con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.

Actividad 4. Monitoreo del desempeño del proveedor : Objetivo de Control: Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos del negocio actuales y que se apega de manera continua a los acuerdos del contrato y a los convenios de niveles de servicio, y que el desempeño es competitivo respecto a los proveedores alternativos y a las condiciones del mercado.

PROCESO DS3. ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD.

La necesidad de administrar el desempeño y la capacidad de los recursos de TI requiere de un proceso para revisar periódicamente el desempeño actual y la capacidad de los recursos de TI. Este proceso incluye el pronóstico de las necesidades futuras, basadas en los requerimientos de carga de trabajo, almacenamiento y contingencias. Este proceso brinda la seguridad de que los recursos de información que soportan los requerimientos del negocio están disponibles de manera continua.

Actividad 1. Planeación del desempeño y la capacidad: Objetivo de Control: Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los SLAs. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelado apropiadas para producir un modelo de desempeño, de capacidad y de rendimiento de los recursos de TI, tanto actual como pronosticado.

Actividad 2. Capacidad y desempeño actual: Objetivo de Control: Revisar la capacidad y desempeño actual de los recursos de TI en intervalos regulares para

determinar si existe suficiente capacidad y desempeño para prestar los servicios con base en los niveles de servicio acordados.

Actividad 3. Capacidad y desempeño futuros: Objetivo de Control: Llevar a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares para minimizar el riesgo de interrupciones del servicio originadas por falta de capacidad o degradación del desempeño. Identificar también el exceso de capacidad para una posible redistribución. Identificar las tendencias de las cargas de trabajo y determinar los pronósticos que serán parte de los planes de capacidad y de desempeño.

Actividad 4. Disponibilidad de recursos de TI: Objetivo de Control: Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI.

Actividad 5. Monitoreo y reporte: Objetivo de Control: Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:

Mantener y poner a punto el desempeño actual dentro de TI y atender temas como resiliencia, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.

Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los SLAs. Acompañar todos los reportes de excepción con recomendaciones para llevar a cabo acciones correctivas.

PROCESO DS4. GARANTIZAR LA CONTINUIDAD DEL SERVICIO.

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

Actividad 1. Marco de trabajo de continuidad de TI: Objetivo de Control: Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI.

Actividad 2. Planes de continuidad de TI: Objetivo de Control: Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

Actividad 3. Recursos críticos de TI: Objetivo de Control: Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que

la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

Actividad 4. Mantenimiento del plan de continuidad de TI: Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

Actividad 5. Pruebas del plan de continuidad de TI: Objetivo de Control: Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

Actividad 6. Entrenamiento del plan de continuidad de TI: Objetivo de Control: Asegurarse de que todos las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

Actividad 7. Distribución del plan de continuidad de TI: Objetivo de Control: Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén

disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

Actividad 8. Recuperación y reanudación de los servicios de TI: Objetivo de Control: Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio

Actividad 9. Almacenamiento de respaldos fuera de las instalaciones: Objetivo de Control: Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

Actividad 10. Revisión post-reanudación: Objetivo de Control: Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

PROCESO DS5. GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad

Actividad 1. Administración de la seguridad de TI: Objetivo de Control: Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.

Actividad 2. Plan de seguridad de TI: Objetivo de Control: Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios.

Actividad 3. Administración de identidad: Objetivo de Control: Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y

procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso.

Actividad 4. Administración de cuentas del usuario: Objetivo de Control: Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario. Debe incluirse un procedimiento que describa al responsable de los datos o del sistema como otorgar los privilegios de acceso. Estos procedimientos deben aplicar para todos los usuarios, incluyendo administradores (usuarios privilegiados), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relacionados al acceso a los sistemas e información de la empresa son acordados contractualmente para todos los tipos de usuarios. La gerencia debe llevar a cabo una revisión regular de todas las cuentas y los privilegios asociados.

Actividad 5. Pruebas, vigilancia y monitoreo de la seguridad: Objetivo de Control: Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

Actividad 6. Definición de incidente de seguridad: Objetivo de Control: Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes. Las características incluyen una descripción de lo que se considera un incidente de seguridad y su nivel de impacto. Un número limitado de niveles de impacto se definen para cada

incidente, se identifican las acciones específicas requeridas y las personas que necesitan ser notificadas.

Actividad 7. Protección de la tecnología de seguridad: Objetivo de Control: Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo. Sin embargo no hay que hacer que la seguridad de los sistemas dependa de la confidencialidad de las especificaciones de seguridad

Actividad 8. Administración de llaves criptográficas: Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

Actividad 9. Prevención, detección y corrección de software malicioso: Objetivo de Control: Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).

Actividad 10. Seguridad de la red: Objetivo de Control: Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.

Actividad 11. Intercambio de datos sensitivos: Objetivo de Control: Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar

autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen

PROCESO DS6. IDENTIFICAR Y ASIGNAR COSTOS.

La necesidad de un sistema justo y equitativo para asignar costos de TI al negocio, requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa. Este proceso incluye la construcción y operación de un sistema para capturar, distribuir y reportar costos de TI a los usuarios de los servicios. Un sistema equitativo de costos permite al negocio tomar decisiones más informadas respectos al uso de los servicios de TI.

Actividad 1. Definición de servicios: Objetivo de Control: Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente. Los servicios de TI deben vincularse a los procesos del negocio de forma que el negocio pueda identificar los niveles de facturación de los servicios asociados.

Actividad 2. Contabilización de TI: Objetivo de Control: Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido. Las variaciones entre los presupuestos y los costos actuales deben analizarse y reportarse de acuerdo con los sistemas de medición financiera de la empresa.

Actividad 3. Modelación de costos y cargos: Objetivo de Control: Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa. El modelo de costos de TI debe garantizar que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos. La gerencia del usuario debe poder verificar el uso actual y los cargos de los servicios.

Actividad 4. Mantenimiento del modelo de costos: Objetivo de Control: Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

PROCESO DS7. EDUCAR Y ENTRENAR A LOS USUARIOS.

Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.

Actividad 1. Identificación de necesidades de entrenamiento y educación: Objetivo de Control: Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya:

• Estrategias y requerimientos actuales y futuros del negocio.

• Valores corporativos (valores éticos, cultura de control y seguridad, etc.)

• Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones)

• Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias.

• Métodos de impartición (por ejemplo, aula, Web), tamaño del grupo objetivo, accesibilidad y tiempo

Actividad 2. Impartición de entrenamiento y educación: Objetivo de Control: Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño.

Actividad 3. Evaluación del entrenamiento recibido: Objetivo de Control: Al finalizar la entrenamiento, evaluar el contenido de la entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

PROCESO DS8. ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES.

Actividad 1. Mesa de Servicios: Objetivo de Control: Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los SLAs, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI

Actividad 2. Registro de consultas de clientes: Objetivo de Control: Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Debe trabajar estrechamente con los procesos de administración de incidentes, administración de problemas, administración de cambios, administración de capacidad y administración de disponibilidad. Los incidentes deben clasificarse de acuerdo al negocio y a la prioridad del servicio y enrutarse al equipo de administración de problemas apropiado y se debe mantener informados a los clientes sobre el estatus de sus consultas

Actividad 3. Escalamiento de incidentes: Objetivo de Control: Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA y, si es adecuado, brindar soluciones alternas. Garantizar que la asignación de incidentes y el monitoreo del ciclo de

vida permanecen en la mesa de servicios, independientemente de qué grupo de TI esté trabajando en las actividades de resolución.

Actividad 4. Cierre de incidentes: Objetivo de Control: Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes. Cuando se resuelve el incidente la mesa de servicios debe registrar la causa raíz, si la conoce, y confirmar que la acción tomada fue acordada con el cliente.

Actividad 5. Análisis de tendencias: Objetivo de Control: Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

PROCESO DS9. ADMINISTRAR LA CONFIGURACIÓN.

Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoria de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.

Actividad 1. Repositorio de configuración y línea base: Objetivo de Control: Establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe

mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios.

Actividad 2. Identificación y mantenimiento de elementos de configuración: Objetivo de Control: Contar con procedimientos en orden para: • Identificar elementos de configuración y sus atributos • Registrar elementos de configuración nuevos, modificados y eliminados • Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones. • Actualizar los elementos de configuración existentes en el repositorio de configuraciones. • Prevenir la inclusión de software no-autorizado

Actividad 3. Revisión de integridad de la configuración: Objetivo de Control: Revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar periódicamente contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse.

PROCESO DS10. ADMINISTRACIÓN DE PROBLEMAS.

Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario.

Actividad 1. Identificación y clasificación de problemas: Objetivo de Control: Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para

clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte.

Actividad 2. Rastreo y resolución de problemas: Objetivo de Control: El sistema de administración de problemas debe mantener pistas de auditoria adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando: • Todos los elementos de configuración asociados • Problemas e incidentes sobresalientes • Errores conocidos y sospechados

Actividad 3. Cierre de problemas: Objetivo de Control: Disponer de un procedimiento para cerrar registros de problemas ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con el negocio cómo manejar el problema de manera alternativa.

Actividad 4. Integración de las administraciones de cambios, configuración y problemas: Objetivo de Control: Para garantizar una adecuada administración de problemas e incidentes, integrar los procesos relacionados de administración de cambios, configuración y problemas. Monitorear cuánto esfuerzo se aplica en apagar fuegos, en lugar de permitir mejoras al negocio y, en los casos que sean necesarios, mejorar estos procesos para minimizar los problemas

PROCESO DS11. ADMINISTRACIÓN DE DATOS.

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio

Actividad 1. Requerimientos del negocio para administración de datos: Objetivo de Control: Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas.

Actividad 2. Acuerdos de almacenamiento y conservación: Objetivo de Control: Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encripción y autenticación

Actividad 3. Sistema de administración de librerías de medios: Objetivo de Control: Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso. Los procedimientos deben permitir la revisión oportuna y el seguimiento de cualquier discrepancia que se perciba

Actividad 4. Eliminación: Objetivo de Control: Definir e implementar procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso. Dichos procedimientos deben garantizar que los datos marcados como borrados o desechados no puedan recuperarse

Actividad 5. Respaldo y restauración: Objetivo de Control: Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el

plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración.

Actividad 6. Requerimientos de seguridad para la administración de datos: Objetivo de Control: Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos. Esto incluye registros físicos, transmisiones de datos y cualquier información almacenada fuera del sitio.

PROCESO DS12. ADMINISTRACIÓN DEL AMBIENTE FÍSICO.

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal

Actividad 1. Selección y diseño del centro de datos: Objetivo de Control: Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro de datos debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

Actividad 2. Medidas de seguridad física: Objetivo de Control: Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la

presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

Actividad 3. Acceso Físico: Objetivo de Control: Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones, incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

Actividad 4. Protección contra factores ambientales: Objetivo de Control: Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipo especializado para monitorear y controlar el ambiente

Actividad 5. Administración de instalaciones físicas: Objetivo de Control: Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

PROCESO DS13. ADMINISTRACIÓN DE OPERACIONES.

Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

Actividad 1. Procedimientos e instrucciones de operación: Objetivo de Control: Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

Actividad 2. Programación de tareas: Objetivo de Control: Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el rendimiento y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar agendados

Actividad 3. Monitoreo de la infraestructura de TI: Objetivo de Control: Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones

Actividad 4. Documentos sensitivos y dispositivos de salida.: Objetivo de Control: Establecer resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad

Actividad 5. Mantenimiento preventivo del hardware: Objetivo de Control: Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.

DOMINO (M&E) MONITOREAR Y EVALUAR

PROCESO ME1. MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI.

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.

Actividad 1. Enfoque del Monitoreo: Objetivo de Control: Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI. El marco de trabajo se debería integrar con el sistema de administración del desempeño corporativo

Actividad 2. Definición y recolección de datos de monitoreo: Objetivo de Control: Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes. Los indicadores de desempeño deberían incluir:

- La contribución al negocio que incluya, pero que no se limite a, la información financiera
- Desempeño contra el plan estratégico del negocio y de TI
- Riesgo y cumplimiento de las regulaciones
- Satisfacción del usuario interno y externo
- Procesos clave de TI que incluyan desarrollo y entrega del servicio
- Actividades orientadas a futuro, por ejemplo, la tecnología emergente, la infraestructura re-utilizable, habilidades del personal de TI y del negocio

Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.

Actividad 3. Método de monitoreo: Objetivo de Control: Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.

Actividad 4. Evaluación del desempeño: Objetivo de Control: Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes

Actividad 5. Reportes al consejo directivo y a ejecutivos: Objetivo de Control: Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas administrativas adecuadas.

Actividad 6. Acciones correctivas: Objetivo de Controlo: Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con:

- Revisión, negociación y establecimiento de respuestas administrativas
- Asignación de responsabilidades por la corrección
- Rastreo de los resultados de las acciones comprometidas

PROCESO ME2. MONITOREAR Y EVALUAR EL CONTROL INTERNO.

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

Actividad 1. Monitorear el marco de trabajo de control interno: Objetivo de Control: Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se debería utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI.

Actividad 2. Revisiones de Auditoria: Objetivo de Control: Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoria incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.

Actividad 3. Excepciones de control: Objetivo de Control: Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones se deberían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas.

Actividad 4. Auto-evaluación de control: Objetivo de Control: Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.

Actividad 5. Aseguramiento del control interno: Objetivo de Control: Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros. Dichas revisiones pueden ser realizadas por la función de cumplimiento corporativo o, a solicitud de la gerencia, por auditoria interna o por auditores y consultores externos o por organismos de certificación. Se deben verificar las aptitudes de los individuos que realicen la auditoria, por ej. Un Auditor de Sistemas de Información CertificadoTM (CISA® por sus siglas en Inglés) debe asignarse.

Actividad 6. Control interno para terceros: Objetivo de Control: Determinar el estado de los controles internos de cada proveedor externos de servicios. Confirmar que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios y con las obligaciones contractuales. Esto puede ser provisto por una auditoria externa o se puede obtener de una revisión por parte de auditoria interna y por los resultados de otras auditorias.

Actividad 7. Acciones correctivas: Objetivo de Control: Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con:

- La revisión, negociación y establecimiento de respuestas administrativas
- La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos)
- El rastreo de los resultados de las acciones comprometidas

PROCESO ME3. GARANTIZAR EL CUMPLIMIENTO REGULATORIO.

Una supervisión efectiva del cumplimiento regulatorio requiere del establecimiento de un proceso independiente de revisión para garantizar el cumplimiento de las leyes y regulaciones. Este proceso incluye la definición de un estatuto de auditoria, independencia de los auditores, ética y estándares profesionales, planeación, desempeño del trabajo de auditoria y reportes y seguimiento a las

actividades de auditoria. El propósito de este proceso es proporcionar un aseguramiento positivo relativo al cumplimiento de TI de las leyes y regulaciones.

Actividad 1. Identificar las leyes y regulaciones con impacto potencial sobre TI: Objetivo de Control: Definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI. Tomar en cuenta las leyes y reglamentos de comercio electrónico, flujo de datos, privacidad, controles internos, reportes financieros, reglamentos específicos de la industria, propiedad intelectual y derechos de autor, además de salud y seguridad

Actividad 2. Optimizar la respuesta a requerimientos regulatorios: Objetivo de Control: Revisar y optimizar las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.

Actividad 3. Evaluación del cumplimiento con requerimientos regulatorios: Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos

Actividad 4. Aseguramiento positivo del cumplimiento: Objetivo de Control: Definir e implantar procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento. Integrar los reportes de avance y estado del cumplimiento de TI con salidas similares provenientes de otras funciones de negocio

Actividad 5. Reportes integrados.: Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio

PROCESO ME4. PROPORCIONAR GOBIERNO DE TI.

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales.

Actividad 1. Establecer un marco de trabajo de gobierno para TI: Objetivo de Control: Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales

Actividad 2. Alineamiento estratégico: Objetivo de Control: Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología. Garantizar que existe un entendimiento compartido entre el negocio y la función de TI sobre la contribución potencial de TI a la estrategia del negocio. Asegurarse de que exista un entendimiento claro de que el valor de TI sólo se obtiene cuando las inversiones habilitadas con TI se administran como un portafolio de programas que incluyen el alcance completo de los cambios que el negocio debe realizar para optimizar el valor proveniente de las capacidades que tiene TI para lograr la estrategia.

Actividad 3. Entrega de valor: Objetivo de Control: Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales. Asegurarse de que los resultados de negocio esperados de las inversiones habilitadas por TI y el alcance completo del esfuerzo requerido

para lograr esos resultados esté bien entendido, que se generen casos de negocio integrales y consistentes, y que los aprueben los interesados, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa del logro de los beneficios, tales como la contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a los requerimientos de los clientes.

Actividad 4. Administración de recursos: Objetivo de Control: Optimizar la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio. La dirección debería implantar políticas claras, consistentes y reforzadas sobre recursos humanos y políticas de sustitución para garantizar que se satisfagan los requerimientos de recursos de manera efectiva y para adaptarse a las políticas y estándares de la arquitectura. La infraestructura de TI se debe evaluar periódicamente para asegurar que esté estandarizada siempre que sea posible y que exista la interoperabilidad según sea requiera.

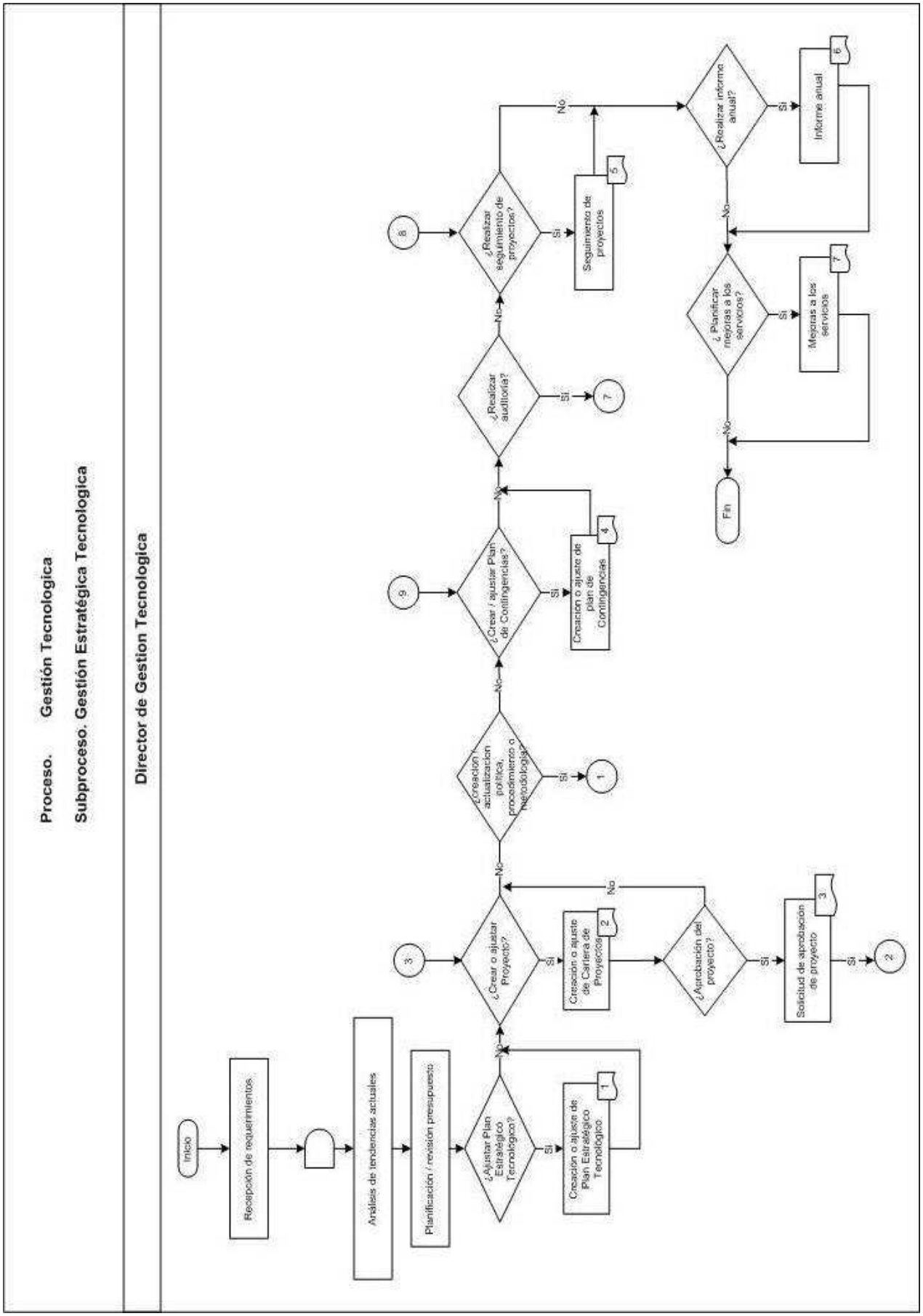
Actividad 5. Administración de riesgos.: Objetivo de Control: Trabajar en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa. Comunicar este nivel de riesgo hacia la organización y acordar el plan de administración de riesgos de TI. Integrar las responsabilidades de administración de riesgos en la organización, asegurando que tanto el negocio como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto en el negocio. Garantizar que la gerencia de TI haga seguimiento a la exposición a los riesgos, poniendo especial atención en las fallas y debilidades de control interno y de supervisión, así como su impacto actual y potencial en el negocio. La posición de riesgo empresarial en TI debería ser transparente para todos los interesados.

Actividad 6. Medición del desempeño.: Objetivo de Control: Informar el desempeño relevante del portafolio de los programas de TI al consejo directivo y a

los ejecutivos de manera oportuna y precisa. Los infor-mes administrativos que se deben entregar a la alta dirección para su revisión deben incluir el avance de la empresa hacia metas identificadas. Los reportes de estatus deben incluir el grado al cual se han logrado los objetivos planeados, entregables obtenidos, metas de desempeño alcanzadas y los riesgos mitigados. Integrar los informes con salidas similares de otras funciones del negocio. Las mediciones de desempeño deberían ser aprobadas por los interesados clave. El consejo directivo y los ejecutivos deberían cuestionar estos informes de desempeño y la gerencia de TI debería tener la oportunidad de explicar las desviaciones y los problemas de desempeño. Después de la revisión, se deben iniciar y controlar las acciones administrativas apropiadas

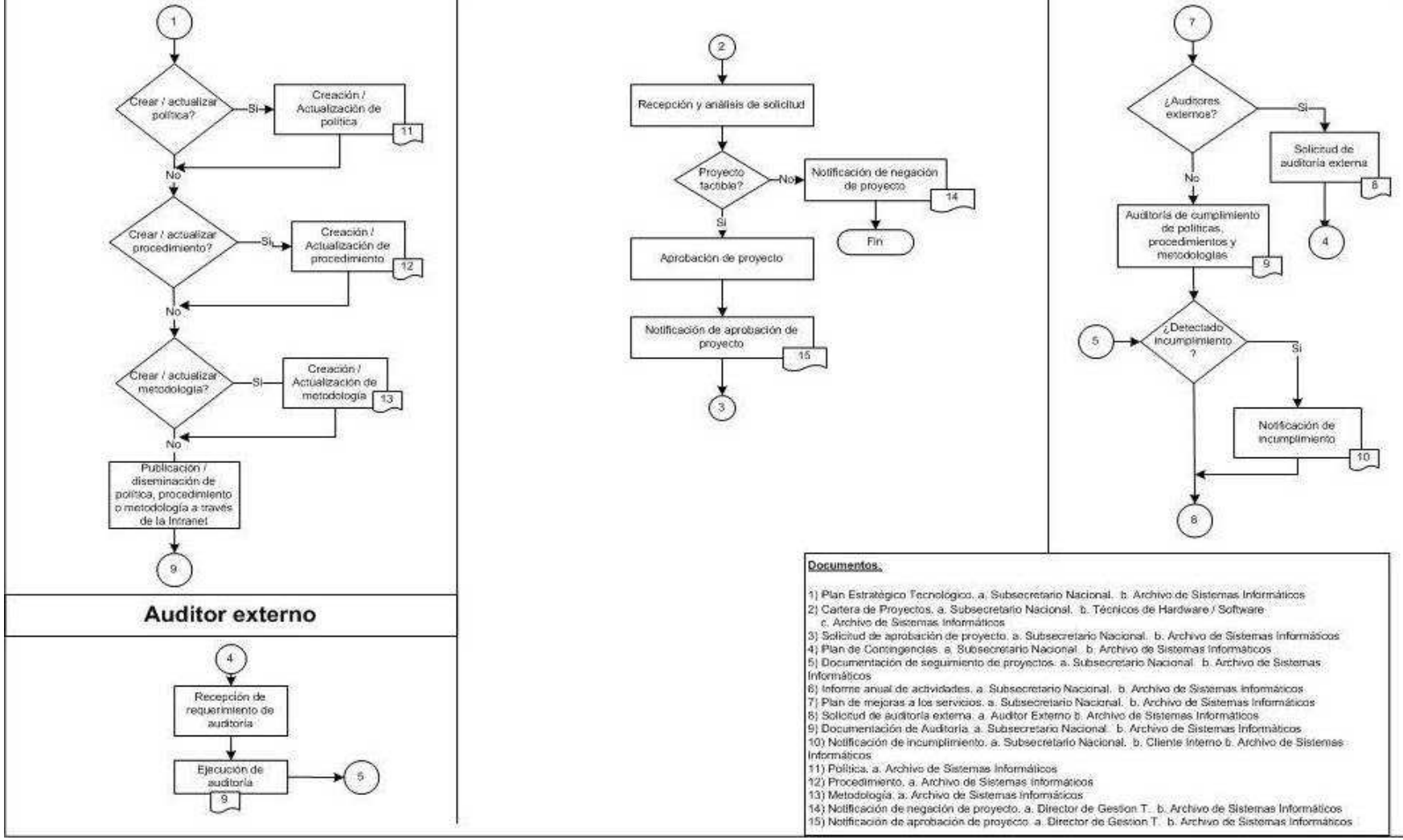
Actividad 7. Aseguramiento independiente.: Objetivo de Control: Garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo esto ocurrirá probablemente a través de un comité de auditoria – aseguramiento independiente y oportuno sobre el cumplimiento que tiene TI respecto a sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas

ANEXO B. PROCEDIMIENTO SUBPROCESO GESTIÓN ESTRATÉGICA TECNOLÓGICA


Proceso. Gestión Tecnologica
Subproceso. Gestión Estratégica Tecnologica
Director de Gestion Tecnologica
Inicio
Recepción de requerimientos
Análisis de tendencias actuales
Planificación / revisión presupuesto
¿Ajustar Plan Estratégico Tecnológico?
Si
No
Creacion o ajuste de Plan Estratégico Tecnologico
1
¿Crear o ajustar Proyecto?
Si
No
Creación o ajuste de Carrera de Proyectos
2
¿Aprobación del proyecto?
Si
No
Solicitud de aprobación de proyecto
3
¿Creación / actualización política, procedimiento o metodología?
Si
No
1
¿Crear / ajustar Plan de Contingencias?
Si
No
Creacion o ajuste de plan de Contingencias
4
¿Realizar auditoria?
Si
No
7
¿Realizar seguimiento de proyectos?
Si
No
Seguimiento de proyectos
5
¿Realizar informe anual?
Si
No
Informe anual
6
¿ Planificar mejoras a los servicios?
Si
No
Mejoras a los servicios
7
Fin
8
9
2
3

Proceso. Gestión Tecnologica

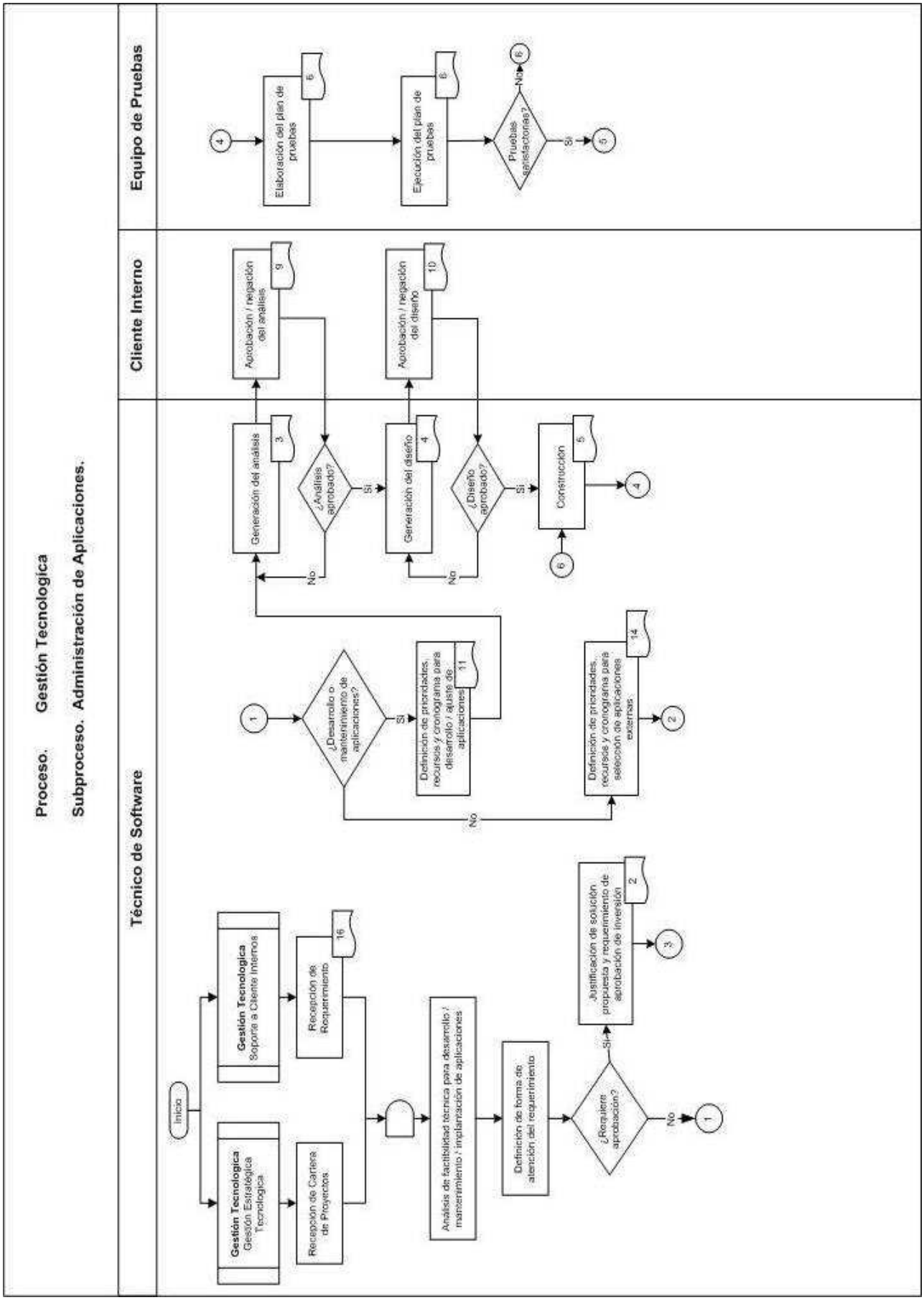
Subproceso. Gestión Estratégica Tecnologica

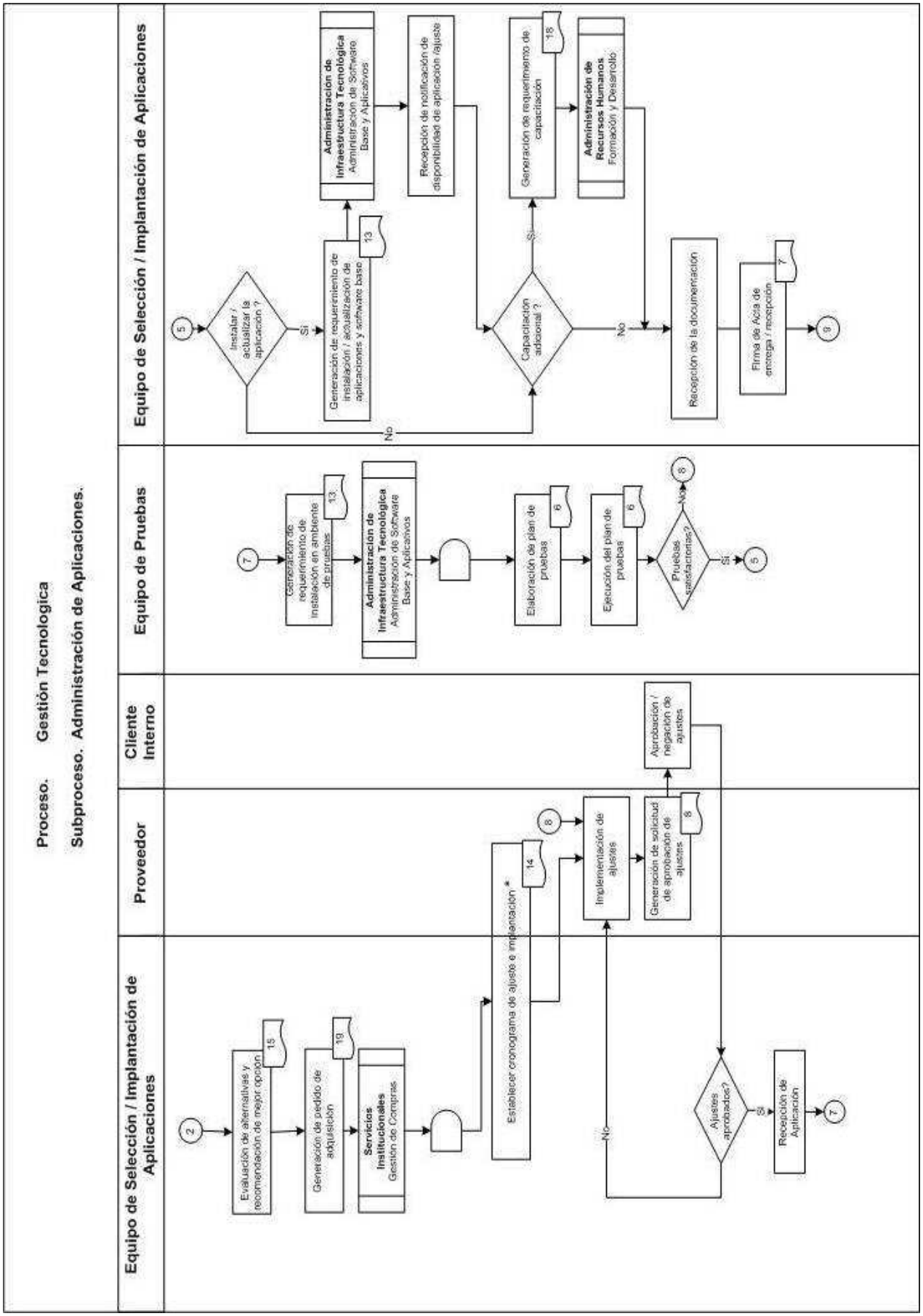


Documentos.

1) Plan Estratégico Tecnológico. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
2) Cartera de Proyectos. a. Subsecretario Nacional. b. Técnicos de Hardware / Software c. Archivo de Sistemas Informáticos
3) Solicitud de aprobación de proyecto. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
4) Plan de Contingencias. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
5) Documentación de seguimiento de proyectos. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
6) Informe anual de actividades. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
7) Plan de mejoras a los servicios. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
8) Solicitud de auditoría externa. a. Auditor Externo b. Archivo de Sistemas Informáticos
9) Documentación de Auditoría. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
10) Notificación de incumplimiento. a. Subsecretario Nacional. b. Cliente Interno b. Archivo de Sistemas Informáticos
11) Política. a. Archivo de Sistemas Informáticos
12) Procedimiento. a. Archivo de Sistemas Informáticos
13) Metodología. a. Archivo de Sistemas Informáticos
14) Notificación de negación de proyecto. a. Director de Gestion T.. b. Archivo de Sistemas Informáticos
15) Notificación de aprobación de proyecto. a. Director de Gestion T.. b. Archivo de Sistemas Informáticos

ANEXO C. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE APLICACIONES

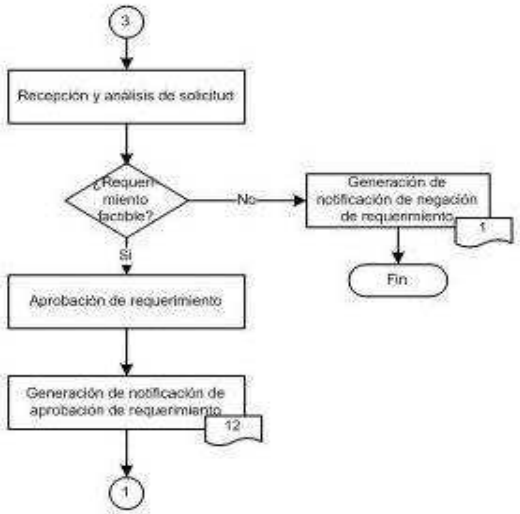

Proceso. Gestión Tecnologica
Subproceso. Administración de Aplicaciones.
Técnico de Software
Cliente Interno
Equipo de Pruebas
Inicio
Gestión Tecnologica
Gestión Estratégica Tecnologica
Gestión Tecnologica
Soporte a Cliente Internos
Recepción de Carteras de Proyectos
Recepción de Requerimiento
16
Análisis de factibilidad técnica para desarrollo / mantenimiento / implantación de aplicaciones
Definición de forma de atención del requerimiento
¿Requiere aprobación?
Si
No
Justificación de solución propuesta y requerimiento de aprobación de inversión
2
3
1
¿Desarrollo o mantenimiento de aplicaciones?
Si
No
Definición de prioridades, recursos y cronograma para desarrollo / ajuste de aplicaciones
11
Definición de prioridades, recursos y cronograma para selección de aplicaciones externas
14
2
Generación del análisis
3
¿Análisis aprobado?
Si
No
Aprobación / negación del análisis
9
Generación del diseño
4
¿Diseño aprobado?
Si
No
Aprobación / negación del diseño
10
Construcción
5
6
4
Elaboración del plan de pruebas
5
Ejecución del plan de pruebas
6
Pruebas satisfactorias?
Si
No
6
5

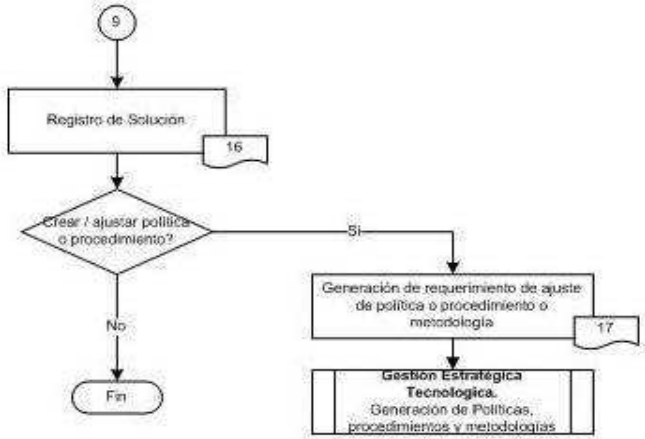

Proceso. Gestión Tecnologica
Subproceso. Administración de Aplicaciones.
Equipo de Selección / Implantación de Aplicaciones
Proveedor
Cliente Interno
Equipo de Pruebas
Equipo de Selección / Implantación de Aplicaciones
Evaluación de alternativas y recomendación de mejor opción
Generación de pedido de adquisición
Servicios Institucionales Gestión de Compras
Establecer cronograma de ajuste e implantación *
Implementación de ajustes
Generación de solicitud de aprobación de ajustes
Aprobación / negación de ajustes
Ajustes aprobados?
Recepción de Aplicación
Generación de requerimiento de instalación en ambiente de pruebas
Administración de Infraestructura Tecnológica Administración de Software Base y Aplicativos
Elaboración de plan de pruebas
Ejecución del plan de pruebas
Pruebas satisfactorias?
Instalar / actualizar la aplicación ?
Generación de requerimiento de instalación / actualización de aplicaciones y software base
Administración de Infraestructura Tecnológica Administración de Software Base y Aplicativos
Recepción de notificación de disponibilidad de aplicación /ajuste
Capacitación adicional ?
Generación de requerimiento de capacitación
Administración de Recursos Humanos Formación y Desarrollo
Recepción de la documentación
Firma de Acta de entrega / recepción
Si
No

Proceso. Gestión Tecnologica

Subproceso. Administración de Aplicaciones.

Subsecretario Nacional	Técnico de Software

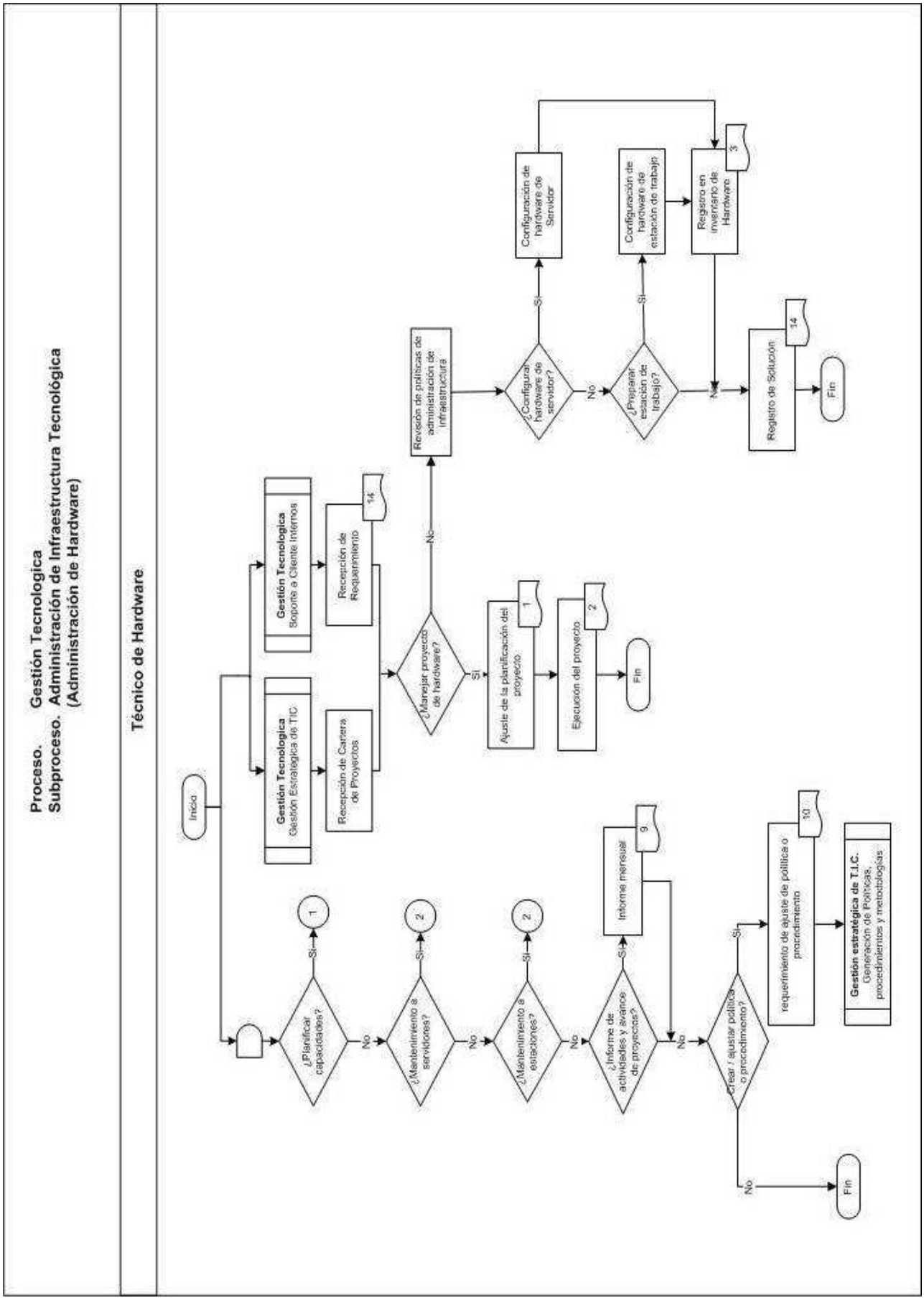


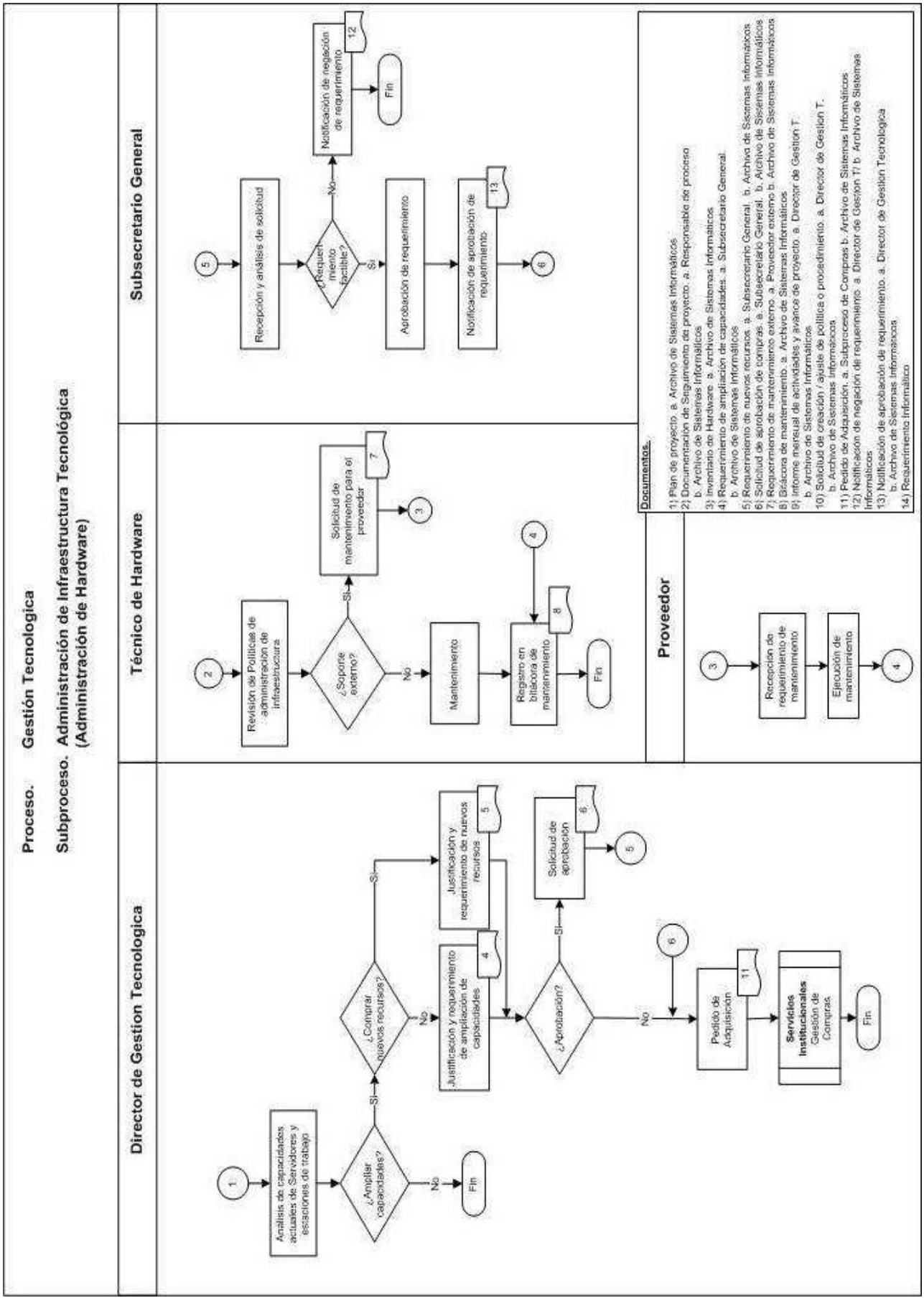


Documentos.

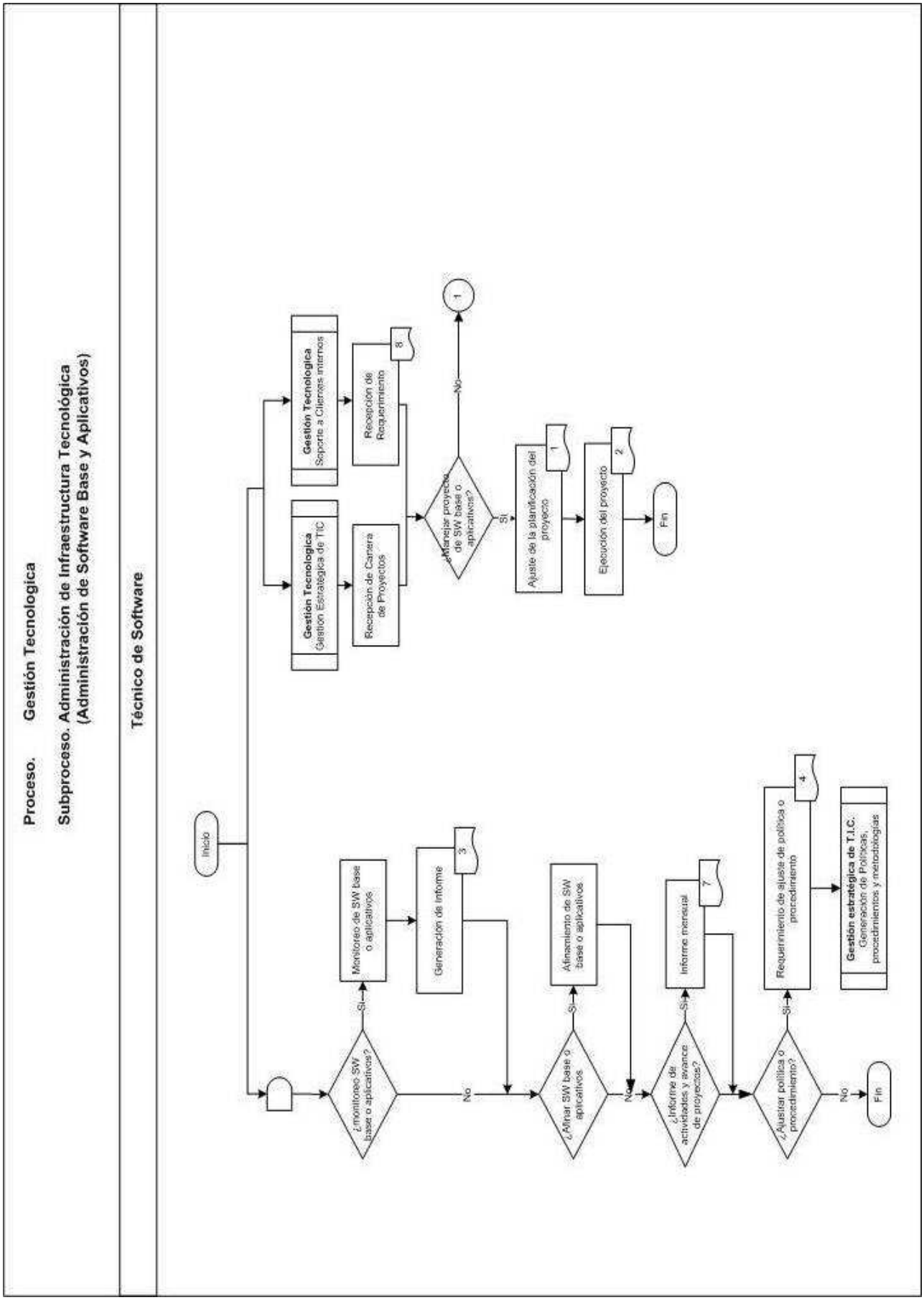
1) Notificación de negación de requerimiento. a. Técnico de Software. b.Director de Gestion T.
2) Propuesta técnica y económica. a. Subsecretario General. b. Archivo de Sistemas Informáticos
3) Documentación de análisis. a. Cliente Interno. b. Archivo de Sistemas Informáticos
4) Documentación de diseño. a. Cliente Interno. b. Archivo de Sistemas Informáticos
5) Documentación de la aplicación. a. Cliente Interno. b. Archivo de Sistemas Informáticos
6) Plan de pruebas. a. Director de Gestion T. b. Archivo de Sistemas Informáticos
7) Acta de entrega / recepción de aplicación o ajuste. a. Director de Gestion T. b. Cliente Interno c. Archivo de Sistemas Informáticos
8) Solicitud de aprobación de ajustes. a. Cliente Interno. b. Archivo de Sistemas Informáticos
9) Acta de aprobación de análisis. a. Cliente Interno. b. Archivo de Sistemas Informáticos
10) Acta de aprobación de diseño. a. Cliente Interno. b. Archivo de Sistemas Informáticos
11) Cronograma de desarrollo / ajuste de aplicación. a. Gerente de proyecto. b. Archivo de Sistemas Informáticos
12) Notificación de aprobación de requerimiento. a. Técnico de Software b. Director de Gestion T
13) Requerimiento de instalación / actualización de aplicaciones y software base. a. Técnico de Software b. Archivo de Sistemas Informáticos
14) Cronograma de selección e implantación de aplicación externa. a. Proveedor b. Archivo de Sistemas Informáticos
15) Informe Técnico - Económico. a. Subproceso de Compras. b. Archivo de Sistemas Informáticos.
16) Requerimiento Informático
17) Solicitud de creación / ajuste de política o procedimiento. a. Director de Gestion T b. Archivo de Sistemas Informáticos
18) Requerimiento de capacitación. a. Analista de RRHH b. Archivo de Sistemas Informáticos
19) Pedido de Adquisición. a. Subproceso de Compras b. Archivo de Sistemas Informáticos

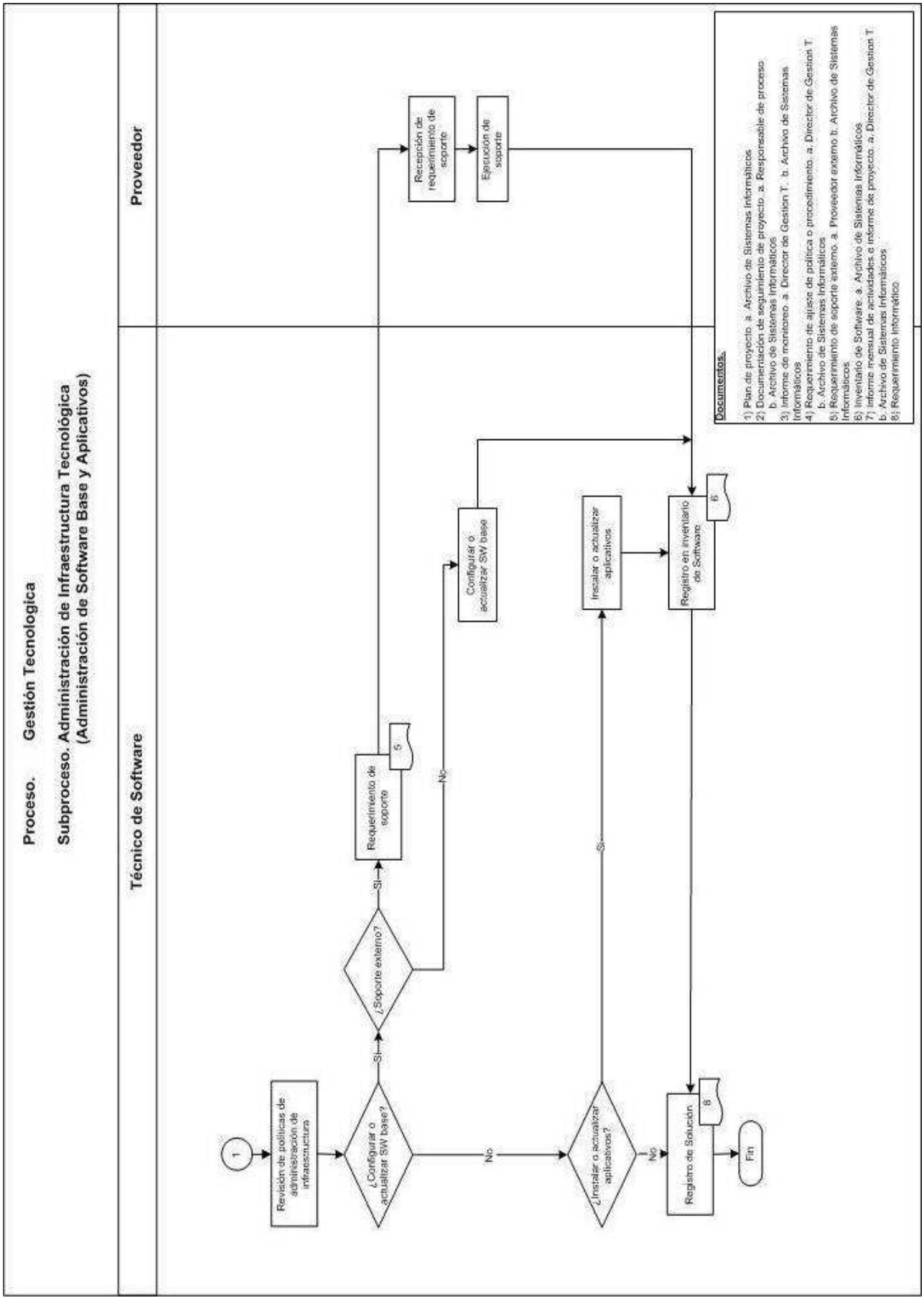
ANEXO D. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE HARDWARE


Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica
(Administración de Hardware)
Técnico de Hardware
Inicio
Gestión Tecnologica
Gestión Estrategica de TIC
Gestión Tecnologica
Soporte a Cliente Internos
Recepción de Cartera de Proyectos
Recepción de Requerimiento
14
¿Manejar proyecto de hardware?
Si
No
Ajuste de la planificación del proyecto
1
Ejecución del proyecto
2
Fin
Revisión de políticas de administración de infraestructura
¿Configurar hardware de servidor?
Si
No
Configuración de hardware de Servidor
¿Preparar estación de trabajo?
Si
No
Configuración de hardware de estación de trabajo
Registro en inventario de Hardware
3
Registro de Solución
14
Fin
¿Planificar capacidades?
Si
No
1
¿Mantenimiento a servidores?
Si
No
2
¿Mantenimiento a estaciones?
Si
No
2
¿Informe de actividades y avance de proyectos?
Si
No
Informe mensual
9
¿Crear / ajustar política o procedimiento?
Si
No
requerimiento de ajuste de política o procedimiento
10
Gestión estratégica de T.I.C.
Generación de Políticas, procedimientos y metodologías
Fin

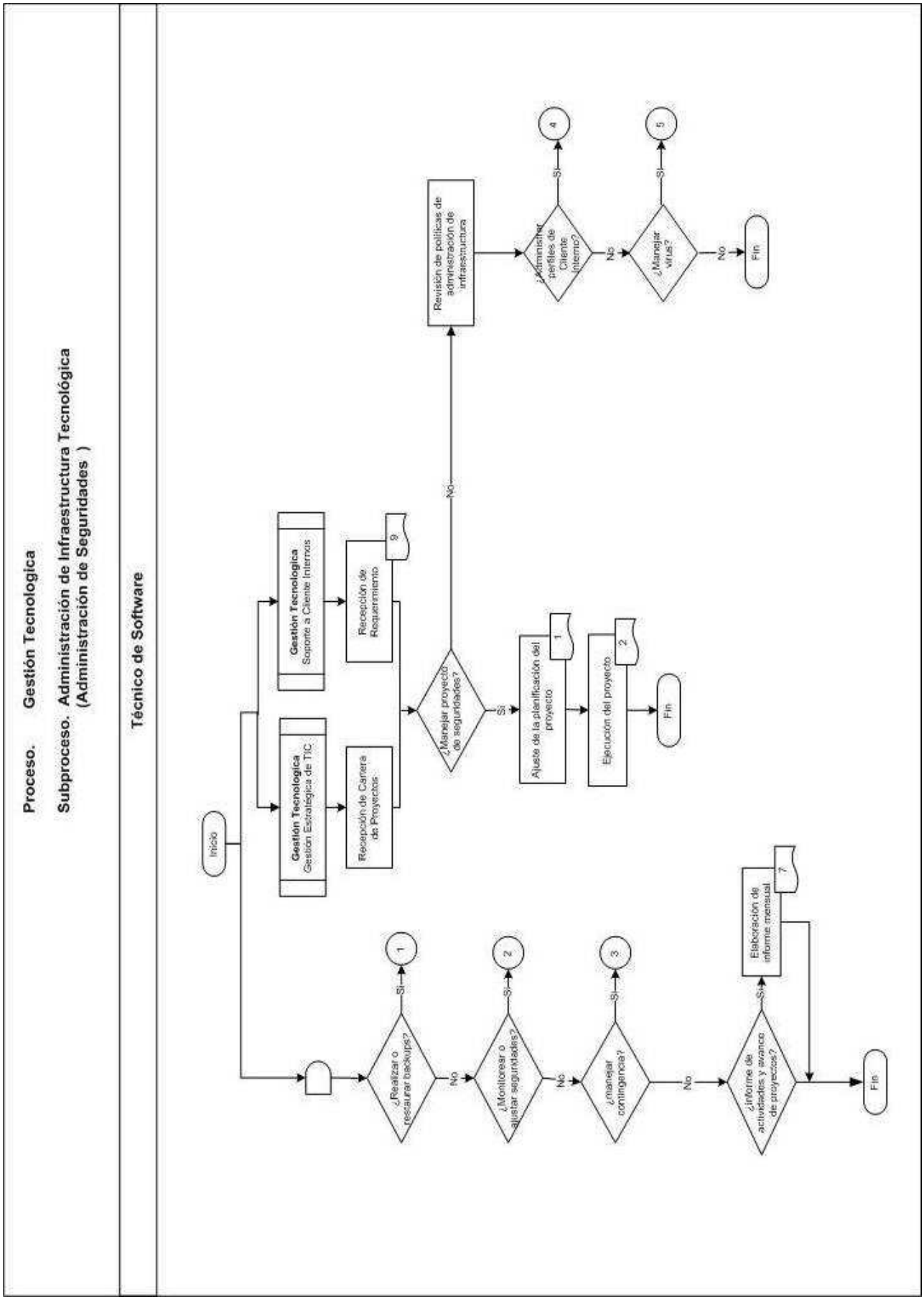

Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica (Administración de Hardware)
Director de Gestion Tecnologica
Técnico de Hardware
Subsecretario General
Proveedor
Documentos.
1) Plan de proyecto. a. Archivo de Sistemas Informáticos
2) Documentación de Seguimiento de proyecto. a. Responsable de proceso b. Archivo de Sistemas Informáticos
3) Inventario de Hardware. a. Archivo de Sistemas Informáticos
4) Requerimiento de ampliación de capacidades. a. Subsecretario General b. Archivo de Sistemas Informáticos
5) Requerimiento de nuevos recursos. a. Subsecretario General. b. Archivo de Sistemas Informáticos
6) Solicitud de aprobación de compras. a. Subsecretario General. b. Archivo de Sistemas Informáticos
7) Requerimiento de mantenimiento externo. a. Proveedor externo b. Archivo de Sistemas Informáticos
8) Bitácora de mantenimiento. a. Archivo de Sistemas Informáticos
9) Informe mensual de actividades y avance de proyecto. a. Director de Gestion T. b. Archivo de Sistemas Informáticos
10) Solicitud de creación / ajuste de política o procedimiento. a. Director de Gestion T. b. Archivo de Sistemas Informáticos
11) Pedido de Adquisición. a. Subproceso de Compras b. Archivo de Sistemas Informáticos
12) Notificación de negación de requerimiento. a. Director de Gestion T/ b. Archivo de Sistemas Informáticos
13) Notificación de aprobación de requerimiento. a. Director de Gestion Tecnologica b. Archivo de Sistemas Informáticos
14) Requerimiento Informático
Análisis de capacidades actuales de Servidores y estaciones de trabajo
¿Ampliar capacidades?
Si
No
Fin
¿Comprar nuevos recursos?
Si
No
Justificación y requerimiento de nuevos recursos
Justificación y requerimiento de ampliación de capacidades
¿Aprobación?
Si
No
Solicitud de aprobación
Pedido de Adquisición
Servicios Institucionales Gestión de Compras
Fin
Revisión de Políticas de administración de infraestructura
¿Soporte externo?
Si
No
Solicitud de mantenimiento para el proveedor
Mantenimiento
Registro en bitácora de mantenimiento
Fin
Recepción y análisis de solicitud
¿Requerimiento factible?
Si
No
Notificación de negación de requerimiento
Fin
Aprobación de requerimiento
Notificación de aprobación de requerimiento
Recepción de requerimiento de mantenimiento
Ejecución de mantenimiento

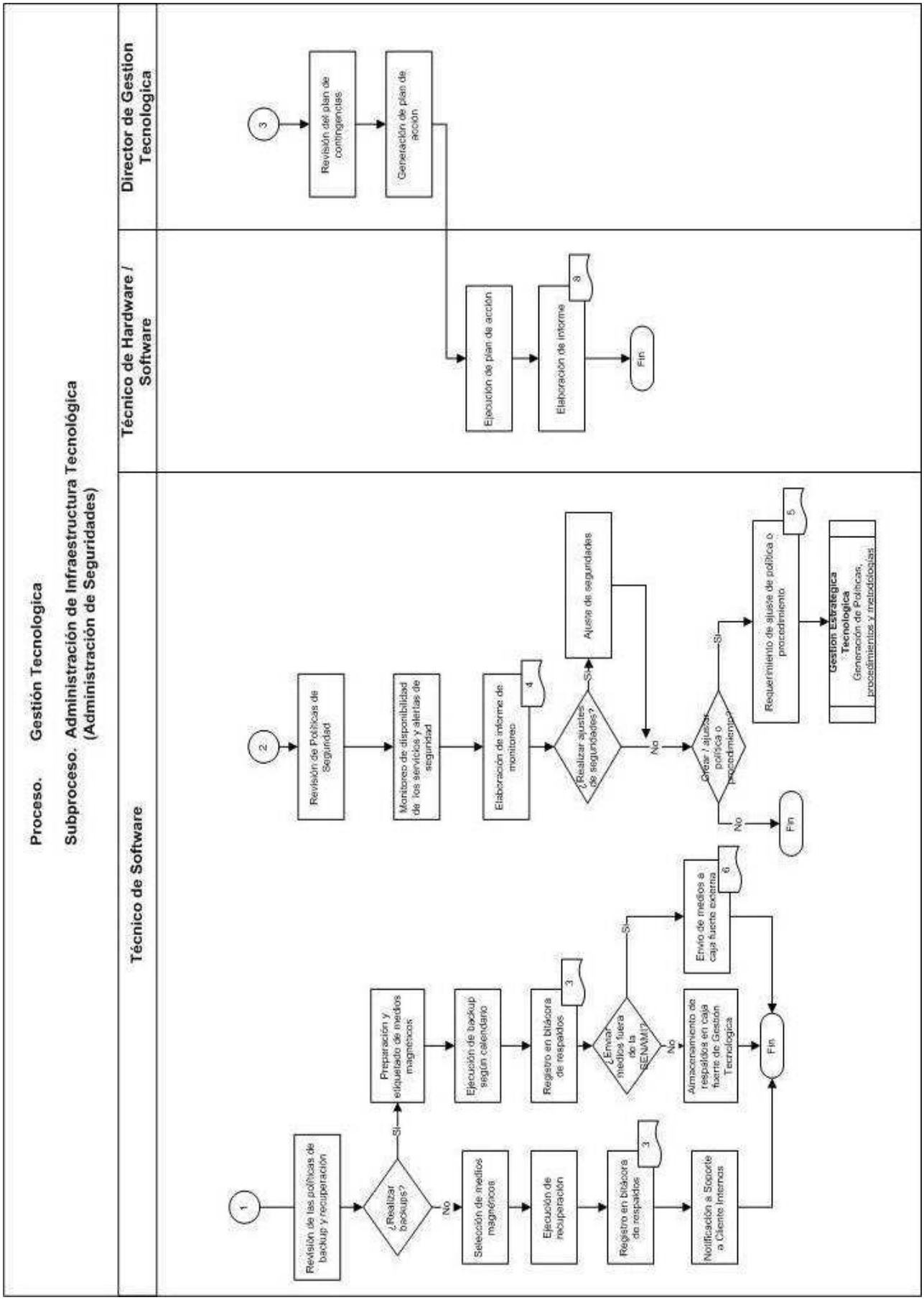
ANEXO E. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE SW BASE Y APLICATIVOS

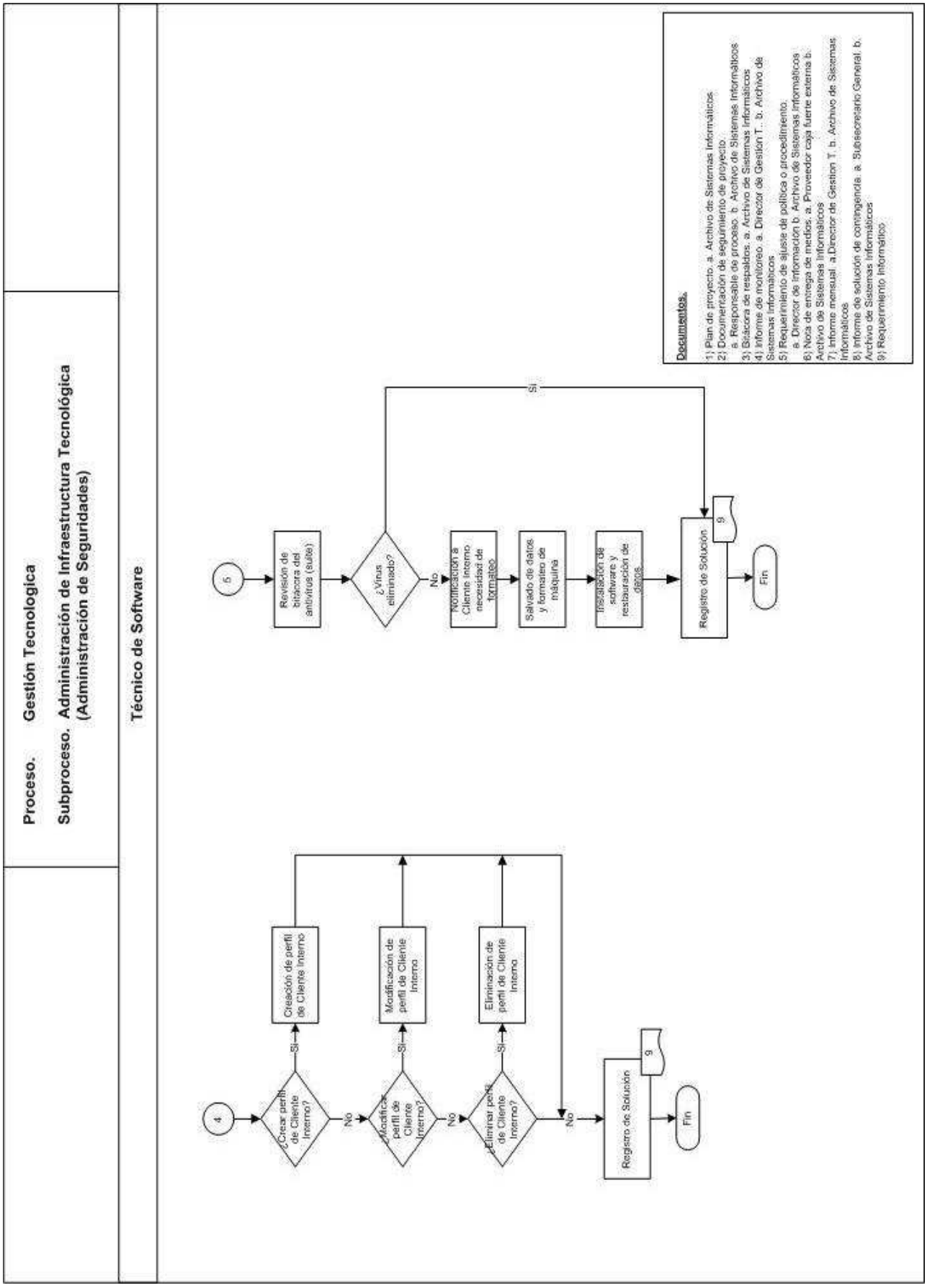

Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica (Administración de Software Base y Aplicativos)
Técnico de Software
Inicio
¿monitoreo SW base o aplicativos?
Si
No
Monitoreo de SW base o aplicativos
Generación de Informe
3
¿Afinar SW base o aplicativos
Si
No
Afinamiento de SW base o aplicativos
¿Informe de actividades y avance de proyectos?
Si
No
Informe mensual
7
¿Ajustar política o procedimiento?
Si
No
Requerimiento de ajuste de política o procedimiento
4
Gestión estratégica de T.I.C.
Generación de Políticas, procedimientos y metodologías
Fin
Gestión Tecnologica
Gestión Estratégica de TIC
Gestión Tecnologica
Soporte a Clientes internos
Recepción de Cartera de Proyectos
Recepción de Requerimiento
8
¿Manejar proyecto de SW base o aplicativos?
Si
No
1
Ajuste de la planificación del proyecto
1
Ejecución del proyecto
2
Fin


Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica (Administración de Software Base y Aplicativos)
Técnico de Software
Proveedor
1
Revisión de políticas de administración de infraestructura
¿Configurar o actualizar SW base?
Si
No
¿Soporte externo?
Si
No
Requerimiento de soporte
5
Configurar o actualizar SW base
Recepción de requerimiento de soporte
Ejecución de soporte
¿Instalar o actualizar aplicativos?
Si
No
Instalar o actualizar aplicativos
Registro de Solución
8
Registro en inventario de Software
6
Fin
Documentos.
1) Plan de proyecto. a. Archivo de Sistemas Informáticos
2) Documentación de seguimiento de proyecto. a. Responsable de proceso b. Archivo de Sistemas Informáticos
3) Informe de monitoreo. a. Director de Gestion T.. b. Archivo de Sistemas Informáticos
4) Requerimiento de ajuste de política o procedimiento. a. Director de Gestion T b. Archivo de Sistemas Informáticos
5) Requerimiento de soporte externo. a. Proveedor externo b. Archivo de Sistemas Informáticos
6) Inventario de Software. a. Archivo de Sistemas Informáticos
7) Informe mensual de actividades e informe de proyecto. a. Director de Gestion T b. Archivo de Sistemas Informáticos
8) Requerimiento informático

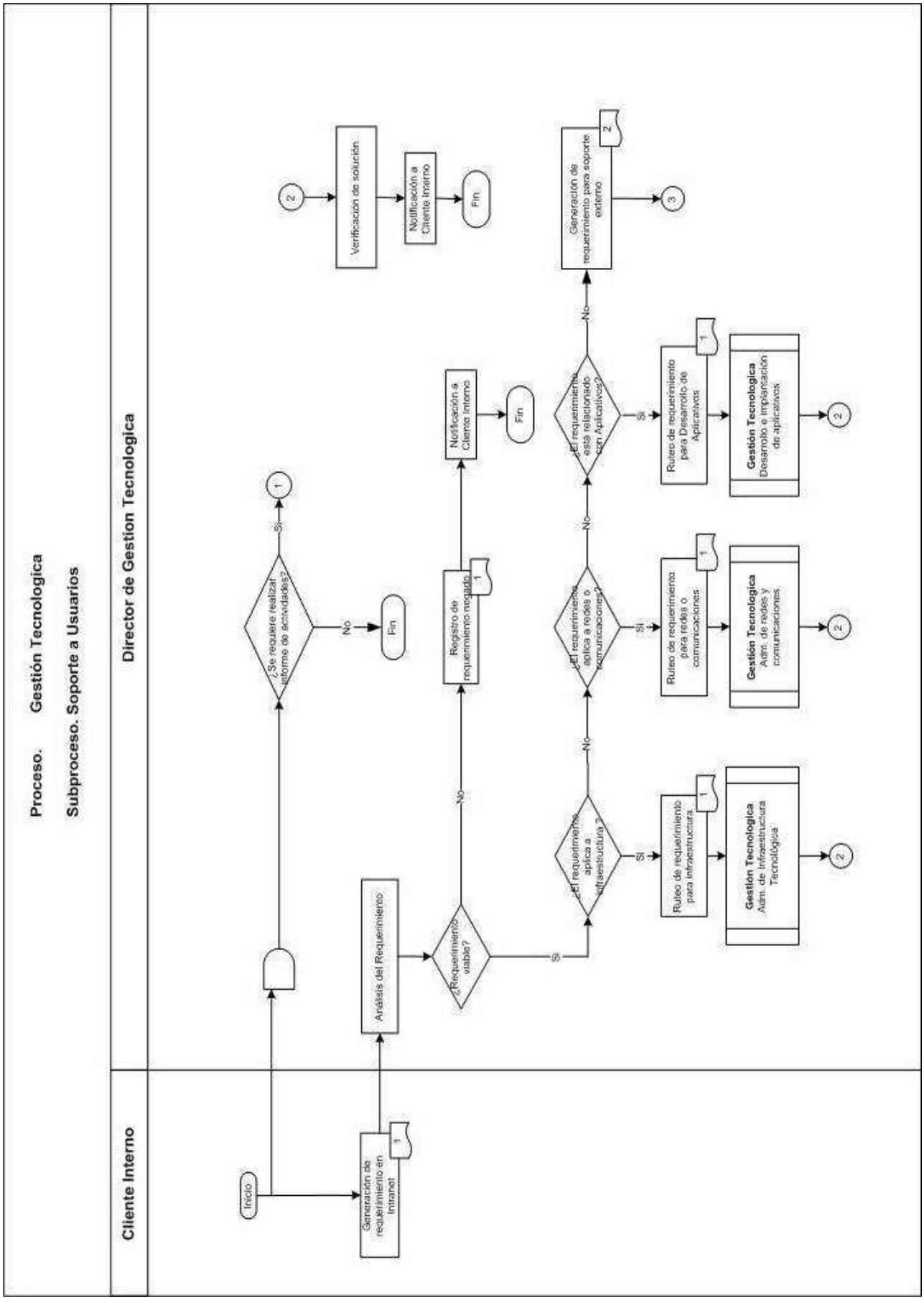
ANEXO F. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE SEGURIDADES


Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica (Administración de Seguridades)
Técnico de Software
Inicio
Gestión Tecnologica
Gestión Estratégica de TIC
Gestión Tecnologica
Soporte a Cliente Internos
Recepción de Cartera de Proyectos
Recepción de Requerimiento
9
¿Manejar proyecto de seguridades?
No
Si
Revisión de políticas de administración de infraestructura
¿Administrar perfiles de Cliente interno?
Si
4
No
¿Manejar virus?
Si
5
No
Fin
Ajuste de la planificación del proyecto
1
Ejecución del proyecto
2
Fin
¿Realizar o restaurar backups?
Si
1
No
¿Monitorear o ajustar seguridades?
Si
2
No
¿manejar contingencia?
Si
3
No
¿Informe de actividades y avance de proyectos?
Si
Elaboración de informe mensual
7
Fin


Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica (Administración de Seguridades)
Técnico de Software
Técnico de Hardware / Software
Director de Gestion Tecnologica
Revisión de las políticas de backup y recuperación
¿Realizar backups?
Si
No
Preparación y etiquetado de medios magnéticos
Selección de medios magnéticos
Ejecución de backup según calendario
Ejecución de recuperación
Registro en bitácora de respaldos
Registro en bitácora de respaldos
¿Enviar medios fuera de la SENAMI?
Si
No
Envio de medios a caja fuerte externa
Almacenamiento de respaldos en caja fuerte de Gestión Tecnologica
Notificación a Soporte a Cliente Internos
Fin
Revisión de Políticas de Seguridad
Monitoreo de disponibilidad de los servicios y alertas de seguridad
Elaboración de informe de monitoreo
¿Realizar ajustes de seguridades?
Si
No
Ajuste de seguridades
Crear / ajustar política o procedimiento?
Si
No
Fin
Requerimiento de ajuste de política o procedimiento
Gestion Estrategica Tecnologica
Generación de Políticas, procedimientos y metodologías
Revisión del plan de contingencias
Generación de plan de acción
Ejecución de plan de acción
Elaboración de informe
Fin


Proceso. Gestión Tecnologica
Subproceso. Administración de Infraestructura Tecnológica (Administración de Seguridades)
Técnico de Software
4
¿Crear perfil de Cliente Interno?
Si
Creación de perfil de Cliente Interno
No
¿Modificar perfil de Cliente Interno?
Si
Modificación de perfil de Cliente Interno
No
¿Eliminar perfil de Cliente Interno?
Si
Eliminación de perfil de Cliente Interno
No
Registro de Solución
9
Fin
5
Revisión de bitacora del antivirus (suite)
¿Virus eliminado?
No
Notificación a Cliente interno necesidad de formateo
Salvado de datos y formateo de máquina
Instalación de software y restauración de datos
Si
Registro de Solución
9
Fin
Documentos.
1) Plan de proyecto. a. Archivo de Sistemas Informáticos
2) Documentación de seguimiento de proyecto.
a. Responsable de proceso. b. Archivo de Sistemas Informáticos
3) Bitácora de respaldos. a. Archivo de Sistemas Informáticos
4) Informe de monitoreo. a. Director de Gestión T.. b. Archivo de Sistemas Informáticos
5) Requerimiento de ajuste de política o procedimiento.
a. Director de Información b. Archivo de Sistemas Informáticos
6) Nota de entrega de medios. a. Proveedor caja fuerte externa b. Archivo de Sistemas Informáticos
7.) Informe mensual. a.Director de Gestion T.. b. Archivo de Sistemas Informáticos
8) Informe de solución de contingencia. a. Subsecretario General. b. Archivo de Sistemas Informáticos
9) Requerimiento informático

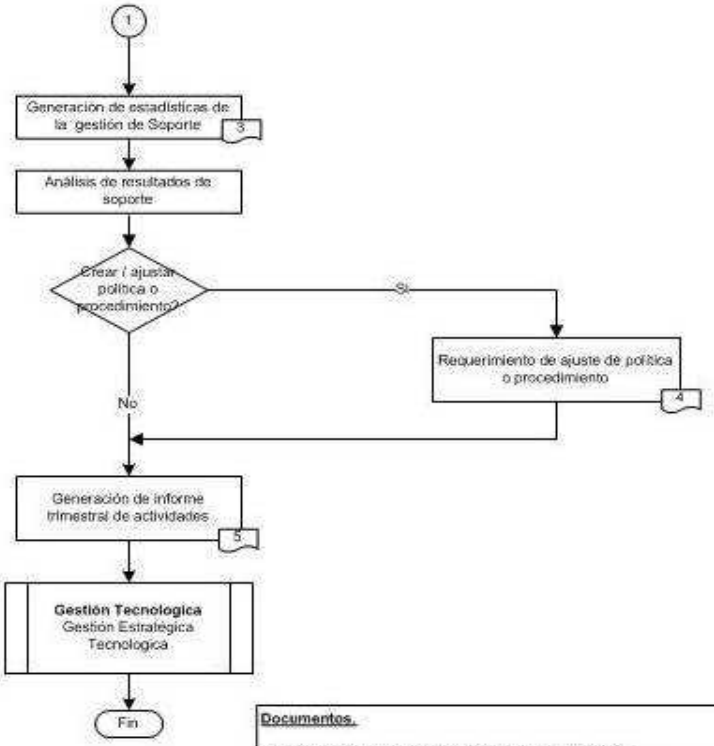
ANEXO G. PROCEDIMIENTO. SUBPROCESO. SOPORTE A USUARIOS


Proceso. Gestión Tecnologica
Subproceso. Soporte a Usuarios
Cliente Interno
Director de Gestion Tecnologica
Inicio
Generación de requerimiento en Intranet
Análisis del Requerimiento
¿Requerimiento viable?
No
Registro de requerimiento negado
Notificación a Cliente Interno
Fin
Si
¿El requerimiento aplica a infraestructura?
Si
Ruteo de requerimiento para Infraestructura
Gestión Tecnologica
Adm. de Infraestructura Tecnológica
No
¿El requerimiento aplica a redes o comunicaciones?
Si
Ruteo de requerimiento para redes o comunicaciones
Gestión Tecnologica
Adm. de redes y comunicaciones
No
¿El requerimiento esta relacionado con Aplicativos?
Si
Ruteo de requerimiento para Desarrollo de Aplicativos
Gestión Tecnologica
Desarrollo e implantación de aplicativos
No
Generación de requerimiento para soporte externo
¿Se requiere realizar informe de actividades?
Si
No
Fin
Verificación de solución
Notificación a Cliente Interno
Fin

Proceso. Gestión Tecnologica

Subproceso. Soporte a Usuarios

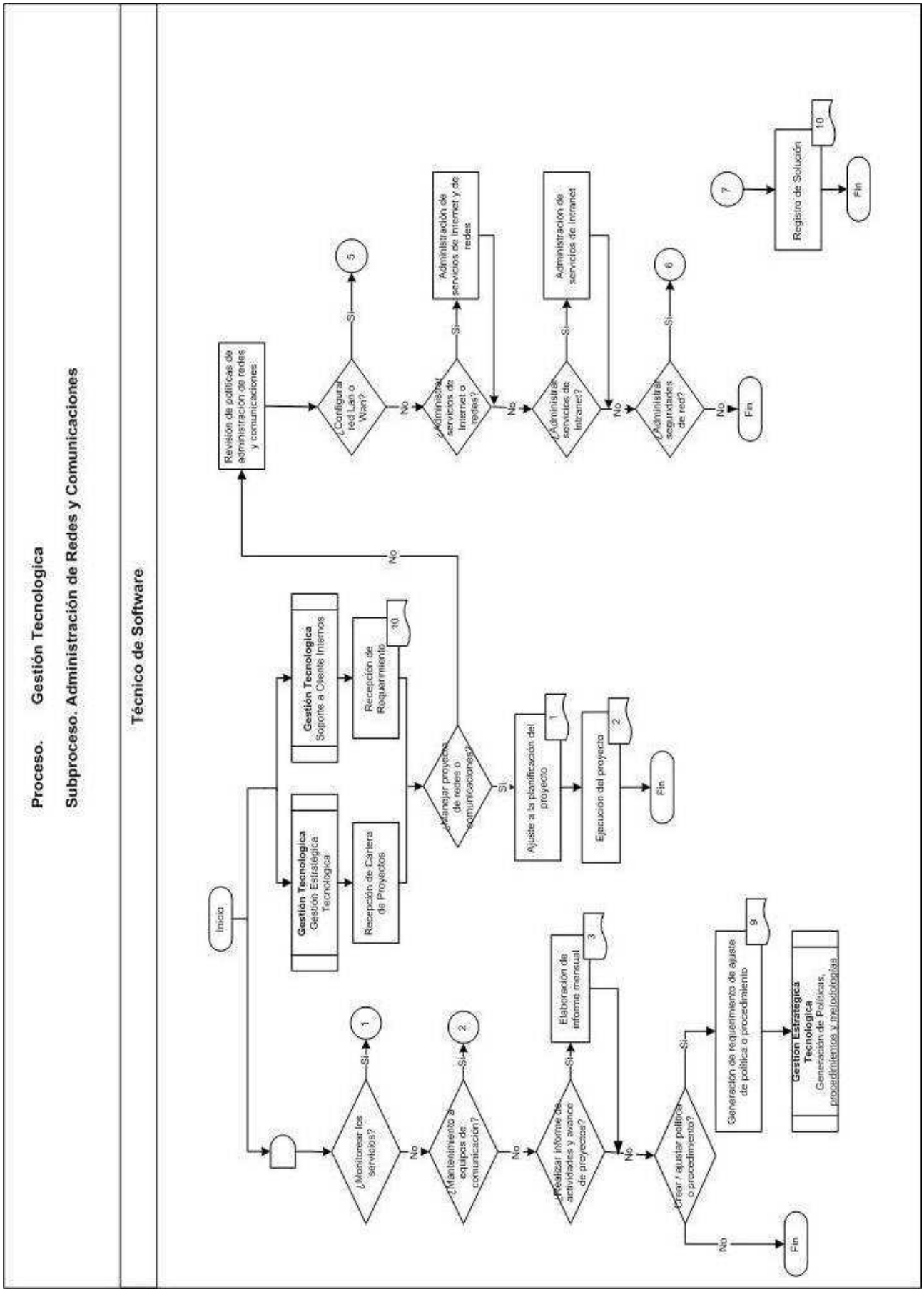
Proveedor	Técnico de Software

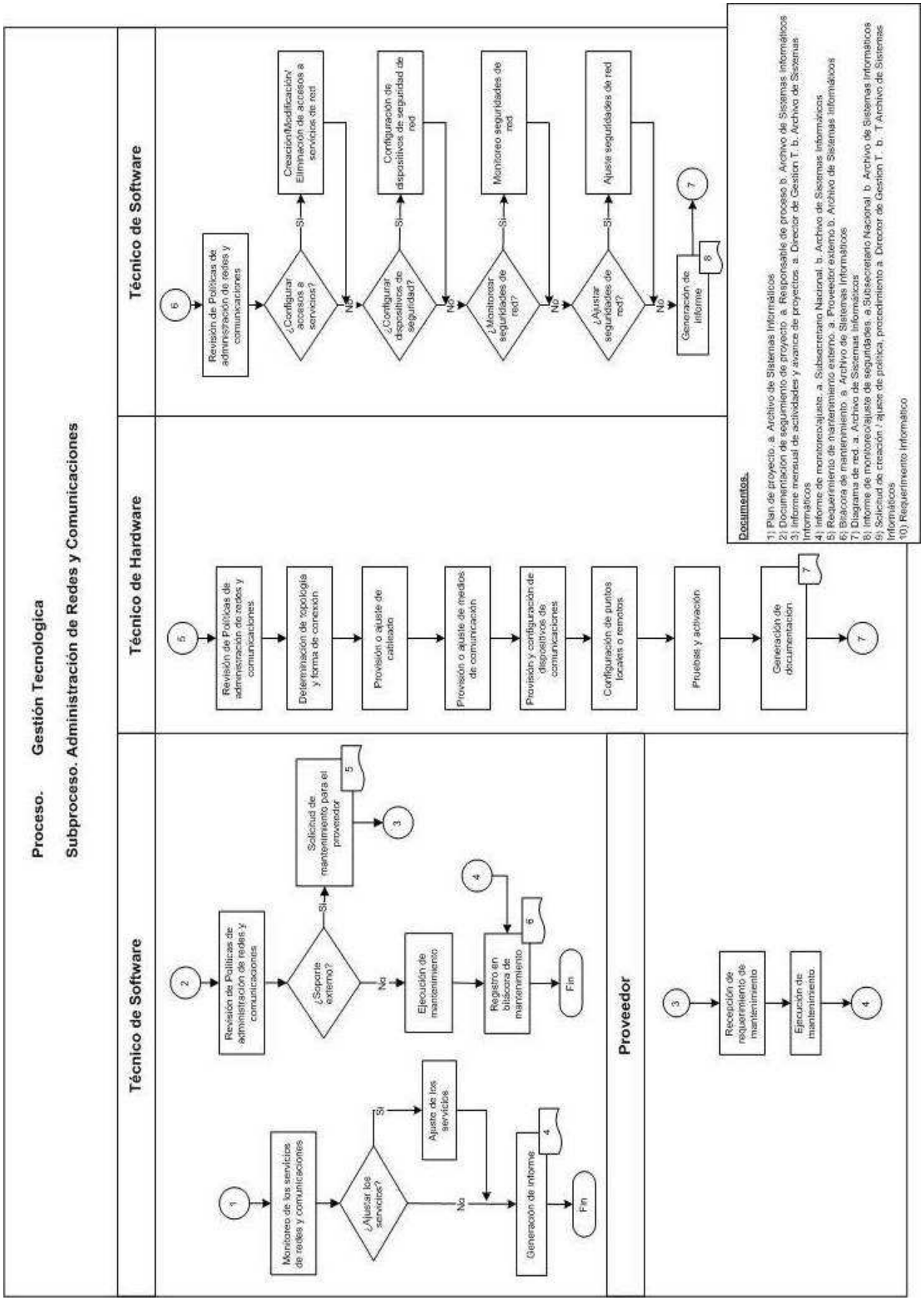


Documentos.

1) Requerimiento Informático. a. Intranet de la SENAMI
2) Requerimiento de Soporte externo. a. Proveedor externo b. Archivo de Sistemas Informáticos
3) Estadísticas de la gestión de Soporte. a. Director de Gestion T. b. Archivo de Sistemas Informáticos
4) Requerimiento de ajuste a políticas o procedimientos. a. Director de Gestion T. b. Archivo de Sistemas Informáticos
5) Informe trimestral de actividades. a. Director de Gestion T. b. Archivo de Sistemas Informáticos

ANEXO H. PROCEDIMIENTO. SUBPROCESO. ADMINISTRACIÓN DE REDES Y COMUNICACIONES


Proceso. Gestión Tecnologica
Subproceso. Administración de Redes y Comunicaciones
Técnico de Software
Inicio
Gestión Tecnologica
Gestion Estrategica Tecnologica
Gestión Tecnologica
Soporte a Clientes Internos
Recepción de Cartera de Proyectos
Recepción de Requerimiento
10
¿Manejar proyecto de redes o comunicaciones?
Si
No
Ajuste a la planificación del proyecto
1
Ejecución del proyecto
2
Fin
Revisión de políticas de administración de redes y comunicaciones
¿Configurar red Lan o Wan?
5
Si
No
¿Administrar servicios de Internet o redes?
Administración de servicios de Internet y de redes
¿Administrar servicios de Intranet?
Administración de servicios de Intranet
¿Administrar seguridades de red?
6
Fin
7
Registro de Solución
10
Fin
¿Monitorear los servicios?
1
¿Mantenimiento a equipos de comunicación?
2
¿Realizar informe de actividades y avance de proyectos?
Elaboración de informe mensual
3
¿Crear / ajustar política o procedimiento?
Generación de requerimiento de ajuste de política o procedimiento
9
Gestion Estrategica Tecnologica
Generación de Políticas, procedimientos y metodologías
Fin


Proceso. Gestión Tecnologica
Subproceso. Administración de Redes y Comunicaciones
Técnico de Software
Técnico de Hardware
Técnico de Software
Proveedor
Monitoreo de los servicios de redes y comunicaciones
¿Ajustar los servicios?
Si
No
Ajuste de los servicios
Generación de informe
Fin
Revisión de Políticas de administración de redes y comunicaciones
¿Soporte externo?
Si
No
Solicitud de mantenimiento para el proveedor
Ejecución de mantenimiento
Registro en bitácora de mantenimiento
Fin
Recepción de requerimiento de mantenimiento
Ejecución de mantenimiento
Revisión de Políticas de administración de redes y comunicaciones
Determinación de topología y forma de conexión
Provisión o ajuste de cableado
Provisión o ajuste de medios de comunicación
Provisión y configuración de dispositivos de comunicaciones
Configuración de puntos locales o remotos
Pruebas y activación
Generación de documentación
Revisión de Políticas de administración de redes y comunicaciones
¿Configurar accesos a servicios?
Si
No
Creación/Modificación/ Eliminación de accesos a servicios de red
¿Configurar dispositivos de seguridad?
Si
No
Configuración de dispositivos de seguridad de red
¿Monitorear seguridades de red?
Si
No
Monitoreo seguridades de red
¿Ajustar seguridades de red?
Si
No
Ajuste seguridades de red
Generación de informe
Documentos.
1) Plan de proyecto. a. Archivo de Sistemas Informáticos
2) Documentación de seguimiento de proyecto. a. Responsable de proceso b. Archivo de Sistemas Informáticos
3) Informe mensual de actividades y avance de proyectos. a. Director de Gestion T. b. Archivo de Sistemas Informáticos
4) Informe de monatoreo/ajuste. a. Subsecretario Nacional. b. Archivo de Sistemas Informáticos
5) Requerimiento de mantenimiento externo. a. Proveedor externo b. Archivo de Sistemas Informáticos
6) Bitácora de mantenimiento. a. Archivo de Sistemas Informáticos
7) Diagrama de red. a. Archivo de Sistemas Informáticos
8) Informe de monitoreo/ajuste de seguridades. a.Subsecretario Nacional b. Archivo de Sistemas Informáticos
9) Solicitud de creación / ajuste de política, procedimiento a. Director de Gestion T. . b. T.Archivo de Sistemas Informáticos
10) Requerimiento Informático