VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD
UNIDAD DE GESTIÓN DE POSTGRADOS

MAESTRIA EN GERENCIA DE SISTEMAS
IX PROMOCION

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: MODELO DE GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DEL CENTRO DE DATOS DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES POLICÍA NACIONAL, APLICANDO COBIT 4.1 DOMINIO PLANIFICAR Y ORGANIZAR

AUTORES
ING. ALDÁS SÁNCHEZ GABRIELA DE LOS ÁNGELES
ING. ARIAS MIÑO NÉSTOR GONZALO

DIRECTOR: ING. PROCEL SILVA CARLOS TEIRON MSc.

SANGOLQUÍ

2016

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD
UNIDAD DE GESTIÓN DE POSTGRADOS

MAESTRÍA EN GERENCIA DE SISTEMAS
IX PROMOCIÓN

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***MODELO DE GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DEL CENTRO DE DATOS DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES POLICÍA NACIONAL, APLICANDO COBIT 4.1 DOMINIO PLANIFICAR Y ORGANIZAR***" realizado por los señores **INGENIERA GABRIELA DE LOS ÁNGELES ALDÁS SÁNCHEZ E INGENIERO NÉSTOR GONZALO ARIAS MIÑO**, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar a los señores **INGENIERA GABRIELA DE LOS ÁNGELES ALDÁS SÁNCHEZ E INGENIERO NÉSTOR GONZALO ARIAS MIÑO** para que lo sustenten públicamente.

Sangolquí, 06 de enero de 2016

ING. CARLOS TEIRON PRÓCEL SILVA, MS.

DIRECTOR

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD
UNIDAD DE GESTIÓN DE POSTGRADOS

MAESTRIA EN GERENCIA DE SISTEMAS
IX PROMOCION

AUTORÍA DE RESPONSABILIDAD

Nosotros, **INGENIERA GABRIELA DE LOS ÁNGELES ALDÁS SÁNCHEZ** con cédula de identidad N° 1713987137 e **INGENIERO NÉSTOR GONZALO ARIAS MIÑO**, con cédula de identidad N° 1709393399, declaramos que este trabajo de titulación "***MODELO DE GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DEL CENTRO DE DATOS DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES POLICÍA NACIONAL, APLICANDO COBIT 4.1 DOMINIO PLANIFICAR Y ORGANIZAR***" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 06 de enero de 2016

GABRIELA ALDÁS SÁNCHEZ
CC: 1713987137

GONZALO ARIAS MIÑO
CC: 1709393399

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD
UNIDAD DE GESTIÓN DE POSTGRADOS

MAESTRIA EN GERENCIA DE SISTEMAS
IX PROMOCION

AUTORIZACIÓN

Nosotros, **INGENIERA GABRIELA DE LOS ÁNGELES ALDÁS SÁNCHEZ** e **INGENIERO NÉSTOR GONZALO ARIAS MIÑO**, autorizamos a la Universidad de las Fuerzas ESPE publicar en la biblioteca Virtual de la institución el presente trabajo de titulación "***MODELO DE GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN DEL CENTRO DE DATOS DE LA DIRECCIÓN NACIONAL DE COMUNICACIONES POLICÍA NACIONAL, APLICANDO COBIT 4.1 DOMINIO PLANIFICAR Y ORGANIZAR***" cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 06 de enero de 2016

GABRIELA ALDÁS SÁNCHEZ
CC: 1713987137

GONZALO ARIAS MIÑO
CC: 1709393399

DEDICATORIA

Dedicamos el presente trabajo a nuestros familiares porque son el pilar fundamental de nuestras vidas y a quienes ofrendamos todos nuestros esfuerzos y sacrificios.

A la Dirección Nacional de Comunicaciones y a sus Directores, quienes facilitaron y permitieron la elaboración del presente proyecto y a su vez a todo el personal del Centro de Datos que en todo momento colaboraron ante nuestros requerimientos.

AGRADECIMIENTO

En primera instancia al Arquitecto Todopoderoso del Universo; Dios, que en su grandeza nos ha permitido llegar hasta éste justo momento y lugar, con bienestar y fortaleza, llenando nuestros espíritu de júbilo y esperanza de mejores días.

A nuestros familiares quienes en todo momento apoyaron nuestro sacrificio y esfuerzo para la consecución de este objetivo, que sin duda también es de ellos.

A nuestro Director de Proyecto, Ing. Carlos Prócel Silva MSc, quien nos apoyó incondicionalmente para la consecución de nuestro objetivo, compartiendo con nosotros sus grandes capacidades profesionales, docentes y personales.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto es una investigación realizada para la implementación de un modelo de gestión de TI, en el Centro de Datos de la Dirección Nacional de Comunicaciones de la Policía Nacional fundamentados en las mejores prácticas. Este Centro de Datos, concentra la principal infraestructura de TI para el cumplimiento de las tareas operativas policiales que se apoyan en el uso de datos e información confiable y disponible en todo momento, por lo cual se considera de importancia crítica para garantizar la misión Institucional de brindar seguridad y protección a la ciudadanía y sus bienes. Los estándares internacionales aseguran el cumplimiento efectivo de los objetivos de TI de cualquier Institución sea pública o privada. Para este proyecto hemos seleccionado a COBIT como fundamento para proponer un modelo de gestión por su versatilidad y adaptabilidad a la situación actual del Centro de Datos. Es indispensable la implementación de buenas prácticas y un modelo de gestión de TI efectivo, para asegurar el cumplimiento de los procesos de gestión tecnológica de la Policía Nacional que cumplan con normas exigidas por las entidades Gubernamentales como la Contraloría, Fiscalía, Función Judicial entre otros en nuestro país y la INTERPOL a nivel internacional. Mediante la ejecución del proyecto, se prevé alcanzar un nivel de gestión de TI administrado óptimamente y medible en sus actividades, para permitir a la esfera gerencial de la Dirección Nacional de Comunicaciones, tomar decisiones en el mejoramiento permanente de sus servicios a la Policía Nacional.

PALABRAS CLAVE

COBIT
MODELO DE GESTIÓN
PROCESO
POLICÍA NACIONAL,
MODELO DE MADUREZ

ABSTRACT

The following project is an investigation with the purpose of the IT management model implementation at Centro de Datos de la Dirección Nacional de Comunicaciones de la Policía Nacional based in the best practices. This data center focuses in the main infrastructure of the IT for the accomplishment of the operative policial tasks, which uses the reliable and available data and information at any moment. Therefore, it is considered of crucial priority for the assurance of the Institutional mission to bring security and protection for the community and their goods. The international standards assure the effective accomplishment of the IT objectives coming from any type of Institution, whether being public or private. For this project, we have elected a COBIT as the modeling tool for its versatility and adaptability for the data center current situation. It is fundamental to implement the good practices and management model for the IT effectiveness, to guarantee the fulfillment of the technological management processes of the National Police and that also accomplishes with the governmental policies such as: Contraloría, Fiscalía, Función Judicial among others, inside the country and the INTERPOL at an international level. Throughout the application of the project, it is expected to achieve a management IT level which is administrated optimally and measurably in its activities, to allow the management level of the Dirección Nacional de Comunicaciones, take the best decisions for the improvement of its services for the National Police.

KEY WORDS

COBIT
MODELO DE GESTIÓN
PROCESO
POLICÍA NACIONAL,
MODELO DE MADUREZ

CAPÍTULO I

GENERALIDADES

1.1 Introducción

La Policía Nacional es una Institución de servicio público, que fundamenta su accionar en su misión establecida en el Art. 163, de la Constitución de la República del Ecuador del 2008, (ECUADOR, CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, 2008) que dice:

> La Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional. (p. 88).

Dentro de su estructura orgánica se encuentra la Dirección Nacional de Comunicaciones, que tiene como misión:

> Liderar la prestación de los servicios de comunicaciones e informática, a través de una constante preparación del elemento humano y la utilización de la tecnología adecuada, que garantice la eficacia y eficiencia en su empleo, en beneficio institucional y de la comunidad. (Orgánico Funcional de la Dirección Nacional de Comunicaciones, 2000, p.17)

La Dirección Nacional de Comunicaciones es el órgano técnico que regula y genera las políticas en materia de Tecnología para apoyar las labores de la Policía para optimizar la gestión institucional.

Dentro de la estructura orgánica de la Dirección Nacional de Comunicaciones existe una sección denominada Centro de Proceso de Datos cuyo objetivo primordial es la administración y control de los diferentes sistemas informáticos y de comunicaciones que son utilizados por las diferentes unidades policiales a nivel nacional.

Los objetivos de la Dirección Nacional de Comunicaciones están alineados con el Plan Estratégico de la Policía Nacional 2013- 2017, que constituye una herramienta para el desarrollo integral de la Policía Nacional; permite construir con éxito los

objetivos en él planteados, orientando todas las acciones hacia el logro de la visión institucional.

El Plan Estratégico de la Policía Nacional ha sido reformulado de acuerdo al Plan Nacional del Buen Vivir, que es el marco de referencia para las acciones que este gobierno debería cumplir para lograr sus objetivos.

Según la disposición de la Constitución de la República del Ecuador del 2008contenida en el:

> Art. 280.- El Plan Nacional de Desarrollo hoy denominado Plan Nacional para el Buen Vivir, es el instrumento al que se sujetarán las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto del Estado; y la inversión y la asignación de los recursos públicos; y coordinar las competencias exclusivas entre el Estado central y los gobiernos autónomos descentralizados. Su observancia será de carácter obligatorio para el sector público e indicativo para los demás sectores. (p. 132).

De igual manera debemos mencionar que está en ejecución el PLAN ESTRATÉGICO DE LA POLICÍA NACIONAL DEL ECUADOR 2013-2017, (Interior, 2013) que propone el mejoramiento del servicio que brinda la Institución hacia la ciudadanía, a través de 7 objetivos estratégicos:

El presente proyecto se alinea al Objetivo Estratégico 2, que es **Incrementar la efectividad operativa de los servicios policiales**, con las siguientes acciones:

- Desarrollar investigaciones, diagnósticos periódicos y prospectivos de los incidentes de seguridad ciudadana.
- Sistematizar la planificación de las operaciones policiales sobre la base de georeferenciación del delito a nivel nacional.
- Mejorar los sistemas de control de las operaciones policiales.
- Mejorar el sistema de evaluación operativa policial.

1.2 Justificación e Importancia

El vertiginoso y constante crecimiento y, desarrollo de las Tecnologías de la Información y Comunicaciones a nivel mundial, de las cuales nuestro país no puede

abstraerse, han determinado que cada vez más sea necesaria la formación y capacitación de profesionales competentes capaces de gestionar estas tecnologías, orientadas a satisfacer los requerimientos tanto de empresas públicas como privadas.

La continua evolución de la especie humana, ha estado marcada por el desarrollo y la aplicación de tecnologías que le han permitido superar exitosamente los desafíos que la historia le ha impuesto. Actualmente, nos encontramos en uno de esos instantes, el desafío es la globalización, y las tecnologías de información y comunicaciones que conforman los Sistemas de Infocomunicaciónes, están cambiando de una manera radical, la forma como nos relacionamos los seres que habitamos este planeta, para dar cabida a esta nueva realidad socio-económica-c.

El desarrollo tecnológico de la industria de la información y las comunicaciones, se ha convertido en uno de los fenómenos más significativos en el ámbito de las relaciones sociales y el quehacer empresarial, acelerando y cambiando rápidamente las formas colectivas de informarse, comunicarse y vivir. El concepto tradicional de distancia ha desaparecido, estamos a un "clic del mouse del computador" del resto del mundo. El Internet ha dejado de ser un fenómeno tecnológico para convertirse en un fenómeno cultural.

Las Tecnologías de la Información y las Comunicaciones (TIC’s) son definidas como el conjunto de recursos y métodos que, convenientemente asociados, permiten el adecuado registro, tratamiento, transformación, almacenamiento, acceso, utilización, presentación y circulación de la información.

Los sistemas de Infocomunicaciones permanentemente están cambiando nuestro trabajo y nuestra forma de vida. Las herramientas de comunicación global basadas en la computadora personal y otros inventos tecnológicos definen un nuevo espacio para la investigación científica, los negocios y la interacción social.

Las posibilidades que estas tecnologías abren, en lo referente a la disponibilidad y accesibilidad de la información así como a la rapidez y facilidad para distribuirla y compartirla, están actuando a modo de motor en la transformación de las relaciones entre individuos y entre organizaciones.

En una primera fase, se trató de una alteración aparentemente simple: lo que cambió no fue lo que se hacía, sino el modo de hacerlo. A medida que las herramientas que estuvieron detrás se difundieron y que las ventajas de este primer

cambio se hicieron evidentes, la propia mutación se modificó, y se avanzó hacia una segunda fase, en la cual la modificación instrumental de un entorno estable dejó su lugar a una transformación sociocultural, a la aparición de un nuevo paradigma que, como tal, incluye esos nuevos modelos de comportamiento, esas nuevas actividades y esas nuevas expectativas que caracterizan a la Sociedad de la Información y del Conocimiento.

Esta relación entre tecnologías avanzadas y cambio social no es unidireccional ni estática, sino recíproca y dinámica. A medida que los individuos y las organizaciones van contribuyendo al cambio y adaptándose a él en las áreas que les conciernen, demandan, cada vez con mayor insistencia, que el resto de organizaciones con las que se relacionan hagan lo mismo; de este modo, las tecnologías avanzadas son percibidas no sólo como un agente de transformación social sino también como una exigencia de esa sociedad dinámica y como una fuente de ventaja competitiva.

Los tipos de trabajo que esta sociedad de información demanda, son distintos de los que se conocieron. Hoy en día se requieren nuevas habilidades y el desarrollo de las destrezas esenciales en el manejo de tecnologías de la información es tan necesario como la lectura, la escritura o los conocimientos matemáticos básicos. La formación en estas herramientas será determinante en términos de acceso al mundo laboral.

Los negocios de las organizaciones tienden a ser globales, y todas ellas tendrán que implantar modernas infraestructuras tecnológicas para potenciar su actividad y competitividad, y así prestar nuevos servicios hasta ahora no imaginados, o atender expectativas de los clientes que no podían ser satisfechas con los medios tradicionales.

También las empresas de Servicio Público han encontrado en los Sistemas de Infocomunicaciones, la posibilidad de lograr una mayor y mejor atención igualitaria a todos los ciudadanos, por medio de una mayor integración de los diferentes sistemas de información correspondientes a las distintas esferas del gobierno central y de los gobiernos seccionales. Actualmente, se hace imprescindible el diseño, por parte de las diferentes Administraciones Públicas, de políticas y estrategias corporativas en la introducción y en la gestión de las tecnologías de la información y de las comunicaciones, así como la búsqueda de acuerdos sobre la compatibilidad de

los sistemas de información, dando lugar a lo que se conoce como “Gobierno Electrónico”.

Por otra parte, constituye una tarea de trascendental importancia, asegurar la privacidad y confidencialidad de la información que puede afectar a los ciudadanos en su vida personal y a las organizaciones en el desarrollo legal y legítimo de sus actividades, situación que se pone ampliamente de manifiesto en las actividades de comercio electrónico y gobierno electrónico que el Ecuador está empeñado en desarrollar dentro de los próximos años.

Ante este escenario, se precisa generalizar el conocimiento sobre estas nuevas herramientas y disminuir las barreras que dificultan su utilización y su implantación, apoyando de esa manera la innovación tecnológica en las Organizaciones y la Sociedad en general.

El Gobierno Nacional, preocupado por el desarrollo científico y tecnológico de nuestro país, está impulsando e incentivando totalmente, la masificación del uso de las tecnologías de información y comunicaciones, en instituciones públicas y centros de educación a todo nivel, así como en empresas privadas.

Actualmente se trabaja con el concepto de Gobierno en línea, lo que significa que las instituciones del Estado se conecten a la red para recibir pagos y contratar mediante Internet.

Por ello, hoy en día se requieren nuevas habilidades y la aplicación de “Buenas Practicas” se transformó en una frase frecuente en el mundo de los negocios actual. Desde la compra de equipos hasta la gestión del centro de datos o los procesos de flujo de trabajo, siempre hay una lista de pasos por cumplir y varios factores que deben tenerse en cuenta para aumentar las posibilidades de éxito. Sin embargo, no siempre es fácil implementar estas listas en la vida real, donde la complejidad de los procesos y la naturaleza caótica de las empresas activas dificultan la imposición de una estructura.

La Policía Nacional como una Institución fundamental dentro de la estructura del Estado Ecuatoriano, no es ajena a esta realidad, en la última década ha tenido grandes transformaciones en el ámbito tecnológico, es así que el Centro de Datos de la Dirección Nacional de Comunicaciones de la Policía Nacional, tiene bajo su responsabilidad la administración y control de los diferentes sistemas informáticos y

de comunicaciones policiales, por esto se propone el desarrollo de un modelo que permita mejorar la gestión de las Tecnologías de Información aplicando COBIT 4.1 en el dominio planificar y organizar.

1.3 Planteamiento del problema

La Policía Nacional del Ecuador al ser el ente encargado de proteger el orden público requiere de herramientas de TI, confiables, seguras y con alta disponibilidad. Al momento toda la infraestructura y servicios de TI se concentran en el Centro de Datos de la Dirección Nacional de Comunicaciones por lo que se debe contar con métricas y estándares internacionales de gestión de las mismas, por su alta criticidad y riesgo operativo.

La organización y la gestión de TI no están basadas en normas y estándares de buenas prácticas, situación que es corroborada por los estudios y auditorias técnicas realizadas por entes de control del Estado y cuerpos colegiados de alto nivel como es el caso de la ESPE, mismos que en años anteriores realizaron sendas auditorías a la operatividad del Sistema Informático Integrado de la Policía Nacional.

1.4 Formulación del problema

- ¿Es posible determinar el uso de procesos estandarizados en el Centro de Datos de la Dirección Nacional de Comunicaciones?
- ¿Es posible determinar una estructura organizacional en la gestión de las actividades del Centro de Datos de la Dirección Nacional de Comunicaciones?
- ¿Es posible determinar los roles y responsabilidades para el personal de TI?

1.5 Objetivo General

Diseñar un modelo de gestión de Tecnologías de Información del Centro de Datos de la Dirección Nacional de Comunicaciones Policía Nacional, aplicando COBIT 4.1 Dominio Planificar y Organizar 4.1.

1.6 Objetivos Específicos

- Definir la estructura organizacional del Centro de Datos alineados en los procesos PO4 y PO9.
- Establecer procesos de TI enfocados en los procesos PO4 y PO9.
- Establecer roles y responsables alineados en los procesos PO4 y PO9.
- Establecer Modelos de madurez alineados en los procesos PO4 y PO9.
- Establecer Mapas de control alineados en los procesos PO4 y PO9.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes del estado del arte

La estandarización de procesos de gestión de TI, es un hecho coyuntural que se aplica en las organizaciones de TI para lograr la efectividad en la prestación de sus servicios. Los estándares internacionalmente aceptados dan métricas de diseño e implementación de modelos de gestión estudiados ampliamente y con casos probados de éxito, que permiten a otras organizaciones acoger estas recomendaciones técnicas para la explotación de sus recursos de TI.

La Institución Policial encargada de velar por la seguridad ciudadana, requiere implementar "Buenas Prácticas" en la gestión de TI, que contribuyan con el cumplimiento de la misión Institucional.

En la actualidad no existen otros estudios similares que hagan referencia a la gestión administrativa de TI del Centro de Datos de la Dirección Nacional de Comunicaciones de la Policía Nacional, por este motivo se propone diseñar un modelo de gestión de las Tecnologías de la Información del Centro de Datos de la Dirección Nacional de Comunicaciones Policía Nacional, con la aplicación del marco de trabajo COBIT.

COBIT, al ser un estándar probado y reconocido en materia de "Buenas Practicas" de administración de TI, es el soporte del presente proyecto ya que ofrece una guía que se ajusta a los requerimientos del Centro de Datos de la Dirección Nacional de Comunicaciones.

2.2 Marco teórico

En la actualidad la Policía Nacional cuenta con unidades de tecnología descentralizadas en cada una de las Direcciones Generales, Nacionales o Unidades Especiales que gestionan TI, evidenciándose que sus funciones no se basan en las "Buenas Prácticas".

Es importante la elaboración del presente proyecto pues la aplicación de estándares internacionales de "Buenas Prácticas" contribuye al mejoramiento continuo y en la eficiencia de los servicios de TI brindados hacia la ciudadanía.

2.3 Marco Conceptual

Las organizaciones a nivel mundial consideran que la información es uno de los activos más valiosos que poseen, por ello es importante el manejo confidencial de la misma. Actualmente existen algunos estándares y "Buenas Prácticas", que direccionan la forma de administrar las TI.

Entre los estándares más utilizados en TI están los siguientes:

Tabla N° 1
Estándares de TI

TEMA	ESTÁNDAR
Gestión de TI	ISO 20000, ITIL, COBIT, MOF
Gestión de Seguridad	ISO 27000, NIST, COBIT Security baseline
Gestión de Calidad	ISO 9001
Gestión de Riesgo	ISO 31000, ISO 277005, COSO
Auditoria	ISO 19011, COBIT

2.3.1 Gestión de TI

ISO 20000

ISO20000 describe un conjunto integrado de procesos que permiten prestar en forma eficaz servicios de TI a las organizaciones y a sus clientes. (ISO) (ITIL)

ITIL Information Technology Infrastructure Library

Es un conjunto de "Buenas Practicas" destinadas a mejorar la gestión y provisión de servicios de TI. Su objetivo último es mejorar la calidad de los servicios TI ofrecidos, evitar los problemas asociados a los mismos y en caso de que estos ocurran ofrecer un marco de actuación para que estos sean solucionados con el menor impacto y a la mayor brevedad posible. (ITIL)

COBIT Control Objectives for Information and related Technology

Es el marco de trabajo que sirve para planear, organizar, dirigir y controlar toda la función informática dentro de una empresa. Actúa sobre la dirigencia y ayuda a estandarizar la organización. (isaca)

2.3.2 Gestión de Seguridad

ISO 27000 International Organization for Standardization

Es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por (NIST)cualquier tipo de organización, pública o privada, grande o pequeña. (ISO)

NIST

Se encarga de generar Publicaciones *draft*, es decir, un borrador, y versiones finales de sus recomendaciones, que consisten en elaborar y promover patrones de la medición, laborar estándares y la tecnología con el fin de realzar la productividad y facilitar el comercio y mejorar la calidad de vida. (NIST)

COBIT SECURITY BASELINE

Proporciona directrices sobre la adopción de un estándar de gobierno y control de TI; cubre la seguridad y otros riesgos que se producen en los ambientes de TI. (isaca)

2.3.3 Gestión de Calidad

ISO 9001

Es la base del sistema de gestión de la calidad ya que es una norma internacional y se centra en todos los elementos de administración de calidad, con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios. (ISO)

2.3.4 Gestión de Riesgo

ISO 31000

"Gestión del riesgo, principios y directrices" es un estándar desarrollado en colaboración por ISO e IEC que proporciona principios y directrices genéricas sobre la gestión del riesgo. Se trata de una norma general de aplicación a cualquier organización independientemente del tamaño o sector y que no es certificable. (ISO)

ISO 27005

Esta norma contiene recomendaciones y directrices generales para la gestión de riesgos en sistemas de seguridad de la Información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada como soporte

para aplicar satisfactoriamente un SGSI basado en un enfoque de gestión de riesgos. (ISO)

COSO

El informe COSO presenta una compilación de cuatro trabajos relacionados con el control interno de TI, referentes a: Definición, Componentes, Evaluación de Riesgos, Actividades de Control, Supervisión, Normas Generales del Control Interno, Misión y Objetivos, Asignación de Autoridad y Responsabilidad. (COSO)

ISO 19011

La nueva norma ISO 19011 proporciona una guía para que las organizaciones y los auditores entiendan el enfoque de las auditorias de sistemas de gestión, elaboren y gestionen el programa de auditorías y busquen la mejora en el desempeño de los auditores a través del desarrollo de su competencia. (ISO)

2.3.5 Estándares de Data Center

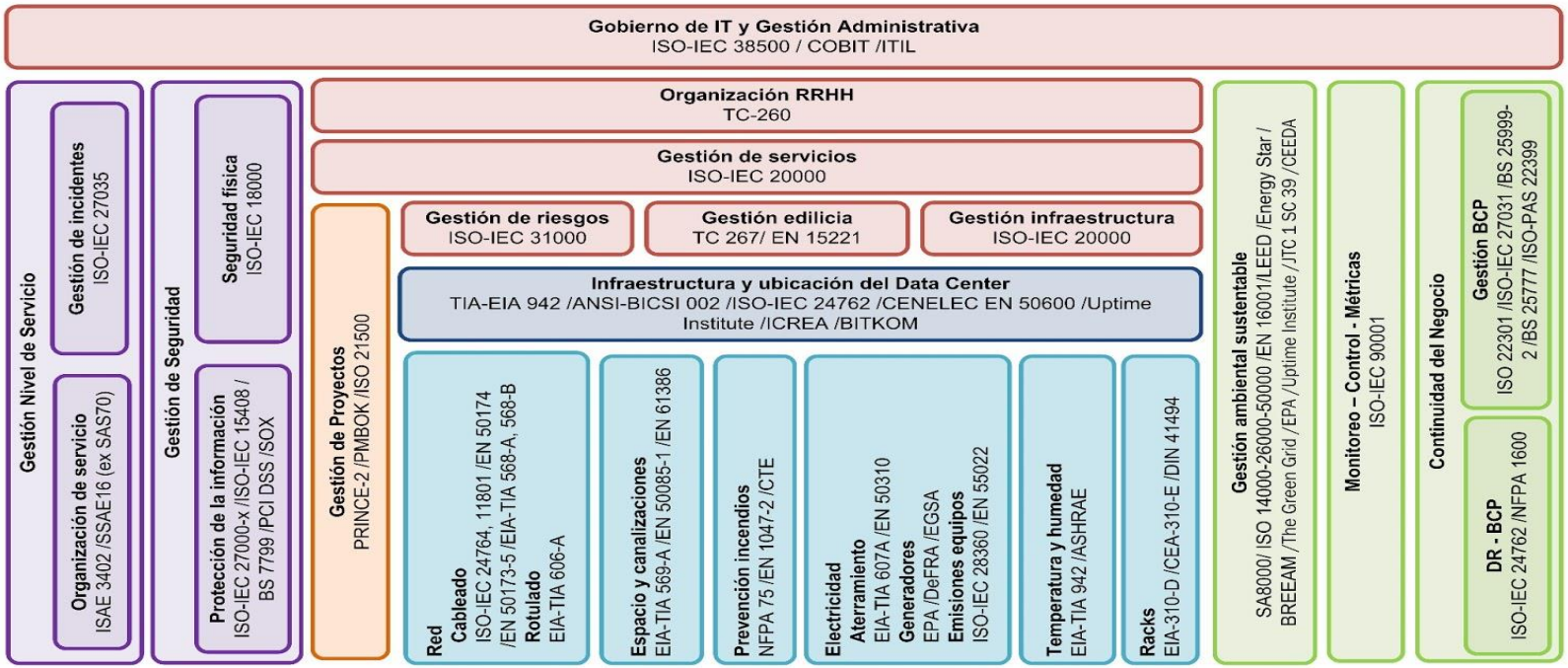
Se denomina Centro de Datos al lugar donde se concentran equipos y sistemas de TI para el procesamiento de la información, posee características especiales como: cableado estructurado, climatización, alimentación eléctrica estabilizada e

ininterrumpida, sistemas contra incendios, control de acceso, sistemas de video vigilancia, sistemas contra incendios, control de temperatura.

De la investigación realizada se determina que existen una infinidad de estándares que regulan la operatividad de un Centro de Datos, con el objetivo de tener una visión simplificada de todos los estándares y como se relacionan entre ellos, a continuación se presenta el Figura 1 elaborado por Germán Pacio (2013), en el cual se pueden observar cómo se encuentran agrupados los estándares y Frameworks más importantes en el mundo TI. (PACIO)

Además se puede observar la interrelación entre las diversas áreas ya que se hallan agrupados por módulos, que van desde la gestión de los recursos del Centro de Datos, hasta la gestión estrategia del Gobierno de IT (Figura 1).

Estándares en el Data Center



Los gráficos de burbujas representan subdivisiones por módulos agrupadas por color según el área de aplicación, en letra negrita se pueden el nombre de cada módulo o subdivisión. Los números representan los más estándares o Frameworks más importantes para ese módulo en particular.

Figura 1, Estándares de Data Center

Como podemos observar en esta representación el gobierno de TI es el módulo más importante dentro de la estructura de un Centro de Datos.

Dentro de lo que es el gobierno de TI, se menciona a COBIT, que se propone aplicar en el presente proyecto.

COBIT es "un marco de referencia que se enfoca en lo que se requiere para lograr una administración y un control adecuado de TI y contribuye en la organización de las actividades de TI a través de un modelo de procesos".

COBIT propone los siguientes productos: 1) El resumen informático al consejo sobre el gobierno de TI, 2da. Edición, diseñado para ayudar a los ejecutivos a entender porque el gobierno de TI es importante, 2) Directrices Gerenciales / Modelos de madurez, que ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas de capacidad, 3) Marco de Referencia, que explica como COBIT organiza los objetivos de gobierno y las "Buenas Practicas" de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio, 4) Objetivos de control, que brindan objetivos a la dirección basados en las "Buenas Practicas" genéricas para todos los procesos, 5) Guía de Implementación de Gobierno de TI, usando COBIT y Val TI 2da Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI, 6) Prácticas de Control de COBIT, que es una guía para conseguir los objetivos de control para el éxito de Gobierno de TI 2da edición que proporciona una guía de por qué vale la pena implementar controles y como implementarlos y 7) Guía de aseguramiento de TI que proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Metodología de la investigación

Se ha escogido a la investigación de tipo exploratoria como el patrón para el presente proyecto, conceptualmente la investigación exploratoria es el estudio de un tema o caso del que no conocemos con precisión su estado actual y del que no se disponen datos referenciales, es decir que no ha sido investigado anteriormente.

La investigación exploratoria cuenta con una gama de recursos y técnicas para su ejecución como la revisión de bibliografía especializada, búsqueda bibliográfica en internet, revisión documental institucional, entre otros. (Hernández, 1994) Estos recursos fundamentarán el actual trabajo.

Por otro lado la recolección de evidencias, entrevistas, observación in situ, análisis de datos operativos/administrativos existentes, también aportarán en el desarrollo del presente proyecto.

3.2 Ubicación Geográfica

El proyecto se lo desarrollará en la Dirección Nacional de Comunicaciones de la Policía Nacional, ubicado en la provincia de Pichincha, Cantón Quito, en el sector de La Gasca, el área de influencia específica es el Centro de Datos.

3.3 Método de investigación

3.3.1 El Método Analítico

El método analítico se refiere al análisis de las cosas o de los fenómenos; que proviene de la raíz griega análisis, que significa descomposición; significa examinar, descomponer o estudiar minuciosamente una cosa. Por tanto el método analítico comienza con el todo de un fenómeno y lo revisa parte por parte (descomposición del todo), comprendiendo su funcionamiento y su relación intrínseca.
(TESIS, ING. ALFREDO VÁSQUEZ ESPINOSA, 2008, p. 23.)

El método analítico a utilizarse en el presente proyecto refiere al estudio de la realidad técnica/operativa del Centro de Datos de la Dirección Nacional de Comunicaciones, tomando en cuenta que se tiene una determinada funcionalidad o finalidad operativa del mismo; en los que se concentran una serie de procesos que no están claramente definidos o identificados, los cuales posteriormente serán diagnosticados.

Como apoyo a la utilización del método analítico también utilizaremos el método deductivo, que en su conceptualización se refiere a que la deducción va de lo general a lo particular. Inicia en la recopilación de datos generales que se suponen verdaderos, para que a través del razonamiento lógico y la comprobación, determinen su validez absoluta.

Para la elaboración del presente proyecto utilizaremos las siguientes técnicas: entrevistas, inspección de archivos y observación in situ.

CAPITULO IV

MARCO DE TRABAJO COBIT

4.1 Importancia de la gestión de TI

La evolución de la sociedad ha hecho indispensable el uso de herramientas tecnológicas en casi todos los aspectos de su diario convivir. Todas las empresas para desarrollar sus actividades incluyen procesos y sistemas de tecnología para la consecución de sus objetivos. Las inversiones en TI son altas y costosas constituyéndose en parte de los activos empresariales.

La dependencia de las TIC´s en los procesos empresariales, ha hecho que se conformen departamentos especializados en el análisis, estudio y mantenimiento de éstas herramientas. Ligado a éstos departamentos de igual manera se han creado los conceptos de gobernabilidad de TI que se adaptan a las realidades estructurales y operacionales de las empresas. El término de "gobernabilidad de TI" es reciente e involucra un estudio profundo de las empresas a nivel de su constitución, procesos, estructura, fines y principalmente de sus capacidades para realizar inversiones en tecnología para conseguir sus objetivos y metas.

Enfocándonos en el concepto de "Gobierno de TI", es importante mencionar el uso de las herramientas tecnológicas en el ámbito gubernamental que se ha generalizado, incluyendo normativas y regulaciones que en la mayoría de los casos se han vuelto obligatorias. Ahora se menciona la importancia de las infraestructuras de TI como un patrimonio de los Estados y los datos e información como bienes intangibles de los mismos.

Ésta valoración, hace que el Gobierno de TI, sea fuente de estudio para las Instituciones públicas y privadas en el contexto nacional y que las normativas y estándares internacionales de las buenas prácticas en ésta materia, sean aprobados y reconocidas para su aplicación y/o adaptación a las realidades Institucionales.

4.2 Marco de trabajo COBIT 4.1

El Marco de trabajo COBIT 4.1 integra y concilia normas y reglamentaciones existentes como: ISO (9000-3), Códigos de Conducta del Consejo Europeo ISACF (1),COSO (2), IFAC, IIA, AICPA y otras, además incluye el contenido de los Objetivos de Control emitidos por ISACA. La misión de COBIT 4.1 es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.
(Cobit 4.1, 2007, p. 13)

4.3 Características de COBIT

A medida que pasa el tiempo cada vez más nos damos cuenta del impacto que la información aporta en el éxito de una empresa, basado en este precepto el marco de trabajo Cobit define razones de **por qué** se necesita el Gobierno de TI, los interesados (**quién**) y **qué** se necesita para cumplir con el gobierno de TI.
(Cobit 4.1, 2007, p. 9).

Por qué: la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos
- Cuente con un manejo juicioso de los riesgos que enfrenta
- Alinear la estrategia de TI con la estrategia del negocio
- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa

- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas
- Medir el desempeño de TI
- Se organicen sus actividades en un modelo de procesos generalmente aceptado
- Riesgos crecientemente complejos de TI como la seguridad de redes

Quién: "Un marco de referencia de gobierno y de control requiere servir a una variedad de interesados internos y externos, cada uno de los cuales tiene necesidades específicas" (Cobit 4.1, 2007, p. 9):

- Interesados dentro de la empresa que tienen interés en generar valor de las inversiones en TI:
  - – Aquellos que toman decisiones de inversiones
  - – Aquellos que deciden respecto a los requerimientos
  - – Aquellos que utilizan los servicios de TI
- Interesados internos y externos que proporcionan servicios de TI:
  - – Aquellos que administran la organización y los procesos de TI
  - – Aquellos que desarrollan capacidades
  - – Aquellos que operan los servicios
- Interesados internos y externos con responsabilidades de control/riesgo:
  - – Aquellos con responsabilidades de seguridad, privacidad y/o riesgo
  - – Aquellos que realizan funciones de cumplimiento
  - – Aquellos que requieren o proporcionan servicios de aseguramiento

Qué: "Para satisfacer los requerimientos previos, un marco de referencia para el gobierno y el control de TI, debe satisfacer las siguientes especificaciones generales" (Cobit 4.1, 2007, p. 9):

- Brindar un enfoque de negocios que permita la alineación entre las metas de negocio y de TI.
- Establecer una orientación a procesos para definir el alcance y el grado de cobertura, con una estructura definida.

- Ser generalmente aceptable al ser consistente con las mejores prácticas y estándares de TI aceptados, y que sea independiente de tecnologías específicas.
- Proporcionar un lenguaje común, con un juego de términos y definiciones que sean comprensibles en general para todos los Interesados.
- Ayudar a satisfacer requerimientos regulatorios, al ser consistente con estándares de gobierno corporativo generalmente aceptados (COSO) y con controles de TI esperados por reguladores y auditores externos.

4.4 Orientado al negocio

La orientación a negocios es el tema principal de COBIT. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.
(Cobit 4.1, 2007, p. 10)

El marco de trabajo COBIT se basa en el siguiente principio: Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida (Figura 2).

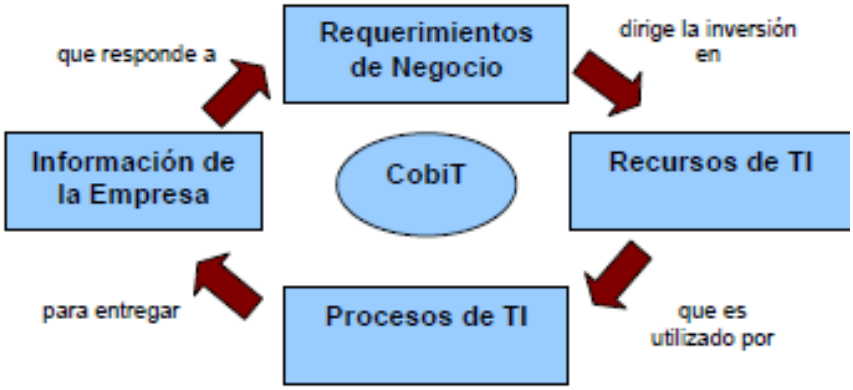


Figura 2, Procesos COBIT

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

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 más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- La **efectividad** tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- La **eficiencia** consiste en que la información sea generada con el óptimo (más productivo y económico.
- La **confidencialidad** se refiere a la protección de información sensitiva contra revelación no autorizada.
- La **integridad** está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La **disponibilidad** se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- El **cumplimiento** tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es

decir, criterios de negocios impuestos externamente, así como políticas internas.

- La **confiabilidad** se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

4.5 Metas de Negocio y de TI

Toda empresa usa TI para habilitar iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI. COBIT proporciona una matriz de metas genéricas de negocios y metas de TI y como se asocian con los criterios de la información.
(Cobit 4.1, 2007, p. 11)

Si se pretende que 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).

4.6 Recurso 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.
(Cobit 4.1, 2007, pág. 11)

Los recursos de TI identificados en COBIT se pueden definir como sigue:

Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

La información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

4.7 Orientado por procesos

COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar.
(Cobit 4.1, 2007, p. 12)

4.7.1 Planear y Organizar

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas.
(Cobit 4.1, 2007, pág. 12)

Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia
:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

4.7.2 Adquirir e implementar

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.
(Cobit 4.1, 2007, pág. 13)

Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

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

4.7.3 Entrega y Soporte

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos.
(Cobit 4.1, 2007, pág. 13)

Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

4.7.4 Monitorear y Evaluar

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.
(Cobit 4.1, 2007, pág. 13)

Por lo general abarca las siguientes preguntas de la gerencia:

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

4.8 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 se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Características:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:

- Seleccionando aquellos aplicables.
- Decidir aquellos que deben implementarse.
- Elegir como implementarlos (frecuencia, extensión, automatización, etc.)
- Aceptar el riesgo de no implementar aquellos que podrían aplicar.

4.9 Impulsado por la medición

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar. Para decidir el nivel correcto, la gerencia debe preguntarse: ¿Hasta dónde debemos ir?, y ¿está el costo justificado por el beneficio?
(Cobit 4.1, 2007, pág. 17)

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. COBIT atiende estos temas a través de:

- Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad
- Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard).
- Metas de actividades para facilitar el desempeño efectivo de los procesos.

4.10 Modelos de madurez

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior.

(Cobit 4.1, 2007, pág. 17)

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

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa
- El crecimiento requerido entre “como es” y “como será”

Para hacer que los resultados sean utilizables con facilidad en resúmenes gerenciales, donde se presentarán como un medio para dar soporte al caso de negocio para planes futuros, se requiere contar con un método Figura de presentación (Figura 3):

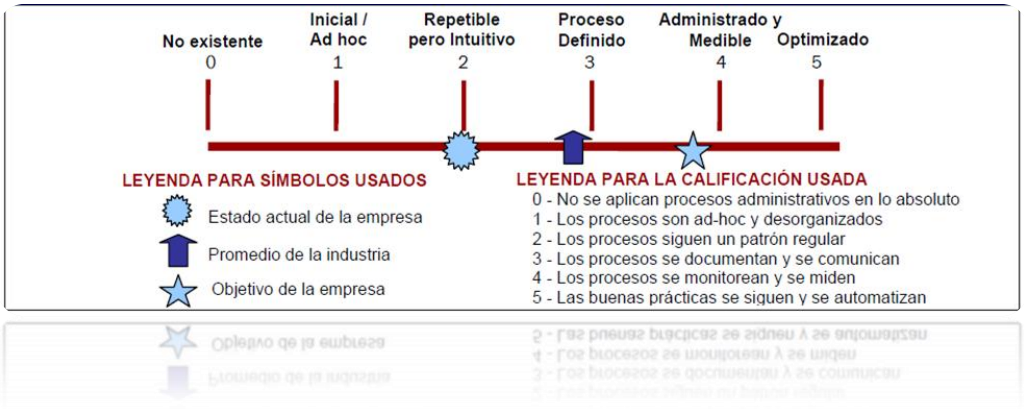


Figura 3. Modelo de Madurez

CAPÍTULO V

MODELO DE GESTIÓN

5.1 Diseño del modelo de gestión de tecnologías de Información del Centro de Datos de la Dirección Nacional de Comunicaciones.

5.1.1 *Descripción de la Empresa*

La Policía Nacional es una Institución de servicio público cuya misión fundamental es mantener el orden y la paz social. Su organización es de tipo jerárquico con funciones centralizadas para la administración y manejo de los recursos humanos, económicos y materiales.

La Institución dentro de la estructura orgánica cuenta con organismos asesores como el Estado Mayor que es el máximo organismo de planificación estratégica de las operaciones policiales, cuya misión es asesorar, recomendar y facilitar el ejercicio del mando al Comandante General, a quien se subordina para los efectos funcionales y operacionales; está integrado por Direcciones Generales y Nacionales (Figura 4). (ECUADOR, LEY ORGANICA POLICIA NACIONAL, 1988)

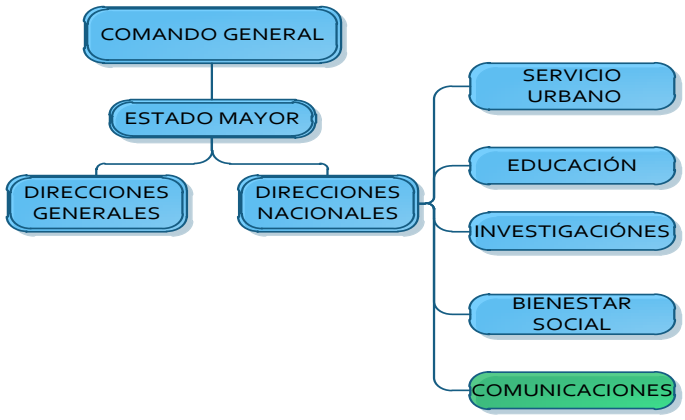


Figura 4. Estructura Organizacional de la Policía Nacional

El 3 de octubre del 2000, se crea la DIRECCIÓN NACIONAL DE COMUNICACIONES, mediante resolución No. 2000-353-CG-PN, y tiene como misión "Liderar la prestación de los servicios de comunicaciones e informática, a través de una constante preparación del elemento humano y la utilización de la tecnología adecuada, que garantice la eficacia y eficiencia en su empleo, en beneficio institucional y de la comunidad".

Los objetivos de la Dirección Nacional de Comunicaciones se sintetizan en los siguientes puntos:

- Lograr y mantener el más alto grado de calidad en los servicios de comunicaciones e informática de la Policía Nacional.
- Procurar la excelencia administrativa de la infraestructura existente en la Policía Nacional, en materia de comunicaciones e informática.
- Estandarizar la infraestructura tecnológica.
- Centralizar las decisiones tecnológicas y desconcentrar las acciones operacionales en esta área.
- Promover la modernización constante y el desarrollo continuo en los servicios de comunicaciones e informática.
- Fortalecer la participación policial con la comunidad a través del asesoramiento en materia de comunicaciones e informática.

Enfocándonos en el Centro de Datos se debe indicar que la estructura organizacional de la DNC es la siguiente:

- Nivel Directivo
- Nivel Asesor
- Nivel Administrativo
- Nivel Técnico-Operativo

En el Figura 5 se observa la estructura organizacional actual de la DNC.

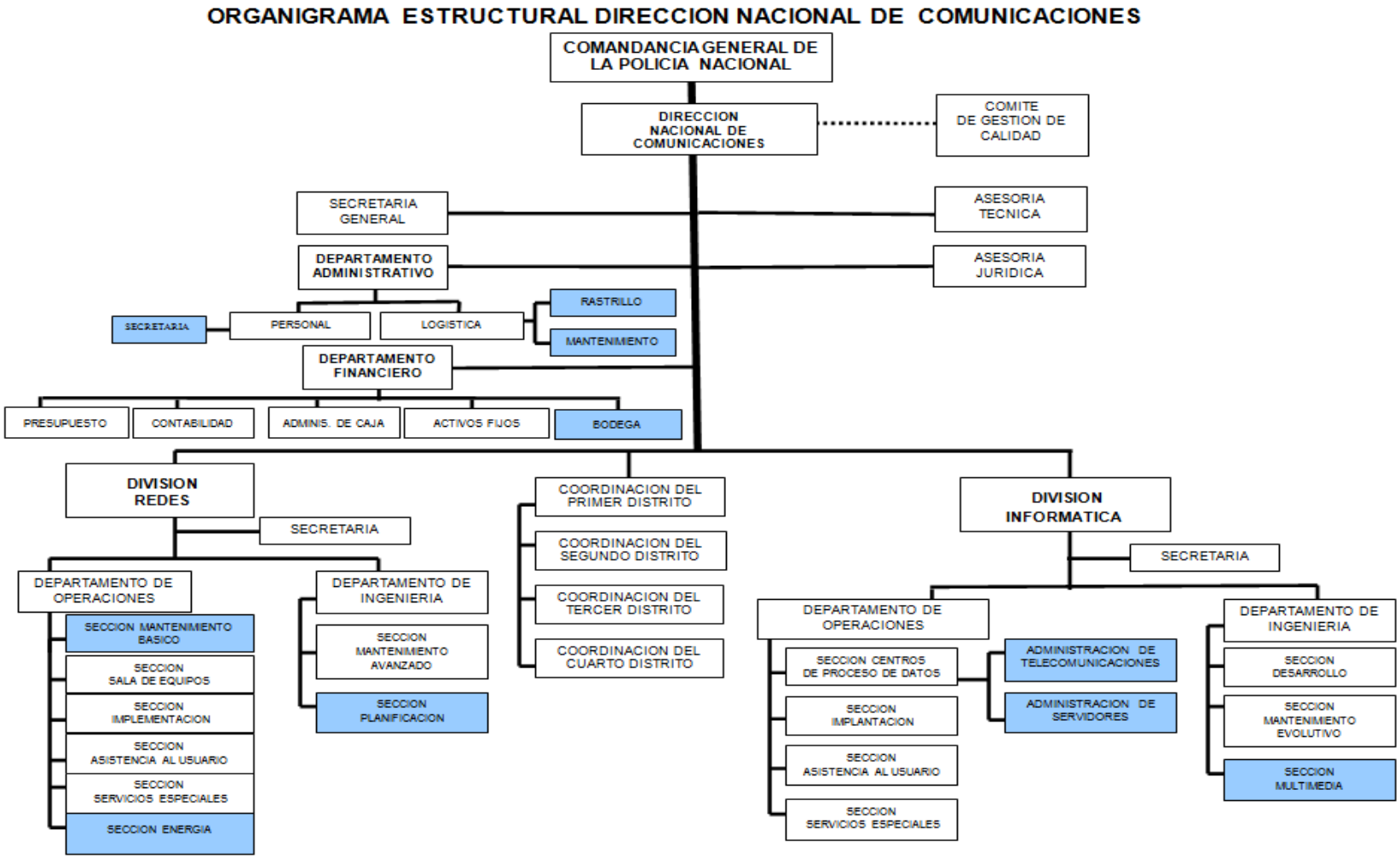


Figura 5. Estructura Organizacional de la DNC

En el nivel Técnico-Operativo está la División Informática y bajo su dependencia el Centro de Datos, esta sección a pesar de estar orgánicamente creada, no cuenta con objetivos, estructura, procesos, relaciones, roles y responsabilidades de TI bien definidos, es decir todo lo que las buenas prácticas en materia de TI recomiendan.

5.1.2 Objetivos de control aplicados a la Dirección Nacional de Comunicaciones

Para el cumplimiento de este objetivo es necesario mencionar que la metodología COBIT indica que el proceso PO4, es función directa de los altos ejecutivos y gerencia del negocio, por lo cual debemos necesariamente puntualizar que la Dirección Nacional Comunicaciones, debe implementar y mantener un sistema de control interno y un marco de trabajo alineado al Plan Estratégico de la Policía Nacional.

Se han establecido objetivos de control propios del nivel directivo de la DNC, que deben ser cumplidos obligatoriamente para que el modelo de gestión propuesto, se pueda ejecutar.

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, rendición de cuentas, autoridad, roles, responsabilidades y supervisión.
(Cobit 4.1, 2007, pág. 41)

Tabla N° 2
Objetivos de Control para la DNC

Objetivos de control aplicados a la Dirección Nacional de Comunicaciones	
PO4.1 Marco de Trabajo de Procesos de TI	La DNC debe elaborar el Plan estratégico de TI. Definir un marco de trabajo que incluya estructura organizacional, relaciones entre procesos, medición del desempeño.
PO4.2 Comité Estratégico de TI	La DNC debe establecer un Comité Estratégico de TI a nivel Asesor de la Dirección.
PO4.3 Comité Directivo de TI	No aplica a la estructura organizacional de la DNC, debido a que posee una estructura jerarquizada diferente a otras estructuras organizacionales.
PO4.4Ubicación Organizacional de la función de TI	No aplica a la estructura organizacional de la DNC, debido a que posee una estructura jerarquizada diferente a otras estructuras organizacionales.
PO4.5 Estructura Organizacional	La DNC debe establecer la estructura organizacional de TI interna que se ajuste a los objetivos de la Dirección y justifique los requerimientos de personal.
PO4.6 Establecimiento de Roles y Responsabilidades	La DNC debe definir los roles y las responsabilidades para el personal de TI.
PO4.7 Responsabilidad de aseguramiento de calidad de TI	No aplica a la estructura organizacional de la DNC.

Continua

PO4.8 Responsabilidad sobre riesgo, la seguridad y el cumplimiento	La DNC debe establecer la propiedad y la responsabilidad de los riesgos relacionados con TI al nivel jerárquico apropiado debe definir y asignar roles para administrar los riesgos y las responsabilidades de la seguridad de la información y la seguridad física.
PO4.9 Propiedad de datos y sistemas	No aplica a la estructura organizacional de la DNC.
PO4.10 Supervisión	La DNC debe implementar prácticas adecuadas dentro de la función de TI para garantizar y evaluar que los roles y responsabilidades se ejecuten de forma apropiada y generar indicadores de desempeño.
PO4.11 Segregación de Funciones	La DNC debe implementar una división de roles y responsabilidades para que no recaiga la responsabilidad de procesos críticos en una sola persona.
PO4.12 Personal de TI	La DNC debe evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente operativo para garantizar el cumplimiento de las funciones de TI.
PO4.13 Personal clave de TI	La DNC debe definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo que realiza una función crítica.
PO4.14 Políticas y procedimientos para el personal contratado	No aplica a la estructura organizacional de la DNC.
PO4.15 Relaciones	No aplica a la estructura organizacional de la DNC.

PROCESO P09

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"

(Cobit 4.1, 2007, pág. 63)

El proceso PO9, tiene una relación directa con el objetivo de control PO4.8, en donde se estructura y definen responsabilidades sobre el riesgo, en este sentido son Objetivos de Control de la DNC del proceso PO9 los siguientes:

Tabla N° 3
Objetivos de Control para la DNC

Objetivos de control aplicados a la Dirección Nacional de Comunicaciones	
PO9.1 Marco de Trabajo de Administración de Riesgos	La DNC debe definir el marco de trabajo de administración de riesgos, que afecten al cumplimiento de los objetivos de TI.
PO9.2 Establecimiento del Contexto del Riesgo	La DNC debe establecer clara y contextualmente cuales son los riegos que afecten al cumplimiento de sus funciones específicas como responsables de TI.
PO9.3 Identificación de Eventos	La DNC debe identificar todos los eventos de TI que puedan ser considerados como riesgos o vulnerabilidades, con todas sus implicaciones de carácter legal, económico y operativo.
PO9.4 Evaluación de Riesgos de TI	La DNC debe tomar en cuenta todas las connotaciones que acarrearían un evento nocivo de TI y su eventual paralización y/o negación de servicios tecnológicos.

Continua 

PO9.5 Respuesta a los Riesgos	La DNC debe desarrollar y mantener un proceso de respuesta a riesgos identificar estrategias para evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.
PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos	La DNC debe priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la determinación de costos, beneficios y la responsabilidad en la ejecución de estos planes

5.2 Definir la estructura organizacional del Centro de Datos alineados en los procesos PO4 y PO9.

Enfocándonos en los objetivos específicos del tema del proyecto propuesto relacionados al Centro de Datos de la DNC y analizados los objetivos de control de los procesos PO4 y PO9, mencionados anteriormente, la realidad organizacional, operativa y técnica se enfoca en la siguiente propuesta:

5.2.1 Estructura Organizacional

COBIT define que este objetivo de control es: Establecer la estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implementar 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 del negocio esperados y las circunstancias cambiantes. (Cobit 4.1, 2007, pág. 42)

Acorde a los mejores criterios y buenas prácticas de TI, es necesario definir el concepto de lo que es el Centro de Datos de la DNC, para lo que se proponen los siguientes criterios:

5.2.2 Definición del Centro De Datos de la DNC

Es el departamento técnico especializado donde se centraliza y administra la infraestructura tecnológica de los sistemas informáticos de la Policía Nacional, para alcanzar los objetivos de TI de la Dirección Nacional de Comunicaciones.

5.2.3 Objetivo general del Centro de Datos de la DNC

Administrar la infraestructura tecnológica de hardware y software, fundamentados en las mejores prácticas de TI, para garantizar la operatividad de los sistemas informáticos de la Policía Nacional.

5.2.4 Objetivos específicos del Centro de Datos de la DNC

- Administrar redes informáticas
- Administrar servidores
- Administrar las seguridades y los riesgos
- Gestionar incidentes
- Administrar los respaldos de la información

5.2.5 Estructura organizacional del Centro de Datos

A continuación se propone la siguiente estructura que establece un conjunto de actividades, que se agrupan de manera ordenada y especializada, conformando secciones técnicas que coordinadamente permitirán el cumplimiento de los objetivos del Centro de Datos:

1. Jefatura

1.1. Redes informáticas

1.2. Servidores

1.3. Seguridades y administración de riesgos

1.4. Gestión de Incidentes

1.5. Respaldos de la información

FIGURA 6, Estructura Organizacional del Centro de Datos

Para fundamentar esta estructura propuesta se han tomado los siguientes criterios:

- Esta estructura técnica organizacional se acopla a la realidad organizacional de la Policía Nacional.
- Esta estructura establece secciones técnicas claramente definidas, que se fundamentan en buenas prácticas de TI.
- Al contar con una estructura definida se logrará establecer procesos, roles y responsabilidades.

5.3 Establecer procesos de TI enfocados en los procesos PO4 y PO9

Se plantean los siguientes procesos con base en la nueva estructura organizacional del Centro de Datos:

Tabla N° 4
Jefatura

PROCESO:	**Dirigir y controlar todas las actividades que se ejecutan en el Centro de Datos.**
ACTIVIDADES:	• Gestionar, ejecutar y controlar el cumplimiento de los procesos existentes en el Centro de Datos. • Evaluar el cumplimiento de roles y responsabilidades. • Proponer buenas prácticas de TI para mejorar los procesos y el cumplimiento de los objetivos.

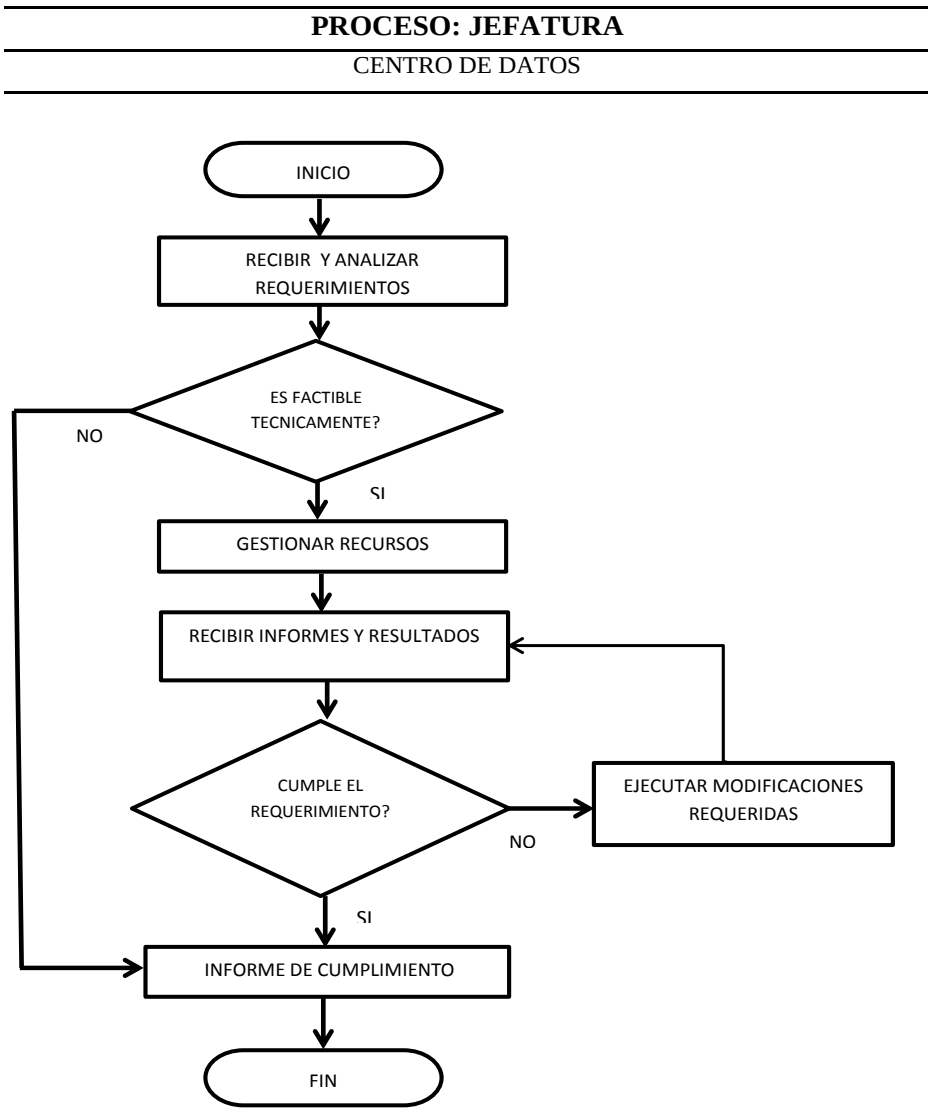


Figura 7, Proceso de la Jefatura

Tabla N° 5
Redes Informáticas

PROCESO:	**Administrar las redes informáticas.**
ACTIVIDADES:	• Asegurar la disponibilidad de las redes. • Diseñar física y lógicamente las redes. • Ejecutar análisis y pruebas de nuevas tecnologías de redes. • Generar políticas para la administración de redes informáticas.

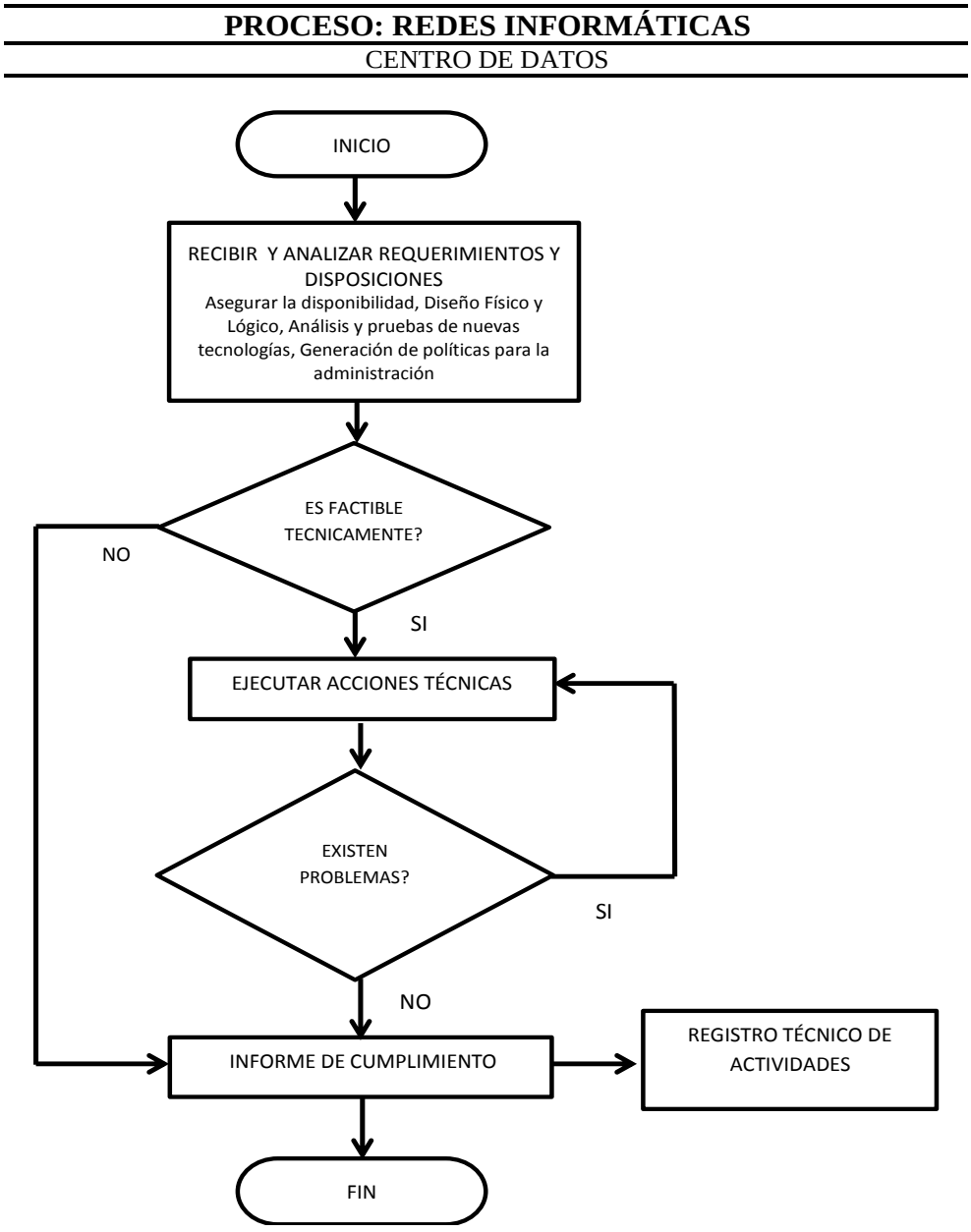


Figura 8, Proceso de Redes Informáticas

Tabla No. 6
Servidores

PROCESO:	**Administrar los servidores**
ACTIVIDADES:	• Asegurar la operatividad de los servidores. • Ejecutar el mantenimiento de los servidores. • Ejecutar análisis y pruebas de nuevas tecnologías de servidores. • Generar políticas para la administración de servidores

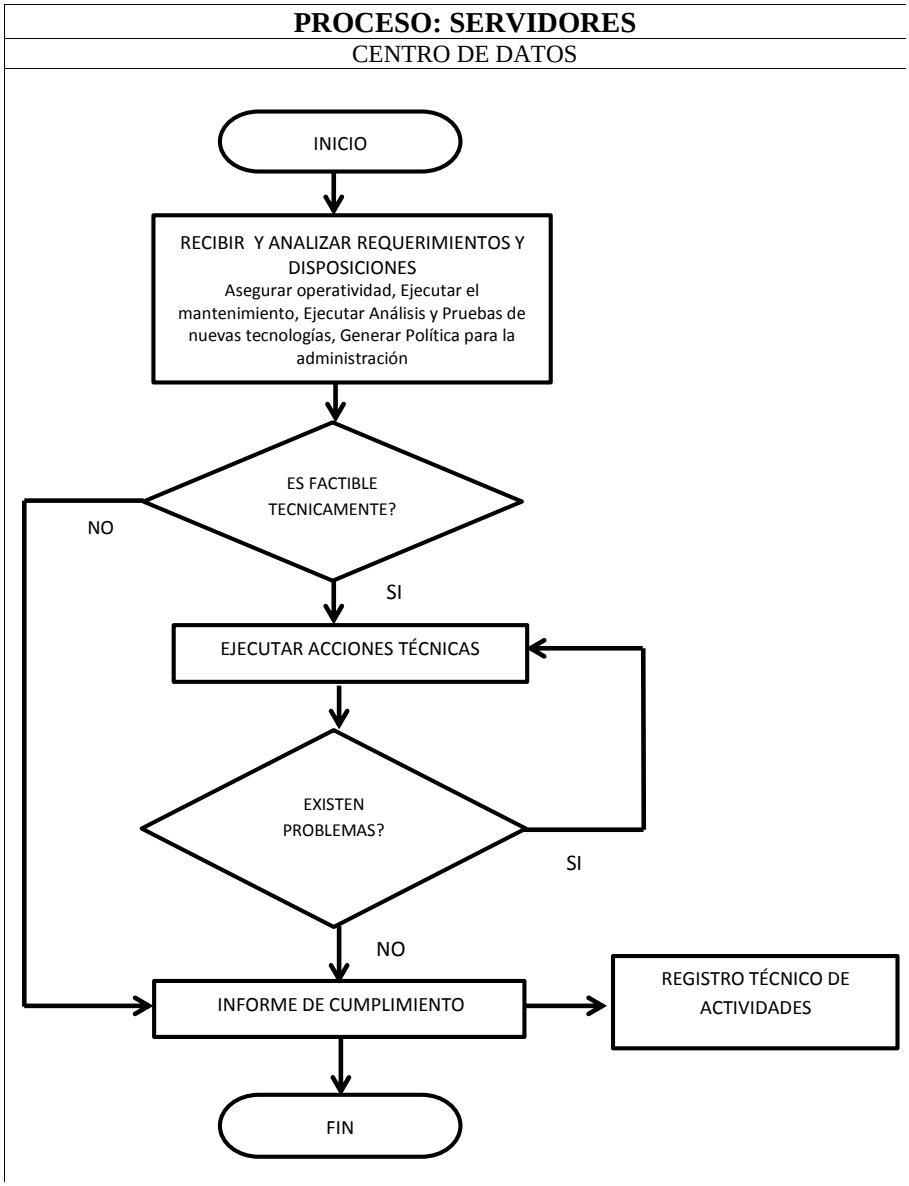


Figura 9, Proceso de Servidores

Tabla No. 7
Seguridades y Administración De Riesgos

PROCESO:	**Administrar las seguridades y riesgos**
ACTIVIDADES:	• Implementar seguridades a nivel de hardware y software. • Generar políticas de seguridades físicas y lógicas del Centro de Datos. • Determinar la alineación de la administración de riesgos. • Identificar los objetivos internos de TI y establecer el contexto del riesgo. • Evaluar y seleccionar respuestas a riesgos • Priorizar y planear actividades de control de riesgos • Mantener y monitorear un plan de acción de riesgos

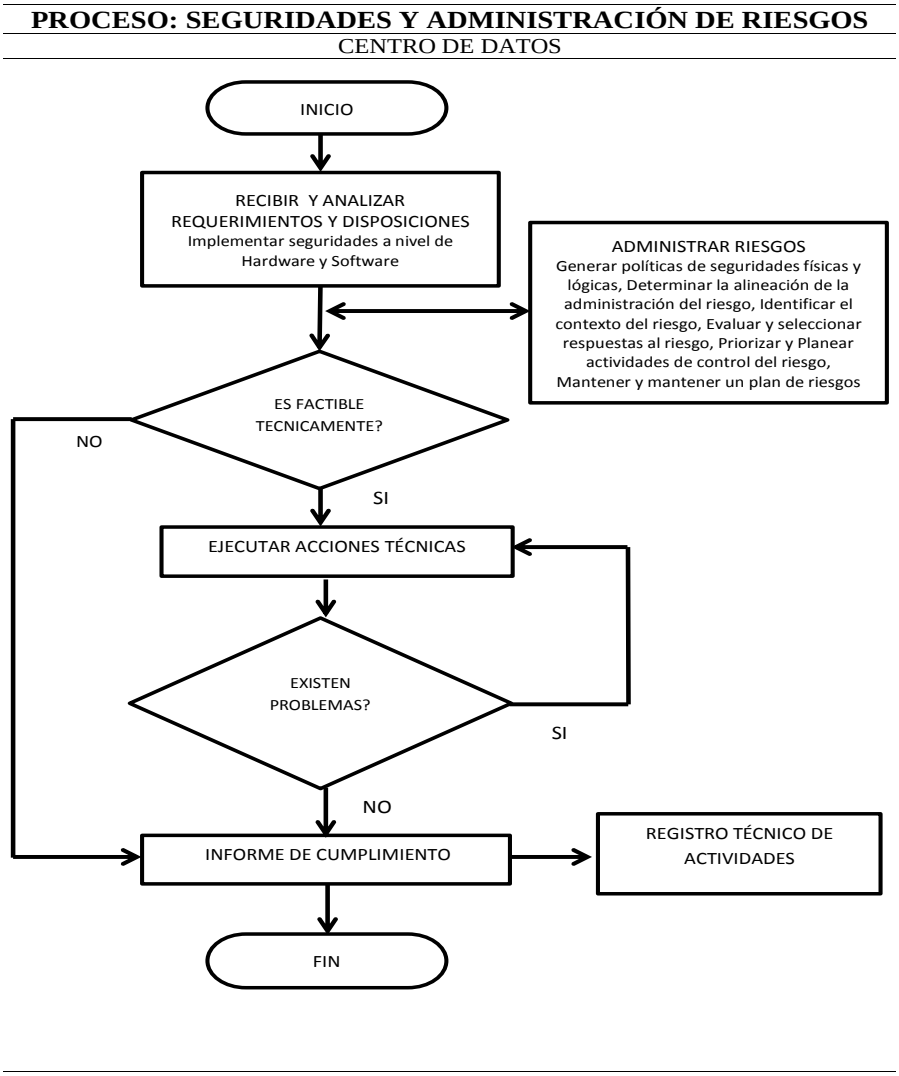


Figura 10, Proceso de Administración de Riesgos

Tabla No. 8
Gestión de Incidentes

PROCESO:	**Brindar atención oportuna y efectiva a los incidentes escalados al Centro de Datos**
ACTIVIDADES:	• Atender los incidentes escalados al Centro de Datos • Sugerir políticas para la gestión de incidentes.

PROCESO: GESTIÓN DE INCIDENTES
CENTRO DE DATOS

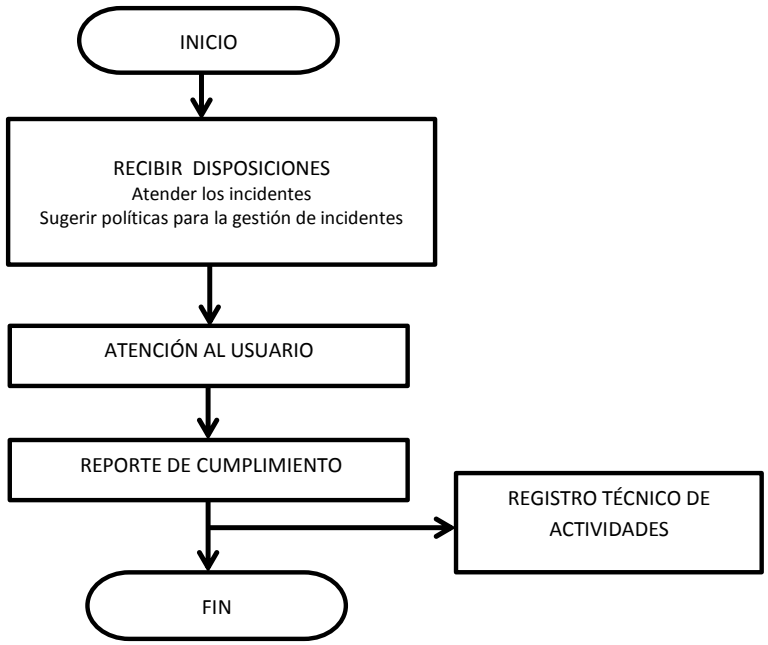


Figura 11, Proceso de Gestión de Incidentes

Tabla No. 8
Respaldo de la Información

PROCESO:	**Administrar los respaldos de la información**
ACTIVIDADES:	• Crear procesos para proteger la información, sistemas y bases de datos del Centro de Datos. • Coordinar con las diferentes secciones del Centro de Datos para establecer procesos de recuperación en caso de posibles fallos o desastres. • Generar políticas y planes de acción para el respaldo de la información.

PROCESO: RESPALDO DE LA INFORMACIÓN
CENTRO DE DATOS

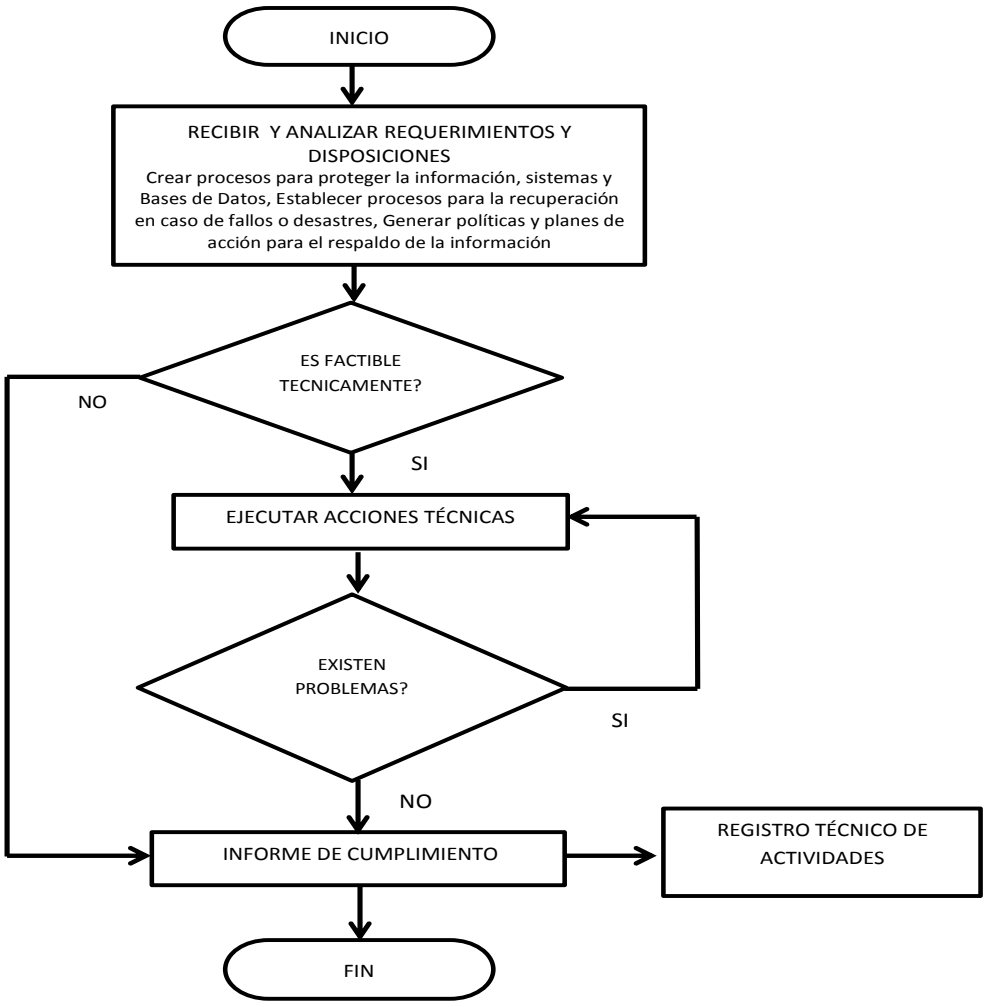


Figura 12, Proceso de Respaldo de la Información

5.4 Establecer roles y responsables alineados en los procesos PO4 y PO9

Basado en el objetivo de control PO4.6 de la metodología COBIT, se plantea el siguiente esquema de roles y las responsabilidades para el personal de Centro de Datos:

Tabla No. 9
Roles y responsabilidades – Jefatura

JEFATURA	
ROL	**RESPONSABILIDADES**
Jefe	Ejecutar todas las acciones necesarias para el cumplimiento de las funciones asignadas en las Leyes y Reglamentos Policiales.
	Administrar los servicios, las herramientas, los servidores y equipos de informática y comunicaciones del Centro de Datos.
	Difundir en todas las secciones del Centro de Datos, las normas, políticas y procedimientos establecidos para el uso de TIC.
	Realizar reuniones de trabajo con los responsables de las secciones a fin de revisar la calidad y eficiencia de los servicios brindados.
	Gestionar ante la División Informática u otros proveedores de servicios, la inmediata asistencia técnica de las fallas que se presenten en el hardware y/o software del Centro de Datos.
	Coordinar y controlar que los proveedores de las TIC, ejecuten los servicios de mantenimientos preventivos, correctivos y vigencia de garantías de los equipos del Centro de datos, de acuerdo a los procedimientos establecidos.
	Solicitar la designación de personal técnico policial permanente para la operatividad adecuada del Centro de Datos.
	Disponer el adecuado empleo de los recursos de TIC del Centro de datos.
	Gestiona la implementación de normas y procedimientos de seguridad y salud ocupacional para el personal bajo su mando.
	Proponer procedimientos para conservar la integridad y garantizar la confidencialidad de la información que se encuentra en el Centro de Datos.
	Asesorar al Departamento de Informática en la definición y el seguimiento de proyectos de TI.

Tabla No. 10
Roles y Responsabilidades – Redes Informáticas

REDES INFORMÁTICAS	
ROL	**RESPONSABILIDADES**
Administrador de Redes	Cumplir con los procedimientos de administración, control y mantenimiento de toda la infraestructura de redes.
	Planificar y diseñar la infraestructura tecnológica y la adquisición de equipos y software para la implementación de un backbone.
	Administrar las claves de la cuentas de usuario root y administrador de los equipos que administra.
	Administrar los equipos activos de la red.
	Coordinar el trabajo para cumplir los procedimientos de administración de redes.
	Mantener activo el servicio de comunicaciones LAN y de Internet.
	Mantener actualizado el inventario de hardware y software perteneciente a la infraestructura de redes
	Mantener actualizado el listado de usuarios administradores de los equipos activos de las redes.
	Elaborar el plan de contingencia para mantener la continuidad del Centro de Datos.
	Cumplir las normas y procedimientos de seguridad y salud ocupacional del personal que labora en la administración de redes.
	Proponer y ejecutar procedimientos para conservar la integridad y garantizar la confidencialidad de la información.
	Documentar los procesos y procedimientos sobre la administración de la infraestructura de redes.

Tabla No. 11
Roles y responsabilidades - Servidores

SERVIDORES	
ROL	**RESPONSABILIDADES**
Administrador de Servidores	Cumplir con los procedimientos de administración, control y mantenimiento de los servidores del Centro de Datos.
	Mantener actualizado el inventario de los servidores tanto de hardware como de software (Sistema operativo, licencias, utilitarios y demás).
	Mantener actualizado el listado de usuarios administradores de los servidores.
	Elaborar el plan de contingencia para mantener la continuidad del Centro de Datos.
	Cumplir las normas y procedimientos de seguridad y salud ocupacional del personal que labora en la administración de servidores.
	Optimizar el uso de recursos en su área de trabajo
	Proponer y vigilar el cumplimiento de procedimientos para conservar la integridad y garantizar la confidencialidad de la información.
	Documentar los procesos y procedimientos sobre la administración de servidores.

Tabla No. 12
Roles y responsabilidades – Seguridad y Administración de Riesgos

SEGURIDADES Y ADMINISTRACIÓN DE RIESGOS	
ROL	**RESPONSABILIDADES**
Oficial de Seguridad y Riesgos	Realizar las funciones correspondientes al rol de Oficial de seguridad y riesgos del Centro de Datos.
	Responder por las actividades asignadas en la administración de seguridades y evaluación y administración de riesgos.
	Definir e implementar políticas de Seguridad Informática basadas en las buenas prácticas.
	Administrar y monitorear los planes de acción sobre las políticas implementadas y riesgos residuales.
	Determinar la asignación de responsabilidades de seguridad de la información.
	Elaborar las políticas de seguridad del uso de la información.
	Administrar los sistemas de acceso físico al Centro de Datos.
	Elaborar el plan de contingencia que permita mantener la continuidad del negocio del Centro de datos en el caso de desastres.
	Optimizar el uso de recursos en su área de trabajo
	Presentar informes al Jefe del Centro de Datos y Jefe de la División Informática y demás autoridades de la Institución.
	Elaborar y ejecutar el Plan de gestión de riesgos.
	Documentar los procesos y procedimientos sobre la administración de seguridades y riesgos.
	Cumplir con los procedimientos de administración de seguridades y riesgos.

Tabla No. 13
Roles y Responsabilidades – Gestión de Incidentes

GESTIÓN DE INCIDENTES	
ROL	**RESPONSABILIDADES**
Encargado de Gestión de Incidentes	Cumplir con los procedimientos de atención al usuario.
	Atender a requerimientos de los Subadministradores de las Unidades Policiales y escalarlos a la sección correspondiente.
	Registrar y monitorear las llamadas, incidentes, solicitudes de servicio y necesidades de información.
	Optimizar el uso de recursos en su área de trabajo.

Tabla No. 14
Roles y Responsabilidades – Administrador de Respaldos

ADMINISTRACIÓN DE RESPALDOS	
ROL	**RESPONSABILIDADES**
Administrador de Respaldos	Ejecutar todas las acciones necesarias para el cumplimiento de las funciones asignadas en las Leyes y Reglamentos Policiales.
	Cumplir con los procedimientos de administración, control y mantenimiento de los respaldos de información
	Obtener y almacenar los respaldos de la información, bases de datos, contraseñas, sistemas operativos, software base y todo archivo necesario para el normal funcionamiento de las actividades.
	Documentar los procesos y procedimientos de la administración de respaldos.
	Cumplir las normas y procedimientos de seguridad y salud ocupacional del personal que labora en la administración de respaldos.

5.5 Establecer Modelos de madurez alineados en los procesos PO4 y PO9

Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.
(Cobit 4.1, 2007, pág. 17)

La propuesta de ésta proyecto es que una vez definida la estructura y establecidos los procesos del Centro de Datos, se alcance un nivel de madurez genérico de **nivel 4**, es decir **Administrado;** basados en los siguientes fundamentos teóricos en la metodología COBIT:

Tabla No. 15
Tabla de atributos

Conciencia y Comunicación	Hay entendimiento de los requerimientos completos. Se aplican técnicas maduras de comunicación y se usan herramientas estándar de comunicación.
Políticas, Estándares y Procedimientos	El proceso es sólido y completo; se aplican las mejores prácticas internas. Todos los aspectos del proceso están documentados y son repetibles. La dirección ha terminado y aprobado las políticas. Se adoptan y siguen estándares para el desarrollo y mantenimiento
Herramientas y Automatización	Se implantan las herramientas de acuerdo a un plan estándar y algunas se han integrado con otras herramientas relacionadas. Se usan herramientas en las principales áreas para automatizar la administración del proceso y monitorear las actividades y controles.

Continua

Habilidades y Experiencia	Los requerimientos de habilidades se actualizan rutinariamente para todas las áreas, se asegura la capacidad para todas las áreas críticas y se fomenta la certificación. Se aplican técnicas maduras de entrenamiento de acuerdo al plan de entrenamiento y se fomenta la compartición del conocimiento.
Responsabilidad y Rendición de Cuentas	Las responsabilidades y la rendición de cuentas sobre los procesos están aceptadas y funcionan de modo que se permite al dueño del proceso descargar sus responsabilidades. Existe una cultura de recompensas que activa la acción positiva.
Establecimiento y Medición de Metas	La eficiencia y la efectividad se miden y comunican y están ligadas a las metas del negocio y al plan estratégico de TI. Se implementa el balanced scorecard de TI en algunas áreas, con excepciones conocidas por la gerencia y se está estandarizando el análisis

Específicamente en el proceso PO4 se establecen los siguientes fundamentos para proponer un nivel de madurez nivel 4:

Tabla No. 16
Fundamentos propuestos

CONCEPTO COBIT	FUNDAMENTO PROPUESTA
La organización de TI responde de forma proactiva al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio	El Centro de Datos necesariamente responderá proactivamente a la implantación de una estructura, organización y procesos definidos que aseguren el cumplimiento de los objetivos de ésta unidad técnica.
La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas	Al definirse clara y específicamente procesos, roles y responsabilidades se

Continua 

	estará asegurando la ejecución de actividades técnicas propias y exclusivas del Centro de Datos con control y supervisión, aplicando las mejores prácticas y estándares de TI. **C**ada miembro de ésta área técnica sustentará sus actividades en estándares y normativas que no existían anteriormente especialmente evitando la concentración de responsabilidades en una o varias personas.
Se han aplicado buenas prácticas internas en la organización de las funciones de TI	Al implementarse éste proyecto se constituiría la primera ocasión en que se ejecuten estándares y procesos basados en las mejores prácticas de TI en el Centro de Datos de la Dirección Nacional de Comunicaciones
La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implementar y monitorear la organización deseada y las relaciones.	Es imprescindible que quien ocupe el cargo de Director Nacional de Comunicaciones, cuente con el perfil y la experiencia requeridos para cumplir eficazmente con los objetivos de TI de la Policía Nacional.
Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar.	Los procesos de TI establecidos en el Centro de Datos deberán estar permanentemente actualizados y alineados a las buenas prácticas, para dar cumplimiento a los objetivos institucionales.

Continua

Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional.	Es imprescindible contar con un inventario de habilidades y destrezas, para conocer los problemas de dependencia de personas, así como las falencias en conocimientos para ejecutar procesos de capacitación y desarrollo profesional en las diferentes especialidades técnicas.
Existe equilibrio entre las habilidades y los recursos disponibles internamente	Se dispondrá de recursos claramente identificados los cuales deberán ser efectivamente administrados por el personal técnico del Centro de Datos.
La estructura organizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesos estratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.	El Centro de Datos ejecuta el proceso macro estratégico en materia de TI de la Policía Nacional. La implementación de éste proyecto alineará los requerimientos de TI aplicando las mejores prácticas en esta materia a la infraestructura tecnológica existente y eliminará los servicios que actualmente se alinean a tecnologías aisladas.

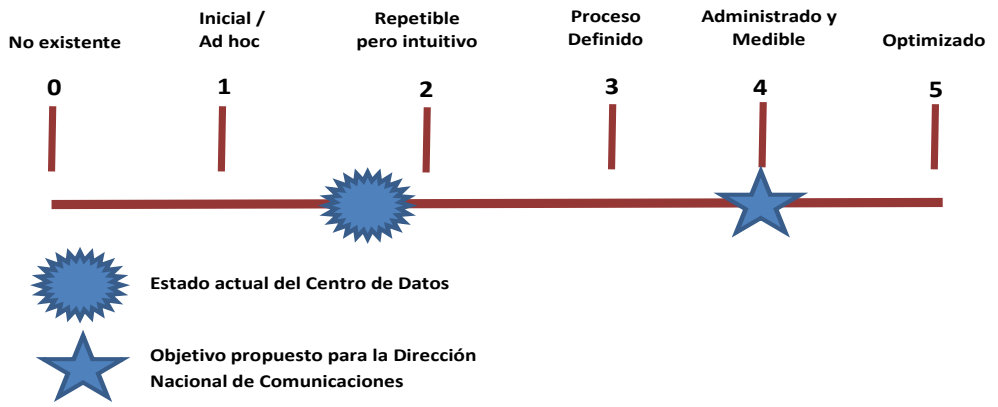


FIGURA 13, Modelo de madurez propuesto

5.6 Establecer Mapas de control alineados en los procesos PO4 y PO9.

Para que TI tenga éxito en satisfacer los requerimientos del negocio, la Dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

- Estableciendo un vínculo con los requerimientos del negocio
- Organizando las actividades de TI en un modelo de procesos generalmente aceptado
- Identificando los principales recursos de TI a ser utilizados
- Definiendo los objetivos de control gerenciales a ser considerados

Se debe observar que, a pesar de que el material es recolectado de cientos de expertos, después de una rigurosa investigación y revisión, las entradas, salidas, responsabilidades, métricas y metas son ilustrativas y no así preceptivas o exhaustivas. Proporcionan una base de conocimiento base del cual cada empresa debe seleccionar lo que aplica de forma eficiente y efectiva, con base en las metas y políticas de la estrategia empresarial.
(Cobit 4.1, 2007, pág. 32)

Sobre la base de lo anteriormente descrito, definimos que los mapas de control son herramientas gráficas, que permite visualizar quién debe rendir cuentas, a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar, lo que en el marco de control COBIT se determina como Matriz RACI.

A continuación se describen las matrices RACI, de los procesos planteados anteriormente:

PROCESO JEFATURA									
FUNCIONES / ACTIVIDADES	Jefe de la División Informática	Jefe del CDD	Administrador de redes	Administrador de servidores	Oficial de seguridad y riesgos	Encargado de Gestión de Incidentes	Administrador de respaldos		
Gestionar, ejecutar y controlar el cumplimiento de los procesos existentes en el Centro de Datos.	I	R							
Evaluar el cumplimiento de roles y responsabilidades.	I	R	A	A	A	A	A		
Proponer buenas prácticas de TI para mejorar los procesos y el cumplimiento de los objetivos	C	R	C	C	C	C	C		

Figura 14, Matriz RACI proceso Jefatura

PROCESO SERVIDORES								
FUNCIONES / ACTIVIDADES	Jefe del CDD	Administrador de redes	Administrador de servidores	Oficial de seguridad y riesgos	Encargado de Gestión de Incidentes	Administrador de respaldos		
Asegurar la operatividad de los servidores		C	R	C		C		
Ejecutar el mantenimiento de los servidores	I	C	R	C	I	C		
Ejecutar análisis y pruebas de nuevas tecnologías de servidores	C	I	R	I	I	I		
Generar políticas para la administración de servidores	C	I	R	I		I		

Figura 15, Matriz RACI Proceso Servidores

PROCESO REDES INFORMÁTICAS								
FUNCIONES / ACTIVIDADES	Jefe del CDD	Administrador de redes	Administrador de servidores	Oficial de seguridad y riesgos	Encargado de Gestión de Incidentes	Administrador de respaldos		
Asegurar la disponibilidad de las redes	I	R	C	C		C		
Diseñar física y lógicamente las redes	C	R	C	C		C		
Ejecutar análisis y pruebas de nuevas tecnologías de redes	C	R	C	C	I	I		
Generar políticas para la administración de redes informáticas	C	R	C	C	I	C		

Figura 16, Matriz RACI Proceso Redes Informáticas

PROCESO SEGURIDADES Y ADMINISTRACIÓN DE RIESGOS								
ACTIVIDADES / FUNCIONES	Jefe del CDD	Administrador de redes	Administrador de servidores	Oficial de seguridad y riesgos	Encargado de Gestión de Incidentes	Administrador de respaldos		
Implementar seguridades a nivel de hardware y software	C	C	C	R		C		
Generar políticas de seguridades físicas y lógicas del Centro de Datos	C	C	C	R		C		
Determinar la alineación de la administración de riesgos	I	I	I	R		I		
Identificar los objetivos internos de TI y establecer el contexto del riesgo	C	C	C	R		C		
Evaluar y seleccionar respuestas a riesgos	I/C	I/C	I/C	R		I/C		
Priorizar y Planear actividades de control	I	I	I	R		I		
Mantener y Monitorear un plan de acción de riesgos	C	C	C	R	I	C		

Figura 17, Matriz RACI Proceso Seguridades y Riesgos

PROCESO GESTION INCIDENTES								
ACTIVIDADES / FUNCIONES	Jefe del CDD	Administrador de redes	Administrador de servidores	Oficial de seguridad y riesgos	Encargado de Gestión de Incidentes	Administrador de respaldos		
Atender los incidentes escalados al Centro de Datos	I	I	I	I	R	I		
Sugerir políticas para la gestión de incidentes	C	C	C	C	R	C		

Figura 18, Matriz RACI Proceso Gestión de Incidentes

PROCESO RESPALDOS DE LA INFORMACIÓN								
ACTIVIDADES / FUNCIONES	Jefe del CDD	Administrador de redes	Administrador de servidores	Oficial de seguridad y riesgos	Encargado de Gestión de Incidentes	Administrador de respaldos		
Crear procesos para proteger la información, sistemas y bases de datos del Centro de Datos	C	C	C	C		R		
Coordinar con las diferentes secciones del Centro de Datos para establecer procesos de recuperación en caso de posibles fallos o desastres	I	C	C	C		R		
Generar políticas y planes de acción para el respaldo de la información	C	I	I	I	I	R		

Figura 19. Matriz RACI Proceso Respaldos de la Información

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se diseñó un modelo de gestión de las Tecnologías de Información del Centro de Datos de la Dirección Nacional de Comunicaciones de la Policía Nacional, aplicando COBIT 4.1 Dominio Planificar y Organizar.
- La estructura organizacional propuesta para el Centro de Datos se fundamentó en el marco de trabajo COBIT, es decir orientada a negocios, orientada a procesos y basada en controles.
- Se establecieron procesos alineados a las mejores prácticas de TI, concordantes a la estructura organizacional propuesta y cumplen con las recomendaciones del marco de Trabajo de COBIT.
- Se establecieron roles y responsabilidades para cada uno de los procesos, identificando quien y que actividad se debe realizar.
- Se propuso un modelo de madurez para la gestión de TI del Centro de Datos de nivel 4 "Administrado". Esté nivel de madurez garantizará la calidad de la gestión de TI del Centro de Datos.
- Los mapas de control formulados, se han definido como herramientas gráficas que permitirán visualizar los roles y responsabilidades del personal del Centro de Datos. En relación al marco de trabajo COBIT, estos mapas se diseñaron para controlar y asegurar que los objetivos del Centro de Datos se cumplan y los eventos no deseados se prevengan, se detecten y corrijan.

Recomendaciones

- La implementación de éste modelo de gestión deberá ser analizado y aprobado por el nivel Gerencial de la Dirección Nacional de Comunicaciones para su trámite legal ante las instancias superiores, ya que se está creando unidades técnico operativas que necesitan ser incorporadas en el Reglamento Orgánico Funcional de la DNC.
- Para la asignación de roles y responsabilidades del personal del Centro de Datos; es necesaria la evaluación del personal técnico existente, y la selección de nuevo personal que cuente con el perfil idóneo para cubrir los requerimientos de los procesos planteados.
- Para alcanzar el nivel de madurez propuesto será necesario ejecutar las recomendaciones anteriores y mantener un control permanente al cumplimiento de los objetivos de control propuestos.
- Los mapas de control deben ser permanentemente supervisados y actualizados con la finalidad de que las estructuras, procesos, roles y responsabilidades alcancen los objetivos del Centro de Datos.

BIBLIOGRAFIA

Cobit 4.1. (2007). *Cobit 4.1.* USA: IT Governance Insitute.

COSO. (s.f.). Recuperado el 16 de 10 de 2015, de http://www.coso.org

ECUADOR, A. N. (1988). LEY ORGANICA POLICIA NACIONAL. En A. N. ECUADOR, *LEY ORGÁNICA DE LA POLICÍA DEL ECUADOR* (pág. 12). Quito: Registro Oficial de la República del Ecuador.

ECUADOR, A. N. (2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. En A. N. CONSTITUYENTE.

Hernández, R. F. (1994). Metodología de la Investigación. En *Metodología de la Investigacón.* Mc. Graw-Hill Colombia (3era ed) Mexico, D.F.

Interior, M. d. (2013). Plan Estratégico Policía Nacional. En R. González, *Plan Estratégico Policía Nacional 2013-2017*.

isaca. (s.f.). Recuperado el 16 de 10 de 2015, de www.isaca.org

ISO. (s.f.). *ISO*. Recuperado el 16 de 10 de 2015, de http://www.iso.org

ITIL. (s.f.). *ITIL*. Recuperado el 10 de 16 de 2015, de www.itilv3.osiatis.es

NIST. (s.f.). Recuperado el 16 de 10 de 2015, de www.nist.gov

PACIO, G. (s.f.). Recuperado el 19 de 10 de 2015, de http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html

GLOSARIO DE TÉRMINOS

COBIT: Objetivos de Control para la información y Tecnologías Relacionada.

ISO: Organización Internacional de Normalización.

ITIL: Information Technology Infrastructure Library. Librería de Infraestructura de Tecnología de la Información.

SI: Sistemas de Información.

TI: Tecnología de la Información.

TIC: Tecnología de la Información y Telecomunicaciones.

NIST: Instituto Nacional de Estándares y Tecnologías

SGSI: Sistema de Gestión de Seguridad Informática

COSO: Comité de Organizaciones Patrocinadoras de la Comisión Treadway

DNC: Dirección Nacional de Comunicaciones