ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROPUESTA DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN PARA EL DEPARTAMENTO ADMINISTRACIÓN PLATAFORMAS DSLAMs DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES E.P.

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DEL GRADO DE MAGISTER (MSc) EN GESTIÓN DE COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

ING. FLORES OSORIO DARWIN SANTIAGO
santifloreso@hotmail.com

DIRECTOR: ING. GUSTAVO SAMANIEGO, MSc.
gustavo.samaniego@epn.edu.ec

Quito, Julio del 2016

DECLARACIÓN

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

A través de la presente declaración cedo mis 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.DARWIN SANTIAGO FLORES OSORIO

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Ing. Darwin Santiago Flores Osorio, bajo mi dirección.

Ing. Gustavo Samaniego, MSc.
Director de Tesis

AGRADECIMIENTO

En primer lugar agradezco a mi DIOS PADRE, a la Virgen y a los Ángeles por darme la oportunidad de estar aquí y estar siempre a mi lado, a mis padres porque son los pilares fundamentales de mi vida, a Jonathan Carrillo quien me brindo todo su apoyo necesario para culminar este proyecto gracias Jony, a mis profesores que supieron compartir sus conocimientos.

Gracias a todos, he logrado culminar mi carrera, de todo corazón Gracias.

DEDICATORIA

Este trabajo está dedicado con mucho cariño para mis padres Alberto Flores y Avelina Osorio a mis hijos Santi y Daniel, hermanas, hermanos quienes con su apoyo y confianza me han ayudado siempre a alcanzar mis objetivos.

Para todos ellos dedico mi Tesis.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P., brinda el servicio de Internet y Datos a sus clientes a nivel nacional, por ende requiere investigar posibles debilidades en sus procesos elaborando una Propuesta de Gobierno de Tecnologías de la Información, ejecutando un análisis con Metas de Negocio, Metas TI y Procesos COBIT, ITIL V3 e ISO-27001.

El presente proyecto se apalanca con el análisis de la situación actual del Departamento Administración Plataformas DSLAMs, el cual se encarga de gestionar y operar la plataforma DSLAMs, este análisis permite describir los elementos de TI a nivel tecnológico.

Con el análisis propuesto, se elabora el mapeo entre COBIT basado en el dominio de “Entregar y dar Soporte”, ITIL V3 aplicando las mejores prácticas de la “Operación del Servicio” e ISO-27001 enfocado a las actividades de “Control de acceso”.

Para elaborar la propuesta del Gobierno de Tecnologías de la Información se toma como referencia el Mapa de Ruta del Gobierno de TI de COBIT 4.1, el cual permite mapear los objetivos de TI con las metas de negocio y procesos, a fin de cumplir y mejorar las actividades que se ejecutan en el Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.

Para la evaluación de la aplicabilidad de la propuesta, se toma como referencia la actividad “Implementar la Solución” descrita en el mapa de ruta de Gobierno de TI de COBIT 4.1, definiendo los procesos que requiere el Gobierno de TI, para el Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.

INTRODUCCIÓN

La propuesta de Gobierno de Tecnologías de la información (TI) se encarga de definir responsabilidades en los procesos del Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P., que brinda el servicio de Internet y Datos a sus clientes a nivel nacional.

El Gobierno de Tecnologías de la Información, es la base para asegurar la estabilidad de los servicios del negocio basándose en la calidad y costes predecibles, con el propósito de satisfacer a los usuarios del Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.

Con el mapeo de las estrategias de negocio, metas de TI y los procesos COBIT “Entregar y dar Soporte”, ITIL V3 “Operación del Servicio” e ISO-27001 “Control de acceso”, se puede medir el desempeño de Gobierno de TI, lo cual permite al Departamento Administración Plataformas DSLAMs conocer sus fortalezas para llevar una buena administración y sus debilidades para realizar correcciones y cumplir con sus objetivos proyectados.

CAPÍTULO 1

SITUACIÓN ACTUAL DEL GOBIERNO DE TI

El presente capítulo tiene como objetivo analizar la situación actual del Gobierno de TI (Tecnologías de la Información) del Departamento Administración Plataformas DSLAMs (Digital Subscriber Line Access Multiplexer) de la Corporación Nacional de Telecomunicaciones E.P., (CNT E.P.).

Posteriormente en base al mapeo de las mejores prácticas de COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas), ITIL (Biblioteca de Infraestructura de Tecnologías de Información) e ISO 27001 (Sistema de Gestión de la Seguridad de la Información) se establecerá una propuesta de Gobierno de TI para este departamento, tomando en cuenta el anunciado de ITIL "*el Gobierno de Tecnologías de la Información es parte del Gobierno Corporativo centrándose en las implicaciones de los servicios e infraestructura de TI para que en un futuro la empresa tenga sostenibilidad y credibilidad asegurando su alineación con los objetivos estratégicos".[10].*

1.1. INFORMACIÓN CORPORATIVA

A continuación se realizará una descripción de la información corporativa del Departamento Administración Plataformas DSLAMs (APD).

1.1.1. ANTECEDENTES

La Corporación Nacional de Telecomunicaciones E.P., es una empresa estatal de telefonía, Internet y Datos del Ecuador, resultado de la fusión de las sociedades anónimas Andinatel y Pacifictel a finales de 2008 y Alegro PCS a comienzos de 2010.

Entre los servicios principales que presta la CNT E.P. podemos mencionar los siguientes: telefonía fija (local, regional e internacional), provisión de servicios de

acceso a Internet, DSL (Digital Subscriber Line, "línea de suscripción digital"), servicios corporativos y telefonía celular. [11]

Zonas de Distribución

Desde Noviembre de 2010 la Corporación Nacional de Telecomunicaciones E.P, se encuentra interconectada por medio de la Zona Andina (Andinatel S.A) como se ilustra en la Figura 1 y Zona Pacífico (Pacifictel S.A) como se ilustra en la Figura 2. La interconexión tiene el objetivo de integrar los servicios de telecomunicaciones utilizando la infraestructura de las dos zonas (andina y pacífico) con la finalidad de brindar los servicios de Telefonía/Internet/Datos por una sola red de Telecomunicaciones para todo el país.

Figura 1. Zona Andina (Andinatel S.A)
Fuente: Estructura enero 2012 CNT EP

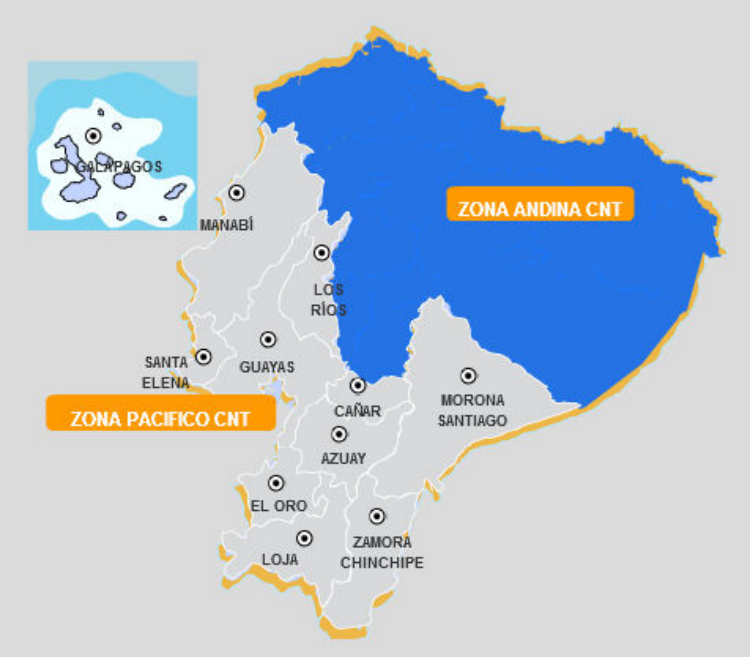


Figura 2. Zona Pacífico (Pacífico S.A)
Fuente: Estructura enero 2012 CNT EP

Para la unificación de la interconexión de la Zona Andina y Zona Pacífico, la Gerencia Nacional de tecnologías de información de la CNT E.P, encargada del proceso de integración nacional (en coordinación con el Gerente Nacional y los coordinadores Informáticos), ha establecido lineamientos para la atención, coordinación y publicación de los requerimientos de las diferentes áreas de la organización utilizando los medios de comunicación internos de la empresa. [11]

1.1.2. MISIÓN, VISIÓN, OBJETIVOS Y VALORES

A continuación se menciona la misión, visión, objetivos y valores de la Corporación Nacional de Telecomunicaciones E.P. [11]

Misión

Unimos a todos los ecuatorianos integrando nuestro país al mundo, mediante la provisión de soluciones de telecomunicaciones innovadoras, con talento humano comprometido y calidad de servicio de clase mundial.

Visión

Ser la empresa líder de telecomunicaciones del país, por la excelencia en su gestión, el valor agregado que ofrece a sus clientes y el servicio a la sociedad, que sea orgullo de los ecuatorianos.

Objetivos (Eje Crecimiento)

Incrementar la cobertura y la tasa de clientes en todas las líneas de negocio de la empresa.
Incrementar el acceso de los ciudadanos a la banda ancha y tecnología de la información y comunicación.

Objetivos (Eje Productividad)

Proveer productos y servicios de telecomunicaciones, comercialmente ser promotores de calidad incrementando la participación de la CNT E.P como principal proveedor de telecomunicaciones en el sector público.

Valores

Trabajamos en equipo.

Sumamos nuestros esfuerzos individuales para cumplir los objetivos de la CNT E.P.

Actuamos con Integridad

Actuamos con responsabilidad, honestidad, transparencia y lealtad, propiciando un entorno de trabajo ético.

Estamos Comprometidos con el servicio

Atendemos a nuestros clientes con excelencia, calidez y alegría, generando confianza y ofreciendo soluciones de última generación.

Cumplir con los objetivos empresariales

Aplicamos el empoderamiento de funciones con excelencia y la equidad social, para lograr la consecución de metas con innovación.

Somos socialmente responsables

Buscamos el bienestar de nuestros grupos de interés, siendo una empresa sustentable que aplica el desarrollo sostenible.

1.1.3. DEPARTAMENTO ADMINISTRACIÓN PLATAFORMAS DSLAMs CNT E.P.

El Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P. dispone a nivel nacional de equipamiento DSLAMs de diferentes marcas y proveedores tales como Huawei, Alcatel, ZTE y CTC, ver Tabla 1, los mismos que son operados y monitoreados a través de los sistemas de gestión. [3]

MARCA/PROVEEDOR	NACIONALIDAD/ORIGEN
Huawei	China
Alcatel	Belgica
ZTE	China
CTC	ESPAÑA

Tabla 1 Equipamiento DSLAM

La infraestructura DSL (Línea de suscripción digital) se encuentra monitoreada a través de los siguientes sistemas de gestión: iManager, Access Management System, NETNUMEN y CTC que permiten verificar la estabilidad de las líneas DSL y el correcto funcionamiento de los equipos (DSLAMs).[3]

Es indispensable que los sistemas de gestión se encuentren activos los 24x7x365 días al año, para que puedan hacer uso de estas aplicaciones los distintos departamentos de la CNT E.P tales como: NOC del inglés Network Operations Center (Centro de Control de la Red), Call Center UIO/GYE, Gestión Administración Plataformas DSLAMs y unidades regionales de la CNT E.P.

Actualmente la infraestructura de gestión del Departamento Administración Plataformas DSLAMs se encuentra conectada mediante dos redes denominadas MPLS del inglés Multiprotol Label Switching y SISTEMAS como se ilustra en Figura 3. El tráfico de voz, Internet y datos de los clientes cursa por la red MPLS y el tráfico de los usuarios internos cursa por la red de SISTEMAS, con la finalidad de gestionar las aplicaciones y monitorear la de disponibilidad de los servicios de los clientes.[3]

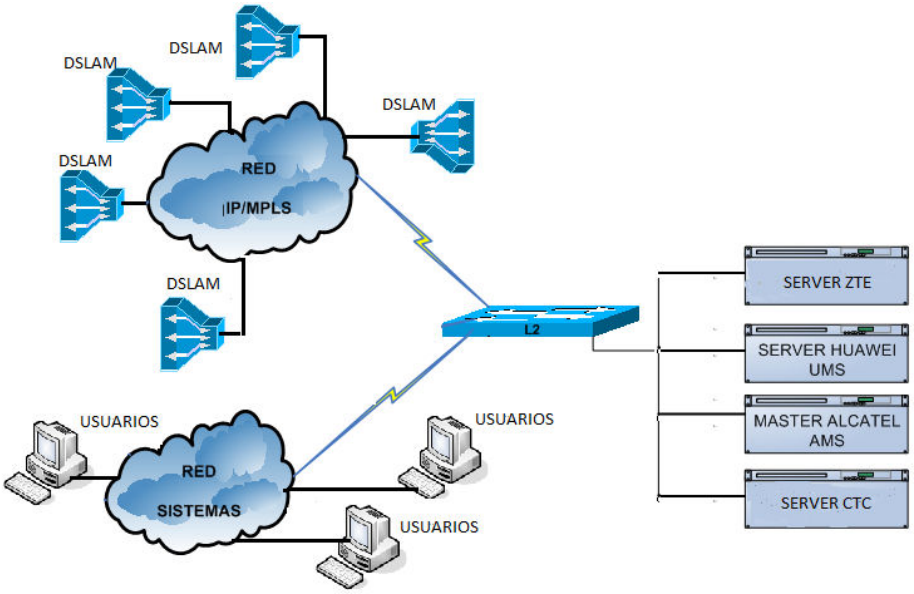


Figura 3 Conexión de las redes DSLAMs con los Sistemas Gestión

El Departamento Administración Plataformas DSLAMs de la CNT E.P., tiene instalado equipamiento en las 24 provincias del Ecuador, en las provincias de Pichincha y Guayas existe un mayor número de clientes y por ende mayor número de equipos, como se indica en la Tabla 2.

PROVINCIAS	NÚMERO DE DSLAMs	NÚMERO DE CLIENTES
AZUAY	37	4352
BOLIVAR	31	5841
CAÑAR	36	9184
CARCHI	43	5976
CHIMBORAZO	115	24676
COTOPAXI	83	16106
EL ORO	106	23636
ESMERALDAS	63	15542
GALAPAGOS	14	2188
GUAYAS	348	106712
IMBABURA	83	21357
LOJA	84	21821

PROVINCIAS	NÚMERO DE DSLAMs	NÚMERO DE CLIENTES
LOS RIOS	58	17486
MANABI	129	38283
MORONA SANTIAGO	22	4932
NAPO	21	5262
ORELLANA	27	5280
PASTAZA	29	6637
PICHINCHA	763	222311
SANTA ELENA	48	10851
SUCUMBIOS	42	6455
TUNGURAHUA	117	33920
ZAMORA CHINCHIPE	27	3625
SANTO DOMINGO DE TSÁCHILAS	48	11456
Total General	2374	623889

Tabla 2 Número de Dslams instalados por provincias del Ecuador

1.1.3.1 ELEMENTOS DE TECNOLOGÍAS DE INFORMACIÓN DSLAMs DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES E.P.

A continuación se presenta los elementos de TI del Departamento Administración Plataformas DSLAMs de la CNT E.P: [3]

- **DSLAM**

El DSLAM es un multiplexor localizado en la central telefónica que proporciona a los abonados el acceso a los servicios DSL (Internet, datos, voz y video), sobre un cable de par trenzado de cobre.[2]

Para brindar estos servicios la comunicación se realiza a través del DSLAM y el MODEM “dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras.” xDSL “se refiere a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica”, por medio de dos interfaces llamadas ATU-R o "ADSL Terminal Unit-Remote" (del lado del cliente o

abonado) y ATU-C o "ADSL Terminal Unit-Central" (del lado del proveedor del servicio). Delante de cada modem se coloca un dispositivo denominado splitter, el mismo que consta de dos filtros, uno de paso alto y otro de paso bajo, cuya finalidad es la de separar las señales transmitidas de baja frecuencia (telefonía) y las de alta frecuencia (datos).[2]

El Departamento Administración Plataformas DSLAMs, administra, opera y controla los DSLAMs a nivel nacional, como se ilustra en la (Tabla 3):

CANTIDAD TOTAL A NIVEL NACIONAL	DESCRIPCIÓN	MARCA
900	DSLAMs - ALCATEL	ALCATEL
850	DSLAMs - HUAWEI	HUAWEI
60	DSLAMs – ZTE	ZTE
20	DSLAMs – CTC	CTC
TOTAL=1830		

Tabla 3 Cantidad de Equipos DSLAM

- **Infraestructura**

El Departamento de Administración Plataformas DSLAMs (APD) maneja varias Plataformas tecnológicas para brindar el servicio. Por cuestiones de seguridad se presenta la información básica de la infraestructura del Departamento APD que es administrada y controlada a nivel nacional. La información sobre la infraestructura se encuentra dividida en tres componentes básicos: Hardware, Software y Sistemas de Gestión.

En la Tabla 4 se presenta el Hardware que opera en el Departamento APD.

HARDWARE			
CANT.	UBICACIÓN	DESCRIPCIÓN	MARCA
1	Gerencia	PC Intel inside Core i7 / laptop	HP
1	Jefatura	PC Intel inside Core i7	HP
7	Ingenieros	PC Intel inside Core i7	HP
1	Administrativos	Laptops	HP
8	Técnicos	Laptop HP / PC Intel inside Core i7	HP
1	Sala de servidores	N2000Server / Sun blade 2500	SUN
1	Sala de servidores	USMAWS552314 / Sun-Fire-V210	SUN

HARDWARE			
CANT.	**UBICACIÓN**	**DESCRIPCIÓN**	**MARCA**
1	Sala de servidores	USMAWS552312 / Sun-Fire-V210	SUN
1	Sala de servidores	USMAWS552313 / Sun-Fire-V210	SUN
1	Sala de servidores	USMAWS552316 / Sun-Fire-V210	SUN
1	Sala de servidores	USMAWS552317 / Sun-Fire-V240	SUN
1	Sala de servidores	aws552372 / Sun-Fire-V245	SUN
1	Sala de servidores	U2000 / Sun-M4000	SUN
1	Sala de servidores	AMS / Sun - T5120	SUN
1	Sala de servidores	N2000Server / Sun blade 2500	SUN
1	Sala de servidores	USMAWS552314 / Sun-Fire-V210	SUN
1	Sala de servidores	USMAWS552312 / Sun-Fire-V210	SUN
2	Sala de servidores	HP	HP
900	Nivel Nacional	DSLAMs - ALCATEL	ALCATEL
850	Nivel Nacional	DSLAMs - HUAWEI	HUAWEI
60	NIVEL NACIONAL	DSLAMs – ZTE	ZTE
20	REGIONAL 1,2,3	DSLAMs – CTC	CTC
1	Administración Plataformas DSLAMs (Servers)	UPS – 1200 VA (Energía Asegurada)	
1	DSLAMs depende la cantidad de equipamiento	UPS – 900 VA (Energía Asegurada)	
1	Sala de Servidores	UPS – 1200 VA (Energía Asegurada)	

Tabla 4 Recurso de Hardware
Fuente: Administración Plataformas DSLAMs

En la Tabla 5 se presenta el software que se encuentra licenciado y que opera en el Departamento APD.

SOFTWARE	
NOMBRE	**VERSIÓN**
Microsoft Windows	Windows 7
Microsoft Windows	2000 Server
Solaris	10
SUSE LINUX	10
Alcatel	4,3
Huawei	R6
Zte	R3
Ctc	R2
Oracle	9i
Open.Flexis	9i

Tabla 5 Recurso Software
Fuente: Administración Plataformas DSLAMs

En la Tabla 6 se presenta los sistemas de gestión del Departamento APD los cuales se encuentran desarrollados en arquitectura **cliente-servidor** con tecnología e interfaces **JAVA.**

SISTEMAS DE GESTIÓN				
CANT.	**NOMBRE**	**GESTIÓN DE TODA LA PLATAFORMA**	**BASE DE DATOS**	**MODULOS DE COBERTURA**
1	Imanager	Huawei	SYBASE	• Gestión de los DSLAMs (en función la plataforma) • Administración de usuarios a nivel nacional • Administración de los DSLAMs • Administración de perfiles de velocidad a nivel nacional. • Activación de puertos
1	Access managament system	Alcatel	SQL SERVER	
1	Netnumen	ZTE		
1	CTC	CTC		

Tabla 6. Sistemas de Gestión
Fuente: Administración Plataformas DSLAMs

- **Comunicaciones**

Para brindar el servicio de Administración de los DSLAMs de la CNT E.P, se utilizan varios medios de transmisión, entre los principales tenemos: fibra óptica, par trenzado, microonda y coaxial.

Para las comunicaciones de los DSLAMs (que brinda el servicio de Internet, datos, voz y video) se utiliza la Red MPLS.

En la Tabla 7 se presenta los medios de comunicación del Departamento Administración Plataformas DSLAMs.

COMUNICACIÓN	
RECURSO	**TIPO**
Cableado	UTP cat 5
Cableado	UTP cat 6
Fibra Óptica	Fibra
Radio	microondas
MPLS	MPLS

Tabla 7. Medios de Comunicación del Departamento Administración Plataformas DSLAMs
Fuente: Administración Plataformas DSLAMs

- **Estándares y Procedimientos**

El Departamento de Administración de Plataformas DSLAMs (ADP) de la Corporación Nacional de Telecomunicaciones E.P., maneja estándares y procedimientos para controlar, evaluar y mejorar los servicios de Internet y Datos a nivel nacional mediante los equipos de acceso (DSLAM) e infraestructura para sus clientes internos como externos.[3]

La CNT E.P. cuenta en la actualidad con certificaciones de los estándares ISO/IEC 9001: 2008 e ISO/IEC 27001. [2]

Es importante indicar que los procesos de seguridad del Departamento Administración Plataformas DSLAMs (APD) en la actualidad se encuentra en el fortalecimiento de los controles de confiabilidad, integridad, disponibilidad y de acceso para mantener los servicios activos 7x24, para todos los clientes internos como externos de la Corporación Nacional de Telecomunicaciones E.P.

Para tal efecto, se está implementando una estrategia de seguridad que abarque todos los sistemas del Departamento APD.

En la Tabla 8 se presentan los procedimientos del Departamento APD:

NOMBRE PROCEDIMIENTO	ELABORADO POR	FECHA DE APROBACIÓN	REVISADO POR	APROBADO POR
Configuración de Perfiles de Ancho de Banda y VLANS	Plataforma DSLAM CNT EP	Agosto 2013	Jefatura O&M Soluciones Internet, TV y Datos	Gerencia O&M Core Plataformas
Contingencia de Servidores de Gestión DSLAM	Administrador de Servidores de Gestión Plataforma DSLAM CNT EP	Agosto 2013		
Control de Cambios en Plataforma DSLAM	Plataforma DSLAM CNT EP	Agosto 2013		
Monitoreo Plataforma DSLAM	Plataforma DSLAM CNT EP	Julio 2013		
Mantenimiento en la Plataforma DSLAM	Plataforma DSLAM CNT EP	Agosto 2013		

Tabla 8 Procedimientos del Departamento de APD

- **Activación en las plataformas**

La activación de las plataformas es un procedimiento que configura un puerto específico para que un cliente pueda obtener el servicio que ha contratado. El objetivo del Departamento Administración Plataformas DSLAMs es automatizar esta actividad.

Al momento la activación de las plataformas se encuentra en un proceso de elaboración de un sistema de configuración automática de los IP-DSLAM de plataforma ALCATEL y HUAWEI. Luego de la puesta en producción del sistema, se continuará con el desarrollo de configuración automática de las plataformas CTC y ZTE.

De la misma manera, actualmente se está realizando un proceso de actualización de los datos en OpenFlexis ”Base de Datos que almacena la información de los clientes y de las plataformas para llevar un registro contable del uso de los servicios”.

- **Estructura Organizacional**

Dentro de la estructura organizacional de la CNT E.P, el Departamento de Administración Plataformas DSLAMs se encuentra bajo la gerencia de O&M de Core y Plataformas y de la Gerencia Nacional Técnica quienes lideran y direccionan al personal para brindar los servicios de TI a los clientes. [3]

A continuación, en la Figura 4 se ilustra la Estructura Organizacional descrita anteriormente.

Figura 4. Organigrama estructural del Departamento Administración Plataformas DSLAMs.
Fuente: Estructura CNT EP.

En la actualidad son 16 profesionales los que se encuentran laborando en el Departamento Administración Plataformas DSLAMs. Cada uno de ellos cuenta con funciones y responsabilidades establecidas por la Jefatura de O&M de Soluciones (Internet TV y Datos) como se ilustra en la Figura 4. Es importante indicar que dos (2) ingenieros de TI se encuentran a cargo de la administración de los servidores de gestión DSLAMs donde residen las aplicaciones; los restantes ingenieros de TI (5) y todos los tecnólogos (7) son dedicados a las tareas de administración de operación y mantenimiento DSLAMs.

CONFORMACIÓN APD	
Profesional	**Cantidad**
Autoridad	1
Ingenieros de TI	7
Administrativo	1
Tecnólogos de TI	7
TOTAL	**16**

Tabla 9 Recurso Humano
Fuente: Departamento Administración Plataforma DSLAMs

1.2. DIAGNOSTICO ACTUAL DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

Para realizar el diagnóstico del Gobierno de Tecnologías de la Información del Departamento Administración Plataformas DSLAMs se realizará un análisis del tratamiento de la información y también se efectuará la caracterización del Departamento APD utilizando la técnica de análisis FODA.

1.2.1. TRATAMIENTO DE LA INFORMACIÓN.

Al momento el Departamento APD genera información de diferente índole y con varios niveles de confidencialidad. Aunque la CNT E.P cuenta con la certificación ISO 27001, es importante fortalecer los siguientes controles. [3]

1. **Ingreso Físico:** Controlar el ingreso a los nodos y acceso a los servidores de gestión del Departamento APD por medio de un sistema de control de acceso.
2. **Información Escrita:** Los documentos que se generen en el departamento deben estar debidamente resguardados por personal administrativo. En el caso que se requiera acceder a esa información el solicitante debe tener el permiso respectivo.
3. **Información Electrónica:** Es necesario que la información digital sea custodiada y respaldada debidamente bajo un esquema de gestión de

versiones Ejemplo: Manuales, Diagramas de red, bases de datos. Backup Nodos, backup servers, CDs, discos externos.

4. **Correos Electrónicos:** Es importante controlar que el envió de información sea únicamente al personal que se encuentra involucrado en el proceso de administración y Operación del Departamento.
5. **Documentación Impresa:** Los documentos no deben encontrarse al alcance del personal que no corresponde al departamento APD. Por ejemplo: reportes, documentos de contratos, información personal, entre otros.

Las acciones que se recomiendan para el tratamiento de la información anteriormente descrita son las siguientes:

- Establecer responsables para el desarrollo de cada procedimiento en la información.
- Establecer responsables para la revisión de los procedimientos.
- Establecer responsables para la aprobación de los procedimientos.
- Levantar la Documentación.
- Levantar y Aprobar la Política de Documentación.
- Realizar una campaña de entrenamiento con la documentación levantada.
- Concientizar a los Directivos y Operativos de la necesidad de procedimientos y su utilización.
- Llegar a acuerdos con Recursos Humanos para las sanciones en caso de no cumplir con las políticas.
- Incluir en el reglamento interno de la empresa las sanciones.

1.2.2. CARACTERIZACIÓN DEL DEPARTAMENTO ADMINISTRACIÓN PLATAFORMAS DSLAMs (APD)

A continuación un breve análisis del Departamento Administración Plataformas DSLAMs.

- **Análisis del Departamento Administración Plataformas DSLAMs (APD)**

La Corporación Nacional de Telecomunicaciones E.P., dispone a nivel nacional de equipamiento DSLAM, los mismos que son gestionados a través de la plataforma de gestión de diferentes proveedores Huawei/Alcatel/ZTE/CTC. Estas plataformas adicionalmente permiten verificar la estabilidad de las líneas de DSL y la correcta operación de los equipos DSLAMs.

En la actualidad, estas plataformas de gestión son accedidas por distintos departamentos de la CNT E.P., como NOC, Call Center UIO/GYE y unidades regionales a nivel nacional, para ejecutar tareas de administración, monitoreo, configuración, instalación de puertos, mantenimiento preventivo y correctivo de los equipos de acceso de Internet y Datos (DSLAM) que se encuentra en la red CNT E.P., a nivel nacional la cual es Administrada por el Departamento Administración Plataformas DSLAMs.

Por ello, siendo primordial que la disponibilidad del servicio de las plataformas sea de tipo Carrier Class (99.999%), es necesario establecer procedimientos de Operación Soporte y Acceso en esta plataforma.

A continuación se realizara un análisis fundamentado en el Departamento Administración Plataformas DSLAMs.

- **Análisis FODA**

En las Tablas 10 y 11 se presenta el análisis de las Fortalezas, Debilidades, Oportunidades y Amenazas del Departamento Administración Plataformas DSLAMs, basado en un análisis interno y externo.

- **Análisis Interno.**

ANÁLISIS INTERNO	
FORTALEZAS	**DEBILIDADES**
-Experiencia de los recursos humanos. -Procesos técnicos y administrativos para alcanzar los objetivos de la organización. -Presupuesto dedicado al área de Gestión. -Características especiales de los productos. -Calidad del servicio.	-Capital Humano de Trabajo mal utilizado. -Cambios gerenciales continuos. -Segmento del mercado dividido. -Problemas con calidad. -Falta de capacitación. -Falta de Procedimientos. -Escasos controles de acceso.

Tabla 10 FODA Análisis Interno
Fuente: Administración Plataformas DSLAMs

- **Análisis Externo.**

ANÁLISIS EXTERNO	
AMENAZAS	**OPORTUNIDADES**
-Competencia agresiva. -Cambios en la legislación. -Tendencias desfavorables en el mercado.	-Mercado mal atendido. -Necesidad del producto. -Poder adquisitivo. -Creación de nuevos servicios.

Tabla 11 FODA Análisis Externo
Fuente: Administración Plataformas DSLAMs

Mediante una matriz FODA, Tabla 12, se relacionan los cuatro dominios que presentan las estrategias FA, DA, FO, DO.

- **Matriz FODA.**

ANALISIS INTERNO / **ANALISIS EXTERNO**	**FORTALEZAS** -Experiencia de los recursos humanos. -Procesos técnicos y administrativos para alcanzar los objetivos de la organización. -Presupuesto dedicado al área de Gestión. -Características especiales de los productos. -Calidad del servicio.	**DEBILIDADES** -Capital Humano de Trabajo mal utilizado. -Cambios gerenciales continuos. -Segmento del mercado dividido. -Problemas con calidad. -Falta de capacitación. -Falta de procedimientos. -Escasos controles de acceso.
AMENAZAS -Competencia agresiva. -Cambios en la legislación. -Tendencias desfavorables en el mercado	**ESTRATEGIA FA:** Garantizar que los servicios de telecomunicaciones sean eficientes, competitivos y efectivos.	**ESTRATEGIA DA:** -Capacitación en venta y promoción de productos. -Ser patrocinadores en grandes eventos.
OPORTUNIDADES -Mercado mal atendido -Necesidad del producto -Poder adquisitivo. -Creación de nuevos servicios.	**ESTRATEGIA FO:** Diferenciación en base al costo, beneficio y calidad en el servicio.	**ESTRATEGIA DO:** Desarrollar nuevas infraestructuras de telecomunicaciones que brinden y posibiliten la inclusión del servicio de la sociedad.

Tabla 12 Matriz FODA
Fuente: Administración Plataformas DSLAMs

En base al análisis se puntualiza lo siguiente del Departamento Administración Plataformas DSLAMs respecto a la Gestión de TI:

- Se debe establecer un diagnóstico inicial de qué procedimientos se requieren en las plataformas DSLAMs y sistemas de gestión.
- Se debe efectuar un análisis de tiempos para levantar la documentación del Departamento APD.
- El organigrama estructural (Figura 4) no contempla unidades administrativas como: Unidad Seguridad, Unidad Abastecimientos, Unidad de Operación y Unidad de Soporte.
- Existe un administrador de seguridad sin reconocimiento del Departamento Administración Plataformas DSLAMs y organizacional.
- La gestión de los servicios del Departamento Administración Plataformas DSLAMs es limitada, no se alinea a los objetivos Institucionales.
- El Departamento Administración Plataformas DSLAMs no se alinea a la misión, visión y objetivos de la CNT E.P.
- Por la falta de objetivos claros y de recursos, el Departamento Administración Plataformas DSLAMs, no es soporte de los objetivos de la CNT E.P., disminuyendo su competitividad frente a otros proveedores del servicio de Internet y Datos.
- La situación actual del Departamento Administración Plataformas DSLAMs no le permite ser proactiva en la marcha de la CNT E.P. Se debe proponer el mejoramiento continuo de los servicios de Internet y Datos a través de los planes Estratégico, Contingencia, Seguridades, Continuidad, Gestión de Riesgos y Recuperación de Desastres, etc.
- El Departamento Administración Plataformas DSLAMs desconoce los costos y servicios que actualmente ofrece CNT E.P.
- El Departamento Administración Plataformas DSLAMs no tiene claro el dar soporte a los clientes tanto internos como externos.
- El Departamento Administración Plataformas DSLAMs debe establecer lineamientos para la atención, coordinación y publicación de los requerimientos de las diferentes áreas de la organización en los medios de comunicación interna de la empresa.

- El Departamento Administración Plataformas DSLAMs es el encargado del proceso de integración de equipos de acceso en coordinación con el Gerente Nacional y los coordinadores técnicos de cada zona los cuales deben demostrar sus capacidades que le permitan realizar una labor ágil y productiva.
- El Departamento Administración Plataformas DSLAMs es el encargado de liderar implementaciones de los sistemas así como de la capacitación de los funcionarios.

CAPÍTULO 2

ELABORACIÓN DE LA PROPUESTA DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

En este capítulo, se realiza un análisis de cómo se referencian COBIT, ITIL V3 e ISO-27001 para elaborar una propuesta de Gobierno de Tecnologías de la Información para el Departamento de Administración de Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P. En cuanto a COBIT esta investigación se basa en el dominio de "Entregar y dar Soporte", en cuanto a ITIL se basa en las mejores prácticas de la "Operación del Servicio", y en cuanto a ISO-27001 el mismo se enfoca en las actividades de "Control de acceso", tal y como muestra la Figura 5:

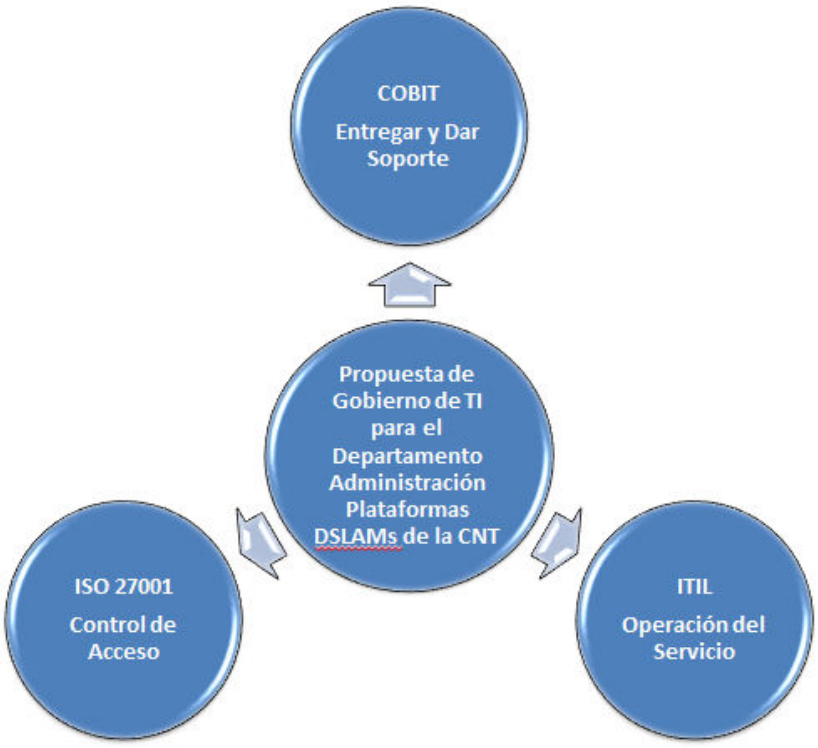


Figura 5. Mejores Prácticas para desarrollar la Propuesta de Gobierno de TI para el Departamento de Administración Plataformas DSLAMs CNT E.P.

2.1. MAPEO DE COBIT, ITIL e ISO-27001

Para tal efecto se realizará un mapeo de los procesos utilizando la siguiente metodología como se ilustra en la Figura 6:

- **PASO 1. IDENTIFICACIÓN:** Identificar los objetivos de control para COBIT (Entregar y Dar Soporte), procesos de ITIL (Operación del Servicio) y controles de la ISO 27001 (Control de Acceso).
- **PASO 2. COBIT Vs ITIL:** Referenciar o mapear la cobertura de los objetivos de control de COBIT y los procesos de ITIL V3.
- **PASO 3. COBIT vs ISO 27001:** Referenciar o mapear la cobertura de los objetivos de control de COBIT y los controles de la ISO 27001.
- **PASO 4. INTEGRACIÓN:** Articular los pasos 2 y 3, es decir, integrar los procesos de control de COBIT, ITIL e ISO 27001 y presentar los resultados del mapeo.

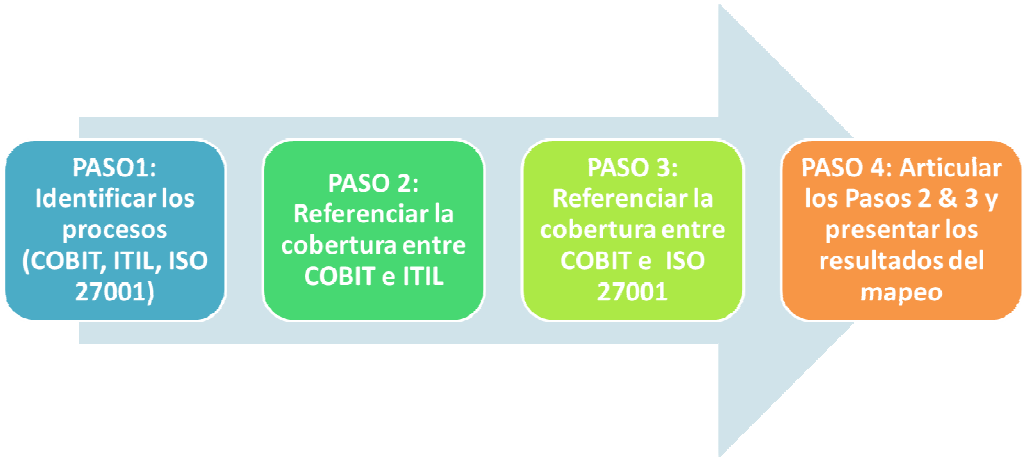


Figura 6. Metodología de Mapeo COBIT, ITIL V3 e ISO 27001

2.1.1 PASO 1. IDENTIFICACIÓN:

A continuación, en la Tabla 13 se presenta los objetivos de control de COBIT 4.1 del dominio **Entregar y Dar Soporte (DS)**: [8]

COBIT 4.1 – ENTREGAR Y DAR SOPORTE (DS)
DS1 Definir y administrar los niveles de servicio
DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio
DS1.2 Definición de Servicios
DS1.3 Acuerdos de Niveles de Servicio
DS1.4 Acuerdos de Niveles de Operación
DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio
DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos
DS2 Administrar los servicios de terceros
DS2.1 Identificación de todas las relaciones con proveedores
DS2.2 Gestión de relaciones con proveedores
DS2.3 Administración de riesgos del proveedor
DS2.4 Monitoreo del desempeño del proveedor
DS3 Administrar el desempeño y la capacidad
DS3.1 Planeación del desempeño y la capacidad
DS3.2 Capacidad y desempeño actual
DS3.3 Capacidad y desempeño futuros
DS3.4 Disponibilidad de recursos de TI
DS3.5 Monitoreo y reportes
DS4 Garantizar la continuidad del servicio
DS4.1 Marco de trabajo de continuidad de TI
DS4.2 Planes de continuidad de TI
DS4.3 Recursos críticos de TI
DS4.4 Mantenimiento de plan de continuidad de TI
DS4.5 Pruebas del plan de continuidad de TI
DS4.6 Entrenamiento del plan de continuidad de TI
DS4.7 Distribución del plan de continuidad de TI
DS4.8 Recuperación y reanudación de los servicios de TI
DS4.9 Almacenamiento de respaldos fuera de las instalaciones
DS5 Garantizar la seguridad de los sistemas
DS5.1 Administración de la seguridad de TI
DS5.2 Plan de seguridad de TI
DS5.3 Administración de Identidad
DS5.4 Administración de cuentas de usuario
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad
DS5.6 Definición de incidentes de seguridad
DS5.7 Protección de la tecnología de seguridad
DS5.8 Administración de llaves criptográficas
DS5.9 Prevención, Detención y corrección de software malicioso
DS5.10 Seguridad de la red
DS5.11 Intercambio de datos sensitivos
DS6 Identificar y asignar costos
DS6.1 Definición de servicios
DS6.2 Contabilización de TI
DS6.3 Modelación de costos y cargos

COBIT 4.1 – ENTREGAR Y DAR SOPORTE (DS)
DS6.4 Mantenimiento del modelo de costos
DS7 Educar y entrenar a los usuarios
DS7.1 Identificación de Necesidades de Entrenamiento y Educación
DS7.2 Impartición de Entrenamiento y Educación
DS7.3 Evaluación del Entrenamiento Recibido
DS8 Administrar la mesa de servicio y los incidentes
DS8.1 Mesa de servicio
DS8.2 Registro de consultas de clientes
DS8.3 Escalamiento de incidentes
DS8.4 Cierre de incidentes
DS8.5 Análisis de tendencias
DS9 Administrar la configuración
DS9.1 Repositorio y Línea Base de configuración
DS9.2 Identificación y Mantenimiento de elementos de configuración
DS9.3 Revisión de integridad de la configuración
DS10 Administrar los problemas
DS10.1 Identificación y clasificación de problemas
DS10.2 Rastreo y resolución de problemas
DS10.3 Cierre de problemas
DS10.4 Integración de las administraciones de cambios, configuración y Problemas.
DS11 Administrar los datos
DS11.1 Requerimientos del Negocio para Administración de Datos
DS11.2 Acuerdos de Almacenamiento y Conservación
DS11.3 Sistemas de Administración de Librerías de Medidas
DS11.4 Eliminación
DS11.5 Respaldo y Restauración
DS11.6 Requerimientos de Seguridad para la Administración de Datos
DS12 Administrar el ambiente físico
DS12.1 Selección y Diseño del Centro de Datos
DS12.2 Medidas de Seguridad Física
DS12.3 Acceso Físico
DS12.4 Protección Contra Factores Ambientales
DS12.5 Administración de Instalaciones Físicas
DS13 Administrar las operaciones
DS13.1 Procedimientos e instrucciones de operación
DS13.2 Programación de tareas
DS13.3 Monitoreo de la infraestructura de TI
DS13.4 Documentos sensitivos y dispositivos de salida
DS13.5 Mantenimiento preventivo del hardware

Tabla 13. COBIT - Objetivos de Control: Entregar y Dar Soporte
Fuente: COBIT 4.1

De la misma manera, en la Tabla 14 se presenta los procesos de ITIL referidos a las actividades de **Operación del Servicio (SO): [10]**

ITIL V3 – OPERACIÓN DEL SERVICIO (SO)
SO1 Introducción
SO2 Gestión del Servicio como una Práctica
SO 2.1 Qué es la gestión del servicio?
SO 2.2 Cuáles son los servicios?
SO 2.3 Funciones y procesos en todo el ciclo de vida
SO 2.4 Servicio fundamentos de operación
SO3 Principales Servicio de Operación
SO 3.1 Funciones , grupos, equipos , departamentos y divisiones
SO 3.2 Lograr equilibrio en la operación servicio
SO 3.2.4 Reactive vs. Proactive Organizaciones
SO 3.3 Proporcionar servicio
SO 3.4 Personal de operaciones involucradas en el diseño del servicio y el servicio
SO 3.5 Salud operacional
SO 3.6 Comunicación
SO 3.7 Documentación
SO4 Procesos de operación de servicio
SO 4.1 Gestión de eventos
SO 4.1.5.1 Ocurrencia de eventos
SO 4.1.5.2 Notificación de eventos
SO 4.1.5.3 Detección de eventos
SO 4.1.5.4 Filtrado de eventos
SO 4.1.5.5 Significado de eventos
SO 4.1.5.6 Correlación de eventos
SO 4.1.5.7 Trigger
SO 4.1.5.8 Respuestas de selección
SO 4.1.5.9 Revisión y acciones
SO 4.1.5.10 Cierre de eventos
SO 4.2 Gestión de incidentes
SO 4.2.5.1 identificación de Incidentes
SO 4.2.5.2 Registro de incidentes
SO 4.2.5.3 Categorización de incidentes
SO 4.2.5.4 Priorización de incidentes
SO 4.2.5.5 Diagnóstico inicial
SO 4.2.5.6 Escalación de incidentes
SO 4.2.5.7 Investigación y diagnostico
SO 4.2.5.8 Resolución y recuperación
SO 4.2.5.9 Cierre de incidentes
SO 4.3 Solicitud cumplimiento

ITIL V3 – OPERACIÓN DEL SERVICIO (SO)
SO 4.3.5.1 Menu selección
SO 4.3.5.2 Aprobación financiera
SO 4.3.5.3 Otra aprobación
SO 4.3.5.4 Cumplimiento
SO 4.3.5.5 Cierre
SO 4.4 Gestión de problemas
SO 4.4.5.1 Detección de problemas
SO 4.4.5.2 Registro de problemas
SO 4.4.5.3 Categorización de problemas
SO 4.4.5.4 Priorización de problemas
SO 4.4.5.5 Investigación de problemas y diagnóstico
SO 4.4.5.6 Soluciones provisionales
SO 4.4.5.7 Levantamiento de registro de error conocido
SO 4.4.5.8 Resolución de problemas
SO 4.4.5.9 Cierre de problemas
SO 4.4.5.10 Revisión de problemas mayores
SO 4.4.5.11 Errores detectados en el entorno del desarrollo
SO 4.5 Gestión de Acceso
SO 4.5.5.1 Solicitando accesos
SO 4.5.5.2 Verificación
SO 4.5.5.3 Proporcionando derechos
SO 4.5.5.4 Monitoreando el estado de identidad
SO 4.5.5.5 Registro y seguimiento del acceso
SO 4.5.5.6 Eliminación o restricción de los derechos
SO 4.6 Actividades operacionales de los procesos cubiertos en otros ciclo de vida
SO 4.6.1 La gestión del cambio (como las actividades operacionales)
SO 4.6.2 Gestión de la configuración (como las actividades operacionales)
SO 4.6.3 Gestión de la configuración (como las actividades operacionales)
SO 4.6.4 Gestión de la capacidad (como las actividades operacionales)
SO 4.6.5 Administración de disponibilidad (como las actividades operacionales)
SO 4.6.6 Gestión del conocimiento (como las actividades operacionales)
SO 4.6.7 Gestión financiera de los servicios de TI (como las actividades operacionales)
SO 4.6.8 Gestión de la continuidad del servicio de TI
SO5 Actividades de operación de servicio común
SO 5.1 Monitoreo y control
SO 5.2 Operaciones de TI
SO 5.2.1 Consola de gestión/puente operaciones
SO 5.2.2 La planificación de tareas
SO 5.2.3 Copia de seguridad y restauración
SO 5.2.4 Imprimir y salida DS13.4 documentos sensibles y dispositivos de salida
SO 5.3 Gestión Mainframe

ITIL V3 – OPERACIÓN DEL SERVICIO (SO)
SO 5.4 Administración de servidores y soporte
SO 5.5 Gestión de redes
SO 5.6 Almacenamiento de archivos
SO 5.7 Administración de base de datos
SO 5.8 Directorio de administración de servicios
SO 5.9 soporte Desktop
SO 5.10 Gestión Middleware
SO 5.11 administración Internet / web
SO 5.12 Facilidades y gestión del centro de datos
SO 5.13 Gestión de seguridad de la información y operación de servicio (vague)
SO 5.14 Mejora de las actividades operacionales (vague)
SO 6 La organización para la operación del servicio
SO 6.1 Funciones
SO 6.2 Service desk
SO 6.3 Gestión técnica
SO 6.4 IT Gestión de operaciones
SO 6.5 Gestión de aplicaciones
SO 6.6 Operación de roles de servicio y responsabilidades
SO 6.7 Operación del servicio y estructura organizacional
SO 7 Consideraciones tecnológicas (concesión de licencias)
SO 8 La implementación de la operación del servicio
SO 9 Retos, factores críticos de éxito y riesgos

Tabla 14. ITIL V3 – Procesos de Operación del Servicio (SO)
Fuente: ITIL V3

En la siguiente Tabla 15 se presenta las actividades de **Control de Acceso (A.11)** de la Norma ISO 27001: [4]

ISO 27001 – CONTROL DE ACCESO (A.11)
A.11.1 Requisitos del Negocio para el Control de Acceso
A.11.1.1 Políticas para el control de acceso
A.11.2 Administración de Accesos de Usuarios
A.11.2.1 Registro de usuarios
A.11.2.2 Administración de privilegios
A.11.2.3 Administración de contraseñas para usuarios
A.11.2.4 Revisión de los derechos de acceso de los usuarios
A.11.3 Responsabilidades de los Usuarios
A.11.3.1 Uso de contraseñas
A.11.3.2 Equipo de cómputo de usuario desatendido
A.11.3.3 Política de puesto de trabajo despejado y bloqueo de pantalla
A.11.4 Control de Acceso a Redes
A.11.4.1 Política de uso de los servicios en red

ISO 27001 – CONTROL DE ACCESO (A.11)
A.11.4.2 Autenticación de usuarios para conexiones externas
A.11.4.3 Identificación de equipos en red
A.11.4.4 Protección de puertos de diagnóstico y configuración remota
A.11.4.5 Segmentación de redes
A.11.4.6 Control de conexión a las redes
A.11.4.7 Control de enrutamiento en la red
A.11.5 Control de Acceso al Sistema Operativo
A.11.5.1 Procedimientos de identificación de usuarios segura
A.11.5.2 Identificación y autenticación de usuarios
A.11.5.3 Sistema de administración de contraseñas
A.11.5.4 Uso de utilidades del sistema
A.11.5.5 Time-out de sesión
A.11.5.6 Limitación del tiempo de conexión
A.11.6 Control de Acceso a la Información y a las Aplicaciones
A.11.6.1 Restricción de acceso a la información
A.11.6.2 Aislamiento de sistemas relevantes
A.11.7 Computación Móvil y Trabajo Remoto
A.11.7.1 Computación y comunicaciones móviles
A.11.7.2 Trabajo remoto

Tabla 15. ISO 27001 – Actividades Control de Acceso
Fuente: ISO 27001

Como se muestran los resultados de las tablas anteriores, COBIT es el marco que cubre o que contiene los procesos de control tanto de ITIL como de ISO 27001, *"como una aproximación completa a la gestión y gobierno de TI"* [8]. La siguiente figura 7 muestra el área de cobertura de estas tres mejores prácticas:

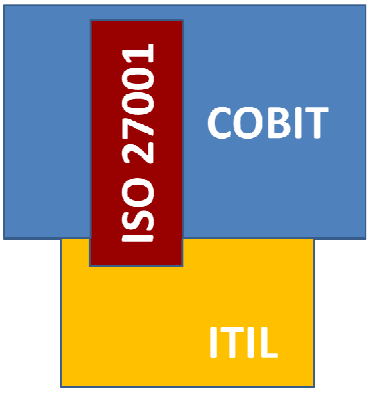


Figura 7. Cobertura de Procesos Mejores Prácticas
Fuente: COBIT 4.1

Por lo tanto, se utilizará como referencia la Figura 7 para mapear los procesos de COBIT, ITIL e ISO 27001, con el fin de presentar resultados y analizarlos desde el punto de vista de Seguridad y de Gobierno de Tecnologías de Información.

2.1.2 PASO 2. COBIT vs ITIL:

En este segundo paso, para mapear los controles se referenciarán la cobertura de los objetivos de control de COBIT del Dominio Entregar y Dar Soporte (DS) y los procesos de Operación del Servicio (SO) de ITIL, **enfocados en la Seguridad de la Información**, con el fin de cumplir los objetivos propuestos para esta investigación. [12]

En la Tabla 16 se encuentra la descripción "OTRO PROCESO/CONTROL DE ITIL", y se refiere a procesos de ITIL que cubren el objetivo de Control de COBIT pero pertenecen a otro Macro Proceso, por ejemplo: Estrategia del Servicio (SS), Diseño del Servicio (SD) o Transición del Servicio (ST) de ITIL V3.

De la misma manera, la especificación "NO EXISTE PROCESO/CONTROL EN ITIL" se refiere a que ITIL no contiene un proceso que abarque las actividades del objetivo de control de COBIT.

Es importante indicar que el mapeo de la Tabla 16 se basa en el documento oficial de ISACA denominado *"Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit"*, 2008. [7]

MAPEO COBIT – ITIL	
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3 (SO)**
DS1 Definir y administrar los niveles de servicio	
DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio	OTRO PROCESO/CONTROL DE ITIL
DS1.2 Definición de Servicios	OTRO PROCESO/CONTROL DE ITIL
DS1.3 Acuerdos de Niveles de Servicio	OTRO PROCESO/CONTROL DE ITIL
DS1.4 Acuerdos de Niveles de Operación	OTRO PROCESO/CONTROL DE ITIL
DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	OTRO PROCESO/CONTROL DE ITIL
DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	OTRO PROCESO/CONTROL DE ITIL
DS2 Administrar los servicios de terceros	
DS2.1 Identificación de todas las relaciones con proveedores	OTRO PROCESO/CONTROL DE ITIL
DS2.2 Gestión de relaciones con proveedores	OTRO PROCESO/CONTROL DE ITIL
DS2.3 Administración de riesgos del proveedor	OTRO PROCESO/CONTROL DE ITIL

MAPEO COBIT – ITIL	
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3 (SO)**
DS2.4 Monitoreo del desempeño del proveedor	OTRO PROCESO/CONTROL DE ITIL
DS3 Administrar el desempeño y la capacidad	
DS3.1 Planeación del desempeño y la capacidad	OTRO PROCESO/CONTROL DE ITIL
DS3.2 Capacidad y desempeño actual	OTRO PROCESO/CONTROL DE ITIL
DS3.3 Capacidad y desempeño futuros	OTRO PROCESO/CONTROL DE ITIL
DS3.4 Disponibilidad de recursos de TI	OTRO PROCESO/CONTROL DE ITIL
DS3.5 Monitoreo y reportes	OTRO PROCESO/CONTROL DE ITIL
DS4 Garantizar la continuidad del servicio	
DS4.1 Marco de trabajo de continuidad de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.2 Planes de continuidad de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.3 Recursos críticos de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.4 Mantenimiento de plan de continuidad de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.5 Pruebas del plan de continuidad de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.6 Entrenamiento del plan de continuidad de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.7 Distribución del plan de continuidad de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.8 Recuperación y reanudación de los servicios de TI	OTRO PROCESO/CONTROL DE ITIL
DS4.9 Almacenamiento de respaldos fuera de las instalaciones	SO 5.2.3
DS5 Garantizar la seguridad de los sistemas	
DS5.1 Administración de la seguridad de TI	SO 5.13
DS5.2 Plan de seguridad de TI	OTRO PROCESO/CONTROL DE ITIL
DS5.3 Administración de Identidad	SO 4.5
DS5.4 Administración de cuentas de usuario	SO 4.5, SO 4.5.5.1, SO 4.5.5.2, SO 4.5.5.3, SO 4.5.5.4, SO 4.5.5.5, SO 4.5.5.6
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	SO 4.5.5.6, SO 5.13
DS5.6 Definición de incidentes de seguridad	OTRO PROCESO/CONTROL DE ITIL
DS5.7 Protección de la tecnología de seguridad	SO 5.4
DS5.8 Administración de llaves criptográficas	NO EXISTE PROCESO/CONTROL EN ITIL
DS5.9 Prevención, Detención y corrección de software malicioso	NO EXISTE PROCESO/CONTROL EN ITIL
DS5.10 Seguridad de la red	SO 5.5
DS5.11 Intercambio de datos sensitivos	NO EXISTE PROCESO/CONTROL EN ITIL
DS6 Identificar y asignar costos	
DS6.1 Definición de servicios	SO 4.6.7
DS6.2 Contabilización de TI	SO 4.6.7
DS6.3 Modelación de costos y cargos	SO 4.6.7
DS6.4 Mantenimiento del modelo de costos	SO 4.6.7
DS7 Educar y entrenar a los usuarios	
DS7.1 Identificación de Necesidades de Entrenamiento y Educación	SO 5.13, SO 5.14
DS7.2 Impartición de Entrenamiento y Educación	NO EXISTE PROCESO/CONTROL EN ITIL
DS7.3 Evaluación del Entrenamiento Recibido	NO EXISTE PROCESO/CONTROL EN ITIL
DS8 Administrar la mesa de servicio y los incidentes	
DS8.1 Mesa de servicio	SO 4.1, SO 4.2, SO 6.2
DS8.2 Registro de consultas de clientes	SO 4.1.5.3, SO 4.1.5.4, SO 4.1.5.5, SO 4.1.5.6, SO 4.1.5.7, SO 4.2.5.1, SO 4.2.5.2, SO 4.2.5.3, SO 4.2.5.4, SO 4.2.5.5, SO 4.3.5.1
DS8.3 Escalamiento de incidentes	SO 4.1.5.8, SO 4.2.5.6, SO 4.2.5.7, SO 4.2.5.8, SO 5.9
DS8.4 Cierre de incidentes	SO 4.1.5.10, SO 4.2.5.9
DS8.5 Análisis de tendencias	SO 4.1.5.9

MAPEO COBIT – ITIL	
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3 (SO)**
DS9 Administrar la configuración	
DS9.1 Repositorio y Línea Base de configuración	OTRO PROCESO/CONTROL DE ITIL
DS9.2 Identificación y Mantenimiento de elementos de configuración	OTRO PROCESO/CONTROL DE ITIL
DS9.3 Revisión de integridad de la configuración	SO 5.4, SO 7, SO 7.1.4
DS10 Administrar los problemas	
DS10.1 Identificación y clasificación de problemas	SO 4.4.5.1, SO 4.4.5.3, SO 4.4.5.4
DS10.2 Rastreo y resolución de problemas	SO 4.4.5.2, SO 4.4.5.5, SO 4.4.5.6, SO 4.4.5.7, SO 4.4.5.8
DS10.3 Cierre de problemas	SO 4.4.5.9, SO 4.4.5.10
DS10.4 Integración de las administraciones de cambios, configuración y problemas.	NO EXISTE PROCESO/CONTROL EN ITIL
DS11 Administrar los datos	
DS11.1 Requerimientos del Negocio para Administración de Datos	OTRO PROCESO/CONTROL DE ITIL
DS11.2 Acuerdos de Almacenamiento y Conservación	SO 5.6
DS11.3 Sistemas de Administración de Librerías de Medidas	NO EXISTE PROCESO/CONTROL EN ITIL
DS11.4 Eliminación	NO EXISTE PROCESO/CONTROL EN ITIL
DS11.5 Respaldo y Restauración	SO 5.2.3
DS11.6 Requerimientos de Seguridad para la Administración de Datos	OTRO PROCESO/CONTROL DE ITIL
DS12 Administrar el ambiente físico	
DS12.1 Selección y Diseño del Centro de Datos	NO EXISTE PROCESO/CONTROL EN ITIL
DS12.2 Medidas de Seguridad Física	SO Apéndice E
DS12.3 Acceso Físico	SO Apéndice E, SO Apéndice F
DS12.4 Protección Contra Factores Ambientales	SO Apéndice E
DS12.5 Administración de Instalaciones Físicas	SO 5.12
DS13 Administrar las operaciones	
DS13.1 Procedimientos e instrucciones de operación	SO 3.7, SO 5, SO APENDICE B
DS13.2 Programación de tareas	SO 5.3
DS13.3 Monitoreo de la infraestructura de TI	SO 4.1, SO 4.1.5.1, SO 4.1.5.9, SO 5.2.1
DS13.4 Documentos sensitivos y dispositivos de salida	SO 5.2.4
DS13.5 Mantenimiento preventivo del hardware	SO 5.3, SO 5.4

Tabla 16. Mapeo COBIT 4.1 - ITIL V3

Con el fin de visualizar el resultado del mapeo anterior, se considera que aquellos objetivos de control de COBIT en el dominio Entregar y Dar Soporte que le corresponden uno o varios procesos (SO) de ITIL, **"cubren"** el requerimiento de seguridad de la información (100%); caso contrario si le corresponde otro proceso/control de ITIL es parcial (50%) y si no existe proceso/control en ITIL es nulo (0%). Para tal efecto se muestra en la Figura 8 los resultados:

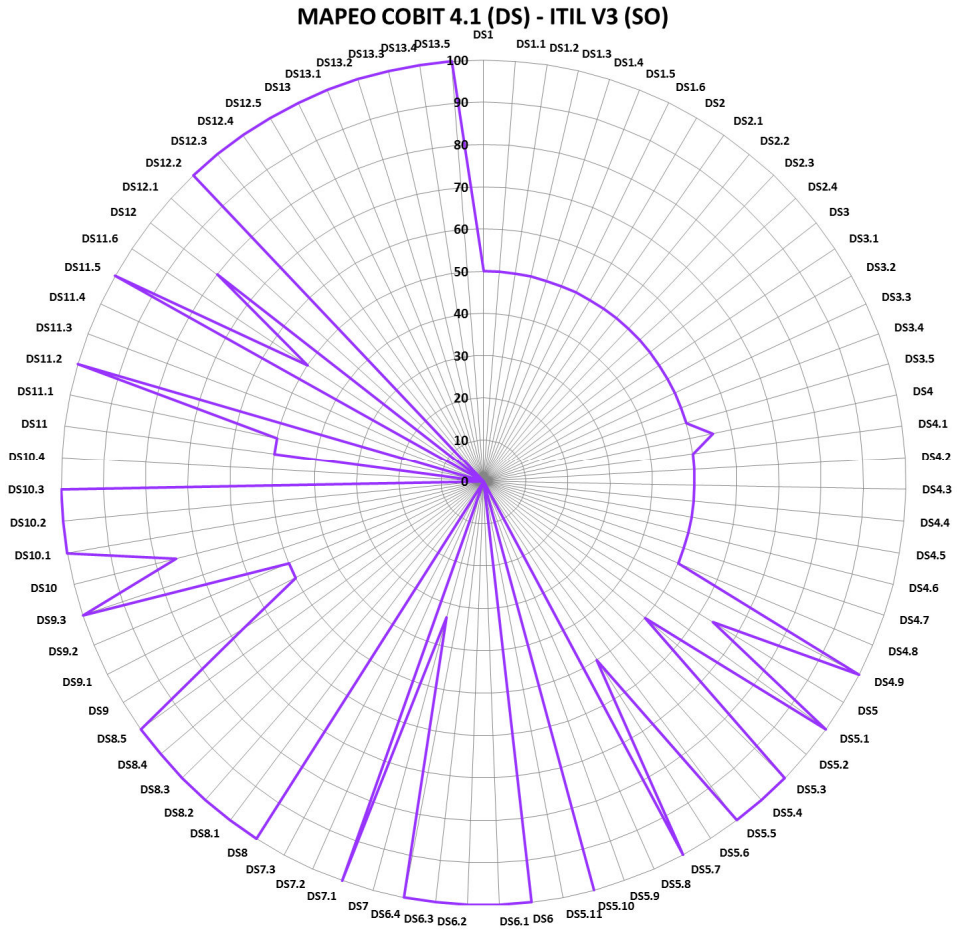


Figura 8. Mapeo COBIT 4.1 (DS) - ITIL V3 (SO)

A base a los resultados que se encuentra en el ANEXO 1 de este documento se puede concluir que ITIL en su proceso Operación del Servicio (SO), alcanza una cobertura del 67% respecto a los objetivos de control de COBIT 4.1 del dominio Entregar y Dar Soporte (DS).

La Figura 8 muestra el gráfico resultante de cobertura y correspondencia de los procesos de (SO) de ITIL respecto a los objetivos de control (DS) de COBIT 4.1.

Con el fin de tener una visión general y amplia de COBIT e ITIL, se procedió a calcular el promedio de los 13 objetivos de Control del dominio Entregar y Dar

Soporte (DS) de COBIT para asignar un valor cuantitativo como se muestra en la Figura 9:

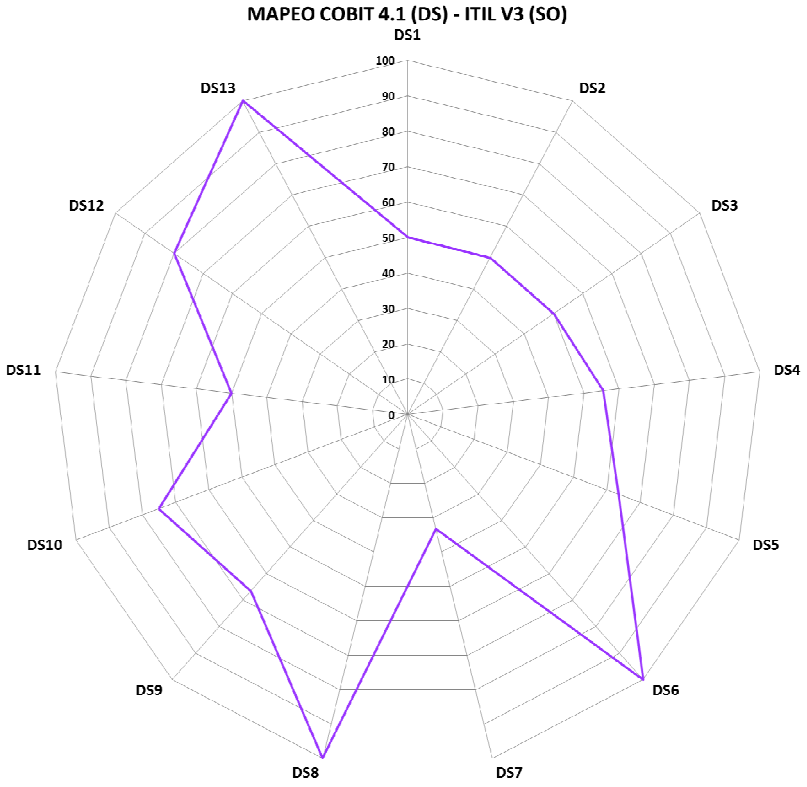


Figura 9. Cobertura de Mapeo COBIT 4.1 (DS) - ITIL V3 (SO)

A base de la Figura 9 podemos destacar que los objetivos de control de COBIT en el Dominio Entregar y Dar Soporte DS6 “Identificar y asignar costos”, DS8 “Administrar la mesa de servicio y los incidentes” y DS13 “Administrar las operaciones” cubren de manera integral los requerimientos de Seguridad de la información.

2.1.3 PASO 3. COBIT vs ISO 27001:

En este tercer paso se referenciará los objetivos de control de COBIT del Dominio Entregar y dar Soporte (DS) con los procesos de control de acceso de la ISO 27001 (A.11), con la característica de que este proceso se encuentra ***enfocado únicamente en la Seguridad de la Información,*** y de esta manera cumplir con los objetivos propuestos para esta investigación. Así mismo en la siguiente Tabla 17 se encuentra la descripción "OTRO DOMINIO/PROCESO DE LA ISO 27001", y se refiere a controles que cubren los procesos de COBIT pero que pertenecen a otra área de Seguridad.

Es conveniente mencionar que el mapeo de la Tabla 17 se basó en el artículo *"An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls", 2012.[4]*

MAPEO COBIT - ISO 27001	
COBIT 4.1 – ENTREGAR Y DAR SPORTE	**ISO 27001 (A.11)**
DS1 Definir y administrar los niveles de servicio	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS2 Administrar los servicios de terceros	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS3 Administrar el desempeño y la capacidad	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS4 Garantizar la continuidad del servicio	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS5 Garantizar la seguridad de los sistemas	A.11.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO A.11.2 ADMINISTRACIÓN DE ACCESOS DE USUARIOS A.11.3 RESPONSABILIDADES DE LOS USUARIOS A.11.4 CONTROL DE ACCESO A REDES A.11.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO A.11.6 CONTROL DE ACCESO A LA INFORMACIÓN Y A LAS APLICACIONES A.11.7 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO
DS6 Identificar y asignar costos	NO EXISTE CONTROL EN LA ISO 27001
DS7 Educar y entrenar a los usuarios	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS8 Administrar la mesa de servicio y los incidentes	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS9 Administrar la configuración	A.11.4 CONTROL DE ACCESO A REDES
DS10 Administrar los problemas	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS11 Administrar los datos	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS12 Administrar el ambiente físico	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS13 Administrar las operaciones	OTRO DOMINIO/PROCESO DE LA ISO 27001

Tabla 17. Mapeo COBIT 4.1 (DS) – ISO 27001 (A.11)

Con el fin de visualizar el resultado del mapeo anterior se considera que aquellos procesos de COBIT que le corresponden uno o varios controles de la ISO 27001, **"cubre"** el requerimiento de seguridad de la información (100%); caso contrario si le corresponde otro dominio/proceso de la ISO 27001 es parcial (50%) y si no existe control equivale a cero (0%).

Los resultados y cálculos respectivos se encuentran en el **ANEXO 2** de este documento.

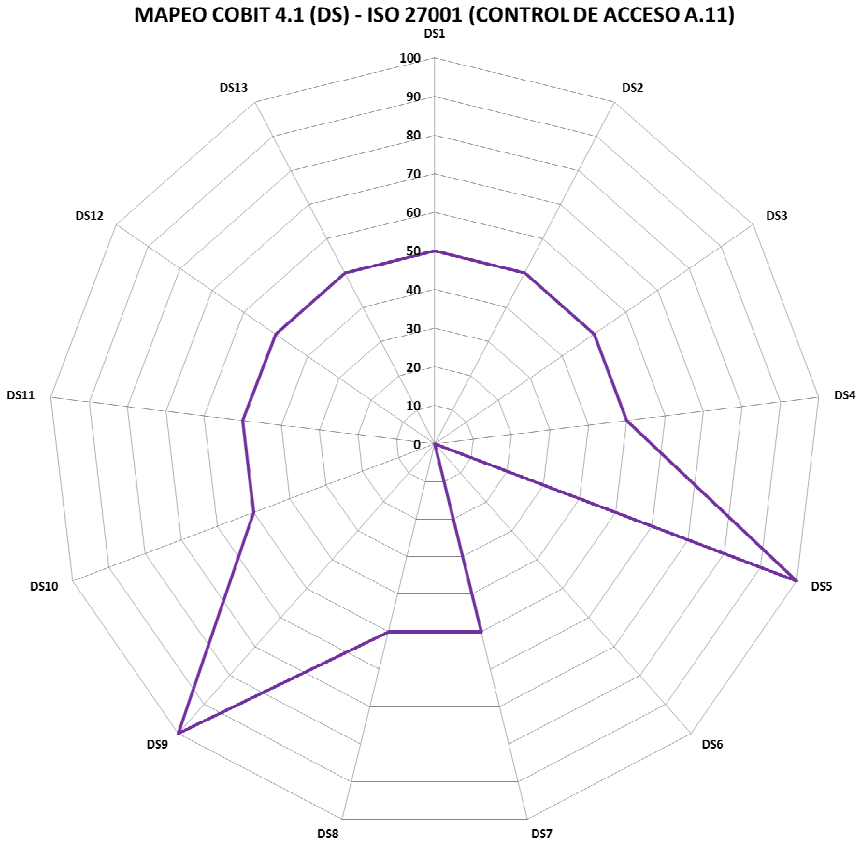


Figura 10. Mapeo COBIT 4.1 (DS) – ISO 27001 (A.11)

De la Figura 10 se puede observar que no existe un proceso de la ISO 27001 que cubra el objetivo de control DS6 “Identificar y asignar costos” de COBIT. Sin embargo ITIL cubre este objetivo de control en su actividad SO4.6.7 “Financial management for IT services (as operational activities)”. Así mismo podemos destacar que los Dominios DS9 “Administrar la configuración” y DS5 “Garantizar la seguridad de los sistemas” son cubiertos de manera Integral por la ISO 27001.

Por lo anterior y de forma general se puede concluir que la Norma ISO 27001 en su proceso Control de Acceso (A.11) alcanza una cobertura del 54% respecto a los objetivos de control del dominio Entregar y Dar Soporte (DS) de COBIT 4.1. [10]

2.1.4 PASO 4. INTEGRACIÓN:

En este punto se articulará los mapeos anteriores con el fin de unificar los resultados y presentar el mapeo de ITIL, COBIT e ISO 27001 de una forma integrada, ver Tabla 18.

MAPEO COBIT 4.1 – ITIL V3 – ISO 27001		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3 – OPERACIÓN DEL SERVICIO (S0)**	**ISO 27001 – CONTROL DE ACCESO (A.11)**
DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	OTRO DOMINIO/PROCESO DE ITIL	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS	OTRO DOMINIO/PROCESO DE ITIL	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS3 ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	OTRO DOMINIO/PROCESO DE ITIL	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS4 GARANTIZAR LA CONTINUIDAD DEL SERVICIO	SO 5.2.3, OTROS DOMINIOS/PROCESOS DE ITIL	OTRO DOMINIO/PROCESO DE LA ISO 27001

MAPEO COBIT 4.1 – ITIL V3 – ISO 27001		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3 – OPERACIÓN DEL SERVICIO (S0)**	**ISO 27001 – CONTROL DE ACCESO (A.11)**
DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	SO 5.13, SO 4.5, SO 4.5, SO 4.5.5.1, SO 4.5.5.2, SO 4.5.5.3, SO 4.5.5.4, SO 4.5.5.5, SO 4.5.5.6, SO 4.5.5.6, SO 5.13, SO 5.4, SO 5.5	A.11.1 REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO A.11.2 ADMINISTRACIÓN DE ACCESOS DE USUARIOS A.11.3 RESPONSABILIDADES DE LOS USUARIOS A.11.4 CONTROL DE ACCESO A REDES A.11.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO A.11.6 CONTROL DE ACCESO A LA INFORMACIÓN Y A LAS APLICACIONES A.11.7 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO
DS6 IDENTIFICAR Y ASIGNAR COSTOS	SO 4.6.7	NO EXISTE CONTROL EN LA ISO 27001
DS7 EDUCAR Y ENTRENAR A LOS USUARIOS	SO 5.13, SO 5.14	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS8 ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES	SO 4.1, SO 4.2, SO 6.2, SO 4.1.5.3, SO 4.1.5.4, SO 4.1.5.5, SO 4.1.5.6, SO 4.1.5.7, SO 4.2.5.1, SO 4.2.5.2, SO 4.2.5.3, SO 4.2.5.4, SO 4.2.5.5, SO 4.3.5.1, SO 4.1.5.8, SO 4.2.5.6, SO 4.2.5.7, SO 4.2.5.8, SO 5.9, SO 4.1.5.10, SO 4.2.5.9, SO 4.1.5.9	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS9 ADMINISTRAR LA CONFIGURACIÓN	SO 5.4, SO 7, SO 7.1.4, OTROS DOMINIOS/PROCESOS DE ITIL	A.11.4 CONTROL DE ACCESO A REDES
DS10 ADMINISTRAR LOS PROBLEMAS	SO 4.4.5.1, SO 4.4.5.3, SO 4.4.5.4, SO 4.4.5.2, SO 4.4.5.5, SO 4.4.5.6, SO 4.4.5.7, SO 4.4.5.8, SO 4.4.5.9, SO 4.4.5.10.	OTRO DOMINIO/PROCESO DE LA ISO 27001

MAPEO COBIT 4.1 – ITIL V3 – ISO 27001		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3 – OPERACIÓN DEL SERVICIO (S0)**	**ISO 27001 – CONTROL DE ACCESO (A.11)**
DS11 ADMINISTRAR LOS DATOS	SO 5.6. SO 5.2.3	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS12 ADMINISTRAR EL AMBIENTE FÍSICO	SO Apéndice E, SO Apéndice F	OTRO DOMINIO/PROCESO DE LA ISO 27001
DS13 ADMINISTRAR LAS OPERACIONES	SO 3.7, SO 5, SO APENDICE B, SO 5.3, SO 4.1, SO 4.1.5.1, SO 4.1.5.9, SO 5.2.1, SO 5.2.4, SO 5.3, SO 5.4	OTRO DOMINIO/PROCESO DE LA ISO 27001

Tabla 18. Mapeo COBIT 4.1 (DS) – ITIL V3 (SO) – ISO 27001 (A.11)

Tomando como referencia las Figuras 9 y 10 de este documento, resultado del mapeo entre COBIT e ITIL y COBIT e ISO 27001 respectivamente, a continuación se muestra en la Figura 11 un mapeo integral de estas 3 mejores prácticas:

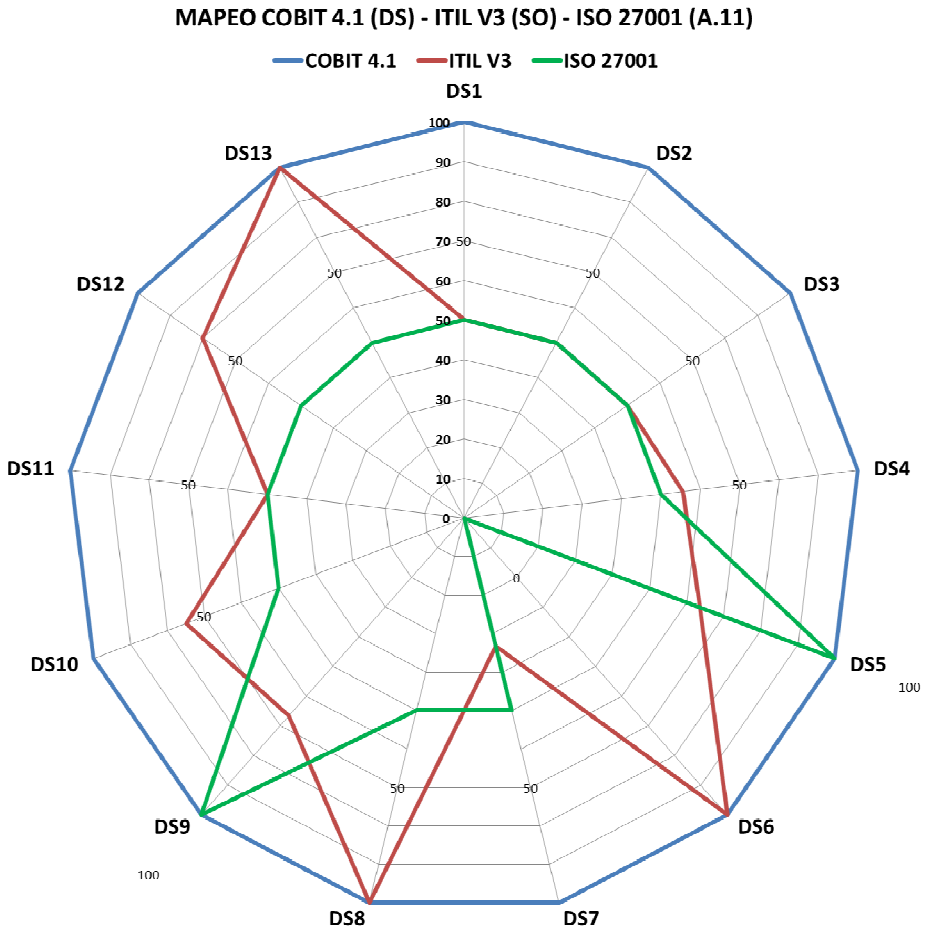


Figura 11. Mapeo COBIT 4.1 (DS) – ITIL V3 (SO) – ISO 27001 (A.11)

2.2. DETERMINACIÓN DE PROCEDIMIENTOS PARA EL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

En función del **mapeo** de COBIT, ITIL e ISO 27001 y fundamentándonos en **las características de la normativa** de estas tres mejores prácticas para que los servicios de TI fluyan de manera transparente, continúa y segura, es importante analizar la Figura 12 con el fin de determinar los procedimientos para el Gobierno de TI del Departamento Administración de Plataformas DSLAMs de la CNT E.P.

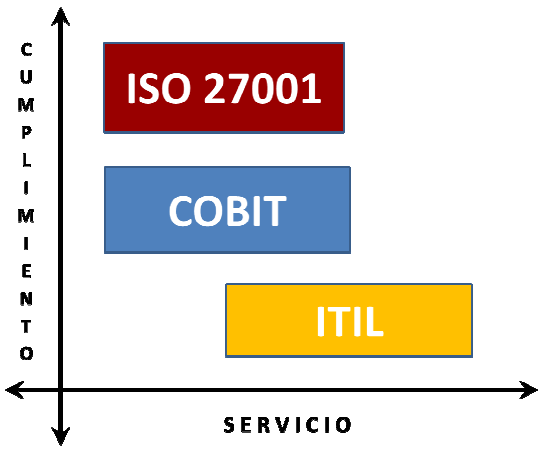


Figura 12. Cumplimiento vs. Servicio (ISO27001-COBIT-ITIL)
Fuente: Oliver Concepción - ¿Qué es COBIT?

Como se puede apreciar en la Figura 12, tenemos la representación de COBIT, ITIL e ISO 27001 en un cuadrante especificado por el CUMPLIMIENTO y el SERVICIO. Mientras mayor es el cumplimento, se puede utilizar la norma ISO 27001. Al mismo nivel se encuentra COBIT, y se lo puede implementar como un marco de control ya que convive de manera natural con las normas de la familia ISO 27000. ITIL se enfoca en el servicio, por lo tanto, se lo puede utilizar para garantizar la satisfacción del cliente y el buen uso de los recursos de tecnología. [7]

En resumen, la Norma ISO 27001 se fundamenta en el cumplimiento de sus procesos, COBIT responde al Gobierno de TI e ITIL habilita los servicios tecnológicos para su utilización efectiva y eficiente por parte de los usuarios o clientes.

La Figura 13 especifica el grado alcanzado por las 3 mejores prácticas objeto de este estudio, referenciado por medio del mapeo realizado en este documento.

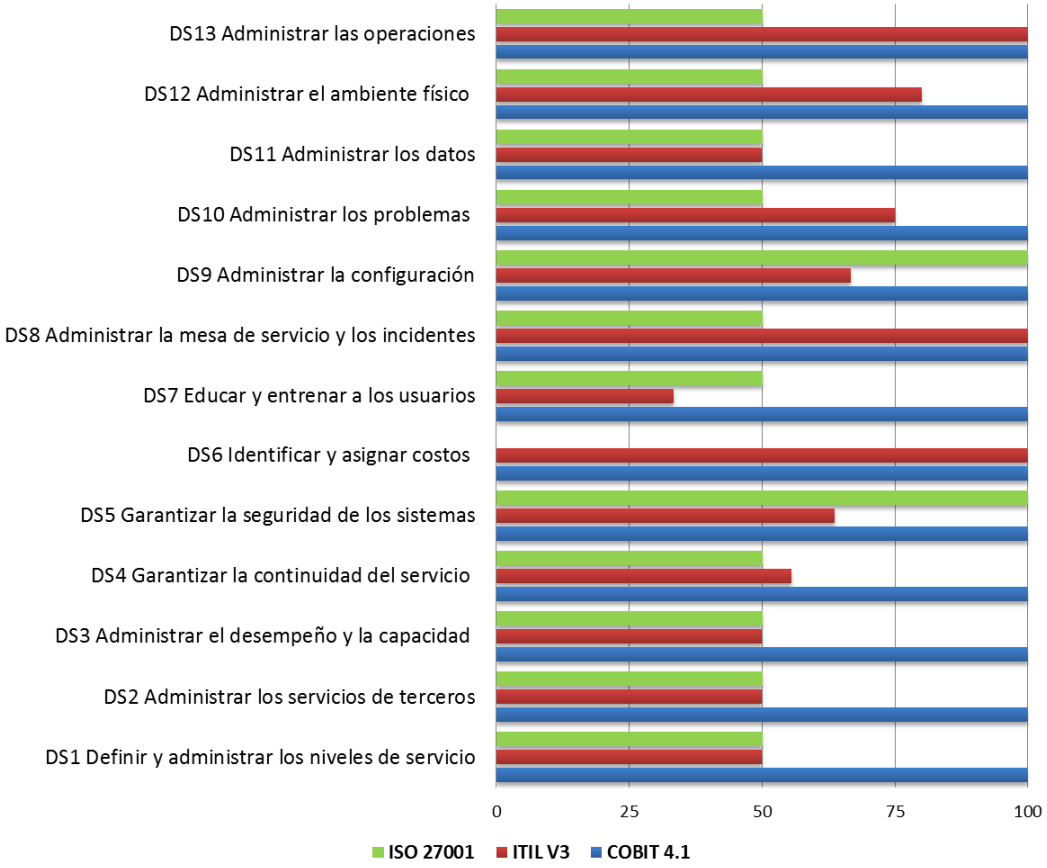


Figura 13. Grado y Mapeo COBIT 4.1 (DS) - ITIL (SO) - ISO 27001 (A.11)

En función de la prioridad de COBIT, ITIL e ISO 27001 especificado por el cumplimiento y el servicio de TI y tomando en cuenta únicamente los procesos de las mejores prácticas en donde su grado es igual al 100% y fundamentado en el mapeo de las mismas, los procedimientos para el Gobierno de TI objeto de esta investigación son los siguientes:

ID	PROCESO	PRIORIDAD	BASE	PROCEDIMIENTOS
1	DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	CUMPLIMIENTO	COBIT	DS1.1, DS1.2, DS1.3, DS1.4, DS1.5, DS1.6
2	ADMINISTRAR LOS SERVICIOS DE TERCEROS	CUMPLIMIENTO	COBIT	DS2.1, DS2.2, DS2.3, DS2.4
3	ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	CUMPLIMIENTO	COBIT	DS3.1, DS3.2, DS3.3, DS3.4, DS3.5
4	GARANTIZAR LA CONTINUIDAD DEL SERVICIO	CUMPLIMIENTO	COBIT	DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.7, DS4.8, DS4.9

ID	PROCESO	PRIORIDAD	BASE	PROCEDIMIENTOS
5	GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	CUMPLIMIENTO	ISO 27001	A.11.1, A.11.2, A.11.3, A.11.4, A.11.5, A.11.6, A.11.7
6	IDENTIFICAR Y ASIGNAR COSTOS	SERVICIO	ITIL	SO 4.6.7
7	EDUCAR Y ENTRENAR A LOS USUARIOS	CUMPLIMIENTO	COBIT	DS7.1, DS7.2, DS7.3
8	ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES	SERVICIO	ITIL	SO 4.1, SO 4.2, SO 6.2, SO 4.1.5.3, SO 4.1.5.4, SO 4.1.5.5, SO 4.1.5.6, SO 4.1.5.7, SO 4.2.5.1, SO 4.2.5.2, SO 4.2.5.3, SO 4.2.5.4, SO 4.2.5.5, SO 4.3.5.1, SO 4.1.5.8, SO 4.2.5.6, SO 4.2.5.7, SO 4.2.5.8, SO 5.9, SO 4.1.5.10, SO 4.2.5.9, SO 4.1.5.9
9	ADMINISTRAR LA CONFIGURACIÓN	CUMPLIMIENTO	ISO 27001	A.11.4
10	ADMINISTRAR LOS PROBLEMAS	CUMPLIMIENTO	COBIT	DS10.1, DS10.2, DS10.3, DS10.4
11	ADMINISTRAR LOS DATOS	CUMPLIMIENTO	COBIT	DS11.1, DS11.2, DS11.3, DS11.4, DS11.5, DS11.6
12	ADMINISTRAR EL AMBIENTE FÍSICO	CUMPLIMIENTO	COBIT	DS12.1, DS12.2, DS12.3, DS12.4, DS12.5
13	ADMINISTRAR LAS OPERACIONES	SERVICIO	ITIL	SO 3.7, SO 5, SO APENDICE B, SO 5.3, SO 4.1, SO 4.1.5.1, SO 4.1.5.9, SO 5.2.1, SO 5.2.4, SO 5.3, SO 5.4

Tabla 19. Determinación de Procedimientos para el Gobierno de TI para el Departamento de Administración Plataformas DSLAMS de la CNT E.P

2.3. LA PROPUESTA DE GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN BASADO EN COBIT, ITIL E ISO-27001.

La propuesta de Gobierno de Tecnologías de la Información, se basa en la guía publicada por el IT Governance Institute denominada "Board Briefing on TI Governance" desarrollado por Deloite&Touch, "IT Governance Institute, COBIT 4.1 en español" e "IT_Governance_Implementation_Guide.4.1", debido a la importancia de identificar las estrategias de TI y las estructuras que unen los procesos de TI con los recursos de TI, para cumplir con los objetivos de la empresa concentrándose en obtener el valor de TI, gestión de riesgos, asignación de responsables y medición de resultados.[5]

Este proceso que se muestra en la Figura 14 indica "comienza a establecer los objetivos para la TI de la empresa, proporcionando la dirección inicial. A partir de ahí se establece un circuito continuo de desempeño que se mide y compara con los objetivos, lo que da como resultado una nueva dirección en las actividades, cuando sea necesario, y el cambio de objetivos, cuando sea conveniente. Mientras que los objetivos son principalmente responsabilidad de la dirección y las medidas de desempeño de la administración, es evidente que deben desarrollarse en armonía, de modo que los objetivos sean realistas y las medidas representen correctamente los objetivos." [1] [5]

[1] ISACA, Board Briefing on IT Governance, Pág 12

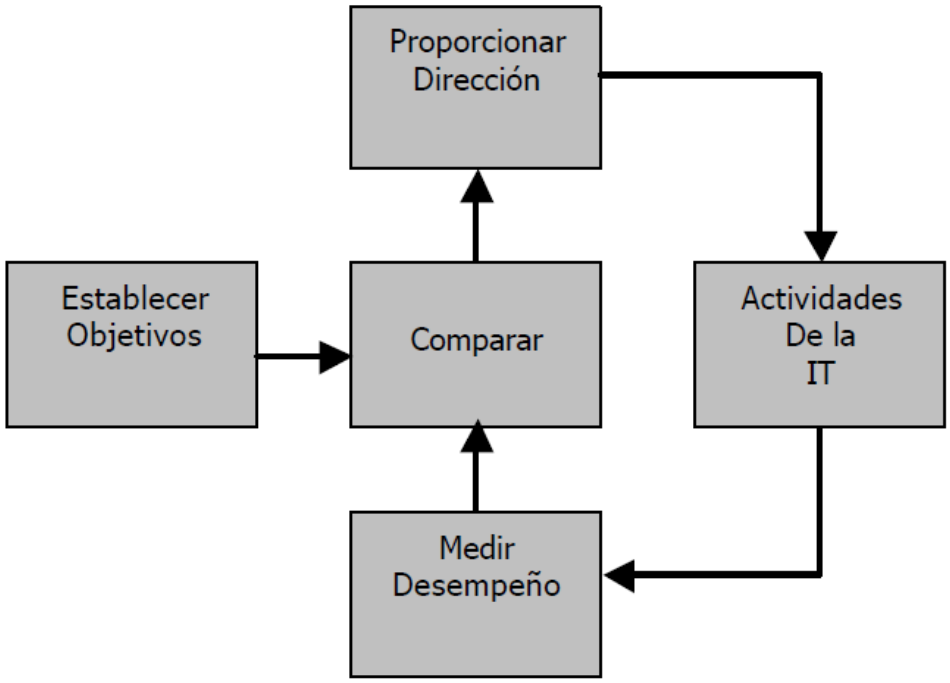


Figura 14 Hoja de ruta para el gobierno de TI
Fuente: Board Briefing on TI Governance Español Pág 12

"Es importante enfocar la función de TI en la producción de beneficios al incrementar la automatización y hacer a la empresa más eficaz al reducir los costos y hacer que toda la organización sea más eficiente; y en manejar los riesgos (seguridad, confianza y cumplimiento de las normas)." [2][5]

2.3.1 ALINEACIÓN ESTRATÉGICA DE LAS TI

"La alineación de TI ha sido un sinónimo de su estrategia, esto es, la estrategia de la TI sustenta la estrategia de la compañía, la alineación comprende más que la integración estratégica entre la futura organización de la TI y la futura organización de la empresa. También implica que las operaciones de la TI estén alineadas con las operaciones empresariales en curso, Figura 15" [3][5]

[2] ISACA, Board Briefing on IT Governance, Pág 12
[3] ISACA, Board Briefing on IT Governance, Pág 20

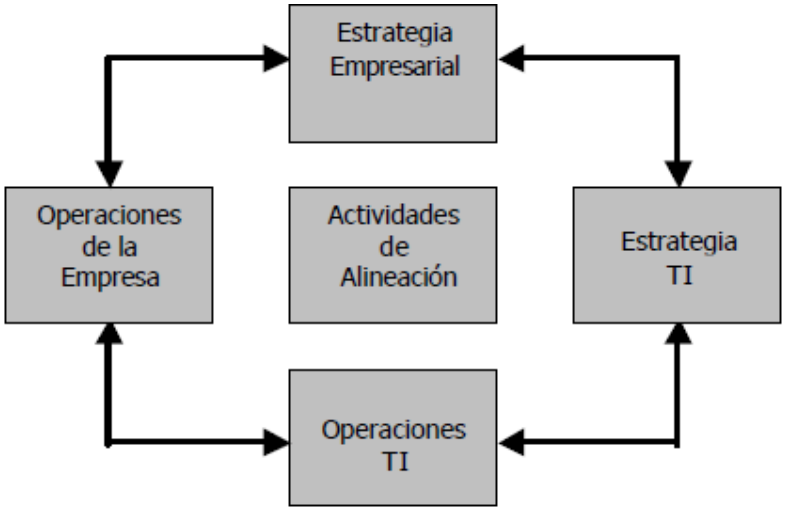


Figura 15 Operaciones TI alineadas con operaciones empresariales
Fuente: ISACA, Board Briefing on IT Governance, Pág 20

La dirección debe llevar la alineación del negocio como:

- Asegurar que la estrategia de la TI esté alineada con la estrategia del negocio.
- Asegurar que la TI preste un servicio según la estrategia.
- Tomar decisiones acerca del enfoque de los recursos de la TI.

2.3.2 VALOR DERIVADO DE TI

Los principios básicos del valor de TI son: entregar a tiempo, dentro del presupuesto y con los beneficios prometidos; además para esta propuesta se requiere levantar a tiempo los servicios en caso de una interrupción de los equipos del Departamento Administración Plataformas DSLAMs, tanto para los clientes internos como para clientes externos.

"Para tener éxito, la empresa necesita estar consciente de distintos contextos estratégicos que requieren diferentes indicadores de valor. Tendrán que asignar

responsabilidad explícita en la organización para cada medida de evaluación y establecer las medidas del valor entre el negocio y la TI." [4][5]

El Departamento Administración Plataformas DSLAMs para la entrega de los servicios se basa en procesos y políticas, por lo que es necesario verificar sus aplicaciones según sea el caso, por ende es imprescindible que los ingenieros estén capacitados para el monitoreo de 24x7x365 días del año y atender las emergencias que se presenten en cualquier momento.

Para cumplir con este objetivo es necesario brindar las capacitaciones en los sistemas de gestión, equipos y procedimientos del Departamento Administración Plataformas DSLAMs, con esto estaríamos alcanzando la estabilidad de los servicios que son responsabilidad del Departamento APD y la CNT E.P.

2.3.3 MEDICIÓN DEL DESEMPEÑO

"TI hace más que proporcionar información para obtener una imagen global acerca de donde se encuentra la organización y hacia donde va. También permite y mantiene soluciones para las metas actuales establecidas en las dimensiones financieras (manejo de los recursos empresariales), del cliente (manejo de la relación con el cliente), del proceso (internet y herramientas del circuito de producción) y aprendizaje (manejo del conocimiento)."[5][5]

La medición del desempeño y la identificación del nivel de madurez del Departamento Administración Plataformas DSLAMs de la CNT E.P se basan en los criterios ilustrados en la Figura 16.

"Las Empresas necesitan evaluar que tan bien se están desempeñando en la actualidad y ser capaces de identificar donde y como pueden mejorar. Esto se aplica tanto al proceso de operación de la TI en sí, como a todos los procedimientos que necesitan manejarse dentro de la TI". [5]

[4] ISACA, Board Briefing on IT Governance, Pág 23
[5] ISACA, Board Briefing on IT Governance, Pág 24

El uso de modelos de madurez simplifica enormemente esta tarea y proporciona un enfoque pragmático y estructurado para medir qué tan bien desarrollados están sus procesos según una escala consistente y fácil de entender; a continuación la Figura 16 ilustra el modelo de madurez del manejo de la TI. [5]

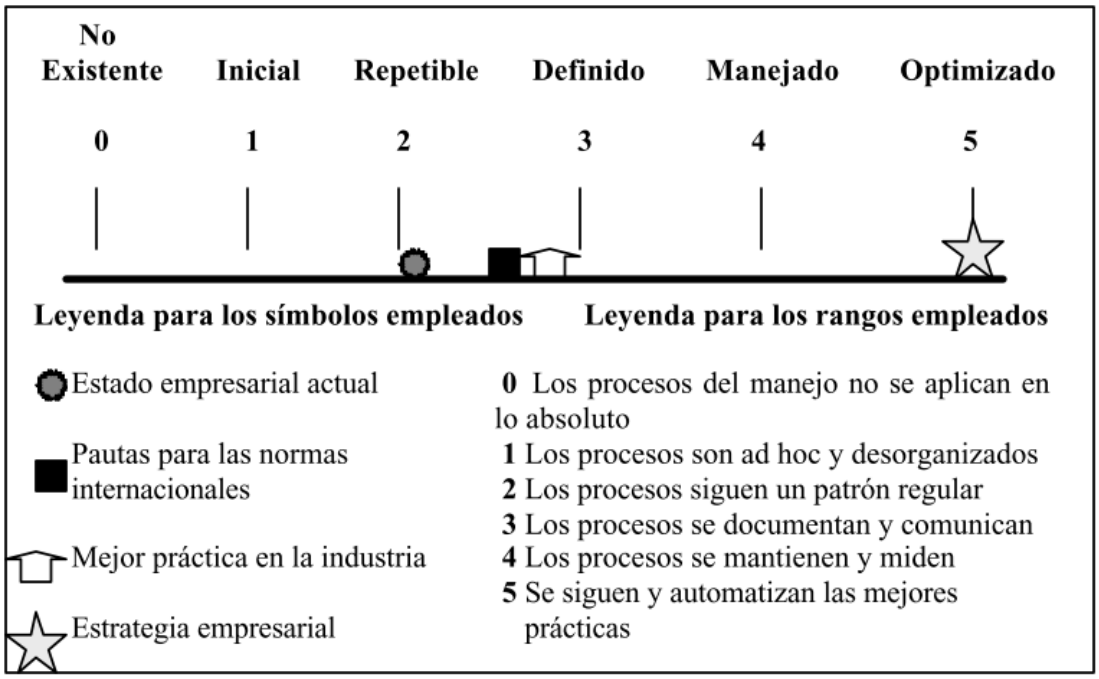


Figura 16 Modelo de Madurez del Manejo de la TI
Fuente: Board Briefing on TI Governance Español Pág 42

0 No existente. Existe una completa falta de procesos en el manejo de la TI que sea reconocible.

1 Inicial/ad hoc. La organización ha reconocido que los asuntos relacionados con el manejo de la TI existen y es necesario atenderlos.

2 Repetible pero Intuitivo. Existe conciencia de los objetivos del manejo de la TI, los gerentes desarrollan y aplican las prácticas.

3 Definido. La necesidad de actuar con respecto al manejo de la TI se comprende y acepta. Se desarrolla una base de indicadores del manejo de la TI, donde los vínculos entre las medidas del resultado y los conductores del

desempeño se definen, documentan e integran en los procesos de monitoreo y planeación estratégica y operativa

4 Manejado y Medible. Existe una total comprensión de los asuntos del manejo de la TI en todos sus niveles, con apoyo de la capacitación formal. Existe un claro entendimiento acerca de quién es el cliente y las responsabilidades se definen y verifican por medio de acuerdos sobre el nivel de servicio.

5. Optimizado. Existe una comprensión formal y con miras a futuro de los problemas y soluciones relacionados con la TI. La capacitación y la comunicación se apoyan en conceptos y técnicas de punta. Los procesos han sido refinados hasta alcanzar el nivel de las mejores prácticas externas, con base en resultados de mejoramiento continuo y modelos de madurez de otras organizaciones."[6][5]

2.3.4 MANEJO DE RIESGOS

"Las empresas dependen de la infraestructura de la TI y se encuentran en consecuente vulnerabilidad a nuevos riesgos tecnológicos.

Los mandos administrativos deben tomar conciencia que la responsabilidad final del manejo de los riesgos yace en la dirección."[7][5]

El método consta de las siguientes fases:

- Establecimiento de la Metodología de TI
- Identificación de Riesgos de TI
- Análisis del Riesgo de TI
- Evaluación y Priorización de Riesgos de TI
- Tratamiento de Riesgos de TI (Controles Definitivos)

[6] ISACA, Board Briefing on IT Governance, Pág 30,31
[7] ISACA, Board Briefing on IT Governance, Pág 26

2.3.5 DESARROLLO DE LA PROPUESTA DE GOBIERNO DE TI.

El desarrollo de la propuesta de Gobierno de Tecnologías de la Información para el Departamento Administración Plataformas DSLAMs se realizara en base al mapa de ruta indicado en la Figura 17 el cual establece cinco grupos de actividades: Identificar Necesidades, Visualizar la Solución, Planear la Solución, Implementar la Solución y Volver Operativa la Solución.

A continuación, en la Figura 17 se indica el mapa de ruta del Gobierno de TI:[6]

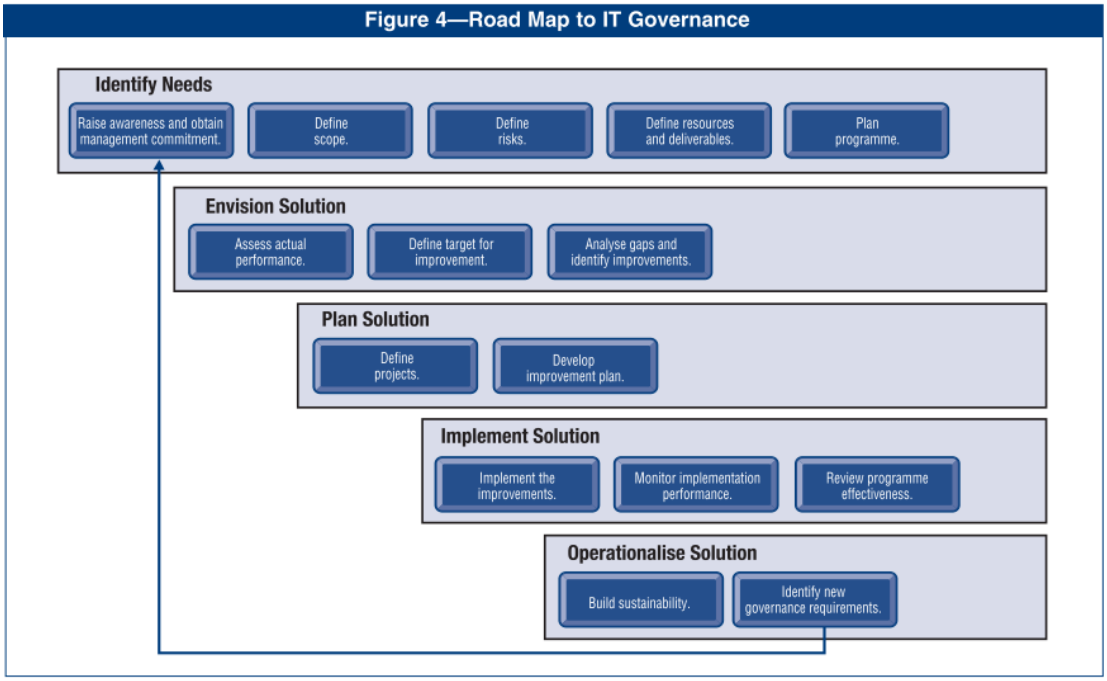


Figura 17 Mapa de Ruta del Gobierno de TI
Fuente: IT Governance Implementation Guide 4.1 Pág. 10

2.3.5.1 IDENTIFICAR NECESIDADES

Para identificar las necesidades del Gobierno de TI se requiere seguir los siguientes pasos: Despertar Conciencia y Obtener Compromiso, Definir el Alcance, Definir los Riesgos, Definir Recursos y Entregables y Planear el Programa.

- **DESPERTAR CONCIENCIA Y OBTENER COMPROMISO DE LA ADMINISTRACIÓN.**

Para despertar conciencia y obtener compromiso de la administración es necesario que el nivel directivo del Departamento APD de la CNT E.P., promueva medidas efectivas y oportunas encaminadas a tratar puntos administrativos y operativos.

ADMINISTRATIVO	OPERATIVO
Procesos de capacitaciones	Buen nivel de manejo de los sistemas gestión / DSLAM y procedimientos.
Presupuestos para equipamiento (Proyectos)	Instalación de nuevo equipamiento para brindar servicio a zonas aledañas
Estándares y Procedimientos	Ejecución y monitoreo en las plataformas.
Índices e indicadores	Operar y mantener las plataformas que brindan el servicio.
Manejo estructural organizacional	Delegación de funciones

Tabla 20 Puntos Administrativos y Operativos

Por lo tanto para el personal del Departamento Administración Plataformas DSLAMs es necesario levantar procedimientos para las funciones encargadas tanto a nivel administrativo como operativo; como se puede observar en la Tabla 20, se fomenta la cultura y comunicación de todos los involucrados con la finalidad de proporcionar la responsabilidad de cumplir y mantener activos los servicios.

Por consiguiente, son necesarias las políticas corporativas, la dirección y la administración ejecutiva con la finalidad de proporcionar el liderazgo en los procesos y estructuras del departamento, para asegurar que las TI sustente y amplíe los objetivos y estrategias del Departamento APD.

- **DEFINIR EL ALCANCE**

A continuación se realizara un análisis y mapeo de las Metas de Negocio, Metas de TI y Procesos para elaborar la propuesta del Gobierno de TI para el Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P; para este desarrollo se sigue el siguiente orden de procesos: Identificar las Metas de Negocio, Metas de TI y Procesos TI del Departamento APD, Identificar e Implementar la solución. [2]

- **IDENTIFICACIÓN Y MAPEO DE LAS METAS DE NEGOCIO Y METAS DE TI DEL DEPARTAMENTO ADMINISTRACIÓN PLATAFORMAS DSLAMs.**

Para efecto de esta investigación se realizará la identificación de las metas de negocio (MN), metas de TI (MT) y procesos TI (PT) del Departamento Administración Plataformas DSLAMs de la CNT EP. A continuación en la Tabla 21 se presenta las metas de negocio.[2]

METAS DE NEGOCIO (MN)	
MN1	Ejecutar acciones de mantenimiento preventivo, correctivo y emergente de los equipos DSLAM, según los procedimientos establecidos por la Gerencia de Operación y Mantenimiento, en coordinación con las diferentes áreas de O&M.
MN2	Ejecutar órdenes de trabajo para implementación, ampliación de infraestructura, migración de servicios y/o equipos, reparaciones, descongestión, cambio y/o actualización de hardware y software de equipos que conforman la red DSLAM.
MN3	Elaborar los planes de operación y mantenimiento, para la mejora continua de servicios, equipos y recursos de los DSLAM, con las diferentes áreas de la Gerencia de Operación & Mantenimiento y los grupos O&M Provinciales de ser el caso en base a la normativa y manuales correspondientes a cada sistema.
MN4	Elaborar órdenes de trabajo para rutinas de operación y mantenimiento de los equipos DSLAMs que conforman la red a nivel nacional.
MN5	Asegurar el aprovisionamiento, activación de servicios masivos /corporativos en los equipos de la red DSLAM.

METAS DE NEGOCIO (MN)	
MN6	Soporte de nivel 2 y 3 sobre equipos y servicios masivos/corporativos de telefonía, internet, datos e IPTV de los DSLAM.
MN7	Ejecutar rutinas de monitoreo de todos los elementos y equipos que conforman la red de los DSLAM para garantizar la disponibilidad.
MN8	Administrar servidores, sistemas de gestión, usuarios y políticas de accesos de los equipos que conforman la red DSLAMs que se encuentran en operación.
MN9	Actualizar el inventario de equipamiento de los DSLAM en el sistema OPEN
MN10	Atender y dar seguimiento a las incidencias reportadas por el NOC
MN11	Participar en calificación de ofertas en procesos de compra de diferentes proyectos de los DSLAMs y sistemas de gestión.
MN12	Fiscalizar contratos de proyectos concernientes a las plataformas DSLAM
MN13	Realizar pruebas de aceptación y concepto de equipos de ampliaciones y nueva infraestructura sobre la red DSLAM.

Tabla 21 Metas del Negocio Departamento Administración Plataformas DSLAM

En la Tabla 22 se presenta las Metas de TI del Departamento Administración Plataformas DSLAMs.[2]

METAS DE TI (MT)	
MT1	Identificar requerimientos del servicio sobre las características de las necesidades de los clientes y requerimientos del negocio.
MT2	Establecer SLAs (Acuerdos de niveles de servicio) para un servicio eficiente tomando en cuenta y cumpliendo los niveles de servicio.
MT3	Formalizar acuerdos internos (personal Departamento APD) y externos (Proveedores y clientes) cumpliendo los procedimientos establecidos.

METAS DE TI (MT)	
MT4	Establecer SLOs (Acuerdos de niveles de operación) con el fin de cumplir los niveles de operación para que expliquen cómo serán entregados técnicamente los SLAs y garantizar que la infraestructura de TI pueda resistir y recuperarse de errores y fallas.
MT5	Mitigar el impacto producido en el caso de una interrupción de los servicios de TI para la continuidad del negocio.
MT6	Brindar satisfacción a los usuarios finales ofreciendo niveles de servicio acorde a los estándares y procedimientos de la CNT E.P.
MT7	Mantener la comunicación entre el Departamento APD y Recursos Humanos para asignar cargos (estructura organizacional de la CNT E.P.) y capacitación en función de la necesidad del personal, avance tecnológico e instalación de nuevos equipos.
MT8	Definir políticas y estándares de seguridad en el Departamento APD para detección y resolución de incidentes en el caso de que existan.
MT9	Usar efectivamente los sistemas de gestión del Departamento APD y la información que generan, mediante la instalación, operación, monitoreo y definición de procedimientos para la configuración y resolución de incidentes y problemas de la infraestructura, ofreciendo de esta manera integridad de la información y disponibilidad de los servicios.
MT10	Mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar los problemas reportados de los elementos de TI a nivel de hardware, sistemas operativos, bases de datos y aplicaciones.
MT11	Garantizar los respaldos y recuperación de la información almacenándolos en sitios seguros que permitan mantener la integridad, exactitud, disponibilidad y protección de los datos.
MT12	Proporcionar un buen clima laboral para el personal y un buen ambiente físico para proteger los equipos DSLAM, infraestructura, comunicaciones y sistemas de gestión (servidores), utilizando medidas de control y seguridad en las instalaciones.
MT13	Establecer e implementar procedimientos de mantenimiento oportunos con el personal del Departamento APD y los proveedores para que se pueda reducir la frecuencia de impacto o fallas en la infraestructura.

Tabla 22 Metas de TI Departamento Administración Plataformas DSLAMs

A continuación el Mapeo de las Metas de Negocio con las Metas de TI

Para el mapeo de las metas se ha identificado las Metas de Negocio en la Tabla 21, Metas de TI en la Tabla 22, para este efecto se procederá a realizar el mapeo de las Metas Negocio y Metas de TI Tabla 23 con la finalidad de presentar el grado de cumplimiento para la Propuesta de Gobierno de TI.

MAPEO DE LAS METAS DE NEGOCIO (MN) Y LAS METAS DE TI (MT)								
ID	**METAS DE NEGOCIO (MN)**	**METAS DE TI (MT)**						
MN1	Ejecutar acciones de mantenimiento preventivo, correctivo y emergente de los equipos DSLAM, según los procedimientos establecidos por la Gerencia de Operación y Mantenimiento, en coordinación con las diferentes áreas de O&M.	MT3	MT4	MT10	MT11	MT13		
MN2	Ejecutar órdenes de trabajo para implementación, ampliación de infraestructura, migración de servicios y/o equipos, reparaciones, descongestión, cambio y/o actualización de hardware y software de equipos que conforman la red DSLAM.	MT1	MT4	MT6	MT9	MT13		
MN 3	Elaborar los planes de operación y mantenimiento, para la mejora continua de servicios, equipos y recursos de los DSLAM, con las diferentes áreas de la Gerencia de Operación & Mantenimiento y los grupos O&M Provinciales de ser el caso en base a la normativa y manuales correspondientes a cada sistema.	MT1	MT3	MT4	MT5	MT6	MT10	MT13
MN 4	Ejecutar todas las tareas en el							

MAPEO DE LAS METAS DE NEGOCIO (MN) Y LAS METAS DE TI (MT)								
ID	**METAS DE NEGOCIO (MN)**	**METAS DE TI (MT)**						
	ámbito de su competencia con respecto a la implantación del nuevo sistema operacional y transaccional.	MT1	MT7	MT8	MT11	MT12		
MN 5	Asegurar el aprovisionamiento, activación de servicios masivos /corporativos en los equipos de la red DSLAM.	MT1	MT3	MT5	MT6	MT8	MT9	
MN 6	Soporte de nivel 2 y 3 sobre equipos y servicios masivos/corporativos de telefonía, internet, datos e IPTV de los DSLAM.	MT1	MT5	MT6	MT11	MT12		
MN 7	Ejecutar rutinas de monitoreo de todos los elementos y equipos que conforman la red de los DSLAM para garantizar la disponibilidad.	MT3	MT8	MT9	MT10	MT11	MT13	
MN 8	Administrar servidores, sistemas de gestión, usuarios y políticas de accesos de los equipos que conforman la red DSLAMs que se encuentran en operación.	MT4	MT8	MT9	MT12			
MN 9	Actualizar el inventario de equipamiento de los DSLAM en el sistema OPEN.	MT3	MT10	MT11				
MN 10	Ejecutar Thoubleshooting Atender y dar seguimiento a las incidencias reportadas por el NOC, Call Center, áreas operativas y grupos de O&M Provinciales.	MT4	MT5	MT8	MT12	MT13		
MN 11	Participar en calificación de ofertas en procesos de compra de diferentes proyectos de los DSLAMs y sistemas de gestión.	MT1	MT2					

MAPEO DE LAS METAS DE NEGOCIO (MN) Y LAS METAS DE TI (MT)								
ID	**METAS DE NEGOCIO (MN)**	**METAS DE TI (MT)**						
MN 12	Fiscalizar contratos de proyectos concernientes a las plataformas DSLAM.	MT2	MT4					
MN 13	Realizar pruebas de aceptación y concepto de equipos de ampliaciones y nueva infraestructura sobre la red DSLAM.	MT1	MT5	MT10	MT11			

Tabla 23 Mapeo de las Metas de Negocio y las Metas de TI

- **MAPEO DE LAS METAS DE TI CON LOS PROCESOS DE TI**

En la Tabla 24 se presenta los Procesos TI (PT), basado en las mejoras prácticas las cuales son fundamentadas en el mapeo COBIT, ITIL e ISO 27001.

PROCESOS DE TI		
NOMBRE		**PROCEDIMIENTO**
PT1	DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	DS1.1, DS1.2, DS1.3, DS1.4, DS1.5, DS1.6
PT2	ADMINISTRAR LOS SERVICIOS DE TERCEROS	DS2.1, DS2.2, DS2.3, DS2.4
PT3	ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	DS3.1, DS3.2, DS3.3, DS3.4, DS3.5
PT4	GARANTIZAR LA CONTINUIDAD DEL SERVICIO	DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.7, DS4.8, DS4.9
PT5	GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	A.11.1, A.11.2, A.11.3, A.11.4, A.11.5, A.11.6,

PROCESOS DE TI		
		A.11.7
PT6	IDENTIFICAR Y ASIGNAR COSTOS	SO 4.6.7
PT7	EDUCAR Y ENTRENAR A LOS USUARIOS	DS7.1, DS7.2, DS7.3
PT8	ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES	SO 4.1, SO 4.2, SO 6.2, SO 4.1.5.3, SO 4.1.5.4, SO 4.1.5.5, SO 4.1.5.6, SO 4.1.5.7, SO 4.2.5.1, SO 4.2.5.2, SO 4.2.5.3, SO 4.2.5.4, SO 4.2.5.5, SO 4.3.5.1, SO 4.1.5.8, SO 4.2.5.6, SO 4.2.5.7, SO 4.2.5.8, SO 5.9, SO 4.1.5.10, SO 4.2.5.9, SO 4.1.5.9
PT9	ADMINISTRAR LA CONFIGURACIÓN	A.11.4
PT10	ADMINISTRAR LOS PROBLEMAS	DS10.1, DS10.2, DS10.3, DS10.4
PT11	ADMINISTRAR LOS DATOS	DS11.1, DS11.2, DS11.3, DS11.4, DS11.5, DS11.6
PT12	ADMINISTRAR EL AMBIENTE FÍSICO	DS12.1, DS12.2, DS12.3, DS12.4, DS12.5
PT13	ADMINISTRAR LAS OPERACIONES	SO 3.7, SO 5, SO APENDICE B, SO 5.3, SO 4.1, SO 4.1.5.1, SO 4.1.5.9, SO 5.2.1, SO 5.2.4, SO 5.3, SO 5.4

Tabla 24 Procesos de TI DS: COBT – A: ISO27001 – SO: ITIL

A continuación en la Tabla 25 se procederá con el mapeo de las Metas de TI (MT) Tabla 22 y Procesos de TI (PT) Tabla 24, en base a un estudio de campo con el personal del Departamento Administración Plataformas DSLAMs, basado en el documento IT Governance Institute Cobit 4.1 Página 170.[6]

Para identificar los criterios de información se consideran los siguientes parámetros: [6]

P = (Primario)

S = (Secundario)

MAPEO DE LAS METAS DE TI(MT) A PROCESOS DE TI(PT)									CRITERIOS DE INFORMACIÓN						
ID	METAS DE TI (MT)	PROCESOS DE TI (PT)							EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIDENCIALIDAD
MT1	Identificar requerimientos del servicio sobre las características de las necesidades de los clientes y requerimientos del negocio.	PT1	PT3						P	P		S	S		
MT2	Establecer SLAs (Acuerdos de niveles de servicio) para un servicio eficiente tomando en cuenta y cumpliendo los niveles de servicio.	PT1	PT2	PT7	PT8	PT10	PT13		P	P		S	S		
MT3	Formalizar acuerdos internos (personal APD) y externos (Proveedores y clientes) cumpliendo los procedimientos establecidos.	PT3	PT4	PT5	PT7	PT10	PT11	PT12	PT13		S		P			S

MT4	Establecer SLOs (Acuerdos de niveles de operación) con el fin de cumplir los niveles de operación para que expliquen cómo serán entregados técnicamente los SLAs y garantizar que la infraestructura de TI pueda resistir y recuperarse de errores y fallas.	PT2	PT5	PT8	PT9	PT10	PT13			P	P	S	S	S	S	S
MT5	Mitigar el impacto producido en el caso de una interrupción de los servicios de TI para la continuidad del negocio.	PT1	PT2	PT6	PT10	PT13				P	P				S	S
MT6	Brindar satisfacción a los usuarios finales ofreciendo niveles de servicio acorde a los estándares y procedimientos de la CNT E.P.	PT5	PT9	PT7	PT12					S	S	P	P	P	S	S
MT7	Mantener la comunicación entre el Departamento APD y Recursos Humanos para asignar cargos (estructura organizacional de la CNT E.P.) y capacitación en función de la necesidad del personal, avance tecnológico e instalación de nuevos equipos.	PT7	PT8							P	S					
MT8	Definir políticas y estándares															

	de seguridad en el Departamento APD para detección y resolución de incidentes en el caso de que existan.	PT5	PT11	PT12								P	P	S	S	S
MT9	Usar efectivamente los sistemas de gestión del Departamento APD y la información que generan, mediante la instalación, operación, monitoreo y definición de procedimientos para la configuración y resolución de incidentes y problemas de la infraestructura, ofreciendo de esta manera integridad de la información y disponibilidad de los servicios.	PT4	PT5	PT12	PT13					P	S		P	S		
MT10	Mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar los problemas reportados de los elementos de TI a nivel de hardware, sistemas operativos, bases de datos y aplicaciones.	PT4	PT12	PT8						P	S		S	P		
MT11	Garantizar los respaldos y recuperación de la información almacenándolos en sitios seguros que permitan mantener la integridad, exactitud, disponibilidad y protección de	PT3	PT5	PT7	PT9					S	P					

	los datos.															
MT12	Proporcionar un buen clima laboral para el personal y un buen ambiente físico para proteger los equipos DSLAM, infraestructura, comunicaciones y sistemas de gestión (servidores), utilizando medidas de control y seguridad en las instalaciones.	PT3	PT4	PT8	PT11	PT12	PT13			P	P			P		
MT13	Establecer e implementar procedimientos de mantenimiento oportunos con el personal del Departamento APD y los proveedores para que se pueda reducir la frecuencia de impacto o fallas en la infraestructura.	PT5	PT7	PT9	PT10	PT11	PT12	PT13		P	P		P	P		S

Tabla 25 Enlace de las Metas de TI a Procesos TI

La propuesta de Gobierno de TI se basa en el mapeo de las Metas Negocio (MN), Metas de TI (MT), Procesos TI (PT) y Criterios de Información para el Departamento Administración Plataformas DSLAMs, que servirá como parámetro de evaluación para medir el nivel de cumplimiento, basándose en las necesidades encontradas en el diagnóstico del Gobierno de TI (Punto 1.2 de este documento) del Departamento Administración Plataformas DSLAMs.

En la Tabla 25 se indica la intersección entre Metas de TI, Procesos de TI y Criterios de Información.

- **DEFINIR RIESGOS**

"Es importante medir el grado de riesgo que presentan los activos de información del Departamento Administración Plataformas DSLAMs, este proceso ayudara a la administración a balancear las operaciones y los costos económicos; esta actividad es importante para implementar medidas de protección las cuales deben ser aplicadas en los sistemas de información".[1]

El proceso para la definición del riesgo involucra las siguientes actividades:

- Identificación de riesgos
- Análisis de los riesgos
- Selección e implementación
- Seguimiento y medición
- Determinación del riesgo

A continuación se describe el rango de selección que se tomará en cuenta para la evaluación del riesgo del Departamento Administración Plataformas DSLAMs, considerando las amenazas, vulnerabilidades e impacto.

NIVEL	ESPECIFICACIÓN DE RIESGO	PROBABILIDAD/DEGRADACIÓN
0	NULO	Daño entre 0% y 35% 0<=RS<35
1	BAJO	Daño entre 35% y 65% 35<=RS<65
2	MEDIO	Daño entre 65% y 85% 65<=RS<85
3	ALTO	Daño entre 85% y 100% 85<=RS<=100

Tabla 26 Rango de selección de Riesgo del Departamento Administración Plataformas DSLAMs

- **Identificación de Riesgos**

Es necesario identificar los riesgos a los que están expuestos los activos de información del Departamento Administración Plataformas DSLAMs.

En base al estudio de campo se presenta los activos de información del Departamento Administración Plataformas DSLAMs sobre los cuales se va a evaluar los riesgos.

#	ACTIVO DE INFORMACIÓN SUJETO A RIESGOS
1	Equipos de comunicación de red y prestación de servicios Datos/Internet DSLAM
2	Servidores de Gestión DSLAM
3	Copia de Respaldo de la configuración de los equipos DSLAMs
4	Copia de Respaldo de los servidores de Gestión
5	Personal especializado
6	File Server (Archivo de Ingenierías)

Tabla 27 Activo de información sujeto a riesgos del Departamento Administración Plataformas DSLAMs
Fuente: Departamento Administración Plataformas DSLAMs

- **Análisis de los riesgos**

Para el análisis de riesgos es necesario identificar los activos de información dependiendo la criticidad debido a que no todos los activos de información tiene un mismo valor, por ende es necesario establecer una valoración donde los propietarios de los activos clasifiquen según las tres características básicas de seguridad de la información, confidencialidad, integridad y disponibilidad.[1]

CARACTERÍSTICAS BÁSICAS DE SEGURIDAD DE LA INFORMACIÓN		VALOR
CONFIDENCIALIDAD	Información que puede ser conocida y utilizada sin autorización por cualquier funcionario dentro o fuera de la del Departamento APD.	0
	Información que puede ser conocida y utilizada por todos los agentes del Departamento APD.	1
	Información que sólo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.	2
	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio del Departamento APD.	3
INTEGRIDAD	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades del Departamento APD.	0
	Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio para el Departamento APD.	1
	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para el Departamento APD.	2
	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades.	3
DISPONIBILIDAD	Información cuya inaccesibilidad permanente no afecta la actividad normal del Departamento APD.	0
	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para el Departamento APD.	1
	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades del Departamento APD.	2
	Información cuya inaccesibilidad permanente durante una hora podría impedirla ejecución de las actividades del Departamento APD.	3

Tabla 28 Características básicas de seguridad de la información

Fuente: Universidad Nacional de Luján - Departamento de Seguridad Informática

Para obtener el valor de la criticidad se toma el valor máximo del resultado de las características básicas de seguridad de la información, como se puede apreciar en la Tabla 29.

ACTIVO	CARACTERISTICAS BÁSICAS DE SEGURIDAD DE LA INFORMACIÓN			CRITICIDAD
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	
Equipos de comunicación de red y prestación de servicios Datos/Internet DSLAM	2	3	3	3
Servidores de Gestión DSLAM	2	2	2	2
Copia de Respaldo de la configuración de los equipos DSLAM	3	2	1	3
Copia de Respaldo de los servidores de Gestión	3	2	1	3
Personal especializado	2	2	2	2
File Server (Archivo de Ingenierías)	1	0	1	1

Tabla 29 Criticidad de los Activos del Departamento Administración Plataformas DSLAMs
Fuente: Departamento Administración Plataformas DSLAMs

- **Selección e implementación**

El objeto de este paso es identificar las vulnerabilidades de los activos y dar un listado de las amenaza del departamento Administración plataformas DSLAMs que está siendo evaluado para la implementación de controles que reduzcan los riesgos.

"Una vulnerabilidad es toda debilidad en un activo de información, proporcionada comúnmente por la inexistencia o ineficiencia de un control, una amenaza es todo elemento que hace uso o aprovecha una vulnerabilidad, atenta o pueda atentar contra la seguridad de un activo de información, las amenazas surgen a partir de la existencia de vulnerabilidades" .[1]

A continuación la identificación de vulnerabilidades y amenazas.

ACTIVO	CRITICIDAD	VULNERABILIDAD	AMENAZA
Equipos de comunicación de red y prestación de servicios Datos/Internet DSLAM	3	Falta de procedimientos de monitoreo de hardware.	Fallas técnicas
Servidores de Gestión DSLAM	2	Monitoreo inadecuado de los servidores	Temperatura/humedad externas
Copia de Respaldo de la configuración de los equipos DSLAM	3	Administración inadecuada de la seguridad de la red	Falla en servicio de comunicación
Copia de Respaldo de los servidores de Gestión	3	Falta de log	Acceso no autorizado a datos
Personal especializado	2	Desconocimiento de los procedimientos establecidos	Procedimientos no documentados Falta de conocimiento y entrenamiento oportuno
File Server (Archivo de Ingenierías)	1	Falta de políticas y procedimientos de control de cambios	Eliminación no autorizado a datos

Tabla 30 Identificación de vulnerabilidades y amenazas.
Fuente: Departamento Administración Plataformas DSLAMs

- **Seguimiento y medición**

La valoración de amenazas y determinación del impacto adverso como resultado de la ejecución de una amenaza se considera la degradación de la confidencialidad, integridad y disponibilidad.

El impacto se calcula en base al máximo valor de degradación que la amenaza produce sobre un activo y la criticidad del activo definida en los pasos anteriores.

El Impacto total es igual a la criticidad por el valor máximo de la degradación porcentual dividido para el cien por ciento.[1]

AMENAZA	CRITICIDAD	DEGRADACION			IMPACTO (TOTAL)
		CONFID	INTEGRID	DISPONIB	
Fallas técnicas	3	80%	100%	100%	3
Temperatura/humedades externas	2	50%	50%	50%	1
Falla en servicio de comunicación	3	80%	100%	100%	3
Acceso no autorizado a datos	3	100%	90%	100%	3
Procedimientos no documentados y Falta de conocimiento y entrenamiento oportuno	2	50%	50%	50%	1
Eliminación no autorizado a datos	1	100%	100%	50%	1

Tabla 31 Valoración de amenazas y determinación del impacto
Fuente: Departamento Administración Plataformas DSLAMs

- **Determinación del Riesgo.**

La determinación del riesgo se basara en un estudio de campo al personal del Departamento APD, se verificara en base a la frecuencia con la que podría ocurrir un evento anual.

El Riesgo es igual a la frecuencia por el impacto.

ACTIVO	AMENAZA	FRECUENCIA (ANUAL)	IMPACTO (TOTAL)	RIESGO	NIVEL
Equipos de comunicación de red y prestación de servicios Datos/Internet DSLAM	Fallas técnicas	1	3	3	ALTO
Servidores de Gestión DSLAM	Temperatura/humedad externas	1	1	1	BAJO
Copia de Respaldo de la configuración de los equipos DSLAMs	Falla en servicio de comunicación	1	3	3	ALTO
Copia de Respaldo de los servidores de Gestión	Acceso no autorizado a datos	1	3	3	ALTO
Personal especializado	Procedimientos no documentados y Falta de conocimiento y entrenamiento oportuno	1	1	1	BAJO
File Server (Archivo de Ingenierías)	Eliminación no autorizado a datos	2	1	2	MEDIO

Tabla 32 Determinación de riesgo Departamento Administración Plataformas DSLAMs
Fuente: Departamento Administración Plataformas DSLAMs

Según los valores indicados en la Tabla 32 el promedio del RIESGO es de 2.1 identificándose en un nivel MEDIO, degradación entre 65% y 85%, según el rango de selección de la Tabla 26.

Se puede identificar la necesidad de mitigar los riesgos de los siguientes activos de información: Equipos de comunicación de red y prestación de servicios Datos/Internet DSLAMs, Copia de Respaldo de la configuración de los equipos DSLAMs y Copia de Respaldo de los servidores de Gestión. Estos activos se encuentran en el nivel 3 identificándose en un riesgo ALTO, con un daño entre 85% y 100%.

- **DEFINIR RECURSOS Y ENTREGABLES**

Se define el marco de Gobernabilidad de TI con los procesos del Departamento Administración plataformas DSLAMs y basándonos en los procesos de COBIT, ITIL V3 e ISO 27001 con los cuales se realizara el estudio de campo con los dueños de cada proceso del Departamento APD.

Los recursos definidos que serán utilizados para el gobierno de TI y administración de procesos son los presentados en la siguiente Tabla 33.

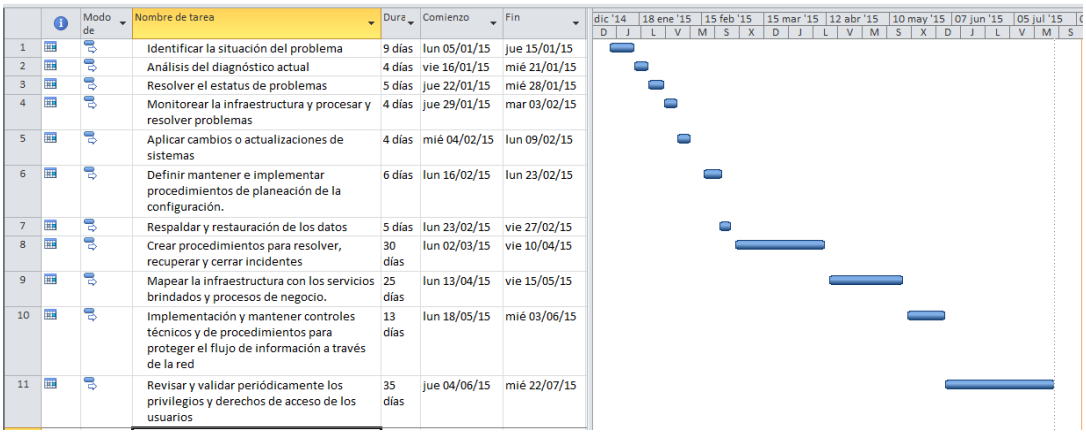
	PROCESOS DE TI	**OBJETOS DE CONTROL**
PT1	DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	DS1.1, DS1.2, DS1.3, DS1.4, DS1.5, DS1.6
PT2	ADMINISTRAR LOS SERVICIOS DE TERCEROS	DS2.1, DS2.2, DS2.3, DS2.4
PT3	ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	DS3.1, DS3.2, DS3.3, DS3.4, DS3.5
PT4	GARANTIZAR LA CONTINUIDAD DEL SERVICIO	DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.7, DS4.8, DS4.9
PT5	GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	A.11.1, A.11.2, A.11.3, A.11.4, A.11.5, A.11.6, A.11.7
PT6	IDENTIFICAR Y ASIGNAR COSTOS	SO 4.6.7
PT7	EDUCAR Y ENTRENAR A LOS USUARIOS	DS7.1, DS7.2, DS7.3
PT8	ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES	SO 4.1, SO 4.2, SO 6.2, SO 4.1.5.3, SO 4.1.5.4, SO 4.1.5.5, SO 4.1.5.6, SO 4.1.5.7, SO 4.2.5.1, SO 4.2.5.2, SO 4.2.5.3, SO 4.2.5.4, SO 4.2.5.5, SO 4.3.5.1, SO 4.1.5.8, SO 4.2.5.6, SO 4.2.5.7, SO 4.2.5.8, SO 5.9, SO 4.1.5.10, SO 4.2.5.9, SO 4.1.5.9
PT9	ADMINISTRAR LA CONFIGURACIÓN	A.11.4
PT10	ADMINISTRAR LOS PROBLEMAS	DS10.1, DS10.2, DS10.3, DS10.4

	PROCESOS DE TI	OBJETOS DE CONTROL
PT11	ADMINISTRAR LOS DATOS	DS11.1, DS11.2, DS11.3, DS11.4, DS11.5, DS11.6
PT12	ADMINISTRAR EL AMBIENTE FÍSICO	DS12.1, DS12.2, DS12.3, DS12.4, DS12.5
PT13	ADMINISTRAR LAS OPERACIONES	SO 3.7, SO 5, SO APENDICE B, SO 5.3, SO 4.1, SO 4.1.5.1, SO 4.1.5.9, SO 5.2.1, SO 5.2.4, SO 5.3, SO 5.4

Tabla 33 Administración de Procesos

- **PLANEAR PROGRAMA**

Para el estudio de los procesos y los recursos del Departamento Administración Plataformas DSLAMs., se desarrollara una matriz RACI y la definición de tiempos y recursos.



	Modo de	Nombre de tarea	Dura	Comienzo	Fin
1		Identificar la situación del problema	9 días	lun 05/01/15	jue 15/01/15
2		Análisis del diagnóstico actual	4 días	vie 16/01/15	mié 21/01/15
3		Resolver el estatus de problemas	5 días	jue 22/01/15	mié 28/01/15
4		Monitorear la infraestructura y procesar y resolver problemas	4 días	jue 29/01/15	mar 03/02/15
5		Aplicar cambios o actualizaciones de sistemas	4 días	mié 04/02/15	lun 09/02/15
6		Definir mantener e implementar procedimientos de planeación de la configuración.	6 días	lun 16/02/15	lun 23/02/15
7		Respaldar y restauración de los datos	5 días	lun 23/02/15	vie 27/02/15
8		Crear procedimientos para resolver, recuperar y cerrar incidentes	30 días	lun 02/03/15	vie 10/04/15
9		Mapear la infraestructura con los servicios brindados y procesos de negocio.	25 días	lun 13/04/15	vie 15/05/15
10		Implementación y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red	13 días	lun 18/05/15	mié 03/06/15
11		Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios	35 días	jue 04/06/15	mié 22/07/15

Figura 18 Definición de tiempos y recursos

Para estructurar la matriz RACI se requiere definir quién es Responsable (R), quien debe rendir cuentas (A), quien debe ser consultado (C) y quien debe ser Informado (I) sobre las actividades del Departamento APD.

ACTIVIDADES	GERENTE NACIONAL	GERENTE O&M	JEFATURA APD	ANALISTA O&M
Identificar la situación del problema	I	I	R	A
Análisis del diagnóstico actual	I	I		

ACTIVIDADES	GERENTE NACIONAL	GERENTE O&M	JEFATURA APD	ANALISTA O&M
Resolver el estatus de problemas			R	I
Monitorear la infraestructura y procesar y resolver problemas			A	R
Aplicar cambios o actualizaciones de sistemas		I	A/R	R
Definir mantener e implementar procedimientos de planeación de la configuración.	I	I	A/R	R
Respaldar y restauración de los datos			A/R	R
Crear procedimientos para resolver, recuperar y cerrar incidentes	I	I	A	R
Mapear la infraestructura con los servicios brindados y procesos de negocio.	I	I	A/R	R
Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red	I	I	A/R	R
Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios			A/R	R

Tabla 34 Actividades Departamento APD
Fuente: IT Governance Institute - cobit 4.1

En base a la matriz de la Tabla 34 se identifica las responsabilidades para el Departamento Administración Plataformas DSLAMs.

2.3.5.2 VISUALIZAR LA SOLUCIÓN

Para visualizar la solución se realizan tres pasos, primero la organización debe definir donde se encuentra con la evaluación de la capacidad actual y la madurez en los procesos de TI, segundo se definirá los objetivos de mejora según el nivel de madurez para cada uno de los procesos y finalmente se analizara las definiciones y determinaciones de las mejoras.

- **EVALUAR EL DESEMPEÑO ACTUAL**

A continuación el cuadro del modelo de madurez del Departamento Administración Plataformas DSLAMs.

Para determinar el nivel de madurez que actualmente posee el Departamento Administración Plataformas DSLAMs e identificar la Propuesta de Gobierno de TI objeto de esta investigación, se realizó un estudio de campo (punto 1.2 de este documento) dialogando con el Personal del Departamento Administración Plataformas DSLAMs que administra cada uno de los procesos identificados en la Tabla 35.

BASE	PROCESO	GRADO DE MADUREZ DEL DEPARTAMENTO ADMINSTRACIÓN PLATAFORMAS DSLAMs	GRADO DE MADUREZ
COBIT	1.DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio	2
		DS1.2 Definición de Servicios	3
		DS1.3 Acuerdos de Niveles de Servicio	3
		DS1.4 Acuerdos de Niveles de Operación	4
		DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	4
		DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	3
COBIT	2.ADMINISTRAR LOS SERVICIOS DE TERCEROS	DS2.1 Identificación de todas las relaciones con proveedores	4
		DS2.2 Gestión de relaciones con proveedores	3
		DS2.3 Administración de riesgos del proveedor	3
		DS2.4 Monitoreo del desempeño del proveedor	3
COBIT	3.ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	DS3.1 Planeación del desempeño y la capacidad	2
		DS3.2 Capacidad y desempeño actual	3
		DS3.3 Capacidad y desempeño futuros	3
		DS3.4 Disponibilidad de recursos de TI	3
		DS3.5 Monitoreo y reportes	2
COBIT	4.GARANTIZAR LA CONTINUIDAD DEL SERVICIO	DS4.1 Marco de trabajo de continuidad de TI	3
		DS4.2 Planes de continuidad de TI	4
		DS4.3 Recursos críticos de TI	3
		DS4.4 Mantenimiento de plan de continuidad de TI	3
		DS4.5 Pruebas del plan de continuidad de TI	2
		DS4.6 Entrenamiento del plan de continuidad de TI	1
		DS4.7 Distribución del plan de continuidad de TI	1
		DS4.8 Recuperación y reanudación de los servicios de TI	2
		DS4.9 Almacenamiento de respaldos fuera de las instalaciones	0
		A.11.1 Requerimiento de negocio de control de acceso	0
		A.11.2 Administración de Accesos de Usuarios	1

BASE	PROCESO	GRADO DE MADUREZ DEL DEPARTAMENTO ADMINSTRACIÓN PLATAFORMAS DSLAMs	GRADO DE MADUREZ
ISO 27001	5.GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	A.11.3 Responsabilidades de los usuario	1
		A.11.4 Control de acceso a red	2
		A.11.5 Control de acceso del sistema operativo	1
		A.11.6 Control de Acceso en la información y a las aplicaciones	1
		A.11.7 Computación móvil y el teletrabajo	1
ITIL	6.IDENTIFICAR Y ASIGNAR COSTOS	SO 4.6.7 Financial management for IT services (as operational activities)	1
COBIT	7.EDUCAR Y ENTRENAR A LOS USUARIOS	DS7.1 Identificación de Necesidades de Entrenamiento y Educación	1
		DS7.2 Impartición de Entrenamiento y Educación	1
		DS7.3 Evaluación del Entrenamiento Recibido	2
ITIL	8.ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES	SO 4.1 gestión de eventos	3
		SO 4.1.5.3 Detección de eventos	3
		SO 4.1.5.4 Filtrado de eventos	3
		SO 4.1.5.5 Significado de eventos	3
		SO 4.1.5.6 Correlación de eventos	3
		SO 4.1.5.7 Trigger	3
		SO 4.1.5.8 Respuestas de selección	4
		SO 4.1.5.10 Cierre de eventos	4
		SO 4.2 Gestión de incidentes	4
		SO 4.2.5.1 identificación de Incidentes	4
		SO 4.2.5.2 Registro de incidentes	3
		SO 4.2.5.3 Categorización de incidentes	3
		SO 4.2.5.4 Priorización de incidentes	3
		SO 4.2.5.5 Diagnóstico inicial	3
		SO 4.2.5.6 Escalación de incidentes	3
		SO 4.2.5.7 Investigación y diagnostico	1
		SO 4.2.5.8 Resolución y recuperación	3
		SO 4.3.5.1 Menú selección	3
		SO 4.2.5.9 Cierre de incidentes	3
		SO 4.1.5.9 Revisión y acciones	3
		SO 5.9 soporte Desktop	2
		SO 6.2 Service desk	1
ISO 27001	9.ADMINISTRAR LA CONFIGURACIÓN	A.11.4 Network access control	3
	10.ADMINISTRAR	DS10.1 Identificación y clasificación de problemas	3
		DS10.2 Rastreo y resolución de problemas	4

BASE	PROCESO	GRADO DE MADUREZ DEL DEPARTAMENTO ADMINSTRACIÓN PLATAFORMAS DSLAMs	GRADO DE MADUREZ
COBIT	LOS PROBLEMAS	DS10.3 Cierre de problemas	3
		DS10.4 Integración de las administraciones de cambios, configuración y problemas.	3
COBIT	11.ADMINISTRAR LOS DATOS	DS11.1 Requerimientos del Negocio para Administración de Datos	3
		DS11.2 Acuerdos de Almacenamiento y Conservación	3
		DS11.3 Sistemas de Administración de Librerías de Medidas	0
		DS11.4 Eliminación	0
		DS11.5 Respaldo y Restauración	2
		DS11.6 Requerimientos de Seguridad para la Administración de Datos	1
COBIT	12.ADMINISTRAR EL AMBIENTE FÍSICO	DS12.1 Selección y Diseño del Centro de Datos	0
		DS12.2 Medidas de Seguridad Física	0
		DS12.3 Acceso Físico	1
		DS12.4 Protección Contra Factores Ambientales	3
		DS12.5 Administración de Instalaciones Físicas	2
ITIL	13.ADMINISTRAR LAS OPERACIONES	SO 3.7 Documentación	0
		SO 5 Actividades de operación de servicio común	2
		SO 4.1 gestión de eventos	3
		SO 4.1.5.1 Ocurrencia de eventos	2
		SO 4.1.5.9 Revisión y acciones	2
		SO 5.2.1 Consola de gestión/puente operaciones	3
		SO 5.2.4 Impresión y salidas	3
		SO 5.3 Gestión Mainframe	2
		SO 5.4 Administración de servidores y soporte	3
		SO APENDICE B	3

Tabla 35 Grado de Madurez Procesos TI

Para obtener el grado de madurez actual de la Tabla 35 del Departamento Administración Plataformas DSLAMs, se realizó la evaluación en base a la documentación del **Anexo 3**, **Anexo 5** utilizando los procesos de COBIT, ITIL e ISO27001 y en base al **MODELO DE MADUREZ** de este documento.

- **DEFINIR OBJETIVOS DE MEJORA**

Los objetivos de mejora de los procesos del Departamento APD se basan en la medición del grado de madurez, Figura 19, según la evaluación del desempeño actual.

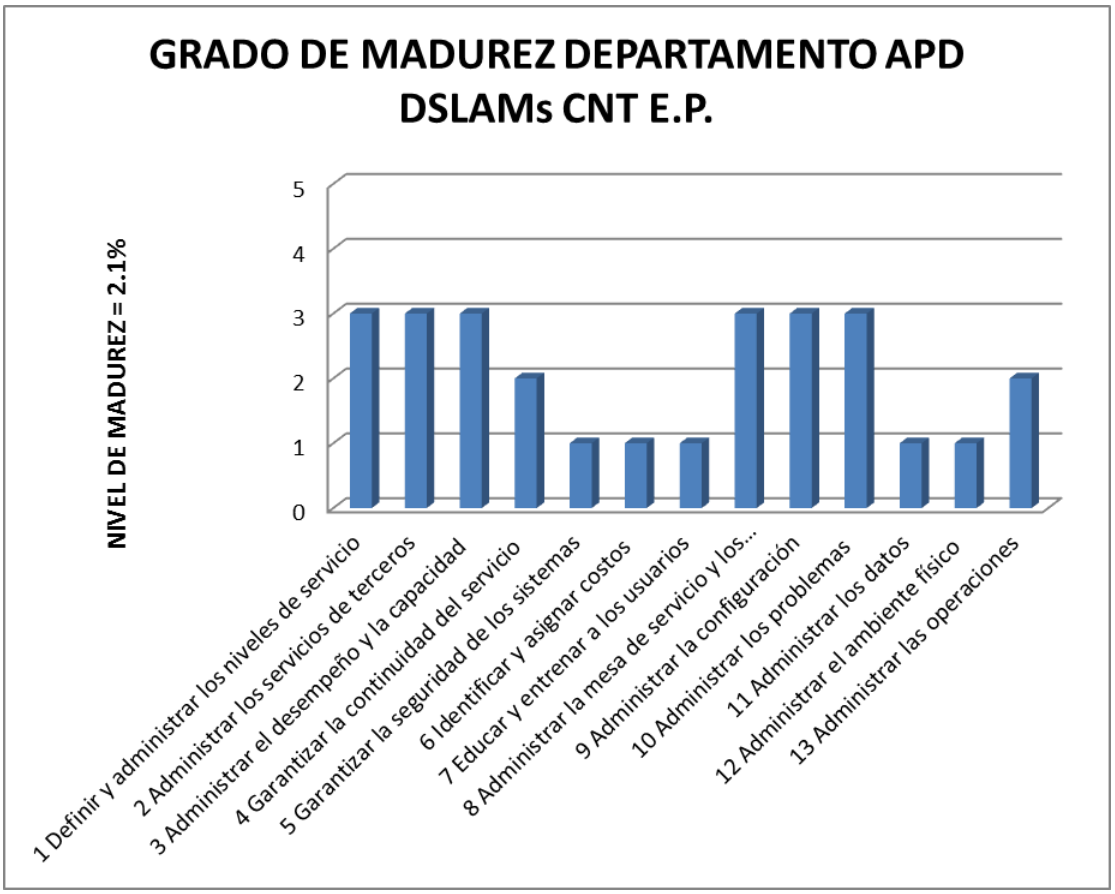


Figura 19 Grado de Madurez Departamento Administración Plataformas DSLAMs

En la Figura 19 se presenta el grado de madurez actual del Departamento Administración Plataformas DSLAMs ubicándose en el Nivel 2, esto nos indica que se encuentran los procesos en un PATRÓN REGULAR, en el cual existe conciencia del manejo de los procesos de Tecnologías de Información;

basándonos en esta información es necesario identificar los procesos que tienen un grado de madurez de 0, 1 y 2 los cuales requieren mejoría, objeto de esta investigación.

- **ANALIZAR BRECHAS Y DETERMINAR LAS MEJORAS**

En base a la evaluación actual de los procesos del Departamento Administración Plataformas DSLAMs y con la finalidad de mejorar su desempeño en los procesos se tomara como referencia el modelo de madurez del manejo de la TI del punto 2.3.3 de este documento.

A continuación se describe los procesos seleccionados que necesitan mejoras:

- **GARANTIZAR LA CONTINUIDAD DEL SERVICIO**

  Para garantizar la continuidad de los servicios se realizarán mejoras en los siguientes objetivos de control.

  - ✓ **DS4.5 Pruebas del plan de continuidad de TI.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular, este objetivo de control está enfocado en recuperar los sistemas de forma efectiva para lo cual se debe crear procedimientos de planes de acción para cada sistema de gestión y DSLAMs en caso de que exista interrupciones.

  - ✓ **DS4.6 Entrenamiento del plan de continuidad de TI.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, los administradores de cada plataforma deben tener un grado de responsabilidad y experticia en los sistemas en caso de una inhibición del servicio.

  - ✓ **DS4.7 Distribución del plan de continuidad de TI.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, para este proceso el departamento APD debe realizar planes de contingencia y estrategias para que el servicio siempre se encuentre activo.

- ✓ **DS4.8 Recuperación y reanudación de los servicios de TI.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular, deben fortalecer en los procedimientos para recuperar los servicios en caso de que exista una falla, como tener sistemas de redundancia a nivel de servidores o transmisión de DSLAMs en caso de que existan fallas la recuperación sea inmediata sin que afecte a los clientes.

- ✓ **DS4.9 Almacenamiento de respaldos fuera de las instalaciones**. Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto, no existe respaldos fuera de las instalaciones se debe ejecutar procedimientos de respaldo para que la información se traslade físicamente a otros lugares con todos los cuidados del caso.

- ➢ **GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS**

Para garantizar la seguridad de los servicios es necesario garantizar el control definido a continuación.

- ✓ **A.11.1 Requisitos del Negocio para el Control de Acceso.** Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto. Es necesario crear procedimientos para el acceso a la información y a los sistemas del negocio (OPEN) creando políticas de acceso a los usuarios y comprometiendo su responsabilidad en base de actas.

- ✓ **A.11.2 Administración de Accesos de Usuarios.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, se debe aplicar políticas, procedimientos y control de acceso a los usuarios que requieran ingresar a los sistemas de gestión y DSLAMs.

- ✓ **A.11.3 Responsabilidades de los Usuarios.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados; el personal que requiere el acceso de usuario debe firmar actas de confidencialidad y responsabilidad, no dejar activas las sesiones, las contraseñas deben tener un número mínimo de caracteres especiales.

- ✓ **A.11.4 Control de Acceso a Redes.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular, existen procesos implementados pero necesitan ser reforzados los controles y procedimientos de autenticación y acceso como: por regiones, privilegios de puertos, aplicaciones, tipos de nodos, modelos.

- ✓ **A.11.5 Control de Acceso al Sistema Operativo.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, los procesos deben ser organizados creando formularios de acceso, ingreso a la red por redes privadas o redes internas, el usuario debe ser único y las contraseñas debe tener un mínimo de caracteres.

- ✓ **A.11.6 Control de Acceso a la Información y a las Aplicaciones.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados; se controlara por usuarios y determinando la responsabilidad que se asignara a cada uno, como restricción por IP, por horarios, por sesiones y determinar la función exacta que cada usuario requiere.

- ✓ **A.11.7 Computación Móvil y Trabajo Remoto.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados; se implementará el acceso a la red, sistemas operativos y aplicaciones a través de la redes privadas virtuales, firewall, antivirus y sistemas que encripten la información.

- ➢ **IDENTIFICAR Y ASIGNAR COSTOS**

Para garantizar la continuidad de los servicios se realizará mejoras en los siguientes objetivos de control.

- ✓ **SO 4.6.7 Gestión Financiera para los servicios de TI**. Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, el departamento debe levantar requerimientos que son necesarios para mejorías de los sistemas de gestión y servicio, realizar una planificación presupuestaria semestral en caso de que exista ajustes para los recursos que demande el departamento APD.

- ➢ **EDUCAR Y ENTRENAR A LOS USUARIOS**

  Es necesario identificar las necesidades de entrenamiento que requiere cada usuario sobre los sistemas de gestión y DSLAMs.

- ✓ **DS7.1 Identificación de Necesidades de Entrenamiento y Educación.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, es necesario realizar un plan de capacitaciones periódicas en base a las tecnologías de gestión y DSLAMs fundamentándonos en las nuevas aplicaciones, software y sistemas operativos.

- ✓ **DS7.2 Impartición de Entrenamiento y Educación.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, las capacitaciones para el personal del departamento APD deben ser impartidas con instructores expertos en los temas a capacitar y llevar un registro de evaluaciones y desempeño del aprendizaje de la instrucción impartida.

- ✓ **DS7.3 Evaluación del Entrenamiento Recibido.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular, impartida la capacitación deben llevar un registro con los resultados de valor para definiciones futuras.

- **ADMINISTRAR LOS DATOS**

  Administrar la información en base a procedimientos que ayude a mantener la disponibilidad de los datos del departamento.

- ✓ **DS11.3 Sistemas de Administración de Librerías de Medidas.** Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto, se debe implementar un sistema de almacenamiento de información de los sistemas de gestión y DSLAMs, el cual se pueda guardar y recuperar la información dependiendo el tiempo que requiera.

- ✓ **DS11.4 Eliminación.** Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto, levantar procedimientos que ayude a realizar trabajos de eliminación de archivos, información sensible o archivos del sistemas operativos.

- ✓ **DS11.5 Respaldo y Restauración.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular, necesita llevar un proceso de respaldo y restauración de los sistemas de gestión y DSLAMs.

- ✓ **DS11.6 Requerimientos de Seguridad para la Administración de Datos.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados, implementar procedimientos y políticas de seguridad como firewall, protocolos de encriptación a la conexión de la red y servidores.

- **ADMINISTRAR EL AMBIENTE FÍSICO**

  Para la protección de los dispositivos es necesario mantener las instalaciones en buen estado físico.

- ✓ **DS12.1 Selección y Diseño del Centro de Datos.** Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto, por diferentes causas naturales o de nombre es necesario llevar un diseño de activo standby geográfico para los sistemas centralizados.

- ✓ **DS12.2 Medidas de Seguridad Física.** Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto; es necesario levantar procedimiento de ingreso a los sitios donde se encuentran alojados los servidores o los DSLAMs; se requiere implementar un sistema de ingreso a cada sitio, formularios que identifiquen quien es responsable y que autorice el ingreso a los nodos.

- ✓ **DS12.3 Acceso Físico.** Se encuentra en un nivel 1 es decir los procesos son ad hoc y desorganizados; cualquier persona del departamento APD, personal de la CNT, proveedores o personal externo deben limitarse a los procedimientos llenando un formulario con una persona que autorice y sea responsable del ingreso físico a los nodos.

- ✓ **DS12.5 Administración de Instalaciones Físicas.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular; debe implementarse procedimientos de la administración de todos los dispositivos que conforman los nodos.

- ➢ **ADMINISTRAR LAS OPERACIONES**

- ✓ **SO 3.7 Documentación.** Se encuentra en un nivel 0 es decir los procesos del manejo no se aplican en lo absoluto; implementar procedimientos para todos los equipos, aplicaciones, sistemas operativos y manuales de procesos , los cuales deben estar actualizados siempre y cuando exista actualizaciones, nuevos sistemas o sistemas que salgan de operación.

- ✓ **SO 5 Actividades de operación de servicio común.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular; estas actividades debemos alinearlas al departamento APD en base a los sistemas de gestión y DSLAMs para su gestión oportuna y brindar un buen servicio a los clientes.

- ✓ **SO 4.1.5.1 Ocurrencia de eventos.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular, por ende para levantar los eventos

de los sistemas de gestión es necesario involucrar al personal que opera los procesos del departamento APD.

- ✓ **SO 4.1.5.9 Revisión y acciones.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular; los procesos deben ser manejados apropiadamente, los eventos deben ser filtrados por su criticidad o acciones como críticos, de mayor o menor grado según el incidente.

- ✓ **SO 5.3 Gestión Mainframe.** Se encuentra en un nivel 2 es decir los procesos siguen un patrón regular; es importante levantar un sistema de gestor de gestores para la administración de los equipos que conforman el departamento APD de la CNT, los procesos necesarios para gestionar inventario, activación, alarmas y performance.

2.3.5.3 PLANEAR LA SOLUCIÓN

La tercera fase de la hoja de ruta identifica las iniciativas para las mejoras, alineado el negocio con los factores de riesgo del Departamento Administración Plataformas DSLAMs para lo cual es necesario definir proyectos y desarrollar un plan de mejoras.

- **DEFINIR PROYECTOS**

Se define el proyecto en base a los niveles de cumplimiento de la propuesta de Gobierno de TI para el Departamento Administración Plataformas DSLAMs con las metas de TI, Procesos TI y mapeo de COBIT, ITIL e ISO-27001, en base a la escala de valores y rango de selección definida en la Tabla 36.

Se evaluara y definirá directamente con los dueños de los procesos del Departamento Administración Plataformas DSLAMs de la CNT E.P., según la evaluación de los objetivos de control de la tabla 37, identificados los procesos se verificara las necesidades para proceder a definir la solución y mejora en cada uno de los procedimientos, políticas y estándares.

- **DESARROLLAR UN PLAN DE MEJORAS**

Para desarrollar un plan de mejoras primero se identificara los procesos que se encuentran con inconsistencias en base a una evaluación de un estudio de campo para cada objeto de control, como segundo punto se identificara el por qué se originan los problemas para posteriormente definir qué mejoras se deben realizar para cada uno de los procesos del departamento administración plataformas DSLAMs según el punto 2.3.5.4 de este documento.

2.3.5.4 IMPLEMENTAR LA SOLUCIÓN

Para la implementación de la solución se desarrollara los siguientes temas: Implementar las Mejoras, Monitorear el Desempeño de la Implementación y Revisar la Efectividad del Programa.

- **IMPLEMENTAR LAS MEJORAS**

Para implementar las mejoras se tomara como referencia el mapeo de las Metas de TI (MT) y Procesos TI (PT) para el Departamento Administración Plataformas DSLAMs de la CNT E.P., a continuación se detalla los procesos a considerar para la implementación.

Como se ilustra en la Figura 20 el proceso de implementación de las mejoras se definirá en las siguientes fases:

- FASE 1: Definir una escala de valores
- FASE 2: Establecer un rango de selección
- FASE 3: Evaluar los procesos de Gobierno de TI

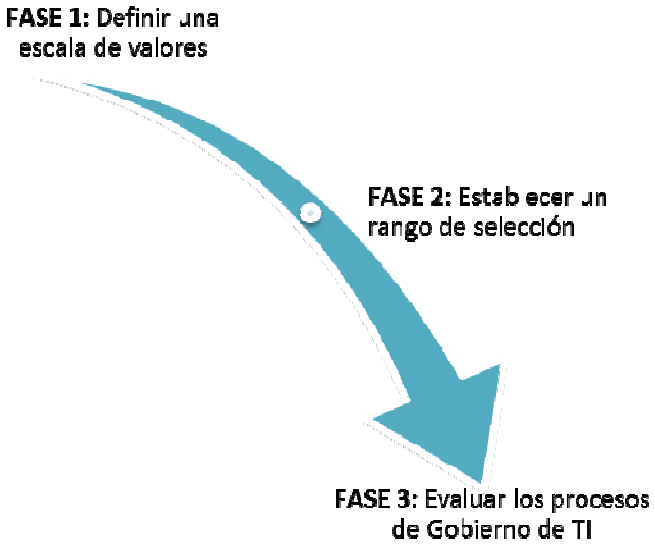


Figura 20 Fases de los procesos de evaluación

FASE 1: Definir una Escala de Valores

Para la ejecución de la evaluación del Gobierno de TI del Departamento Administración Plataformas DSLAMs de la CNT E.P, se utilizará como marco de referencia la propuesta definida en este capítulo, utilizando una escala de valores cuantitativos y cualitativos.

Valores Cuantitativos

Son valores numéricos entre 0 y 100 por ciento. Los valores mencionados sirven para medir el porcentaje de cumplimiento respecto a la propuesta de Gobierno de TI definido en este documento para el Departamento Administración Plataformas DSLAMs de la CNT E.P.

Valores Cualitativos

Son valores que representan el nivel de cumplimiento de las actividades del Departamento Administración Plataformas DSLAMs. Para tal efecto se utilizará una escala de tres valores: no cumple, parcial y cumple.

FASE 2: Establecer un Rango de Selección

El rango de selección (RS) son los valores para definir el nivel de cumplimiento de los objetivos de control (COBIT 4.1), procesos (ITIL V3) y controles (ISO 27001) con las metas de TI.

A continuación se describe el rango de selección que se tomará en cuenta para la evaluación de las actividades del Departamento Administración Plataformas DSLAMs:

GRADO DE CUMPLIMIENTO	ESPECIFICACIÓN	RANGO DE SELECCIÓN (RS)
NO CUMPLE	Este parámetro se refiere a las actividades de Gobierno de TI que **NO se encuentran** en un rango aceptable.	Entre 0% y 25% 0<=RS<25
PARCIAL	Hace referencia a ciertas actividades de Gobierno de TI **que se encuentran en un rango medio o parcial** de aceptabilidad.	Entre 25% y 70% 25<= RS < 70
CUMPLE	Este parámetro hace referencia cuando cierta actividad de Gobierno de TI **se encuentra en un rango de selección aceptable**.	Entre 70% y 100% 70 <= RS <= 100

Tabla 36 Especificaciones del Rango de Selección (RS) del Proceso de Evaluación de la Propuesta de Gobierno de TI

FASE 3: Evaluar Los Procesos TI

Esta fase se encargará de establecer los niveles de cumplimiento en base a la Propuesta de Gobierno de TI con las metas de TI, Procesos TI y basándose en COBIT, ITIL e ISO-27001 definida en la Tabla 37 de este documento.

- **MONITOREAR EL DESEMPEÑO DE LA IMPLEMENTACIÓN**

Al monitorear el desempeño de la implementación se considera la escala de valores especificados en la Fase 1 y del Rango de Selección (RS) determinados en la Fase 2 definidos en este documento. Para tal efecto se realizaran las siguientes actividades:

a) Evaluar los procesos definidos para la propuesta de Gobierno de TI de esta investigación, el cual contiene las metas de TI y procesos de TI, los objetivos de control para COBIT (Entregar y Dar Soporte), procesos de ITIL (Operación del Servicio) y Controles de la ISO 27001 (Control de Acceso). Así mismo la propuesta se basa en los elementos tecnológicos y de infraestructura que se relacionan directamente con el Departamento Administración Plataformas DSLAMs CNT E.P.

   Tomando en cuenta el rango de selección de la Tabla 36 se otorga un valor cuantitativo (Entre 0 y 100) y de esta manera se determinará cuantitativa y cualitativamente el grado de cumplimiento que actualmente soporta el Departamento de Administración Plataformas DSLAMs de la CNT E.P.

b) Seleccionar las actividades que se encuentran en un rango aceptable. Una vez realizada la evaluación se selecciona las actividades que son mayores o iguales a 70%. Esta selección se visualiza en la siguiente Tabla 37 de evaluación mediante la disposición de colores de la siguiente manera:

- Rojo: No cumple (Entre 0% y menor 25%)
- Amarillo: Parcial (mayor o igual al 25% y menor al 70%)
- Verde: Cumple (mayor o igual al 70%)

A continuación la tabla de evaluación.

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
1 Definir y administrar los niveles de servicio																	
DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio	83	85				78								**82**	**82**		
DS1.2 Definición de Servicios	66	75				80								**74**	**74**		
DS1.3 Acuerdos de Niveles de Servicio	87	80				76								**81**	**81**		
DS1.4 Acuerdos de Niveles de Operación	90	76				85								**84**	**84**		
DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	87	78				86								**84**	**84**		
DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	76	77				87								**80**	**80**		
2 Administrar los servicios de terceros																	
DS2.1 Identificación de todas las relaciones con proveedores	80	74		86										**80**	**80**		
DS2.2 Gestión de relaciones con proveedores	88	85		80										**84**	**84**		
DS2.3 Administración de riesgos del proveedor	75	88		78										**80**	**80**		
DS2.4 Monitoreo del desempeño del proveedor	73	89		74										**79**	**79**		

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
3 Administrar el desempeño y la capacidad																	
DS3.1 Planeación del desempeño y la capacidad			80											**80**	**80**		
DS3.2 Capacidad y desempeño actual			78											**78**	**78**		
DS3.3 Capacidad y desempeño futuros			73											**73**	**73**		
DS3.4 Disponibilidad de recursos de TI			80											**80**	**80**		
DS3.5 Monitoreo y reportes			75											**75**	**75**		
4 Garantizar la continuidad del servicio																	
DS4.1 Marco de trabajo de continuidad de TI		80	78		84				78					**80**	**80**		
DS4.2 Planes de continuidad de TI		90	85		80				80					**84**	**84**		
DS4.3 Recursos críticos de TI		90	78		75				76					**80**	**80**		
DS4.4 Mantenimiento de plan de continuidad de TI		95	75		78				80					**82**	**82**		
DS4.5 Pruebas del plan de continuidad de TI		76	70		75				78					**75**	**75**		
DS4.6 Entrenamiento del plan de continuidad de TI		70	73		80				73					**74**	**74**		
DS4.7 Distribución del plan de continuidad de		76	72		85				70					**76**	**76**		

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
TI																	
DS4.8 Recuperación y reanudación de los servicios de TI		96	75		77				73					**80**	**80**		
DS4.9 Almacenamiento de respaldos fuera de las instalaciones		56	50		78									**61**	**61**		
5 Garantizar la seguridad de los sistemas																	
A.11.1 Requisitos del Negocio para el Control de Acceso			75	76	72	78		78	73		76	76		**76**			**76**
A.11.2 Administración de Accesos de Usuarios			70	80	81	84		69	78		78	79		**77**			**79**
A.11.3 Responsabilidades de los Usuarios			73	70	73	78		78	75		69	80		**75**			**75**
A.11.4 Control de Acceso a Redes			75	78	81	88		89	80		78	79		**81**			**82**
A.11.5 Control de Acceso al Sistema Operativo			79	74	75	86		68	74		80	89		**78**			**81**
A.11.6 Control de Acceso a la información y a las Aplicaciones			80	80	78	89		68	76		78	90		**80**			**82**
A.11.7 Computación móvil y Trabajo Remoto			78	73	76	78		74	72		73	78		**75**			**75**
6 Identificar y asignar costos																	
SO 4.6.7 Financial management for IT services (as operational activities)						88								**88**		**88**	

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
7 Educar y entrenar a los usuarios																	
DS7.1 Identificación de Necesidades de Entrenamiento y Educación	93		78				89	78	60	65			78	**77**	**75**		
DS7.2 Impartición de Entrenamiento y Educación	84		73				78	72	62	68			85	**75**	**73**		
DS7.3 Evaluación del Entrenamiento Recibido	80		76				78	72	60	67			80	**73**	**72**		
8 Administrar la mesa de servicio y los incidentes																	
SO 4.1 Gestión de eventos		76		77	70	78		73	75	78				**75**		**75**	
SO 4.1.5.3 Detección de eventos		71		75	79	82		76	72	72				**75**		**76**	
SO 4.1.5.4 Filtrado de eventos		75		73	78	80		70	72	71				**74**		**74**	
SO 4.1.5.5 Significado de eventos		78		72	78	83		73	73	73				**76**		**75**	
SO 4.1.5.6 Correlación de eventos		80		75	80	78		78	70	70				**76**		**75**	
SO 4.1.5.7 Trigger		72		71	72	89		72	70	74				**74**		**75**	
SO 4.1.5.8 Respuestas de selección		74		70	74	70		78	67	65				**71**		**71**	
SO 4.1.5.10 Cierre de eventos		79		70	78	78		75	70	73				**75**		**74**	
SO 4.2 Gestión de incidentes		73		81	80	76		77	70	77				**76**		**77**	

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
SO 4.2.5.1 Identificación de Incidentes		75		77	80	89		78	72	78				**78**		**79**	
SO 4.2.5.2 Registro de incidentes		78		71	70	87		78	60	68				**73**		**72**	
SO 4.2.5.3 Categorización de incidentes		75		80	77	79		76	68	68				**75**		**75**	
SO 4.2.5.4 Priorización de incidentes		89		73	78	88		78	75	73				**79**		**78**	
SO 4.2.5.5 Diagnóstico inicial		76		71	80	80		72	70	78				**75**		**75**	
SO 4.2.5.6 Escalasión de incidentes		85		77	90	76		78	75	78				**80**		**79**	
SO 4.2.5.7 Investigación y diagnostico		74		73	80	87		80	68	67				**76**		**76**	
SO 4.2.5.8 Resolución y recuperación		75		72	76	74		75	70	73				**74**		**73**	
SO 4.3.5.1 Menú selección		74		77	70	75		74	70	72				**73**		**73**	
SO 4.2.5.9 Cierre de incidentes		80		71	80	80		78	74	74				**77**		**76**	
SO 4.1.5.9 Revisión y acciones		75		77	78	78		79	70	71				**75**		**75**	
SO 5.9 Soporte Desktop		76		65	75	73		78	72	72				**73**		**73**	
SO 6.2 Service desk		73		60	76	70		78	71	71				**71**		**71**	
9 Administrar la configuración																	
A.11.4 Network access control				78					76			78	76	**77**			**77**
10 Administrar los problemas																	

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
DS10.1 Identificación y clasificación de problemas			75	85	80				65	73			77	**76**	**76**		
DS10.2 Rastreo y resolución de problemas			78	80	89				65	71			76	**77**	**77**		
DS10.3 Cierre de problemas			78	78	78				75	72			78	**77**	**77**		
DS10.4 Integración de las administraciones de cambios, configuración y problemas.			76	74	86				73	70			78	**76**	**76**		
11 Administrar los datos																	
DS11.1 Requerimientos del negocio para Administración de Datos			80						78		73	78	80	**78**	**78**		
DS11.2 Acuerdos de almacenamiento y conservación			79						73		76	75	78	**76**	**76**		
DS11.3 Sistemas de administración de librerías de medidas			75						65		78	73	89	**76**	**76**		
DS11.4 Eliminación			70						65		68	65	66	**67**	**67**		
DS11.5 Respaldo y restauración			79						76		70	75	77	**75**	**75**		
DS11.6 Requerimientos de seguridad para la administración de datos			80						74		71	71	78	**75**	**75**		
12 Administrar el ambiente físico																	
DS12.1 Selección y Diseño del Centro de Datos			65								72		78	**72**	**72**		

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
DS12.2 Medidas de seguridad física			65								77		77	**73**	**73**		
DS12.3 Acceso físico			87								73		78	**79**	**79**		
DS12.4 Protección contra factores ambientales			60								75		89	**75**	**75**		
DS12.5 Administración de instalaciones físicas			78								76		80	**78**	**78**		
13 Administrar las operaciones																	
SO 3.7 Documentación			80	70	80		88		77	78	73	67	89	**78**		**78**	
SO 5 Actividades de operación de servicio común			76	67	78		76		76	70	75	71	76	**74**		**74**	
SO 4.1 Gestión de eventos			78	89	89		72		78	72	71	72	77	**78**		**76**	
SO 4.1.5.1 Ocurrencia de eventos			77	75	87		89		72	71	70	71	76	**76**		**76**	
SO 4.1.5.9 Revisión y acciones			80	77	90		76		65	68	73	73	78	**76**		**77**	
SO 5.2.1 Consola de gestión/puente operaciones			72	80	86		76		74	71	79	70	75	**76**		**76**	
SO 5.2.4 Impresión y salidas			75	70	72		75		72	73	78	70	70	**73**		**73**	
SO 5.3 Gestión mainframe			70	70	79		72		74	74	80	68	71	**73**		**73**	
SO 5.4 Administración de servidores y soporte			76	73	90		77		79	76	85	73	85	**79**		**79**	
SO APENDICE B			80	71	88		72		78	72	71	71	71	**75**		**75**	

PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
EVALUACIÓN A NIVEL DE METAS DE TI	82	79	75	75	79	81	78	77	72	72	75	75	78	77	77	76	78

Tabla 37 Proceso de Evaluación de las Metas TI y Procesos TI para el Departamento Administración Plataformas DSLAMs de la CNT E.P.
Fuente: Autor

- **REVISAR LA EFECTIVIDAD DEL PROGRAMA**

Se describe los **OBJETIVOS DE CONTROL** que se encuentran con un rango de selección *PARCIAL*, menor a **70%** según la escala de valores cuantitativos, en base a la evaluación de las Metas de TI y Proceso TI Tabla 37, que se encuentran identificadas de **COLOR AMARILLO** es decir Parcial (mayor o igual al 25% y menor al 70%) para los cuales se describe las acciones para cada caso.

En relación al proceso **DS1.2 Definición de Servicios** el cumplimiento es parcial en las Metas de TI (MT1) con un valor de 66%. Este objetivo de control está enfocado al portafolio de servicios, debe tener un procedimiento donde socialice e informe al Departamento Administración Plataformas DSLAMs que tipos de servicios van a ser agregados o desagregados en el negocio.

En relación al proceso **A.11.2 Administración de Accesos de Usuarios,** el cumplimiento es parcial en las Metas de TI (MT8) con un 69%. Debido a que no se está cumpliendo con los procedimientos y políticas de acceso, es necesario obtener un chequeo para validar la existencia de un proceso y establecer la mitigación de la administración de acceso de usuarios y activos de la información.

En relación al proceso **A.11.3 Responsabilidades de los Usuarios,** el cumplimiento es parcial en las Metas de TI (MT11) con un 69%, los usuarios no aplican buenas prácticas con los equipos de su administración siendo muy peligroso ya que pueden existir acciones mal intencionadas. Es importante concientizar a los usuarios para asegurar los equipos que no están siendo utilizados, aplicando las políticas y procedimientos como es el bloqueo de las pantallas y cuidado de los mismos que se encuentran a su cargo. Esto ayudara a reducir los riesgos de ataques externos e internos.

En relación al proceso **A.11.5 Control de Acceso al Sistema Operativo,** el cumplimiento es parcial en las Metas de TI (MT8) con un 69%. Ya que los usuarios no aplican los procedimientos en las infraestructuras. Para esto es necesario verificar que todos los sistemas tengan políticas de seguridad y puedan ser aplicadas por los usuarios con la finalidad de prevenir el acceso no autorizado a los sistemas. Controlando el acceso a los servicios de información, identificador único de usuario, administración de contraseñas, tiempos de las sesiones y conexiones seguras.

En relación al proceso **A.11.6 Control de Acceso en la información y a las aplicaciones,** el cumplimiento es parcial en las Metas de TI (MT8) con un 69%. En la actualidad existen sistemas del Departamento Administración Plataformas DSLAMs con un cierto grado de vulnerabilidad, por lo cual, es muy importante realizar escaneos para verificar las inseguridades simulando ataques en los sistemas y de esa manera identificar cuáles son sus debilidades. Una vez identificado, se debe tomar acciones para no permitir el acceso a los sistemas maliciosos, los cuales pueden hacer daño al negocio de Internet/Datos de la CNT E.P.

En relación al proceso **DS7.1 Identificación de Necesidades de Entrenamiento y Educación,** el cumplimiento es parcial en la evaluación a nivel de Metas de TI (MT9) con un 60% y (MT10) con un 65%. Por falta de conocimiento existen errores en el manejo de los sistemas debido a que el personal requiere mejorar el uso de las herramientas que utilizan en el trabajo diario. Por lo cual es indispensable establecer programas de capacitación en base a los temas actuales y futuros del negocio como: valores corporativos, seguridad, redes, hardware, software, aplicaciones y procedimientos del Departamento Administración Plataformas DSLAMs de la CNT E.P. Esto mejorará el proceso del departamento para cumplir con los objetivos de la empresa.

En relación al proceso **DS7.2 Impartición de Entrenamiento y Educación,** el cumplimiento es parcial en las Metas de TI (MT9) con un 62% y (MT10) con un 68%. Debido a que no existe un presupuesto adecuado para el tema de las capacitaciones, por lo cual no todo el personal es beneficiado en los entrenamientos sobre el tema del manejo y administración de las herramientas que son utilizadas para cumplir las funciones asignadas a diario. Por ende es muy importante levantar procesos de entrenamiento donde no influya el presupuesto, tiempo, disponibilidad del personal y que los instructores profundicen en los temas más relevantes en la administración de las herramientas del Departamento Administración Plataformas DSLAMs.

En relación al proceso **DS7.3 Evaluación del Entrenamiento Recibido,** el cumplimiento es parcial en las Metas de TI (MT9) con un 60% y (MT10) con un 67%, Debido a que no se lleva un seguimiento en las capacitaciones inducidas al personal, existen procesos que de alguna manera son repetitivos, por lo cual es necesario, llevar un control al personal que reciba los entrenamientos analizando las evaluaciones y midiendo el grado de conocimiento adquirido.

En relación al proceso **SO 4.1.5.8 Respuestas de selección,** el cumplimiento es parcial en las Metas de TI (MT9) con un 67% y (MT10) con un 65%, debido a que no lleva un registro de todos los eventos de los sistemas de gestión, para el caso de las auditorias es muy necesario llevar los registros de las acciones ejecutadas anteriormente por ende es importante llevar un control por parte del personal del Departamento APD mediante de un sistema de respuestas de selección sobre los eventos presentados.

En relación al proceso **SO 4.2.5.2 Registro de incidentes,** el cumplimiento es parcial en las Metas de TI (MT9) con un 60% y (MT10) con un 68%, en base a que no lleva un sistema de incidentes en el Departamento Administración Plataformas DSLAMs. Pero tiene un personal que se encarga de almacenar y

analizar las alarmas enviadas por los gestores, para luego enviar a las áreas especializadas en el tema, este trabajo lo realiza de forma manual, pero es necesario levantar un sistema automático que registre y pueda estar a la mano de todos los funcionarios que requieran utilizar esta información de las incidencias presentadas en los nodos.

En relación al proceso **SO 4.2.5.3 Categorización de incidentes**, el cumplimiento es parcial en las Metas de TI (MT9) con un 68% y (MT10) con un 68%, debido a que no se lleva un registro de categorización de incidentes fuera de los sistemas de gestión, es importante generar un proceso para la implementación de un sistema que re categorice las incidencias presentadas por niveles en todos los nodos, el sistema debe realizar un análisis de cada registro y categorizar en el nivel correspondiente.

En relación al proceso **SO 4.2.5.7 Investigación y diagnostico** el cumplimiento es parcial en las Metas de TI (MT9) con un 68% y (MT10) con un 67%, debido a que no se lleva una investigación en las incidencias ocurridas en la red del Departamento Administración plataformas DSLAMs, es necesario levantar un procedimiento y cuando exista un diagnostico se debe dar un seguimiento y llevar un histórico de las afectaciones.

En relación al proceso **SO 5.9 Soporte Desktop,** el cumplimiento es parcial en las Metas de TI (MT4) con un 65%, En base a que no se dispone de un servicio de interfaz centralizado y debido a que el Departamento Administración Plataformas DSLAMs no tiene una relación directa con los usuarios. Pero tiene una línea especializada que se encarga de almacenar y analizar todas las solicitudes y requerimientos, para luego enviar a las áreas específicas. Es necesario integrar acuerdos de nivel de servicio en el que interactúe directamente con los usuarios, donde pueda tener muchas opciones de selección en base a los servicios que

presta y en lo posible sea resuelto de forma automática en los sistemas del departamento.

En relación al proceso **SO 6.2 Service Desk,** el cumplimiento es parcial en la evaluación a nivel de las Metas de TI (MT4) con un 60%. Los SLOs no están incluidos en el proceso de Service Desk ya que es un proceso netamente técnico el cual corresponde al Departamento Administración Plataformas DSLAMs, que se encarga de las incidencias reportadas o monitoreadas por el personal responsable que administra los sistemas del departamento.

En relación al proceso **DS10.1 Identificación y clasificación de problemas,** el cumplimiento es parcial en las Metas de TI (MT9) con un 65%. Debido a que no cuenta con un proceso de clasificación de problemas. Es necesario implementar procedimientos en el Departamento Administración DSLAMs para identificar cual es el impacto en la infraestructura o en la red que administra el departamento. Para actuar de mejor manera y para brindar disponibilidad de los servicios.

En relación al proceso **DS10.2 Rastreo y resolución de problemas,** el cumplimiento es parcial en las Metas de TI (MT9) con un 65%. Debido a que todos y cada uno de los sistemas de información, aplicaciones, recursos, servicios y redes de comunicación del Departamento Administración de plataformas DSLAMs CNT E.P. no cuenta con un sistema de auditoria en el desarrollo de sus actividades diarias, por lo cual es muy importante que los usuarios manejen bitácoras o llevar un rastreo continuo de los problemas y levantar un proceso para el departamento.

En relación al proceso **DS11.3 Sistemas de Administración de Librerías de Medidas,** el cumplimiento es parcial en las Metas de TI (MT1) con un 67%. Se debe a que el Departamento Administración Plataformas DSLAMs no cuenta con un sistema de librerías de medidas específicas, por lo cual es importante levantar

un proceso para la implementación de esta herramienta ya que es necesario para mantener a salvo la información de los DSLAMs y llevar un control interno adecuado de toda la información.

En relación al proceso **DS12.1 Selección y Diseño del Centro de Datos** el cumplimiento es parcial en las Metas de TI (MT3) con un 65%, debido a que en el Departamento Administración Plataformas DSLAMs no existe un centro de datos dimensionado y estructurado para la capacidad de información que manejan los servidores de gestión y DSLAMs, por lo cual es necesario levantar un proceso para rediseñar un centro de datos a medida que el negocio lo requiera.

En relación al proceso **DS12.2 Medidas de Seguridad Física** el cumplimiento es parcial en las Metas de TI (MT3) con un 65%, debido a que ciertos equipos se encuentran fuera del perímetro de seguridad del Departamento Administración Plataformas DSLAMs. Se requiere levantar un proceso de seguridad para que se pueda obtener el control de los sitios estén fuera del monitoreo que administra el departamento.

En relación al proceso **DS12.4 Protección Contra Factores Ambientales** el cumplimiento es parcial en las Metas de TI (MT3) con un 60%, el Departamento Administración Plataformas DSLAMs no cuenta con un sistema de monitoreo contra incidencias ambientales como en el caso de inundaciones. Es importante comprar un sistema que mida el nivel ambiental en las centrales y envié un reporte al personal del Departamento APD para que tome las acciones pertinentes del caso.

En relación al proceso **SO 3.7 Documentación** el cumplimiento es parcial en las Metas de TI (MT12) con un 67%. Debido a que no vive una cultura de levantar procedimientos de las actividades que son relacionadas con el Departamento Administración Plataformas DSLAMs o en caso de que exista los procedimientos

no están siendo actualizados. Es necesario levantar una política de creación y modificación de procedimientos o informes en el caso de intervención en los sistemas que maneja el departamento.

En relación al proceso **SO 5 Actividades de operación de servicio común** el cumplimiento es parcial en las Metas de TI (MT4) con un 67%. Esto se debe a que en el Departamento APD no tiene definido un plan de contingencias que apoye al proceso, por lo que es importante delegar esta actividad para que sea desarrollada tomando en cuenta todos los parámetros necesarios de operación.

En relación al proceso **SO 4.1.5.9 Revisión y Acciones,** el cumplimiento es parcial en las Metas de TI (MT9) con un 65% y (MT10) con un 68%. Debido a que registran varios eventos en los sistemas del Departamento Administración Plataformas DSLAMs y notando que no tienen una secuencia de acciones bien definidas y un análisis de sus eventos, por ende es muy necesario levantar un proceso automático para analizar los acontecimientos más relevantes de tal manera que se pueda medir la criticidad y verificar si afecta la operación en los sistemas o en los servicios de los usuarios.

En relación al proceso **SO 5.3 Gestión Mainframe,** el cumplimiento es parcial en las Metas de TI (MT12) con un 68%. Debido a que los sistemas del Departamento Administración Plataformas DSLAMs no cuentan con un sistema centralizado para sus operaciones diarias, por ende es muy importante optar por un sistema gestor de gestores para centralizar todas las plataformas de Internet/Datos y brindar un soporte ágil y oportuno a todos sus usuarios y previniendo la pérdida de su servicio.

2.3.5.5 VOLVER OPERATIVA LA SOLUCIÓN

La retroalimentación es muy importante en los procesos definidos en la implementación, por ende es necesario el monitoreo de las mejoras para construir la sostenibilidad e identificar nuevos requerimientos de gobernabilidad.

- **CONSTRUIR LA SOSTENIBILIDAD**

Mejorar la estructura de la organización en base a cada uno de los procesos, roles y responsabilidades con el personal del Departamento Administración Plataformas DSLAMs y la gerencia de la CNT E.P.

Identificados los nuevos objetivos de gobernabilidad en base a la experiencia del personal del Departamento APD se llegara a un acuerdo en lo que compete a las necesidades y establecer objetivos y prioridades.

Para construir la matriz RACI se define quien es Responsable (R), quien debe rendir cuentas (A), quien debe ser consultado (C) y o Informado (I) para este proyecto, ver Tabla 38.[8]

ACTIVIDADES	GERENTE NACIONAL	GERENTE O&M	JEFATURA APD	ANALISTA O&M
Establecer estructura organizacional de TI, incluyendo comités y ligas a los interesados y proveedores	I	R	I/R	A
Diseñar marco de trabajo para el proceso de TI	I	I/C	R	A
Identificar dueños de sistemas	I	I	R	R
Identificar dueños de datos	I	I	A	R
Establecer e implantar roles y responsabilidades de TI, incluida la supervisión y segregación de funciones	I	I/C	A/R	I/R

Tabla 38 Roles y Responsabilidades Administración Plataformas DSLAMs
Fuente: IT Governance Institute - cobit 4.1

Utilizando los procedimientos, políticas, acuerdos y compromisos se dará a conocer a cada gerente, ingeniero o técnico para la ejecución en la implementación de los procesos de gobernabilidad de las Tecnologías de la Información para el Departamento APD.

- **IDENTIFICAR NUEVOS REQUERIMIENTOS DE GOBERNABILIDAD**

Con el resultado de la evaluación planteada en la Tabla 37 se determina el cumplimiento de la propuesta de Gobierno de Tecnologías de Información con un grado de 77% como se muestran en la Figura 21, de esta manera podemos verificar los nuevos requerimientos de gobernabilidad.

Figura 21 Control del Grado de Madurez de los Procesos Departamento APD

Fuente: Autor

La identificación de los requerimientos de gobernabilidad se basa en la tabla 37 de este documento con la evaluación de la propuesta de las Metas de TI, Proceso de TI y los objetivos de control COBIT “entrega y Dar Soporte”, ITIL “Operación del Servicio” e ISO 27001 “Control de Acceso” y fundamentándonos en los procesos TI DSLAMs**,** podemos verificar que en la Figura 21 tenemos dos objetivos de control **(DS4.9 Almacenamiento de respaldos fuera de las instalaciones y DS11.4 Eliminación)** que se encuentran con un rango de selección *PARCIAL*, es decir, menor a **70%** según la escala de valores cuantitativos y **evaluación a nivel de proceso.**

- **GARANTIZAR LA CONTINUIDAD DEL SERVICIO**

  - ✓ **DS4.9 Almacenamiento de respaldos fuera de las instalaciones**

Respecto al proceso DS4.9 Almacenamiento de respaldos fuera de las instalaciones, el grado de cumplimiento es parcial con un 61% y en base a las Metas de TI. Esto se debe a que los respaldos que se realizan se encuentran en la misma localidad geográfica, por lo que es importante definir una política que garantice la recuperación y la integridad de la información mediante el uso de las redes y la infraestructura de la Corporación Nacional de Telecomunicaciones E.P, utilizando sistemas y aplicaciones de apoyo que garanticen estos procedimientos por medio del personal del Departamento Administración de plataformas DSLAMs.

- **ADMINISTRAR LOS DATOS**

  - ✓ **DS11.4 Eliminación**

En relación al proceso DS11.4 Eliminación, el cumplimiento es parcial en la evaluación a nivel de proceso TI y metas de TI con un 67%. Este objetivo de control es muy delicado debido a que un mal procedimiento en la eliminación puede influir mucho en el funcionamiento de los sistemas, por ende es necesario implementar procedimientos que sean ejecutados por el personal del Departamento Administración Plataformas DSLAMs, obteniendo de esta manera una administración consolidada en todos sus sistemas.

CAPÍTULO 3

EVALUACIÓN DE LA APLICABILIDAD DE LA PROPUESTA PARA EL DEPARTAMENTO ADMINISTRACIÓN PLATAFORMAS DSLAMs DE LA CNT E.P.

3.1 APLICACIÓN DE LA PROPUESTA

La aplicación de la propuesta se basa en el grupo de actividades “Implementar la Solución” del punto 2.3.5.4 de este documento, el cual contiene las siguientes actividades:

Implementar las Mejoras: Definiendo una escala de valores y estableciendo un rango de selección para evaluar los procesos de Gobierno de TI.

Monitorear el Desempeño de la Implementación: Evaluando los procesos definidos en la propuesta de gobierno de TI otorgando valores cuantitativos y cualitativos.

Revisar la Efectividad del Programa: Se describe los objetivos de control que se encuentran con un rango de selección parcial es decir menor a 70% según la escala de valores cuantitativos del Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.

Por lo expuesto anteriormente se puede determinar que la Aplicación de la Propuesta es aceptable para los procesos que superan el 70% según el grado de cumplimiento.

A continuación un resumen a nivel de proceso de la aplicación de la propuesta, como se puede apreciar en la Tabla 39 el grado de cumplimiento es mayor a 70%.

PROCESOS TI	EVALUACIÓN A NIVEL DE PROCESO
1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO	81
2 ADMINISTRAR LOS SERVICIOS DE TERCEROS	81
3 ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD	77
4 GARANTIZAR LA CONTINUIDAD DEL SERVICIO	77
5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	77
6 IDENTIFICAR Y ASIGNAR COSTOS	88
7 EDUCAR Y ENTRENAR A LOS USUARIOS	75
8 ADMINISTRAR LA MESA DE SERVICIO Y LOS INCIDENTES	75
9 ADMINISTRAR LA CONFIGURACIÓN	77
10 ADMINISTRAR LOS PROBLEMAS	76
11 ADMINISTRAR LOS DATOS	75
12 ADMINISTRAR EL AMBIENTE FÍSICO	75
13 ADMINISTRAR LAS OPERACIONES	76

Tabla 39 Resumen de aceptación de la aplicación de la propuesta

La aplicabilidad de la Propuesta del Gobierno de TI del Departamento Administración Plataformas DSLAMs se ha evaluado con los dominios/procesos/controles de COBIT, ITIL v3 e ISO 27001 descrito en el Capítulo 2. Como se ilustra en la Figura 22, el porcentaje de cumplimiento de los dominios es mayor a 70% según el rango de selección y nivel de aceptación para cada proceso y actividad del Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.

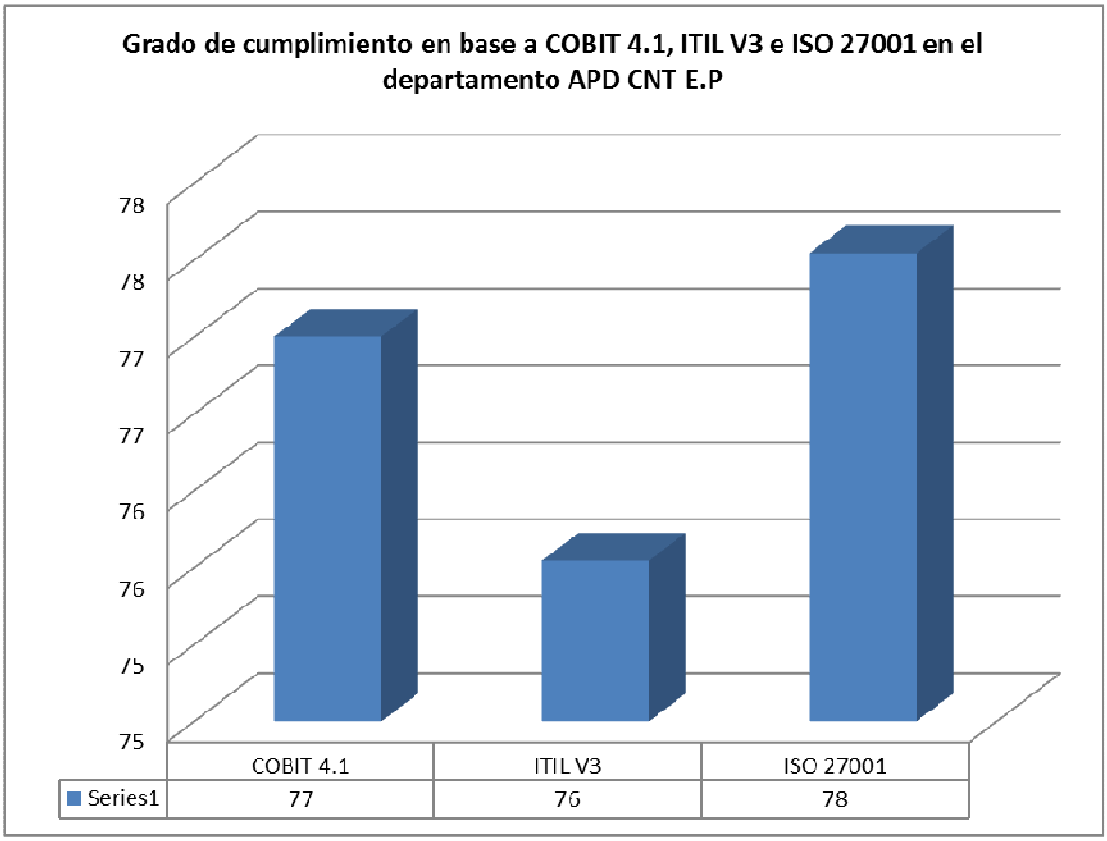


Figura 22 Grado de cumplimiento en base a COBIT 4.1, ITIL V3 e ISO 27001 en el departamento APD CNT E.P

Por lo expuesto, el Gobierno de TI fue diseñado para cubrir las siguientes expectativas del Departamento APD.

- Aumentar el promedio del grado de madurez de los procesos del Departamento Administración Plataformas DSLAMs.
- Educar al personal del Departamento Administración Plataformas DSLAMs para que acojan las bondades que tiene TI y apoyen en el liderazgo de la gobernabilidad de los objetivos y estrategias en los procesos.
- Los procesos deben estar bien definidos para todos los usuarios tanto internos como externos.

- Los roles y responsabilidades deben ser involucrados con todo el personal del Departamento Administración Plataformas DSLAMs.
- Mejorar continuamente los procesos que requiere el Departamento Administración Plataformas DSLAMs.

Aplicada la propuesta se puede verificar el grado de madurez en base a los resultados obtenidos en la evaluación de la aplicabilidad del Gobierno de TI del Departamento Administración Plataformas DSLAMs.

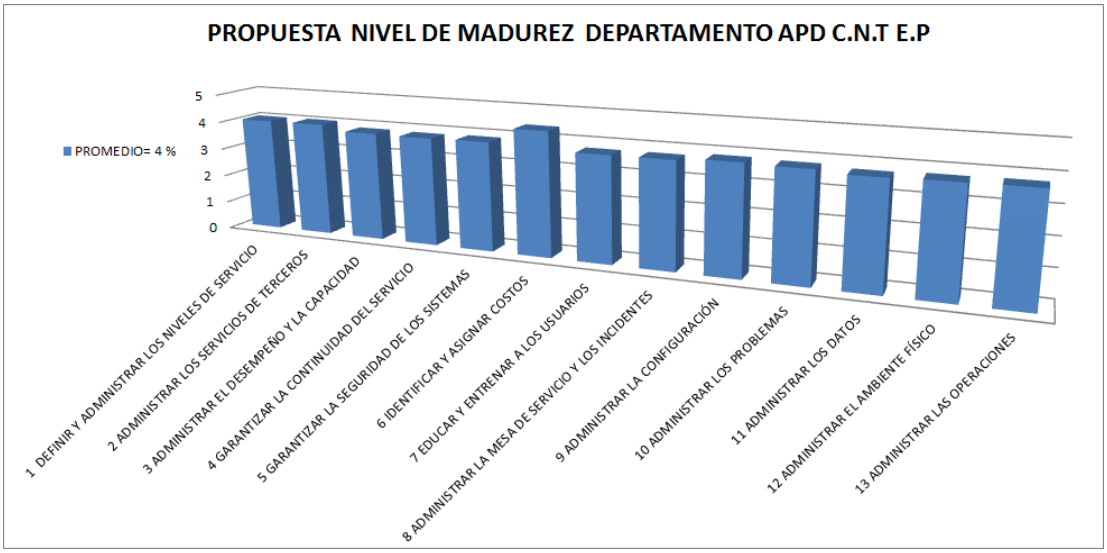


Figura 23 Grado de Madurez propuesto del Departamento APD CNT E.P.

En la Figura 23 se ilustra que el Departamento Administración Plataformas DSLAMs se encuentra en promedio con un grado de Madurez que se ubica en el **nivel 4, es decir los procesos se mantiene y miden**, lo que hace que la propuesta sea aplicable.

3.2 ANÁLISIS DE RESULTADOS

Los PROCESOS descritos en la Tabla 37 fluyen de manera transparente, continúa y segura debido al rango de selección CUMPLE, es decir, mayor a 70% según la escala de valores cuantitativos de la EVALUACIÓN A NIVEL DE PROCESO, con esta definición se ha determinado el CUMPLIMIENTO de los procedimientos para el Gobierno de TI del Departamento Administración de Plataformas DSLAMs de la CNT E.P.

Se realizará el análisis de resultados de la evaluación de las Metas de TI y Procesos de TI, en base a los resultados de la Tabla 37 y de la aplicabilidad de la propuesta para el Departamento Administración Plataformas DSLAMs de la CNT E.P.

A continuación, en la Figura 24 se muestran los resultados de la evaluación de la aplicabilidad de la propuesta para el Departamento Administración Plataformas DSLAMs, para la propuesta de Gobierno de TI:

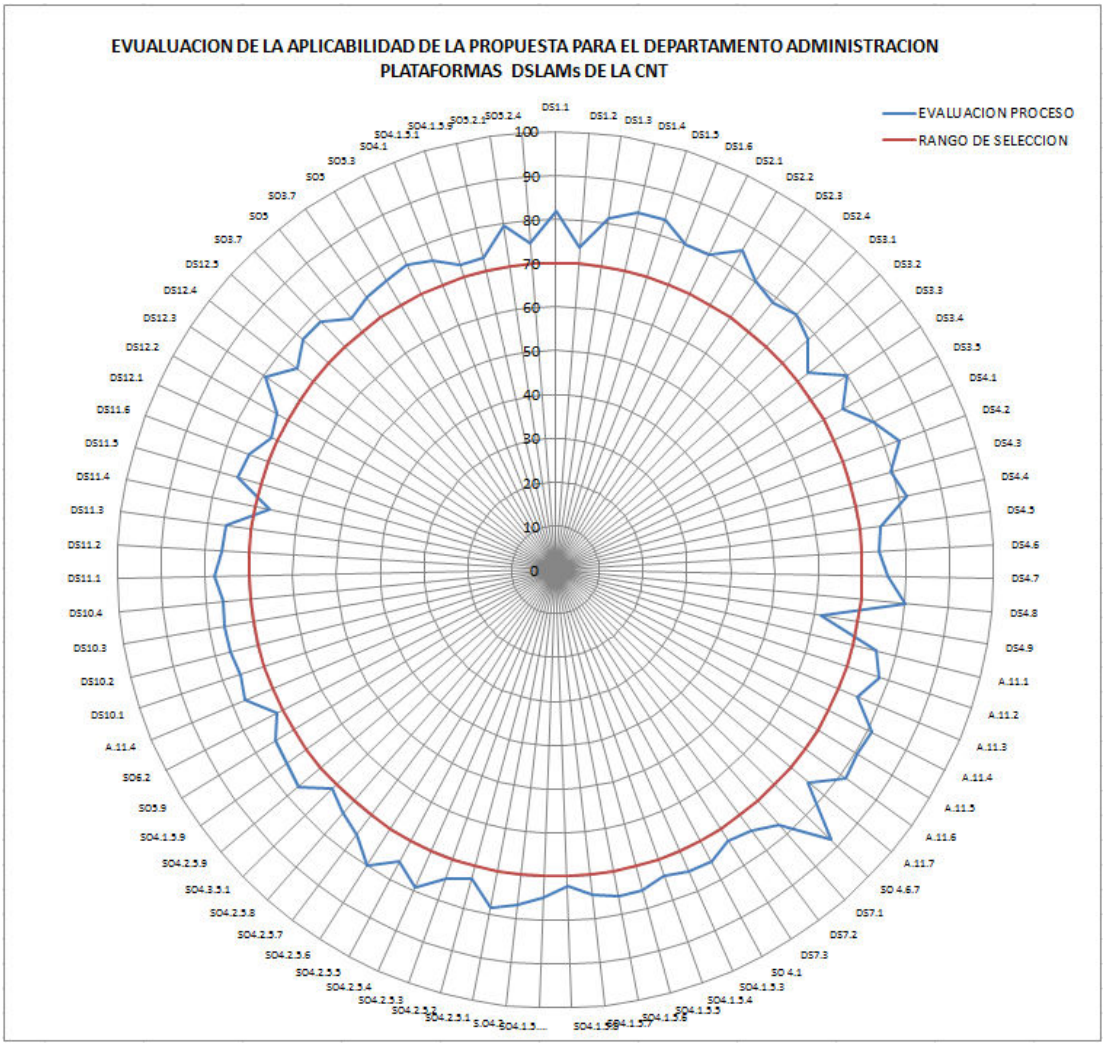


Figura 24 Evaluación de la aplicabilidad de la propuesta para el Departamento Administración Plataformas DSLAMs de la CNT E.P.

De esta manera se puede determinar para la **Propuesta de Gobierno de TI** es necesario **mitigar y controlar** los riesgos existes en los procesos de TI DSLAMs identificados en esta investigación, con un rango de selección menor a 70% "PARCIAL" en los procesos del Departamento Administración Plataformas DSLAMs descritos en este documento.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- La propuesta de Gobierno de TI para el Departamento de Administración de Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P. se basa en Metas de Negocio (MN), Metas de TI (MT) y Procesos TI (PT) con COBIT en el dominio de "Entregar y dar Soporte", en cuanto a ITIL se basa en las mejores prácticas de la "Operación del Servicio", y en cuanto a la ISO-27001 se enfoca en las actividades de "Control de acceso". Con los estándares mencionados se obtiene el promedio de **77%** en el rango de selección de valores cuantitativos, proporcionando el grado de **CUMPLIMIENTO** en base a los valores cualitativos tomados para esta investigación, por ende se puede verificar que la mayoría de los procesos del departamento cumplen con sus objetivos.
- La efectividad de las mejores prácticas depende de cómo se implementan y mantienen en el Departamento Administración Plataformas DSLAMs.
- Una vez realizada la evaluación de la propuesta de Gobierno, definida en esta investigación y en base a la Figura 24, se obtuvo un análisis específico de los resultados para obtener un panorama completo del estado del Departamento Administración Plataformas DSLAMs de la CNT E.P, con el fin de establecer lineamientos para alcanzar servicios de (Internet/Datos) de acuerdo con las prioridades del negocio, medir la capacidad y el rendimiento de los sistemas y alcanzar confidencialidad, integridad y disponibilidad en los sistemas.

4.2 RECOMENDACIONES

- A fin de proteger la información es necesario garantizar el cumplimiento de políticas y procedimientos que se determinen para el Departamento Administración Plataformas DSLAMs, con un adecuado monitoreo que permita optimizar recursos y alcanzar los objetivos del negocio Internet/Datos.
- Es muy importante que se actualice periódicamente la Propuesta de Gobierno de Tecnologías de la Información de tal manera que se genere conocimientos adecuados en los escenarios del Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.
- Para el Entrenamiento y Educación del personal es importante la identificación de necesidades en los elementos de TI DSLAMs, para levantar programas de entrenamiento en base a los sistemas actuales y futuros del Departamento Administración Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P.
- Para el entrenamiento del plan de continuidad de las Metas de TI y Procesos TI DSLAMs, se debe manejar roles y responsabilidades en base a un desastre o incidencia y brindar capacitaciones en base a los resultados que se determinen.
- Para precautelar la confidencialidad e integridad de la información del Departamento Administración Plataformas DSLAMs es necesario garantizar el cumplimiento de los procedimientos a implementarse.
- Los procesos que tienen un grado de cumplimiento menor a 70% del Departamento de Administración de Plataformas DSLAMs de la Corporación Nacional de Telecomunicaciones E.P., deben ser revisados y controlados, siguiendo un ciclo de mejora continua.

- Se debe realizar continuos análisis de riesgos en los sistemas de las plataformas DSLAMs, y en base a los resultados se implementará procedimientos de mitigación.

REFERENCIAS BIBLIOGRÁFICAS

[1] Universidad Nacional de Luján - Departamento de Seguridad Informática, "Material adicional del Seminario Taller Riesgo vs. Seguridad de la Información,".

[2] Intranet CNT E.P. (2014, septiembre) Sistema MAI, cnt e.p. [Online]. HYPERLINK " http://vmwiso01.andinatel.int/27000/27000/sdi/index.php" http://vmwiso01.andinatel.int/27000/27000/sdi/index.php

[3] Cnt E.P, "Departamento administración plataformas DSLAM," Corporación Nacional de Telecomunicaciones E.P., Quito, 2014.

[4] Razieh Sheikhpour and Modiri Nasser, An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls. Madrid, 2012.

[5] IT GOVERNANCE INSTITUTE, "Board Briefing on IT Governance," in Reunión Informativa del Consejo sobre la Gobernabilidad TI., 2001.

[6] IT GOVERNANCE INSTITUTE, Governance Implementation Guide: Using Cobit and Val IT, 2nd ed.

[7] IT GOVERNANCE INSTITUTE, Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2.: OFFICE OF GOVERNMENT COMMERCE, 2008.

[8] ISACA IT GOVERNANCE INSTITUTE. (2013, JULIO) COBIT 4.1. [Online]. HYPERLINK "http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf" http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf

[9] Alejandro Corletti Estrada. (2006, DICIEMBRE) ISO-27001: LOS CONTROLES (Parte II). [Online]. HYPERLINK "http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf" http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_II.pdf

[10] Sharon OGC Taylor, ITIL V3 Service Operation.

[11] ep cnt. (2014, Septiembre) mision-vision-y-estructura. [Online]. HYPERLINK "http://www.cnt.com.ec/" http://www.cnt.com.ec/

[12] IT GOBERNANCE INSTITUTE, Cobit Mapping of ITIL V3 with COBIT 4.1., 2008.

ANEXOS

ANEXO 1. MAPEO COBIT 4.1 (Entregar y Dar Soporte) Vs. ITIL V3 (Operación del Servicio)

MAPEO COBIT - ITIL		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3**	**VALOR**
DS1 Definir y administrar los niveles de servicio		**50**
DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio	OTRO DOMINIO/PROCESO DE ITIL	50
DS1.2 Definición de Servicios	OTRO DOMINIO/PROCESO DE ITIL	50
DS1.3 Acuerdos de Niveles de Servicio	OTRO DOMINIO/PROCESO DE ITIL	50
DS1.4 Acuerdos de Niveles de Operación	OTRO DOMINIO/PROCESO DE ITIL	50
DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	OTRO DOMINIO/PROCESO DE ITIL	50
DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	OTRO DOMINIO/PROCESO DE ITIL	50
DS2 Administrar los servicios de terceros		**50**
DS2.1 Identificación de todas las relaciones con proveedores	OTRO DOMINIO/PROCESO DE ITIL	50
DS2.2 Gestión de relaciones con proveedores	OTRO DOMINIO/PROCESO DE ITIL	50
DS2.3 Administración de riesgos del proveedor	OTRO DOMINIO/PROCESO DE ITIL	50
DS2.4 Monitoreo del desempeño del proveedor	OTRO DOMINIO/PROCESO DE ITIL	50
DS3 Administrar el desempeño y la capacidad		**50**
DS3.1 Planeación del desempeño y la capacidad	OTRO DOMINIO/PROCESO DE ITIL	50
DS3.2 Capacidad y desempeño actual	OTRO DOMINIO/PROCESO DE ITIL	50
DS3.3 Capacidad y desempeño futuros	OTRO DOMINIO/PROCESO DE ITIL	50
DS3.4 Disponibilidad de recursos de TI	OTRO DOMINIO/PROCESO DE ITIL	50
	OTRO DOMINIO/PROCESO DE ITIL	50
DS4 Garantizar la continuidad del servicio		**50**
DS4.1 Marco de trabajo de continuidad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.2 Planes de continuidad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.3 Recursos críticos de TI	OTRO DOMINIO/PROCESO	50

MAPEO COBIT - ITIL		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3**	**VALOR**
	DE ITIL	
DS4.4 Mantenimiento de plan de continuidad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.5 Pruebas del plan de continuidad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.6 Entrenamiento del plan de continuidad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.7 Distribución del plan de continuidad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.8 Recuperación y reanudación de los servicios de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS4.9 Almacenamiento de respaldos fuera de las instalaciones	SO 5.2.3	100
DS5 Garantizar la seguridad de los sistemas		**63.63**
DS5.1 Administración de la seguridad de TI	SO 5.13	100
DS5.2 Plan de seguridad de TI	OTRO DOMINIO/PROCESO DE ITIL	50
DS5.3 Administración de Identidad	SO 4.5	100
DS5.4 Administración de cuentas de usuario	SO 4.5, SO 4.5.5.1, SO 4.5.5.2, SO 4.5.5.3, SO 4.5.5.4, SO 4.5.5.5, SO 4.5.5.6	100
DS5.5 Pruebas, vigilancia y monitoreo de la seguridad	SO 4.5.5.6, SO 5.13	100
DS5.6 Definición de incidentes de seguridad	OTRO DOMINIO/PROCESO DE ITIL	50
DS5.7 Protección de la tecnología de seguridad	SO 5.4	100
DS5.8 Administración de llaves criptográficas	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS5.9 Prevención, Detención y corrección de software malicioso	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS5.10 Seguridad de la red	SO 5.5	100
DS5.11 Intercambio de datos sensitivos	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS6 Identificar y asignar costos		**100**
DS6.1 Definición de servicios	SO 4.6.7	100
DS3.5 Monitoreo y reportes	SO 4.6.7	100
DS6.3 Modelación de costos y cargos	SO 4.6.7	100
DS6.4 Mantenimiento del modelo de costos	SO 4.6.7	100
DS7 Educar y entrenar a los usuarios		
DS7.1 Identificación de Necesidades de Entrenamiento y Educación	SO 5.13, SO 5.14	100
DS7.2 Impartición de Entrenamiento y Educación	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS7.3 Evaluación del Entrenamiento Recibido	NO EXISTE PROCESO/CONTROL EN ITIL	0

MAPEO COBIT - ITIL		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3**	**VALOR**
DS8 Administrar la mesa de servicio y los incidentes		**33.33**
DS8.1 Mesa de servicio	SO 4.1, SO 4.2, SO 6.2	100
DS8.2 Registro de consultas de clientes	SO 4.1.5.3, SO 4.1.5.4, SO 4.1.5.5, SO 4.1.5.6, SO 4.1.5.7, SO 4.2.5.1, SO 4.2.5.2, SO 4.2.5.3, SO 4.2.5.4, SO 4.2.5.5, SO 4.3.5.1	100
DS8.3 Escalamiento de incidentes	SO 4.1.5.8, SO 4.2.5.6, SO 4.2.5.7, SO 4.2.5.8, SO 5.9	100
DS8.4 Cierre de incidentes	SO 4.1.5.10, SO 4.2.5.9	100
DS8.5 Análisis de tendencias	SO 4.1.5.9	100
DS9 Administrar la configuración		**66.66**
DS9.1 Repositorio y Línea Base de configuración	OTRO DOMINIO/PROCESO DE ITIL	50
DS9.2 Identificación y Mantenimiento de elementos de configuración	OTRO DOMINIO/PROCESO DE ITIL	50
DS9.3 Revisión de integridad de la configuración	SO 5.4, SO 7, SO 7.1.4	100
DS10 Administrar los problemas		**75**
DS10.1 Identificación y clasificación de problemas	SO 4.4.5.1, SO 4.4.5.3, SO 4.4.5.4	100
DS10.2 Rastreo y resolución de problemas	SO 4.4.5.2, SO 4.4.5.5, SO 4.4.5.6, SO 4.4.5.7, SO 4.4.5.8	100
DS10.3 Cierre de problemas	SO 4.4.5.9, SO 4.4.5.10	100
DS10.4 Integración de las administraciones de cambios, configuración y problemas.	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS11 Administrar los datos		**50**
DS11.1 Requerimientos del Negocio para Administración de Datos	OTRO DOMINIO/PROCESO DE ITIL	50
DS11.2 Acuerdos de Almacenamiento y Conservación	SO 5.6	100
DS11.3 Sistemas de Administración de Librerías de Medidas	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS11.4 Eliminación	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS11.5 Respaldo y Restauración	SO 5.2.3	100
DS11.6 Requerimientos de Seguridad para la Administración de Datos	OTRO DOMINIO/PROCESO DE ITIL	50
DS12 Administrar el ambiente físico		**80**
DS12.1 Selección y Diseño del Centro de Datos	NO EXISTE PROCESO/CONTROL EN ITIL	0
DS12.2 Medidas de Seguridad Física	SO Apéndice E	100
DS12.3 Acceso Físico	SO Apéndice E, SO Apéndice	100

MAPEO COBIT - ITIL		
COBIT 4.1 - ENTREGAR Y DAR SOPORTE (DS)	**ITIL V3**	**VALOR**
	F	
DS12.4 Protección Contra Factores Ambientales	SO Apéndice E	100
DS12.5 Administración de Instalaciones Físicas	SO 5.12	100
DS13 Administrar las operaciones		**100**
DS13.1 Procedimientos e instrucciones de operación	SO 3.7, SO 5, SO APENDICE B	100
DS13.2 Programación de tareas	SO 5.3	100
DS13.3 Monitoreo de la infraestructura de TI	SO 4.1, SO 4.1.5.1, SO 4.1.5.9, SO 5.2.1	100
DS13.4 Documentos sensitivos y dispositivos de salida	SO 5.2.4	100
DS13.5 Mantenimiento preventivo del hardware	SO 5.3, SO 5.4	100
	PROMEDIO DE ALCANCE	**67%**

ANEXO 2. MAPEO COBIT 4.1 (Entregar y Dar Soporte) Vs. ISO 27001 (Control de Acceso)

MAPEO COBIT - ISO 27001		
COBIT 4.1 – ENTREGAR Y DAR SPORTE	**ISO 27001 (A.11)**	**VALOR**
DS1 Definir y administrar los niveles de servicio	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS2 Administrar los servicios de terceros	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS3 Administrar el desempeño y la capacidad	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS4 Garantizar la continuidad del servicio	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS5 Garantizar la seguridad de los sistemas	A.11.1 Business requirement for access control A.11.2 User access management A.11.3 User responsibilities A.11.4 Network access control A.11.5 Operating system access control A.11.6 Application and information access control A.11.7 Mobile computing and teleworking	100
DS6 Identificar y asignar costos	NO EXISTE CONTROL EN LA ISO 27001	0

DS7 Educar y entrenar a los usuarios	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS8 Administrar la mesa de servicio y los incidentes	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS9 Administrar la configuración	A.11.4 Network access control	100
DS10 Administrar los problemas	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS11 Administrar los datos	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS12 Administrar el ambiente físico	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
DS13 Administrar las operaciones	OTRO DOMINIO/PROCESO DE LA ISO 27001	50
	PROMEDIO DE ALCANCE	**54%**

ANEXO 3. ISACA, Board Briefing on IT Governance.

Incluido en CD.

ANEXO 4. Evaluación de Metas TI y Procesos TI del departamento Administración Plataformas DSLAMs

	PROCESOS TI / METAS DE TI	MT1	MT2	MT3	MT4	MT5	MT6	MT7	MT8	MT9	MT10	MT11	MT12	MT13	EVALUACION A NIVEL DE PROCESO	COBIT 4.1	ITIL V3	ISO 27001
	1 Definir y administrar los niveles de servicio																	
DS1.1	DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio	83	85				78								**82**	**82**		
DS1.2	DS1.2 Definición de Servicios	66	75				80								**74**	**74**		
DS1.3	DS1.3 Acuerdos de Niveles de Servicio	87	80				76								**81**	**81**		
DS1.4	DS1.4 Acuerdos de Niveles de Operación	90	76				85								**84**	**84**		
DS1.5	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio	87	78				86								**84**	**84**		
DS1.6	DS1.6 Revisión de los acuerdos de niveles de servicio y de los contratos	76	77				87								**80**	**80**		
	2 Administrar los servicios de terceros																	
DS2.1	DS2.1 Identificación de todas las relaciones con proveedores	80	74		86										**80**	**80**		
DS2.2	DS2.2 Gestión de relaciones con proveedores	88	85		80										**84**	**84**		
DS2.3	DS2.3 Administración de riesgos del proveedor	75	88		78										**80**	**80**		

DS2.4	DS2.4 Monitoreo del desempeño del proveedor	73	89		74										**79**	**79**		
	3 Administrar el desempeño y la capacidad																	
DS3.1	DS3.1 Planeación del desempeño y la capacidad			80											**80**	**80**		
DS3.2	DS3.2 Capacidad y desempeño actual			78											**78**	**78**		
DS3.3	DS3.3 Capacidad y desempeño futuros			73											**73**	**73**		
DS3.4	DS3.4 Disponibilidad de recursos de TI			80											**80**	**80**		
DS3.5	DS3.5 Monitoreo y reportes			75											**75**	**75**		
	4 Garantizar la continuidad del servicio																	
DS4.1	DS4.1 Marco de trabajo de continuidad de TI		80	78		84				78					**80**	**80**		
DS4.2	DS4.2 Planes de cotinuidad de TI		90	85		80				80					**84**	**84**		
DS4.3	DS4.3 Recursos críticos de TI		90	78		75				76					**80**	**80**		
DS4.4	DS4.4 Mantenimiento de plan de continuidad de TI		95	75		78				80					**82**	**82**		
DS4.5	DS4.5 Pruebas del plan de continuidad de TI		76	70		75				78					**75**	**75**		
DS4.6	DS4.6 Entrenamiento del plan de continuidad de TI		70	73		80				73					**74**	**74**		
DS4.7	DS4.7 Distribución del plan de continuidad de TI		76	72		85				70					**76**	**76**		
DS4.8	DS4.8 Recuperación y reanudación de los servicios de TI		96	75		77				73					**80**	**80**		
DS4.9	DS4.9 Almacenamiento de respaldos fuera de las instalaciones		56	50		78									**61**	**61**		
	5 Garantizar la seguridad de los sistemas																	
A.11.1	A.11.1 Requerimiento de negocio de control de acceso			75	76	72	78		78	73		76	76		**76**			**76**
A.11.2	A.11.2 Administración de Accesos de Usuarios			70	80	81	84		69	78		78	79		**77**			**78**
A.11.3	A.11.3 Responsabilidades de			73	70	73	78		78	75		69	80		**75**			**75**

	los usuario																	
A.11.4	A.11.4 Control de acceso a red			75	78	81	88		89	80		78	79		**81**			**82**
A.11.5	A.11.5 Control de acceso del sistema operativo			79	74	75	86		69	74		80	89		**78**			**78**
A.11.6	A.11.6 Control de Acceso en la información y a las aplicaciones			80	80	78	89		69	76		78	90		**80**			**80**
A.11.7	A.11.7 Computación móvil y el teletrabajo			78	73	76	78		74	72		73	78		**75**			**75**
	6 Identificar y asignar costos																	
SO 4.6.7	SO 4.6.7 Financial management for IT services (as operational activities)						88								**88**		**88**	
	7 Educar y entrenar a los usuarios																	
DS7.1	DS7.1 Identificación de Necesidades de Entrenamiento y Educación	93		78				89	78	60	65			78	**77**	**75**		
DS7.2	DS7.2 Impartición de Entrenamiento y Educación	84		73				78	72	62	68			85	**75**	**73**		
DS7.3	DS7.3 Evaluación del Entrenamiento Recibido	80		76				78	72	60	67			80	**73**	**72**		
	8 Administrar la mesa de servicio y los incidentes																	
SO 4.1	SO 4.1 gestión de eventos		76		77	70	78		73	75	78				**75**		**75**	
SO4.1.5.3	SO 4.1.5.3 Detección de eventos		71		75	79	82		76	72	72				**75**		**76**	
SO4.1.5.4	SO 4.1.5.4 Filtrado de eventos		75		73	78	80		70	72	71				**74**		**74**	
SO4.1.5.5	SO 4.1.5.5 Significado de eventos		78		72	78	83		73	73	73				**76**		**75**	
SO4.1.5.6	SO 4.1.5.6 Correlación de eventos		80		75	80	78		78	70	70				**76**		**75**	
SO4.1.5.7	SO 4.1.5.7 Trigger		72		71	72	89		72	70	74				**74**		**75**	
SO4.1.5.8	SO 4.1.5.8 Respuestas de selección		74		70	74	70		78	67	65				**71**		**71**	
SO4.1.5.10	SO 4.1.5.10 Cierre de eventos		79		70	78	78		75	70	73				**75**		**74**	
S.O4.2	SO 4.2 Gestión de incidentes		73		81	80	76		77	70	77				**76**		**77**	
SO4.2.5.1	SO 4.2.5.1 identificación de		75		77	80	89		78	72	78				**78**		**79**	

	Incidentes																		
SO4.2.5.2	SO 4.2.5.2 Registro de incidentes		78		71	70	87		78	60	68				**73**		**72**		
SO4.2.5.3	SO 4.2.5.3 Categorización de incidentes		75		80	77	79		76	68	68				**75**		**75**		
SO4.2.5.4	SO 4.2.5.4 Priorización de incidentes		89		73	78	88		78	75	73				**79**		**78**		
SO4.2.5.5	SO 4.2.5.5 Diagnóstico inicial		76		71	80	80		72	70	78				**75**		**75**		
SO4.2.5.6	SO 4.2.5.6 Escalación de incidentes		85		77	90	76		78	75	78				**80**		**79**		
SO4.2.5.7	SO 4.2.5.7 Investigación y diagnostico		74		73	80	87		80	68	67				**76**		**76**		
SO4.2.5.8	SO 4.2.5.8 Resolución y recuperación		75		72	76	74		75	70	73				**74**		**73**		
SO4.3.5.1	SO 4.3.5.1 Menú selección		74		65	70	75		74	70	72				**71**		**71**		
SO4.2.5.9	SO 4.2.5.9 Cierre de incidentes		80		71	80	80		78	74	74				**77**		**76**		
SO4.1.5.9	SO 4.1.5.9 Revisión y acciones		75		77	78	78		79	70	71				**75**		**75**		
SO5.9	SO 5.9 soporte Desktop		76		77	75	73		78	72	72				**75**		**75**		
SO6.2	SO 6.2 Service desk		73		60	76	70		78	71	71				**71**		**71**		
	9 Administrar la configuración																		
A.11.4	A.11.4 Network access control				78					76			78	76	**77**			**77**	
	10 Administrar los problemas																		
DS10.1	DS10.1 Identificación y clasificación de problemas			75	85	80				65	73			77	**76**	**76**			
DS10.2	DS10.2 Rastreo y resolución de problemas			78	80	89				65	71			76	**77**	**77**			
DS10.3	DS10.3 Cierre de problemas			78	78	78				75	72			78	**77**	**77**			
DS10.4	DS10.4 Integración de las administraciones de cambios, configuración y problemas.			76	74	86				73	70			78	**76**	**76**			
	11 Administrar los datos																		
DS11.1	DS11.1 Requerimientos del Negocio para Administración de Datos			80						78		73	78	80	**78**	**78**			
DS11.2	DS11.2 Acuerdos de			79						65		76	75	78	**75**	**75**			

	Almacenamiento y Conservación																	
DS11.3	DS11.3 Sistemas de Administración de Librerias de Medidas			75						73		78	73	89	**78**	**78**		
DS11.4	DS11.4 Eliminación			70						65		68	65	66	**67**	**67**		
DS11.5	DS11.5 Respaldo y Restauración			79						76		70	75	77	**75**	**75**		
DS11.6	DS11.6 Requerimientos de Seguridad para la Administración de Datos			80						74		71	71	78	**75**	**75**		
	12 Administrar el ambiente físico																	
DS12.1	DS12.1 Selección y Diseño del Centro de Datos			65								72		78	**72**	**72**		
DS12.2	DS12.2 Medidas de Seguridad Física			65								77		77	**73**	**73**		
DS12.3	DS12.3 Acceso Físico			87								73		78	**79**	**79**		
DS12.4	DS12.4 Protecccción Contra Factores Ambientales			60								75		89	**75**	**75**		
DS12.5	DS12.5 Administración de Instalaciones Físicas			78								76		80	**78**	**78**		
	13 Administrar las operaciones																	
SO3.7	SO 3.7 Documentación			80	70	80		88		77	78	73	67	89	**78**		**78**	
SO5	SO 5 Actividades de operación de servicio común			76	67	78		76		76	70	75	71	76	**74**		**74**	
SO4.1	SO 4.1 gestión de eventos			78	89	89		72		65	68	71	72	77	**76**		**76**	
SO4.1.5.1	SO 4.1.5.1 Ocurrencia de eventos			77	75	87		89		72	71	70	71	76	**76**		**76**	
SO4.1.5.9	SO 4.1.5.9 Revisión y acciones			80	77	90		76		78	72	73	73	78	**77**		**77**	
SO5.2.1	SO 5.2.1 Consola de gestión/puente operaciones			72	80	86		76		74	71	79	70	75	**76**		**76**	
SO5.2.4	SO 5.2.4 Impresión y salidas			75	70	72		75		72	73	78	70	70	**73**		**73**	
SO 5.3	SO 5.3 Gestión Mainframe			70	70	79		72		74	74	80	68	71	**73**		**73**	
SO 5.4	SO 5.4 Administración de servidores y soporte			76	73	90		77		79	76	85	73	85	**79**		**79**	
SO AP.B	SO APENDICE B			80	71	88		72		78	72	71	71	71	**75**		**75**	
	EVALUACION A NIVEL DE ELEMENTO	**82**	**79**	**75**	**75**	**79**	**81**	**78**	**76**	**72**	**72**	**75**	**75**	**78**	**77**	**77**	**76**	**78**

ANEXO 5 PROCESO MADUREZ COBIT 4.1, ITIL V3 e ISO 27001

PROCESO	PROCESO MADUREZ COBIT 4.1, ITIL V3 e ISO 27001 – ELEMENTOS DE TI	DSLAMs	INFRAESTRUCTURA (HW, SW Y SIST. DE GESTIÓN)	COMUNICACIONES (REDES F.O, COBRE Y MPLS)	ESTAND. Y PROC.(SEGURIDAD , DATOS E INTERNET FAST BOY)	ACTIVACIÓN EN LAS PLATAFORMAS	ESTRUCTURA ORGANIZACIONAL	GRADO DE MADUREZ	COBIT 4.1	ITIL V3	ISO 27001
DS1.1	DS1.1 Marco de trabajo de la Administración de los Niveles de Servicio	1	2	3	0	3	3	**2**	**2**		
DS1.2	DS1.2 Definición de Servicios	2	3	4	5	3	2	**3**	**3**		
DS1.3	DS1.3 Acuerdos de Niveles de Servicio	3	4	5	2	1	2	**3**	**3**		
DS1.4	DS1.4 Acuerdos de Niveles de Operación	4	5	5	4	3	2	**4**	**4**		

DS1.5	servicio	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de	4	5	4	3	3	2	**4**	**4**		
DS1.6	contratos	DS1.6 Revisión de los acuerdos de niveles de servicio y de los	3	3	3	3	5	1	**3**	**3**		
DS2.1		DS2.1 Identificación de todas las relaciones con proveedores	3	4	3	4	5	2	**4**	**4**		
DS2.2		DS2.2 Gestión de relaciones con proveedores	3	4	4	3	3	2	**3**	**3**		
DS2.3		DS2.3 Administración de riesgos del proveedor	3	4	4	2	2	1	**3**	**3**		
DS2.4		DS2.4 Monitoreo del desempeño del proveedor	2	3	4	2	4	2	**3**	**3**		
DS3.1		DS3.1 Planeación del desempeño y la capacidad	2	1	2	3	2	1	**2**	**2**		
DS3.2		DS3.2 Capacidad y desempeño actual	4	3	4	2	2	2	**3**	**3**		
DS3.3		DS3.3 Capacidad y desempeño futuros	2	3	4	4	2	4	**3**	**3**		
DS3.4		DS3.4 Disponibilidad de recursos de TI	5	3	3	3	2	2	**3**	**3**		
DS3.5		DS3.5 Monitoreo y reportes	2	2	3	2	3	2	**2**	**2**		
DS4.1		DS4.1 Marco de trabajo de continuidad de TI	2	3	4	3	2	3	**3**	**3**		
DS4.2		DS4.2 Planes de cotinuidad de TI	5	4	4	2	4	2	**4**	**4**		
DS4.3		DS4.3 Recursos críticos de TI	4	4	4	3	3	2	**3**	**3**		
DS4.4		DS4.4 Mantenimiento de plan de continuidad de TI	4	3	4	2	2	2	**3**	**3**		
DS4.5		DS4.5 Pruebas del plan de continuidad de TI	2	2	3	2	2	2	**2**	**2**		
DS4.6		DS4.6 Entrenamiento del plan de continuidad de TI	1	1	1	0	1	0	**1**	**1**		
DS4.7		DS4.7 Distribución del plan de continuidad de TI	1	1	1	1	1	0	**1**	**1**		
DS4.8		DS4.8 Recuperación y reanudación de los servicios de TI	2	1	3	1	1	1	**2**	**2**		
DS4.9		DS4.9 Almacenamiento de respaldos fuera de las instalaciones	0	0	0	0	0	0	**0**	**0**		
A.11.1		A.11.1 Requerimiento de negocio de control de acceso	1	2	1	1	1	1	**0**			**0**
A.11.2		A.11.2 Administración de Accesos de Usuarios	1	1	1	1	1	1	**1**			**1**
A.11.3		A.11.3 Responsabilidades de los usuario	1	1	1	1	1	1	**1**			**1**
A.11.4		A.11.4 Control de acceso a red	1	2	2	2	1	2	**2**			**2**
A.11.5		A.11.5 Control de acceso del sistema operativo	1	1	2	1	1	1	**1**			**1**
A.11.6		A.11.6 Control de Acceso en la información y a las aplicaciones	1	1	1	1	0	0	**1**			**1**
A.11.7		A.11.7 Computación móvil y el teletrabajo	1	1	1	1	1	1	**1**			**1**
SO 4.6.7	activities)	SO 4.6.7 Financial management for IT services (as operational	1	2	2	1	1	0	**1**		1	
DS7.1		DS7.1 Identificación de Necesidades de Entrenamiento y	1	1	1	1	1	1	**1**	1		

	Educación										
DS7.2	DS7.2 Impartición de Entrenamiento y Educación	1	1	1	1	1	1	**1**	1		
DS7.3	DS7.3 Evaluación del Entrenamiento Recibido	1	1	2	2	2	1	**2**	2		
SO 4.1	SO 4.1 gestión de eventos	4	4	3	3	2	2	**3**		3	
SO4.1.5.3	SO 4.1.5.3 Detección de eventos	3	3	4	3	3	2	**3**		3	
SO4.1.5.4	SO 4.1.5.4 Filtrado de eventos	3	3	3	2	2	2	**3**		3	
SO4.1.5.5	SO 4.1.5.5 Significado de eventos	3	3	3	2	3	2	**3**		3	
SO4.1.5.6	SO 4.1.5.6 Correlación de eventos	3	2	4	3	4	2	**3**		3	
SO4.1.5.7	SO 4.1.5.7 Trigger	4	4	3	3	4	1	**3**		3	
SO4.1.5.8	SO 4.1.5.8 Respuestas de selección	5	4	4	2	4	2	**4**		4	
SO4.1.5.10	SO 4.1.5.10 Cierre de eventos	5	4	4	3	3	2	**4**		4	
S.O4.2	SO 4.2 Gestión de incidentes	5	4	4	3	3	3	**4**		4	
SO4.2.5.1	SO 4.2.5.1 identificación de Incidentes	5	4	5	3	4	3	**4**		4	
SO4.2.5.2	SO 4.2.5.2 Registro de incidentes	3	3	3	3	3	2	**3**		3	
SO4.2.5.3	SO 4.2.5.3 Categorización de incidentes	4	3	3	3	3	2	**3**		3	
SO4.2.5.4	SO 4.2.5.4 Priorización de incidentes	3	3	3	2	3	2	**3**		3	
SO4.2.5.5	SO 4.2.5.5 Diagnóstico inicial	3	3	3	3	3	3	**3**		3	
SO4.2.5.6	SO 4.2.5.6 Escalación de incidentes	3	4	4	3	3	3	**3**		3	
SO4.2.5.7	SO 4.2.5.7 Investigación y diagnostico	1	1	1	1	1	1	**1**		1	
SO4.2.5.8	SO 4.2.5.8 Resolución y recuperación	4	4	4	2	3	2	**3**		3	
SO4.3.5.1	SO 4.3.5.1 Menú selección	3	4	4	0	4	3	**3**		3	
SO4.2.5.9	SO 4.2.5.9 Cierre de incidentes	3	3	3	1	3	3	**3**		3	
SO4.1.5.9	SO 4.1.5.9 Revisión y acciones	3	3	3	1	4	1	**3**		3	
SO5.9	SO 5.9 soporte Desktop	3	3	3	1	2	1	**2**		2	
SO6.2	SO 6.2 Service desk	3	1	1	1	1	0	**1**		1	
A.11.4	A.11.4 Network access control	3	4	2	2	2	2	**3**			3
DS10.1	DS10.1 Identificación y clasificación de problemas	3	4	3	3	4	3	**3**	3		
DS10.2	DS10.2 Rastreo y resolución de problemas	4	5	5	4	4	2	**4**	4		
DS10.3	DS10.3 Cierre de problemas	5	3	3	3	3	3	**3**	3		
DS10.4	DS10.4 Integración de las administraciones de cambios, configuración y problemas.	3	2	4	3	3	3	**3**	3		

DS11.1	DS11.1 Requerimientos del Negocio para Administración de Datos	3	2	3	3	3	3	**3**	3		
DS11.2	DS11.2 Acuerdos de Almacenamiento y Conservación	3	3	2	2	4	2	**3**	3		
DS11.3	DS11.3 Sistemas de Administración de Librerías de Medidas	0	0	0	0	0	0	**0**	0		
DS11.4	DS11.4 Eliminación	1	0	0	0	0	0	**0**	0		
DS11.5	DS11.5 Respaldo y Restauración	3	3	2	1	1	1	**2**	2		
DS11.6	DS11.6 Requerimientos de Seguridad para la Administración de Datos	2	2	1	1	1	1	**1**	1		
DS12.1	DS12.1 Selección y Diseño del Centro de Datos	1	1	0	0	0	0	**0**	0		
DS12.2	DS12.2 Medidas de Seguridad Física	0	0	0	0	0	1	**0**	0		
DS12.3	DS12.3 Acceso Físico	1	1	1	1	1	1	**1**	1		
DS12.4	DS12.4 Protección Contra Factores Ambientales	3	3	3	4	4	2	**3**	3		
DS12.5	DS12.5 Administración de Instalaciones Físicas	1	1	2	1	2	2	**2**	2		
SO3.7	SO 3.7 Documentación	1	0	0	0	0	0	**0**			
SO5	SO 5 Actividades de operación de servicio común	2	2	2	1	1	2	**2**			
SO4.1	SO 4.1 gestión de eventos	3	3	3	3	3	2	**3**		3	
SO4.1.5.1	SO 4.1.5.1 Ocurrencia de eventos	1	2	2	1	1	2	**2**		2	
SO4.1.5.9	SO 4.1.5.9 Revisión y acciones	3	1	2	2	3	3	**2**		2	
SO5.2.1	SO 5.2.1 Consola de gestión/puente operaciones	3	3	3	3	2	3	**3**		3	
SO5.2.4	SO 5.2.4 Impresión y salidas	2	3	3	3	3	2	**3**		3	
SO 5.3	SO 5.3 Gestión Mainframe	3	3	3	1	3	1	**2**		2	
SO 5.4	SO 5.4 Administración de servidores y soporte	5	3	3	3	3	3	**3**		3	
SO AP.B	SO APENDICE B	3	3	3	3	3	1	**3**		3	
	EVALUACION A NIVEL DE ELEMENTO	**3**	**3**	**3**	**2**	**2**	**2**	**2**	**2**	**3**	**1**