ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

AUDITORÍA DE RIESGOS INFORMÁTICOS EN EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DEL MINISTERIO DE INCLUSIÓN ECONÓMICA Y SOCIAL

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÀTICOS Y DE COMPUTACIÒN

MERCY SORAYA ANDAGANA JUNTA

mercy.andagana@gmail.com

PAUL ALEXANDER CARRILLO ESTRADA

alexsunset@hotmail.com

DIRECTOR: ING. RAÚL CÓRDOVA

rcordova@epn.ecu.ec

Quito, Septiembre 2009

DECLARACIÓN

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

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

Mercy Andagana	**Paúl Carrillo**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Mercy Andagana y Paúl Carrillo, bajo mi supervisión.

Msc. Raúl Córdova
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios por permitirme cristalizar uno de mis sueños, a mis padres y hermanos por todo el apoyo que me brindan día a día, al Ing. Raúl Córdova por su guía y por ser más que un tutor un amigo y a todas las personas que de una u otra manera contribuyeron a la culminación de este proyecto. Gracias amiguis..!!!!!

MERCY

A Dios por su eterna protección y ayuda, a mi familia por su apoyo incondicional, a mis amigos más cercanos por todas la experiencias que hemos compartido, a Mercedes por su cariño y estar siempre a mi lado, a mis compañeros con los cuales compartí todos mis años de estudio, al Ing. Raúl Córdova por su guía y a todos quienes pusieron un granito de arena para alcanzar esta meta.

PAÚL

DEDICATORIAS

Este trabajo está dedicado a mis padres por todo el amor y apoyo incondicional.

MERCY

Va dedicado a mis padres y hermanos porque son la mejor familia que Dios pudo darme. Esta meta la alcanzamos juntos, de corazón gracias.

PAÚL

CONTENIDO

ÍNDICE DE TABLAS

CAPÍTULO 2

CAPÍTULO 3

ÌNDICE DE FIGURAS

CAPÍTULO 2

CAPTULO 3

RESUMEN

El trabajo que se presenta a continuación tiene como objetivo realizar una Auditoría de Riesgos Informáticos en el Departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social (MIES), basada en el estándar COBIT, ya que abarca los criterios de las mejores prácticas y estándares lo cual nos asegura que está en constante actualización y adaptación a los cambios del desarrollo tecnológico y gerencial-administrativo. De este modo el presente trabajo será segmentado de la siguiente manera

El Capitulo I, **JUSTIFICACIÓN DEL USO DE COBIT Y HERRAMIENTAS,** justifica el uso de COBIT como marco de referencia, además de las herramientas a utilizar para llevar a cabo la auditoria de Riesgos Informáticos del Departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social.

El Capitulo II, **EJECUCIÓN DE LA AUDITORIA**, identifica y analiza los riesgos existentes y potenciales inherentes al Departamento de Gestión Tecnológica basados en las cláusulas de control de seguridad del estándar ISO 17799:2005. Adicionalmente en este capítulo se escogen los procesos COBIT aplicables al presente trabajo. Finalmente, el proceso de auditoría se lleva a cabo después de hacer un mapeo entre la norma ISO 17799:2005 y el marco referencial COBIT 4.0.

El Capítulo III, **ANÁLISIS Y PRESENTACIÓN DE RESULTADOS**, presenta un informe sobre las evaluaciones realizadas, en el que constan los resultados obtenidos que reflejan la situación actual del Departamento de Gestión Tecnológica del MIES

El Capítulo IV, **CONCLUSIONES Y RECOMENDACIONES**, plantea las conclusiones y recomendaciones en base a la Auditoria de Riesgos Informáticos realizados en el Departamento obtenidos en la elaboración del presente proyecto de titulación.

PRESENTACIÓN

La información se ha convertido en el eje promotor de cambios sociales, económicos y culturales. El auge de las telecomunicaciones ha producido una transformación de las tecnologías de la información y de la comunicación, cuyo impacto ha afectado a todos los sectores de la economía y de la sociedad.
Hoy en día, los progresos en las denominadas tecnologías de la información (TI), que abarcan los equipos y aplicaciones informáticas y las telecomunicaciones, están teniendo un gran efecto. De hecho, se dice que estamos en un nuevo tipo de sociedad llamada Sociedad de la información o Sociedad de Conocimiento,

Por tanto, es evidente que las nuevas tecnologías son un elemento imprescindible y en continuo desarrollo dentro de cualquier empresa y aun mas para organizaciones gubernamentales como el Ministerio de Inclusión Económica y Social. No obstante a la vez que las TI proveen medios más rápidos y seguros también han desencadenado el aparecimiento de nuevos tipos de amenazas que ponen en riesgo la continuidad de la organización.

Para poder prever qué tipo de riesgos son los que amenazan a la infraestructura tecnológica y sobre todo a la información es importante considerar la ejecución de una auditoría de riesgos informáticos, basada en los estándares internacionales adecuados, que evalúan la situación actual y así generan planes que permiten actuar de forma rápida ante cualquier eventualidad. Otorgar seguridad en el manejo de la información y a la estructura tecnológica adyacente, es la principal premisa que se busca alcanzar con la elaboración de una auditoría de riesgos informáticos.

CAPÍTULO 1. JUSTIFICACIÓN DEL USO DE COBIT Y HERRAMIENTAS

1.1 JUSTIFICACIÓN DEL USO DE COBIT

La evaluación de los requerimientos del negocio, los recursos y procesos IT, son puntos bastante importantes para el buen funcionamiento del Ministerio de Inclusión Económica y Social, razón por la cual en el presente proyecto se utiliza COBIT (Control Objectives for Information and related Technology), que es precisamente un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización.

COBIT es una herramienta perfectamente aplicable para la presente auditoria, dado que la administración del MIES requiere de prácticas generalmente aplicables y aceptadas de control y gobierno en TI para medir en forma comparativa tanto su ambiente de TI existente, como su ambiente planeado.
COBIT está orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas.

Adicionalmente, COBIT es un modelo de referencia para establecer controles sobre las TI y es una guía para realizar auditorías de esos mismos controles, ya que proporciona un conjunto de buenas prácticas muy útiles que permiten juzgar el desempeño en base a métricas establecidas, mismas que están orientadas fuertemente al control de los procesos de TI. Suplementariamente, COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad de TI y abarca controles específicos de TI desde una perspectiva de negocios.

Del mismo modo la utilización de COBIT en este proyecto se argumenta por la especial importancia que el marco de trabajo proporciona al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos, así también por la propuesta de COBIT en un marco de acción donde se evalúan los criterios de información, como por

ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización.

1.2 JUSTIFICACION DEL USO DE HERRAMIENTAS

Las herramientas con las cuáles se llevará a cabo el presente proceso de auditoría de riesgos informáticos son las siguientes:

- ISO/IEC 17799:2005
- Modelos de Madurez (tomados de COBIT 4.0)

1.2.1 ESTANDAR INTERNACIONAL ISO/IEC 17799 – 2005

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funciona como un facilitador para evitar o reducir los riesgos relevantes, razón por la cual es esencial que el Ministerio de Inclusión Económica y Social identifique sus requerimientos de seguridad. Para ello en la presente auditoría se utiliza el estándar ISO/IEC 17799 – 2005 que es una norma que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información.

La utilización de la norma ISO/IEC 17799 es conveniente para el ministerio ya que la norma es particularmente interesante si la protección de la información es crítica, como es el caso del sector público.

Adicionalmente, una auditoría basada en ISO/IEC 17799 – 2005 proporciona información precisa acerca del nivel de cumplimiento de la norma a diferentes niveles: global, por dominios, por objetivos y por controles.

El uso de la norma garantiza la selección de controles de seguridad adecuados y proporcionales que permiten proteger los activos de información y otorga confianza a cualquiera de las partes interesadas. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y

mejorar un Sistema Gestión Sistemas de Información, enfoque necesario para una institución tan importante como el MIES.

1.2.2 MODELOS DE MADUREZ

El modelado de la madurez para la administración y el control de los procesos de TI permite evaluar al ministerio desde un nivel de no-existente (0) hasta un nivel de optimizado (5). La utilización del modelado de madurez COBIT permite medir la eficacia de los procesos de administración desarrollados en el ministerio. Este modelado es el que proporciona una medición cuantitativa, la cual permitirá establecer el nivel de madurez en los diferentes procesos, basándose en los objetivos de control de COBIT, para así poder llevar a cabo acciones correctivas en dónde sea requerido.

COBIT es un marco de referencia general dirigido a la administración de TI y como tal estas escalas son prácticas para aplicar y razonablemente fáciles de entender. El modelado de madurez permite también analizar los vacíos existentes en el ministerio para determinar lo que es necesario hacer para alcanzar un nivel deseado.

En conclusión, el modelado de madurez permite identificar la situación actual del MIES, la situación actual de la industria, la situación actual de los estándares internacionales y finalmente la estrategia del ministerio para mejoramiento. Esta medición es primordial para obtener las conclusiones y recomendaciones en cuanto a las vulnerabilidades y las posteriores mejoras en el ministerio.

CAPÍTULO 2. EJECUCIÓN DE LA AUDITORÍA

2.1 CARACTERIZACIÓN DEL MINISTERIO

A continuación se procede a caracterizar el Ministerio de Inclusión Económica y Social (MIES), a través de sus antecedentes, misión, visión, objetivos, principios y valores y estructura organizacional, mismos que fueron obtenidos a través de la página Web del MIES: http://www.mies.gov.ec

2.1.1 ANTECEDENTES

El Ministerio de Bienestar Social inició su accionar en programas específicos como: Seguridad Social, Protección de Menores, Cooperativismo, Promoción Popular y Bienestar Social.
Posteriormente debido a las demandas de la sociedad y de los sectores más necesitados el Ministerio proyectó un desarrollo programático y ampliación de cobertura geográfica mediante la implementación de programas y proyectos orientados a la atención de los sectores vulnerables en forma directa y la generación de fuentes de trabajo a través de convenios con organizaciones no gubernamentales, comunitarias y organismos del sector público.

El 29 de agosto del 2008, el Ministerio de Bienestar Social, a través de su ministra, Jeannette Sánchez, cambia de nombre por el de Ministerio de Inclusión Económica y Social. Partiendo del hecho que la inclusión debe ser un derecho adquirido desde el momento en que nace cualquier ecuatoriano y ecuatoriana; debe ser una práctica radicalmente humanista, responsable y obligatoria en toda nuestra sociedad; debe ser el inicio de un pensamiento renovado y renovador en nuestra patria, y en este sentido, absolutamente revolucionario porque aspira trasformar esta sociedad que excluye, separa, fracciona, y crea privilegios y distancias entre sus ciudadanos. La inclusión social no es una ley del gobierno o un decreto que aparece inscrito en el registro oficial, Es, sobre todo, un proceso que tiene que ser construido colectivamente, con esperanza, buenas voluntad, alegría, organización, disciplina y honestidad, y puesto en práctica por toda la población de las regiones de nuestra patria. El MIES, será un garante de los

derechos de los y las ecuatorianas, mientras el sistema no los incluya adecuadamente.

2.1.2 MISIÓN

El MIES promoverá y fomentará activamente la inclusión económica y social de la población, de tal forma que se asegure el logro de una adecuada calidad de vida para todos los ciudadanos y ciudadanas, mediante la eliminación de aquellas condiciones, mecanismos o procesos que restringen la libertad de participar en la vida económica, social y política de la comunidad y que permiten, facilitan o promueven que ciertos individuos o grupos de la sociedad sean despojados de la titularidad de sus derechos económicos y sociales, y apartados, rechazados o excluidos de las posibilidades de acceder y disfrutar de los beneficios y oportunidades que brinda el sistema de instituciones económicas y sociales.

2.1.3 VISIÓN

Soñamos con una Patria para todos, sin exclusión, sin pobreza, con igualdad de oportunidades económicas, sociales y políticas para todos los ciudadanos y ciudadanas, independientemente de su sexo, color, raza, etnia, edad, procedencia, estrato social, condición de salud, y orientación sexual.

2.1.4 OBJETIVOS

- Ampliar las capacidades de su población objetivo mediante la generación o garantía de las oportunidades de acceder a los servicios sociales de educación, formación, capacitación, salud, nutrición, y otros aspectos básicos de la calidad de vida que influyen en la libertad fundamental del individuo para vivir mejor.
- Promover la inclusión económica de su población objetivo mediante la generación o garantía de las oportunidades de poseer, acceder y utilizar los recursos económicos de la sociedad para consumir, producir o realizar intercambios, de tal forma que se garanticen las oportunidades de acceso a trabajo, ingreso y activos.

- Garantizar el derecho de su población objetivo a la protección social y especial, de modo que no sufran grandes privaciones como consecuencia de cambios materiales que afectan negativamente sus vidas, mediante la regeneración sistemática de un nivel mínimo de ingresos y la protección o restitución de sus derechos económicos y sociales, de tal forma que se garanticen las oportunidades para vivir con seguridad y satisfactoriamente.
- Fomentar la ciudadanía, la organización y la cohesión social mediante la promoción o garantía de participación de los ciudadanos y ciudadanas como actores fundamentales de su propio desarrollo, el reconocimiento de su capacidad transformadora y de emprender acciones que les permitan acceder o recobrar la titularidad de los derechos económicos y sociales, y la ampliación de las oportunidades de la población para interrelacionarse.

2.1.5 PRINCIPIOS Y VALORES

- **Transparencia**: Criterio técnico, información clara y rendición de cuentas en los actos públicos.
- **Solidaridad**: Sentir como propia la problemática de los demás y construcción de la Minga como expresión de acción solidaria.
- **Equidad**: Garantizar la igualdad de oportunidades, luchar contra la exclusión y generar condiciones para el ejercicio de los derechos ciudadanos establecidos por la Constitución Política de la República.
- **Potenciación de los Talentos y capacidades humanas**: Identificar y desarrollar las potencialidades de la población y apoyar su constitución como actores activos del desarrollo humano.
- **Participación**: Promover la participación ciudadana, la auditoría social y el fortalecimiento de la organización popular.
- **Interculturalidad**: Reconocer la diversidad cultural del país y promover su desarrollo inclusivo.
- **Calidad**: Cumplimiento de estándares mínimos establecidos para la provisión de servicios eficientes y eficaces.
- **Sustentabilidad**: Reconocer la diversidad natural y promover la convivencia armoniosa con el medio ambiente.

2.1.6 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional del Ministerio de Inclusión Económica y Social se encuentra formada por tres niveles, como se muestra en la *Figura 2.1*:

- **Nivel Directivo**: En este nivel se encuentra la máxima autoridad del MIES, que es el/la Ministro (a), juntamente con la Subsecretaría General.

- **Nivel Asesor:** En el nivel asesor se encuentran las áreas de Comunicación, Planificación, Asesoría Legal, Auditoría Interna y DIPLASEDE.

- **Nivel Operativo:** En este nivel se encuentra la Subsecretaría Administrativa Financiera, Subsecretaría de Protección Familiar, Subsecretaría de Economía Solidaria, Subsecretaría de Desarrollo Social y Subsecretarías Regionales cada una con sus respectivas áreas; también se encuentran en este nivel las Direcciones Provinciales, los programas a cargo del MIES y los adscritos Cuerpos de Bomberos.

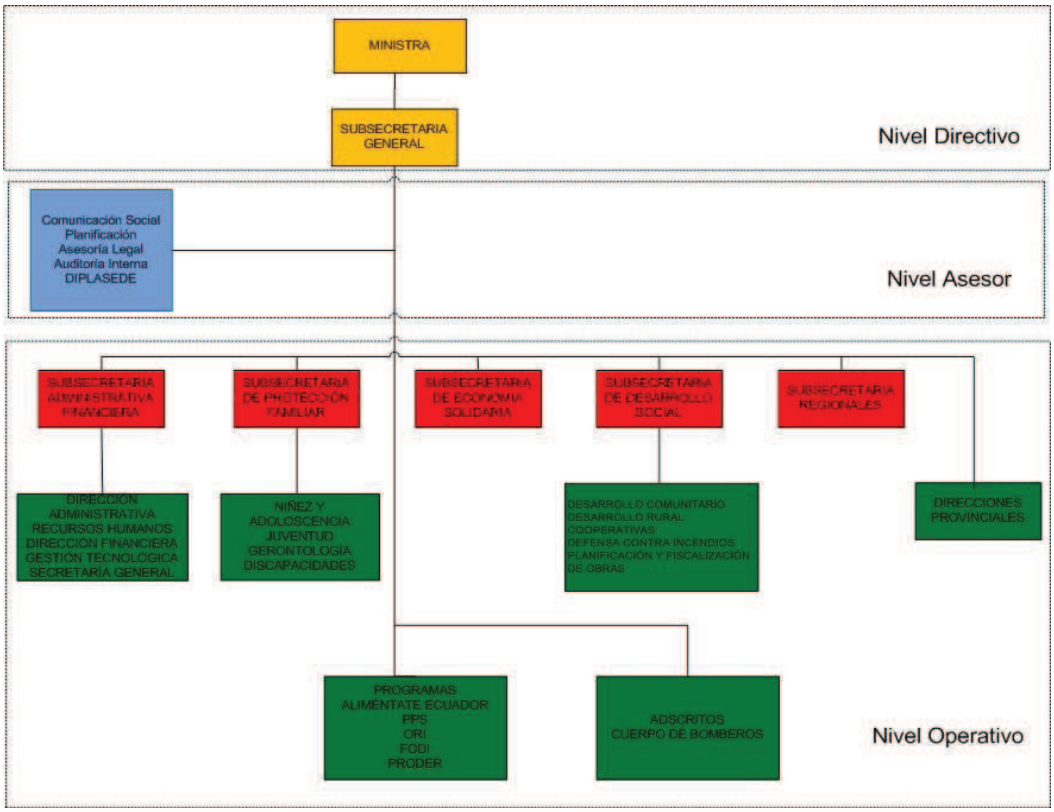

Figura 2.1: Estructura Organizacional del Ministerio de Inclusión Económica y Social

2.2 SITUACIÓN ACTUAL DEL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA

A continuación se describe la situación actual del Departamento de Gestión Tecnológica.

2.2.1 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional del Departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social se encuentra distribuida como se muestra a continuación en la *Figura 2.2*

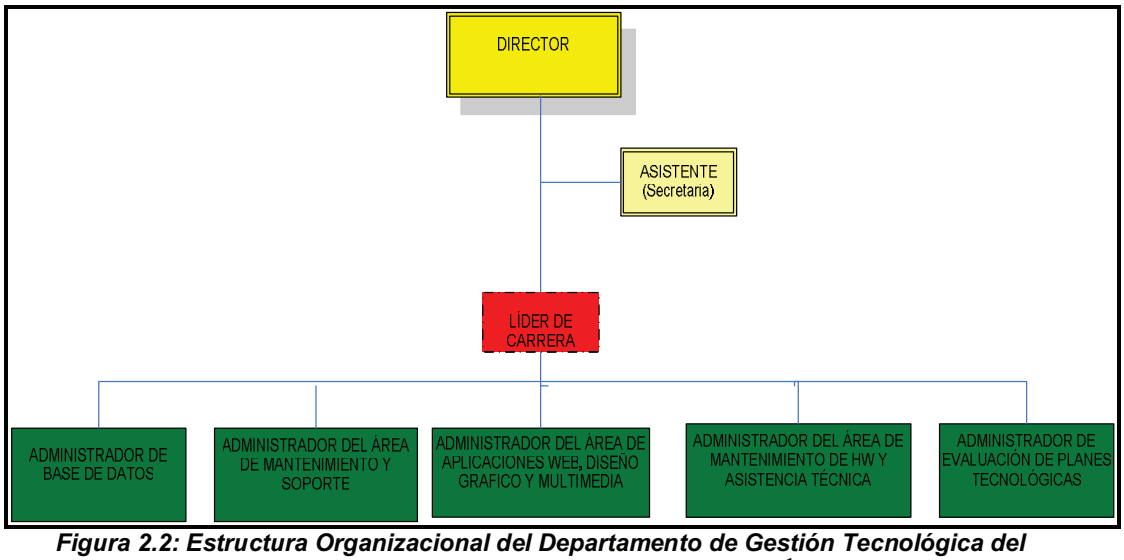

Figura 2.2: Estructura Organizacional del Departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social[1]

2.2.1.4 RECURSOS HUMANOS

El Departamento de Gestión Tecnológica actualmente cuenta con 11 funcionarios, a continuación se detalla el área asignada a cada funcionario *Tabla 2.1*.

Funcionario	Área de Trabajo
Ramiro Correa	Director de Área
Mariana Moreno	Secretaria
Guillermo Pachacama	Asistente Administrativo
Francisco Orozco	Mantenimiento de Hardware y Asistencia Técnica de

[1] Departamento Gestión Tecnológica del MIES

	escritorio
Marlon Serrano	Mantenimiento de Hardware y Asistencia Técnica de escritorio
Patricio Alvear	Seguimiento, Evaluación de Planes Tecnológicos, capacitación, mejora de procesos
Jenny Rodríguez	Administración, desarrollo y soporte de Aplicaciones Web, Diseño Gráfico y Multimedia.
Jorge Racines	Mantenimiento de Hardware y Asistencia Técnica de escritorio
Christian Jiménez	Administración, soporte y mantenimiento de Redes, Telecomunicaciones y Seguridad Informática
Ricardo Sotomayor	Administración, desarrollo y soporte de Aplicaciones, Bases de Datos y auditoría informática.
Andrés Yánez	Administración, soporte y mantenimiento de Redes, Telecomunicaciones y Seguridad Informática

Tabla 2.1: Recursos Humanos Departamento de Gestión Tecnológica[2]

2.2.1.5 FUNCIONES DEL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA[3]

Entre las principales funciones asignadas al Departamento de Gestión Tecnológica se encuentran:

- Administrar el Sistema de Software y Hardware del Ministerio y coordinar la provisión de los servicios informáticos y de comunicaciones para el procesamiento de datos e información institucional.
- Coordinar permanente con organismos públicos y privados en asuntos relacionados al área de informática a fin de realizar actividades conjuntas.
- Diseñar, implantar y desarrollar sistemas informáticos computarizados necesarios para lograr eficiencia y economía en las actividades desarrolladas por las dependencias ministeriales.

[2] Departamento de Gestión Tecnológica del MIES
[3] Departamento de Gestión Tecnológica del MIES

- Estudiar y emitir informes sobre las necesidades de adquisiciones y/o rentas de equipos y paquetes informáticos y poner a consideración de la máxima autoridad del Ministerio.
- Organizar y mantener actualizados los inventarios informáticos y establecer un control de los sistemas existentes.
- Administrar los recursos informáticos, orientar, capacitar y proporcionar el apoyo técnico necesario a los operadores y usuarios de los sistemas informáticos, en planta central y dependencias ministeriales desconcentradas.
- Cumplir y hacer cumplir la legislación y normas relacionadas con el área de informática.
- Establecer la infraestructura tecnológica compatible y de punta para lograr el desarrollo institucional del Ministerio.
- Analizar y determinar el uso adecuado de los equipos de acuerdo a las necesidades técnicas de las unidades administrativas ministeriales.
- Velar por el buen uso de los equipos, normas de seguridad e instalaciones de los sistemas.
- Implantar mecanismos de protección y salvaguarda contra pérdidas de los equipos e información sistematizada.
- Establecer estándares técnicos de diseño y construcción dentro del Marco de Conectividad y sitios Web.
- Administrar, desarrollar y dar soporte a Aplicaciones, Bases de Datos.
- Administrar, proveer soporte y mantenimiento de Redes, Telecomunicaciones y Seguridad Informática.
- Administrar, desarrollar y dar soporte de Aplicaciones Web, Diseño Gráfico y Multimedia.
- Proveer mantenimiento de Hardware y Asistencia Técnica de escritorio a los usuarios de la red del MIES.

2.2.2 INFRAESTRUCTURA DE RED INFORMÁTICA DEL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA

A continuación se describe la infraestructura de red del Departamento de Gestión Tecnológica del MIES a través del inventario de Hardware y Software así como de la topología de red.

2.2.2.1 INVENTARIO DE HARDWARE Y SOFTWARE

Plataforma De Servidores[4]

A continuación se describe el inventario de hardware perteneciente a la plataforma de servidores con sus respectivos roles e inventario de software.

4 Servidores: Blade Proliant BL P20, 2 procesadores Xeon DC 3 GHZ, memoria 4 GB, 2 Discos Duros de 33.3 GB.
Software: Microsoft Windows 2003 Server.

2 Servidores: Blade Proliant BL P20, 2 procesadores Xeon DC 3 GHZ, memoria 4 GB, 5 Discos Duros de 300 GB.
Software: Microsoft Windows 2003 Server, Servidor de Base de Datos SQL Server 2000.

1 Servidor: Blade Proliant BL P20, 2 procesadores Xeon DC 3 GHZ, memoria 4 GB, 5 Discos Duros de 33.3 GB.
Software: Microsoft Windows 2003 Server.

1 Servidor: Blade Proliant BL P20, 2 procesadores Xeon DC 3 GHZ, memoria 4 GB, 2 Discos Duros de 300 GB.
Software: Microsoft Windows 2003 Server.

1 Servidor: Blade Proliant ML 370 2G, 2 procesadores P III 966 MHZ, memoria 1 GB, 4 discos duros de 16.9 GB.
Software: Microsoft Windows 2003 Server.

[4] Departamento de Gestión Tecnológica del MIES

1 Servidor: Blade Proliant ML 370 36G, 2 procesadores Xeon 3.06 GHZ, memoria 1 GB, 3 Discos Duros de 33.9 GB.
Software: Microsoft Windows 2003 Server.

1 Servidor: HP xw4400 WorkSation, 1 procesador Dual Core 3.0 GHZ, memoria 3 GB, 1 Discos Duros de 120GB.
Software: Linux Centos 5.0.

3 Servidores: HP Compaq ,1 procesador Dual Core 3.0 GHZ, memoria GB, 1 Discos Duros de 150GB.
Software: Linux Centos 5.0, Microsoft Windows 2003 Server.

1 Servidor: Kypus Appliance KSA-100, 1 procesador Mobile Intel Celeron ™ CPU650M, memoria RAM 512MB, memoria FLASH 512MB, Disco Duro de 80GB.
Software: Kypus SO 1.3.0.8, Consola de Administración 1.3.

Aplicaciones ministeriales

En la *Tabla 2.2* se describen las diferentes aplicaciones que actualmente son utilizadas en el Ministerio de Inclusión Económica y Social con los respectivos sistemas operativos, plataformas y base de datos sobre los que funcionan las aplicaciones.

N.	Sistema Operativo	Aplicación	Plataforma	Base de Datos
1	Windows 2003 Server	Web Server	.Net 2005	SQL Server 2000
2	Windows 2003 Server	Control y Registro de Documentación	Visual Studio 6,0	SQL Server 2000
3	Windows 2003 Server	Lexis	Lexis	DB Interna
4	Centos 5.0	Mail Server	Send Mail	DB Interna
5	Centos 5.0	Mail Scanner	Mail Wacht	My SQL
6	Centos 5.0	Servicio de Directorio	LDAP	My SQL
8	Windows 2003 Server	Sistema de Recursos Humanos	.Net 2005	SQL Server 2000
9	Windows 2003 Server	Sistema de Registro de Cooperativas	Visual Basic 6	SQL Server 2005

***Tabla 2.2: Aplicaciones Ministeriales*[5]**

Cabe mencionar que en las estaciones de trabajo del MIES encontramos como Sistema operativo Windows XP y como software de escritorio Open Office 3.4, Microsoft Office 2003 y Microsoft Office 2007.

2.2.2.2 TOPOLOGÍA DE RED

En la *Figura 2.3* se describe la topología de red correspondiente a Planta Central del Ministerio de Inclusión Económica y Social.
La oficina matriz del Ministerio de Inclusión Económica y Social funciona en un edificio de 11 pisos. En este edificio existe una red LAN de tipo Ethernet, topología estrella, distribuida físicamente en 9 segmentos horizontales que se conectan al segmento vertical principal mediante un sistema de cableado estructurado de cable UTP categoría 6, actualmente se cuenta con 296 estaciones de trabajo y 14 servidores en planta central.

En la red del MIES los Switches 3Com 5.500 de 48 puertos de capa de red administrables se encuentran enlazados entre sí, de este modo comparten la carga de trabajo en un 50% cada uno, trabajando en forma redundante. La redundancia significa que el momento en que uno de los switches sufra alguna avería el otro asume el 100% de la carga con lo que no se cae el servicio puesto que cada uno tiene la capacidad de asumir las tareas del otro.

El conmutador está ubicado físicamente en el cuarto de control principal, contiene 12 puertos de comunicación LAN tipo Ethernet con velocidad de 1 Gbps. Este dispositivo se encarga de enviar el tráfico entre el módulo de servidores y módulo de edificio, utilizando únicamente los servidores de capa de enlace del dispositivo. Los switches 3Com 5.500 de 48 puertos de capa de red administrables soportan las siguientes características:

- Administración mediante protocolo SNMP
- Disponibilidad para crear redes virtuales

[5] Departamento de Gestión Tecnológica del MIES

- Soporta hasta la capad de Enlace

Los usuarios del MIES tienen acceso a Internet a través del Router Cisco 2800 Series ubicado en el quinto piso en el Departamento de Gestión Tecnológica, mismo que brinda conectividad con el proveedor de servicios de Internet (ISP) Megadatos. El router se conecta a la red MAN del proveedor. La seguridad que brinda el proveedor, está determinada por sus equipos. El enlace se lo realiza a través de fibra óptica y la velocidad es de 2048 Mbps, existiendo también un enlace back up por medio de cobre.

Existe también un canal dedicado de Internet por parte de Andinatel. Este proyecto fue ejecutado por la Presidencia de la República, se tendieron varios anillos de fibra óptica a través de los cuales se interconectan todas las instituciones públicas con la presidencia de la república. A través de estos canales se están brindando el servicio de Video Conferencia y de Internet con un canal de 3 Mbps solo para Internet.

El nivel de la calidad del servicio brindado por Megadatos está definido mediante un Acuerdo de Nivel de Servicio (SLA, Service Level Agreement). En el SLA se ha determinado:

- Velocidad y Calidad de Enlace
- Horario de soporte técnico
- Tiempo de respuesta

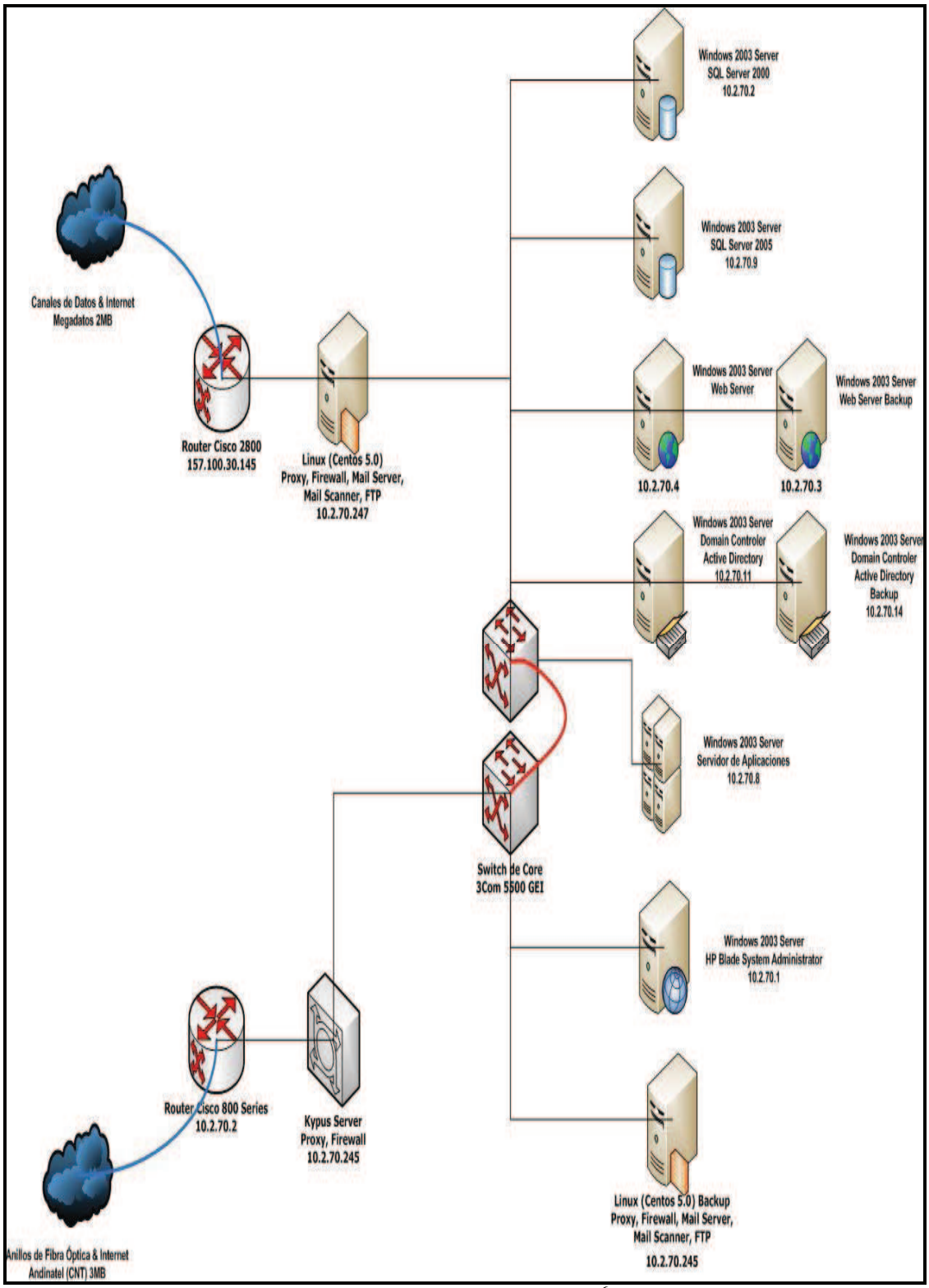

Figura 2.3: Topología de red MIES[6]

[6] Departamento de Gestión Tecnológica del MIES

2.2.3 EVALUACION DE LA SITUACIÓN ACTUAL DE RIESGOS INFORMÁTICOS EN EL DEPARTAMENTO DE GESTIÓN TECNOLÓGICA DEL MIES BASADO EN EL ESTÁNDAR ISO/IEC 17799

Para realizar esta tarea, se obtuvo la información necesaria mediante entrevistas realizadas a funcionarios del Departamento de Gestión Tecnológica del MIES. Además, se realiza una descripción sobre la situación actual de la seguridad en el Departamento según las cláusulas consideradas desde el numeral 5 del estándar:

I. Política de seguridad de la información

a) Política de seguridad de la información

El departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social no cuenta con un plan de seguridad de la información definido, pero cuenta con políticas de seguridad en cuanto a tópicos relevantes de la unidad.

La información en esta Cartera de Estado, está siendo administrada bajo los siguientes parámetros:

- **Confidencialidad:** La información debe ser accesible sólo a aquellas personas autorizadas a tal fin, bajo ningún motivo ningún usuario puede tener acceso a información no competente en su ámbito.
- **Integridad**: La información y sus métodos de procesamiento deben ser completos y exactos.
- **Disponibilidad**: La información y sus recursos relacionados deben estar disponibles cada vez que se los requiera.

II. Organización de la seguridad de la información

a) Organización interna

La información está organizada de acuerdo al área de su competencia, esto implica que los usuarios de la red del MIES únicamente tendrán acceso a la información que les compete a ellos directamente y no al de otras áreas. Para administrar la información se usa el DNS (Domain Name Service) primario de la institución, en el cual se establecen las políticas necesarias de acceso a la información de acuerdo al perfil de cada usuario.

El acceso a la información de las bases de datos está siendo administrado localmente por cada aplicación, donde se dan privilegios a los usuarios que deben trabajar en una determinada aplicación.

b) Grupos o personas externas

El acceso externo a la información institucional se la realiza a través del portal del Ministerio, permitiendo acceder a reportes de los trámites que se llevan a cabo en los diferentes programas adscritos.

III. Gestión de activos

a) Responsabilidades sobre los activos

La gestión de activos es llevada por la Unidad de Inventarios del Ministerio, el cual lleva un registro completo de todo el parque informático a nivel nacional, el mismo que ya esta sistematizado en el Sistema de Inventarios.

Cada activo existente en la institución está a cargo del funcionario que lo ocupa, los mismos que son entregados mediante un acta entrega recepción, al momento de salir de Guarda Almacén en donde son registrados y posteriormente inventariados.

b) Clasificación de la información

En el MIES se clasifica únicamente la información de acuerdo al departamento al que pertenece dicha información, no se maneja ningún otro criterio de clasificación.

IV. Seguridad de Recursos Humanos

a) Antes del empleo

Inicialmente se receptan las carpetas en el departamento de Recursos Humanos, carpetas que luego son seleccionadas de acuerdo a los requerimientos de la plaza vacante en el MIES. Después de una investigación positiva acerca de los antecedentes del candidato, finalmente se elige a la persona idónea al cargo.

Una vez escogida a la persona indicada, se coordina una entrevista para tratar el cargo y las responsabilidades correspondientes, una vez que las dos partes se encuentran satisfechas se firma un contrato para finalizar la contratación.

b) Durante el desempeño de funciones

Una vez seleccionado el nuevo personal se registra en las bases de datos institucionales después de formalizar toda la parte contractual con la institución, tras una notificación de la Unidad de Recursos Humanos, en la cual se indican los datos del nuevo funcionario y el área donde se va a desempeñar.

Con estos datos se procede a generar lo siguiente:

- Asignación de Tarjeta de Registro de Personal
- Usuario de Red
- Mail Ministerial
- Registro Directorio Institucional LDAP
- Activación de Perfiles de Usuario

En el Departamento de Gestión Tecnológica se tienen roles y responsabilidades definidos, es decir cada funcionario se desempeña en un campo específico y realiza sus actividades de acuerdo al mismo.

Por otro lado no se proporciona a los funcionarios capacitación sobre los procedimientos de seguridad y uso adecuado de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad.

c) Terminación o cambio de empleo

El proceso de terminación no es un proceso formal de manera que no se realiza una devolución oficial de software o hardware que hayan sido responsable el funcionario y muchas veces los derechos de acceso a la red del Ministerio no son retirados oportunamente.

V. Seguridad física y ambiental

a) Áreas seguras

El Ministerio de Inclusión Económica y Social cuenta con el servicio de guardianía privada de manera que para ingresar al edificio es necesario registrarse con el guardia asignado para esta labor.

El acceso al departamento de Gestión Tecnológica por parte de personas ajenas a la unidad no está permitido aunque esta regla no siempre es acatada, ya que muchos funcionarios del MIES ingresan sin previa autorización.

Para el acceso al Centro de Datos se cuenta con mayor seguridad, ya que solo pueden ingresar las personas a las que se les fueron asignadas una tarjeta

magnética de acceso, adicionalmente están implementados los siguientes elementos de seguridad:

- Sistema de control de acceso
- Puerta blindada anti ruido
- Sistema de alarma y alertas
- Sistema contra incendios, con nitrógeno líquido

b) Equipos de seguridad

El acceso no autorizado tanto al departamento como a la información no esta permitido, por el control de acceso implementado en el departamento.

Todas las estaciones cuentan con instalaciones eléctricas debidamente polarizadas, una regleta o cortapicos y un UPS o regulador de voltaje, de este modo evitar algún daño al equipo informático por alteraciones de voltaje. Cabe mencionar que el cableado de la red se encuentra protegido por canaletas como medida de seguridad.

Adicionalmente el Ministerio cuenta con un generador eléctrico, el cual trabaja de forma inmediata apenas haya un corte de energía.

Para proteger el cableado de la red se cuentan con canaletas que se encuentran implementadas en todo el edificio.

VI. Gestión de las comunicaciones y operaciones

a) Procedimientos y Responsabilidades operacionales

Existe un estricto monitoreo de todas las instalaciones informáticas de la institución entra las cuales tenemos:

- Monitoreo de Servicios y Aplicaciones criticas, tales como bases de datos, DNS, etc.
- Monitoreo, Mantenimiento y Administración del portal Web institucional www.mies.gov.ec.
- Monitoreo continuo de los dos servidores de comunicaciones existentes.
- Monitoreo en coordinación con el ISP de los 23 nodos institucionales a nivel nacional.

- Monitoreo, Mantenimiento y Administración del mail server institucional.
- Monitoreo, Mantenimiento y Administración del dominio www.mies.gov.ec.
- Verificación del óptimo acceso a los diferentes recursos de red

Los procesos de operación no se encuentran debidamente documentados de manera que no se encuentran a disposición de los funcionarios que los requieran.

b) Gestión de la entrega del servicio de terceros

La entrega de servicios por un tercero constantemente esta siendo monitoreada por los funcionarios del departamento responsables del servicio, de manera que se controla el cumplimiento de estándares y cambios para satisfacer los requerimientos definidos para la entrega de servicios.

c) Planeación y aceptación del sistema

Para poder optimizar los diferentes trabajos que lleva a cabo esta Cartera de Estado, se realiza un levantamiento de información de las diferentes unidades que requieren la automatización de un determinado proceso. Tras este estudio se define los requerimientos reales para su implementación con la respectiva autorización del usuario, con esto se empieza la etapa de desarrollo del sistema ya sea de manera local o tercerizada.

Previa la implementación del nuevo sistema se realiza las pruebas necesarias para comprobar que cumpla con los requerimientos operacionales establecidos, de esta manera asegurar el desempeño el sistema.

d) Protección contra el código malicioso

La institución cuenta con varias herramientas de control y monitoreo que ayuda a controlar los ataques que podrían producirse y de esta manera afectar la información vital del Ministerio.

Esta protección se la realiza de manera interna así como externa, con las siguientes herramientas:

- Firewall
- Plataforma de Antivirus y Antispam Centralizada
- Relay de Mails institucionales salientes contra un servidor externo del ISP.

e) Respaldo o backup

El sistema de backups que se maneja en la institución esta estructurado del siguiente modo:

Plataforma de Servidores:

Se mantienen replicas o backups de los servicios más críticos de la institución, a nivel de hardware así como se software, entre ellos tenemos los siguientes:

Backup de Servidor de Comunicaciones (Linux Centos 5.0), con todos los servicios que tiene el servidor en producción:

- Mail Server
- Mail Scanner
- Relay de mail institucional ris@mies.gov.ec de la Unidad de Comunicación Social
- Proxy
- Tablas de Ruteo
- LDAP

Backup de Servidor de Controlador de Dominio, con todos los servicios que tiene el servidor en producción:

- Directorio Activo
- Controlador de Dominio
- Políticas de Administración
- Unidades Organizacionales
- Reversas de servicio de acceso a aplicativos

Backup Web Server, con todos los servicios que tiene el servidor en producción:

- Portal Web Institucional

Bases de Datos: Se mantienen un sistema de backups automatizado mediante un robot de backup el cual saca respaldos de bases de datos y archivos especificados por el usuario, en cintas de almacenamiento masivo de 800 GB cada una.

Los backups son generados a las 0:00 horas de manera diaria todos los días, al momento de terminarse la capacidad de una cinta de backup, está es almacenada en un lugar seguro en caso de ser necesario su utilización.

Se está por crear una política de seguridad, la cual permitirá guardar el respaldo de la información crítica de institución en una bóveda bancaria.
En algunos casos dependiendo de la necesidad de la información los respaldos son sobre escritos para de este modo optimizar la utilización de los recursos.

f) Gestión de seguridad de la red

La red está siendo administrada, por intermedio de diferentes herramientas de monitoreo, las cuales permiten el óptimo control del tráfico de la red institucional.
Como medida primordial para asegurar el funcionamiento en un 100% de todos los servicios de red, se maneja una política que consiste en mantener un backup de los servidores que comprenden la parte neuronal de la Red, tales como: Controlador Primario de Dominio, Firewall, Mail Server.
Las políticas de administración están siendo implantadas por intermedio del Active Directory, el cual permite asignar las diferentes reglas de acceso a los servicios de red de acuerdo a las necesidades reales de trabajo de los usuarios basado en los perfiles de usuario.

g) Gestión de medios

No existen políticas para la gestión de medios, no se han establecidos procedimientos de operación adecuados para evitar la divulgación, modificación o eliminación de documentación o medios removibles pertenecientes al Ministerio.

h) Intercambio de información

El intercambio o replicas de información mediante la red institucional, se la realiza en un horario fijo, preferiblemente en horas de la noche. El traslado de la información se lo realiza mediante los diferentes enlaces que se tienen con las Unidades Ministeriales Provinciales.
A través de estos se replican la información concentrada en los diferentes nodos, con las bases de datos principales en la Planta Central de este modo se mantiene actualizada la información a nivel nacional de una manera segura.
Estos enlaces impiden que sean jaqueados o exista alguna perdida de información, las herramientas de réplica de información arrojan reportes diarios informando cualquier novedad que pudiera presentarse en el proceso de réplica de información.

La transmisión de información dentro del MIES se lo realiza a través del mail institucional, mismo que utiliza Microsoft Outlook como gestor de correo electrónico.

i) Servicio de comercio electrónico

El Ministerio de Inclusión Económica y Social no utiliza este servicio

j) Monitoreo

Existen en la institución diferentes herramientas, las cuales permiten monitorear los diferentes servicios con los que cuenta esta Cartera de Estado, especialmente los diferentes nodos de las Unidades Provinciales a Nivel Nacional.

Estos programas monitorean constantemente todos los eventos suscitados en las redes a nivel nacional, estos lanzan alarmas al momento de detectarse alguna novedad, para de este modo tomar las medidas respectivas pertinentes.

VII. Control de acceso

a) Requerimiento del negocio para el control de acceso

En Ministerio de Inclusión Económica y Social no se encuentran reglas plenamente establecidas en cuanto a las políticas para la divulgación y autorización de la información.

Para que un usuario pueda tener acceso a la información existente en la institución, necesita los permisos necesarios para que pueda contar con una determinada información, para ello requiere formar parte de la institución así como la debida justificación correspondiente.

En el MIES existen dos tipos de usuarios:

- Usuario avanzado.
- Administrador

b) Gestión de acceso del usuario

Una vez que el departamento de Recursos Humanos contrata un nuevo funcionario debe informar de manera oficial al Departamento de Gestión Tecnológica para la creación y asignación de permisos de recursos de red al nuevo usuario.

Con estos datos se procede a la generación del usuario de red, la asignación al grupo de trabajo al que pertenece y los servicios de red que puede contar para el desarrollo de sus actividades.

Básicamente se manejan dos perfiles de usuario: usuario avanzado y administrador.

- **Usuario Avanzado**: Incluyen pocos privilegios administrativos tales como instalación de ciertos aplicativos y ciertos cambios de configuración de sistema operativo.
- **Usuario Administrador**: Existe un manejo completo del computador para su mejor desempeño y es utilizado por personal técnico de la institución.

La administración de usuarios no es una tarea asignada a una sola persona sino que hay más de una realizándola al igual que el manejo de contraseñas para todo el personal del MIES.

En relación a las contraseñas estas son creadas por los técnicos del departamento de acuerdo a un formato establecido, pero esta contraseña puede ser cambiada posteriormente por el nuevo usuario. Adicionalmente las contraseñas deben ser cambiadas por los usuarios periódicamente cada 3 meses.

c) Responsabilidades del usuario

El usuario es responsable de utilizar los servicios de red, únicamente para el desarrollo de las actividades diarias que desempeña. El usuario es el responsable de mantener confidencialidad con los datos y su contraseña de usuario de red, para de esta manera precautelar de la información tanto personal como institucional de la que él está a cargo.

d) Control de acceso a la red

El control de acceso a la red institucional viene siendo controlado por los privilegios asignados a cada usuario.

Estos permisos comprenden la utilización de los servicios de red que el usuario necesita para el desarrollo óptimo de labores diarias.

Este control permite administrar de mejor manera los diferentes servicios de red, únicamente permitiendo el acceso al personal que realmente necesita trabajar con un determinado servicio, por ejemplo mail institucional, acceso a los aplicativos con los que cuenta la institución.

e) Control de acceso al sistema operativo

El control de acceso a los diferentes sistemas operativos con los que cuenta la institución está siendo administrado centralizadamente con la generación de un usuario único para cada funcionario, al cual se le asigna los privilegios con los que ellos cuentan adicionalmente se les asigna una contraseña única.

Mediante esta información el usuario tiene acceso a su información personal en una determinada estación de trabajo de manera única y es la única manera de acceder a los servicios proporcionados a través de la red institucional a nivel nacional.

f) Control de acceso a la aplicación y la información

Para tener acceso a la información institucional o a las diferentes aplicaciones utilizadas el usuario debe tener permisos de acceso a estas, de acuerdo al perfil al que corresponde.

Cada una de las aplicaciones tiene su propio control de acceso, como segunda medida de seguridad, a esta únicamente el usuario puede acceder su cuenta con un usuario de acceso y contraseña para la aplicación que deberá utilizar.

Los usuarios únicamente tienen acceso a la información necesaria para el cumplimiento de sus labores, en ningún momento tienen acceso a información que no es de su competencia.

g) Computación y tele-trabajo móvil

Los medios de computación móvil no se encuentran físicamente protegidos contra robo. No se encuentran definidos procedimientos relacionados a los requerimientos legales, de seguros y otros requerimientos de seguridad del Ministerio para casos de robo o pérdida de los medios móviles. No se define un cuidado especial para asegurar que no se comprometa la información perteneciente al Ministerio.

El personal que utiliza computación móvil no ha establecido un nivel de conciencia sobre los riesgos adicionales que resultan de esta forma de trabajo.

VIII. Adquisición, desarrollo, mantenimiento de los sistemas de información

a) Requerimientos de seguridad de los sistemas de información

Se exige que todo Sistema de Información desarrollado internamente o adquirido a una empresa externa, debe contar con un modulo de seguridad, el cual debe controlar de manera óptima al acceso a la información que este contiene. Adicionalmente debe contar con un sistema de generación de reportes de los diferentes incidentes presentados en el proceso diario de la información institucional.

b) Procesamiento correcto en las aplicaciones

Todas las aplicaciones son monitoreadas de forma diaria, de esta manera se controla la pérdida o mal uso de la información en las aplicaciones. Este monitoreo permite mantener en óptimas condiciones el correcto procesamiento de las aplicaciones que manejan la información de vital importancia para la institución.

c) Controles criptográficos

No se manejan políticas sobre el uso de controles criptográficos para la protección de la confidencialidad, autenticidad e integridad de la información.

d) Seguridad de los archivos del sistema

La seguridad de los archivos de los sistemas utilizados, son establecidos mediante los perfiles asignados a cada usuario, estos perfiles establecen políticas mediante las cuales el usuario que no tiene perfil de Administrador no puede modificar o borrar archivos del sistema o realizar instalaciones de programas nocivos, tanto para los Sistemas de Información como para los Sistemas Operativos.

e) Seguridad en los procesos de desarrollo y soporte

Cuando se desarrolla o se adquiere en forma externa sistemas de aplicación el procedimiento para el desarrollo y pruebas es controlado rigurosamente por la persona responsable del sistema, de manera que el sistema de aplicación se desarrolle de acuerdo a los requerimientos establecidos para no arriesgar la información que manejará el sistema.

f) Gestión de la Vulnerabilidad Técnica

No se manejan políticas sobre la gestión de vulnerabilidades técnicas de los sistemas de información que se utilizan, de manera que se desconocen todos los riesgos a los que esta cartera de estado puede estar expuesta.

IX. Gestión de un incidente en la seguridad de la información

a) Reporte de los eventos y debilidades de la seguridad de la información

No existe una política de reporte de debilidades definida. Cuando se presenta un caso de emergencia se soluciona y se documenta dicho caso especificando lo sucedido y se lo presenta al Director del Departamento de Gestión Tecnológica.

Si los eventos son leves se los documenta en hojas de registros de eventualidades que son controladas periódicamente por el personal del departamento.

b) Gestión de los incidentes y mejoras en la seguridad de la información

Basados en las hojas de registros de eventualidades se controla los incidentes que se han producido, de esta manera se observan los eventos mas comunes y se procura dar una solución para que disminuyan o desaparezcan en su totalidad.

X. Gestión de la continuidad de negocio

a) Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

El ministerio tiene algunas políticas de seguridad, las cuales garantizan un óptimo funcionamiento de las diferentes actividades; después de algún acontecimiento natural o algún incidente fuera de los parámetros normales, que pueda provocar la falla de los servicios informáticos, evitando así la suspensión de las labores.

Para esto, la parte neuronal en donde se encuentran ejecutándose todas las Bases de Datos, sistemas de información, core principal de telecomunicaciones está debidamente acondicionado y protegido en el Centro de Datos de la institución el cual cuenta con las siguientes medidas de seguridad

- Control de Acceso solo a personal debidamente autorizado.
- Sistema de Monitoreo de tos los eventos suscitados con los diferentes equipos informáticos.

- Sistema Contra Incendios, con medidor de temperatura, el cual se dispara automáticamente al encontrar alguna anomalía.
- Sistemas de Alimentación Ininterrumpida UPS redundantes para mantener los servicios en línea en caso de un corte eléctrico no previsto.

Adicionalmente a esto, se cuenta con un backup de todos los servicios principales para el óptimo funcionamiento de la Institución, a nivel de servidores, software, canales dedicados de Internet, backups de la información almacenada en las bases de datos.

XI. Cumplimiento

a) Cumplimiento de los requerimientos legales

La Unidad de Gestión Tecnológica, ha venido normando todos los requerimientos legales que exigen la implementación y soporte técnico de una plataforma tecnológica completa como es el licenciamiento del software utilizado y actualización de plataformas.

b) Cumplimiento de las políticas y estándares de seguridad y cumplimiento técnico

Las políticas y estándares establecidos en la institución para el manejo de toda la plataforma informática implementada, son cumplidas a cabalidad de acuerdo a las normas establecidas en los diferentes manuales de procedimiento.

c) Consideración de auditoría de los sistemas de información

Se ha realizado una auditoría informática a cargo de estudiantes universitarios con propósitos específicamente académicos, los resultados obtenidos solo fueron expuestos al Director del Departamento de Gestión Tecnológica de manera que ningún otro funcionario conoce dichos resultados.

2.2.4 MAPEO ESTANDAR ISO/IECE 17799-2005 – COBIT 4.0

La presente auditoría trata de riesgos informáticos en el departamento de Gestión Tecnológica del MIES, razón por la que se utiliza el estándar ISO/IECE 17799-2005, norma que es perfectamente utilizable en el proyecto ya que se orienta específicamente a la gestión de seguridad de la información. Dado que la norma solo detalla los objetivos de control a evaluar y no proporciona ninguna

herramienta de evaluación, se hace necesaria la utilización del marco de referencia COBIT, mismo que aporta los medios para establecer el nivel de madurez que tienen los procesos de TI y adicionalmente permite plantear mejoras en base a las mejores prácticas promulgadas en el marco de trabajo.

Debido a la utilización de los dos estándares en el proyecto, se requiere de una herramienta que permita llevar a cabo la transición entre ellos, esta herramienta es *Mapping ISO*/IEC *17799*:*2005* With *COBIT* 4.0, tomado del documento COBIT SECURITY BASELINE; donde se realiza un mapeo de los objetivos de control de COBIT con las cláusulas de control del estándar ISO/IECE 17799-2005.

Partiendo de la integración definida en el documento COBIT SECURITY BASELINE, la presente auditoría se limita a utilizar los objetivos de control ya definidos, que corresponden a la evaluación de riesgos informáticos.

Ver *ANEXO 1.* Tabla de integración ISO/IECE 17799-2005 – COBIT 4.0

Realizar el mapeo antes mencionado permite elaborar una evaluación con la cual se conocerá el nivel en que se encuentra el ministerio con respecto a la seguridad de sus recursos y sistemas de información.

2.3 REALIZACIÓN DE LA AUDITORÍA DE RIESGOS INFORMÁTICOS

2.3.1 ALCANCE DE LA AUDITORÍA

Siendo el MIES una entidad importante en el Estado Ecuatoriano, requiere que su activo más importante, la información, esté salvaguardada ante la creciente amenaza de los riesgos informáticos; por ello se llevará a cabo la Auditoría que comenzará con la identificación de los riesgos existentes y potenciales inherentes al Departamento de Gestión Tecnológica, posteriormente se aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles; para finalizar con las conclusiones y recomendaciones para el mejoramiento de la administración de riesgos informáticos.

2.3.2 OBJETIVOS DE LA AUDITORÍA

- Identificar los riesgos informáticos a los que está expuesto el Departamento de Gestión Tecnológica del MIES.

- Aplicar COBIT en la auditoría para establecer mejoras en la administración de riesgos informáticos del Departamento de Gestión Tecnológica del MIES.
- Elaborar el informe de auditoría estableciendo las recomendaciones que ayuden a mitigar el impacto que los riegos informáticos pueden tener en el Departamento de Gestión Tecnológica del MIES.

2.3.3 DETERMINACIÓN DE LOS PROCESOS COBIT REFERENTES A LA AUDITORÍA DE RIESGOS INFORMATICOS.

La determinación de los procesos COBIT implicados para la realización de la auditoría de Riesgos Informáticos en el Departamento de Gestión Tecnológica del Ministerio de Inclusión Económica y Social, fue efectuada de acuerdo al mapeo de los procesos COBIT con la norma ISO anteriormente descrita.

A continuación se detallan los objetivos de control seleccionados por dominios según el Mapeo ISO 17799 y COBIT 4.0, para la realización de la Auditoría de Riesgos Informáticos.

En el *ANEXO 2* se listan los objetivos de control detallados para cada uno de los Objetivos de Control COBIT referentes al presente caso de estudio.

DOMINIO: Planeación y Organización

PO1 Definir el plan estratégico para TI
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica
PO4 Definir procesos, organización y relaciones de TI
PO5 Administrar la inversión de TI
PO6 Comunicar las aspiraciones y la dirección de la gerencia
PO7 Administrar recursos humanos de TI
PO9 Evaluar y Administrar Riesgos de TI
PO10 Administrar proyectos

DOMINIO: Adquirir e Implementar

AI1 Identificar Soluciones Automatizadas
AI2 Adquirir y mantener el software aplicativo

AI3 Adquirir y mantener la infraestructura tecnológica

AI4 Facilitar la operación y el uso

AI5 Adquirir recursos de TI.

AI6 Administrar cambios

AI7 Instalar y Acreditar soluciones y cambios

DOMINIO: Entregar y Dar Soporte

DS2 Administrar servicios de terceros

DS3 Administrar desempeño y capacidad

DS4 Garantizar la Continuidad del Servicio

DS5 Garantizar la Seguridad de los Sistemas

DS7 Educar y entrenar a los usuarios

DS8 Administrar la mesa de servicio y los incidentes

DS9 Administrar la configuración

DS10 Administrar los problemas

DS11 Administrar los datos

DS12 Administrar el ambiente físico

DS13 Administrar las operaciones

DOMINIO: Monitorear Evaluar

ME1 Monitorear y evaluar el desempeño de TI

ME2 Monitorear y evaluar el control interno

ME3 Garantizar cumplimiento regulatorio

2.3.5.1 MODELADO DE MADUREZ DE LOS PROCESOS DE TI

A continuación se presentan los cuadros correspondientes al modelo de madurez para el control interno según COBIT para cada uno de los Objetivos de Control seleccionados, en los que se evalúa el estatus del ambiente de control interno en el Departamento de Gestión Tecnológica del MIES, estableciendo los niveles de madurez adecuados para cada uno de los objetivos de control COBIT.

Esta evaluación se lleva a cabo en base a entrevistas realizadas a funcionarios del departamento con el objetivo de conocer la situación actual de los procesos de TI. El listado de preguntas que se realizaron está en el ANEXO 5.

Donde:

✓ = Si cumple

DOMINIO: PLANEAR Y ORGANIZAR

PO1: DEFINIR EL PLAN ESTRATEGICO DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando: no se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.
✓	**1 Inicial/Ad Hoc** cuando La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requisito de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.
	2 Repetible pero intuitiva cuando: La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.
	3 Proceso definido cuando: Una política define cómo y cuándo realizar la planeación estratégica de TI. La planeación estratégica de TI sigue un enfoque estructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Sin embargo, se otorga discrecionalidad a gerentes individuales específicos con respecto a la implantación del proceso, y no existen procedimientos para analizar el proceso. La estrategia general de TI incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador o como seguidor. Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías. La planeación estratégica de TI se discute en reuniones de la dirección del negocio.
	4 Administrado y medible cuando: La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La planeación estratégica de TI es una función administrativa definida con responsabilidades de alto nivel. La dirección puede monitorear el proceso estratégico de TI, tomar decisiones informadas con base en el plan y medir su efectividad. La planeación de TI de corto y largo plazo sucede y se distribuye en forma de cascada hacia la organización, y las actualizaciones se realizan según son necesarias. La estrategia de TI y la estrategia organizacional se vuelven cada vez más coordinadas al abordar procesos de negocio y capacidades de valor agregado y al aprovechar el uso de aplicaciones y tecnologías por medio de la re-ingeniería de procesos de negocio. Existen procesos bien definidos para determinar e uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas.
	5 Optimizado cuando: La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Las consideraciones de riesgo y de valor agregado se actualizan de modo constante en el proceso de planeación estratégica de TI. Se desarrollan planes realistas a largo plazo de TI y se actualizan de manera constante para reflejar los cambiantes avances tecnológicos y el progreso relacionado al negocio. Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia. El plan estratégico incluye cómo los nuevos avances tecnológicos pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.

Tabla 2.3: Modelo de Madurez PO1

PO2: DEFINIR LA ARQUITECTURA DE LA INFORMACION	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando: No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.
	1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.
✓	**2 Repetible pero intuitiva** cuando: Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas. Los requerimientos tácticos impulsan el desarrollo de los componentes de la arquitectura de la información por parte de los individuos.
	3 Proceso definido cuando: La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información. Las herramientas automatizadas se empiezan a utilizar, aunque los procesos y reglas son definidos por los proveedores de software de bases de datos. Se definen, documentan y aplican actividades formales de entrenamiento de manera formal.
	4 Administrado y medible cuando: Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. La responsabilidad sobre el desempeño del proceso del desarrollo de la arquitectura se refuerza y se mide el éxito de la arquitectura de información. Las herramientas automatizadas de soporte están ampliamente generalizadas, pero todavía no están integradas. Se han identificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es pro-activo y se enfoca en resolver necesidades futuras del negocio. La organización de administración de datos está activamente involucrada en todos los esfuerzos de desarrollo de las aplicaciones, para garantizar la consistencia. Un repositorio automatizado está totalmente implantado. Se encuentran en implantación modelos de datos más complejos para aprovechar el contenido informativo de las bases de datos. Los sistemas de información ejecutiva y los sistemas de soporte a la toma de decisiones aprovechan la información existente.
	5 Optimizado cuando: La arquitectura de información es reforzada de forma consistente a todos los niveles. El valor de la arquitectura de la información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y dar mantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio. La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua. La estrategia para el aprovechamiento de la información por medio de un almacén de datos y tecnologías de minería de datos está bien definida. La arquitectura de la información se encuentra en mejora continua y toma en cuenta información no tradicional sobre los procesos, organizaciones y sistemas.

Tabla 2.4: Modelo de Madurez PO2

PO3: DETERMINAR LA DIRECCION TECNOLOGICA	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento de que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.
	1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implantación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.
✓	**2 Repetible pero intuitiva** cuando Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de los cambios tecnológicos se delega a individuos que siguen procesos intuitivos, aunque similares. Las personas obtienen sus habilidades sobre planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. Están surgiendo técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.
	3 Proceso definido cuando La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional. Los proveedores clave se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos, de forma consistente con la dirección de la organización.
	4 Administrado y medible cuando La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidades necesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentes se toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica ha sido asignada. El proceso para desarrollar el plan de infraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. La estrategia de recursos humanos está alineada con la dirección tecnológica, para garantizar que el equipo de TI pueda administrar los cambios tecnológicos. Los planes de migración para la introducción de nuevas tecnologías están definidos. Los recursos externos y las asociaciones se aprovechan para tener acceso a la experiencia y a las habilidades necesarias. La dirección ha evaluado la aceptación del riesgo de usar la tecnología como líder, o rezagarse en su uso, para desarrollar nuevas oportunidades de negocio o eficiencias operativas.
	5 Optimizado cuando Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avances industriales e internacionales, en lugar de estar orientada por los proveedores de tecnología. El impacto potencial de los cambios tecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe una aprobación ejecutiva formal para el cambio de la dirección tecnológica o para adoptar una nueva. La entidad cuenta con un plan robusto de infraestructura tecnológica que refleja los requerimientos del negocio, es sensible a los cambios en el ambiente del negocio y puede reflejar los cambios en éste. Existe un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica. Las mejores prácticas de la industria se usan de forma amplia para determinar la dirección técnica.

Tabla 2.5: Modelo de Madurez PO3

PO4: DEFINIR LOS PROCESOS , ORGANIZACIÓN Y RELACIONES DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.
	1 Inicial/Ad Hoc cuando Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. IT se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizadas ni reforzadas.
✓	**2 Repetible pero intuitiva** cuando La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores.
	3 Proceso definido cuando Existen roles y responsabilidades definidos para la organización de TI y para terceros. La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno. Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores. La organización de TI está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. Existe una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades está definida e implantada.
	4 Administrado y medible cuando La organización de TI responde de forma pro-activa al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas. Se han aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear la organización deseada y las relaciones. Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional. El equilibrio entre las habilidades y los recursos disponibles internamente, y los que se requieren de organizaciones externas están definidos y reforzados. La estructura organizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesos estratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.
	5 Optimizado cuando La estructura organizacional de TI es flexible y adaptable. Se ponen en funcionamiento las mejores prácticas de la industria. Existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI. La tecnología se aprovecha para apoyar la complejidad y distribución geográfica de la organización. Un proceso de mejora continua existe y está implantado.

Tabla 2.6: Modelo de Madurez PO4

PO5: ADMINISTRAR LA INVERSION DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No existe conciencia de la importancia de la selección y presupuesto de las inversiones en TI. No existe seguimiento o monitoreo de las inversiones y gastos de TI
	1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de administrar la inversión en TI, aunque esta necesidad se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal. Las inversiones en TI se justifican de una forma ad hoc. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.
	2 Repetible pero intuitiva cuando Existe un entendimiento implícito de la necesidad de seleccionar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. El cumplimiento depende de la iniciativa de individuos dentro de la organización. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.
✓	**3 Proceso definido** cuando Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología. El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio. Los procesos de selección de inversiones en TI y de presupuestos están formalizados, documentados y comunicados. Surge el entrenamiento formal aunque todavía se basa de modo principal en iniciativas individuales. Ocurre la aprobación formal de la selección de inversiones en TI y presupuestos. El personal de TI cuenta con la experiencia y habilidades necesarias para desarrollar el presupuesto de TI y recomendar
	4 Administrado y medible cuando La responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan a un individuo específico. Las diferencias en el presupuesto se identifican y se resuelven. Se realizan análisis formales de costos que cubren los costos directos e indirectos de las operaciones existentes, así como propuestas de inversiones, considerando todos los costos a lo largo del ciclo completo de vida. Se usa un proceso de presupuestos pro-activo y estándar. El impacto en los costos operativos y de desarrollo debidos a cambios en hardware y software, hasta cambios en integración de sistemas y recursos humanos de TI, se reconoce en los planes de inversión. Los beneficios y los retornos se calculan en términos financieros y no financieros.
	5 Optimizado cuando Se utilizan las mejores prácticas de la industria para evaluar los costos por comparación e identificar la efectividad de las inversiones. Se utiliza el análisis de los avances tecnológicos en el proceso de selección y presupuesto de inversiones. El proceso de administración de inversiones se mejora de forma continua con base en las lecciones aprendidas provenientes del análisis del desempeño real de las inversiones. Las decisiones de inversiones incluyen las tendencias de mejora de precio/desempeño. Se investigan y evalúan formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital existente en la organización, mediante el uso de métodos formales de evaluación. Existe la identificación pro-activa de varianzas. Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión.

Tabla 2.7: Modelo de Madurez PO5

PO6: COMUNICAR LAS ASPIRACIONES Y LA DIRECCION DE LA GERENCIA	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando La gerencia no ha establecido un ambiente positivo de control de información. No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.
	1 Inicial/Ad Hoc cuando La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.
	2 Repetible pero intuitiva cuando La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales. La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción de gerentes y áreas de negocio individuales. La calidad se reconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales. El entrenamiento se realiza de forma individual, según se requiera.
✓	**3 Proceso definido** cuando La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concientización. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad están estandarizadas y formalizadas.
	4 Administrado y medible cuando La gerencia asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad y asigna suficientes recursos para mantener el ambiente en línea con los cambios significativos. Se ha establecido un ambiente de control de información positivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen y comunican, y forman un componente de buenas prácticas internas. Se ha establecido un marco de trabajo para la implantación y las verificaciones subsiguientes de cumplimiento.
	5 Optimizado cuando El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora. Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación. El monitoreo, la auto-evaluación y las verificaciones de cumplimiento están extendidas en la organización. La tecnología se usa para mantener bases de conocimiento de políticas y de concientización y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado en computadora.

Tabla 2.8: Modelo de Madurez PO6

PO7: ADMINISTRAR LOS RECURSOS DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No existe conciencia sobre la importancia de alinear la administración de recursos humanos de TI con el proceso de planeación de la tecnología para la organización. No hay persona o grupo formalmente responsable de la administración de los recursos humanos de TI.
	1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de contar con administración de recursos humanos de TI. El proceso de administración de recursos humanos de TI es informal y reactivo. El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal de TI. Se está desarrollando la conciencia con respecto al impacto que tienen los cambios rápidos de negocio y de tecnología, y las soluciones cada vez más complejas, sobre la necesidad de nuevos niveles de habilidades y de competencia.
✓	**2 Repetible pero intuitiva** cuando Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar de hacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.
	3 Proceso definido cuando Existe un proceso definido y documentado para administrar los recursos humanos de TI. Existe un plan de administración de recursos humanos. Existe un enfoque estratégico para la contratación y la administración del personal de TI. El plan de entrenamiento formal está diseñado para satisfacer las necesidades de los recursos humanos de TI. Está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.
	4 Administrado y medible cuando La responsabilidad de la elaboración y el mantenimiento de un plan de administración de recursos humanos para TI ha sido asignado a un individuo o grupo con las habilidades y experiencia necesarias para elaborar y mantener el plan. El proceso para elaborar y mantener el plan de administración de recursos humanos de TI responde al cambio. La organización cuenta con métricas estandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de TI con énfasis especial en el manejo del crecimiento y rotación del personal. Las revisiones de compensación y de desempeño se están estableciendo y se comparan con otras organizaciones de TI y con las mejores prácticas de la industria. La administración de recursos humanos es proactiva, tomando en cuenta el desarrollo de un plan de carrera.
	5 Optimizado cuando El plan de administración de recursos humanos de TI se actualiza de forma constante para satisfacer los cambiantes requerimientos del negocio. La administración de recursos humanos de TI está integrada y responde a la dirección estratégica de la entidad. Los componentes de la administración de recursos humanos de TI son consistentes con las mejores prácticas de la industria, tales como compensación, revisiones de desempeño, participación en foros de la industria, transferencia de conocimiento, entrenamiento y adiestramiento. Los programas de entrenamiento se desarrollan para todos los nuevos estándares tecnológicos y productos antes de su implantación en la organización.

Tabla 2.9: Modelo de Madurez PO7

PO9: EVALUAR Y ADMINISTRAR RIESGOS DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
✓	**0 No existente** cuando La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI
	1 Inicial/Ad Hoc cuando Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan a gerentes específicos con poca frecuencia. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.
	2 Repetible pero intuitiva cuando Existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implantación donde se identifican riesgos.
	3 Proceso definido cuando Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.
	4 Administrado y medible cuando La evaluación y administración de riesgos son procesos estándar. Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI. La administración de riesgos de TI es una responsabilidad de alto nivel. Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI. La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con la TI. La gerencia puede monitorear la posición de riesgo y tomar decisiones informadas respecto a la exposición que está dispuesta a aceptar. Todos los riesgos identificados tienen un propietario denominado, y la alta dirección, así como la gerencia de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar. La gerencia de TI ha elaborado medidas estándar para evaluar el riesgo y para definir las proporciones riesgo/retorno. La gerencia presupuesta para que un proyecto operativo de administración de riesgos re-evalúe los riesgos de manera regular. Se establece una base de datos administrativa y parte del proceso de administración de riesgos se empieza a automatizar. La gerencia de TI toma en cuenta las estrategias de mitigación de riesgo.
	5 Optimizado cuando La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detectará y actuará cuando se realicen decisiones grandes de inversión, operación o de TI, sin tomar en cuenta el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.

Tabla 2.10: Modelo de Madurez PO9

PO10: ADMINISTRAR PROYECTOS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando Las técnicas de administración de proyectos no se usan y la organización no toma en cuenta los impactos al negocio asociados con la mala administración de los proyectos y con las fallas de desarrollo en el proyecto
✓	**1 Inicial/Ad Hoc** cuando El uso de técnicas y enfoques de administración de proyectos dentro de TI es una decisión individual que se deja a los gerentes de TI. Existe una carencia de compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos. Las decisiones críticas sobre administración de proyectos se realizan sin la intervención de la gerencia usuaria ni del cliente. Hay poca o nula participación del cliente y del usuario para definir los proyectos de TI. No hay una organización clara dentro de TI para la administración de proyectos. Los roles y responsabilidades para la administración de proyectos no están definidas. Los proyectos, calendarios y puntos clave están definidos pobremente, si es que lo están. No se hace seguimiento al tiempo y a los gastos del equipo del proyecto y no se comparan con el presupuesto.
	2 Repetible pero intuitiva cuando La alta dirección ha obtenido y comunicado la conciencia de la necesidad de una administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos de proyecto a proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción del gerente de proyecto.
	3 Proceso definido cuando El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados. Los proyectos de TI se definen con los objetivos técnicos y de negocio adecuados. La alta dirección del negocio y de TI, empiezan a comprometerse y a participar en la administración de los proyectos de TI. Se ha establecido una oficina de administración de proyectos dentro de TI, con roles y responsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, calendarios y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento en administración de proyectos es un resultado principalmente de las iniciativas individuales del equipo. Los procedimientos de aseguramiento de calidad y las actividades de implantación post-sistema han sido definidos, pero no se aplican de manera amplia por parte de los gerentes de TI. Los proyectos se empiezan a administrar como portafolios.
	4 Administrado y medible cuando La gerencia requiere que se revisen métricas y lecciones aprendidas estandarizadas y formales después de terminar cada proyecto. La administración de proyectos se mide y evalúa a través de la organización y no solo en TI. Las mejoras al proceso de administración de proyectos se formalizan y comunican y los miembros del equipo reciben entrenamiento sobre estas mejoras. La gerencia de TI ha implantado una estructura organizacional de proyectos con roles, responsabilidades y criterios de desempeño documentados. Los criterios para evaluar el éxito en cada punto clave se han establecido. El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos. Cada vez más, los proyectos abordan las metas organizacionales, en lugar de abordar solamente las específicas a TI. Existe un apoyo fuerte y activo a los proyectos por parte de los patrocinadores de la alta dirección, así como de los interesados. El entrenamiento relevante sobre administración de proyectos se planea para el equipo en la oficina de proyectos y a lo largo de la función de TI.
	5 Optimizado cuando Se encuentra implantada una metodología comprobada de ciclo de vida de proyectos, la cual se refuerza y se integra en la cultura de la organización completa. Se ha implantado una iniciativa continua para identificar e institucionalizar las mejores prácticas de administración de proyectos. Se ha definido e implantado una estrategia de TI para contratar el desarrollo y los proyectos operativos. La oficina integrada de administración de proyectos es responsable de los proyectos y programas desde su concepción hasta su post-implantación. La planeación de programas y proyectos en toda la organización garantiza que los recursos de TI y del usuario se utilizan de la mejor manera para apoyar las iniciativas estratégicas.

Tabla 2.11: Modelo de Madurez PO10

DOMINIO: ADQUIRIR E IMPLEMENTAR

AI1: IDENTIFICAR SOLUCIONES AUTOMATIZADAS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando La organización no requiere de la identificación de los requerimientos funcionales y operativos para el desarrollo, implantación o modificación de soluciones, tales como sistemas, servicios, infraestructura y datos. La organización no está consciente de las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.
	1 Inicial/Ad Hoc cuando Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas. Grupos individuales se reúnen para analizar las necesidades de manera informal y los requerimientos se documentan algunas veces. Los individuos identifican soluciones con base en una conciencia limitada de mercado o como respuesta a ofertas de proveedores. Existe una investigación o análisis estructurado mínimo de la tecnología disponible.
	2 Repetible pero intuitiva cuando Existen algunos enfoques intuitivos para identificar que existen soluciones de TI y éstos varían a lo largo del negocio. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de unos cuantos individuos clave. La calidad de la documentación y de la toma de decisiones varía de forma considerable. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.
	3 Proceso definido cuando Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.
✓	**4 Administrado y medible** cuando Existe una metodología establecida para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos. La documentación de los proyectos es de buena calidad y cada etapa se aprueba adecuadamente. Los requerimientos están bien articulados y de acuerdo con las estructuras predefinidas. Se consideran soluciones alternativas, incluyendo el análisis de costos y beneficios. La metodología es clara, definida, generalmente entendida y medible. Existe una interfaz definida de forma clara entre la gerencia de TI y la del negocio para la identificación y evaluación de las soluciones de TI.
	5 Optimizado cuando La metodología para la identificación y evaluación de las soluciones de TI está sujeta a una mejora continua. La metodología de adquisición e implantación tiene la flexibilidad para proyectos de grande y de pequeña escala. La metodología está soportada en bases de datos de conocimiento internas y externas que contienen material de referencia sobre soluciones tecnológicas. La metodología en sí misma genera documentación en una estructura predefinida que hace que la producción y el mantenimiento sean eficientes. Con frecuencia, se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general. La gerencia detecta y toma medidas si las soluciones de TI se aprueban sin considerar tecnologías alternativas o los requerimientos funcionales del negocio.

Tabla 2.12: Modelo de Madurez AI1

AI2: ADQUIRIR Y MANTENER EL SOFTWARE APLICATIVO	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.
	1 Inicial/Ad Hoc cuando Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición y mantenimientos de software aplicativo varían de un proyecto a otro. Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.
	2 Repetible pero intuitiva cuando Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro de la operación de TI. El mantenimiento es a menudo problemático y se resiente cuando se pierde el conocimiento interno de la organización. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.
✓	**3 Proceso definido** cuando Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia de TI y del negocio. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que se salten pasos. Las actividades de mantenimiento se planean, programan y coordinan.
	4 Administrado y medible cuando Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso de prueba y requerimientos para la documentación. Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones. Han evolucionado prácticas y procedimientos para ajustarlos a la medida de la organización, los utilizan todo el personal y son apropiados para la mayoría de los requerimientos de aplicación.
	5 Optimizado cuando Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base en componentes, con aplicaciones predefinidas y estandarizadas que corresponden a las necesidades del negocio. El enfoque se extiende para toda la empresa. La metodología de adquisición y mantenimiento presenta un buen avance y permite un posicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantes del negocio. La metodología de adquisición e implantación de software aplicativo ha sido sujeta a mejora continua y se soporta con bases de datos internas y externas que contienen materiales de referencia y las mejores prácticas. La metodología produce documentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento.

Tabla 2.13: Modelo de Madurez AI2

AI3: ADQUIRIR Y MANTENER LA INFRAESTRUCTURA TECNOLOGICA	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.
✓	**1 Inicial/Ad Hoc** cuando Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.
	2 Repetible pero intuitiva cuando No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.
	3 Proceso definido cuando Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.
	4 Administrado y medible cuando Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.
	4 Administrado y medible cuando Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.

Tabla 2.14: Modelo de Madurez AI3

AI4: FACILITAR LA OPERACIÓN Y EL USO	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.
✓	**1 Inicial/Ad Hoc** cuando Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.
	2 Repetible pero intuitiva cuando Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.
	3 Proceso definido cuando Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.
	4 Administrado y medible cuando Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas y las unidades de negocio, de manera que se pueden observar los procesos desde una perspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfaces. Existen controles para garantizar que se adhieren los estándares y que se desarrollan y mantienen procedimientos para todos los procesos. La retroalimentación del negocio y del usuario sobre la documentación y el entrenamiento se recopila y evalúa como parte de un proceso continuo de mejora. Los materiales de documentación y entrenamiento se encuentran generalmente a un buen nivel, predecible, de confiabilidad y disponibilidad. Se implanta un proceso emergente para el uso de documentación y administración automatizada de procedimiento. El desarrollo automatizado de procedimientos se integra cada vez más con el desarrollo de sistemas aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega de documentación, materiales y programas de entrenamiento.
	5 Optimizado cuando El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante que se mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, workflow y tecnologías de distribución, que los hacen accesibles y fáciles de mantener. El material de documentación y entrenamiento se actualiza para reflejar los cambios en la organización, en la operación y en el software. Tanto el desarrollo de materiales de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones de proceso del negocio, siendo así un apoyo a los requerimientos de toda la organización y no tan sólo procedimientos orientados a TI.

Tabla 2.15: Modelo de Madurez AI4

AI5: ADQUIRIR RECURSOS DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No existe un proceso definido de adquisición de recursos de TI. La organización no reconoce la necesidad de tener políticas y procedimientos claros de adquisición para garantizar que todos los recursos de TI se encuentren disponibles y de forma oportuna y rentable.
	1 Inicial/Ad Hoc cuando La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe un relación *ad hoc* entre los procesos de administración de adquisiciones y contratos corporativos y TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.
	2 Repetible pero intuitiva cuando Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización del negocio. Los procesos de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.
	3 Proceso definido cuando La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos. La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de TI.
✓	**4 Administrado y medible** cuando La adquisición de TI se integra totalmente con los sistemas generales de adquisición de la organización. Se utilizan los estándares para la adquisición de recursos de TI en todos los procesos de adquisición. Se toman medidas para la administración de contratos y adquisiciones relevantes para los casos de negocio que requiran la adquisición de TI. Se dispone de reportes que sustentan los objetivos de negocio. La administración está consciente por lo general, de las excepciones a las políticas y procedimientos para la adquisición de TI. Se está desarrollando una administración estratégica de relaciones. La administración de TI implanta el uso de procesos de administración para adquisición y contratos en todas las adquisiciones mediante la revisión de medición al desempeño.
	5 Optimizado cuando La administración instituye y da recursos a procesos exhaustivos para la adquisición de TI. La administración impulsa el cumplimiento de las políticas y procedimientos de adquisición de TI. Se toman las medidas en la administración de contratos y adquisiciones, relevantes en casos de negocio para adquisición de TI. Se establecen buenas relaciones con el tiempo con la mayoría de los proveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Los estándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejan estratégicamente y responden a la medición del proceso. La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI.

Tabla 2.16: Modelo de Madurez AI5

AI6: ADMINISTRAR CAMBIOS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio
	1 Inicial/Ad Hoc cuando Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.
✓	**2 Repetible pero intuitiva** cuando Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio.
	3 Proceso definido cuando Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado. Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente. El análisis de impacto de los cambios de TI en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.
	4 Administrado y medible cuando El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. El proceso es eficiente y efectivo, pero se basa en manuales de procedimientos y controles considerables para garantizar el logro de la calidad. Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción. Se da un proceso de aprobación para cambios. La documentación de administración de cambios es vigente y correcta, con seguimiento formal a los cambios. La documentación de configuración es generalmente exacta. La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio. Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio. Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.
	5 Optimizado cuando El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas. El proceso de revisión refleja los resultados del monitoreo. La información de la configuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.

Tabla 2.17: Modelo de Madurez AI6

AI7: INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando Hay una ausencia completa de procesos formales de instalación o acreditación y ni la gerencia senior ni el personal de TI reconocen la necesidad de verificar que las soluciones se ajustan para el propósito deseado.
✓	**1 Inicial/Ad Hoc** cuando Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares y los enfoques que se toman varían. La acreditación formal y la autorización son raras o no existentes.
	2 Repetible pero intuitiva cuando Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología. Los equipos individuales de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.
	3 Proceso definido cuando Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto. El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales. La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación.
	4 Administrado y medible cuando Los procedimientos son formales y se desarrollan para ser organizados y prácticos con ambientes de prueba definidos y con procedimientos de acreditación. En la práctica, todos los cambios mayores de sistemas siguen este enfoque formal. La evaluación de la satisfacción a los requerimientos del usuario es estándar y medible, y produce mediciones que la gerencia puede revisar y analizar de forma efectiva. La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, aún con niveles razonables de problemas posteriores a la implantación. La automatización del proceso es *ad hoc* y depende del proyecto. Es posible que la gerencia esté satisfecha con el nivel actual de eficiencia a pesar de la ausencia de una evaluación posterior a la implantación. El sistema de prueba refleja adecuadamente el ambiente de producción. La prueba de stress para los nuevos sistemas y la prueba de regresión para sistemas existentes se aplican para proyectos mayores.
	5 Optimizado cuando Los procesos de instalación y acreditación se han refinado a un nivel de buena práctica, con base en los resultados de mejora continua y refinamiento. Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente de entrenamiento, pruebas y transición a producción para los nuevos sistemas. Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción. La acreditación toma lugar regularmente sin repetición de trabajos, y los problemas posteriores a la implantación se limitan normalmente a correcciones menores. Las revisiones posteriores a la implantación son estándar, y las lecciones aprendidas se canalizan nuevamente hacia el proceso para asegurar el mejoramiento continuo de la calidad. Las pruebas de stress para los nuevos sistemas y las pruebas de regresión para sistemas modificados se aplican en forma consistente.

Tabla 2.18: Modelo de Madurez AI7

DOMINIO: ENTREGAR Y DAR SOPORTE

DS2: ADMINISTRAR SERVICIOS DE TERCEROS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando Las responsabilidades y la rendición de cuentas no están definidas. No hay políticas y procedimientos formales respecto a la contratación con terceros. Los servicios de terceros no son ni aprobados ni revisados por la gerencia. No hay actividades de medición y los terceros no reportan. A falta de una obligación contractual de reportar, la alta gerencia no está al tanto de la calidad del servicio prestado.
✓	**1 Inicial/Ad Hoc** cuando La gerencia está consciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. No hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva. Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).
	2 Repetible pero intuitiva cuando El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.
	3 Proceso definido cuando Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operacionales y de control. Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero esta valorado y reportado.
	4 Administrado y medible cuando Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, calendario, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.
	5 Optimizado cuando Los contratos firmados con los terceros son revisados de forma periódica en intervalos predefinidos. La responsabilidad de administrar a los proveedores y la calidad de los servicios prestados está asignada. Se monitorea el cumplimiento de las condiciones operacionales, legales y de control y se implantan acciones correctivas. El tercero está sujeto a revisiones periódicas independientes y se le retroalimenta sobre su desempeño para mejorar la prestación del servicio. Las mediciones varían como respuesta a los cambios en las condiciones del negocio. Las mediciones ayudan a la detección temprana de problemas potenciales con los servicios de terceros. La notificación completa y bien definida del cumplimiento de los niveles de servicio, está asociada con la compensación del tercero. La gerencia ajusta el proceso de adquisición y monitoreo de servicios de terceros con base en los resultados de los KPIs y KGIs.

Tabla 2.19: Modelo de Madurez DS2

DS3: ADMINISTRAR DESEMPEÑO Y CAPACIDAD	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando La gerencia no reconoce que los procesos clave del negocio pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.
✓	**1 Inicial/Ad Hoc** cuando Los usuarios, con frecuencia, tienen que llevar acabo soluciones alternas para resolver las limitaciones de desempeño y capacidad. Los responsables de los procesos del negocio valoran poco la necesidad de llevar a cabo una planeación de la capacidad y del desempeño. Las acciones para administrar el desempeño y la capacidad son típicamente reactivas. El proceso de planeación de la capacidad y el desempeño es informal. El entendimiento sobre la capacidad y el desempeño de TI, actual y futuro, es limitado.
	2 Repetible pero intuitivo cuando Los responsables del negocio y la gerencia de TI están concientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.
	3 Proceso definido cuando Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.
	4 Administrado y medible cuando Hay procesos y herramientas disponibles para medir el uso del sistema, el desempeño y la capacidad, y los resultados se comparan con metas definidas. Hay información actualizada disponible, brindando estadísticas de desempeño estandarizadas y alertando sobre incidentes causados por falta de desempeño o de capacidad. Los problemas de falta de desempeño y de capacidad se enfrentan de acuerdo con procedimientos definidos y estandarizados. Se utilizan herramientas automatizadas para monitorear recursos específicos tales como espacios en disco, redes, servidores y compuertas de red. Las estadísticas de desempeño y capacidad son reportadas en términos de los procesos de negocio, de forma que los usuarios y los clientes comprendan los niveles de servicio de TI. Los usuarios se sienten por lo general satisfechos con la capacidad del servicio actual y pueden solicitar nuevos y mejores niveles de disponibilidad. Se han acordado los KGIs y KPIs para medir el desempeño y la capacidad de TI, pero puede ser que se aplican de forma esporádica e inconsistente.
	5 Optimizado cuando Los planes de desempeño y capacidad están completamente sincronizados con las proyecciones de demanda del negocio. La infraestructura de TI y la demanda del negocio están sujetas a revisiones regulares para asegurar que se logre una capacidad óptima con el menor costo posible. Las herramientas para monitorear recursos críticos de TI han sido estandarizadas y usadas a través de diferentes plataformas y vinculadas a un sistema de administración de incidentes a lo largo de toda la organización. Las herramientas de monitoreo detectan y pueden corregir automáticamente problemas relacionados con la capacidad y el desempeño. Se llevan a cabo análisis de tendencias, los cuales muestran problemas de desempeño inminentes causados por incrementos en los volúmenes de negocio, lo que permite planear y evitar problemas inesperados. Las métricas para medir el desempeño y la capacidad de TI han sido bien afinadas dentro de los KGIs y KPIs para todos los procesos de negocio críticos y se miden de forma regular. La gerencia ajusta la planeación del desempeño y la capacidad siguiendo los análisis de los KGIs y KPIs.

Tabla 2.20: Modelo de Madurez DS3

DS4: GARANTIZAR LA CONTINUIDAD DEL SERVICIO	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.
✓	**1 Inicial/Ad Hoc** cuando Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.
	2 Repetible pero intuitivo cuando Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.
	3 Proceso definido cuando La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir capacitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.
	4 Administrado y medible cuando Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda capacitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.
	5 Optimizado cuando Los procesos integrados de servicio continuo toman en cuenta referencias de la industria y las mejores prácticas externas. El plan de continuidad de TI está integrado con los planes de continuidad del negocio y se le da mantenimiento de manera rutinaria. El requerimiento para asegurar continuidad es garantizado por los proveedores y principales distribuidores. Se realizan pruebas globales de continuidad del servicio, y los resultados de las pruebas se utilizan para actualizar el plan. La recopilación y el análisis de datos se utilizan para mejorar continuamente el proceso. Las prácticas de disponibilidad y la continua planeación de la continuidad están totalmente alineadas. La gerencia asegura que un desastre o un incidente mayor no ocurrirá como resultado de un punto único de falla. Las prácticas de escalamiento se entienden y se hacen cumplir a fondo. Los KGIs y KPIs sobre el cumplimiento de la continuidad de los servicios se miden de manera sistemática. La gerencia ajusta la planeación de continuidad como respuesta a los KGIs y KPIs.

Tabla 2.21: Modelo de Madurez DS4

DS5: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.
	1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.
	2 Repetible pero intuitivo cuando Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.
✓	**3 Proceso definido** cuando Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.
	4 Administrado y Medible cuando Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.
	5 Optimizado cuando La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan acabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIs para ajustar el plan de seguridad en un proceso de mejora continua.

Tabla 2.22: Modelo de Madurez DS5

DS7: EDUCAR Y ENTRENAR USUARIOS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
✓	**0 No-existente** cuando Hay una total falta de programas de entrenamiento y educación. La organización no reconoce que hay un problema a ser atendido respecto al entrenamiento y no hay comunicación sobre el problema.
	1 Inicial/Ad Hoc cuando Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre la seguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.
	2 Repetible pero intuitivo cuando Hay conciencia sobre la necesidad de un programa de entrenamiento y educación, y sobre los procesos asociados a lo largo de toda la organización. El entrenamiento está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se han desarrollado hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores, cubriendo los mismos temas de materias con diferentes puntos de vista. Algunas de las clases abordan los temas de conducta ética y de conciencia sobre prácticas y actividades de seguridad en los sistemas. Hay una gran dependencia del conocimiento de los individuos. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.
	3 Proceso definido cuando El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento y educación son monitoreados, pero no todas las desviaciones son susceptibles de detección por parte de la gerencia. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.
	4 Administrado y medible cuando Hay un programa completo de entrenamiento y educación que produce resultados medibles. Las responsabilidades son claras y se establece la propiedad sobre los procesos. El entrenamiento y la educación son componentes de los planes de carrera de los empleados. La gerencia apoya y asiste a sesiones de entrenamiento y de educación. Todos los empleados reciben entrenamiento sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. Todos los empleados reciben el nivel apropiado de entrenamiento sobre prácticas de seguridad en los sistemas para proteger contra daños originados por fallas que afecten la disponibilidad, la confidencialidad y la integridad. La gerencia monitorea el cumplimiento por medio de revisión constante y actualización del programa y de los procesos de entrenamiento. Los procesos están en vía de mejora y fomentan las mejores prácticas internas.
	5 Optimizado cuando El entrenamiento y la educación dan como resultado la mejora del desempeño individual. El entrenamiento y la educación son componentes críticos de los planes de carrera de los empelados. Se asignan suficientes presupuestos, recursos, instalaciones e instructores para los programas de entrenamiento y educación. Los procesos se afinan y están en continua mejora, tomando ventaja de las mejores prácticas externas y de modelos de madurez de otras organizaciones. Todos los problemas y desviaciones se analizan para identificar las causas de raíz, se identifican y llevan a cabo acciones de forma expedita. Hay una actitud positiva con respecto a la conducta ética y respecto a los principios de seguridad en los sistemas. La TI se utiliza de manera amplia, integral y óptima para automatizar y brindar herramientas para los programas de entrenamiento y educación. Se utilizan expertos externos en entrenamiento y se utilizan benchmarks del mercado como orientación.

Tabla 2.23: Modelo de Madurez DS7

	NIVEL DE MADUREZ
	0 No-existente cuando No hay soporte para resolver problemas y preguntas de los usuarios. Hay una completa falta de procesos para la administración de incidentes. La organización no reconoce que hay un problema que atender.
	1 Inicial/Ad Hoc cuando La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan.
✓	**2 Repetible pero intuitivo** cuando Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo.
	3 Proceso definido cuando Se reconoce y se acepta la necesidad de contar con una función de mesa de servicio y un proceso para la administración de incidentes. Los procedimientos se estandarizan y documentan, pero se lleva acabo entrenamiento informal. Se deja la responsabilidad al individuo de conseguir entrenamiento y de seguir los estándares. Se desarrollan guías de usuario y preguntas frecuentes (FAQs), pero los individuos deben encontrarlas y puede ser que no las sigan. Las consultas y los incidentes se rastrean de forma manual y se monitorean de forma individual, pero no existe un sistema formal de reporte. No se mide la respuesta oportuna a las consultas e incidentes y los incidentes pueden quedar sin resolución. Los usuarios han recibido indicaciones claras de dónde y cómo reportar problemas e incidentes.
	4 Administrado y medible cuando En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está capacitado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.
	5 Optimizado cuando El proceso de administración de incidentes y la función de mesa de servicio están bien organizados y establecidos y se llevan a cabo con un enfoque de servicio al cliente ya que son expertos, enfocados al cliente y útiles. Los KPIs y KGIs son medidos y reportados sistemáticamente. Una amplia y extensa cantidad de preguntas frecuentes son parte integral de la base de conocimientos. Existen a disposición del usuario, herramientas para llevar a cabo auto diagnósticos y para resolver incidentes. La asesoría es consistente y los incidentes se resuelven de forma rápida dentro de un proceso estructurado de escalamiento. La gerencia utiliza una herramienta integrada para obtener estadísticas de desempeño del proceso de administración de incidentes y de la función de mesa de servicio. Los procesos han sido afinados al nivel de las mejores prácticas de la industria, con base en los resultados del análisis de los KPIs y KGIs, de la mejora continua y de benchmarking con otras organizaciones.

Tabla 2.24: Modelo de Madurez DS8

DS9: ADMINISTRAR LA CONFIGURACION	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando La gerencia no valora los beneficios de tener un proceso implementado que sea capaz de reportar y administrar las configuraciones de la infraestructura de TI, tanto para configuraciones de hardware como de software.
✓	**1 Inicial/Ad Hoc** cuando Se reconoce la necesidad de contar con una administración de configuración. Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de hardware y software pero de manera individual. No están definidas prácticas estandarizadas.
	2 Repetible pero intuitivo cuando La gerencia esta consciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales como administración de cambios y administración de problemas.
	3 Proceso definido cuando Los procedimientos y las prácticas de trabajo se han documentado, estandarizado y comunicado, pero la capacitación y la aplicación de estándares dependen del individuo. Además se han implementado herramientas similares de administración de configuración entre plataformas. Es poco probable detectar las desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se lleva a cabo algún tipo de automatización para ayudar a rastrear cambios en el software o en el hardware. La información de la configuración es utilizada por los procesos interrelacionados.
	4 Administrado y medible cuando En todos los niveles de la organización se reconoce la necesidad de administrar la configuración y las buenas prácticas siguen evolucionando. Los procedimientos y los estándares se comunican e incorporan a la capacitación y las desviaciones son monitoreadas, rastreadas y reportadas. Se utilizan herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad. Los sistemas de administración de configuraciones cubren la mayoría de los activos de TI y permiten una adecuada administración de liberaciones y control de distribución. Los análisis de excepciones, así como las verificaciones físicas, se aplican de manera consistente y se investigan las causas desde su raíz.
	5 Optimizado cuando Todos los activos de TI se administran en un sistema central de configuraciones que contiene toda la información necesaria acerca de los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Hay una completa integración de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los reportes de auditoría de los puntos de referencia, brindan información esencial sobre el software y hardware con respecto a reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se fomentan las reglas para limitar la instalación de software no autorizado. La gerencia proyecta las reparaciones y las actualizaciones utilizando reportes de análisis que proporcionan funciones de programación de actualizaciones y de renovación de tecnología. El rastreo de activos y el monitoreo de activos individuales de TI los protege y previene de robo, de mal uso y de abusos.

Tabla 2.25: Modelo de Madurez DS9

DS10: ADMINISTRAR LOS PROBLEMAS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.
	1 Inicial/Ad Hoc cuando Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.
✓	**2 Repetible pero intuitivo** cuando Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.
	3 Proceso definido cuando Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y capacitación. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.
	4 Administrado y medible cuando El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramente establecidas. Los métodos y los procedimientos son documentados, comunicados y medidos para evaluar su efectividad. La mayoría de los problemas están identificados, registrados y reportados, y su solución ha iniciado. El conocimiento y la experiencia se cultivan, mantienen y desarrollan hacia un nivel más alto a medida que la función es vista como un activo y una gran contribución al logro de las metas de TI y a la mejora de los servicios de TI. La administración de problemas está bien integrada con los procesos interrelacionados, tales como administración de incidentes, de cambios, y de configuración, y ayuda a los clientes para administrar información, instalaciones y operaciones. Se han acordado los KPIs y KGIs para el proceso de administración de problemas.
	5 Optimizado cuando El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones de problemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.

Tabla 2.26: Modelo de Madurez DS10

DS11: ADMINISTRAR LOS DATOS	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando Los datos no son reconocidos como parte de los recursos y los activos de la empresa. No está asignada la propiedad sobre los datos o sobre la rendición de cuentas individual sobre la administración de los datos. La calidad y la seguridad de los datos son deficientes o inexistentes.
	1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal. No se lleva a cabo capacitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Los procedimientos de respaldo y recuperación y los acuerdos sobre desechos están en orden.
	2 Repetible pero intuitivo cuando A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos son documentados por individuos clave. Se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.
✓	**3 Proceso definido** cuando Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos / recuperación y desecho de equipo. Se lleva a cabo algún tipo de monitoreo sobre la administración de datos. Se definen métricas básicas de desempeño. Comienza a aparecer el entrenamiento sobre administración de información.
	4 Administrado y medible cuando Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización. La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización. Los procedimientos se formalizan y son ampliamente conocidos, el conocimiento se comparte. Comienza a aparecer el uso de herramientas. Se acuerdan con los clientes los indicadores de desempeño y meta y se monitorean por medio de un proceso bien definido. Se lleva a cabo entrenamiento formal para el personal de administración de los datos.
	5 Optimizado cuando Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva. Las responsabilidades sobre la propiedad de los datos y la administración de los mismos están establecidas de forma clara, se conocen ampliamente a lo largo de la organización y se actualizan periódicamente. Los procedimientos se formalizan y se conocen ampliamente, la compartición del conocimiento es una práctica estándar. Se utilizan herramientas sofisticadas con un máximo de automatización de la administración de los datos. Se acuerdan con los clientes los indicadores de desempeño y meta, se ligan con los objetivos del negocio y se monitorean de manera regular utilizando un proceso bien definido. Se exploran constantemente oportunidades de mejora. El entrenamiento para el personal de administración de datos se institucionaliza.

Tabla 2.27: Modelo de Madurez DS11

DS12: ADMINISTRAR EL AMBIENTE FISICO	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.
	1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.
✓	**2 Repetible pero intuitivo** cuando Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.
	3 Proceso definido cuando Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.
	4 Administrado y medible cuando Se entiende por completo la necesidad de mantener un ambiente de cómputo controlado y se evidencia en la estructura organizacional y en la distribución del presupuesto. Los requerimientos de seguridad físicos y ambientales están documentados y el acceso se monitorea y controla estrictamente. Se establecen y comunican las responsabilidades. El personal de las instalaciones ha sido entrenado por completo respecto a situaciones de emergencia, así como en prácticas de salud y seguridad. Están implementados mecanismos de control estandarizados para la restricción de accesos a instalaciones y para contrarrestar los factores ambientales y de seguridad. La gerencia monitorea la efectividad de los controles y el cumplimiento de los estándares establecidos. La gerencia ha establecido KPIs y KGIs para medir la administración del ambiente de cómputo. La capacidad de recuperación de los recursos de cómputo se incorpora en un proceso organizacional de administración de riesgos. La información integrada se usa para optimizar la cobertura de los seguros y de los costos asociados.
	5 Optimizado cuando Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente cómputo de la organización. Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.). Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización. El acceso es monitoreado continuamente y controlado estrictamente con base en las necesidades del trabajo, los visitantes son acompañados en todo momento. El ambiente se monitorea y controla por medio de equipo especializado y las salas de equipo funcionan sin operadores humanos. Los KPIs y KGIs se miden regularmente. Los programas de mantenimiento preventivo fomentan un estricto apego a los horarios y se aplican pruebas regulares a los equipos sensibles. Las estrategias de instalaciones y de estándares están alineadas con las metas de disponibilidad de los servicios de TI y están integradas con la administración de crisis y con la planeación de continuidad del negocio. La gerencia revisa y optimiza las instalaciones utilizando los KPIs y KGIs de manera continua, capitalizando oportunidades para mejorar la contribución al negocio.

Tabla 2.28: Modelo de Madurez DS12

DS13: ADMINISTRAR LAS OPERACIONES	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No-existente cuando La organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.
	1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen.
✓	**2 Repetible pero intuitivo** cuando La organización esta consciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Se asignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de capacitación para el operador y hay algunos estándares de operación formales.
	3 Proceso definido cuando Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna capacitación durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas de manera formal. Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia. Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.
	4 Administrado y medible cuando Las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y la propiedad está asignada. Las operaciones se soportan a través de presupuestos de recursos para gastos de capital y de recursos humanos. La capacitación se formaliza y está en proceso. Las programaciones y las tareas se documentan y comunican, tanto a la función interna de TI como a los clientes del negocio. Es posible medir y monitorear las actividades diarias con acuerdos estandarizados de desempeño y de niveles de servicio establecidos. Cualquier desviación de las normas establecidas es atendida y corregida de forma rápida. La gerencia monitorea el uso de los recursos de cómputo y la terminación del trabajo o de las tareas asignadas. Existe un esfuerzo permanente para incrementar el nivel de automatización de procesos como un medio de mejora continua. Se establecen convenios formales de mantenimiento y servicio con los proveedores. Hay una completa alineación con los procesos de administración de problemas, capacidad y disponibilidad, soportados por un análisis de causas de errores y fallas.
	5 Optimizado cuando Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima. Los procesos de administración de operaciones de TI están estandarizados y documentados en una base de conocimiento, y están sujetos a una mejora continua. Los procesos automatizados que soportan los sistemas contribuyen a un ambiente estable. Todos los problemas y fallas se analizan para identificar la causa que los originó. Las reuniones periódicas con los responsables de administración del cambio garantizan la inclusión oportuna de cambios en las programaciones de producción. En colaboración con los proveedores, el equipo se analiza respecto a posibles síntomas de obsolescencia y fallas, y el mantenimiento es principalmente de naturaleza preventiva.

Tabla 2.29: Modelo de Madurez DS13

DOMINIO: MONITOREAR Y EVALUAR

ME1: MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de forma independiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de los procesos no se reconoce.
	1 Inicial/Ad Hoc cuando La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.
✓	**2 Repetible pero intuitiva** cuando Se han identificado algunas mediciones básicas a ser monitoreadas. Los métodos y las técnicas de recolección y evaluación existen, pero los procesos no se han adoptado en toda la organización. La interpretación de los resultados del monitoreo se basa en la experiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.
	3 Proceso definido cuando La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se han definido, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de satisfacción del cliente y los niveles de servicio están definidas. Se ha definido un marco de trabajo para medir el desempeño.
	4 Administrado y medible cuando La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechan en toda la organización para recolectar y monitorear la información operativa de las aplicaciones, sistemas y procesos. La gerencia puede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas. Las mediciones de la función de TI están alienadas con las metas de toda la organización.
	5 Optimizado cuando Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos, tales como el Balanced Scorecard. El monitoreo de los procesos y el rediseño continuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización. Benchmarks contra la industria y los competidores clave se han formalizado, con criterios de comparación bien entendidos.

Tabla 2.30: Modelo de Madurez ME1

ME2: MONITOREAR Y EVALUAR EL CONTROL INTERNO	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando La organización carece de procedimientos para monitorear la efectividad de los controles internos. Los métodos de reporte de control interno gerenciales no existen. Existe una falta generalizada de conciencia sobre la seguridad operativa y el aseguramiento del control interno de TI. La gerencia y los empleados no tienen conciencia general sobre el control interno.
	1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.
✓	**2 Repetible pero intuitiva** cuando La organización utiliza reportes de control informales para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. La gerencia de servicios de información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.
	3 Proceso definido cuando La gerencia apoya y ha institucionalizado el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI. Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos.
	4 Administrado y medible cuando La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno. Se realizan revisiones entre pares para verificar el monitoreo del control interno.
	5 Optimizado cuando La gerencia ha implantado un programa de mejora continua en toda la organización que toma en cuenta las lecciones aprendidas y las mejores prácticas de la industria para monitorear el control interno. La organización utiliza herramientas integradas y actualizadas, donde es apropiado, que permiten una evaluación efectiva de los controles críticos de TI y una detección rápida de incidentes de control de TI. La compartición del conocimiento, específico de la función de servicios de información, se encuentra implantada de manera formal. El benchmarking con los estándares de la industria y las mejores prácticas está formalizado.

Tabla 2.31: Modelo de Madurez ME2

ME3: GARANTIZAR EL CUMPLIMIENTO REGULATORIO	
CUMPLIMIENTO	**NIVEL DE MADUREZ**
	0 No existente cuando Existe poca conciencia respecto a los requerimientos externos que afectan a TI, sin procesos referentes al cumplimiento de requisitos regulatorios, legales y contractuales.
✓	**1 Inicial/Ad Hoc** cuando Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorías o revisiones.
	2 Repetible pero intuitiva cuando Existe el entendimiento de la necesidad de cumplir con los requerimientos externos y la necesidad se comunica. En los casos en que el cumplimiento se ha convertido en un requerimiento recurrente., como en los reglamentos regulatorios o en la legislación de privacidad, se han desarrollado procedimientos individuales de cumplimiento y se siguen año con año. No existe, sin embargo, un enfoque estándar. Hay mucha confianza en el conocimiento y responsabilidad de los individuos, y los errores son posibles. Se brinda entrenamiento informal respecto a los requerimientos externos y a los temas de cumplimiento.
	3 Proceso definido cuando Se han desarrollado, documentado y comunicado políticas, procedimientos y procesos, .para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizá no se sigan y algunas quizá estén desactualizadas o sean poco prácticas de implantar. Se realiza poco monitoreo y existen requisitos de cumplimiento que no han sido resueltos. Se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y se instruye respecto a los procesos de cumplimiento definidos. Existen contratos pro forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales
	4 Administrado y medible cuando Existe un entendimiento completo de los eventos y de la exposición a requerimientos externos, y la necesidad de asegurar el cumplimiento a todos los niveles. Existe un esquema formal de entrenamiento que asegura que todo el equipo esté consciente de sus obligaciones de cumplimiento. Las responsabilidades son claras y el empoderamiento de los procesos es entendido. El proceso incluye una revisión del entorno para identificar requerimientos externos y cambios recurrentes. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos externos, reforzar las prácticas internas e implantar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas raíz, con el objetivo de identificar soluciones sostenibles. Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos vigentes y contratos recurrentes de servicio.
	5 Optimizado cuando Existe un proceso bien organizado, eficiente e implantado para cumplir con los requerimientos externos, basado en una sola función central que brinda orientación y coordinación a toda la organización. Hay un amplio conocimiento de los requerimientos externos aplicables, incluyendo sus tendencias futuras y cambios anticipados, así como la necesidad de nuevas soluciones. La organización participa en discusiones externas con grupos regulatorios y de la industria para entender e influenciar los requerimientos externos que la puedan afectar. Se han desarrollado mejores prácticas que aseguran el cumplimiento de los requisitos externos, y esto ocasiona que haya muy pocos casos de excepciones de cumplimiento. Existe un sistema central de rastreo para toda la organización, que permite a la gerencia documentar el flujo de trabajo, medir y mejorar la calidad y efectividad del proceso de monitoreo del cumplimiento. Un proceso externo de auto-evaluación de requerimientos existe y se ha refinado hasta alcanzar el nivel de buena práctica. El estilo y la cultura administrativa de la organización referente al cumplimiento es suficientemente fuerte, y se elaboran los procesos suficientemente bien para que el entrenamiento se limite al nuevo personal y siempre que ocurra un cambio significativo.

Tabla 2.32: Modelo de Madurez ME3

JUSTIFICACION NIVELES DE MADUREZ

A continuación se justifica los niveles de madurez escogidos para cada uno de los objetivos de control COBIT seleccionados para la presente Auditoria de Riesgos Informáticos en el Departamento de Gestión Tecnológica del MIES; en base a las entrevistas realizadas con funcionarios del departamento.

Planear y Organizar

PO1 Definir el Plan Estratégico de TI

Nivel de madurez 1: la planeación de TI por parte del Departamento de Gestión Tecnológica se la realiza según se necesite como respuesta a un requisito del negocio específico. En las reuniones de la dirección de TI la planeación estratégica se discute de forma esporádica.

PO2 Definir la Arquitectura de la Información

Nivel de madurez 2: se manejan procedimientos informales que son seguidos por distintos funcionarios dentro del Ministerio. Ellos obtienen sus destrezas al construir la arquitectura de información a través de experiencia práctica y la ejecución frecuentada de técnicas.

PO3 Determinar la dirección tecnológica

Nivel de madurez 2: la planeación es táctica y se orienta a crear soluciones técnicas a problemas técnicos, y no utiliza la tecnología para satisfacer las necesidades del negocio. Las personas obtienen sus destrezas acerca de planeación tecnológica por medio de un aprendizaje práctico y de una ejecución frecuentada de las técnicas.

PO4 Definir procesos, organización y relaciones de TI.

Nivel de madurez 2: el Departamento de Gestión Tecnológica está organizado de manera que pueda satisfacer en forma táctica aunque inconsistente a las necesidades de los funcionarios del MIES y a las relaciones con los proveedores. Existen técnicas habituales para administrar la organización de TI así como las relaciones con los proveedores.

PO5 Administrar la inversión de TI.

Nivel de madurez 3: los procesos de selección de inversiones en TI y de presupuestos están formalizados y documentados. Adicionalmente, se manejan

procedimientos para la aprobación formal de la selección de inversiones en TI y presupuestos.

PO6 Comunicar las aspiraciones y la dirección de la gerencia

Nivel de madurez 3: en el departamento existe un marco general de desarrollo para las políticas y estándares de control, pero el monitoreo del cumplimiento de estas políticas y estándares es inconsistente.

PO7 Administrar recursos humanos de TI.

Nivel de madurez 2: la contratación y administración del personal del Departamento está basado en necesidades específicas de proyectos. El personal nuevo es capacitado a través de entrenamiento informal, para después recibir entrenamiento de acuerdo a las necesidades.

PO9 Evaluar y Administrar Riesgos de TI.

Nivel de madurez 0: la administración de riesgos no se considera algo importante para adquirir soluciones de TI. No existe evaluación de riesgos para los procesos y las decisiones de negocio.

PO10 Administrar proyectos

Nivel de madurez 3: la alta dirección del MIES y del Departamento responsable de TI participa en la administración de los proyectos de TI. Los proyectos de TI son monitoreados para garantizar el cumplimiento de calendarios y presupuestos. El entrenamiento en administración de proyectos es el resultado de iniciativas individuales del equipo.

Adquirir e Implementar

AI1 Identificar Soluciones Automatizadas

Nivel de madurez 4: los proyectos son debidamente documentados y se consideran soluciones alternativas como el análisis de costos y beneficios. La metodología que se utiliza es clara y generalmente entendida.

AI2 Adquirir y mantener el software aplicativo

Nivel de madurez 3: no se aplican procesos de adquisición y mantenimiento en forma consistente por medio de diferentes aplicaciones y proyectos. Las acciones de

mantenimiento que se llevan a cabo en el Departamento son planeadas y programadas.

AI3 Adquirir y mantener la infraestructura tecnológica

Nivel de madurez 1: no se planifican cambios a la infraestructura para cada nueva aplicación, estos son llevados a cabo sin ningún plan. El mantenimiento a la infraestructura tecnológica reacciona a necesidades de corto plazo. No se cuenta con un ambiente de pruebas, ya que el ambiente de producción es el ambiente de pruebas.

AI4 Facilitar la operación y el uso

Nivel de madurez 1: el Departamento considera que la documentación de procesos es necesaria pero esta práctica no es aplicada consistentemente. La documentación se genera esporádicamente y su distribución se la realiza únicamente a determinados grupos.

AI5 Adquirir recursos de TI.

Nivel de madurez 4: las políticas y procedimientos en el Departamento de Gestión Tecnológica se basan en el proceso general de adquisición del MIES. Los proveedores de recursos de TI se integran dentro de los reglamentos de administración de proyectos del MIES desde una perspectiva de administración de contratos.

AI6 Administrar cambios

Nivel de madurez 2: no existe un proceso estructurado de cambios. La mayor parte de los cambios siguen un enfoque de administración de cambios informal, por tanto es muy vulnerable a errores.

AI7 Instalar y Acreditar soluciones y cambios

Nivel de madurez 1: se consideran importantes la verificación y confirmación que las soluciones implantadas cumplen con el objetivo deseado, pero no se realizan pruebas en forma consistente. Se realizan pruebas para determinados proyectos y la acreditación formal y la autorización son poco frecuentes.

Entregar y Dar Soporte

DS2 Administrar servicios de terceros

Nivel de madurez 1: no existen condiciones estandarizadas para los acuerdos con los proveedores de servicios. El monitoreo de los servicios prestados es informal y reactivo.

DS3 Administrar desempeño y capacidad

Nivel de madurez 1: los funcionarios del MIES constantemente tienen que ejecutar soluciones alternas para remediar las limitaciones de desempeño y capacidad. Las acciones que se manejan para la administración del desempeño y la capacidad son generalmente reactivas.

DS4 Garantizar la Continuidad del Servicio

Nivel de madurez 1: la orientación de la gerencia sobre la continuidad del servicio reside en los recursos de infraestructura, mas no en los servicios de TI. Las acciones en respuesta a las interrupciones de TI generalmente son reactivas.

DS5 Garantizar la Seguridad de los Sistemas

Nivel de madurez 3: las responsabilidades de la seguridad de TI están definidas pero no han sido implementadas, adicionalmente se cuenta con un plan de seguridad de TI, así como soluciones de seguridad. Ocasionalmente se realizan capacitaciones en seguridad para TI, pero no son planificadas y son comunicadas informalmente.

DS7 Educar y entrenar a los usuarios

Nivel de madurez 0: no se cuenta con programas de entrenamiento y educación. La dirección del Departamento no lo considera como un aspecto relevante, por tanto no es un problema debidamente atendido.

DS8 Administrar la mesa de servicio y los incidentes

Nivel de madurez 2: existe soporte o ayuda de manera informal a través de los funcionarios del Departamento de Gestión Tecnológica. Estos funcionarios manejan herramientas comunes para brindar ayudar en la solución de incidentes.

DS9 Administrar la configuración

Nivel de madurez 1: en el Departamento no se ha definido prácticas estandarizadas. Se ejecutan tareas básicas de administración de configuraciones.

DS10 Administrar los problemas

Nivel de madurez 2: dentro de la administración de TI existen individuos clave capaces de identificar y resolver problemas. La información en el Departamento es

compartida entre el personal de manera informal y reactiva. Se cuenta con un nivel de servicio limitado.

DS11 Administrar los datos

Nivel de madurez 3: en el Departamento se definen responsabilidades sobre la administración de los datos, adicionalmente se determina la pertenencia sobre los datos a los responsables de controlar la integridad y la seguridad.

DS12 Administrar el ambiente físico

Nivel de madurez 2: no se cuenta con un proceso formal sobre la seguridad física. Las formas de mantenimiento de las instalaciones del Departamento no se encuentran bien documentados, mas bien obedecen a las buenas prácticas de ciertos funcionarios. La dirección no garantiza que se cumplan los objetivos de seguridad.

DS13 Administrar las operaciones

Nivel de madurez 2: los procedimientos de soporte de TI son informales e intuitivos. Las operaciones de soporte dependen de las destrezas de los funcionarios del Departamento de Gestión Tecnológica y no se cuenta con documentación sobre las instrucciones de procedimientos de soporte.

Monitorear y Evaluar

ME1 Monitorear y evaluar el Desempeño de TI.

Nivel de madurez 2: el Departamento ha definido mediciones básicas para ser monitoreadas y los resultados del monitoreo pueden ser únicamente entendidos por ciertos funcionarios clave.

ME2 Monitorear y evaluar el control interno

Nivel de madurez 2: se inician acciones correctivas basadas en los reportes de control informales. Se utiliza herramientas para monitorear controles internos, dichos monitoreos no son planificados.

ME3 Garantizar cumplimiento regulatorio

Nivel de madurez 1: se siguen procesos informales para mantener el cumplimiento, y se ejecutan acciones en forma reactiva si existe la necesidad o como respuesta a auditorías o revisiones.

A continuación en la *Tabla 2.33 s*e muestran los valores correspondientes a los niveles de madurez obtenidos para cada uno de los objetivos de control COBIT evaluados en el Departamento de Gestión Tecnológica:

OBJETIVOS DE CONTROL COBIT		Nivel de Madurez
PLANEAR Y ORGANIZAR		
PO1	Definir el Plan Estratégico de TI	1
PO2	Definir la Arquitectura de la Información	2
PO3	Determinar la dirección tecnológica	2
PO4	Definir procesos, organización y relaciones de TI.	2
PO5	Administrar la inversión de TI.	3
PO6	Comunicar las aspiraciones y la dirección de la gerencia	3
PO7	Administrar recursos humanos de TI.	2
PO9	Evaluar y Administrar Riesgos de TI.	0
PO10	Administrar proyectos	3
ADQUIRIR E IMPLEMENTAR		
AI1	Identificar Soluciones Automatizadas	4
AI2	Adquirir y mantener el software aplicativo	3
AI3	Adquirir y mantener la infraestructura tecnológica	1
AI4	Facilitar la operación y el uso	1
AI5	Adquirir recursos de TI.	4
AI6	Administrar cambios	2
AI7	Instalar y Acreditar soluciones y cambios	1
ENTREGAR Y DAR SOPORTE		
DS2	Administrar servicios de terceros	1
DS3	Administrar desempeño y capacidad	1
DS4	Garantizar la Continuidad del Servicio	1
DS5	Garantizar la Seguridad de los Sistemas	3
DS7	Educar y entrenar a los usuarios	0
DS8	Administrar la mesa de servicio y los incidentes	2
DS9	Administrar la configuración	1
DS10	Administrar los problemas	2
DS11	Administrar los datos	3
DS12	Administrar el ambiente físico	2
DS13	Administrar las operaciones	2
MONITOREAR Y EVALUAR		
ME1	Monitorear y evaluar el Desempeño de TI.	2
ME2	Monitorear y evaluar el control interno	2
ME3	Garantizar cumplimiento regulatorio	1

Tabla: 2.33 Resultados niveles de madurez

ANÁLISIS DE RESULTADOS

Para analizar los resultados se tomará como referencia el cuadro de interpretación conforme lo sugiere COSO[7] (Sponsoring Organizations of the Treadway Commission) referente a Nivel de Riesgo (*Tabla 2.34*). Ver *ANEXO 3.*

Grado de Confianza	Nivel de Riesgo	Calificación %		Promedio %
Bajo B	Alto A	15	50	32
Moderado M	Moderado M	51	75	63
Alto A	Bajo B	76	95	86

Tabla 2.34: Cuadro de interpretación según COSO

A partir de las calificaciones se obtuvo un promedio para cada uno de los grados de confianza así como los niveles de riesgos, mismos que se muestran en la Tabla 2.34. Cabe mencionar que no se muestran el Grado de Confianza y Nivel de Riesgo correspondiente a Vacío dado que posee valores nulos.

Para obtener los valores numéricos correspondientes a los impactos sobre los Criterios de Tecnologías de la Información (TI) de cada uno de los procesos seleccionados para la Auditoría de Riesgos Informáticos realizado en el Departamento de Gestión Tecnológica del MIES, se comienza designando valores numéricos a los grados de impacto establecidos según COBIT (Primario=P, Secundario=S) con los valores especificados en el cuadro de interpretación según COSO, como se muestra en la Tabla 2.35:

Grado de Confianza	Nivel de Riesgo	Promedio %	Grado de impacto
Alto	Bajo	**86**	Primario **P**
Moderado	Moderado	**63**	Secundario **S**

Tabla 2.35: Asignación numérica a los grados de impacto

[7] COSO: Comité de organizaciones patrocinadoras de la Comisión Treadway Estándar aceptado a nivel internacional para el gobierno corporativo.

A continuación se muestran los Objetivos de Control COBIT seleccionados para la realización del presente trabajo de Auditoría con sus respectivos grados de impacto sobre los Criterios de Información de COBIT así como sobre los Recursos de TI, donde los grados de impacto son: P= Primario y S= Secundario. Esta información será utilizada como referencia para el análisis de resultados de la presente Auditoría.

		CRITERIOS DE INFORMACION							**RECURSOS DE TI**			
OBJETIVOS DE CONTROL COBIT		**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Aplicaciones**	**Información**	**Infraestructura**	**Personas**
PLANEAR Y ORGANIZAR												
PO1	Definir el Plan Estratégico de TI	P	S						X	X	X	X
PO2	Definir la Arquitectura de la Información	S	P	S	P				X	X		
PO3	Determinar la dirección tecnológica	P	P						X		X	
PO4	Definir procesos, organización y relaciones de TI.	P	P									X
PO5	Administrar la inversión de TI.	P	P					S	X		X	X
PO6	Comunicar las aspiraciones y la dirección de la gerencia	P					S			X		X
PO7	Administrar recursos humanos de TI.	P	P									X
PO9	Evaluar y Administrar Riesgos de TI.	S	S	P	P	P	S	S	X	X	X	X
PO10	Administrar proyectos	P	P						X		X	X
ADQUIRIR E IMPLEMENTAR												
AI1	Identificar Soluciones Automatizadas	P	S						X		X	
AI2	Adquirir y mantener el software aplicativo	P	P		S			S	X			
AI3	Adquirir y mantener la infraestructura tecnológica	S	P		S	S					X	
AI4	Facilitar la operación y el uso	P	P		S	S	S	S	X		X	X
AI5	Adquirir recursos de TI.	S	P				S		X	X	X	X
AI6	Administrar cambios	P	P		P	P		S	X	X	X	X
AI7	Instalar y Acreditar soluciones y cambios	P	S		S	S			X	X	X	X
ENTREGAR Y DAR SOPORTE												
DS2	Administrar servicios de terceros	P	P	S	S	S	S	S	X	X	X	X
DS3	Administrar desempeño y capacidad	P	P			S			X		X	
DS4	Garantizar la Continuidad del Servicio	P	S			P			X	X	X	X

DS5	Garantizar la Seguridad de los Sistemas			P	P	S	S	S	X	X	X	X
DS7	Educar y entrenar a los usuarios	P	S									X
DS8	Administrar la mesa de servicio y los incidentes	P	P						X			X
DS9	Administrar la configuración	P	S			S		S	X	X	X	
DS10	Administrar los problemas	P	P			S			X	X	X	X
DS11	Administrar los datos				P			P		X		
DS12	Administrar el ambiente físico				P	P					X	
DS13	Administrar las operaciones	P	P		S	S			X	X	X	X
MONITOREAR Y EVALUAR												
ME1	Monitorear y evaluar el Desempeño de TI.	P	P	S	S	S	S	S	X	X	X	X
ME2	Monitorear y evaluar el control interno	P	P	S	S	S	S	S	X	X	X	X
ME3	Garantizar cumplimiento regulatorio						P	S	X	X	X	X

Tabla 2.36: Impacto de los Objetivos de Control sobre los Criterios de Información y Recursos de TI

A continuación se reemplaza los grados de impacto P y S por los valores numéricos asignados a dichos grados de impacto, mostrados en la tabla *Asignación numérica a los grados de impacto (Tabla 2.37).*

		CRITERIOS DE INFORMACION						
OBJETIVOS DE CONTROL COBIT		**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**
PLANEAR Y ORGANIZAR								
PO1	Definir el Plan Estratégico de TI	0,86	0,63					
PO2	Definir la Arquitectura de la Información	0,63	0,86	0,63	0,86			
PO3	Determinar la dirección tecnológica	0,86	0,86					
PO4	Definir procesos, organización y relaciones de TI.	0,86	0,86					
PO5	Administrar la inversión de TI.	0,86	0,86					0,63
PO6	Comunicar las aspiraciones y la dirección de la gerencia	0,86					0,63	
PO7	Administrar recursos humanos de TI.	0,86	0,86					
PO9	Evaluar y Administrar Riesgos de TI.	0,63	0,63	0,86	0,86	0,86	0,63	0,63
PO10	Administrar proyectos	0,86	0,86					

ADQUIRIR E IMPLEMENTAR								
AI1	Identificar Soluciones Automatizadas	0,86	0,63					
AI2	Adquirir y mantener el software aplicativo	0,86	0,86		0,63			0,63
AI3	Adquirir y mantener la infraestructura tecnológica	0,63	0,86		0,63	0,63		
AI4	Facilitar la operación y el uso	0,86	0,86		0,63	0,63	0,63	0,63
AI5	Adquirir recursos de TI.	0,63	0,86				0,63	
AI6	Administrar cambios	0,86	0,86		0,86	0,86		0,63
AI7	Instalar y Acreditar soluciones y cambios	0,86	0,63		0,63	0,63		
ENTREGAR Y DAR SOPORTE								
DS2	Administrar servicios de terceros	0,86	0,86	0,63	0,63	0,63	0,63	0,63
DS3	Administrar desempeño y capacidad	0,86	0,86			0,63		
DS4	Garantizar la Continuidad del Servicio	0,86	0,63			0,86		
DS5	Garantizar la Seguridad de los Sistemas			0,86	0,86	0,63	0,63	0,63
DS7	Educar y entrenar a los usuarios	0,86	0,63					
DS8	Administrar la mesa de servicio y los incidentes	0,86	0,86					
DS9	Administrar la configuración	0,86	0,63			0,63		0,63
DS10	Administrar los problemas	0,86	0,86			0,63		
DS11	Administrar los datos				0,86			0,86
DS12	Administrar el ambiente físico				0,86	0,86		
DS13	Administrar las operaciones	0,86	0,86		0,63	0,63		
MONITOREAR Y EVALUAR								
ME1	Monitorear y evaluar el Desempeño de TI.	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME2	Monitorear y evaluar el control interno	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME3	Garantizar cumplimiento regulatorio						0,86	0,63

Tabla 2.37: Asignación de valores a los impactos sobre los Criterios de Información

Como siguiente paso se procede a realizar una multiplicación entre los niveles de madurez obtenidos para el Departamento de Gestión Tecnológica del MIES, mostrados en la *Tabla 2.33*, y los valores asignados a los impactos sobre los Criterios de Información según COBIT, mostrados en la *Tabla 2.37*.

Para finalmente obtener un resultado total de la situación actual del Departamento, al sumar los valores obtenidos por cada columna correspondiente a cada uno de los Criterio de Información según COBIT considerando todos los Objetivos de Control COBIT evaluados, como se muestra en la *Tabla 2.38*:

Nivel de madurez del objetivo de control x Valor asignado al grado de impacto sobre los criterios de información

OBJETIVOS DE CONTROL COBIT		CRITERIOS DE INFORMACION						
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
PLANEAR Y ORGANIZAR								
PO1	Definir el Plan Estratégico de TI	0,86	0,63	0	0	0	0	0
PO2	Definir la Arquitectura de la Información	1,26	1,72	1,26	1,72	0	0	0
PO3	Determinar la dirección tecnológica	1,72	1,72	0	0	0	0	0
PO4	Definir procesos, organización y relaciones de TI.	1,72	1,72	0	0	0	0	0
PO5	Administrar la inversión de TI.	2,58	2,58	0	0	0	0	1,89
PO6	Comunicar las aspiraciones y la dirección de la gerencia	2,58	0	0	0	0	1,89	0
PO7	Administrar recursos humanos de TI.	1,72	1,72	0	0	0	0	0
PO9	Evaluar y Administrar Riesgos de TI.	0	0	0	0	0	0	0
PO10	Administrar proyectos	2,58	2,58	0	0	0	0	0
ADQUIRIR E IMPLEMENTAR								
AI1	Identificar Soluciones Automatizadas	3,44	2,52	0	0	0	0	0
AI2	Adquirir y mantener el software aplicativo	2,58	2,58	0	1,89	0	0	1,89
AI3	Adquirir y mantener la infraestructura tecnológica	0,86	0,86	0	0,63	0,63	0	0
AI4	Facilitar la operación y el uso	0,86	0,86	0	0,63	0,63	0,63	0,63
AI5	Adquirir recursos de TI.	2,52	3,44	0	0	0	2,52	0
AI6	Administrar cambios	1,72	1,72	0	1,72	1,72	0	1,26
AI7	Instalar y Acreditar soluciones y cambios	0	0	0	0	0	0	0
ENTREGAR Y DAR SOPORTE								
DS2	Administrar servicios de terceros	0,86	0,86	0,63	0,63	0,63	0,63	0,63
DS3	Administrar desempeño y capacidad	0,86	0,86	0	0	0,63	0	0
DS4	Garantizar la Continuidad del Servicio	0,86	0,63	0	0	0,86	0	0
DS5	Garantizar la Seguridad de los Sistemas	0	0	2,58	2,58	1,89	1,89	1,89
DS7	Educar y entrenar a los usuarios	0	0	0	0	0	0	0
DS8	Administrar la mesa de servicio y los incidentes	1,72	1,72	0	0	0	0	0
DS9	Administrar la configuración	0,86	0,63	0	0	0,63	0	0,63

DS10	Administrar los problemas	1,72	1,72	0	0	1,26	0	0
DS11	Administrar los datos	0	0	0	2,58	0	0	2,58
DS12	Administrar el ambiente físico	0	0	0	1,72	1,72	0	0
DS13	Administrar las operaciones	1,72	1,72	0	1,26	1,26	0	0
MONITOREAR Y EVALUAR								
ME1	Monitorear y evaluar el Desempeño de TI.	1,72	1,72	1,26	1,26	1,26	1,26	1,26
ME2	Monitorear y evaluar el control interno	1,72	1,72	1,26	1,26	1,26	1,26	1,26
ME3	Garantizar cumplimiento regulatorio	0	0	0	0	0	0,86	0,63
	TOTAL	**39,04**	**36,23**	**6,99**	**17,88**	**14,38**	**10,94**	**14,55**

Tabla 2.38: Resultados obtenidos del impacto sobre los Criterios de Información

A continuación se realizará una comparación, para ello inicialmente se considerará una situación ideal en la que el nivel de madurez para cada uno de los Objetivos de Control COBIT tome el valor ideal *5*, correspondiente al nivel óptimo, es decir, se multiplicará los valores presentados en la *tabla 2.34*, para los grados de impacto por *5*. Para luego proceder a la suma de los valores obtenidos por cada columna correspondiente a cada uno de los Criterio de Información COBIT y de esta manera conseguir un valor total ideal, como se muestra en la *Tabla 2.39*:

Nivel de madurez óptimo (5) x Valor asignado al grado de impacto sobre los criterios de información

		CRITERIOS DE INFORMACION						
OBJETIVOS DE CONTROL COBIT		**Efectividad**	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiablidad**
PLANEAR Y ORGANIZAR								
PO1	Definir el Plan Estratégico de TI	4,30	3,15	0	0	0	0	0
PO2	Definir la Arquitectura de la Información	3,15	4,30	3,15	4,30	0	0	0
PO3	Determinar la dirección tecnológica	4,30	4,30	0	0	0	0	0
PO4	Definir Procesos, organización y relaciones de TI.	4,30	4,30	0	0	0	0	0
PO5	Administrar la inversión de TI.	4,30	4,30	0	0	0	0	3,15
PO6	Comunicar las aspiraciones y la dirección de la gerencia	4,30	0	0	0	0	3,15	0
PO7	Administrar recursos humanos de TI.	4,30	4,30	0	0	0	0	0
PO9	Evaluar y Administrar Riesgos de TI.	3,15	3,15	4,30	4,30	4,30	3,15	3,15

PO10	Administrar Proyectos	4,30	4,30	0	0	0	0	0
ADQUIRIR E IMPLEMENTAR								
AI1	Identificar soluciones Automatizadas	4,30	3,15	0	0	0	0	0
AI2	Adquirir y mantener el software aplicativo	4,30	4,30	0	3,15	0	0	3,15
AI3	Adquirir y mantener la infraestructura tecnológica	3,15	4,30	0	3,15	3,15	0	0
AI4	Facilitar la operación y el uso	4,30	4,30	0	3,15	3,15	3,15	3,15
AI5	Adquirir recursos de TI.	3,15	4,30	0	0	0	3,15	0
AI6	Administrar cambios	4,30	4,30	0	4,30	4,30	0	3,15
AI7	Instalar y Acreditar soluciones y cambios	4,30	3,15	0	3,15	3,15	0	0
ENTREGAR Y DAR SOPORTE								
DS2	Administrar servicios de terceros	4,30	4,30	3,15	3,15	3,15	3,15	3,15
DS3	Administrar desempeño y capacidad	4,30	4,30	0	0	3,15	0	0
DS4	Garantizar la Continuidad del servicio	4,30	3,15	0	0	4,30	0	0
DS5	Garantizar la seguridad de los sistemas	0	0	4,30	4,30	3,15	3,15	3,15
DS7	Educar y entrenar a los usuarios	4,30	3,15	0	0	0	0	0
DS8	Administrar la mesa de servicio y los incidentes	4,30	4,30	0	0	0	0	0
DS9	Administrar la configuración	4,30	3,15	0	0	3,15	0	3,15
DS10	Administrar los Problemas	4,30	4,30	0	0	3,15	0	0
DS11	Administrar los datos	0	0	0	4,30	0	0	4,30
DS12	Administrar el ambiente físico	0	0	0	4,30	4,30	0	0
DS13	Administrar las operaciones	4,30	4,30	0	3,15	3,15	0	0
MONITOREAR Y EVALUAR								
ME1	Monitorear y evaluar el Desempeño de TI.	4,30	4,30	3,15	3,15	3,15	3,15	3,15
ME2	Monitorear y evaluar el control interno	4,30	4,30	3,15	3,15	3,15	3,15	3,15
ME3	Garantizar cumplimiento regulatorio	0	0	0	0	0	4,30	3,15
	TOTAL IDEAL	***107,20***	***99,45***	***21,20***	***51,00***	***51,85***	***29,50***	***38,95***

Tabla 2.39: Resultado ideal del impacto sobre Criterios de Información

Para realizar la comparación se utilizarán los resultados obtenidos del impacto sobre los Criterios de Información correspondientes a la situación actual del Departamento de Gestión Tecnológica del MIES, mostrados en la *Tabla 2.38*; así como los resultados ideales del impacto sobre los Criterios de Información mostrados en la *Tabla 2.39*, de esta manera se compararan los resultados reales con los resultados ideales, para así obtener un resultado promedio que muestre porcentualmente el impacto sobre los Criterios de Información que se obtuvo en el presente trabajo de Auditoría de Riesgos Informáticos en el Departamento de Gestión Tecnológica del MIES, resultados que se muestran en la *Tabla 2.40*:

CRITERIOS DE INFORMACION

Descripción	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Resultado Obtenido	39,04	36,23	6,99	17,88	14,38	10,94	14,55
Resultado Ideal	107,20	99,45	21,20	51,00	51,85	29,50	38,95
Resultado Promedio	**36,42%**	**36,43%**	**32,97%**	**35,06%**	**27,73%**	**37,08%**	**37,36%**

Tabla 2.40: Resultado promedio del impacto sobre Criterios de Información

CAPITULO 3. ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

3.1 ELABORACIÓN DEL INFORME FINAL DE LA AUDITORÍA

A continuación se presenta un análisis de acuerdo a los resultados obtenidos para cada proceso COBIT seleccionado para la realización de la presente Auditoría de riesgos informáticos para el Departamento de Gestión Tecnológica del MIES, estableciendo observaciones, riesgos y recomendaciones para cada uno, también se presenta un análisis de acuerdo a los criterios de información según COBIT.

3.1.1 ANÁLISIS POR PROCESOS

PLANEAR Y ORGANIZAR

PO1 Definir el Plan Estratégico de TI *(Nivel de madurez 1)*

Observaciones: No se manejan políticas que definan cómo y cuándo realizar la planeación estratégica de TI. La planeación estratégica de TI solamente se la realiza en respuesta a algún requerimiento del negocio, adicionalmente es un tema poco considerado por la dirección.

Las decisiones estratégicas son definidas en cada proyecto, por ello dichas decisiones no son consistentes con una estrategia global del Ministerio, además las consideraciones de riesgo estratégico se definen informalmente en cada proyecto.

Riesgos: El desinterés de la dirección sobre las capacidades tecnológicas actuales limita la gestión de oportunidades que ofrece TI para un rumbo futuro, de hecho este desinterés se expande a los implicados en el área de TI, impidiendo que la orientación de la dirección del negocio esté bien entendida.

La falta de evaluación del desempeño de los planes existentes y de sistemas de información referente a su contribución a los objetivos del negocio no permite conocer las capacidades actuales de TI, así como su proyección a futuro. La carencia de una planeación estratégica de TI correctamente definida no contribuye ni permite la realización de los objetivos estratégicos del Ministerio.

Recomendaciones: Se requiere de la intervención de los ejecutivos y la dirección del Departamento de Gestión Tecnológica del MIES para alinear la planeación estratégica de TI con las necesidades del negocio actuales y futuras.

PO2 Definir la Arquitectura de la Información *(Nivel de madurez 2)*

Observaciones: No existe un nivel de seguridad de datos y controles de protección para los mismos. Adicionalmente no se cuenta con un diccionario de datos que permita estandarizar la sintaxis manejada entre las diferentes aplicaciones utilizadas en el MIES. Existen procedimientos intuitivos por parte de ciertos funcionarios que han ganado habilidades al construir una arquitectura de información por medio de la práctica y la aplicación repetitiva de las técnicas utilizadas.

Riesgos: Al no existir un nivel de seguridad de datos y controles de protección establecidos para los mismos, se podría provocar la pérdida de información vital para el negocio. La falta de estándares en cuanto a la sintaxis en las aplicaciones podría provocar la duplicidad de información. Al ser intuitivos los procedimientos utilizados en el desarrollo de la arquitectura de la información, no se garantiza la integridad de la información del ministerio.

Recomendaciones: Establecer esquemas de clasificación de datos aplicables a todo el Ministerio, que permita especificar que tan crítica y sensible es la información, así como establecer los controles de acceso a la información vital del ministerio, definir un diccionario y reglas de sintaxis de datos, para evitar la creación de elementos de datos incompatibles. Implantar procedimientos para garantizar la integridad de los datos en todo el ministerio.

PO3 Determinar la dirección tecnológica *(Nivel de madurez 2)*

Observaciones: El Departamento cuenta con un plan de infraestructura tecnológica, que considera la dirección tecnológica incluyendo acuerdos de contingencias en caso de presentarse algún problema en el desarrollo de las actividades primordiales del Ministerio. Adicionalmente se contempla el desarrollo vertiginoso de nuevas tecnologías que podrían mejorar sustancialmente el manejo del negocio.

La evaluación de los cambios tecnológicos es responsabilidad de personas que siguen procesos intuitivos estas personas obtienen sus habilidades por medio de un aprendizaje práctico y por la repetición de técnicas.

Riesgos: Dado que la planeación en el departamento es táctica no se utiliza adecuadamente los recursos tecnológicos, además no se garantiza la generación de soluciones tecnológicas efectivas, consistentes y seguras para todo el Ministerio.

No se garantiza que las directrices proporcionadas por los responsables de las evaluaciones de los cambios tecnológicos sean efectivas, dada su falta de capacitación.

Debido a que el proceso de mejora del plan de infraestructura tecnológica no es continuo no garantiza la actualización de tecnología de punta existente en el mercado, pudiendo quedar rezagados dentro del ambiente tecnológico.

Recomendaciones: Establecer un consejo de arquitectura, que dirija el diseño de la arquitectura de TI y verifique el cumplimiento regulatorio y requerimientos de continuidad. Establecer un proceso para monitorear continuamente las nuevas tendencias en el ambiente competitivo referente a infraestructuras tecnológicas así como regulatorias. Adicionalmente proporcionar soluciones consistentes, efectivas y seguras para el Ministerio.

PO4 Definir procesos, organización y relaciones de TI *(Nivel de madurez 2)*

Observaciones: Los roles y responsabilidades del personal están definidas de acuerdo a las necesidades del negocio, clientes y relaciones con los proveedores, cabe destacar que la toma de decisiones es una tarea exclusivamente asignada al director del departamento, el mismo que se encarga de supervisar que se ejerzan los roles y responsabilidades asignados. Existe personal clave de TI, con el que se mantiene una dependencia excesiva, no existe un plan para contactar al personal clave en caso de presentarse una emergencia. La dirección no asegura que el personal realice solamente las actividades autorizadas relevantes a su función.

Riesgos: Debido a que no existe una revisión continua de la estructura organizacional de TI, se desconoce los requerimientos de personal y no se definen estrategias internas para cumplir con los objetivos del Ministerio.

Al existir una dependencia máxima con ciertos funcionarios claves de TI y no contar con un plan para contactarlos en caso de emergencia, se pone en riesgo la continuidad del negocio al no superar en un tiempo prudencial una situación adversa.
Recomendaciones: Debe existir una revisión continua de la estructura organizacional de TI, que permita conocer los requerimientos del personal que permitan definir estrategias internas para cumplir con los objetivos del Ministerio.
Implantar prácticas apropiadas de supervisión de las funciones de TI, para garantizar que el personal ejecute solo las tareas autorizadas en función de su cargo.
Mantener un plan de registro de contactos de los funcionarios clave de TI, en caso de presentarse alguna emergencia que implique la suspensión temporal del negocio.

PO5 Administrar la inversión de TI. *(Nivel de madurez 3)*
Observaciones: La asignación de responsabilidades de selección de inversiones de TI y de desarrollo de propuestas se hace de una manera inicial, mediante documentación formal a través de las cuales se toman decisiones presupuestarias de un modo operativo.
Se maneja un proceso de toma de decisiones que permite priorizar la asignación de recursos a las Tecnologías de la Información para proyectos y mantenimiento de TI.
Aunque el personal de TI cuenta con experiencia y habilidades requeridas para el desarrollo del presupuesto de TI, incluso para recomendar inversiones de TI, estas capacidades muchas veces fueron adquiridas por iniciativas individuales mas no por entrenamientos formales.
Riesgos: La falta de entrenamientos formales maximiza la probabilidad de ocurrencia de errores en el desarrollo del presupuesto de TI, mismos que afectarían la gestión de la inversión de TI.
A causa de no contar con políticas de administración de beneficios y criterios formales de inversión, se desconoce si la contribución obtenida a través de los proyectos de TI a los resultados del negocio es la contribución esperada.
Recomendaciones: Manejar criterios formales de de inversión como: ROI Retorno de Inversión, Periodo de Reintegro, NPV Valor Presente Neto; adicionalmente medir y evaluar el valor del negocio en comparación con el pronóstico del mismo.

PO6 Comunicar las aspiraciones y la dirección de la gerencia *(Nivel de madurez 3)*

Observaciones: La dirección acepta la responsabilidad de difundir las políticas de control interno, pero no se asignan responsables y tampoco recursos para mantener un ambiente completo de administración de calidad y control de la información. Las políticas, procedimientos y estándares de control son considerablemente sólidos y cubren temas de gran importancia para el Departamento. Existe un inconsistente monitoreo de cumplimiento sobre las políticas y estándares de control.

Riesgos: Al no existir un monitoreo de cumplimiento en el ambiente de control de la información no se realizarán actualizaciones y mejoras sobre políticas, procedimientos y estándares de control, por tanto no se cuenta con un ambiente de políticas y de control adecuado.

Recomendaciones: La dirección debe tomar mayor conciencia sobre la administración de políticas de TI, debe implantar políticas de TI y difundirlas a todo el Ministerio en un programa de comunicación continua, adicionalmente se debería establecer un ambiente de control positivo y proactivo.

PO7 Administrar recursos humanos de TI *(Nivel de madurez 2)*

Observaciones: No se maneja un enfoque estratégico para la contratación y administración del personal de TI. El entrenamiento que recibe el nuevo personal es informal y la capacitación surge de acuerdo a necesidades.

Se realizan evaluaciones periódicas de desempeño de los funcionarios, pero no se otorga adiestramiento a los empleados sobre su conducta y desempeño de acuerdo a los resultados obtenidos.

Existe cierta dependencia sobre empleados clave dentro del Departamento de Gestión Tecnológica, el conocimiento es parcialmente conocido entre los funcionarios de TI.

Riesgos: La carencia de un adecuado plan de administración de recursos humanos de TI evita la adquisición, mantenimiento y motivación de la fuerza de trabajo para la creación y entrega de servicios de TI.

El Departamento es vulnerable a incumplimientos de funciones por parte del nuevo personal a causa de la falta de entrenamiento y orientación formal, así como la inexperiencia o falta de habilidades para el cargo.

La dependencia crítica sobre individuos clave pone en riesgo la continuidad del negocio en caso de ausencia.

Recomendaciones: Establecer un plan de administración de recursos humanos de TI que se actualice constantemente para satisfacer los requerimientos cambiantes del negocio. Manejar programas de entrenamiento continuo para proveer y mantener conocimientos, aptitudes, habilidades y conciencia sobre la seguridad con el fin de satisfacer los requerimientos del Ministerio.

Minimizar las dependencias con elementos claves del Departamento y concienciar al personal sobre compartición de conocimientos y planeación de la sucesión.

Se requiere trabajar con los resultados de evaluación del desempeño de los empleados, para impartir adiestramiento sobre su desempeño y conducta.

PO9 Evaluar y Administrar Riesgos de TI *(Nivel de madurez 0)*

Observaciones: El Departamento de Gestión Tecnológica del MIES no considera importante la gestión de riesgos de TI, por tanto no existe una evaluación de riesgos para los procesos y las decisiones que se manejan en el departamento y tampoco existen estrategias de mitigación de riesgos.

No se ha definido políticas para la comunicación de planes de acción para mitigar riesgos.

Riesgos: Maximizar la posibilidad y el impacto de los riesgos de TI. El departamento es susceptible a todo tipo de amenazas, dado que no se han identificado todos los eventos que podrían tener un impacto potencial sobre las operaciones del departamento. Presentar una respuesta con lentitud e ineficiencia a las amenazas poniendo en riesgo la continuidad del negocio.

Recomendaciones: Tomar consciencia sobre la administración de riesgos, como parte fundamental de las operaciones del departamento. Definir políticas de evaluación y administración de riesgos. Identificar los posibles eventos y sus respectivos impactos que puedan afectar el buen funcionamiento del departamento.

Evaluar frecuentemente la posibilidad de ocurrencia de los riesgos identificados basados en métodos cualitativos y cuantitativos. Manejar políticas de mantenimiento y monitoreo de un plan de acción para mitigar los riesgos que incluya respuesta a los riegos, identificación de costos, beneficios y responsabilidades de la ejecución.

PO10 Administrar proyectos *(Nivel de madurez 3)*

Observaciones: El Departamento maneja procesos de administración de proyectos de TI establecidos dentro del departamento. Se realiza un monitoreo constante de calendario, desempeño y presupuesto sobre los proyectos de TI, el entrenamiento sobre administración de proyectos no se planifica y es el resultado de la iniciativa del personal responsable del proyecto. No se manejan planes de calidad y control de cambios para los proyectos de TI. Al finalizar los proyectos, los interesados no se aseguran que el proyecto haya generado los resultados y beneficios esperados.

Riesgos: Dado que en el Departamento el entrenamiento sobre administración de proyectos se obtiene individualmente, no se garantiza que el proyecto se lleve a cabo en las mejores condiciones o que se cumpla con el calendario, desempeño y presupuesto establecidos inicialmente.

En caso de requerirse cambios en el desarrollo del proyecto, estos pueden no acoplarse a la línea base del proyecto ya que no existe un sistema de control de cambios para cada proyecto. No se garantiza que los proyectos reporten los resultados esperados.

Recomendaciones: Definir e implantar marcos de trabajo para la administración de proyectos de TI en el que se defina alcance, limites de administración de proyectos así como las metodologías a utilizarse para el desarrollo de los proyectos.

Establecer políticas de administración de riesgos de proyectos, para mitigar los riesgos asociados con los proyectos. Establecer planes de calidad del proyecto al igual que sistemas de control de cambios que se adapten al marco de trabajo para la administración de proyectos establecidos.

Definir como política la revisión del proyecto en la etapa de cierre, para conocer los resultados y beneficios obtenidos con el proyecto desarrollado.

ADQUIRIR E IMPLEMENTAR

AI1 Identificar soluciones automatizadas *(Nivel de madurez 4)*

Observaciones: En el Departamento se han establecido metodologías que identifican y evalúan soluciones de TI, mismas que son utilizadas en todos los proyectos, cada proyecto cuenta con una documentación de calidad, realizada en un formato preestablecido, en donde se establecen las necesidades reales para el óptimo desarrollo del mismo.

No existen políticas de análisis de riesgos asociados con el desarrollo de proyectos de TI. Existen estudios de factibilidad técnica y económica para el desarrollo de proyectos TI en base a las necesidades del negocio. Los requerimientos institucionales consideran las necesidades técnicas, seguridades, disponibilidad, continuidad, compatibilidad y funcionalidad del Ministerio. La decisión final referente a la elección y adquisición de la solución, recae únicamente en la autorización de la Subsecretaria Administrativa Financiera.

Riesgos: Dado que la metodología de identificación y evaluación de soluciones de TI se encuentra establecida y no está sujeta a una mejora continua, no se optimiza el desarrollo de los proyectos de TI.

Al no identificar, documentar y analizar los riesgos asociados con el desarrollo de proyectos se maximiza la vulnerabilidad del departamento ante amenazas a la integridad, seguridad y disponibilidad de los datos que maneja el Departamento de Gestión Tecnológica.

Dado que la autorización del desarrollo de los Proyectos de TI es responsabilidad de una sola persona ajena a la unidad no se garantiza el desarrollo de importantes proyectos departamento.

Recomendaciones: Mantener una metodología de identificación y evaluación de soluciones de TI, así como un proceso de mejora continua, para la optimización de proyectos de tecnología. Manejar reportes de análisis de riesgos asociados con los procesos del negocio para el desarrollo de los requerimientos del mismo.

La decisión final para la aprobación y autorización del desarrollo de un proyecto de TI debe ser dada por la autoridad competente en base a las necesidades técnicas del Ministerio.

AI2 Adquirir y mantener software aplicativo *(Nivel de madurez 3)*

Observaciones: Existe una metodología informal que incluyen procesos de especificación, diseño de software y un criterio de adquisición. El Departamento de Gestión Tecnológica cuenta con prácticas y procedimientos de implementación

Riesgos: Al no contar con un proceso establecido de pruebas existe el riesgo de tener diferentes problemas en la puesta en producción de una determinada plataforma. No aplicar procesos necesarios para el correcto desarrollo de proyectos debido a la utilización de mecanismos de aprobación preestablecidas de documentación.

Recomendaciones: Se debe contar con un proceso establecido de pruebas que ayude al correcto desarrollo del software, adicionalmente permitirá realizar pruebas correspondientes al funcionamiento del software con el objetivo de depurar oportunamente los errores que se podrían presentar antes de la puesta en producción.

AI3 Adquirir y mantener infraestructura de tecnológica *(Nivel de madurez 1)*

Observaciones: No se maneja un plan para adquirir, implantar y mantener infraestructura tecnológica, tampoco se consideran futuras extensiones para la realización de cambios en la infraestructura de TI. Se cuenta con medidas de seguridad durante para la configuración y mantenimiento de hardware y software de la infraestructura de TI, con el objeto de proteger la integridad y disponibilidad de los recursos. Se monitorea periódicamente la administración de parches, actualizaciones y requerimientos de seguridad pero no se llevan a cabo evaluaciones sostenidas de vulnerabilidades.

No se ha establecido ambientes de pruebas para soportar la efectividad y eficiencia previa la adquisición y desarrollo de nuevas aplicaciones e infraestructura tecnológica.

Riesgos: Dado que la actividad de mantenimiento de infraestructura de TI no se basa en un plan, y actúa solamente en forma reactiva satisfaciendo las necesidades a corto plazo, no se consideran planes estratégicos que permitan controlar con anticipación problemas que afectarían el óptimo desempeño de la infraestructura de TI. Al no realizar un monitoreo constante de riesgos y evaluación de vulnerabilidades se atenta contra la integridad, disponibilidad de los recursos de infraestructura tecnológica del Ministerio.

El ambiente de producción es el ambiente de pruebas, esto no garantiza la funcionalidad, efectividad y eficiencia durante la implementación de cambios en la infraestructura tecnológica.

Recomendaciones: Establecer un plan de adquisición de tecnología que satisfaga los requerimientos funcionales y técnicos del departamento. Definir un plan de mantenimiento que controle los cambios que se realizan en la infraestructura tecnológica en el departamento.

Mantener un ambiente de prueba fuera del ambiente de producción en el que previamente se pruebe la factibilidad e integración de aplicaciones e infraestructura.

AI4 Facilitar la operación y el uso *(Nivel de madurez 1)*

Observaciones:

El departamento no maneja políticas para la transferencia de conocimiento a los usuarios finales, o planes de entrenamiento que incluyan capacitación inicial y continua, se manejan manuales de usuario, asistencia a usuarios en forma parcial y son únicamente distribuidos a grupos limitados.

La transferencia de conocimientos al personal de soporte técnico generalmente se la realiza únicamente a través de un entrenamiento inicial.

Riesgos: La falta de capacitación y entrenamiento a usuarios finales e incluso a la dirección del departamento no garantiza la utilización en forma efectiva y eficiente de la infraestructura o aplicaciones que se manejan en el Ministerio.

La forma en la que actualmente se capacita al personal de soporte técnico no garantiza la entrega de un apoyo técnico efectivo y eficiente donde sea requerido.

Recomendaciones: Desarrollar un plan para soluciones de operación en el que se identifiquen y documenten aspectos técnicos y capacidad de información en forma clara y entendible acerca de aplicaciones e infraestructura que maneja el Ministerio, garantizar la disponibilidad de esta documentación para la transferencia de conocimiento dentro del departamento.

Entrenar a usuarios finales, a la dirección del departamento técnico y al personal de soporte técnico a través de entrenamiento inicial y continuo, material de entrenamiento, manual de operación y manuales de usuarios acerca de aplicaciones e infraestructura que maneja el Ministerio.

AI5 Adquirir recursos de TI *(Nivel de madurez 4)*

Observaciones: Se manejan procesos de selección de proveedores en forma justa y formal para la elección del mejor, basados en los requerimientos técnicos, calidad y costos establecidos.

Para la adquisición de recursos de TI se consideran procesos de adquisición de software, licenciamiento, propiedad intelectual y aspectos de conveniencia que incluye seguridad, custodia y derechos de acceso.

Derechos y obligaciones son incluidos y respetados tanto por el oferente como por el contratante de acuerdo a los términos establecidos en los contratos de adquisición.

Se utiliza la documentación estándar para la adquisición de recursos de TI en todos los procesos de compras públicas o privadas.

Riesgos: Los procesos de adquisiciones estandarizados, pueden ocasionar algún impedimento para la correcta adquisición del software solicitado, ya que no se los actualiza frecuentemente.

Al no estandarizar políticas claras de adquisición para software de desarrollo se puede incurrir en la adquisición de varias plataformas de TI, ocasionando problemas de integración de información necesaria para el Ministerio.

Recomendaciones: La integración de diferentes plataformas debe ser llevada a cabo de forma coordinada, analizando la escalabilidad entre el software existente y la plataforma adquirida, de esta manera se mejorará el manejo global de la información

ministerial. Se deben mantener actualizadas las políticas de licenciamiento de software ministerial.

AI6 Administrar cambios *(Nivel de madurez 2)*

Observaciones: No se manejan procedimientos de administración de cambios para gestionar estandarizadamente cambios de aplicaciones, procedimientos o servicios. No se ha establecido ningún sistema de seguimiento y reporte para comunicar a los interesados sobre el estado en los que se encuentran los cambios que se han solicitado.

Cuando se implantan cambios en los sistemas, la actualización en la documentación de usuario y procedimientos correspondientes se lo realiza solamente en forma parcial, adicionalmente no se cuenta con procesos de seguimiento que aseguren que la implantación de determinado cambio fue ejecutado completamente.

Riesgos: No considerar muchas solicitudes importantes de cambio en diferentes aspectos del departamento por la falta de procedimientos formales en la gestión de cambios no permite el mejoramiento continuo del departamento. Dada la falta de seguimiento de los cambios realizados en el departamento se desconoce si estos se realizaron completamente y si se obtuvieron los resultados esperados.

La desactualización en la documentación de usuario y procedimientos después de ejecutarse un cambio provoca que las personas relacionadas en el cambio no se desempeñen en forma efectiva y eficiente con aplicaciones, procedimientos o servicios que hayan sufrido cambios, dando paso a interrupciones en el ambiente de producción.

Recomendaciones: Establecer estándares y procedimientos formales de administración de cambios para las diferentes solicitudes de cambios que se soliciten dentro del departamento, evaluar el impacto que los cambios pueden producir en el sistema operacional y funcional en el Departamento de Gestión Tecnológica del MIES.

Establecer un sistema de seguimiento y reporte del estado de cambios, que comunique a los solicitantes e interesados en que situación se encuentra su solicitud

de cambio. Después de implantar cambios al sistema es recomendable actualizar la documentación de usuario y procedimientos correspondientes.

AI7 Instalar y acreditar soluciones y cambios *(Nivel de madurez 1)*

Observaciones: No existen procesos formales para la instalación y monitoreo de soluciones de TI implantadas en el departamento, la dirección del departamento reconoce la necesidad de evaluar y reportar que las soluciones se ajustan al propósito deseado.

No se cuenta con un plan de pruebas, no se ha definido responsables, responsabilidades, preparación de pruebas y tampoco un ambiente de pruebas. El MIES no maneja un ambiente de pruebas, solamente el ambiente de producción.

La liberación del software no esta regulada con procedimientos formales, esta práctica se lleva a cabo con procedimientos de respaldo y notificación al usuario y a la dirección.

Las revisiones posteriores a la implantación del sistema de información son ejecutadas en forma reactiva en caso de presentarse algún inconveniente con dicho sistema.

Se desconoce el nivel de satisfacción de usuarios con los sistemas implantados

Riesgos: En el Departamento de Gestión Tecnológica no garantiza que la calidad de los nuevos sistemas de información implantados en el Ministerio sea satisfactoria, debido a la falta de procedimientos formales de instalación y ambientes de prueba definidos.

Ineficacia e ineficiencia en el desempeño de labores de los usuarios, producto de la insatisfacción con el nuevo sistema implantado, ya que se desconoce si el cambio satisfizo los requerimientos de los usuarios y si este entregó los beneficios visualizados.

Recomendaciones: Entrenar al personal de los departamentos de usuario afectados por los cambios o las nuevas soluciones, se debe establecer una metodología de prueba y realizar la planeación de la liberación antes de llevar a producción las nuevas soluciones o cambios.

ENTREGAR Y DAR SOPORTE

DS2 Administrar servicios de terceros *(Nivel de madurez 1)*

Observaciones: Se identifica y clasifica los proveedores de acuerdo al tipo de servicios que presta, pero dicha información no se encuentra formalmente documentada. Se manejan acuerdos de niveles de servicio para asegurar la calidad del servicio y la respuesta oportuna por parte de los proveedores.

No se han establecido procesos de monitoreo generales de un proveedor, únicamente se monitorean los acuerdos y convenios de niveles de servicio establecidos en el contrato. No se identifica riesgos relacionados con los proveedores, que garanticen la efectiva entrega de servicios así como la continuidad del negocio.

Riesgos: No se controla en forma adecuada roles, responsabilidades, metas, entregables esperados por parte de los proveedores, dada la inexistencia de documentación formal de relaciones técnicas y organizacionales. No se garantiza que el servicio prestado por los proveedores sea de calidad, pudiendo afectar así el óptimo desempeño de los servicios que se presta el Departamento de Gestión Tecnológica del MIES.

La prestación de servicios por parte del proveedor no cumpla a satisfacción con los requerimientos acordados en el contrato.

Recomendaciones: La Dirección debe tomar conciencia acerca de la importancia de establecer políticas documentadas para la administración de servicios de terceros. Identificar y mitigar riesgos de los proveedores para asegurar la entrega de servicios en forma efectiva y eficiente. Monitorear y medir el desempeño de prestación de servicios por parte de los proveedores basados en los acuerdos establecidos en los contratos, para garantizar el cumplimiento óptimo de los niveles de servicios definidos.

DS3 Administrar desempeño y capacidad *(Nivel de madurez 1)*

Observaciones: El Departamento no cuenta con procesos de planeación de observación del desempeño y capacidad de los recursos de TI, por tanto no se

cuenta con pronósticos de desempeño y capacidad de recursos de TI que puedan ser incluidos en planes de desempeño y capacidad futuros.

La capacidad y desempeño entregados no considera cargas de trabajo, requerimientos de almacenamiento o contingencias de los recursos de TI ya que no se identifican excesos de capacidad y tampoco tendencias de cargas de trabajo.

El monitoreo del desempeño y capacidad realizado en el departamento es parcial ya que únicamente se monitorean los procesos de alto impacto que pueden afectar el desarrollo de actividades prioritarias del MIES.

Riesgos: Las limitaciones de desempeño y capacidad no sean resueltas oportunamente por parte de los usuarios. Dado que la planeación del desempeño y la capacidad es informal, no se optimizan los recursos de TI de acuerdo a las necesidades del negocio.

La falta de un monitoreo constante del desempeño y capacidad de los recursos de TI maximiza el riesgo de interrupciones ya que se desconoce si existe exceso de capacidad o altas cargas de trabajo que necesiten redistribuirse.

Recomendaciones: Establecer procedimientos de planeación para la revisión del desempeño de los recursos de TI, que permitan ejecutar acciones de administración del desempeño y la capacidad en forma proactiva.

Monitorear periódicamente la capacidad y el desempeño de almacenamiento, procesamiento, mantenimiento de los recursos de TI, para determinar si existe la capacidad y desempeño necesario para la óptima prestación de servicios.

DS4 Garantizar la Continuidad del Servicio *(Nivel de madurez 1)*

Observaciones: La información está organizada de forma que solo las personas autorizadas tengan acceso a la misma, sin embargo esto solo se lo maneja de forma departamental y no se tiene una política global en cuanto a la seguridad de la información. Se busca garantizar la continuidad del servicio mediante el cumplimiento de los parámetros de confidencialidad, integridad y disponibilidad.

Las políticas de seguridad están enfocadas a los aspectos físicos que pueden poner en riesgo el trabajo del Ministerio. El Departamento considera el control de acceso, la protección contra incendios y posibles eventualidades en el sistema de fluido

eléctrico. El licenciamiento de software se maneja de correctamente al tener las licencias de todos los programas que se utilizan en la institución.

Riesgos: Al no existir una política global en la seguridad de la información, hay la posibilidad que personas externar puedan aprovechar probables brechas en la seguridad, poniendo en riesgo la información, los activos fijos y por ende el funcionamiento del ministerio.

Recomendaciones: Elaborar planes de contingencia que garanticen la continuidad del servicio ante una posible interrupción de los servicios de TI. Realizar pruebas de los planes de contingencia y entrenar al personal. Además se debe tener un respaldo de los planes y la información en otro lugar que no sea el edificio en el cual tiene sede el ministerio. Realizar una revisión sobre la política de seguridad de la información para eliminar las posibles falencias existentes.

DS5 Garantizar la Seguridad de los Sistemas *(Nivel de madurez 3)*

Observaciones: La seguridad física de los sistemas está garantizada mediante los diferentes previsiones que se han tomado en lo referente al control de acceso, asignación de roles, prevención contra desastres naturales, pero no existen planes de contingencia definidos. Además no existen controles en el uso de medios extraíbles, con lo cual la información puede ser sustraída o infectada.

No es permitido que personas ajenas tengan acceso a los sistemas del ministerio o a la información. Únicamente la información que sea de acceso público está disponible para cualquier persona a través de la página Web.

No existen procedimientos para la gestión de cambios en los sistemas, no se considera la identificación y registro de cambios significativos, planeación y prueba de cambios así como tampoco la evaluación de los impactos potenciales incluyendo los impactos de seguridad.

Riesgos: Se debe implementar un control más efectivo de los cambios que se llevan a cabo, puesto que los mismos generan momentos de vulnerabilidad que pueden provocar ataques o pérdidas de tiempo de trabajo.

Recomendaciones: Realizar un seguimiento más efectivo de los cambios para minimizar los riesgos asociados a los mismos. Se debe tener controles más regulares de los sistemas de seguridad para asegurar su correcto funcionamiento.

DS7 Educar y entrenar a los usuarios *(Nivel de madurez 0)*

Observaciones: Cada usuario es responsable de salvaguardar su información y evitar que personas no autorizadas tengan acceso a los sistemas e información a través de usuarios que cuentan con permisos. Además no existe un reglamento para la capacitación del nuevo personal, por lo cual los funcionarios adquieren experiencia mediante el transcurso de sus labores cotidianas.

Riesgos: La falta de capacitación al nuevo personal puede generar problemas en la seguridad de los sistemas e información, pues por desconocimiento ellos eventualmente permiten el acceso a personas no autorizadas, provocan fallas de funcionamiento, y en general ponen en riesgo la información del ministerio.

Recomendaciones: Crear planes para el entrenamiento del nuevo personal para permitir que puedan desenvolverse de forma más eficiente lo más pronto posible, logrando así una mejor adaptación a sus actividades laborales.

DS8 Administrar la mesa de servicio y los incidentes *(Nivel de madurez 2)*

Observaciones: No se maneja una política de reporte de debilidades definida, pero cuando se presentan un caso de emergencia se soluciona y se documenta dicho caso especificando lo sucedido y se lo presenta al Director del Departamento de Gestión Tecnológica.

Cuando los eventos son leves se los documenta en hojas de registros de eventualidades que son controladas periódicamente por el personal del departamento.

Basados en las hojas de registros de eventualidades se controla los incidentes que se han producido en el Ministerio, de esta manera se observan los eventos mas comunes y se procura dar una solución para que disminuyan o desaparezcan en su totalidad.

Riesgos: La falta de una política con respecto al reporte de las debilidades provoca pérdida de tiempo de trabajo cuando se presentan incidentes asociados a las mismas.

Recomendaciones: Es adecuado tener una base de conocimiento sobre las soluciones que se dan a los incidentes que se presentan en el día a día, con lo cual se minimiza su impacto cuando estos se presentan.

DS9 Administrar la configuración *(Nivel de madurez 1)*

Observaciones: Se tiene un registro completo de los activos informáticos de la institución, con lo cual está definida la configuración adecuada para cada uno de los mismos de acuerdo al uso que se le va a dar.

El acceso a los archivos de configuración y del sistema solo está permitido para el personal calificado que trabaja en el Departamento de Gestión Tecnológica. Además se siguen los lineamientos proveídos por las casas desarrolladoras y fabricantes de las diferentes plataformas para intentar garantizar su correcto funcionamiento.

No se tiene un repositorio de las configuraciones de los equipos. La configuración de los mismos se la realiza desde cero cada vez que se lo requiera, lo cual provoca pérdida de tiempo.

Riesgos: Al no existir un repositorio completo y preciso de las diferentes configuraciones se genera lentitud en el proceso de configuración e los equipos y servicios. El hecho de no utilizar un estándar generalizado para el control del inventario de los equipos, puede generar inconsistencias en la información que se maneja en este aspecto.

Recomendaciones: Se deben definir prácticas estandarizadas para el control e inventario de los equipos. Crear un repositorio centralizado de las configuraciones, identificando a qué equipo está asociada la misma; Además se deben realizar revisiones periódicas de estas configuraciones para monitorear su integridad y funcionamiento. A su vez, reforzar los controles en el acceso a los privilegios del usuario avanzado para llegar a un 100% de protección de los archivos del sistema.

DS10 Administrar los problemas *(Nivel de madurez 2)*

Observaciones: Existen controles para manejar incidentes leves y se los documenta para tener conocimiento de las consecuencias que provocan.

Para evita pérdidas de información se realizan backups de la información más sensible sin la cual el ministerio no podría funcionar de forma eficiente. Esto genera un mínimo tiempo de interrupción de los servicios cuando por alguna razón estos se ven afectados.

Riesgos: La falta de de un control más estricto de los incidentes y los problemas pueden provocar que no se minimice su impacto.

Recomendaciones: Adoptar los lineamientos de las mejores prácticas y estándares aceptados a nivel mundial para mejorar el manejo de los incidentes, buscando eliminar los daños que estos puedan provocar.

DS11 Administrar los datos *(Nivel de madurez 3)*

Observaciones: Los datos se manejan de acuerdo al departamento que los genera o utiliza. Sólo las personas autorizadas tienen acceso a los mismos; sin embargo no se maneja otro tipo clasificación de los datos.

Se realizan respaldos de la información que generan las aplicaciones y de los datos utilizados por las diferentes plataformas de los servidores. Esto con la intención de poner nuevamente en funcionamiento los mismos en caso de una interrupción no planificada por los administradores de los diferentes sistemas.

Existe falta de una política definida para el traslado de la información y el manejo de los medios extraíbles.

Riesgos: Ante la falta de control en el traslado de la información se presenta la posibilidad de pérdida de integridad y confidencialidad de la misma. La libre utilización de medios extraíbles trae el riesgo de contagiar con virus o códigos maliciosos a los sistemas del ministerio.

Recomendaciones: Crear políticas claras para el traslado de la información, manteniendo su confidencialidad e integridad. Informar y entrenar a los usuarios sobre estas reglas para que se las cumpla e implementar una verdadera cultura de seguridad.

Se deberían desactivar los puertos de los medios extraíbles para que no se puedan realizar copias o extracciones no autorizadas de datos. Únicamente los usuarios avanzados podrían activar dichos puertos, previa verificación que solo usuarios autorizados tengan acceso a la información.

DS12 Administrar el ambiente físico *(Nivel de madurez 2)*

Observaciones: El ambiente físico se ha manejado de forma aceptable mediante la implementación de sistemas de seguridad, protección y acceso a las distintas dependencias; pero ninguna de estas prácticas se encuentra debidamente documentada. No se maneja un proceso formal para la administración del ambiente físico. Los mantenimientos están basados en las buenas prácticas de algunos usuarios en este ámbito y la dirección de TI no vigila que se cumplan con los lineamientos de seguridad existentes.

Riesgos: La continuidad del negocio se ve amenazada por la falta de procedimientos documentados y estandarizados; así como también por la falta de planes de contingencia que entren en acción ante situaciones de emergencia.

Recomendaciones: Se debe alinear las medidas de seguridad física con los requerimientos del negocio. Establecer procedimientos para el manejo de los privilegios del acceso, tanto a las oficinas como a la información; esto de acuerdo a las necesidades de la organización, siempre tomando en cuenta las posibles emergencias que se puedan presentar.

Documentar los procedimientos de seguridad, creando planes de contingencia que ayuden a garantizar la continuidad el negocio.

DS13 Administrar las operaciones *(Nivel de madurez 2)*

Observaciones: Los procesos de operación no se hallan documentados, con lo que se genera desinformación cuando existen fallas de operación. Las eventualidades de carácter físico están cubiertas con las precauciones que se han tomado. La clasificación de la información por departamentos facilita el trabajo dentro de los mismos. Mediante el reporte y documentación de los incidentes leves se busca minimizar el impacto de estos cuando se vuelvan a presentar.

Riesgos: La para en las operaciones es frecuente cuando los procesos no están documentados y no existe el personal con la suficiente experiencia y conocimiento para sobre llevar esas situaciones.

Recomendaciones: Documentar los procesos de operación y sociabilizar los mismos al personal adecuado, llevando a cabo entrenamientos y capacitaciones. Con esto se tiene un respaldo cuando se presenten los incidentes que amenazan las operaciones.

MONITOREAR Y EVALUAR

ME1 Monitorear y evaluar el desempeño de TI *(Nivel de madurez 2)*

Observaciones: Se realizan monitoreos de las plataformas tecnológicas implementadas en el ministerio pero no se lleva a cabo una medición del desempeño de las actividades y servicios que brinda el Departamento de Gestión Tecnológica.

Riesgos: No llevar evaluaciones de desempeño de TI puede generar en bajas de rendimiento en la prestación del servicio.

Recomendaciones: Realizar mediciones del desempeño de TI y llevar las mismas a un mejoramiento continúo en la calidad del servicio. Esto se lo puede llevar a cabo con el apoyo de los usuarios quienes pueden hacer evaluaciones de primera mano sobre su percepción en la calidad de los servicios del Departamento de Gestión Tecnológica.

ME2 Monitorear y evaluar el control interno *(Nivel de madurez 2)*

Observaciones: Se manejan políticas de manejo de información, de cumplimiento de los requerimientos legales, de acceso de los usuarios a los diferentes sistemas e información; sin embargo no se llevan a cabo controles del funcionamiento y manejo tanto de los sistemas, como de la información por parte de los usuarios y terceras personas.

Riesgos: No llevar a cabo un control interno puede provocar que se generen probabilidades de futuras fallas en las operaciones dado que no se tiene una actitud de prevención y pro actividad.

Recomendaciones: Crear controles internos asociados al marco de trabajo del gobierno de TI, logrando mejoras en cuanto a la efectividad y eficiencia de las operaciones con lo cual además se beneficiará de igual forma a la gerencia de la organización.

ME3 Garantizar cumplimiento regulatorio *(Nivel de madurez 1)*

Observaciones: Se siguen procesos informales para mantener el cumplimiento, y se ejecutan acciones en forma reactiva si existe la necesidad o como respuesta a auditorías o revisiones. Para su uso, se cumplen con los procedimientos proveídos por los fabricantes y desarrolladores en los manuales de los equipos y software. Se hace seguimiento a las regulaciones de rigen el uso de programas; su licenciamiento y actualización. Para optimizar el funcionamiento de los equipos se cuentan con sistemas de protección ante fallas de energía eléctrica, y eventualidades causadas por accidentes o desastres.

Riesgos: La falta de procedimientos formales que garanticen el cumplimiento regulatorio, conlleva el riesgo de infringir los marcos legales tanto nacionales e internacionales por desconocimiento o no actualización de los mismos. Esto puede traer problemas a la organización relacionados con licencias, copyright, derechos de autor e inclusive demandas por uso de software sin licencia.

Recomendaciones: Establecer procesos formales y documentados para mantener el cumplimiento regulatorio; para lo cual es necesario identificar de manera oportuna los requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios relacionados con la información, con la prestación de servicios de información Realizar evaluaciones y revisiones de forma eficiente y periódica, para garantizar el cumplimiento de los estándares, políticas y procedimientos de TI.

3.1.2 ANÁLISIS POR CRITERIOS DE INFORMACION

A continuación se presentan recomendaciones para alcanzar un grado óptimo en cada uno de los criterios de información COBIT, basados en los resultados obtenidos previamente y presentados en el *Capitulo 2 Tabla 2.40.*

***Efectividad**:* (Porcentaje 36,42%) Para alcanzar un grado óptimo de efectividad en el Departamento de Gestión Tecnológica del MIES, la información relevante manejada por el departamento debe ser la apropiada para el proceso del negocio, de igual manera su entrega debe ser oportuna, correcta y consistente.

***Eficiencia**:* (Porcentaje 36,43%) Para alcanzar un grado óptimo de eficiencia en el Departamento se deberá utilizar los recursos en forma óptima para la provisión de información.

***Confidencialidad**:* (Porcentaje 32,97%). Para alcanzar un grado óptimo de confidencialidad el Departamento deberá proteger la información sensible de divulgación no autorizada.

Integridad: (Porcentaje 35,06%). Para alcanzar un grado óptimo de integridad el Departamento de Gestión Tecnológica deberá manejar la información de una manera segura y disponible en el momento necesario, con el rendimiento adecuado y sólo para quien lo precise, construyendo así un equilibrio adecuado entre disponibilidad y seguridad de la información.

***Disponibilidad**:* (Porcentaje 27,73%). Para alcanzar un grado óptimo de disponibilidad en el Departamento, la información deberá estar disponible cuando ésta sea requerida por el proceso de negocio en cualquier momento. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas

***Cumplimiento**:* (Porcentaje 37,08%). Para alcanzar un grado óptimo de cumplimiento en el Departamento se deberá cumplir con leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto.

***Confiabilidad**:* (Porcentaje 37,36%). Para alcanzar un grado óptimo de fiabilidad el Departamento deberá proveer información apropiada para operar la gestión del MIES.

3.2 PRESENTACIÓN DEL INFORME FINAL DE LA AUDITORÍA

Informe Ejecutivo

El presente informe muestra los resultados de la evaluación realizada en el Departamento de Gestión Tecnológica del MIES, basado en los grados de madurez de los diferentes criterios de control inmersos en COBIT 4.0

Alcance de la auditoria

Siendo el MIES una entidad importante en el Estado Ecuatoriano, requiere que su activo más importante, la información, esté salvaguardada ante la creciente amenaza de los riesgos informáticos; por ello se llevará a cabo la Auditoría que comenzará con la identificación de los riesgos existentes y potenciales inherentes al Departamento de Gestión Tecnológica, posteriormente se aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles; para finalizar con las conclusiones y recomendaciones para el mejoramiento de la administración de riesgos informáticos.

Objetivos de la auditoría

- Identificar los riesgos informáticos a los que está expuesto el Departamento de Gestión Tecnológica del MIES.
- Aplicar COBIT en la auditoría para establecer mejoras en la administración de riesgos informáticos del Departamento de Gestión Tecnológica del MIES.
- Elaborar el informe de auditoría estableciendo las recomendaciones que ayuden a mitigar el impacto que los riegos informáticos pueden tener en el Departamento de Gestión Tecnológica del MIES.

Resultados

En la *Tabla 3.1* se presenta un resumen de los resultados obtenidos en cuanto a la madurez de los procesos, esto para que el gobierno de la empresa y de TI alcancen un entendimiento sobre dónde están ubicados y así realizar el análisis respectivo que conlleve a la puesta en práctica de las recomendaciones.

OBJETIVOS DE CONTROL COBIT	Nivel de

		Madurez
PLANEAR Y ORGANIZAR		
PO1	Definir el Plan Estratégico de TI	1
PO2	Definir la Arquitectura de la Información	2
PO3	Determinar la dirección tecnológica	2
PO4	Definir procesos, organización y relaciones de TI.	2
PO5	Administrar la inversión de TI.	3
PO6	Comunicar las aspiraciones y la dirección de la gerencia	3
PO7	Administrar recursos humanos de TI.	2
PO9	Evaluar y Administrar Riesgos de TI.	0
PO10	Administrar proyectos	3
ADQUIRIR E IMPLEMENTAR		
AI1	Identificar Soluciones Automatizadas	4
AI2	Adquirir y mantener el software aplicativo	3
AI3	Adquirir y mantener la infraestructura tecnológica	1
AI4	Facilitar la operación y el uso	1
AI5	Adquirir recursos de TI.	4
AI6	Administrar cambios	2
AI7	Instalar y Acreditar soluciones y cambios	1
ENTREGAR Y DAR SOPORTE		
DS2	Administrar servicios de terceros	1
DS3	Administrar desempeño y capacidad	1
DS4	Garantizar la Continuidad del Servicio	1
DS5	Garantizar la Seguridad de los Sistemas	3
DS7	Educar y entrenar a los usuarios	0
DS8	Administrar la mesa de servicio y los incidentes	2
DS9	Administrar la configuración	1
DS10	Administrar los problemas	2
DS11	Administrar los datos	3
DS12	Administrar el ambiente físico	2
DS13	Administrar las operaciones	2
MONITOREAR Y EVALUAR		
ME1	Monitorear y evaluar el Desempeño de TI.	2
ME2	Monitorear y evaluar el control interno	2
ME3	Garantizar cumplimiento regulatorio	1

Tabla 3.1: Niveles de madurez obtenidos de la evaluación

Los valores referenciales asignados para cada nivel de madurez están definidos en la *Tabla 3.2*

REPRESENTACIÓN DE LOS MODELOS DE MADUREZ		
Valor	**Representación**	**Significado**
0	No existente	No se aplican procesos administrativos en lo absoluto
1	Inicial	Los procesos son ad-hoc y desorganizados
2	Repetible	Los procesos siguen un patrón regular
3	Definido	Los procesos se documentan y se comunican
4	Administrado	Los procesos se monitorean y se miden
5	Optimizado	Las buenas prácticas se siguen y se automatizan

Tabla 3.2: Representación de los modelos de madurez

Temas críticos

Los siguientes procesos tienen un grado de madurez 0; es decir que no se aplican procesos administrativos en absoluto, por lo cual se considera crítico la aplicación de las recomendaciones adyacentes a cada proceso.

P09 Evaluar y administrar riesgos de TI

Observaciones: El Departamento de Gestión Tecnológica del MIES no considera importante la gestión de riesgos de TI, por tanto no existe una evaluación de riesgos para los procesos y las decisiones que se manejan en el departamento y tampoco existen estrategias de mitigación de riesgos.

No se ha definido políticas para la comunicación de planes de acción para mitigar riesgos.

Riesgos: Maximizar la posibilidad y el impacto de los riesgos de TI. El departamento es susceptible a todo tipo de amenazas, dado que no se han identificado todos los eventos que podrían tener un impacto potencial sobre las operaciones del departamento. Presentar una respuesta con lentitud e ineficiencia a las amenazas poniendo en riesgo la continuidad del negocio.

Recomendaciones: Tomar consciencia sobre la administración de riesgos, como parte fundamental de las operaciones del departamento. Definir políticas de evaluación y administración de riesgos. Identificar los posibles eventos y sus respectivos impactos que puedan afectar el buen funcionamiento del departamento. Evaluar frecuentemente la posibilidad de ocurrencia de los riesgos

identificados basados en métodos cualitativos y cuantitativos. Manejar políticas de mantenimiento y monitoreo de un plan de acción para mitigar los riesgos que incluya respuesta a los riegos, identificación de costos, beneficios y responsabilidades de la ejecución.

DS7 Educar y entrenar a los usuarios

Observaciones: cada usuario es responsable de salvaguardar su información y evitar que personas no autorizadas tengan acceso a los sistemas e información a través de usuarios que cuentan con permisos. Además no existe un reglamento para la capacitación del nuevo personal, por lo cual los funcionarios adquieren experiencia me diente el transcurso de sus labores cotidianas.

Riesgos: la falta de capacitación al nuevo personal puede generar problemas en la seguridad de los sistemas e información, pues por desconocimiento ellos eventualmente permiten el acceso a personas no autorizadas, provocan fallas de funcionamiento, y en general ponen en riesgo la información del ministerio.

Recomendaciones: crear planes para el entrenamiento del nuevo personal para permitir que puedan desenvolverse de forma más eficiente lo más pronto posible, logrando así una mejor adaptación a sus actividades laborales.

Impacto sobre los criterios de Información

El porcentaje del impacto sobre los criterios de información de COBIT se resume en la *Tabla 3.3.*

CRITERIOS DE INFORMACION

	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Promedio	**36,42%**	**36,43%**	**32,97%**	**35,06%**	**27,73%**	**37,08%**	**37,36%**

Tabla 3.3: Porcentaje del impacto sobre los criterios de información

En la *Figura 3.1* se presentan los promedios mencionados en la *Tabla 3.3* de forma gráfica para una mejor visualización de los resultados.

```
ERROR: typecheck
OFFENDING COMMAND: image

STACK:

-dictionary-
-mark-
-savelevel-
```