PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE ESMERALDAS



ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TÉSIS DE GRADO

TEMA:

"EVALUACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA BASADO EN ESTÁNDARES DE CONTROL INTERNO. CASO PRÁCTICO: CENTRO DE PRIVACIÓN DE LIBERTAD VARONES ESMERALDAS"

PREVIO OBTENCIÓN DEL TÍTULO DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR:

ALFREDO MARIO PEREA CAICEDO

ASESORA:

ING. SUSANA PATIÑO

ESMERALDAS, 2018

CERTIFICACIÓN

Disertación aprobada luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de grado de la PUCESE, previa a lo obtención del título de Ingeniero de Sistemas y Computación.

PRESIDENTE DEL TRIBUNAL DE GRADUACIÓN.

Ing. César Godoy
LECTOR 1.

Mgt. José Luis Carvajal
LECTOR 2.

Ing. Susana Patiño
DIRECTOR DE TESIS.

Mgt. Xavier Quiñónez
DIRECTOR DE ESCUELA.

AUTORÍA

Yo, PEREA CAICEDO ALFREDO MARIO, portador de la cédula de ciudadanía Nº 080207585-3, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes.

Perea Caicedo Alfredo Mario

AUTOR

DEDICATORIA

Dedico este trabajo de investigación a mis padres, mis hermanos, familia en general, compañeros de trabajo por el apoyo que me han brindado a lo largo de toda mi etapa académica ya que con su apoyo han sabido encaminarme para ser una persona de bien tanto en el aspecto humano como profesional.

Mario Perea Caicedo

AGRADECIMIENTO

En especial agradezco a las instituciones que me han abierto las puertas para ofrecer mis servicios profesionales que con mérito propio me he ganado su reconocimiento y que ha servido para fortalecerme como persona y a la vez como profesional de la carrera informática en varios años de actividades.

Ellos han sido indudablemente un buen ejemplo a seguir para ser una persona correcta, proba y con metas firmes a cumplir.

Mario Perea Caicedo

INDICE DE CONTENIDO

AUTORÍA iii

DEDICATORIA iv

AGRADECIMIENTO v

INDICE DE CONTENIDO vi

INDICE DE TABLAS viii

INDICE DE ANEXOS 11

RESUMEN EJECUTIVO 12

INTRODUCCIÓN 14

Presentación de la investigación 14

Planteamiento del problema 15

Justificación 17

Objetivos 19

Objetivo General 19

Objetivos específicos 19

CAPÍTULO I 20

1.1. Marco de referencia 20

1.1.1 Antecedentes (Estudios Previos) 20

1.2 Bases teóricas científicas 22

Comprensión de Objetivos y Procesos de negocio relacionados *33*

CAPÍTULO II 37

2. Metodología 37

2.1 Centro de Privación de Libertad de Personas Adultas Varones Esmeraldas..... 37
2.2. Funciones de la Dirección de TIC..... 40
2.2.3 Unidad de Redes y Comunicaciones 40
2.2.4 Unidad de Soporte Técnico y Mantenimiento..... 41
2.3 Método de investigación 42
2.3.1 Métodos y Técnicas..... 43
2.4 Población y muestra 43
2.5 Técnicas de procesamiento y análisis estadístico de datos empleados 43
CAPITULO III..... 44
3. Resultados 44
3.1 Análisis e interpretación de los resultados 44
CAPÍTULO IV 52
4. Propuesta..... 52
4.1 Evaluación de la infraestructura tecnológica..... 52
5. Conclusiones y recomendaciones 75
5.1 Conclusiones generales 75
5.2 Recomendaciones generales..... 76
Referencias bibliográficas 77

INDICE DE TABLAS

Tabla 1:	Niveles y Atributos, COBIT 5 PAM.	31
Tabla 2:	Escala de evaluación y porcentajes.	32
Tabla 3:	Calificación del proceso.	32
Tabla 4:	Niveles de riesgos.	34
Tabla 5:	Procesos y Riesgos.	35
Tabla 6:	Funcionarios de TIC y áreas.	40
Tabla 7:	Objetivos de la Unidad de TIC del CRSVE.	44
Tabla 8:	Procesos de la Unidad de TIC del CRSVE.	45
Tabla 9:	Riesgos de la Unidad de TIC	46
Tabla 10:	Matriz Objetivos y Procesos.	47
Tabla 11:	Matriz Objetivos y Riesgos.	47
Tabla 12:	Riesgos e Impactos.	48
Tabla 13:	Matriz Procesos y Riesgos.	49
Tabla 14:	Procesos de COBIT y Procesos de la Unidad de TIC	50
Tabla 15:	Cuestionario de Preguntas PROC-APO09.	55
Tabla 16:	Nivel de Madurez Obtenido PROC-APO09.	56
Tabla 17:	Cuestionario de Preguntas PROC-APO12.	57
Tabla 18:	Nivel de Madurez Obtenido PROC-APO12.	58
Tabla 19:	Cuestionario de Preguntas PROC-APO13.	59
Tabla 20:	Nivel de Madurez Obtenido PROC-APO13.	60
Tabla 21:	Cuestionario de Preguntas PROC- BAI09.	61
Tabla 22:	Nivel de Madurez Obtenido PROC- BAI09.	62
Tabla 23:	Cuestionario de Preguntas PROC- DSS02.	63
Tabla 24:	Nivel de Madurez Obtenido PROC- DSS02.	64
Tabla 25:	Cuestionario de Preguntas PROC-DSS04.	65

Tabla 26: Nivel de Madurez Obtenido PROC-DSS04. 66

Tabla 27: Cuestionario de Preguntas PROC-DSS05. 67

Tabla 28: Nivel de Madurez Obtenido PROC-DSS05. 68

Tabla 29: Cuestionario de Preguntas PROC-MEA02. 69

Tabla 30: Nivel de Madurez Obtenido PROC-MEA02. 70

Tabla 31: Resumen de Evaluación de los Procesos de COBIT. 72

INDICE DE ILUSTRACIONES

Ilustración 1:	Componentes del Gobierno Corporativo.	23
Ilustración 2:	Gobierno Corporativo y Activos Críticos.	25
Ilustración 3:	Predecesores a COBIT 5.	26
Ilustración 4:	Evolución de COBIT.	27
Ilustración 5:	Objetivos de COBIT.	27
Ilustración 6:	Áreas clave de COBIT.	28
Ilustración 7:	Dominios y Procesos de COBIT.	29
Ilustración 8:	Modelo de Riesgo del Negocio.	33
Ilustración 9:	Análisis de Riesgos.	33
Ilustración 10:	Orgánico funcional del CRSVE.	38
Ilustración 11:	Orgánico Estructural de la Unidad de TIC	38
Ilustración 12:	Orgánico Funcional de la Dirección Nacional de TIC.	39
Ilustración 13:	Modelo de Evaluación, COBIT 5.	42
Ilustración 14:	Diagrama de red del CRSVE.	53
Ilustración 15:	Evaluación del proceso de seguridad de información.	71

INDICE DE ANEXOS

Anexo 1:	Cuestionarios.	80
Anexo 2:	Documentos institucionales.	84
Anexo 3:	Valoración del Nivel de Madurez del PROC-APO09.	85
Anexo 4:	Valoración del Nivel de Madurez del PROC-APO12.	87
Anexo 5:	Valoración del Nivel de Madurez del PROC-APO13.	90
Anexo 6:	Valoración del Nivel de Madurez del PROC-BAI09.	93
Anexo 7:	Valoración del Nivel de Madurez del PROC-DSS02.	95
Anexo 8:	Valoración del Nivel de Madurez del PROC-DSS04.	97
Anexo 9:	Valoración del Nivel de Madurez del PROC-DSS05.	99
Anexo 10:	Valoración del Nivel de Madurez del PROC-MEA02.	101

RESUMEN EJECUTIVO

La presente investigación fue desarrollada en la Unidad de TIC del Centro de Rehabilitación Social Varones Esmeraldas (CRSVE), que pertenece al Ministerio de Justicia, Derechos Humanos y Cultos (MJDHC) con sede en la ciudad de Quito, en la cual se analizaron los procesos acerca de la infraestructura tecnológica que se cumplen en la Unidad de TIC, con la finalidad de aplicar una metodología de control interno que mejore la gestión de T.I. que permite identificar el riesgo que puede afectar a los procesos y determinar la toma de decisiones por parte de la Dirección de TIC que para el desarrollo del estudio se utilizó la investigación descriptiva cualitativa ya que se describieron procesos, aplicando indicadores y criterios de evaluación en la gestión de T.I.; como técnica de recopilación de información se emplearon entrevistas para determinar el nivel de la gestión que manejan los miembros de la Unidad de TIC, a quienes también se procedió a realizarles entrevistas con la finalidad de describir los procesos que se utilizan para realizar el control interno aplicando el marco de trabajo COBIT 5 con el cual se hace un seguimiento de las recomendaciones para la Unidad de TIC con base a un análisis de los procesos críticos y el nivel de madurez o capacidad de los procesos allí ejecutados se pudo concluir con una propuesta de intervención, con la cual se determinó que la gestión de T.I. en el CRSVE se cumple en un nivel de madurez al menos gestionado en determinados procesos pero que puede mejorarse siguiendo ciertas recomendaciones técnicas que se describen en el estudio.

PALABRAS CLAVES

Auditoria Basada en Riesgos, Evaluación de Infraestructura, Estándar de Control, Nivel de Madurez.

ABSTRACT

The present investigation was developed in the ICT Unit of the Social Rehabilitation Center Varones Esmeraldas (CRSVE), which belongs to the Ministry of Justice, Human Rights and Worship (MJDHC) with headquarters in the city of Quito, in which the processes were analyzed. about the technological infrastructure that are met in the ICT Unit, in order to apply an internal control methodology that improves IT management which allows to identify the risk that can affect the processes and determine the decision making by the ICT Directorate that for the development of the study qualitative descriptive research was used since processes were described, applying indicators and evaluation criteria in the IT management; As a technique for gathering information, interviews were used to determine the level of management handled by the members of the ICT Unit, who were also interviewed in order to describe the processes used to perform internal control by applying The COBIT 5 framework, which tracks the recommendations for the ICT Unit based on an analysis of the critical processes and the level of maturity or capacity of the processes executed there, could be concluded with an intervention proposal , with which it was determined that IT management in the CRSVE it is fulfilled at a level of maturity at least managed in certain processes but that can be improved by following certain technical recommendations that are described in the study.

KEYWORDS

Risk Based Audit, Infrastructure Evaluation, Control Standard, Maturity Level.

INTRODUCCIÓN

Presentación de la investigación

Hoy en día las Tecnologías de la Información están vinculadas al manejo sistemático de las instituciones, por ende, los estándares y normativas de T.I. deben estar, alineados a las políticas institucionales. El CRSVE es una Institución pública, regida por el Ministerio de Justicia, la cual requiere implementar un modelo metodológico apropiado para el control de los recursos de T.I., el CRSVE precisa de la aplicación de tales procedimientos para la Evaluación de la Infraestructura Tecnológica para apoyar la gestión de sus directivos.

Las instituciones modernas son apoyadas estratégicamente a por las TIC, pero estas a la vez no son independientes y debido a su influencia en las actividades de la institución, se apoya en la Auditoría Informática a través del Control interno. Por tanto, la meta de la auditoría es asegurar que se cumplan con las políticas y los requerimientos legales, y la información que surja como consecuencia de los procesos informatizados sea la correcta, exacta y confiable.

En el CRSVE se maneja sistemas de gestión penitenciaria, cuenta con una unidad de sistemas que reporta a administración central, gestión de T.I., recursos tecnológicos requeridos por la Institución y brinda apoyo técnico a la infraestructura tecnológica del centro, por estas razones se ha contemplado llevar a cabo una Evaluación de la Infraestructura Tecnológica, con base al control del Gobierno de T.I. a través de COBIT 5 basado en un amplio marco de trabajo con lo que se analizó los procesos y actividades de las Unidad de TIC Se desarrolló la metodología con el objetivo de evaluar los niveles de cumplimiento de los objetivos de control interno de T.I. en el CRSVE, mediante la aplicación de encuestas y entrevistas al personal técnico de la institución.

Planteamiento del problema

El Ministerio de Justicia Derechos Humanos y Cultos (MJDHC), es una entidad del estado ecuatoriano que coordina y trata de mejorar la Justicia juntamente con otros organismos como Ministerio del Interior, Judicatura y Centros de privación de Libertad pertenecientes a la Dirección Nacional de Rehabilitación Social (Ministerio de Justicia, 2017).

Dentro de la estructura organizacional del MJDHC se encuentra la Dirección de Tecnologías de la Información, la cual está al frente de todos los procesos de índole tecnológica a nivel nacional; esta Dirección se apoya de las unidades de tecnología de los centros de privación de libertad provinciales para realizar sus funciones. Actualmente la Dirección de Tecnologías de la Información está mejorando su infraestructura tecnológica con el objetivo de conseguir que los procesos estratégicos e institucionales sean más eficientes (Ministerio de Justicia, 2017).

En la ciudad de Esmeraldas existen tres Centros de Privación de Libertad de Personas: 1) Centro de Rehabilitación Social Varones (CRSVE), 2) Centro de Rehabilitación Social Femenino (CRSFE) y 3) Centro de Adolescentes Infractores (CAI); en los cuales se ejecutan actividades administrativas concernientes a los lineamientos institucionales del MJDHC; por tanto los funcionarios administrativos dependen mucho de la tecnología informática para realizar sus labores cotidianas: reportes a planta central, uso de plataformas informáticas gubernamentales, correo electrónico institucional, casilleros electrónicos, Software de Gestión Documental , etc. (Ministerio de Justicia, 2017).

La infraestructura de equipos informáticos en los centros de privación de libertad de la ciudad de Esmeraldas en los últimos años ha mejorado considerablemente, y es la recientemente creada Unidad de Tecnología Informática, la encargada de realizar una correcta administración y de identificar las mejores estrategias de aprovechamiento de los recursos tecnológicos existentes.

Las actividades de la Unidad de Tecnología del Ministerio de Justicia Derechos Humanos y Cultos de la ciudad de Esmeraldas consisten en: 1) Realizar mantenimiento preventivo de computadoras; 2) Monitoreo del sistema de video vigilancia de los centros; 3) Realizar el mantenimiento de equipos, hardware y

software de la institución; 4) Realizar los procesos correspondientes para llevar a cabo las videoconferencias institucionales; 5) Administrar la red de computadoras de los centros y 6) Administrar los lectores biométricos de control de asistencia del personal de los centros.

El problema se presenta debido a que a los directivos del CRSVE se les dificulta la gestión de recursos tecnológicos por la falta de conocimiento técnico en esta área y es indispensable un control minucioso de estos recursos para que exista una correcta gestión administrativa y toma de decisiones que contribuyan al mejoramiento de la administración y suplir las necesidades tecnológicas del Centro con el planteamiento de la propuesta: "Evaluación de la infraestructura tecnológica basada en estándares de control interno. Caso práctico: Centro de Privación de Libertad Varones Esmeraldas."

Los sistemas informáticos sino están perfectamente montados con niveles de control interno que permitan satisfacer que esa información es la correcta pues pueden provocar situaciones en las que la información provista no sea la correcta.

Justificación

La Evaluación de la Infraestructura tecnológica basada en Objetivos de Control Interno en el CRSVE-MJDHC, garantizará la correcta gestión de recursos informáticos, alineamientos de las políticas institucionales del Ministerio de Justicia con el gobierno de TIC y permitirá mejorar el aspecto administrativo del Centro.

Es muy importante efectuar una planificación ordenada y apegada a los objetivos de control interno, tal que permita contrastar el cumplimiento de tales controles, tal como se especifica en el plan, de tal manera que se pueda tener una mejor perspectiva sobre la gestión de T.I. para los directivos.

Los directivos del CRSVE delegan responsabilidades, para ejecutar las actividades o responsabilidad, y el control interno tiene que asegurar que se cumplan con las políticas y los requerimientos legales, y la información que surja como consecuencia de los procesos informatizados sea la correcta, exacta y confiable.

Un plan de evaluación del control interno que esté correctamente dirigido para conseguir los objetivos propuestos es una base real sobre la que descansa la confiabilidad y exactitud de la información circulante, que, a su vez, sirve como fundamento a los directivos para la toma de decisiones puntuales, a tiempo y acertadas.

Para la realización de esta evaluación informática se toma como marco de referencia COBIT 5, el cual es un marco de gobernabilidad de T.I. y un conjunto de herramientas de ayuda que permite a los administradores tener en cuenta y asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos del negocio.

Estos conjuntos de las mejores prácticas permiten evaluar la seguridad, eficacia, calidad y eficiencia de las tecnologías., mediante esto se determinan los riesgos, tener una gestión efectiva de los recursos, medir el desempeño y cumplimiento de metas, y de manera principal medir el nivel de madurez de los procesos de la organización.

Las funciones de control interno y auditoria informática son de vital importancia ya que ayudan a las organizaciones a cumplir obligaciones relativas al control interno mediante el proceso de recoger, agrupar y evaluar hallazgos para determinar si se salvaguarda los activos, se mantiene la integridad de los datos, se lleva a cabo eficazmente los fines de la organización y utilizar eficientemente los recursos.

Los principales beneficiarios de la realización de este proyecto serán: la Dirección de Tecnologías y Dirección del Centro ya que el documento servirá como instrumento de apoyo técnico a las decisiones que se tomen para la gestión de recursos tecnológicos de la institución.

Objetivos

Objetivo General

Evaluar la Infraestructura Tecnológica del Centro de Privación de Libertad Varones Esmeraldas, mediante la aplicación de estándares de control interno de T.I.

Objetivos específicos

- Conocer las bases conceptuales del Control Interno de T.I.
- Describir la situación actual sobre la infraestructura tecnológica del CRSVE.
- Aplicar el análisis de riesgos a los procesos críticos de la Unidad de TIC del CRSVE.
- Determinar el nivel de madurez de la gestión de T.I. mediante el modelo de Evaluación de Procesos Cobit 5.

CAPÍTULO I

1.1. Marco de referencia

1.1.1 Antecedentes (Estudios Previos)

En los últimos años la Auditoria Informática ha sido objeto de estudio en varios trabajos de investigación lo que ha mejorado la perspectiva metodológica en el control de los recursos tecnológicos de medianas y pequeñas organizaciones, varias de ellas instituciones educativas de reconocido prestigio a nivel local y nacional (Vivero, 2016).

Mediante la organización informática de las unidades de tecnología de determinadas instituciones estatales a nivel local. Se ha realizado un diagnóstico en el cual se establece la estructura que debe tener la Unidad de Tecnología, las funciones que deben ejecutar los miembros, las políticas que norman el uso de recursos y servicios tecnológicos y los procedimientos más esenciales que deben ejecutarse, a más del desarrollo de un sistema para la gestión de actividades. Estas propuestas son de gran importancia y utilidad, para cumplir con los objetivos encomendados, brindar servicios con calidad y calidez a usuarios internos y externos, y a cumplir con lo estipulado por la Contraloría General del Estado en las Normas de Control Interno, específicamente en la Norma 410 referente a Tecnología de la Información (Lastra Vernaza, 2014).

Es así que en varios textos investigativos (Jara, 2012) se determina la importancia de implementar la Auditoría Informática y los procesos de Control T. I. en las instituciones a fin de que sea un aporte para las decisiones de los directivos de dichas organizaciones.

No obstante, la aplicación de dichas auditorias también implica determinar falencias en los sistemas de información, muchas veces de alta relevancia nacional, como por ejemplo ,el Sistema de Escrutinios del Consejo Nacional Electoral (CNE), el cual está regido por un Reglamento de Auditoria de los Procesos Electorales (CNE, 2016).

Se puede definir a la vulnerabilidad como cualquier tipo de falencia que tiene un sistema mismo que pueda comprometer los activos informáticos de una institución (Andrade, 2016)

Mediante la constatación y el cumplimiento de los lineamientos de seguridad de la información luego de haber sido generadas, definidas, documentadas y socializadas dentro de la organización, ayudarán a la preservación y aseguramiento de la confidencialidad, integridad y disponibilidad de la información (Andrade, 2016).

La utilización de una infraestructura adecuada, reducirá las vulnerabilidades de los recursos informáticos garantizando el desarrollo regular de funciones y procesos tecnológicos de las instituciones (Cedeño, 2017).

Sin embargo, las investigaciones no han evaluado la infraestructura tecnológica para determinar y mejorar las políticas que rigen la gestión de recursos de tecnología e información en centros penitenciarios.

1.2 Bases teóricas científicas

La Auditoría Informática realiza un análisis minucioso de las normas, controles, técnicas y procedimientos que se norman en una institución, la gestión de la infraestructura tecnológica y poder tomar dediciones que permitan impedir una mala gestión (Leal, 2010).

La auditoría informática ha sufrido cambios importantes desde hace ya varios años con la intervención de la tecnología informática en la manera de tratar la información para los directivos de una institución. La prioridad de conseguir y mantener actualizados los diferentes sistemas de información se torna cada vez más apremiante (Actualidad Tecnológica, 2016).

Los auditores informáticos realizan un trabajo estrictamente técnico, demostrando su solvencia con la tecnología informática. Se continúa con el tema del control de auditoría, y los técnicos en auditoría informática de sistemas informáticos solventan soluciones a la empresa y a los otros auditores en todo lo concerniente a dichos controles (Actualidad Tecnológica, 2016).

Un buen gobierno corporativo electrónico es el marco de trabajo sostenible mediante el cual, las organizaciones son manejadas y controladas, de manera óptima y transparente, y generando armonía, compromiso e integración entre sus grupos de interés y sus diversas expectativas. Su fundamento es el desarrollo económico y competitivo, la ética y el crecimiento sostenible (Viteri, 2016).

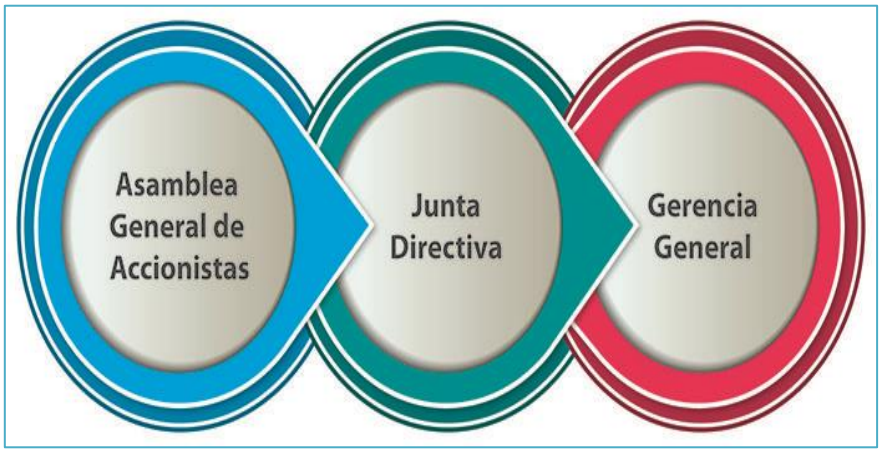
Gobernance es definida como el arte de liderazgo público, en el cual el actor principal es el Estado. Por lo tanto, el régimen político, la administración pública, y la capacidad del gobierno son elementos sensitivos para la buena gobernanza (UTADEO, 2010).

Esta perspectiva prioriza la necesidad de que haya mecanismos que dirijan, guíen a la comunidad, y adjudica este papel al Estado en forma principal.

La gobernanza implica dar una dirección centrada a la sociedad y que ésta es una función del Estado, independientemente de las transiciones en las estructuras gubernamentales promovidas por la descentralización y democratización (UTADEO, 2010).

Las buenas prácticas de gobierno corporativo en una organización ha probado ser vinculante en la forma en que las organizaciones asimilan y se adecuan a cambios de su ambiente y contrarrestan crisis o amenazas de cualquier tipo. Así mismo, si se desarrolla de acuerdo con la estrategia particular de la organización se convierte en una herramienta para ejecutar políticas eficientemente y conducirlas de buena manera en momentos de incertidumbre. (UTADEO, 2010)

Ilustración 1: Componentes del Gobierno Corporativo



Fuente: (ESSA, 2017)

Para alcanzar un mejor entendimiento de lo que consiste el Gobierno Corporativo, se puede plantear una analogía entre la buena estructuración de una organización y el gobierno. Si establecemos una analogía entre los administradores de una compañía y los gobernantes de un país, por un lado, y entre accionistas y ciudadanos, por otro lado se hallaran algunos principios de buen gobierno comunes a las sociedades comerciales y a las políticas. Entre ellos, destacan dos: (1) Debe contrarrestarse la acumulación excesiva de poder de los gobernantes, por medio de la fiscalización y control de otras dependencias que lo equilibren; y, (2) Debe haber mecanismos que influyan a los apoderados a proteger los intereses comunes (Mena, 2015).

Entre las actividades principales que definen el concepto de gobierno corporativo se destacan la participación de los accionistas en la toma de decisiones, el equilibrio y diversidad en Directorios o Consejos de Administración, sistemas de monitoreo y control, institucionalidad de la organización, ejecución de regulaciones, sistemas de compensación, responsabilidad social, elaboración de códigos de ética, etc. (Mena, 2015).

Gobierno de T.I. trata sobre un conjunto de procesos y relaciones destinados a administrar y controlar la empresa, con la finalidad de lograr sus objetivos y agregar valor mientras se equilibran los riesgos y la integración sobre T.I. y sus procesos. (ISACA, 2011).

El Gobierno de T.I., es una metodología de trabajo, no una solución definitiva. Está encaminado a proveer las estructuras que integran los procesos de T.I., recursos de T.I. e información con las estrategias y los objetivos de la organización. Además, el Gobierno de T.I. integra y legitima las mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoriza el rendimiento de T.I. para asegurar que la información de la organización y las tecnologías relacionadas soportan los lineamientos organizacionales. (ISACA, 2011).

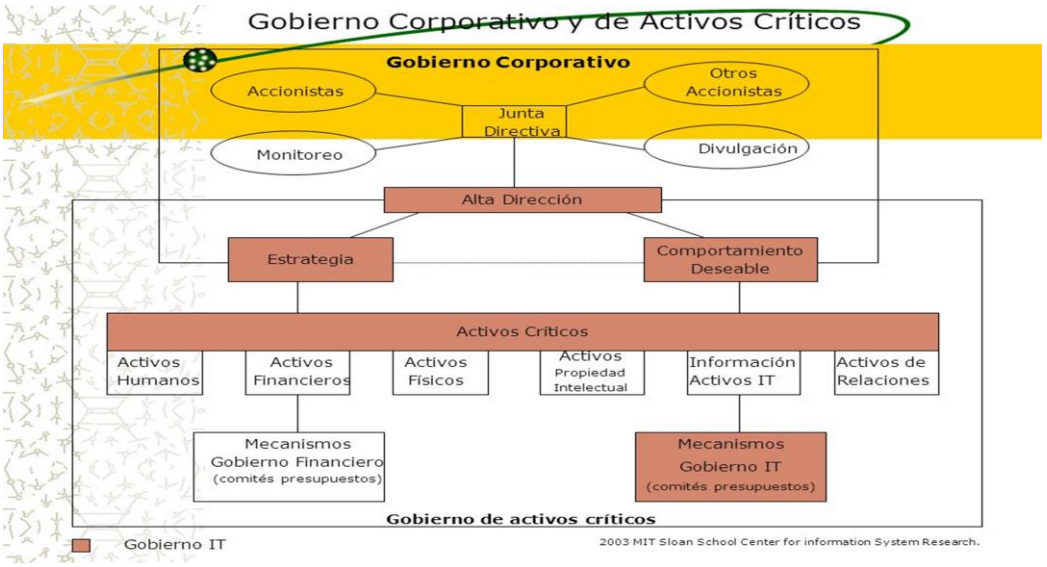
El Gobierno de T.I. viabiliza a la organización a alcanzar ventaja de su información logrando con esto optimizar sus beneficios y obtener ventaja competitiva. (ISACA, 2011).

Por la misma estructura de la tecnología, en muchos casos otras instancias declaran su falta de conocimiento en el tema, lo que contribuye a separar aún más el área de T.I. La enorme dificultad del gobierno de T.I. es alinear los objetivos estratégicos de T.I. con los de la empresa. Supondría esto solo un problema de planeación estratégica pero no es necesariamente solo este factor el que debe considerarse; las áreas de T.I. están presionadas por diferentes instancias, como las regulatorias, técnicas y financieras. La solución a estas presiones puede llevar fácilmente a perder el alineamiento con la organización y dedicarse a resolver problemas puntuales.

En las empresas a las TIC se las considera como un mal necesario y debido a la naturaleza técnica de sus directores el área de T.I. no es capaz de demostrar el valor agregado que presta a la institución, al punto de que, si no fuera demasiado visible, la unidad se extinguiría. Por otro lado, asoman nuevas tecnologías y procesos empresariales que hacen que las TIC deban responder a otros requerimientos u operar bajo otros niveles, como por ejemplo la subcontratación de servicios de T.I. a todos los niveles, el Cloud Computing, Outsourcing étc. Estas nuevas fórmulas sugieren nuevas metas para el desarrollo de los procesos y servicios que debe brindar la unidad de TIC

dentro de una organización. No importa cuál sea el modelo utilizado, las TI deben estar vigente para el apoyo de la institución. (ICESI, 2011).

Ilustración 2: Gobierno Corporativo y Activos Críticos



Fuente: (Laguado, 2017)

Cobit es una metodología para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una empresa, es decir, gobierno de T.I, usuarios y, los auditores que intervienen en el proceso. El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de la línea del negocio la seguridad T.I. y que abarca controles determinados de T.I. desde un punto de vista empresarial (Baquero, 2013).

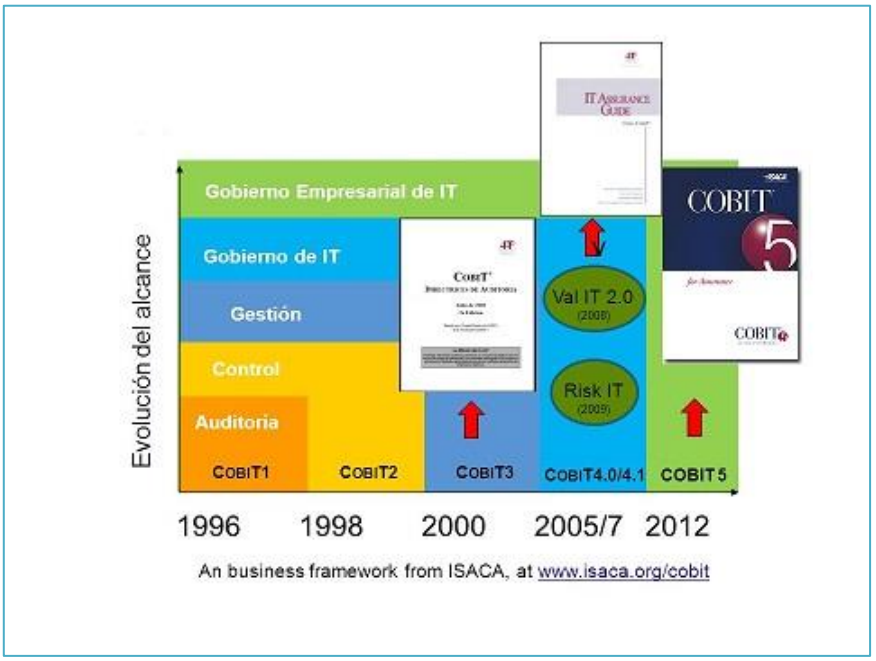
La misión de COBIT es investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control aceptados para las tecnologías de la información y comunicación que sean autorizados, actualizados e internacionales para el uso del día a día de los gestores de negocios, administradores de sistemas, auditores, entre otros (ISACA, 2017).

Ilustración 3: Predecesores a COBIT 5.

Versión de COBIT	Contenido
COBIT 1	Objetivos de Control- Guías de Auditoría
COBIT 2	Guías de Autoevaluación- Actualización de la versión automatizada-Referencias y material de apoyo adicional.
COBIT 3	Incorporación de las Guías de Controles-Mejoras en los objetivos de control-Identificación de indicadores de desempeño.
COBIT 4.1	En su cuarta edición, COBIT tiene 34 procesos que cubren 210 objetivos de control: 1. Planificación y Organización 2. Adquisición y Soporte 3. Supervisión y Evaluación.

Fuente: (ISACA - COBIT 5, 2012)

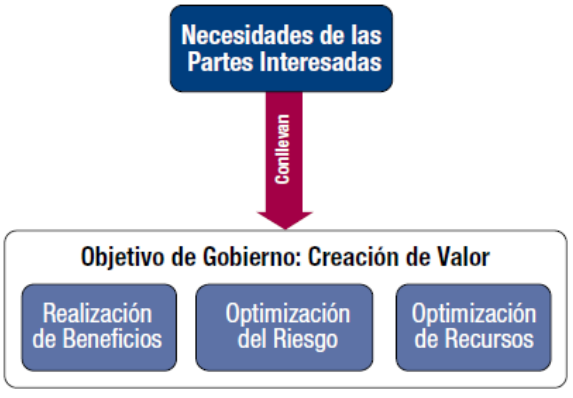
Ilustración 4: Evolución de COBIT



Fuente: (ISACA - COBIT 5, 2012)

COBIT 5 es el marco de gestión y de negocio global para el gobierno y la gestión de las TI de la empresa. Este documento contiene los 5 principios de COBIT 5 y define los 7 catalizadores que componen el marco.

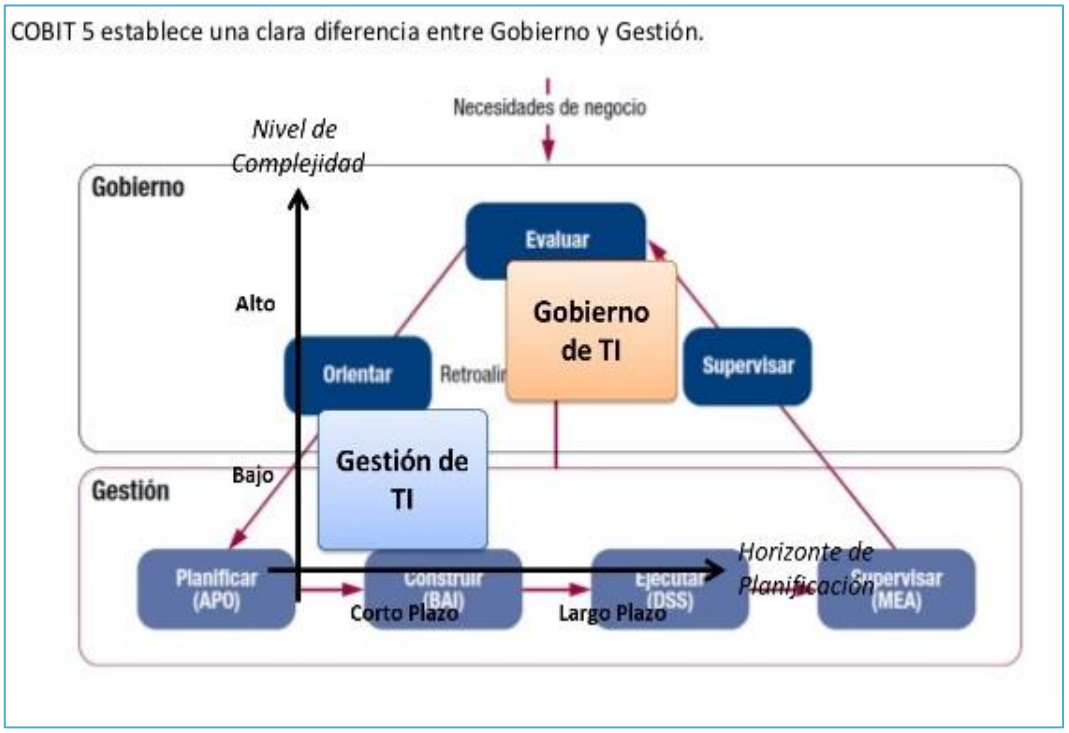
Ilustración 5: Objetivos de COBIT



Fuente: (NONES, 2014)

COBIT 5 establece una notoria diferencia entre gobierno y la gestión de TIC, según la siguiente imagen:

Ilustración 6: Áreas clave de COBIT



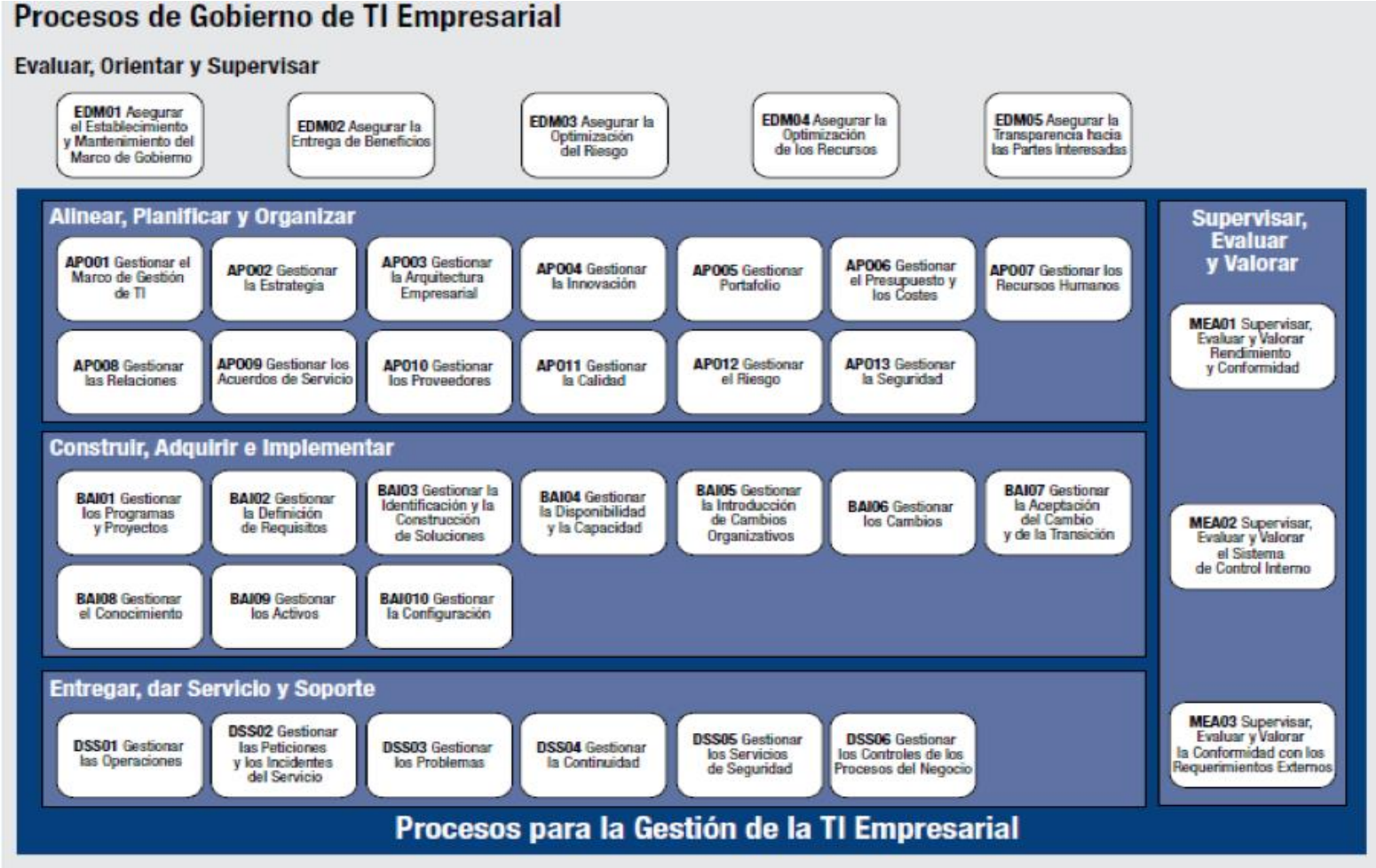
Fuente: (ARANDA, 2013)

Gobierno de T.I.: Participa un solo dominio D-EDM (Evaluar, Dirigir y Monitorear) y se apoya en 5 subprocesos.

Gestión de T.I.: COBIT proporciona control a las áreas de responsabilidad integral. Participan cuatro dominios:

- D-APO Alinear, Planificar y Organizar.
- D-BAI Construir (Build), Adquirir e Implementar.
- D-DSS Entregar, Dar Servicio y Soporte.
- D-MEA Monitorear, Evaluar y Valorar.

Ilustración 7: Dominios y Procesos de COBIT 5



Fuente: (Francavilla, 2012)

COBIT 5 contiene las siguientes guías:

- Guía de Autoevaluación: Se utiliza para evaluar o efectuar un control menos estricto de la capacidad de los procesos de TI.
- Modelo de Procesos de Evaluación PAM: Está orientado a efectuar un control TI más estricto.

En el libro de COBIT 5 Procesos Catalizadores, se especifican las métricas utilizadas en cada uno de los procesos con las cuales se puede medir y evaluar el nivel de madurez. También contiene recomendaciones para mejorar el proceso evaluado.

Los niveles de calificación y atributos lo conforman 5 niveles de madurez de un proceso. Cada nivel está conformado por atributos o características a medir que tiene cada proceso

- **Nivel 0 -Proceso Inexistente:** No existe ninguna acción para obtener la meta. En este nivel, no existe o es insignificante el Meta del proceso.
- **Nivel 1 -Proceso realizado (1 atributo):** El proceso implementado obtiene la meta.
- **Nivel 2 - Proceso Gestionado (2 atributos):** El proceso implementado de una manera planificada.
- **Nivel 3 - Proceso Establecido (2 atributos):** El proceso implementado se basa en un proceso definido.
- **Nivel 4 - Proceso predecible (2 atributos):** El proceso implementado se desenvuelve dentro límites predefinidos para alcanzar la meta.
- **Nivel 5 - Optimización del proceso (2 atributos):** El proceso implementado Continúa mejorado para cumplir con los objetivos y lineamientos institucionales.

Tabla 1: Niveles y Atributos, COBIT 5 PAM

NIVEL DE CAPACIDAD	ATRIBUTO
NIVEL 0: No realizado	
NIVEL 1: Proceso realizado	PA 1.1: Realización del proceso
NIVEL 2: Proceso gestionado	PA 2.1: Gestión de la realización PA 2.2: Gestión del producto de trabajo
NIVEL 3: Proceso establecido	PA 3.1: Definición del Proceso PA 3.2: Despliegue del proceso
NIVEL 4: Proceso predecible	PA 4.1: Medición del Proceso PA 4.2: Control del proceso
NIVEL 5: Proceso optimizado	PA 5.1: Innovación del proceso PA 5.2: Optimización continua

Fuente: (Huerta, 2016)

Tabla de evaluación cada atributo se evalúa mediante una escala de calificación mediante la siguiente nomenclatura:

- **No logrado (NL):** Hay poca o ninguna evidencia del logro del atributo definido en el proceso evaluado.
- **Bajamente logrado (BL):** Hay algunas pruebas de enfoque y algunos logros, del atributo definido en el proceso evaluado. Algunos aspectos de la realización del atributo pueden ser impredecibles.
- **Medianamente Logrado (L):** Hay evidencia de un enfoque sistemático y existe logro significativo de la definición del atributo en el proceso evaluado. Algunos puntos débiles relacionados con este atributo pueden existir en el proceso de evaluación.
- **Suficientemente logrado (SL):** Hay evidencia de un enfoque completo y sistemático, existe un pleno cumplimiento de la definición del atributo en el proceso evaluado. No existen debilidades significativas relacionadas con este atributo en el proceso de evaluación.

Hay una necesidad de garantizar un grado coherente de interpretación a la hora de decidir qué calificación a asignar. En la tabla siguiente se describe la calificación en términos de porcentaje de completado un proceso para determinar la escala de evaluación:

Tabla 2: Escala de evaluación y porcentaje

SÍMBOLOGÍA	CUALIDAD	RANGO
NL	INSUFICIENTE	0 al 15%
BL	BAJO	>15% al 50%
ML	MEDIO	>50% al 85%
SL	SUFICIENTE	>85% al 100%

Fuente: (Huerta, 2016)

En el cuadro siguiente se muestra la evaluación de un proceso de COBIT

En el cual se evalúa el nivel, atributos. La calificación asignada es ¨Nivel 2¨ Es un proceso Gestionado.

Tabla 3: Calificación del Proceso

Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
EDM01		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Evaluación por criterio		SL	SL	ML	BL	NL				
Capacidad Nivel alcanzado				2						

Fuente: (Huerta, 2016)

Comprensión de Objetivos y Procesos de negocio relacionados en cuanto a los objetivos y procesos se tomará en cuenta los siguientes puntos:

- Los objetivos institucionales
- Agregación de valor.
- Las metas temporales de la institución.
- Las metas temporales de los principales directivos.
- La presentación de documentos habilitantes.

Los procesos de negocio deben ser identificados considerando la cadena de valor de la institución. A nivel de la Unidad de TIC los procesos se pueden ubicar de la siguiente manera.

- Procesos operativos
- Procesos de soporte

Identificación de objetivos y riesgos con base al modelo básico de riesgo empresarial.

Ilustración 8: Modelo de Riesgos del Negocio



Fuente: (Barona, 2011)

Análisis de riesgos se utilizará la escala de riesgos siguiente:

Ilustración 9: Análisis de riesgos



Fuente: (Carmona, 2013)

Tabla 4: Niveles de riesgos

NIVEL		DESCRIPCIÓN
MA	MUY ALTO	Requiere inmediata intervención
A	ALTO	Requiere acción de alta gerencia
M	MEDIO	Requiere supervisión de su manejo
B	BAJO	Requiere revisión de rutina

Fuente: (Carmona, 2013)

La evaluación de procesos y riesgos sería analizar cada etapa del proceso para determinar si existe una correlación entre el proceso y el riesgo. Luego de identificar con qué riesgos se asocia un proceso en especial, se deben evaluar las relaciones en función

de si se trata de una correlación principal o secundaria. Las vinculaciones clave son aquellas en las que el proceso desempeña un rol directo y principal en la gestión del riesgo. Las vinculaciones secundarias son aquellas en las que el proceso ayuda a gestionar el riesgo de manera indirecta.

Tabla 5: Procesos y Riesgos

MATRIZ : PROCESOS VS RIESGOS								
P: PRIORITARIO S: SECUNDARIO	RIESGO 1	RIESGO 2	RIESGO 3	RIESGO 4	RIESGO 5	RIESGO 6	RIESGO 7	RIESGO N
PROCESO 1		S		P				
PROCESO 2			S					
PROCESO 3								
PROCESO 4	P							
PROCESO 5				S	S	S	P	
PROCESO 6		P			P	P		
PROCESO 7	S							
PROCESO N								

Fuente: (Carmona, 2013)

Priorización del riesgo: identificar los riesgos más sensitivos para la institución de acuerdo con los resultados de la evaluación.

Plan de auditoría se considera:

- El análisis de asignaciones principales y secundarias entre procesos y riesgos.
- La aplicación del análisis de riesgo.

También se puede hacer una clasificación de los procesos que serían sujetos de auditoría.
Luego de determinar los procesos a ser auditados y las etapas de la auditoría, posteriormente se debe realizar la estimación y asignación de recursos y proceder a la ejecución del plan.
Los planes de auditoría basados en riesgos sugieren ser actualizados periódicamente.

CAPÍTULO II

2. Metodología

El tipo de investigación es descriptiva cualitativa y se basa en el desarrollo de la metodología ABR "Auditoría Basada en Riesgos".

La metodología de COBIT plantea un marco de trabajo donde se evalúan los criterios informáticos, se controlan los recursos informáticos que comprenden la tecnología de información, estos son, infraestructura tecnológica, equipos, sistemas, aplicativos entre otros, y como parte final se realizará una evaluación sobre los procesos tecnológicos institucionales.

2.1 Centro de Privación de Libertad de Personas Adultas Varones Esmeraldas

Es el mayor Centro de privación de libertad de la provincia y uno de los mayores de la Zona 1 (Sucumbíos, Imbabura, Carchi, Esmeraldas) de acuerdo a su población carcelaria (600 internos) y a su área física.

La Misión

Velar por el acceso a una justicia oportuna, independiente y de calidad, promover la paz social, la plena vigencia de los Derechos Humanos, el ejercicio de cultos y su regulación, mejorar la rehabilitación y su reinserción social en las personas adultas privadas de libertad y el desarrollo integral en adolescentes en conflicto con la ley penal, mediante normas, políticas, programas, proyectos y actividades coordinadas con las instituciones relacionadas (Ministerio de Justicia, 2017).

La Visión

Al 2017 el Ministerio de Justicia, Derechos Humanos y Cultos habrá logrado la plena vigencia de los Derechos Humanos, la transformación del sistema de justicia, la regulación del ejercicio de cultos, la atención integral a personas adultas privadas de libertad y adolescentes en conflicto con la ley penal al convertirse en un referente de gestión pública a nivel nacional e internacional (Ministerio de Justicia, 2017).

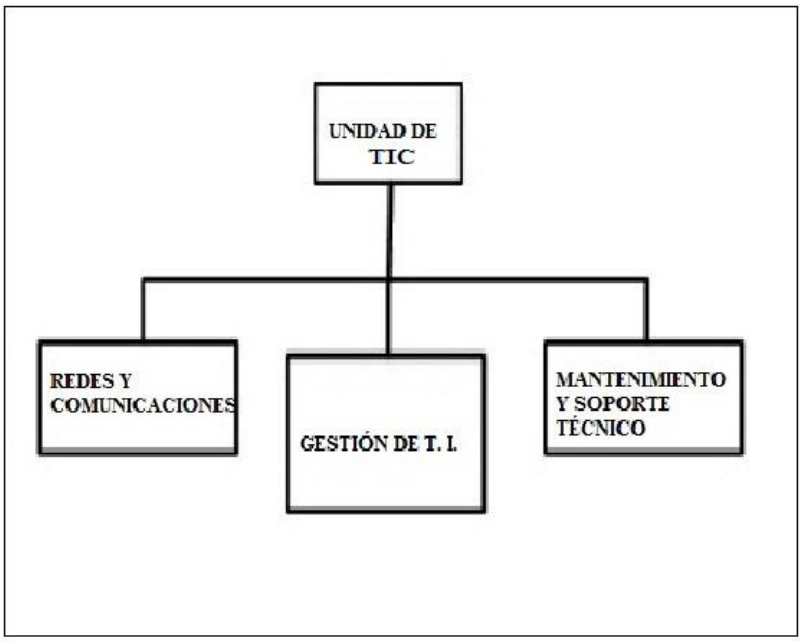
EL CRSVE se encuentra estructurado de la siguiente manera

Ilustración 10: Orgánico funcional del CRSVE



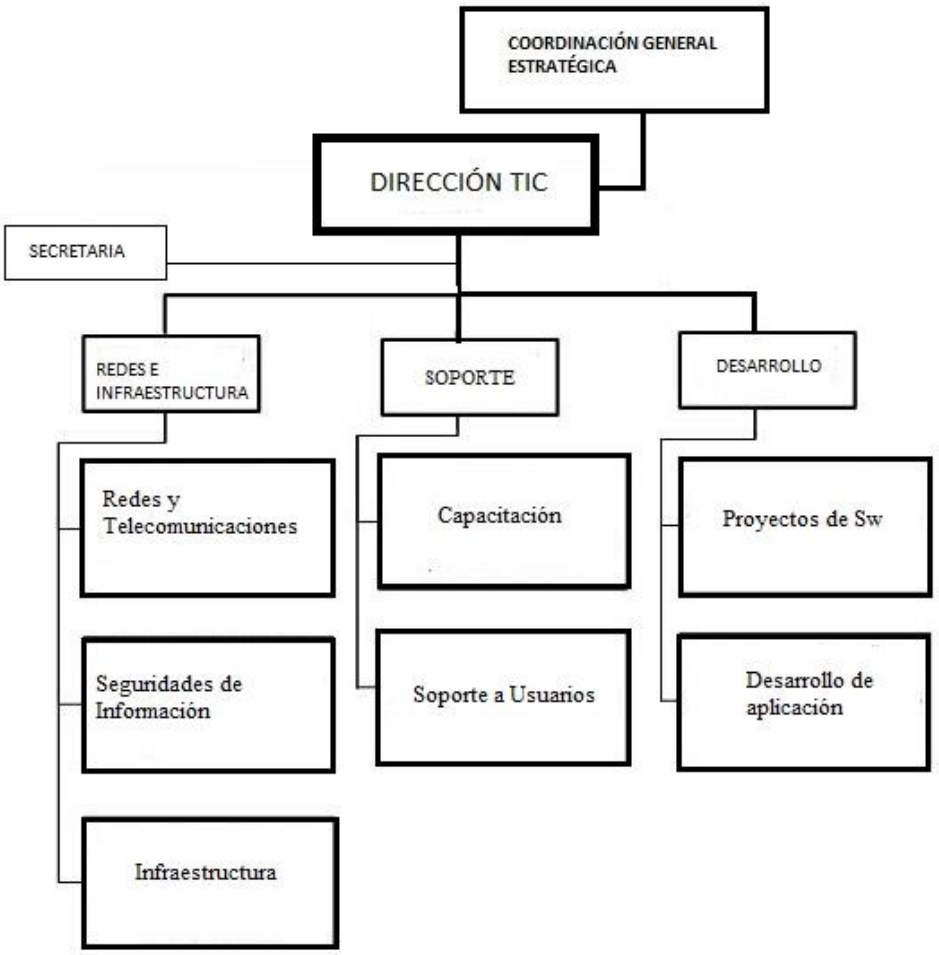
La Unidad de TIC del CRSVE, se encuentra organizada de la siguiente manera:

Ilustración 11: Orgánico Estructural de la Unidad de TIC



El orgánico funcional de la Dirección Nacional de Tecnologías de la Información y Comunicación del Ministerio de Justicia, Derechos Humanos y Cultos con sede en el Edificio de Planta Central en la Ciudad de Quito, se encuentra organizado de la siguiente manera:

Ilustración 12: Orgánico Funcional de La Dirección Nacional de TIC



El personal que labora en la Dirección Nacional de TIC, está conformada por 11 funcionarios organizados de la siguiente manera:

Tabla 6: Funcionarios de TI y Áreas

CANT.	FUNCIÓN	LOCALIZADO	PUESTO
1	Director de TIC	Planta Central	Jefe
1	Secretaria		Secretaria
3	Administración de Redes y Comunicaciones		Analista
3	Administración y Desarrollo de Sistemas		
3	Mantenimiento y Soporte Técnico		

2.2. Funciones de la Dirección de TIC

2.2.3 Unidad de Redes y Comunicaciones

- Implantación de redes informáticas LAN.
- Implantación del equipo, estaciones de trabajo y demás dispositivos electrónicos de las redes informáticas.
- Manejo de sistemas operativos, administración de clientes, aplicaciones y utilitarios.
- Mantener en perfecto funcionamiento las redes de datos y telecomunicaciones.
- Administrar y mantener en perfecto funcionamiento la infraestructura.
- Garantizar la disponibilidad los servicios de tecnología.
- Implementar nuevos requerimientos de comunicación, voz IP, videoconferencia y demás dispositivos electrónicos necesarios para el funcionamiento de las redes informáticas.
- Mantener y actualizar los manuales, planos, especificaciones técnicas y toda la documentación necesaria, relacionado a redes informáticas, telecomunicaciones, infraestructura y sistemas de seguridades de la información.
- Cumplir las políticas de seguridad en todas las redes informáticas.

2.2.4 Unidad de Soporte Técnico y Mantenimiento

- Cumplir políticas de utilización de equipos informáticos.
- Reparación y mantenimiento de equipos informáticos.
- Mantener en perfecto funcionamiento los equipos de computación, en lo referente a Hardware y Software.
- Mantener actualizado el software, las aplicaciones clientes de los sistemas administrativos.
- Gestionar las incidencias, por medio través de HELP DESK.
- Brindar asesoramiento técnico informático a los funcionarios.

2.2.5 Servicios de la Unidad de TIC

Administración de Redes y Datos:

- Administración de redes e infraestructura.
- Seguridades de información.

Mantenimiento y Soporte a Usuarios:

- Soporte técnico.
- Adquisición de equipos y servicios informáticos

2.3 Método de investigación

La evaluación de los procesos se realiza utilizando el método descriptivo, con la descripción de los procesos donde intervienen personas y recursos de tecnología en la Gestión de TI es de alta relevancia para el correcto funcionamiento del CRSVE. Para contener las principales falencias que puedan comprometer seriamente a este organismo se ejecutó la metodología de investigación denominada ABR Auditoría Basada en Riesgos.

La herramienta que se utilizó fue el marco de referencia COBIT versión 5 cuyas directrices y procedimientos de control fueron necesarios para evaluar el gobierno y la gestión de los sistemas de información y comunicación. Las métricas de control de cada proceso fueron fundamentales para determinar el nivel de madurez. Las actividades detalladas claramente en el marco de trabajo fueron guías que hacer cambios y mejorar cada proceso.

La mecánica para evaluar los procesos de Gestión de T.I. será la guía de Autoevaluación y el instructivo del Modelo de Procesos de Evaluación (PAM) de COBIT versión 5.

El modelo de evaluación PAM es una guía bidimensional para calificar el nivel de capacidad del proceso:

- Medición de los procesos.
- Medición de capacidad.

Los atributos proporcionan las métricas auditables de los procesos.

Ilustración 13: Modelo de Evaluación, COBIT 5 PAM



Fuente: (Pedroza, 2014)

2.3.1 Métodos y Técnicas

Las técnicas para recopilación de información utilizadas fueron las siguientes:

Observación: Con esta técnica se logró constatar la mecánica de los procesos en la Unidad de TIC, flujo de la información institucional, documentación relevante, con la finalidad de determinar la fidelidad de los datos.

Entrevista: Especialmente dirigida a los encargados de los departamentos de TIC de la institución a fin de aportar datos importantes a la investigación, actividades, procedimientos de soporte, levantamiento de información y demás aspectos útiles para el desarrollo de la evaluación de la infraestructura tecnológica.

2.4 Población y muestra

La población para este estudio estuvo dado por funcionarios que desarrollan cargos administrativos, e intervienen en la administración de la infraestructura tecnológica del CRSVE, quienes fueron un total de 2 personas: el responsable tecnológico del CRSVE y el responsable tecnológico de la Coordinación Zonal 1.

2.5 Técnicas de procesamiento y análisis estadístico de datos empleados

Para efectuar la recopilación de información se realizó cuestionarios dirigidos principalmente a los encargados de los departamentos de TIC por medio de, cuestionario, y fichas de observación para toda la información de la cual se tenga constancia de elementos importantes para el desarrollo del trabajo investigativo.

Se desarrolló cuestionarios para la aplicación de entrevistas y encuestas con el fin de lograr un mejor análisis de la información recopilada.

CAPITULO III

3. Resultados

3.1 Análisis e interpretación de los resultados

3.1.1 Identificación de los objetivos de la unidad de TIC del CRSVE (MJDHC).

Con base en el Plan Estratégico de la Dirección de TIC, a continuación, se listan los objetivos a ser identificados.

Tabla 7: Objetivos de la Unidad de TIC del CRSVE

ID	DETALLE
OBJ1	Implementar redes de área local en los predios de los centros.
OBJ2	Implementar infraestructura para el sistema de visitas a personas privadas de la libertad (ppl).
OBJ3	Adquirir equipos de video vigilancia y videoconferencias para los centros.
OBJ4	Adquirir sistemas de seguridad electrónicos, para seguridad de los centros.
OBJ5	Adquirir equipamiento informático de última generación para usuarios finales de la institución..
OBJ6	Brindar un soporte técnico rápido y adecuado.
OBJ7	Mantener el parque informático en óptimas condiciones.
OBJ8	Mantener capacitado a los funcionarios en el manejo de las TIC.
OBJ9	Mantener levantados los servicios de TIC dado por el proveedor.

3.1.2 Identificación de los procesos de la unidad de TIC del CRSVE

Considerando el estado actual de la Unidad de TIC, a continuación se listan todos los procesos que se están ejecutando actualmente para ser analizados e identificar su sensibilidad.

Tabla 8: Procesos de la Unidad de TI del CRSVE

ID	DETALLE
PROC1	Administración de Redes y telecomunicaciones
PROC2	Seguridad de la información e infraestructura tecnológica
PROC3	Administración y mantenimiento de sistemas informáticos
PROC4	Adquisición de equipos y servicios de información
PROC5	Soporte técnico

3.1.3 Identificación de los riesgos de la Unidad de TIC del CRSVE

Se identifican todos los riesgos que podrían darse para incumplir con los procesos y objetivos planeados en la Unidad de TIC

Tabla 9: Riesgos de la Unidad de TIC

ID	DETALLE
RSK1	Caída del enlace de fibra óptica.
RSK2	Retardo en el soporte técnico a los funcionarios de los centros.
RSK3	Uso no adecuado de los sistemas informáticos por parte de los funcionarios
RSK4	Caída del servicio de intranet.
RSK5	Caída del servicio de correo institucional.
RSK6	Caída del servicio de telefonía.
RSK7	Daño del switch principal.
RSK8	Daño de otro hardware.
RSK9	Falta de presupuesto para la ejecución de proyectos.

3.1.4 Ejecución de la auditoria basada en riesgos

3.1.4.1 Matriz Objetivos -Procesos

Esta tabla muestra los procesos necesarios para cumplir cada uno de los objetivos planteados por la Unidad de Tecnología.

Tabla 10: Matriz Objetivos y Procesos

OBJ/PROC	PROC1	PROC2	PROC3	PROC4	PROC5
OBJ1	X	X			
OBJ2	X	X		X	
OBJ3	X	X		X	
OBJ4	X	X		X	
OBJ5		X		X	
OBJ6		X	X		X
OBJ7		X			X
OBJ8		X			
OBJ9		X			

3.1.4.2 Matriz Objetivos - Riesgos

Mediante la relación entre los riesgos identificados y los objetivos definidos por la Unidad de TIC, se podrá identificar cuáles son los objetivos de más alto cumplimiento.

Tabla 11: Matriz Objetivos y Riesgos

OBJ/RSK	RSK1	RSK2	RSK3	RSK4	RSK5	RSK6	RSK7	RSK8	RSK9
OBJ1	X								
OBJ2	X								
OBJ3									X
OBJ4									X
OBJ5									X
OBJ6		X							
OBJ7		X					X		
OBJ8			X						
OBJ9				X	X	X			

3.1.4.3 Matriz de Análisis de Riesgos

La finalidad es poder evaluar que tan sensibles son los riesgos identificados por la Unidad de TIC, la escala utilizada para medir el nivel de riesgo es:

MA(Muy Alto) A (Alto) M (Medio) B (Bajo)

Tabla 12: Riesgos e Impactos

RIESGOS		IMPACTO	PROBABILIDAD	NIVEL RIESGO
RSK1	Caída del enlace de fibra óptica.	3	2	M
RSK2	Retardo en el soporte técnico a los funcionarios de los centros.	3	3	A
RSK3	Uso no adecuado de los sistemas informáticos por parte de los funcionarios	2	3	M
RSK4	Caída del servicio de intranet.	3	2	M
RSK5	Caída del servicio de correo institucional.	3	2	M
RSK6	Caída del servicio de telefonía.	2	2	B
RSK7	Daño del switch principal.	5	1	A
RSK8	Daño de otro hardware.	5	1	A
RSK9	Falta de presupuesto para la ejecución de proyectos.	5	3	A

3.1.4.4 Matriz de análisis de Proceso-Riesgo

Esta matriz permitirá identificar cuáles son los procesos más sensibles que tiene la Unidad de Tecnología.

Tabla 13: Matriz Procesos Riesgos

PROC/ RIESGOS	RSK 1	RSK 2	RSK 3	RSK 4	RSK 5	RSK 6	RSK 7	RSK 8	RSK 9	P	S
PROC1	P	S	S	S	S	S	S	P	S	2	7
PROC2	P	P	P	P	P	S	P	P	S	7	2
PROC3	P	S	S	P	P	S	P	P	S	5	4
PROC4	S	S	S	S	S	S	S	S	P	1	8
PROC5	S	P	P	S	S	S	S	S	S	2	7

P: Correlación principal "el riesgo afecta directamente con el proceso"

S: Correlación secundaria "el riesgo no afecta de manera significativa al proceso"

De acuerdo con la tabla No. 13, se identifica que el proceso:

P2: Seguridad de información e infraestructura del CRSVE

Es el más sensitivo dentro de la Unidad de TIC, esto implica que la evaluación se realizará sobre estos procesos.

3.1.4.5 Matriz de procesos sensitivos y procesos de evaluación COBIT5

Una vez que ya se tienen identificados los procesos sensitivos de la Unidad de Tecnología, el siguiente paso que se requiere es realizar un mapeo contra los procesos de COBIT 5 para definir el alcance de la evaluación a realizar.

Tabla 14: Procesos de COBIT y Procesos Unidad de TIC

PROCESOS DE TI/PROCESOS DE COBIT	PROC-APO07	PROC-APO09	PROC-APO12	PROC-APO13	PROC-BAI09	PROC-DSS01	PROC-DSS02	PROC-DSS03	PROC-DSS04	PROC-DSS05	PROC-DSS06	PROC-MEA02
PROC2		x	x	x	x		x		x	x		x

3.1.5 Alcance de la evaluación

De acuerdo con el resultado obtenido en la Matriz de Análisis de Procesos y Riesgos (Tabla No. 13), los alcances para la evaluación de los procesos críticos de la Dirección de Tecnología son:

P2->Seguridad de información e infraestructura del CRSVE que contiene los subprocesos siguientes:

- PROC-**APO-09** Gestionar los acuerdos de servicio.
- PROC-**APO-12** Gestionar el riesgo.
- PROC-**APO-13** Gestionar la seguridad.
- PROC-**BAI-09** Gestionar los activos.
- PROC-**DSS-02** Gestionar los incidentes de servicio.
- PROC-**DSS-04** Gestionar la continuidad.
- PROC-**DSS-05** Gestionar los servicios de seguridad.
- PROC-**MEA-02** Supervisar, monitorear y valorar el sistema de control interno.

3.1.6 Objetivos de control de la evaluación

Los pasos por seguir para realizar la evaluación a los procesos mencionados se detallan a continuación (se consideró el Modelo de Evaluación de Procesos "PAM" de COBIT 5):

- Cuestionarios a las personas encargadas de la Unidad de TIC y Zonal, de acuerdo a las Metas de cada Proceso de COBIT 5.
- Calificación de las Metas de cada Proceso de COBIT (si se realizaron más de dos preguntas por cada meta, se debe considerar la MEDIA de la calificación obtenida), a continuación, se detalla la siguiente tabla de calificación a ser utilizada.

- Llenar la tabla de Valoración del Nivel de Madurez de los procesos de COBIT 5. (ver Anexos)
- Llenar la tabla de Nivel de Madurez Obtenido COBIT 5.
- Evidenciar el nivel de madurez de acuerdo con el resultado obtenido en la evaluación realizada a los procesos de COBIT 5 seleccionados (resultados de los valores coloreados) (Ver Anexos).

La finalidad de la evaluación es obtener el nivel de madurez (NM) de la institución aplicando el estándar COBIT 5, con el cual se determina la capacidad de gestión de los procesos T.I. realizados en el CRSVE.

La descripción de estos procesos, se lleva a cabo mediante recopilación de información con base a documentación institucional, normativas, y entrevistas con los encargados de tecnología de la Coordinación Zonal y Unidad de TIC.

Para la selección de los procesos de gestión de T.I, se identifican los procesos de Cobit como muestra la Tabla 14.

CAPÍTULO IV

4. Propuesta

4.1 Evaluación de la infraestructura tecnológica

4.1.1 Descripción de la infraestructura tecnológica actual del CRSVE

El área de Redes y Comunicaciones, todo lo relacionado con la infraestructura de redes, esto es, racks, switches, routers, enlaces, seguridad informática, y demás componentes de red, asi como también la gestión de infocentros, su espacio físico, puntos eléctricos, conectividad, UPS, sistema de ventilación o aire acondicionado, etc.

Mediante la Unidad de TIC del CRSVE, se maneja todos los componentes que brinda los servicios de tecnología que se consideran como infraestructura, y ésta está conformada por los siguientes elementos:

Rack de enlace principal:

- 2 switch (24 y 16 puertos)
- 1 router
- Enlace de fibra óptica

Rack de enlace secundario:

- 1 switch (24 puertos)

Cableado de red:

- 40 puertos de datos
- 10 puertos de voz

Hardware:

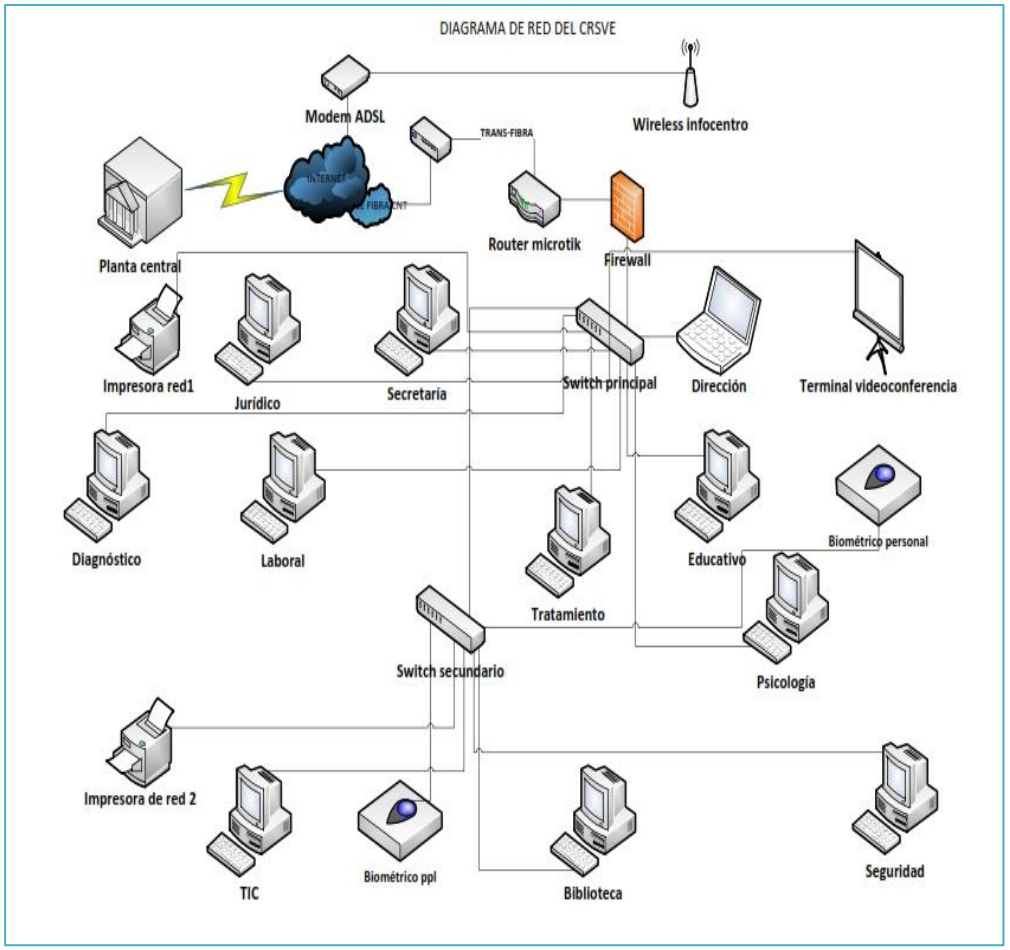
- 25 computadoras en área administrativa
- 3 impresoras Láser Multifunción
- 1 terminal de videoconferencia
- 2 equipos biométricos para control de asistencia
- 1 infocentro (MINTEL)

- 2 computadoras en áreas de seguridad y vigilancia
- 25 UPS

Software (Servidores en Planta Central-Quito):

- Sistema de Visitas
- Sistema de Gestión Penitenciaria
- Videoconferencia
- Módulo de Gestión de Incidencias
- Correo Institucional
- Gestión Documental

Ilustración 14: Diagrama de red del CRSVE



4.1.2 (Guía de Auditoria) Evaluación del proceso seguridad de información e infraestructura

De acuerdo con el resultado obtenido en la Matriz Procesos de COBIT 5 y Procesos de la Unidad de TIC, los procesos a ser evaluados son:

- PROC-**APO-09** Gestionar los acuerdos de servicio.
- PROC-**APO-12** Gestionar el riesgo.
- PROC-**APO-13** Gestionar la seguridad.
- PROC-**BAI-09** Gestionar los activos.
- PROC-**DSS-02** Gestionar peticiones e incidentes de servicio.
- PROC-**DSS-04** Gestionar la continuidad.
- PROC-**DSS-05** Gestionar los servicios de seguridad.
- PROC-**MEA-02** Supervisar, monitorear y valorar el sistema.

4.1.2.1 Proceso COBIT: PROC-APO09 Gestionar los acuerdos de servicio

Cuestionario de preguntas relacionado a las metas del proceso PROC-APO09 para su evaluación.

Tabla 15: Cuestionario de Preguntas PROC-APO09

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-APO09-01	¿Cuál es la proporción de requerimientos de TIC asumidos por los SLA?	3/5	3.5/5	No hay documento.
2	PROC-APO09-01	¿Cuál es la proporción de funcionarios satisfechos porque TIC cumple con los niveles de servicio acordados?	4/5		Registro de solicitudes
3	PROC-APO09-02	¿La proporción de incidentes que no cumplen el nivel de servicio acordado es baja?	5/5	5/5	Registro de solicitudes
4	PROC-APO09-03	¿Cuál es la proporción de requerimientos de TIC que están monitoreados para cumplir los niveles de servicio?	3/5	3/5	Registro de solicitudes
5	PROC-APO09-03	¿Cuál es la proporción de requerimientos de TIC que alcanzan el objetivo de cumplimientos de los niveles de servicio?	4/5		Registro de solicitudes

Alinear los servicios T.I. y los niveles de servicios con los requerimientos institucionales, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios T.I, niveles de servicio e indicadores de rendimiento. (COBIT 5, 2012)

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 16: Nivel de Madurez Obtenido PROC-APO09

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5
PROC-APO09		PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1
Criterio		SL	ML	ML	BL	BL			
Nivel de Madurez				2					

El resultado de evaluación del proceso es "2" que tiene nivel de madurez "gestionado".

4.1.2.2 Proceso COBIT: PROC-APO12 Gestionar el riesgo

Cuestionario de preguntas relacionado a las metas del proceso PROC-APO12 para su evaluación.

Tabla 17: Cuestionario de Preguntas PROC-APO12

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-APO12-01	¿Existe algún proceso para análisis y evaluación de TIC?	4/5	4.5/5	Instructivo Riesgos Informática, Documento de Procesos y Objetivos de B
2	PROC-APO12-01	¿Realizan procesos de control en la Unidad de Tecnología?	5/5		Evaluaciones de la Dirección de auditoría interna y Contraloría.
3	PROC-APO12-02	¿Existe alguna matriz de riesgos donde están identificados los riesgos sensitivos de TIC?	5/5	5/5	Instructivo Riesgos de Informática
4	PROC-APO12-03	¿Existe algún banco de datos donde registran incidentes significativos no identificados para registrar en la matriz de riesgos?	3/5	3.5/5	Instructivo Riesgos de Informática
5	PROC-APO12-03	¿Cuál es la proporción de acciones ejecutadas para minimizar los riesgos?	4/5		Instructivo Riesgos de Informática
6	PROC-APO12-04	¿Cuál es la proporción de acciones definidas para minimizar los riesgos?	5/5		Instructivo Riesgos de Informática

Identificar, evaluar y reducir los riesgos relacionados con T.I. de manera continua, dentro de niveles de tolerancia establecidos por la Dirección Nacional de TIC (COBIT 5, 2012).

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 4), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 18: Nivel de Madurez Obtenido PROC-APO12

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-APO12		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		SL	SL	SL	SL	SL	ML	ML	BL	BL
Nivel de Madurez								4		

El resultado de evaluación del proceso es “4” que tiene nivel de madurez “predecible”.

4.1.2.1 Proceso COBIT: PROC-APO13 Gestionar la seguridad

Cuestionario de preguntas relacionado a las metas del proceso PROC-APO13 para su evaluación.

Tabla 19: Cuestionario de Preguntas PROC-APO13

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-APO13-01	¿El personal encargado de administrar la seguridad de la información es el adecuado?	5/5	5/5	Documento de Roles y funciones de TIC
2	PROC-APO13-01	¿La cantidad de incidentes relacionados con la seguridad es baja?	5/5		Registro de solicitudes.
3	PROC-APO13-02	¿Cuál es el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la institución?	5/5	5/5	No hay documento.
4	PROC-APO13-02	¿Las soluciones de seguridad que se desvían del plan es mínimo?	5/5		Registro de solicitudes de servicio e incidentes.
5	PROC-APO13-03	¿La cantidad de incidentes de seguridad causados por prescindir del plan de seguridad es baja?	5/5	4.5/5	Registro de solicitudes de servicio e incidentes.
6	PROC-APO13-03	¿La cantidad de soluciones desarrolladas con alineamiento al plan de seguridad es alta?	4/5		No hay documento.

Definir, operar y supervisar un sistema para la gestión de la seguridad de la información institucional (COBIT 5, 2012).

Con base en la calificación obtenida sobre el cuestionario se procede a llenar la tabla de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 5), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 20: Nivel de Madurez Obtenido PROC-APO13

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-APO13		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		SL	SL	SL	SL	SL	SL	ML	BL	BL
Nivel de Madurez								4		

El resultado de evaluación del proceso es “4” que tiene nivel de madurez “predecible”.

4.1.2.2 Proceso COBIT: PROC-BAI09 Gestionar los activos

Cuestionario de preguntas relacionado a las metas del proceso PROC-BAI09 para su evaluación.

Tabla 21: Cuestionario de Preguntas PROC-BAI09

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-BAI09-01	¿Existe algún control para identificar el número de licencias?	5/5	3.7/5	Registro uso de licencias
2	PROC-BAI09-01	¿Existe algún control para identificar el número de equipos no utilizados?	5/5		Acta de control de activos
3	PROC-BAI09-01	¿Existe algún proceso para realizar un estudio financiero?	1/5		Acta de control de activos
4	PROC-BAI09-02	¿Existe algún control para identificar el número de equipos obsoletos?	5/5	4.7/5	Documento POA
5	PROC-BAI09-02	¿Existe algún proceso de auditoría respecto a la información financiera de TIC?	5/5		Documentos de proyectos
6	PROC-BAI09-02	¿Cuál es la proporción de servicios TIC con costo /beneficio?	4/5		No hay documento

Gestionar los activos de TI de manera orgánica para asegurar que su uso aporta valor optimizando recursos, que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio sean confiables y estén disponibles (COBIT 5, 2012).

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 6), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 22: Nivel de Madurez Obtenido PROC-BAI09

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-BAI09		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		SL	SL	SL	SL	SL	ML	ML	BL	BL
Nivel de Madurez								4		

El resultado de evaluación del proceso es "4" que tiene nivel de madurez "predecible".

4.1.2.3 Proceso COBIT: PROC-DSS02 Gestionar peticiones e incidentes de servicio

Tabla 23: Cuestionario de Preguntas PROC-DSS02

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-DSS02-01	¿La proporción de incidentes que interrumpen procesos claves institucionales es baja?	4/5	4/5	Registro de solicitudes de servicio e incidentes
2	PROC-DSS02-02	¿La proporción de incidentes resueltos dentro de un periodo acordado es aceptable?	5/5	5/5	Registro de solicitudes de servicio e incidentes
3	PROC-DSS02-03	¿El nivel de satisfacción del usuario con la resolución de las peticiones de servicio es alto?	4/5	3.5/5	Registro de solicitudes de servicio e incidentes
4	PROC-DSS02-04	¿Las soluciones de servicio se solventan según los niveles de servicio acordados?	3/5		Registro de solicitudes de servicio e incidentes

Brindar una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes (COBIT 5, 2012).

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 7), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 24: Nivel de Madurez Obtenido PROC-DSS02

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-DSS02		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		SL	ML	ML	ML	ML	BL			
Nivel de Madurez						3				

El resultado de evaluación del proceso es "3" que tiene nivel de madurez "establecido".

4.1.2.4 Proceso COBIT: PROC-DSS04 Gestionar la continuidad

Cuestionario de preguntas relacionado a las metas del proceso PROC-DSS04 para su evaluación.

Tabla 25: Cuestionario de Preguntas PROC-DSS04

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-DSS04-01	¿Existe un Plan de Continuidad del Negocio?	5/5	5/5	Plan de Continuidad del Negocio.
2	PROC-DSS04-02	¿Qué proporción de sistemas claves para la institución no están cubiertos por un plan de control?	5/5	5/5	Plan de Continuidad del Negocio.
3	PROC-DSS04-03	¿Qué proporción de ejercicios y pruebas realizados para evaluar el plan?	2/5	2/5	Reportes internos
4	PROC-DSS04-04	¿Existe algún proceso de actualización al plan y cuál es su porcentaje de mejoras realizadas?	1/5	1/5	No hay documentos
5	PROC-DSS04-05	¿Cuál es la proporción de interesados internos y externos que tienen conocimiento respecto al plan?	3/5	3.5/5	Reportes internos
6	PROC-DSS04-05	¿Cuál es la proporción de asuntos tratados subsecuentemente en los materiales de información?	4/5		Plan de Continuidad del Negocio.

Establecer y mantener un plan para permitir a la organización y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para la institución y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel institucional aceptable (COBIT 5, 2012).

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 8), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 26: Nivel de Madurez Obtenido

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-DSS04		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		ML	ML	ML	ML	ML	BL	BL		
Nivel de Madurez						3				

El resultado de evaluación del proceso es "3" que tiene nivel de madurez "establecido".

4.1.2.5 Proceso COBIT: PROC-DSS05 Gestionar los servicios de seguridad

Tabla 27: Cuestionario de Preguntas PROC-DSS05

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-DSS05-01	¿La proporción de riesgos de seguridad en las redes de datos y comunicaciones es baja?	5/5	5/5	Login de equipos de red.
2	PROC-DSS05-01	¿La proporción de riesgos encontrados en los equipos de seguridad firewalls, IPS, servidores de antivirus, filtros de páginas web, etc., es baja?	5/5		Login de equipos de seguridad.
3	PROC-DSS05-02	¿Cuál es la proporción de funcionarios que reciben capacitación del uso adecuado de los equipos informáticos?	5/5	5/5	Reportes internos.
4	PROC-DSS05-02	¿La proporción de dispositivos terminales (celulares, laptos personales, tablets) sin autorización conectados a la red es baja?	5/5		Login de equipos de red.
5	PROC-DSS05-03	¿Cuál es la proporción de funcionarios que están identificados de manera única, tienen su cuenta de dominio y tienen permisos de acuerdo con sus cargos institucionales?	5/5	5/5	Login de servidores de dominio.
6	PROC-DSS05-04	¿Realizan pruebas eventualmente de los dispositivos de seguridad para analizar su correcto funcionamiento?	3/5	3/5	No hay documento.
7	PROC-DSS05-05	¿La cantidad de incidentes relacionados con permisos no autorizados a la información es baja?	5/5	5/5	Login de equipos de seguridad.

Proteger la información institucional para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con las políticas de seguridad. Establecer y mantener los roles de seguridad y permisos de acceso de la información y realizar la supervisión de la seguridad (COBIT 5, 2012).

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 9), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez, a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 28: Nivel de Madurez Obtenido PROC-DSS05

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-DSS05		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		SL	SL	SL	SL	SL	ML	ML	BL	BL
Nivel de Madurez								4		

El resultado de evaluación del proceso es “4” que tiene nivel de madurez “predecible”.

4.1.2.6 Proceso COBIT: PROC-MEA02 Supervisar, evaluar y valorar el sistema

Tabla 29: Cuestionario de Preguntas PROC-MEA02

N°	METAS	PREGUNTAS	RESPUESTA	MEDIA	CONSTANCIA
1	PROC-MEA02-01	¿Los procesos, recursos e información cumplen con los requisitos del sistema de control interno?	5/5	4/5	Informe de auditoría interna.
2	PROC-MEA02-01	¿Cantidad de procesos con la seguridad de que son conformes con las metas de control interno?	3/5		Informe de auditoría interna.
3	PROC-MEA02-02	¿El aseguramiento se planea y ejecuta de forma efectiva?	5/5	5/5	Informe de auditoría interna.
4	PROC-MEA02-03	¿Nivel de aseguramiento y estándares de planificación?	4/5	4/5	No hay documento.
5	PROC-MEA02-04	¿Las falencias son identificadas y reportadas?	5/5	5/5	Informe de auditoría interna.
6	PROC-MEA02-04	¿Plazo entre la incidencia de la falencia del control y su comunicación?	5/5		No hay documento.

Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. (COBIT 5, 2012).

Con base a la calificación obtenida sobre el cuestionario se procede a llenar la tabla de Valoración del Nivel de Madurez de COBIT 5 (Ver Anexo 10), tomando en cuenta los criterios de la tabla 3.

Para finalizar el proceso de obtención del nivel de madurez a continuación, se detalla una tabla resumen de la Valoración del Nivel de Madurez obtenido, en la cual también se toma en cuenta los criterios de la tabla 3.

Tabla 30: Nivel de Madurez Obtenido PROC-MEA02

PROCESO	NIVEL 0	NIVEL 1	NIVEL 2		NIVEL 3		NIVEL 4		NIVEL 5	
PROC-MEA-02		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Criterio		SL	SL	SL	SL	SL	SL	SL	SL	ML
Nivel de Madurez										5

El resultado de evaluación del proceso es "5" que tiene nivel de madurez "optimizado".

4.1.3. Resultados de la evaluación

Los ocho procesos críticos del Departamento de Informática fueron evaluados mediante la metodología de COBIT los cuales muestran los siguientes resultados:

Evaluación Proceso Seguridad de información e infraestructura: Los procesos de COBIT 5 revisados son los siguientes:

- **PROC-APO09:** Gestionar los acuerdos de servicio.
- **PROC-APO12:** Gestionar el riesgo.
- **PROC-APO13:** Gestionar la seguridad.
- **PROC-BAI09:** Gestionar los activos.
- **PROC-DSS02:** Gestionar peticiones e incidentes de servicio.
- **PROC-DSS04:** Gestionar la continuidad.
- **PROC-DSS05:** Gestionar los servicios de seguridad.
- **PROC-MEA02**: Supervisar, evaluar y valorar el sistema de control interno.

La evaluación de los procesos de la Unidad de TIC muestra que la mayoría de los procedimientos realizados para garantizar la seguridad informática e infraestructura tecnológica están establecidos y son predecibles; la mayoría de estos procedimientos no están documentados, no se documenta acuerdos de servicios internos, no se efectúan pruebas de la gestión de la continuidad de los aplicativos de T.I.

En la siguiente tabla de resumen se encuentran los resultados de la evaluación general de los procesos de COBIT realizada:

Ilustración 15: Evaluación proceso seguridad de información e infraestructura

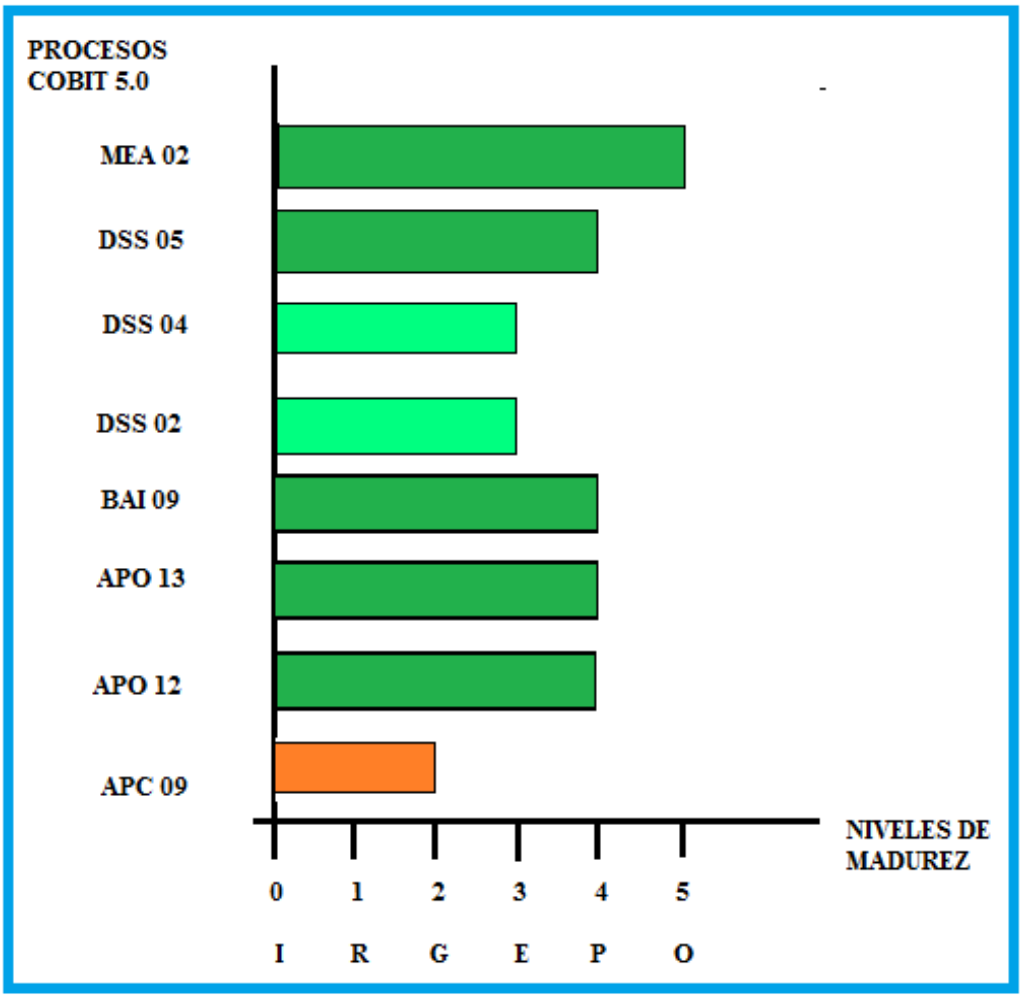


Tabla 31: Resumen de Evaluación de los Procesos de COBIT

ID.PROC	N PROC	NM0	NM1	NM2	NM3	NM4	NM5	CAP. MADUREZ
ALINEAR, PLANIFICAR Y ORGANIZAR								
PROC-APO09	Gestionar los acuerdos de servicio			X				Gestionado
PROC-APO12	Gestionar el riesgo					X		Predecible
PROC-APO13	Gestionar la seguridad					X		Predecible
CONSTRUIR, ADQUIRIR E IMPLEMENTAR								
PROC-BAI09	Gestionar los activos					X		Predecible
ENTREGAR, DAR SERVICIO Y SOPORTE								
PROC-DSS02	Gestionar peticiones				X			Establecido
PROC-DSS04	Gestionar la continuidad				X			Establecido
PROC-DSS05	Gestionar servicios de seguridad					X		Predecible
SUPERVISAR, EVALUAR Y VALORAR								
PROC-MEA02	Supervisar, evaluar y valorar el control interno						X	Optimizado

4.1.4 Recomendaciones de la evaluación

4.1.4.1 Recomendaciones para el proceso seguridad de información e infraestructura

PROC-APO09:

El proceso de los acuerdos de niveles de servicios de TIC se encuentra en un nivel gestionado por el responsable de la Unidad de TIC esto quiere decir que se realiza gestión de todos los subprocesos como: identificación, especificación, diseño, publicación, y demás acuerdos de servicios TI, niveles de servicios e indicadores de rendimiento.

PROC-APO12:

El proceso de gestión del riesgo que se encarga de identificar, evaluar y reducir riesgos asociados con TIC se encuentran alineados con la institución en un nivel predecible.

PROC-APO13:

La gestión de la seguridad de TI que se encarga de operar y supervisar la seguridad de la información se encuentra en un nivel predecible.

PROC-BAI09:

La gestión de los activos de TIC se encuentra en un nivel predecible con la cual se puede garantizar el correcto funcionamiento de los procesos de adquisición de equipos, administración de licencias de software y se encuentra respaldado por la documentación respectiva.

PROC-DSS02:

La gestión de peticiones de soporte a usuarios se encuentra respaldada a un nivel institucional establecido lo que se traduce en un aceptable nivel de respuesta, registro y solución de incidentes.

PROC-DSS04:

El proceso de gestión de la continuidad está en un nivel establecido a nivel institucional, lo que permitirá responder ante eventualidades o riesgos sensitivos y garantiza la fluidez de las operaciones y disponibilidad de la información.

PROC-DSS05:

La protección de la información institucional se encuentra en un nivel de madurez predecible, lo que significa que se debe asignar los roles de seguridad y permisos de acceso y login de usuarios.

PROC-MEA02:

Se encuentra en un nivel predecible el ambiente de control y supervisión de los procesos institucionales asociados a TIC, cumpliendo con evaluaciones y auditorías internas lo que permitirá la identificación de deficiencias en el control y demás evaluaciones y procesos de los procesos.

CAPÍTULO V

5. Conclusiones y recomendaciones

5.1 Conclusiones generales

- Se realizó una revisión de conceptos relacionados a los estándares de control interno de TIC y auditoría informática para las pequeñas y medianas organizaciones, mediante la cual se reforzó el conocimiento de la Gestión y Gobierno de TIC
- La infraestructura tecnológica del CRSVE actualmente está siendo mejorada mediante la intervención del gobierno central, con la adquisición de nuevos equipos y sistemas afines a la Gestión Penitenciaria; todo esto en el marco de mejorar los procesos y actividades administrativas cotidianas de los usuarios.
- La aplicación de la guía metodológica elaborada en esta investigación y aplicada de la Unidad de TI del CRSVE, hace un mapeo de los requerimientos y vulnerabilidades de la gestión de las TI, por medio de actividades, para mejorar la planificación, gestión de riesgos, seguridades, seguimiento del cumplimiento de los objetivos de control interno de las TIC en el CRSVE.
- Se pudo ejecutar la evaluación de la infraestructura tecnológica con base a los objetivos de control interno mediante la identificación de riesgos y seguimiento de procesos de TIC con lo cual se logró obtener resultados cómo son los niveles de madurez, procesos críticos de la Gestión de TIC den el CRSVE.

5.2 Recomendaciones generales

- Las autoridades del CRSVE, deben delegar funciones al personal responsable para tratar el tema de riesgos institucionales con el afán de identificar plenamente todas las vulnerabilidades que afectan a la institución.
- Solicitar información del tema presupuestario a la parte financiera de la Coordinación Zonal, orientado a las inversiones en TIC, para ello se recomienda consultar a la parte financiera para que presente el presupuesto anual y lo que le corresponde a la inversión en infraestructura tecnológica del CRSVE.
- El personal de TIC debe recibir capacitaciones periódicas de temas de control interno y Gestión de Recursos de TI., útiles para un buen funcionamiento y acercamiento con las Normativas del MJDHC.

Referencias bibliográficas

Bibliografía

Actualidad Tecnológica. (2016). CONTROL INTERNO Y AUDITORIA INFORMÁTICA.

Andrade, D. L. (junio de 2016). *www.pucese.net.*

ARANDA. (20 de 3 de 2013). *https://es.slideshare.net.* Obtenido de https://es.slideshare.net/ArandaSoftware/memorias-webcast-17426946

Baquero, K. (2013). *www.monografias.com*. Obtenido de http://www.monografias.com/trabajos93/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas/cobit-objetivo-contro-tecnologia-informacion-y-relacionadas.shtml

Barona, F. R. (2011). *https://es.slideshare.net.* Obtenido de https://es.slideshare.net/feradaba/material-modulo-auditoria-del-c-i-completo

Carmona, M. A. (25 de 10 de 2013). *http://www.iat.es*. Obtenido de http://www.iat.es/2013/10/gestion-riesgo-clave-excelencia-empresarial-iv/

Cedeño, Y. V. (mayo de 2017). *www.pucese.net.*

CNE. (2016). *http://cne.gob.ec.* Obtenido de http://cne.gob.ec/images/d/2016/Elecciones_2017/RESOLUCI%C3%93N_PLE-CNE-4-2-3-2016.pdf

COBIT 5. (2012). *http://www.isaca.org.* Obtenido de http://www.isaca.org/cobit/pages/cobit-5-spanish.aspx

ESSA. (2017). *https://www.essa.com.co*. Obtenido de https://www.essa.com.co/site/%C2%BFQui%C3%A9nessomos/Informaci%C3%B3ncorporativa/Gobiernocorporativo.aspx

Francavilla, C. (9 de 5 de 2012). *https://es.slideshare.net.* Obtenido de https://es.slideshare.net/CarlosFrancavilla/cobit5-introduccion

G, I. L. (s.f.). *http://slideplayer.e.* Obtenido de http://slideplayer.es/slide/69898/

G., L. I. (s.f.). *http://slideplayer.es.* Obtenido de http://slideplayer.es/slide/69898/

https://www.essa.com. (s.f.). Obtenido de https://www.essa.com.co/site/

Huerta, A. E. (8 de 10 de 2016). *https://www.slideshare.net.* Obtenido de https://www.slideshare.net/epifania/iso-ec-15504-gua-de-calidad-para-el-desarrollo-del-software

ICESI. (2011). *https://www.icesi.edu.co*. Recuperado el noviembre de 2016, de https://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/viewFile/1052/1076

ISACA. (19 de junio de 2011). *https://gobiernoti.wordpress.com*. Obtenido de https://gobiernoti.wordpress.com/2011/06/19/gobierno-ti/

ISACA. (2012). *http://www.isaca.org.* Obtenido de http://www.isaca.org/cobit/pages/cobit-5-spanish.aspx

ISACA. (23 de enero de 2017). *https://www.isaca.org*. Obtenido de https://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Jara, C. S. (2012). *www.puce.edu.ec.* Obtenido de http://repositorio.puce.edu.ec/handle/22000/6367

Laguado, I. (2017). *http://slideplayer.es.* Obtenido de http://slideplayer.es/slide/69898/

Lastra Vernaza, A. (enero de 2014). *pucese.edu.ec*. Obtenido de http://repositorio.pucese.edu.ec/handle/123456789/30

Leal. (2010). *http://publicaciones.urbe.edu.* Obtenido de http://publicaciones.urbe.edu/index.php/telematique/article/view/807/1960

Mena, E. O. (19 de junio de 2015). *http://www.pbplaw.com*. Obtenido de http://www.pbplaw.com/que-es-buen-gobierno-corporativo/

Ministerio de Justicia. (2017). *http://www.justicia.gob.ec*. Obtenido de http://www.justicia.gob.ec/organigrama-del-ministerio-de-justicia-derechos-humanos-y-cultos/

NONES, R. (4 de 11 de 2014). *http://www.netmind.es*. Obtenido de http://www.netmind.es/knowledge-center/cobit-5-el-nuevo-marco-para-la-gobernanza-de-las-tic-2/

Pedroza, O. J. (4 de 9 de 2014). *http://gesegtic.blogspot.com*. Obtenido de http://gesegtic.blogspot.com/2014/09/analisis-de-madurez-y-capacidad-de.html

UTADEO. (2010). *https://revistas.utadeo.edu.co.* Obtenido de https://revistas.utadeo.edu.co/index.php/RAI/article/viewFile/24/26

Viteri, A. G. (01 de 2016). *http://ftp.eeq.com.ec.* Obtenido de http://ftp.eeq.com.ec/upload/empresas-publicas-eficientes/Cultura%20Empresarial/Augusto%20Garz%F3n%20-%20Governance%20Ecuador.pdf

Vivero, N. G. (2016). *www.pucese.edu.ec.* Esmeraldas.

ANEXOS

Anexo 1: Cuestionarios

Cuestionarios según procesos de TIC según COBIT 5	
PARTICIPANTES:	Analista tecnológico de la unidad de TIC del CRSVE
	Analista tecnológico de la Coordinación de Justicia Zonal 1
AÑO:	2017
UBICACIÓN:	Esmeraldas y Sucumbíos

No.	**PROCESO: PROC-APO-09 Gestionar los acuerdos de servicio.**
01	¿Cuál es la proporción de requerimientos de TIC asumidos por los SLA?
02	¿Cuál es la proporción de funcionarios satisfechos porque TIC cumple con los niveles de servicio acordados?
03	¿La proporción de incidentes que no cumplen el nivel de servicio acordado es baja?
04	¿Cuál es la proporción de requerimientos de TIC que están monitoreados para cumplir los niveles de servicio?
05	¿Cuál es la proporción de requerimientos de TIC que alcanzan el objetivo de cumplimientos de los niveles de servicio?
	PROCESO: PROC-APO-12 Gestionar el riesgo.
06	¿Existe algún proceso para análisis y evaluación de TIC?
07	¿Realizan procesos de control en la Unidad de Tecnología?
08	¿Existe alguna matriz de riesgos donde están identificados los riesgos sensitivos de TIC?

09	¿Existe algún banco de datos donde registran incidentes significativos no identificados para registrar en la matriz de riesgos?
10	¿Cuál es la proporción de acciones ejecutadas para minimizar los riesgos?
11	¿Cuál es la proporción de acciones definidas para minimizar los riesgos?
	PROCESO: PROC-APO-13 Gestionar la seguridad.
12	¿El personal encargado de administrar la seguridad de la información es el adecuado?
13	¿La cantidad de incidentes relacionados con la seguridad es baja?
14	¿Cuál es el nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la institución?
15	¿Las soluciones de seguridad que se desvían del plan es mínimo?
16	¿La cantidad de incidentes de seguridad causados por prescindir del plan de seguridad es baja?
17	¿La cantidad de soluciones desarrolladas con alineamiento al plan de seguridad es alta?
	PROCESO: PROC-BAI-09 Gestionar los activos.
18	¿Existe algún control para identificar el número de licencias?
19	¿Existe algún control para identificar el número de equipos no utilizados?
20	¿Existe algún proceso para realizar un estudio financiero?
21	¿Existe algún control para identificar el número de equipos obsoletos?
22	¿Existe algún proceso de auditoría respecto a la información financiera de TIC?
23	¿Cuál es la proporción de servicios TIC con costo /beneficio?
	PROCESO: PROC-DSS-02 Gestionar peticiones e incidentes de servicio.

24	¿La proporción de incidentes que interrumpen procesos claves institucionales es baja?
25	¿La proporción de incidentes resueltos dentro de un periodo acordado es aceptable?
26	¿El nivel de satisfacción del usuario con la resolución de las peticiones de servicio es alto?
27	¿Las soluciones de servicio se solventan según los niveles de servicio acordados?
	PROCESO: PROC-DSS-04 Gestionar la continuidad.
28	¿Existe un Plan de Continuidad del Negocio?
29	¿Qué proporción de sistemas claves para la institución no están cubiertos por un plan de control?
30	¿Qué proporción de ejercicios y pruebas realizados para evaluar el plan?
31	¿Existe algún proceso de actualización al plan y cuál es su porcentaje de mejoras realizadas?
32	¿Cuál es la proporción de interesados internos y externos que tienen conocimiento respecto al plan?
33	¿Cuál es la proporción de asuntos tratados subsecuentemente en los materiales de información?
	PROCESO: PROC-DSS-05 Gestionar los servicios de seguridad.
34	¿La proporción de riesgos de seguridad en las redes de datos y comunicaciones es baja?
35	¿La proporción de riesgos encontrados en los equipos de seguridad firewalls, IPS, servidores de antivirus, filtros de páginas web, etc., es baja?
36	¿Cuál es la proporción de funcionarios que reciben capacitación del uso adecuado de los equipos informáticos?
37	¿La proporción de dispositivos terminales (celulares, laptos personales, tablets) sin autorización conectados a la red es baja?
38	¿Cuál es la proporción de funcionarios que están identificados de manera única, tienen su cuenta de dominio y tienen permisos de acuerdo con sus cargos institucionales?

39	¿Realizan pruebas eventualmente de los dispositivos de seguridad para analizar su correcto funcionamiento?
40	¿La cantidad de incidentes relacionados con permisos no autorizados a la información es baja?
	PROCESO: PROC-MEA-02 Supervisar, monitorear y valorar el sistema de control interno.
41	¿Los procesos, recursos e información cumplen con los requisitos del sistema de control interno?
42	¿Cantidad de procesos con la seguridad de que son conformes con las metas de control interno?
43	¿El aseguramiento se planea y ejecuta de forma efectiva?
44	¿Nivel de aseguramiento y estándares de planificación?
45	¿Las falencias son identificadas y reportadas?
46	¿Plazo entre la incidencia de la falencia del control y su comunicación?

Anexo 2: Documentos institucionales

No.	DOCUMENTO OFICIAL
01	Portafolio de servicios, SLA, política de respaldos, informes de rankig.
02	Informe de gestión de TIC
03	Plan de contingencia.
04	Plan de mantenimiento preventivo.
05	Plan de seguridad.
06	Políticas de correo electrónico.
07	Inventario equipos informáticos.
08	Política de seguridad data center
09	Perfiles del personal de TIC
10	Plan de Continuidad del Negocio.

Anexo 3: Valoración del NM PROC-APO09

APO09	Gestionar los acuerdos de servicio					
	Meta	Asegurar que los servicios TI y los niveles de servicio cubren las necesidades.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100%)**
Nivel 0 Inexistente	**El proceso no está implementado o falla en lograr su Meta.**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 Realizado	**PA 1.1 Rendimiento del proceso**	PROC-APO09-O1 La institución puede hacer uso los servicios T.I. tal como se han definido en el catálogo.			ML	
		PROC-APO09-O2 Los SLA muestran las capacidades y requerimientos de la TI.				**SL**
		PROC-APO09-O3 Los servicios T.I. funcionan como está determinado en los acuerdos de servicio.			ML	
Nivel 2 Gestionado	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos de control del proceso son completamente identificados. b) El funcionamiento del proceso está planificado y monitoreado.			**ML**	

Continúa

Nivel	Evaluar si se obtienen los siguientes resultados	Criterio	No logrado (0-15%)	Bajamente logrado (15% - 50%)	Medianamente logrado (50% - 85%)	Suficientemente logrado (85-100%)
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos para el proceso se definen. b) Los requisitos para la documentación se definen.			ML	
Nivel 3 **Establecido**	**PA 3.1 Definición del proceso.**	a) La infraestructura necesaria y marco de trabajo para la realización de un proceso determinado se identifican como parte del proceso. b) Se determinan los métodos adecuados para el seguimiento del proceso.		BL		
	PA 3.2 Despliegue del proceso.	Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado. Los roles del personal y directivos para la realización del procedimiento están definidos, asignados y reportados.		BL		

Anexo 4: Valoración del NM PROC-APO12

APO12	Gestionar el Riesgo					
	Meta	Integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos institucional y equilibrar los costes y beneficios de gestionar riesgos institucionales relacionados con TI.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100%)**
Nivel 0 Inexistente	**El proceso no está implantado o falla en lograr su Meta**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 Realizado	**PA 1.1 Rendimiento del proceso.**	PROC-APO12-O1 El riesgo asociado con T.I. está documentado.				SL
		PROC-APO12-O2 Existe un entorno de riesgo considerado. un entorno de riesgo actual y completo.				SL
		PROC-APO12-O3 La gestión de riesgos está definida.			ML	
		PROC-APO12-O4 La gestión de riesgos están siendo ejecutada.				SL
Nivel 2 Gestionado	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos para el control del proceso se identifican. b) El funcionamiento del proceso está planificado y monitoreado.				SL

Continúa

Nivel	Evaluar si se obtienen los siguientes resultados	Criterio	No logrado (0-15%)	Bajamente logrado (15% - 50%)	Medianamente logrado (50% - 85%)	Suficientemente logrado (85-100%)
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos para los productos de trabajo del proceso se definen. b) Los requisitos para la documentación y el control de los productos de trabajo se definen.				SL
Nivel 3 Establecido	**PA 3.1 Definición del proceso.**	a) Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado. b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.				SL
	PA 3.2 Despliegue del proceso.	a) Un proceso definido es implementado basado en un seleccionado y adaptado proceso estándar. b)Roles, responsabilidades y directrices requeridas para llevar a cabo el proceso definido son asignados y comunicados				SL
Nivel 4 Predecible	**PA 4.1 Medición de procesos.**	a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos. b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.			ML	
	PA 4.2 Control de Procesos.	a) Técnicas de análisis y control son determinadas y aplicadas. b) Se establecen límites de control para el rendimiento normal del proceso.			ML	

Continúa

Nivel 5 **Optimizado**	**PA 5.1** **Innovación del** **Proceso.**	a) Objetivos de mejora de procesos se definen con los objetivos institucionales. b) Los datos adecuados se analizan para identificar las diferencias en el proceso		BL		
	PA 5.2 Proceso **Optimizado.**	a) Efecto de los cambios propuestos es evaluado con base a los objetivos de control del proceso definido. b) La aplicación de todos los cambios acordados es manejado para asegurar la ejecución de los procesos.		BL		

Anexo 5: Valoración del NM PROC-APO13

APO13	Gestionar la seguridad					
	Meta	Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la institución.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100%)**
Nivel 0 Inexistente	**El proceso no está implantado o falla en lograr su Meta.**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 Realizado	**PA 1.1 Rendimiento del proceso**	PROC-APO13-O1 Está ejecutándose un sistema que considera y trata efectivamente los requerimientos de seguridad de la información.				SL
		PROC-APO13-O2 Se ha establecido, aceptado y reportado por toda la institución.				SL
		PROC-APO13-O3 Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la institución.				SL
Nivel 2 Gestionado	PA 2.1 Gestión de rendimiento.	a) Los objetivos de control del proceso se identifican. b) El funcionamiento del proceso está planificado y monitoreado.				SL

Continúa

Nivel	Evaluar si se obtienen los siguientes resultados	Criterio	No logrado (0-15%)	Bajamente logrado (15% - 50%)	Medianamente logrado (50% -	Suficientemente logrado (85-
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos para los productos de trabajo del proceso se definen. b) Los requisitos para la documentación y el control de los Productos de trabajo se definen.				SL
Nivel 3 Establecido	**PA 3.1 Definición del proceso.**	a) Un proceso estándar es definido tanto que describe los elementos que deben ser incorporados en un proceso definido. b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.				SL
	PA 3.2 Despliegue del proceso.	a) Un proceso definido es implementado basado en un seleccionado y adaptado proceso estándar. b) Roles, responsabilidades y directrices requeridas para llevar a cabo el proceso definido son asignados y comunicados.				SL
Nivel 4 Predecible	**PA 4.1 Medición de procesos.**	a) Información sobre el proceso necesario para apoyar a los objetivos institucionales definidos relevantes son establecidos. b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.			ML	

Continúa

	PA 4.2 Control de Procesos.	a) Técnicas de análisis y control son determinada y aplicada en su caso. b) Se establecen límites de control del funcionamiento normal de proceso.			ML	
Nivel 5 **Optimizado**	**PA 5.1** **Innovación del** **Proceso.**	a) Objetivos de mejora de procesos se definen con los objetivos institucionales. b) Los datos adecuados se analizan para identificar las diferencias en el proceso		BL		
	PA 5.2 Proceso **Optimizado**	a) Efecto de los cambios propuestos es evaluado con base a los objetivos de control del proceso definido. b) La aplicación de todos los cambios acordados es manejado para asegurar la ejecución de los procesos.		BL		

Anexo 6: Valoración del NM PROC-BAI09

BAI09	Gestionar los activos					
	Meta	Contabilización de todos los activos de TI y optimización del valor proporcionado por estos activos.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100%)**
Nivel 0 Inexistente	**El proceso no está implementado o falla en lograr su Meta.**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 Realizado	**PA 1.1 Rendimiento del proceso**	BAI09-O1 Las licencias cumplen y están alineadas con las institucionales.			ML	
		BAI09-O2 Los activos se mantienen en condiciones óptimas				SL
Nivel 2 Gestionado	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos para el desempeño del proceso se identifican. b) El rendimiento del proceso está planificado y				SL
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos para los productos de trabajo del proceso se definen. b) Los requisitos para la documentación y el control de los productos de trabajo se definen.				SL

Continúa

Nivel 3 **Establecido**	**PA 3.1 Definición del proceso.**	a) Un proceso definido es implementado basado en un seleccionado y adaptado proceso estándar. b) Se determina la secuencia y la interacción del proceso estándar con otros procesos				SL
	PA 3.2 Despliegue del proceso.	a)Un proceso definido es implementado basado en un apropiadamente seleccionado y adaptado proceso estándar. b)Roles, responsabilidades y directrices requeridas para llevar a cabo el proceso definido son asignados y comunicados				SL
Nivel 4 **Predecible**	**PA 4.1 Medición de procesos.**	a) Información sobre el proceso necesario para apoyar a los objetivos institucionales son establecidos. b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.			ML	
	PA 4.2 Control de Procesos.	a) Técnicas de análisis y control son determinada y aplicada en su caso. b) Se establecen límites de control del funcionamiento normal de proceso.			ML	
Nivel 5 **Optimizado**	**PA 5.1** **Innovación del Proceso.**	a) Objetivos de mejora de procesos se definen con los objetivos institucionales. b) Los datos adecuados se analizan para identificar las diferencias en el proceso.		BL		
	PA 5.2 Proceso **Optimizado.**	a) Efecto de los cambios propuestos es evaluado con base a los objetivos de control del proceso definido. b) La aplicación de todos los cambios acordados es manejado para asegurar el rendimiento del proceso.		BL		

Anexo 7: Valoración del NM PROC-DSS02

DSS02	Gestionar Peticiones e Incidentes de Servicio					
	Meta	Lograr una mayor productividad y minimizar las interrupciones mediante la rápida resolución de consultas de usuario e incidentes.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100%)**
Nivel 0 **Inexistente**	**El proceso no está implementado o falla en lograr su Meta**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
PA 1.1 **Rendimiento del proceso**	**Nivel 1** **Realizado**	PROC-DSS02-O1 Los servicios asociados con TI están disponibles para ser utilizados.			ML	
		PROC-DSS02-O2Los incidentes son resueltos. según los niveles de servicio acordados.				SL
		PROC-DSS02-O3 Las peticiones de servicio son resueltas según los niveles de servicio acordados.			ML	
Nivel 2 **Gestionado**	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos para el desempeño del proceso se identifican. b) El rendimiento del proceso está planificado y			ML	
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos para los productos de trabajo del proceso se definen. b) Los requisitos para la documentación y el control de los productos de trabajo se definen.			ML	

Continúa

Nivel 3 **Establecido**	**PA 3.1 Definición del proceso.**	a) Un proceso definido es implementado y basado en un apropiadamente seleccionado y adaptado proceso estándar. b) Se determina la secuencia y la interacción del proceso estándar con otros procesos. .			ML	
	PA 3.2 **Despliegue del proceso.**	a) Un proceso definido es implementado y basado en un apropiadamente seleccionado y adaptado proceso estándar. b) Roles, responsabilidades y directrices requeridas para llevar a cabo el proceso definido son asignados y comunicados.			ML	
Nivel 4 **Predecible**	**PA 4.1 Medición de procesos.**	a) Información sobre el proceso necesario para apoyar a los objetivos empresariales definidos relevantes son establecidos. b) Objetivos de medición de proceso son derivado de las necesidades de información de proceso.		BL		
	PA 4.2 Control de Procesos.	a) Técnicas de análisis y control son determinada y aplicada en su caso. b) Se establecen límites de control de la variación para el funcionamiento normal de proceso.		BL		

Anexo 8: Valoración del NM PROC-DSS04

DSS04	Gestionar la Continuidad					
	Meta	Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100 %)**
Nivel 0 Inexistente	**El proceso no está implementado o falla en lograr su Meta.**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 Realizado	**PA 1.1 Rendimiento del proceso.**	PROC-DSS04-O1 La información crítica está disponible para la institución.				SL
		PROC-DSS04-O2 Los servicios críticos tienen suficiente resistencia.				SL
		PROC-DSS04-O3 Las pruebas de continuidad del servicio han constatado la efectividad del plan.		BL		
		PROC-DSS04-O4 Un plan de continuidad actualizado refleja las necesidades institucionales actuales.	NL			
		PROC-DSS04-O5 Las partes interesadas han sido formadas en el plan de continuidad.			ML	
Nivel 2 Gestionado	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos para el desempeño del proceso se identifican. b)El rendimiento del proceso está planificado y monitoreado.			ML	

Continúa

Nivel	Evaluar si se obtienen los siguientes resultados	Criterio	No logrado (0-15%)	Bajamente logrado (15% - 50%)	Medianamente logrado (50% - 85%)	Suficientemente logrado (85-100%)
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos para los productos de trabajo del proceso se definen. b) Los requisitos para la documentación y el control de los productos de trabajo se definen.			ML	
Nivel 3 **Establecido**	**PA 3.1** **Definición del proceso.**	a) Un proceso definido es implementado y basado en un adaptado proceso estándar. b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.			ML	
	PA 3.2 **Despliegue del proceso.**	a) Un proceso definido es implementado y basado en un adaptado proceso estándar. b) Roles, responsabilidades y directrices requeridas para llevar a cabo el proceso definido son asignados y comunicados			ML	
Nivel 4 **Predecible**	**PA 4.1 Medición de procesos.**	a) Información sobre el proceso necesario para apoyar a los objetivos institucionales definidos relevantes son establecidos. b) Objetivos de medición de proceso son derivados de las necesidades de información de proceso.		BL		
	PA 4.2 Control de Procesos.	a) Técnicas de análisis y control son determinadas y aplicadas en su caso. b) Se establecen límites de control del funcionamiento normal del proceso.		BL		

Anexo 9: Valoración del NM PROC-DSS05

DSS05	Gestionar los servicios de seguridad					
	Meta	Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% -**	**Suficientemente logrado (85-**
Nivel 0 Inexistente	**El proceso no está implementado o falla en lograr**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 Realizado	**PA 1.1 Rendimiento del proceso**	PROC-DSS05-O1 La seguridad de las redes y las comunicaciones cumple con las necesidades institucionales.				SL
		PROC-DSS05-O2 La información procesada, almacenada y transmitida en los dispositivos de usuario final				SL
		PROC-DSS05-O3 Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles institucionales.				SL
		PROC-DSS05-O4 Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños mientras es procesada, almacenada.		BL		
		PROC-DSS05-O5 La información electrónica tiene las medidas de seguridad adecuadas mientras está almacenada.				SL
Nivel 2 Gestionado	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos para el desempeño del proceso se identifican. b) El rendimiento del proceso está planificado y monitoreado.				SL

Continúa

Nivel	Evaluar si se obtienen los siguientes resultados	Criterio	No logrado (0-15%)	Bajamente logrado (15% - 50%)	Medianamente logrado (50% - 85%)	Suficientemente logrado (85-100%)
Nivel 3 Establecido	**PA 2.2 Gestión del producto de trabajo.**	a) Los requisitos para los productos de trabajo del proceso se definen. b) Los requisitos para la documentación y el control de los productos de trabajo se definen.				SL
	PA 3.1 Definición del proceso.	a) Un proceso definido es implementado y basado en un apropiadamente seleccionado y adaptado proceso estándar. b) Se determina la secuencia y la interacción del proceso estándar con otros procesos.				SL
	PA 3.2 Despliegue del proceso.	a) Un proceso definido es implementado basado en un adaptado proceso estándar. b) Roles, responsabilidades y directrices requeridas para llevar a cabo el proceso definido son asignados y comunicados.				SL

Anexo 10: Valoración del NM PROC-MEA02

MEA02	Supervisar, evaluar y valorar el sistema de control interno					
	Meta	Ofrecer transparencia a las partes interesadas claves respecto de la adecuación del sistema de control interno para generar confianza en las operaciones, en el logro de los objetivos de la compañía y un entendimiento.				
Nivel	**Evaluar si se obtienen los siguientes resultados**	**Criterio**	**No logrado (0-15%)**	**Bajamente logrado (15% - 50%)**	**Medianamente logrado (50% - 85%)**	**Suficientemente logrado (85-100%)**
Nivel 0 **Inexistente**	**El proceso no está implementado o falla en lograr**	En este nivel, no se encuentra evidencia alguna o es muy escasa la ejecución del proceso.				
Nivel 1 **Realizado**	**PA 1.1** **Rendimiento del proceso.**	PROC-MEA02-O1 Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la institución.			ML	
		PROC-MEA02-02 El aseguramiento se planea y ejecuta de manera adecuada.				SL
		PROC-MEA02-03 Se brinda aseguramiento en control interno de manera efectiva.			ML	
		PROC-MEA02-04 El control interno está establecido y las deficiencias son identificadas y documentadas.				SL
Nivel 2 **Gestionado**	**PA 2.1 Gestión de rendimiento.**	a) Los objetivos del proceso se identifican. b) El proceso está planificado y monitoreado.				SL
	PA 2.2 Gestión del producto de trabajo.	a) Los requisitos del proceso se definen. b) Los requisitos para la documentación y el control se definen.				SL

Continúa

Nivel 3 **Establecido**	**PA 3.1 Definición del proceso.**	a) Un proceso es definido tanto que describe los elementos fundamentales. b) Se determina la interacción del proceso estándar con otros procesos.				SL
	PA 3.2 Despliegue del proceso.	a) Un proceso definido es implementado con base a un proceso estándar. b) Responsabilidades requeridas para llevar a cabo el proceso son asignados y comunicados.				SL
Nivel 4 **Predecible**	**PA 4.1 Medición de procesos.**	a) Información sobre el proceso necesario para apoyar a los objetivos institucionales. b) Objetivos de las métricas del proceso son derivados de los requerimientos de información de proceso.				SL
	PA 4.2 Control de Procesos.	a) Técnicas de análisis y control son determinada y aplicada en su caso. b) Se establecen límites de control del funcionamiento normal del proceso.				SL
Nivel 5 **Optimizado**	**PA 5.1 Innovación del Proceso.**	a) Objetivos de mejora de procesos se definen con los objetivos institucionales. b) Los datos adecuados se analizan para identificar las diferencias en el proceso.			ML	
	PA 5.2 Proceso Optimizado.	a) Efecto de los cambios propuestos es evaluado con base a los objetivos de control del proceso definido. b) La aplicación de todos los cambios acordados es manejado para asegurar la ejecución de los procesos.			ML	