ESCUELA POLITÉCNICA DEL EJÉRCITO

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRÍA EN GERENCIA DE SISTEMAS XI PROMOCIÓN

PROYECTO DE INVESTIGACIÓN PRESENTADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

ANÁLISIS DE SITUACIÓN INICIAL Y PLANTEAMIENTO DE PROYECTOS CON EL FIN DE MEJORAR LA GOBERNABILIDAD DE LAS TI EN EL CEC-EPN, BASÁNDOSE PARA ELLO EN LOS PRINCIPALES MANUALES DE MEJORES PRÁCTICAS PARA LAS TI

INGENIERO DANIEL ROBERTO MURILLO PÁEZ

SANGOLQUÍ, MARZO 2013

CERTIFICACIÓN

Se certifica que el trabajo titulado: "**ANÁLISIS DE SITUACIÓN INICIAL Y PLANTEAMIENTO DE PROYECTOS CON EL FIN DE MEJORAR LA GOBERNABILIDAD DE LAS TI EN EL CEC-EPN, BASÁNDOSE PARA ELLO EN LOS PRINCIPALES MANUALES DE MEJORES PRÁCTICAS PARA LAS TI**", fue desarrollado por el Ingeniero Daniel Roberto Murillo Páez, bajo mi supervisión y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

_____

Ing. Giovanni Roldán Crespo

Director del proyecto

DECLARACIÓN DE RESPONSABILIDAD

Yo, Daniel Roberto Murillo Páez

DECLARO QUE:

El proyecto de grado denominado: ”**ANÁLISIS DE SITUACIÓN INICIAL Y PLANTEAMIENTO DE PROYECTOS CON EL FIN DE MEJORAR LA GOBERNABILIDAD DE LAS TI EN EL CEC-EPN, BASÁNDOSE PARA ELLO EN LOS PRINCIPALES MANUALES DE MEJORES PRÁCTICAS PARA LAS TI**”, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros y cuyas fuentes se incorporan en la bibliografía; consecuentemente este trabajo es de mi autoría. En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, marzo 2013

_____

Ing. Daniel Roberto Murillo Páez

AUTORIZACIÓN DE PUBLICACIÓN

Yo, Daniel Roberto Murillo Páez

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo "**ANÁLISIS DE SITUACIÓN INICIAL Y PLANTEAMIENTO DE PROYECTOS CON EL FIN DE MEJORAR LA GOBERNABILIDAD DE LAS TI EN EL CEC-EPN, BASÁNDOSE PARA ELLO EN LOS PRINCIPALES MANUALES DE MEJORES PRÁCTICAS PARA LAS TI**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, marzo del 2013

_____

Ing. Daniel Murillo Páez

AGRADECIMIENTO

Agradezco el apoyo brindado por el Ingeniero Giovanni Roldán, por su tiempo, ayuda y guía brindada durante la elaboración del presente proyecto.

Adicionalmente, quiero agradecer la apertura y el apoyo de los empleados del CEC-EPN, sobremanera a la Coordinación de Gestión Tecnología por su ayuda y contribución para conseguir los resultados deseados.

Daniel Roberto Murillo Páez

DEDICATORIA

Dedico el presente proyecto y el esfuerzo realizado con mucho cariño, a mi esposa Maritza Ramírez quien supo alentarme para culminar esta tesis, aun cuando las dificultades y problemas apremiaban, siempre supo apoyarme y motivarme para lograr este logro profesional tan importante para mi carrera, por lo que sin duda la hago participe de este éxito. Gracias por siempre estar a mi lado.

Daniel Roberto Murillo Páez

INDICE DE CONTENIDO

Tabla de contenido

INDICE DE TABLAS

INDICE DE FIGURAS

PRÓLOGO

La educación continua en el Ecuador es un mercado muy competitivo, debido a las bajas barreras de entrada del mercado y la proliferación de competidores, lo que hace que el CEC-EPN, este en constante búsqueda de ventajas competitivas que le aseguren un lugar preponderante en el mercado. Uno de los principales ejes para establecer esta ventaja es la tecnología. La alta dirección consciente de su potencial, busca darle un papel más importante dentro de la estrategia de la organización y para ello es necesario alinear a la Coordinación de Gestión Tecnológica con los objetivos del negocio y hacerla mucho más eficiente. Las tecnologías de la información(TI) se han convertido en el motor que mueve las organizaciones y que en muchos casos decide la supervivencia o no de las mismas, haciendo que poco a poco sea vista ya no solo como un área de apoyo más, sino como un área estratégica dentro de las organizaciones.

El CEC-EPN consciente de esta realidad ha venido integrando a su área de tecnologías de la información (Coordinación de Gestión Tecnológica), en un principio creándola como un área formal, pues en su creación era parte de la Coordinación de Capacitación y Consultoría, y luego incluyéndola dentro de su Sistema de Gestión de Calidad, con el fin de darle una mayor importancia e irla involucrando dentro de la alta gerencia organizacional.

La Coordinación de Gestión Tecnológica no sigue ninguna norma o manual de buenas prácticas para el gobierno de TI, que rija el manejo adecuado de esta área. En una auditoría informática previa, se ha detectado algunos problemas e incluso se ha recomendado la implementación de algún tipo de mecanismo que permita mejorar el

gobierno de TI, facilitando así la dirección y control de las tecnologías de la información del CEC-EPN.

Para ello es indispensable el establecimiento de un gobierno de TI, sólido y basado en los más prestigiosos manuales de referencia o de mejores prácticas para las Tecnología de la Información, que se ajuste y apuntale los objetivos de la organización.

Este tipo de manual de mejores prácticas o manuales de referencia, hoy por hoy son aplicadas en muchas de las más prestigiosas empresas en el mundo, demostrando que no solo significan una moda sino que realmente son vistos, como verdaderas armas, en la lucha por generar organizaciones más competitivas y que generen mayores réditos.

Es muy importante mencionar, con el fin de ayudar a la definición del problema, que la solución no puede venir dada, solo por un par de correcciones que anule los problemas a corto plazo, sino más bien por una solución que permita mejorar sustancialmente el actual modelo de gobierno de las TI, permitiéndole así soportar las metas del negocio, optimizar la inversión del CEC-EPN en TI, y administrar de forma adecuada los riesgos y oportunidades asociados a las TI.

Este trabajo se orientó, primeramente a establecer la situación inicial de la Coordinación de Gestión Tecnología del CEC-EPN. Para ello se empezó determinando cuales son las actividades más críticas para la Coordinación de Gestión Tecnológica del CEC-EPN, basados en la estrategia empresarial del CEC-EPN.

Luego a estas actividades se las encajó dentro de 8 procesos pertenecientes al manual de referencia COBIT, para posteriormente proceder a verificar su cumplimiento, comparado con dicho manual. Además se analizó en que estados de madurez están cada uno de los procesos seleccionados y así establecer posteriormente cuales son las metas planteadas para los procesos antes mencionados, de cara a un mejoramiento en su gobierno de TI.

Para finalizar, se escogerá los principales lineamientos que recomiendan los principales estándares o manuales de mejores prácticas de TI y, se procederá a plantear proyectos, que en un futuro le permitan al CEC-EPN mejorar su gobierno de TI, con base en los distintos manuales de referencia o de mejores prácticas, relacionados con las Tecnologías de la Información (TI).

RESUMEN

El CEC-EPN brinda capacitación tecnológica e idiomas, apuntalado en tecnología de punta. Pero el área que administra TI en la institución es manejada de forma “empírica”, pues no se rige por ningún manual de mejores prácticas para TI, generando que no esté alineada a los objetivos institucionales de forma planificada y organizada.

La problemática identificada; se analizó las actividades más recurrentes e importantes de TI, partiendo del estudio de la cadena de valor institucional, para determinar en base a una evaluación del riesgo, las de mayor criticidad ante su potencial suceso e impacto.

A dichas actividades, se las encajó en 8 procesos de COBIT, buscando que procesos le darían mejor solución a los potenciales riesgos. Lo siguiente fue realizar una auditoría a los 8 procesos escogidos, usando para ello la guía COBIT ASSURANCE para determinar, según COBIT, en qué nivel de cumplimiento y de madurez se encuentra cada proceso en la organización. El resultado: procesos con niveles de madurez 0 y 1.

Posteriormente se planteó una meta con un modelo de madurez 2 considerando, que sin ser ambiciosa, es realista pues los procesos de planeamiento son los peor evaluados. Con las metas definidas, se hizo un compendio de lo que recomiendan estándares como ISO 27002, ITIL y COBIT para lograr su cumplimiento, y se obtuvo actividades claves, que formarán parte de un conjunto de proyectos que le permitirán al CEC-EPN implementar las mejores prácticas de TI, recogidas de los principales manuales de mejores prácticas de TI.

ABSTRACT

The CEC-EPN provides training language and technology, underpinned by technology. But the area that IT manages in the institution is managed in an "empirical" since it is not governed by a manual of best practices for IT, generating that is not aligned to the corporate objectives in a planned and organized. The problems identified, analyzed the most frequent and important activities of IT, from the study of the corporate value chain, to determine on the basis of a risk assessment, the most critical to its success and impact potential.

In these activities, they fit in 8 COBIT processes, looking for processes that would give best solution to potential risks. The next thing was to audit the 8 chosen processes, using for this ASSURANCE COBIT guide to determine, at what level of compliance and maturity each process is in the organization. The result processes maturity levels 0 and 1.

Then arose a goal with a maturity model 2 considering that without being ambitious, it is realistic because planning processes are the worst rated. With the defined goals, it became a compendium of what recommend standards like ISO 27002, ITIL and COBIT to achieve compliance, obtaining key activities that form part of a set of projects that will allow the CEC-EPN implement best IT practices, collected from leading textbooks IT best practices.

CAPITULO I

1. ANTECEDENTES

1.1. Situación Organizacional

El Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN) fue creado en 1995, con el objetivo de trabajar por el mejoramiento de la competitividad del Ecuador con acciones innovadoras. Su principal compromiso es entender los requerimientos de sus clientes e incrementar su satisfacción a través de la gestión del conocimiento, orientado al desarrollo de competencias, habilidades y destrezas.

En un inicio nació con el fin de capacitar en temas específicos a profesores de la Escuela Politécnica Nacional, pero con el tiempo ha ido extendiendo sus servicios a estudiantes, empleados del sector público, empleados del sector privado, y la comunidad en general, lo que ha llevado a convertir al CEC-EPN en “la cara visible” de la Escuela Politécnica Nacional, manteniendo una cultura de servicio al cliente, promoviendo capacitación de calidad con profesionales altamente calificados y usando tecnología avanzada.

El CEC-EPN cuenta con alrededor de 70 empleados de planta, distribuidos entre las distintas coordinaciones, además de cerca de 200 instructores contratados, de acuerdo a las necesidades de la organización. Este personal está distribuido en sus tres sedes (Veintimilla, EPN, Araucaria).

Como se puede verificar en la Figura 1 y Figura 2, desde su creación el CEC-EPN ha ido encausándose en dos principales negocios que ahora son sus dos principales **procesos productivos**, que son:

- **Capacitación y Consultoría:** Dedicado a dictar cursos tecnológicos y consultoría en ámbitos tecnológicos.

  Sus productos principales son:

  Cursos abiertos.- Dictados al público en general en horarios de lunes a jueves (7am-9am ó 5pm-7pm ó 7pm-9pm), viernes y sábado (6pm-9pm y 8am-1pm), con una duración de 32 horas en ciclos mensuales

Figura 1: Cadena de Valor

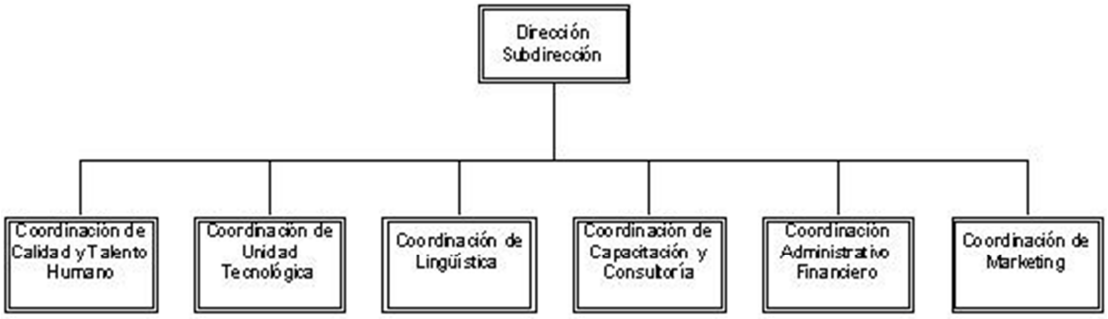

Figura 2: Diagrama Organizacional

Cursos cerrados.- Dictados por requerimiento específico de un cliente cualquiera, pudiendo dictarse en lugar y horario escogido por el cliente.

- **Lingüística:** Dedicado a dictar cursos de idiomas como: Inglés, Mandarín, Alemán y Francés.

  Su producto principal son los cursos de Inglés repartidos en 12 niveles, dictados en horarios que van desde 7 am hasta 8pm, con una duración de 80 horas en ciclos bimestrales.

Como **procesos directivos** se detallan: Dirección, que engloba la gerencia del CEC-EPN; Calidad, encargada de la administración del Sistema de Gestión de la Calidad.

Adicionalmente, en soporte a sus procesos productivos, están los **procesos de apoyo**: Tecnología, Marketing, Administrativo-Financiero, y Talento Humano.

En un intento más por mejorar su gestión, a través del cumplimiento organizado y documentado de sus actividades, y a la vez generar una ventaja competitiva, el CEC-EPN obtuvo en marzo de 2006 la certificación ISO 9001:2000(ahora 9001:2008), que abarca a todos sus procesos, tanto directivos, productivos y de apoyo. Como parte de la certificación antes mencionada, el CEC-EPN ha sido sometido, a auditorías de calidad; ordinarias que se llevan a cabo anualmente y de re-certificación que se llevan a cabo cada 3 años, con el fin de validar que se cumpla lo estipulado dentro de sus procedimientos y buscar oportunidades de mejora.

Como se refleja en la misión del CEC-EPN, uno de los ejes en los que basa su desarrollo y servicio, es la tecnología. La tecnología se ha convertido en el motor que mueve las organizaciones y que en muchos casos decide la supervivencia o no de las mismas, haciendo que poco a poco sean vistas ya no solo como un área de apoyo más, sino como un área estratégica dentro de las organizaciones.

Este cambio de mentalidad, ha venido acompañado de inversiones en el área de las tecnologías de la información (TI) y de una inclusión más importante dentro de las decisiones estratégicas de la organización, lo que ha originado que a las áreas de tecnologías de la información, se les pida resultados y se les asocie con objetivos estratégicos con el fin de medir el retorno de la inversión realizada en el área y de esta manera evaluar si el área de las tecnologías de la información(TI) es productiva.

Por ello el CEC-EPN, desde hace algunos años ha ido fortaleciendo el área de las Tecnologías de la Información, primero creándola como un área independiente y formal, en un principio era parte de la Coordinación de Capacitación y Consultoría, y luego incluyéndola dentro de su Sistema de Gestión de Calidad, con el fin de darle una mayor importancia e irla involucrando dentro de la alta gerencia organizacional.

La Coordinación de Gestión Tecnológica se ha integrado de una manera aceptable dentro del Sistema de Gestión de la Calidad que maneja el CEC-EPN, incluso su proceso ha sido sometido a auditorías de calidad, tanto ordinarías como de re-certificación, no detectándose mayores observaciones al mismo, demostrándose que es

un proceso en el que se cumple con lo que se documenta. Sin embargo la Coordinación de Gestión Tecnológica no sigue ninguna norma o manual de buenas prácticas para el gobierno de TI, que rija el manejo adecuado de esta área.

En una auditoría informática previa, se ha detectado algunos problemas e incluso se ha recomendado la implementación de algún tipo de mecanismo que permita mejorar el gobierno de TI, facilitando así la dirección y control de las tecnologías de la información del CEC-EPN.

1.2. Descripción del problema

Actualmente la Coordinación de Gestión Tecnológica del CEC-EPN, funciona en cierta forma de manera empírica, esto ha llevado a que su organización y administración no sean las más apropiadas, comparadas con los estándares internacionales que norman la dirección y control de las tecnologías de la información (TI) de una organización. La falta de formalización como se puede suponer causa incertidumbre, aumenta el riesgo y genera desorden en la administración, no solo en esta área sino en cualquier área y empresa del mundo.

TI, sin duda es un área muy compleja de manejar pues posee muchas aristas, que fácilmente podrían convertirse en áreas independientes de la empresa como son: infraestructura, desarrollo de software, soporte técnico, administración de base de datos, etc. Debido a esta complejidad, la estandarización, basada en manuales de mejores prácticas de TI, se ha hecho cada vez más común en las más importantes empresas tanto

en el ámbito público, como el privado; debido a su importancia y efectividad a la hora de orientar a los gerentes de TI a mejorar el funcionamiento de sus áreas.

Como se mencionó anteriormente la Coordinación de Gestión Tecnológica del CEC-EPN, no maneja ningún estándar o sigue algún tipo de manual de mejores prácticas de TI; que le brinde la seguridad a la alta dirección, que esta área tan crítica e importante, se maneja bajo casos de éxito que funcionaron en otras organizaciones; dictados por entes con amplios conocimientos de las TI apoyados por profesionales expertos en las distintas ramas que conforman las TI.

Como resultado del manejo actual, se han detectado muchas oportunidades de mejora en lo que respecta a la prestación de sus servicios tanto a clientes internos, como a clientes externos, tal y como lo demostró la última auditoría informática hecha a la coordinación hace un poco más de 3 años; en la que se encontraron falencias en el manejo y seguridad de la información, manejo del soporte, infraestructura, entre las más representativos.

Es muy importante mencionar, con el fin de ayudar a la definición del problema, que la solución no puede venir dada, solo por un par de correcciones que anule los problemas a corto plazo, sino más bien por una solución que permita instaurar un verdadero gobierno de TI que soporte las metas del negocio, optimice la inversión del CEC-EPN en TI, y administre de forma adecuada los riesgos y oportunidades asociados a las TI.

1.3. Justificación de la Tesis

La educación continua en el Ecuador es un mercado muy competitivo, debido a las bajas barreras de entrada del mercado y la proliferación de competidores, lo que hace que el CEC-EPN, este en constante búsqueda de ventajas competitivas que le aseguren un lugar preponderante en el mercado. Una de las principales armas para establecer esta ventaja es la tecnología.

La alta dirección consciente de su potencial, busca darle un papel más importante dentro de la estrategia de la organización y para ello es necesario alinear a la Coordinación de Gestión Tecnológica con los objetivos del negocio y hacerla mucho más eficiente.

Para esto se necesita instaurar un mecanismo que permita formar un sólido gobierno de TI, que se ajuste y apuntale los objetivos de la organización, que busque formalizar el manejo de las tecnologías de la información y permita prestar un mejor servicio a los clientes de la Coordinación de Gestión Tecnológica. Sin duda este mecanismo es la aplicación de un conjunto de "mejores prácticas" que ayuden a consolidar el gobierno de las Tecnologías de la Información (TI), a través de los más influyentes manuales y estándares de referencia.

Este tipo de manual de mejores prácticas o manuales de referencia, hoy por hoy son aplicadas en muchas de las más prestigiosas empresas en el mundo, demostrando que no solo significan una moda sino que realmente son vistos, como verdaderas armas, en la lucha por generar organizaciones más competitivas y que generen mayores réditos.

El CEC-EPN tiene un Sistema de Gestión de la Calidad consolidado, maduro, que entre otras áreas incluye a la Coordinación de Gestión Tecnológica, por lo que presenta las condiciones iníciales propicias para la implementación de un conjunto de mejores prácticas de TI en dicha coordinación, pues una de las bases para la implementación de estas mejores prácticas es que exista al menos cierto nivel de organización, con procedimientos y actividades claramente documentados y difundidos, que es precisamente lo que aporta la ISO 9001:2008

La implementación de un conjunto de mejores prácticas de TI, no es un proceso que pueda tomarse muy a la ligera, todo lo contrario es un proceso complejo, que necesita guiarse por una planificación adecuada, que necesita ser periódica y acorde a las necesidades de la organización.

Esta tesis precisamente busca plantear un conjunto de proyectos que le permitan al CEC-EPN ir implementando un conjunto de mejores prácticas de TI, de forma planificada, progresiva y ordenada, con miras a la formalización y estandarización de los procesos que envuelven a las TI.

Además será para el CEC-EPN la base en la que fundamentará la implementación formal de un estándar o manual de mejores prácticas específico para las TI como COBIT, ITIL, ISO 27000, etc.

.

CAPITULO II

2. ANÁLISIS SITUACIONAL

2.1. Análisis de actividades/procesos organizacionales críticos.

Este análisis estará basado en la cadena de valor (Figura 1) del CEC-EPN, de manera que se describirá primero rápidamente cada uno de los procesos o actividades de la misma estableciendo su relación directa con la Coordinación de Gestión Tecnológica del CEC-EPN. Luego de esta parte introductoria, se analizará cuáles son las actividades más críticas en base a la valoración del riesgo que posee cada una.

2.1.1 Descripción de procesos de la cadena de valor del CEC-EPN

Actividades de Soporte

2.1.1.1 Gestión Administrativa-Financiera

La tarea de esta área es el pago a proveedores y empleados, adquisiciones, pago a instructores, recolección de fondos, administración de la contabilidad y finanzas del CEC-EPN.

La principal tarea que desarrolla la Coordinación Tecnológica en este proceso, es el soporte técnico a aplicativos de terceros y propios del CEC-EPN y equipos informáticos, además de la eventual compra de equipos, que se usan para las distintas actividades de este proceso. La seguridad como es claro, es un tema importante para la Gestión Administrativa-Financiera, pues la información que maneja debe ser confidencial y debe ser preservada con mucha diligencia.

2.1.1.2 Gestión del Recurso Humano

La actividad en esta área se centra en la compra de equipos eventualmente, soporte a equipos informáticos a nivel de infraestructura y el soporte en temas de ofimática, que se usan para las actividades del proceso. Este proceso solo es un centro

de acopio, pues todo el proceso de reclutamiento, control de asistencia y demás lo maneja directamente la Unidad de Recursos Humanos de la Escuela Politécnica Nacional., un ente superior al CEC-EPN para el efecto.

2.1.1.3 Sistema de Gestión de la Calidad

Esta área solo la compone una persona, que se encarga de manejar todo el Sistema de Gestión de Calidad del CEC-EPN, revisando los procesos documentados, realizando correcciones, preparando auditorias parciales. Por el momento los principales esfuerzos de la Coordinación de Tecnología están dedicados a digitalizar la documentación existente, colocarla en la intranet del CEC-EPN y socializar el sistema a toda la organización.

2.1.1.4 Desarrollo Tecnológico

Para este proceso al no existir la figura de la "relación" con la Coordinación de Gestión Tecnología por obvias razones, se describirá las principales falencias que posee dicha Coordinación que forma parte del proceso de soporte *Desarrollo Tecnológico;* partiendo de algunos comentarios de la auditoría realizada a esta coordinación en tiempos anteriores. Esta descripción ayudará a que se pueda tener una idea clara de las necesidades más urgentes y tratar de mitigar los riesgos que estas originan.

Uno de los grandes problemas de la Coordinación de Gestión Tecnológica del CEC-EPN, es la poca formalización de sus actividades. Temas como la administración del soporte son manejados sin un área definida que esté a cargo de una actividad tan

crítica para el CEC-EPN. Algunos esfuerzos son sumamente informales y basados en iniciativas propias.

Otra actividad que se maneja de manera informal es el desarrollo de los proyectos tanto de software como de hardware. Cabe mencionar que esto es una constante en la organización donde no se tiene una cultura de manejar los objetivos en base a proyectos planificados y dirigidos de manera formal. En lo que respecta al software no existe definida una metodología de desarrollo de software que permita formalizar e integrar adecuadamente los distintos proyectos de desarrollo de software que posee la institución.

Una cuestión pendiente para esta Coordinación es la seguridad informática que si bien se han hecho algunos esfuerzos no se ha llegado a estar a tono con las demandas cada vez más exigente de un mundo globalizado y cada vez más involucrado con Internet.

Áreas como la Financiera, Capacitación y Lingüística manejan información confidencial que debería ser administrada bajo estándares de seguridad, aunque si bien es cierto no existe una conciencia real en la organización y alta gerencia por un manejo seguro de la información. Y con relación a todo lo antes dicho, está la inexistencia de la detección, tratamiento y mitigación de los riesgos que se producen con todo la infraestructura informática y el personal relacionado con esta área.

Un aspecto que tuvo cabida en el informe de la auditoría realizada en fechas anteriores a Tecnología fue las condiciones de la red de datos de la institución, pues se encontraron algunos oportunidades de mejorar; como el hecho que no existe una adecuada infraestructura que permita mantener estándares de calidad adecuados, además se determinó que no existía un procedimiento para medir el rendimiento de la red y por tanto no se definían acuerdo de nivel de servicio sobre todo en lo que respecta al uso del internet, tanto para el área administrativa como para el área de los laboratorios.

Actividades Principales

2.1.1.5 Investigación de Mercado

Este proceso se realiza cada vez que un curso inicia, unas veces de manera mucho más técnica y otras veces de manera informal. Anualmente se realiza un estudio de mercado que analiza las nuevas tendencias del mercado para programar los cursos del nuevo año. Además diariamente se analiza los medios de comunicación para conocer la oferta que genera la competencia y definir cuáles son los competidores directos. Estos estudios se plasman en hojas de cálculo que luego son procesadas para obtener resultados tipo gerenciales.

De manera informal se analiza los cursos que no se han vendido para programarlos luego de dos ciclos sino se abren otra vez se considera que el curso no debe ser programado otra vez.

Para este proceso, el apoyo de la Coordinación Tecnológica es netamente el soporte técnico a equipos informáticos, eventualmente compras para mejorar la infraestructura tecnológica, soporte en temas de ofimática.

2.1.1.5 Diseño y Desarrollo

Este proceso se dedica al diseño y elaboración de los pensums de estudio, metodologías, programación y demás por menores de cada uno de los cursos del CEC-EPN. En esta etapa se realiza la selección de los instructores a través de clases demostrativas que son la base de procesos de selección constantes que permiten manejar una buena base de instructores calificados.

Para este proceso el apoyo de la Coordinación Tecnológica es netamente el adquisición de equipos informáticos y soporte técnico a equipos informáticos de los funcionarios.

2.1.1.6 Publicidad y Ventas

Este proceso comienza con el diseño y ejecución de las campañas publicitarias, para luego receptar a los potenciales clientes y cristalizar la venta de los cursos.
Para este proceso el apoyo de la Coordinación de Gestión Tecnológica consiste en el desarrollo, mantenimiento y soporte de sistemas para el análisis de la publicidad y la inscripción de los participantes en los distintos cursos.

En este proceso debe notarse que existen 2 realidades totalmente distintas, mientras por un lado en Lingüística la inscripción de los participantes es crítica, pues

maneja un promedio de 5000 alumnos por ciclo, más de la mitad de este número se inscriben en los últimos 5 días lo que genera acumulaciones y molestias de los clientes, en el otro proceso productivo que es Capacitación el volumen de participantes es mucho menor sin dejar de ser importante la automatización tanto de sus preinscripciones como de las matrículas. Partiendo de esta premisa el sistema de preinscripción, matriculación y facturación (en los dos primeros casos software propio y el tercero software de terceros), necesitan de un constante desarrollo, actualización y manejo de cambios, que le permitan generar mejores ventajas a los clientes del CEC-EPN. Al momento se está promoviendo un módulo para la matriculación on-line con pagos a través de entidades bancarias, que ha marcado un rehacer de algunos módulos dentro del sistema. Obviamente con estos cambios viene la mejora de la infraestructura pues la disponibilidad es crítica para este proceso y una inversión adicional en seguridades para asegurar la confiabilidad e integridad de los datos, pues el sistema está colgado en la Internet como es de suponerse.

El soporte técnico a estos sistemas y en temas de ofimática también tiene importancia en este proceso pues son las dos áreas con más personal dentro del CEC-EPN.

2.1.1.7 Prestación y Evaluación del Servicio

Este proceso consiste en la consecución de toda la cadena de valor, en el producto final, el servicio como tal y basados en la norma ISO 9001:2008, la posterior evaluación del servicio con miras a la mejora continua.

En este proceso las áreas productivas tienen comportamientos totalmente distintos por sus respectivos giros de negocio.

Lingüística brinda sus clases sin ningún componente tecnológico, su método son las clases tradicionales. Capacitación por el contrario ocupa un gran componente tecnológico en este proceso, computadores completos, equipos de proyección, equipos de red, internet, etc; que forman parte de los 8 laboratorios que dispone el CEC-EPN con una capacidad para 250 personas. Estos laboratorios deben ser preparados para cada curso instalando software y configurando los equipos, además debe darse un mantenimiento preventivo y un soporte constante a los clientes que usan los laboratorios, durante toda la jornada laboral e incluso en horarios extendidos y los sábados.

Además Capacitación usa un sistema para la evaluación de su servicio en cada uno de sus cursos, este sistema brinda reportes gerenciales que son utilizados a nivel gerencial, marketing, ventas, etc, para la toma de decisiones y mejora del servicio.

2.1.2 Análisis de Entrevistas

Como forma de complementar la descripción hecha de las distintas actividades de la cadena de valor del CEC-EPN, se realizó entrevistas a los coordinadores[1] de los procesos que más demandan del servicio de la Coordinación de Tecnología que para el

[1] Anexo 19: Entrevistas a Coordinadores

caso son: “Publicidad y Ventas” y “Prestación y Evaluación del Servicio” para poder conocer más claramente su opinión acerca de que actividades son las más críticas en sus procesos y cuál es el papel de la Coordinación de Gestión Tecnología en ellas. Estos procesos se incluyen dentro de algunas coordinaciones como las de **Marketing, Lingüística e Intercambios de Culturales y Capacitación y Consultoría**.

Analizando las entrevistas, la **Coordinación de Marketing** según su titular, tiene muy pocas de sus actividades automatizadas y por lo tanto no cree que tenga mucha injerencia en su proceso la Coordinación de Tecnología, si bien considera importante el apoyo técnico en temas de correo electrónico, página web, etc piensa que hay muchas cosas que hacer en el ámbito tecnológico en su coordinación. El papel de Marketing por el momento está enfocado en la publicidad ya que por temas administrativos no se ha podido establecer un equipo de vendedores, por lo que las ventas corren a cargo de cada una de los procesos productivos.

En lo que respecta a la publicidad el departamento requiere de sistema informáticos que permitan procesar de mejor manera el resultado de campañas de publicidad en la receptividad del mercado.

El Coordinador de **Lingüística e Intercambios Culturales** coincide en que donde interviene de forma importante Tecnología es en el proceso de matriculación donde se han creado sistemas que incluso se integran con bancos para agilizar el

proceso de matriculación y recaudación. Además cree que otro sistema que ha logrado reducir mucho el trabajo de los empleados de su coordinación, es el sistema de notas que ahora permite que el proceso sea más ágil siendo los mismos profesores quienes en línea actualicen notas a diario lo que mejora el servicio para sus clientes. Él considera que el soporte técnico no tiene un papel muy importante luego de estas dos actividades, pero si le parece que Tecnología tiene mucho trabajo a la hora de mantener y optimizar los sistemas, pues opina que los sistemas constantemente deben irse mejorando para ayudar a los procesos a ser más eficientes.

El Coordinador de **Capacitación y Consultoría** considera preponderante la participación de Tecnología en su proceso, pues está presente en cada una de sus actividades comenzando con la configuración de los laboratorios en base a los requerimientos proporcionados por los instructores de cada curso. Esta es la actividad en la que basa el resto de la cadena del servicio. Luego con el sistema informático que apoya a la Coordinación de Capacitación en la pre-inscripción e inscripción de los participantes, que además le sirve para llevar una estadística y control de los cursos y participantes.

Y para concluir en lo que se refiere al soporte técnico a cada uno de los cursos, considera es otro de los apoyos críticos que requiere Capacitación de Tecnología pues marca la disponibilidad de los equipos, imprescindibles para la ejecución de los cursos de su coordinación.

Partiendo de la descripción realizada de cada una de los procesos y su relación con los servicios que presta la Coordinación de Gestión Tecnológica, además de las entrevistas realizadas a los Coordinadores de las áreas que más consumen los servicios de dicha coordinación, se analizarán y listarán las actividades más recurrentes, y se evaluará de una manera sencilla los riesgos que proponen cada una de estas actividades basados en la probabilidad de ocurrencia multiplicada por el impacto causado, obteniendo como resultado la severidad de cada uno de los riesgos. Luego de dicho análisis se determinan solamente las actividades más alta severidad obtuvieron para proseguir a encajarlas en los procesos de COBIT pertinentes.

Escalas de valoración

1 **Insignificante:** Es casi nula su probabilidad de aparecer, y no tiene efecto en actividades críticas relacionadas con la organización.

2 Bajo: Su probabilidad de amenaza es escaza aunque podría presentarse, su efecto podría afectar indirectamente a actividades críticas de la organización.

3 Media: Su probabilidad de amenaza es casi real, su efecto pudiera afectar a actividades como las que contribuyen a la obtención de resultados, las relacionadas con estructuras operativas complejas o con un gran número de empleados.

4 Alta: La probabilidad de ocurrencia es inminente, su efecto pudiera afectar su relación con entes reguladores, con el cliente externo, que afecten la reputación de la empresa y con actividades con volúmenes transaccionales altos.

N°	Producto	Proceso	Descripción Riesgo Relacionado	Probabilidad Amenaza	Impacto	Severidad
1	Desarrollo e implementación software.	Realización de software	No cumplir las expectativas o requerimientos del cliente	3	3	9
2	Unificación módulos o sistemas	Integración software	Sistemas o módulos no integrados adecuadamente causan problemas al negocio.	3	3	9
3	Cambios a software	Control de Cambios	Informalidad en el manejo de cambios que genere software de mala calidad.	3	3	9
4	Computadores con software instalado para c/curso	Atención Requerimientos	Mala configuración equipos, que generen problemas en el desarrollo del curso.	3	4	12
5	Mantenimiento equipos	Mantenimiento Preventivo	No ejecución de plan de mantenimiento preventivo	2	3	6
6	Equipos trabajando el mayor tiempo posible	Soporte a infraestructura	Brindar un soporte a destiempo por el volumen de requerimiento o falta de infraestructura.	2	3	6
7	Correcto uso de software de ofimática	Soporte Ofimática	Falta conocimiento básico de ofimática de personal de la institución.	2	2	4
8	Hardware de Tecnología de punta	Compra Hardware/Mejora Infraestructura	Falta de presupuesto para inversión	2	3	6
9	Compra Software acorde a los requerimientos del negocio	Compra Software	Falta de un adecuado levantamiento de requerimientos de un Sistema Informático.	3	4	12
10	Personal comprometido	Sociabilización de sistemas	Resistencia y falta de apoyo al sistema.	2	3	6
11	Documentación colocada en intranet, para facilidad del acceso	Digitalizar información	Poca planificación en todo el proceso.	2	2	4
12	Personal capacitado en uso de software	Capacitación software	Mal uso de software	3	3	9

13	Funcionamiento adecuado de software	Soporte a software propio	Falta de personal para un soporte oportuno	2	3	6
14	Funcionamiento adecuado de software	Soporte a software terceros	Soporte de mala calidad por parte del proveedor	2	4	8
15	Incluir correcciones por defectos de fabricación del software.	Optimizar /Mejorar software	Degradación de la calidad del software al hacer cambios reiterados en vez de un desarrollo planificado.	3	3	9
16	Formalización del área de soporte técnico	Planificación de TI	No crear área de soporte técnico específicamente	4	3	12
17	Control del soporte técnico	Soporte Técnico	Soporte no administrado ni monitoreado	3	3	9
18	Tratamiento de riesgos	Gestión de riesgos	No darle el tratamiento adecuado al riesgo	4	4	16
19	Generar proyectos para cubrir necesidades	Administración de proyectos	Aplicar acciones simplemente ejecutadas sin estructuración	4	3	12
20	Aseguramiento de la información proveyendo información integra, disponible y confidencial.	Seguridad Informática	Perdida de información, su integridad y confiabilidad	4	4	16
21	Definición de niveles de servicio	Soporte Técnico	Desconocimiento de usuarios acerca de la calidad que debería tener el servicio, que pudieran generar inconformidad en el cliente o directivos	3	3	9
22	Modernizar y optimizar la infraestructura de red	Redes	Degradación del servicio, poca seguridad en su acceso.	4	3	12
23	Monitorear trasferencia de datos en red datos	Redes	Encontrar problemas inesperados, con mayor dificultad para solucionarles	2	3	6
24	No definir metodología para desarrollo de software	Desarrollo Software	Desorganización, desarrollos de mala calidad, dependencia de personas	4	3	12

Tabla 1: Análisis de Actividades Recurrentes

2.2. Selección de Procesos de COBIT

En base a la Tabla 1, se resumió únicamente en las actividades cuyo valor de severidad es igual o mayor a 9 por considerar que son los riesgos más latentes y con real oportunidad de suceder. A continuación se tratará de encajar dichos productos en 8 procesos del manual de referencia COBIT.

Para ello se identificará que proceso de COBIT es el que mejor se adapta a dar una solución al riesgo y se puntuará con dos (2) puntos a dichos procesos, si la solución también puede ser dada por otro proceso pero en menor forma, a este se le asignará una puntuación de un (1) punto en cada ocurrencia del mismo en este análisis. Adicionalmente y con el fin de priorizar los procesos más críticos se adicionarán un (1) punto para los procesos cuya severidad sea igual o superior a 12.

1. **Desarrollo e implementación de software(9)**: Sin duda este producto puede encajarse en los dos procesos relacionados con software que están dentro del dominio Adquisición e Implementación:

   AI1 Identificar soluciones automatizadas: Este proceso abarca hasta el estudio de factibilidad del software a desarrollarse o comprar, que si bien es parte esencial de cualquier desarrollo excluye otras fases muy importantes.

   AI2 Adquirir y mantener software aplicativo: Este proceso se ajusta un poco más a nuestro producto pues va desde el diseño y avanza hasta la realización del software e incluso cubre la implantación del mismo.

   Sin duda el proceso donde mejor encaja este producto es AI2 Adquirir y mantener software aplicativo.

2. **Unificación módulos o sistemas (9):** Este producto está inmerso en el proceso AI2 Adquirir y mantener software aplicativo, y específicamente en el apartado AI2.6 Actualizaciones Importantes de Sistemas Existentes, que básicamente considera una programación para cambios importantes en los sistemas, en esta caso los cambios vendrían dados por añadir funcionalidad a los sistemas a través de la integración de nuevos módulos o sistemas a un nivel macro.

   Por lo tanto este producto se ajusta a AI2 Adquirir y mantener software aplicativo.

3. **Cambios a software (9):** Este producto podría incluirse en AI2 Adquirir y mantener software aplicativo que habla del mantenimiento del software a través del manejo del cambio, existe un proceso en COBIT que específicamente trata del cambio es el AI6 Administrar el Cambio.

4. **Computadores con software instalado para c/curso (12):** Este producto puede encajar dentro del proceso DS9 Administrar la Configuración que habla sobre la administración de la configuración del Hardware y Software, pero la configuración a la que se refiere es una configuración base donde se establece que debe estar instalado en cada equipo en base a argumentos legales y organizacionales con el fin de estandarizar todas las configuraciones del equipo informático. Para el caso específico de CEC-EPN aparte del área administrativa, que se acoplaría perfectamente al proceso antes mencionado, se atiende al área de laboratorios que usa software específico para cada curso aparte del software

base, que es cambiante es decir sería un requerimiento especifico por lo que se ajusta de mejor manera DS10 Administración de Problemas que sería el que organizaría la atención de requerimientos y obviamente administrado por el proceso DS8 Administrar la mesa de servicio y los incidentes.

5. **Compra Software acorde a los requerimientos del negocio (12):** La compra de software en cualquier organización basa su éxito en el levantamiento adecuado de los requerimientos y la validación de los mismos en cualquier ciclo del desarrollo. Y luego la implantación y el servicio post-venta. Todos estos aspectos los cubre AI2 Adquirir y mantener software aplicativo.

6. **Personal capacitado en uso de software (9):** Este producto es necesario para el buen manejo y aprovechamiento del software de la organización. El proceso que se ajusta a este producto es el DS7 Educar y entrenar a los usuarios, pues parte desde la determinación de la necesidad del entrenamiento hasta la evaluación del mismo. Obviamente en este caso la necesidad nace en el momento de implantación del software o un cambio sustancial sobre el mismo. Un proceso muy similar a este es AI4 Facilitar la operación y el uso que incluso integra a la alta gerencia y el desarrollo de documentos de apoyo para los usuarios, además obviamente de la transferencia de conocimiento a los usuarios finales.

7. **Incluir mejoras o correcciones por defectos de fabricación del software (9):** Se producen habitualmente por un mal levantamiento de requerimientos. Este producto podría encajar *en* AI2 Adquirir y mantener software aplicativo en su

primer literal pero con más énfasis es tratada en AI1 Identificar Soluciones Automatizadas. Además implica también ser parte de AI6 Administrar Cambios pues ayudaría mucho tener una cultura de cambios al saber que se tiende a corregir mucho el software.

8. **Formalización del área de soporte técnico (12):** Actualmente la Coordinación de Gestión Tecnológica, posee tres áreas organizativas que son: Subcoordinación de Hardware, Subcoordinación de Software y Subcoordinación de Telecomunicaciones, todas estas áreas tienen funciones específicas pero deben dedicar parte de su tiempo al soporte técnico al no existir una mesa de ayuda o área de soporte técnico que sea primer escalón hacia la solución de problemas tecnológicos. El proceso que más se adapta a este producto es el DS8 Administrar la Mesa de Servicio y los Incidentes, pues habla de la administración de la mesa de ayuda y el tratamiento de los incidentes dentro de la misma. También tiene que ver el proceso P04 Definir los Procesos, Organización y Relaciones de TI que sería la etapa de diseño o planeamiento antes de la implementación de la mesa de ayuda. Incluso PO1 Planificación Estratégica de TI podría colaborar en la fase inicial de la formalización aunque de manera indirecta.

9. **Control del soporte técnico (9)**: Como se especificó en el ítem anterior el área de soporte es informal y el soporte se brinda por todas las subcoordinaciones de Tecnología sin ningún orden.

El soporte entonces no se registra, no se administra, no se realimenta, ni se evalúa en ningún momento, pues no se definen niveles de servicio ni acuerdos de servicio.

El proceso inicial para el mejoramiento de este punto es el DS1 Definir y Administrar los Niveles de Servicio, pues acordar, documentar y monitorear todo lo que se refiere al servicio, con el cliente es la base de lo que sería un servicio de calidad. Luego obviamente el proceso angular es DS8 Administrar la Mesa de Servicio y los Incidentes que es el encargado del establecimiento y administración de la Mesa de Ayuda.

10. **Tratamiento de riesgo (16):** La Coordinación de Gestión Tecnológica no tiene una cultura de riesgo que le permita identificar sus falencias y saber contrarrestarlas a tiempo antes que se conviertan en verdaderas amenazas.

    Sin duda el proceso que más se adapta a dar solución a este producto es P09 Evaluar y Administrar los Riesgos de TI, que abarca, desde la determinación del marco del riesgo hasta el monitoreo posterior a la acción de control de riesgo. Un adecuado tratamiento del riesgo parte de la definición global de la arquitectura del área, como punto de partida del tratamiento de riesgos es decir saber que tengo, para ello el proceso que mejor se adapta es PO2 Definir la arquitectura de la información que abarca desde el diseño de la arquitectura de la información hasta el tema de tratamiento de datos o integridad.

11. **Generar proyectos para cubrir necesidades (12):** Al momento muy pocas coordinaciones llevan adelante sus pedidos a la Coordinación de Gestión

Tecnológica como un proyecto que culminara con un producto que beneficiará a sus procesos. A la interna de la Coordinación de Gestión Tecnológica los proyectos se manejan con cierta informalidad sin una metodología clara.

El proceso que se adapta a este producto es PO10 Administrar los proyectos de TI, pues permite establecer un marco de referencia para los proyectos, define una metodología para su manejo y establece una directiva para todas las fases del proyecto.

12. **Aseguramiento de la información proveyendo información integra, disponible y confidencial (16):** Las soluciones usadas no son las más actuales y los controles son mínimos.

    Un proceso que podría aplicar a este producto sería el AI3 Adquirir y mantener infraestructura tecnológica que abarca la adquisición organizada de la infraestructura tecnológica, pues mucha de la problemática en este tema se debe a una falta de actualización de la infraestructura de seguridad informática. Más sin embargo el proceso que mejor se acoplaría a este producto es DS5 Garantizar la seguridad de los sistemas, pues permite establecer un verdadero plan que busque el fortalecimiento de la seguridad informática de la organización, basado en la planeación, ejecución y medición continua de las medidas de seguridad

13. **Definición de niveles de servicio (9):** La definición de estándares mínimos de los servicios de tecnología son básicos para poder sustentar el servicio que

brinda tecnología a todos sus clientes, pues de esos estándares partirá la satisfacción o no del cliente.

El proceso que más se adapta es el DS1 Definir y administrar niveles de servicio, pues engloba todo lo que se refiere a la definición del servicio, al acuerdo con los clientes sobre niveles de servicio y al monitoreo y mejoramiento de los mismo.

14. **Modernizar y optimizar la infraestructura de red (12)**: El CEC-EPN, desde sus inicios no ha tenido como prioridad la modernización de su infraestructura, mantiene una estructura básica alejada de las nuevas tendencias tecnológicas de cierta manera, pues maneja switchs de acceso para todos los puntos de la red, y la modernización de su cableado también es una tarea pendiente, no se usan routers o swtichs capa 3 que ayuden a balancear y administrar adecuadamente la carga de datos.

Considero que algo muy importante no solo para este proceso o riesgo sino para todos en general es partir de definir un plan estratégico de la unidad, actualmente en el CEC-EPN se maneja un plan estratégico global para toda la institución obviamente los objetivos de la Coordinación de Gestión Tecnológica son demasiado macro y con el fin de obtener metas específicas de la organización pero partiendo de esos objetivos podrían irse desmenuzando para crear objetivos que no solo cumplan las metas sino que potencien la gestión de las TIC. Definiendo que se quiere, se puede tomar en cuenta cosas como remodelar la red o la plana de servidores. Para esto el proceso clave en PO1 Definir un Plan

Estratégico y de alguna manera también PO2 Definir la arquitectura de la información una vez que se tenga esto claro se puede comenzar a trabajar en cualquier mejora de cualquier aspecto de DTIC.

En menor forma en este riesgo podría verse ayudado con una definición de los riesgos de no invertir en nuevo equipamiento de red para así darle una dimensión clara al problema, esto podría obtener soporte en PO9 Evaluar y administrar los riesgos de TI.

Y finalmente el proceso que mejor calzaría para una solución puntual sería el AI3 Adquirir y mantener infraestructura tecnológica.

15. **No definir metodología para desarrollo de software (12):** La definición de una metodología de desarrollo de software hace que se estandarice las actividades que realiza un equipo de desarrolladores y da una idea clara a cualquier persona de Tecnología del proceso llevado, haciendo así que una persona en particular no sea indispensable para el éxito de un proyecto de este tipo.

    Primeramente un proceso que ayudaría mucho a clarificar la idea de del manejo de un proyecto es el proceso PO10 Administrar los proyectos de TI pues brinda el marco de referencia para el manejo de los mismos.

    Además es PO8 Administración de la Calidad: que detalla la definición de estándares para el desarrollo y la adquisición de software.

Como resumen obtendremos la siguiente tabla con los procesos más comunes dentro de este análisis:

Grupo	Proceso	Repetición
DS	(5) Garantizar la seguridad de los sistemas	**3**
AI	(3) Adquirir y mantener infraestructura tecnológica.	**5**
PO	(10) Administrar los proyectos de TI,	**5**
PO	(9) Evaluar y Administrar los Riesgos de TI	**5**
DS	(8) Administrar la Mesa de Servicio y los Incidentes	**8**
DS	(1) Definir y Administrar los Niveles de Servicio,	**3**
PO	(4) Definir los Procesos, Organización y Relaciones de TI.	**3**
AI	(1) Identificar Soluciones Automatizadas	**3**
AI	(6) Administrar Cambios	**4**
DS	(7) Educar y entrenar a los usuarios	**2**
AI	(2) Adquirir y mantener software aplicativo	**7**
DS	(9) Administrar la Configuración	**2**
PO	(1) Definir un Plan Estratégico de TI	**5**
PO	(2) Definir la Arquitectura de la información	**5**
DS	(10) Administración de Problemas	**3**
AI	(4) Facilitar la operación y el uso	**3**
PO	Administrar la Calidad	**3**

Tabla 2: Resumen Procesos COBIT seleccionados

En base a esta Tabla 2 se escogió a los procesos con mayor puntaje para usarlos como base de este proyecto de tesis, y estos son:

- **DS8 Administrar la Mesa de Servicio y los Incidentes**
- **AI2 Adquirir y mantener software aplicativo**
- **PO1 Definir un Plan Estratégico de TI**
- **AI3 Adquirir y mantener infraestructura tecnológica.**
- **PO10 Administrar los proyectos de TI**
- **PO9 Evaluar y Administrar los Riesgos de TI**
- **AI6 Administrar Cambios**
- **PO2 Definir la Arquitectura de la Información.**

2.3. Evaluación de cumplimiento siguiendo COBIT y descripción situación inicial.

La metodología a emplear para la revisión de la evaluación será el checklist sugerido en el Assurance Guide de COBIT para cada uno de los procesos que previamente se determinó que eran los más críticos para el CEC-EPN. Luego los resultados del checklist se procederán a empatar con lo que determina COBIT para establecer en qué nivel de madurez se encuentra el proceso de COBIT en el CEC-EPN. Con esta información se podrá determinar en que situación esta el proceso según COBIT y proyectar a que situación podría aspirar la Coordinación de Gestión Tecnológica y que debe hacer para estar en dicho nivel.

2.3.1 DS8 Administrar la Mesa de Servicio y los Incidentes

Siga los siguientes pasos para probar el resultado de los objetivos de control:

- **Confirme como los clientes y usuarios son informados de los estándares de soporte y examinar la existencia de estos métodos (anuncios del soporte u online, etc).**

  No existe evidencia de algún método que se haya definido para informar a los usuarios finales de los estándares de soporte. En lo que respecta a usuarios externos cuando inicia un curso de capacitación se les comenta sobre cómo se manejará el soporte, donde se almacenan los formularios de soporte, etc.

- **Confirmar la existencia de bitácoras de información de recomendaciones de usuarios.**

  En lo que respecta al soporte externo se lleva una bitácora de todas las solicitudes de soporte, las mismas solo detallan el requerimiento y la solución brindada por el personal de TI, pero no se detallan sugerencias del usuario. En lo que respecta al usuario interno no existe tampoco tales recomendaciones.

- **Pregunte acerca de la eficacia de los sistemas en términos de monitoreo y mejora del índice de satisfacción del cliente.**

  La Unidad de TI lleva un registro de control de indisponibilidad de servicios mensual, este control es analizado por el personal de TI y elabora planes de acción para mejorar la disponibilidad de los servicios.

  Anexo 13: Reporte de indisponibilidad del servicio.

  Además se realiza una encuesta anual donde se evalúa el índice de satisfacción del cliente interno.

  Anexo 14: Encuesta de satisfacción cliente interno

  En cuanto al tema de Atención a Pedidos y Sugerencias de Clientes, se lleva un indicador mensual del número de requerimientos de clientes y un indicador trimestral en el que se relacionan los números de pedidos y sugerencias de clientes con respecto al número total de estudiantes.

- **Preguntar acerca de la existencia de reportes de rendimiento del soporte.**

  En lo que respecta al soporte del cliente interno no se lleva ningún registro, por otro lado para el cliente externo se usan hojas de requerimientos que luego son consolidados en un reporte general de todos los soportes externos. En este reporte se definen datos del soporte como caso solución clasificación, etc, pero no se definen tiempo que tomo el soporte.

  Anexo 16: Reporte consolidado soporte cliente externo

- **Examinar una muestra de requerimientos en la bitácora de llamadas que no fueron solucionadas inmediatamente y determinar si los procesos de escalamiento adecuados fueron seguidos.**

  Se informó que los requerimientos no son escalados de manera formal por lo que no existe evidencia sobre los mismos. Tampoco se describen notas durante la ejecución del caso.

- **Examinar si las métricas reportadas están direccionadas a los objetivos relevantes del Soporte Técnico. Preguntar acerca de quien usa los reportes y con qué propósito.**

  Como se explicó anteriormente el soporte al cliente interno es sumamente informal por lo que no se pudo encontrar reportes de ningún tipo.

  En cuanto al tema de Atención a Pedidos y Sugerencias de Clientes externo, se lleva un indicador mensual del número de requerimientos de clientes y un indicador trimestral en el q se relacionan los números de pedidos y sugerencias de clientes con respecto al número total de estudiantes.(cliente externo). En este

caso los indicadores se muestran en la reunión mensual de coordinadores y el director con el fin de evidenciar la medición del proceso de Gestión Tecnológica. Hay que aclarar que la medición no es específicamente del soporte pues igualmente no se miden tiempo de soporte ni algo parecido, solo se mide el número de soportes brindados, cuales son los casos más recurrentes, etc.

Anexo 16: Reporte consolidado soporte cliente externo

- **Monitorear varios requerimientos de Service Desk para confirmar si existen procedimientos de atención y están siendo seguidos.**

  No se pudo confirmar la existencia de procedimientos de atención de requerimientos de soporte.

  Además se pudo evidenciar que se tienen asignadas todas las aplicaciones y sistemas y que cada uno de los integrantes de TI, tienen asignados sus roles y responsabilidades.

  Anexo 17: Asignaciones aplicaciones y sistemas de TI

- **Preguntar y confirmar que los incidentes son adecuadamente priorizados de acuerdo a políticas de prioridad.**

  No existe priorización de los requerimientos se atienden por orden de llegada simplemente o en el caso de coordinadores o el director se les da un poco de prioridad, pero de ninguna manera esto está documentado.

- **Revisar una muestra de tickets de incidentes para verificar el cumplimiento de las políticas.**

Lo más parecido a un ticket es la solicitud de soporte al cliente externo, pero no se atienden en base a ninguna política según se nos supo decir.

- **Seleccionar solicitud de ejemplo y verificar que los registros de incidentes son actualizados para mostrar la fecha y hora y la asignación de cada solicitud al personal de TI.**

  Las solicitudes no son asignadas formalmente al personal de TI y se estipulan en base a la distribución de actividades y en base a los horarios y sedes asignados a cada empleado de TI.

- **Examinar muestras de documentación de los problemas de los incidentes y confirmar que cada uno de los incidentes se estableció conforme a los niveles de prioridad definidos por las políticas.**

  Se revisa una muestra de documentos y se determina que no existe una priorización según las políticas, pues no existen definidas dichas políticas.

- **Preguntar y confirmar que los usuarios son informados del progreso de la resolución del incidente.**

  Se indicó que en ninguno de los casos se informa al usuario del estado de su solicitud, simplemente se valida cuando el problema a sido solucionado, a menos que el usuario pida información sobre el caso.

- **Pregunte y confirme que todos los registros de llamadas e incidentes son monitoreados a través de su ciclo de vida y verificar en una forma regular para garantizar una oportuna resolución de solicitudes de los clientes.**

  No se ha definido formalmente un ciclo de vida del soporte, el soporte se desarrolla en base a los requerimientos puntuales de los clientes y sin ningún procedimiento en especial.

- **Preguntar y confirmar que las peticiones e incidentes son cerrados solamente después de la confirmación del solicitante.**

  Desde el momento de la emisión del requerimiento o petición no existe retroalimentación del solicitante, por lo que tampoco cierra la petición de manera formal. A veces los requerimientos son validados con el cliente para saber si la solución brindada es la adecuada, sino simplemente el personal realiza la acción que cree conveniente y cierra la petición.

- **Examinar una muestra de incidentes y verificar que ha existido un seguimiento manual o automatizado de la resolución.**

  Los requerimientos luego de ser resueltos se plasma en el reporte consolidado de incidentes del cliente externo, donde entre otra información se define la solución que el personal de TI brindo al requerimiento.

  Anexo 16: Reporte consolidado soporte cliente externo

- **Confirme través de una inspección que los incidentes son revisados para actualizar la base de conocimientos, incluyendo soluciones, errores**

conocidos y la causa raíz para atender similares incidentes que aparezcan en un futuro. Examinar físicamente la base de conocimientos e inspeccionar una muestra de entradas para asegurar que la solución está incluida, así como la causa raíz si se conociera.

Los incidentes no se procesan para generar conocimiento, si bien en el consolidado de soportes, se puede consultar los incidentes y verificar la solución; no se especifica el problema raíz de un determinado caso. Por lo que está muy lejos de ser una base de conocimiento.

- **Examine una muestra de registros de incidentes y verificar si fueron monitoreados y realizados de acuerdo a los SLA's.**

  La unidad de TI no tiene especificado SLA's por lo que no existe monitoreo de atención de incidentes de acuerdo a SLA's.

- **Seleccione una muestra de registros y confirme con el solicitante que éstos fueron cerrados bajo su aprobación.**

  El caso es cerrado por el personal de TI que abrió el caso, el usuario final no tiene injerencia directa en el sistema.

- **Identifique si definiciones apropiadas existen para clasificar los incidentes (por ejemplo: por impacto, por urgencia).**

  No existe una clasificación para los incidentes.

- **Identifique si procedimientos para escalamiento por funcionalidad o jerarquía están definidos.**

  Se determina que no están definidos los procedimientos de escalamiento.

- **Pregunte y confirme que la administración de incidentes es claramente enlazada con planes de continuidad y contingencia.**

  No existe ninguna relación visible entre los planes de continuidad y contingencia con la administración de incidentes.

Análisis Nivel de Madurez

El proceso de soporte no está documentado ni se establece ninguna de información sobre el mismo, sobre todo lo que tiene que ver con el cliente interno, sobre el cual como se detalló durante todo este documento no existe ningún tipo de procedimiento a seguir. Si bien a nivel de cliente externo el proceso está un poco más formalizado donde al menos se tiene un formulario donde se registra el requerimiento y se le da un tipo de seguimiento posterior en el consolidado, todavía no se ha definido la integración del solicitante durante todo el requerimiento, la definición de acuerdos de servicio, etc.

Por lo que se corresponde con el nivel de madurez 1 (Inicial / Ad Hoc)

1 Inicial / Ad Hoc cuando

La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de

incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan

2.3.2 AI2 Adquirir y mantener software aplicativo

Siga los siguientes pasos para probar el resultado de los objetivos de control:

- **Revisar la documentación del diseño del proyecto para verificar que esté de acuerdo con las estrategias y normas del negocio y los planes de TI.**

  Se pudo evidenciar documentación del proyecto que fue elaborado y pertenece al Manual de Calidad del CEC. En dicho documento se ha una completa descripción inicial del proyecto.

  Anexo 4: Proyecto Sisol

- **Obtener y revisar un ejemplo de la documentación de cierre de un proyecto para determinar si han pasado por la fase de cierre de Proyecto y de control de calidad y se ha procedido con la debida autorización por parte de TI y alta dirección de la empresa (los patrocinadores del proyecto).**

  Se pudo evidenciar que existe un formulario de entrega de software donde firma el desarrollador y el cliente, este último deja constancia de que recibe el software a satisfacción.

Anexo 6: Formulario ingreso de solución.

- **Corroborar con la Gerencia de TI y con la documentación relevante para determinar si las especificaciones del diseño del proyecto de ejemplo se alinean con la dirección tecnológica y arquitectura de la información de la organización.**

  Como se explicó el diseño es casi inexistente, los sistemas están basados en las necesidades de cada una de las Coordinaciones. En lo que respecta a la arquitectura de la información, como se vio en el levantamiento de la arquitectura de la información es informal.

- **Revisar el plan de integración y los procedimientos para determinar su idoneidad.**

  No se pudo corroborar la existencia de un procedimiento documentado que detalle el proceso de integración de los sistemas. Los procesos de integridad se realizan de manera informal, en base a la decisión y juicio del equipo desarrollador.

- **Revisar la documentación del proyecto para determinar si el impacto de una nueva implementación sobre aplicaciones e infraestructuras existentes fueron evaluadas y se consideraron los métodos apropiados de integración.**

  No se logró verificar la existencia de documentación que determine el impacto de una nueva implementación. Por lo general estas nuevas implementaciones se las realiza en ambientes de prueba y luego se los implementa en producción.

- **Revisar la documentación de la fase final para confirmar que todas las actividades de desarrollo han sido controladas y que las peticiones de cambio y controles de calidad han seguido un proceso. También confirmar que los interesados han sido plenamente representados y que las evaluaciones de fin de etapa incorporan criterios de aprobación. Inspeccionar la documentación de problemas encontrados e identificar las desviaciones durante el desarrollo.**

  La documentación encontrada sobre el proceso de desarrollo solo describe la redacción del requerimiento y al terminar el documento que establece la entrega formal al cliente, que significa la aceptación del mismo.

  Anexo 7: Requerimiento Validado

- **Revisar la documentación de diseño para confirmar que las soluciones y los enfoques toman en consideración la seguridad y la disponibilidad y para determinar si los requisitos están bien definidos.**

  No se pudo evidenciar que se describa consideraciones acerca de seguridad y disponibilidad.

- **Revisar la documentación de control de calidad y los registros de fallos para asegurar que todas las excepciones de calidad que se detecten tengan medidas correctivas. Inspeccionar la documentación relevante de las evaluaciones de control de calidad, los resultados, y correcciones para**

determinar que las revisiones de control de calidad se repiten cuando es necesario.

El proceso de pruebas y control de calidad se lo realiza de manera informal, no se lleva una bitácora de los errores encontrados durante el proceso de pruebas o control de calidad.

Los errores se corrigen por los desarrolladores y se pasan a producción inmediatamente se obtiene el resultado esperado. Tampoco se tiene un proceso de control de cambios antes de la implantación.

- **Obtener y revisar las solicitudes de cambio para determinar que están clasificadas y priorizadas. Confirme con el personal que el impacto de todas las solicitudes de cambio se ha evaluado.**

  Solo se pudieron encontrar solicitudes de cambio pos-implementación, mas no durante el proceso de desarrollo del software. Las solicitudes no se encuentran priorizadas, para la entrega se necesita que la persona que solicita el cambio lo firme cuando reciba el mismo.

  Anexo 8: Solicitud de cambio

- **Revisar la documentación de control de cambio para confirmar que los cambios aplicados sin seguir el proceso de administración formal de cambios han sido revisados y aprobados y para identificar los cambios que no han sido revisados y aprobados.**

  Se pudo evidenciar que los cambios no necesitan ser aprobados para realizarse, pues solo se evidencia los cambios son planteados por personal de Tecnología en

base a un requerimiento de cada área. Luego el cambio cuando ya se ha hecho se muestra que el cliente la recibe conforme, en el mismo formulario de solicitud de cambio. Los cambios de imprevistos simplemente no se registran.

Anexo: 9 Solicitud de Cambio

- **Revisar la documentación del análisis de riesgos y determinar si los riesgos empresariales y de TI son identificados, examinados, evaluados y comprendidos por el negocio y por TI y que hay evidencia de todo lo involucrado en este tema.**

  No se analizan los riesgos de TI, no existe una administración del riesgo. Existe una planificación estratégica de años anteriores donde se definió un par de riesgos de TI, que se describen a nivel macro.

  Lastimosamente no se pudo obtener físicamente esa planificación estratégica pues el CEC-EPN lo considero un documento confidencial, aunque hay que dejar sentado que se me mostro la misma.

- **Revisar la documentación de estudio de factibilidad para confirmar que la viabilidad técnica y económica han sido considerados adecuadamente.**

  No se pudo evidenciar un estudio de factibilidad en ninguno de los sistemas que indique que se consideró la viabilidad técnica o económica de realizar o no el proyecto.

- **Revisar la documentación de revisión de la calidad, comparar con los criterios originales de aceptación, e identificar las excepciones o desviaciones de los criterios originales de aceptación.**

  No se han definido niveles de aceptación del producto como se dijo solo se presenta una acta recepción del producto o cambio realizado.

  Anexo 10: Intranet solicitud o acta recepción del software.

- **Revisar la documentación de las fases finales para confirmar que el cierre de proyecto obtuvo los enfoques propuestos y si la retroalimentación indica que se requiere un análisis posterior de viabilidad.**

  La documentación lo que permite verificar es que el cliente planteo unos requerimientos y que en base a esto el desarrollador efectuó el sistema y que luego el usuario acepto el sistema.

Análisis Nivel de Madurez

Si bien existe una especificación de requerimientos inicial en los sistemas, no se demuestran que los requerimientos presentes validaciones durante el proceso de desarrollo, que demuestren que nuevos requerimientos fueron incluidos dentro de los sistema. Los cambios efectuados en la mayoría de sistemas no son registrados y el proceso de diseño formal es nulo en cualquiera de los proyectos de desarrollo de software.

Por lo que se corresponde con el nivel de madurez 0 (No existente)

0 No Existente cuando

No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.

2.3.3 PO1 Definir plan estratégico de TI

Siga los siguientes pasos para comprobar el resultado de los objetivos de control:

- **Confirmar a través de entrevistas con los miembros del comité de dirección y con otras fuentes, que los miembros del comité de dirección son apropiadamente representados por TI y el liderazgo de la Dirección (por ejemplo, la conciencia de los roles, matriz de responsabilidades de decisión, y su propiedad).**

  En el CEC-EPN, las decisiones se toman por el consenso de todos los Coordinadores de todas las áreas, con la final aprobación del Director, quién es la última instancia de cualquier decisión que se tome en el CEC-EPN. Es de suponer dentro de dicho comité se encuentra Tecnología.

  No existe un comité específico de TI. Las decisiones en su gran mayoría las toma la Coordinadora de Gestión Tecnológica en base a su criterio con ciertas opiniones del personal de su coordinación.

- **Revisar la carta de constitución del comité directivo y evaluar la relevancia (por ejemplo, funciones, responsabilidad, autoridad, la rendición de cuentas, el alcance y los objetivos son comunicados y comprendidos por todos los miembros del comité).**

  A nivel de TI como se explicó en el ítem anterior no existe un comité constituido formalmente para la toma de decisiones.

  En cuanto al CEC-EPN, que si dispone de este comité, tampoco pudo encontrarse un acta de constitución o donde se especifican aspectos como los propuestos en el ejemplo.

- **Inspeccione los casos de negocio para determinar que la documentación tiene el contenido apropiado (por ejemplo, alcance, objetivos, análisis costo-beneficio y una hoja de ruta detallada, las medidas para el éxito, las funciones y responsabilidades, el impacto de los programas de inversión en TI) y que los casos de negocio se elaboraron y aprobaron en forma oportuna. Confirmar a través de entrevistas, si TI habilito programas de inversión, servicios de TI y los activos de TI se evalúan bajo los criterios de priorización (revisar los criterios de priorización documentados).**

  Se pudieron verificar por ejemplo un planteamiento de un proyecto de software y se pudieron encontrar muchos de los ítems mostrados en el ejemplo.

  Con lo que respecta a la priorización no se ha encontrado evidencia de que la Coordinación de Gestión Tecnológica realice dicha priorización.

Anexo 3: Ejemplo de planteamiento de proyecto

- **Confirmar a través de entrevistas con los miembros de la Coordinación de TI que están informados de las direcciones futuras del negocio así como de las metas, a largo y corto plazo, objetivos, misión y valores.**

  El Sistema de Gestión de la Calidad que posee el CEC-EPN, basa su funcionamiento en esta terminología. Este tipo de información esta presente en el Manual de Calidad del CEC-EPN, así como están colocados en cada una de las oficinas en lo que se refiere a metas objetivos, misión valores. Se reviso que la política de calidad este descrita, la misma que se encontró en el **numeral 3** bajo Política y Objetivos de Calidad, como se puede ver en el

  Anexo 1*:* Manual de Calidad CEC-EPN

- **Preguntar, y confirmar que los objetivos de toda la empresa y los objetivos de TI se incorporan en los proceso de planificación estratégica y táctica de TI y que el proceso de planificación estratégica incluye todas las actividades comerciales y de apoyo.**

  No se pudo evidenciar un plan estratégico de TI. Los planes tácticos de TI no están direccionados a cumplir objetivos empresariales definidos o al menos no se evidencia tal cosa.

En lo que respecta planes tácticos se colocan los proyectos de cada año y se les da seguimiento en su avance. El accionar de la Coordinación de Gestión Tecnológica se basa en el día a día.

Anexo 2: Evidencia de un plan táctico de TI

- **Confirme con el examen de la documentación, así como en actas de reuniones o por correspondencia, que la Dirección y TI están involucrados en el aprovechamiento de la tecnología actual para crear nuevas oportunidades de negocio.**

  En el tema de aprovechamiento de la tecnología, lo define exclusivamente y directamente la Coordinación de Gestión Tecnológica, pues a la interna de dicha coordinación se plantean los proyectos (en base a requerimientos del resto de coordinaciones). La Dirección tiene una información indirecta al autorizar los pagos por ejemplo.

- **Asegúrese de que existe un informe sobre los sistemas de información actuales (incluyendo comentarios sobre el sistema, el uso de las mejoras en el sistema producto de los cambios realizados en el mismo) se mantiene de manera regular.**

  No se encontró información relevante sobre los sistemas únicamente se pudo evidenciar el planteamiento del proyecto y cambios efectuados durante el tiempo en el mismo. Como se explicó en otros procesos, la realización de cambios es sumamente informal y todos los cambios que se realizan no son los que se

reflejan en los documentos, como lo afirma la Coordinadora de Gestión Tecnológica.

- **Revisar el cumplimiento de las metas acordadas, definidas en el anterior plan táctico de TI (por ejemplo, los resultados de la evaluación del desempeño podría incluirse, pero no puede limitarse a, los requisitos actuales, la entrega actual en comparación con los requisitos, las barreras para el logro de los requisitos, y los pasos y costos requeridos para alcanzar las metas de negocio acordadas y requisitos de rendimiento).**

  No existe evidencia de un plan táctico definido por TI.

- **Preguntar y confirmar que las implicaciones de riesgo y el costo de las capacidades de TI requeridas han sido documentados en el plan estratégico de TI.**

  No se pudo evidenciar un plan estratégico de TI.

- **Confirmar que las mediciones de resultados relacionados con los beneficios de negocio identificados, se han firmado por las partes interesadas y que la opinión de los interesados se ha tenido en consideración.**

  No se pudo evidenciar la premisa.

- **Preguntar, y confirmar que el plan estratégico aprobado se comunica y que existe un proceso para determinar que el plan se entiende claramente.**

  No se pudo evidenciar un plan estratégico de TI.

- **Confirmar a través de entrevistas, actas de reuniones, presentaciones que el plan estratégico de TI ha sido aprobado por el comité de dirección de TI y la junta directiva. Preguntar, y confirmar que un proceso formal de aprobación fue seguida.**

  No se pudo evidenciar un plan estratégico de TI, por lo que este ítem no aplica.

- **Preguntar, y confirmar que los planes tácticos están alineados con los planes estratégicos y se actualizan periódicamente. Confirmar a través de entrevistas que los planes tácticos se utilizan como base para la identificación y planificación de los proyectos, la adquisición y la programación de recursos y la aplicación de las técnicas de vigilancia**.

  Como se explicó anteriormente los planes tácticos no tienen una relación fundamentada en los planes estratégicos, porque de hecho no existe un plan estratégico de TI.

  Los planes tácticos se usan para la planificación de los proyectos en el estricto sentido.

  Anexo 2: Evidencia de un plan táctico de TI

- **Preguntar, y confirmar que el contenido de los planes tácticos incluye claramente las definiciones de proyecto, los marcos de tiempo y entregables del proyecto, los recursos requeridos y los beneficios de negocios a ser monitoreados, metas indicadores de rendimiento, el plan de mitigación, plan de contingencia, el protocolo de comunicación, roles, y las responsabilidades**.

  En el plan táctico solo se puede encontrar una descripción breve del proyecto, los hitos de los proyectos, fechas de entrega y responsables.

  Anexo 2: Evidencia de un plan táctico de TI.

- **Confirme que el portafolio/ proyecto seleccionado se ha traducido en el esfuerzo requerido, los recursos, la búsqueda, logro, etc, y que fue aprobado por la alta dirección (por ejemplo, actas de reuniones, actas de revisión de alto gerencia).**

  El proyecto seleccionado fue software SISOL, tiene definido sus objetivos y recursos definidos como hoja de ruta del proyecto.

  Lo que no se pudo evidenciar en si fue aprobado por la alta gerencia pues solo se definen las firmas para el cliente y el personal de UGT. En este caso no existe firma de aceptación del cliente por ejemplo pero se reviso otros proyectos como SOCODO y se pudo determinar que no es una constante

  Anexo 3: Definición proyecto SOCODO

  Anexo 4: Definición proyecto SISOL

- **Confirme que la autoridad requerida para poner en marcha los proyectos aprobados dentro de los programas seleccionados se ha obtenido (actas de las reuniones, el proceso de aprobación formal, la comunicación de mutuo acuerdo del proyecto) de la alta dirección como de TI.**

  Simplemente se pudo evidenciar en el Manual de Calidad que el desarrollo de proyectos tecnológicos está a cargo de la Coordinación Tecnológica, no existe documento adicional que valida la autoridad para cada proyecto. Además nunca es los documentos de desarrollo de software o cualquier otro proyecto aparece la aprobación de Dirección.

• Confirmar que los proyectos que se han retrasado o aplazado o que no han procedido son comunicados a los dueños de negocios y se participan al personal de TI.

Se pregunta sobre los proyectos pospuestos y por ejemplo se pospuso el proyecto de implementación de firewall a cargo directo de la Coordinación de Tecnología, pero nunca se comunica que se había cancelado por ningún medio a los integrantes de la misma Coordinación de Gestión Tecnológica.

Análisis Nivel de Madurez

La planificación estratégica de TI es un tema en el que la alta dirección no ha tenido injerencia. Por el momento la planificación estratégica se ha quedado en una

planificación global para todo el CEC-EPN, pero en ningún momento algo especifico para TI.

Si bien existen planes tácticos estos demuestra que las acciones de TI, solo se ejecuten pero no se planean, o no al menos los suficiente.

Por lo que se corresponde con el nivel de madurez 0 (No Existente)

0 No Existente cuando

No se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.

2.3.4 AI3 Adquirir y Mantener infraestructura Tecnológica

Siga los siguientes pasos para poner a prueba el resultado de los objetivos de control:

- **Revisar que los planes para la adquisición de la infraestructura han sido revisados y aprobados y que los riesgos, costos, beneficios, y la conformidad técnica, han sido considerados. Inspeccione que los planes para confirmar la firma del consejo de TI o equivalente.**

  Se pudo evidenciar que no existe un plan documentado de adquisición de infraestructura, por lo que no se pudo evidenciar un análisis de riesgos, un análisis costo beneficio, etc.

- **Confirmar con el personal responsable que todos los requisitos de seguridad asociados con la instalación de la aplicación de software y los procesos de mantenimiento, se han abordado y que cualquier nuevo riesgo ha sido evaluado y medido.**

  La seguridad por el momento no es prioritaria para la organización, y el manejo de riesgos no ha sido documentado. Se hacen las pruebas necesarias para tratar de no afectar el desenvolvimiento de la aplicación de software en todos los aspectos pero muchas de las pruebas se hacen ya en ambientes de producción. Pero en síntesis no hay procedimientos para este proceso.

  El mantenimiento de cualquier tipo de infraestructura tampoco es documentada por ejemplo el cambio de una memoria RAM o un disco duro, no tiene un procedimiento que lo norme para acordar niveles de aceptación.

- **Confirmar con el departamento de formación y el personal clave, que las personas que utilizan componentes de infraestructura sensibles, han recibido la formación adecuada**

  Se pudo evidenciar que todas las instalaciones de nueva infraestructura vienen acompañadas con una capacitación general del vendedor acerca del uso básico de la herramienta, su instalación y soporte posterior.

  Anexo 11: Contrato con compra de Capacitación.

- **Confirmar con el personal clave que un plan y la estrategia están en marcha para orientar el mantenimiento de la infraestructura, en consecuencia con los cambios a los procedimientos de gestión. Inspeccionar la documentación pertinente del plan para confirmar que todos los aspectos de los requisitos de mantenimiento de infraestructuras (incluidas las solicitudes de cambio, los parches, actualizaciones, correcciones) están incluidos. También confirman que la estrategia y plan están en línea con la dirección tecnológica de la organización, se revisan de manera oportuna y son aprobados por la gerencia responsable.**

  Como se mencionó anteriormente no existe un plan o estrategia documentada en lo que respecta al mantenimiento o adquisición de infraestructura. De manera informal el coordinador de Tecnología, establece la adquisición de nueva infraestructura en base a la vida útil de los equipos o deterioro de los mismos.

  En lo que respecta actualizaciones o parches, para todo lo que es plataforma Windows se tiene funcionando la herramienta WSUS para la descarga y automática actualización de los equipos, en lo que se refiere específicamente a la infraestructura las actualizaciones se dan a criterio del personal de TI o por recomendaciones de los proveedores.

  Intuitivamente la Coordinación de Gestión Tecnológica busca darle una dirección a TI, pero esta no está documentada o definida por la alta dirección.

- **Asegúrese de que el método utilizado para separar los entornos de sistemas, en el desarrollo y la prueba es adecuada.**

La separación de entornos de prueba no es la más adecuada, en lo que respecta a instalaciones de software recientemente se ha implementado un sistema para el control de versiones y manejo de código (CVN-Tortoise), además de un servidor pruebas dirigido exclusivamente a software, pero no se han documentado que tipos de pruebas, periodos o niveles de aceptación para saltar a producción.

En lo que respecta infraestructura se ha implementado un método de versiones en el tiempo por ejemplo si se instala un servidor de antivirus por lo que general se deja intacto el servidor anterior, se instala en un nuevo servidor el nuevo servidor de antivirus y si algo está mal con el nuevo servidor simplemente se conecta al anterior, que no es lo más óptimo además que se maneja mucho el prueba y error.

- **Asegúrese de que un entorno de prueba se ha creado correctamente que considera la funcionalidad, configuración de hardware y software, pruebas de integración y rendimiento, la migración entre entornos de control de versiones, los datos de prueba y herramientas, y la seguridad.**

  Por el momento disponen de aquello en pequeña medida en el área de desarrollo de software donde se tiene un servidor de pruebas donde se almacenan bases de pruebas y una aplicativo (CVN-Tortoise) que maneja el versionamiento del software, además de un control básico del código.

  En lo que respecta infraestructura no se tiene ese ambiente no hay servidores de pruebas o ambientes que los simulen.

Adicionalmente nada de lo referente al ambiente de pruebas se documenta, pues no existe un procedimiento por ejemplo para determinar, responsables, tiempos, niveles de aceptación y tipos de prueba a realizarse en cada uno de los proyectos.

Análisis Nivel de Madurez

La adquisición de la infraestructura se da de forma no planificada, pero siempre tratando de darle la importancia debida a la infraestructura, pues se trata de actualizarla constantemente en base a las posibilidades de la institución a través de los recursos que le asigne la alta gerencia.

La actualización física sobre todo no está normado o definido por procedimientos que acuerden niveles de aceptación sobre las mismas.

Tampoco existen ambientes de pruebas para los proyectos de infraestructura por lo que cualquier cambio se hace en ambientes de producción.

Se puede determinar que su nivel de **madurez corresponde a 1 Inicial / Ad Hoc**

1 Inicial / Ad Hoc cuando

Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.

2.3.5 PO10 Administrar los proyectos de TI

Tome las siguientes medidas para poner a prueba los resultados de los objetivos de control de:

- **Inspeccione la documentación del marco de administración del programa para verificar que el programa adecuadamente evalúa la cartera de proyectos de TI con los objetivos del programa. El programa debe especificar los recursos necesarios, incluida la financiación, gerente de proyecto, equipo de proyecto, los recursos de TI y recursos de negocios, de ser necesario.**

  Los proyectos generados por TI, son administrados por TI, no existe un comité o similar que administre los proyectos a nivel del CEC-EPN.

  Los proyectos en TI son planteados bajo los formularios de planteamiento de proyectos, definido en el Manual de Calidad del CEC-EPN.

  Anexo 4: Ejemplo definición proyecto

  Los proyectos son plasmados de acuerdo a requerimientos poco formales planteados por el resto de áreas del CEC-EPN a TI, o por necesidades detectadas directamente en TI.

- **Inspeccione las actividades de documentación y seguimiento a través del proceso para verificar que el equipo de administración del programa también especifica recursos necesarios, incluidos los administradores de proyectos, financiación, equipos de proyecto, los recursos de TI y recursos de negocios, de ser necesario.**

  Como se explicó anteriormente no existe un comité o área que organice el desarrollo de los proyectos del CEC-EPN. Incluso cuando TI, realiza productos para otras áreas donde debería plantearse un proyecto en conjunto con otras áreas no se hace así y las áreas interesadas solo participan el momento de levantar los requerimientos.

- **Inspeccione las actividades de documentación y seguimiento a través del proceso para verificar que el equipo de administración de los programas efectivamente establece la rendición de cuentas de cada proyecto y que, cuando se asigna la responsabilidad, se acepta y tiene la suficiente autoridad para actuar, la competencia necesaria, los recursos en proporción, líneas claras de rendición de cuentas, una comprensión de los derechos y obligaciones, y las medidas pertinentes de rendimiento.**

  No se ha definido un procedimiento para el desarrollo de un proyecto, por lo que tampoco se define un líder de proyecto que rinda cuentas por el mismo. En TI la misma persona que documenta el proyecto se hace cargo del mismo y es la que rinde cuentas al Coordinador de Gestión Tecnológica.

Anexo 3: Definición de Proyecto

Anexo 2: Evidencia de un plan táctico de TI (seguimiento del proyecto).

- **Inspeccione los cronogramas y otros documentos para determinar si el equipo de gestión de los programas efectivamente descubrió las interdependencias de múltiples proyectos en el programa y desarrollo un calendario para su conclusión de la programación que se debe cumplir.**

  No se pudo evidenciar el tratamiento de interdependencias.

- **Inspeccione las comunicaciones y otros documentos para determinar que el equipo de gestión del programa determina de forma efectiva, los interesados en el programa dentro y fuera de la empresa, se establecen los niveles adecuados de coordinación, comunicación y el enlace con estos actores, y mantiene comunicación con ellos durante la duración del programa.**

  No se pudo evidenciar una coordinación ordenada entre los actores del proyecto. El levantamiento de requerimientos es el único momento que existe una comunicación entre el proponente y TI. Hay que tomar en cuenta que en muchos casos los proyectos son de propiedad de otras áreas y TI solo es un apoyo.

- **Inspeccione las evaluaciones periódicas y otros documentos para verificar que el marco de la gestión de proyectos se utiliza eficazmente como un parte**

integrante, y es consistente con el enfoque de la organización de gestión de programas, y que es conveniente, en la luz de las condiciones cambiantes.

No existen evaluaciones periódicas de los proyectos, lo que se hacen es revisiones de los proyectos para darles un seguimiento, Están revisiones no son documentadas para establecer un seguimiento documentado del proyecto, posibles retrasos, cambios, reprogramación entregables, etc. Únicamente se evidencia en qué etapa de cumplimiento está el proyecto.

Anexo 2: Evidencia de un plan táctico de TI

- **Inspeccione la documentación para verificar que el equipo de gestión de los programas efectivamente asigna a cada proyecto de TI de uno o más patrocinadores con la suficiente autoridad para administrar la ejecución del proyecto dentro del programa estratégico global, la cesión se haga sin ambigüedades, las funciones y responsabilidades quedan claras, y la responsabilidad es aceptada por el cesionario(s).**

  Como se explicó anteriormente no existe un comité que administre los proyectos, por lo que la Coordinadora de Gestión Tecnológica explica que es un problema la definición de roles dentro del proyecto y que la mayoría de proyectos terminan recayendo sobre TI, aunque los proyectos solo necesiten un ligero apoyo de TI. Esto además explica acarrea problemas pues no se genera compromiso en las áreas patrocinadoras.

- **Inspeccione los documentos tales como actas de reuniones y la documentación de cierre de sesión para comprobar que el equipo de gestión de proyectos eficazmente establece el compromiso y la participación de los actores clave, incluyendo la gestión del departamento usuario involucrado y los usuarios clave, en el inicio, la definición y autorización de un proyecto.**

  No se ha podido evidenciar tal información.

- **Inspeccione los documentos tales como actas de las reuniones y el inicio de sesión fuera de las actividades de documentación y seguimiento, a través del proceso para verificar que el compromiso continuo de las partes interesadas y la participación para el resto del ciclo de vida del proyecto se describe con eficacia durante la iniciación del proyecto y un proceso de refinación se utiliza eficazmente durante el proceso.**

  No se logre evidenciar tal compromiso en los documentos que forman parte del archivo de cada uno de los proyectos, que son la definición de requerimientos y la definición del proyecto.

  Anexo 7: Especificación requerimientos

  Anexo 4: Ejemplo definición proyecto.

- **Verifique que el plan de comunicación del proyecto / programa se mantiene eficazmente durante todo el proyecto.**

  No se cuenta con un plan de comunicación formalmente definido, por lo que las comunicaciones según se explicó son informales.

- **Observar solicitudes de cambio, de muestra para verificar que las partes interesadas siempre firman en las mismas.**

  Se revisaron dos solicitudes de cambio y se logró determinar que las firmas que aparecen en el mismo son del desarrollador y de la Coordinadora de TI, pero no existe firma del o los clientes

  Anexo 9: Solicitud de cambio 1.

  Anexo 18: Solicitud de cambio 2

- **Inspeccione los planes, políticas y procedimientos para verificar que el marco de la gestión del proyecto se ha diseñado para proporcionar con eficacia los roles de administradores y usuarios finales de la empresa afectada y las funciones de TI para aprobar y suscribir adelantos a los entregables producidos en cada fase del proyecto del sistema de ciclo de vida del desarrollo, antes de trabajar en la próxima fase.**

  No se encontró evidencio sobre este punto.

- **Inspeccione la documentación para verificar que la base del proceso de aprobación es eficaz para definir claramente los criterios de aceptación acordados con las partes interesadas antes de comenzar el trabajo en la fase de prestación del proyecto y, como mínimo, de antelación a la finalización de las prestaciones de una fase.**

Se evidencia que los proyectos de TI, se estandarizan bajo el formulario de planteamiento de proyectos, del mismo que se tomó una muestra y se observación la aprobación del cliente principal y personal de TI. Lo que no se pudo evidenciar es que en cada fase del proyecto se apruebe los avances.

Anexo 3: Definición de Proyecto

- **Inspeccione los planes, políticas y procedimientos para verificar que el inicio de la fase y la aprobación se ha diseñado con eficacia a considerar los costos reales, gestión del tiempo y el progreso, y para evaluar las diferencias más importantes frente a los beneficios esperados del proyecto.**

  Se pudo evidenciar que la definición del proyecto se define gran parte de los aspectos mencionados.

  Anexo 4: Ejemplo definición proyecto

- **Inspeccionar físicamente la documentación y la búsqueda de rastros de auditoría para verificar que el plan de proyecto integrado permite controlar la gestión el progreso del proyecto.**

  No se pudo evidenciar tal información

- **Inspeccione los documentos para evaluar que el plan integrado del proyecto y los planes dependientes se mantenga al día con el plan de acuerdo principal, para reflejar los progresos reales y cambios importantes al marco de gestión del programa.**

Como se explicó anteriormente no existe un plan integral de proyectos del CEC-EPN. A nivel de Ti existen un conjunto de proyectos que van siendo revisados para analizar su cumplimiento, en este formulario no se puede diferenciar cuando un proyecto está siguiendo su planificación o cuando está haciendo un reajuste o modificación en su planificación.

Anexo 2: Seguimiento de proyecto

- **Inspeccione el organigrama de dirección del proyecto o si el gráfico RACI está completo.**

  No existe tal documento

- **Revisar la evaluación de riesgos relacionados con el proyecto y la documentación minutos/sesión para verificar que los riesgos (internos y externos) son gestionados y discutidos en un nivel apropiado dentro de la estructura de gestión del proyecto durante todo el proyecto.**

  En el CEC-EPN no existe una administración o gestión del riesgo.

- **Determinar que el plan de gestión del riesgo se integra con el plan general del proyecto.**

  No se pudo evidenciar una integración la gestión del riesgo y el plan de proyectos.

- **Inspeccione las evaluaciones y reevaluaciones de los riesgos, cambie la evaluación de solicitud y otros documentos para verificar que**

periódicamente las reevaluaciones son eficaces y responden a cambios en el riesgo a lo largo del proyecto.

No se evalúan los riesgos.

- **Verifique que todas las actualizaciones necesarias se llevan a cabo con el plan de gestión de riesgos.**

  No se lleva un plan de riesgos en ninguno de los proyectos.

- **Inspeccione los documentos, los senderos de búsqueda de auditoría y transacciones a través del proceso de seguimiento para verificar que la gestión de riesgos del proyecto se está llevando a cabo con eficacia, incluyendo soluciones para los riesgos inesperados.**

  No pudo evidenciar, pues no se hace tratamiento de riesgos.

- **Inspeccionar el registro de los riesgos del proyecto, proyecto de registro de los temas y otros documentos para verificar que el registro de los riesgos del proyecto y el registro de los problemas del proyecto se mantiene, junto con las acciones correctivas.**

  No pudo evidenciar, pues no se hace tratamiento de riesgos.

- **Inspeccione la documentación para verificar que el alcance de los objetivos del proyecto se documentan y los resultados principales del proyecto está incluidos y que un proceso de calidad se define.**

En la definición del proyecto constan los objetivos principales y los resultados esperados. No existe un procedimiento o proceso que controle la calidad de los productos. Los proyectos se evalúan en la mayoría de casos por los clientes y ellos mismo verifican si lo que pidieron es lo entregado.

Anexo 4: Ejemplo definición proyecto

Análisis Nivel de Madurez

Si bien existe un procedimiento para la realización de proyectos de TI, este procedimiento aún no está maduro pues no se le da la importancia que debiera al usuario final o cliente pues no se lo involucra formalmente en las decisiones del proyecto.

La alta gerencia no ha organizado un programa que administre los proyectos los integre y verifique su interrelación. Tampoco ha apoyado los mismos de manera que se le asigne la responsabilidad y autoridad necesaria al ejecutor del proyecto para que funcione como la guía necesaria. Los proyectos de TI, entonces son iniciativas de TI, por lo que no tienen el control, evaluación, seguimiento, y gestión del riesgo por parte del CEC-EPN.

Por lo que se corresponde con el nivel de madurez 1 (Inicial /Ad hoc)

Inicial / Ad Hoc cuando

El uso de técnicas y enfoques de administración de proyectos dentro de TI es una decisión individual que se deja a los gerentes de TI.

Existe una carencia de compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos.

Las decisiones críticas sobre administración de proyectos se realizan sin la intervención de la gerencia usuaria ni del cliente. Hay poca o nula participación del cliente y del usuario para definir los proyectos de TI. No hay una organización clara dentro de TI para la administración de proyectos. Los roles y responsabilidades para la administración de proyectos no están definidas. Los proyectos, cronogramas y puntos clave están definidos pobremente, si es que lo están. No se hace seguimiento al tiempo y a los gastos del equipo del proyecto y no se comparan con el presupuesto

2.3.6 PO9 Evaluar y Administrar los Riesgos de TI

Siga los siguientes pasos para poner a prueba el resultado de los objetivos de control:

- **Preguntar si los niveles de tolerancia en la administración del riesgo de TI están en línea con los niveles de tolerancia del riesgo de la empresa. Determinar si tolerancia al riesgo de la organización se utiliza como entrada para los negocios y el desarrollo de la estrategia de TI.**

  El CEC-EPN no mantiene una cultura de riesgo, por lo tanto no evalúa ni administra el riesgo, ni a nivel organizacional ni en ninguna de sus áreas. La última planificación estratégica que se realizo fue en 2007, donde se evaluó a nivel macro los riesgos y en base a ellos se estableció los indicadores para medirlos. La Coordinación de Tecnología como tal no ha definido sus riesgos específicos.

- **Preguntar si existe un proceso para aplicar los niveles de tolerancia del riesgo empresarial a las decisiones en la administración del riesgo de TI. Estimar la comparación del marco de evaluación del riesgo frente a otras organizaciones similares, las normas internacionales pertinentes y las mejores prácticas de la industria ha llevado a cabo.**

  No existe un proceso que defina los niveles de tolerancia del riesgo organizacional que puedan ser aplicados en TI.

- **Compruebe si los riesgos relacionados con la rendición de cuentas y las responsabilidades son entendidos y aceptados. Verifique que las habilidades y recursos necesarios están disponibles para la administración de riesgos**.

  No se han evaluado ni definido los riesgos relacionados con la rendición de cuentas ni responsabilidades.

- **Infórmese, a través de entrevistas con miembros clave del personal, sobre el mecanismo de control y su fin, la rendición de cuentas y que las responsabilidades se entienden y aplican.**

  No se pudo evidenciar ningún mecanismo de control de los riesgos. Tampoco que se establezcan rendición de cuentas o responsables en lo que respecta al riesgo de TI.

- **Inspeccione si las actividades se integraran eficazmente en los procesos de gestión de TI.**

  No pudo evidenciar, que las actividades se integren con la gestión en el contexto de este punto.

- **Inspeccione si los impactos identificados son relevantes y significativos para la empresa y si están sobre o sub-estimados. Determinar si los equipos multifuncionales contribuyen al proceso de análisis de eventos. Verificar a través de entrevistas y los informes de impacto si los miembros del grupo de trabajo que identifican eventos están debidamente capacitados en el marco de gestión del riesgo empresarial. Verificar si las interdependencias y las probabilidades están perfectamente identificadas durante la evaluación de impacto. Revisar cualquier correlación para verificar que se expone a una probabilidad significativamente diferente y los resultados de impacto derivados de tales relaciones.**

  No se encontró documentado riesgo alguno, por lo que no se puede dar un juicio sobre si esta subestimado o no. Tampoco está documentado la conformación de que equipos multifuncionales que valoren los riesgos.

- **Inspeccionar el proceso de administración de riesgos para determinar si las fuentes de información utilizadas en el análisis son razonables.**

  No se encontró evidencia de la gestión de riesgos a nivel de la Coordinación de Gestión Tecnológica, del CEC-EPN.

- **Inspeccione el uso de análisis estadísticos y las determinaciones de probabilidad para medir la probabilidad de riesgo de forma cualitativa o cuantitativa.**

  No pudo evidenciar, pues no se hace tratamiento de riesgos.

- **Recorra a través del proceso para determinar si los riesgos inherentes y residuales se definen y documentan.**

  No pudo evidenciar, pues no se hace tratamiento de riesgos.

- **Inspeccione el plan de acción de riesgo para determinar si, se identifican las prioridades, responsabilidades, horarios, resultados esperados, la mitigación del riesgo, costos, beneficios, las medidas de desempeño y el proceso de revisión es establecido.**

  No pudo evidenciar, pues no se hace tratamiento de riesgos y no existe tal plan.

- **Inspeccione las respuestas a los riesgos de las aprobaciones pertinentes. Revisar las acciones para verificar si la propiedad se le asigna y documenta.**

  No pudo evidenciar, pues no se hace tratamiento de riesgos.

- **Inspeccione si el plan de gestión del riesgo es efectivamente mantenido / ajustado.**

No existe plan de gestión de riesgo, por lo que no se puede evidenciar tal situación.

- **Inspeccionar y revisar los resultados del plan de acción para determinar si se llevan a cabo de conformidad con las directrices de riesgo y el marco refleja los cambios de objetivo del negocio. Revisar el plan para verificar que se ha diseñado en términos de riesgo para evitarlo, reducirlo y compartirlo. Inspeccione si la respuesta a los riesgos que deben incluirse es seleccionada en la relación costo-beneficio.**

  No existe una gestión del riesgo, por lo que no existe el plan de acción que menciona este punto.

Análisis Nivel de Madurez

En este proceso realmente el CEC-EPN no ha hecho nada, no se tiene una cultura de riesgo en ninguna parte de la organización. Específicamente en TI no se evalúan los riesgos ni en proyectos ni en la infraestructura o aplicaciones ya existentes.

Por lo que se corresponde con el nivel de madurez 0 (No existente)

0 No Existente cuando

La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.

2.3.7 AI6 Administración de Cambios

Siga los siguientes pasos para poner a prueba los resultados de los objetivos de control:

- **Para una muestra de cambios, confirmar que lo siguiente ha sido aprobado por los involucrados correspondientes (los propietarios de procesos de negocio y La administración de TI):**

  Solicitud de cambio

  El formulario de **cambio** está definido como parte del sistema de gestión de calidad del CEC-EPN, dicho formulario está presente en el manual de calidad del Coordinación de Gestión Tecnológica y esta accesible para cualquier usuario del CEC en la Intranet institucional.

  Anexo 10 Comunicación a través de intranet del CEC-EPN

  Especificación del cambio

  En el mismo formulario de cambio que se mencionó en el ítem anterior, se pide detallar el cambio a realizar.

  Anexo 5: Formulario Solicitud de Cambio

  Acceso al programa fuente

  Casi la totalidad de los sistemas han sido desarrollados por el CEC-EPN, por lo que se tiene libre acceso al código fuente de los sistemas.

Planificación completa del cambio

No existe una planificación del cambio, además no existe un ambiente controlado y definido de pruebas, en algunos cambios incluso los formularios de solicitud de cambio no son llenados.

Solicitud para mover el programa fuente al entorno de prueba

No existe la solicitud para mover el código fuente a un entorno de pruebas.

Finalización de las pruebas de aceptación

No existe un documento o procedimiento que especifique la finalización de las pruebas de aceptación.

Solicitud de compilación e implementación en el entorno de producción.

No existe un documento que especifique la solicitud de compilación e implementación.

Resolución y aceptación total y específicamente el impacto en la seguridad.

Si existe un documento donde los involucrados en el requerimiento de cambio validen la aceptación de la solución, sin embargo este no especifica nada sobre el impacto en el campo de la seguridad.

Anexo 8 Solicitud de Cambio validada

- **Desarrollo de un proceso de difusión del cambio realizado**.

No existe una comunicación formal o informal de los cambios realizados.

- **Revisar que la documentación de la solicitud de cambio incluya** (Para todos los ítems de esta sección Anexo 8 Solicitud de Cambio, Anexo 9 Solicitud de Cambio

  Fecha de la solicitud del cambio.

  El documento que describe el requerimiento de cambio SI incluye la fecha de solicitud.

  Persona(s) que solicitó el cambio.

  El documento que describe el requerimiento de cambio SI incluye la el nombre de la persona que solicitó el cambio.

  Aprobación de la solicitud de cambio.

  La aprobación de la solicitud de cambio se da por el personal de TI.

  Aprobación de los cambios realizados – Responsabilidad de TI.

  No existe en el documento la aprobación de los cambios a realizar o realizados.

  Aprobación de los cambios realizados – Responsabilidad de los Usuarios.

  No existe en el documento la aprobación de los cambios a realizar o realizados. Solo se cumple con el informar al usuario sobre la terminación de la solución y la validación se la realiza de manera informal.

Fecha de actualización de la documentación.

Cuando se realiza un cambio NO existe en el documento la fecha de actualización de la documentación que fue afectada por el cambio realizado.

Fecha de la implementación en el entorno de producción.

No se especifica la fecha de implementación en el formulario.

Aceptación del Aseguramiento de la Calidad del Cambio.

No existe información sobre la aceptación del aseguramiento de la calidad.

Aceptación por el área de operaciones.

El documento no especifica información sobre la aceptación por parte del área de operaciones.

- **Para una muestra de cambios, revise la documentación para determinar la existencia de un mecanismo de control de versiones.**

  No se tiene un mecanismo que permita llevar un control de versiones.

- **Para una selección de los cambios relacionados con los proveedores de servicios contratados, inspeccione los cambios implementados y determine si siguen las instrucciones vendedor-proveedor.**

Si se verifica el funcionamiento de los cambios realizados sin embargo no se verifican si se cumplen las instrucciones provistas por el proveedor. Hacer referencia a la solicitud de cambio llena.

- **Inspeccione una selección de cambios y determine si las solicitudes han sido clasificadas.**

  No existe una clasificación de los cambios pues no están sistematizados.

- **Inspeccione una selección de cambios y determine si los cambios han sido priorizados en base de criterios predefinidos.**

  No existe un criterio de priorización de requerimientos de cambios, sin embargo aquellas solicitudes que provienen del área gerencial son atendidas con prioridad.

- **Inspeccione una selección de cambios y determine si los cambios han sido evaluados en un método estructurado**.

  No se evidencia que los cambios hayan sido evaluados en un método estructurado.

- **Inspeccione una muestra de cambios de emergencia y verifique que han sido procesados en conformidad con la Administración de cambios. Verifique que los procedimientos han seguido los procesos de autorización, documentar y revocar el acceso después de que el cambio ha sido aplicado.**

Se verifica que cuando han existido cambios emergentes, éstos fueron atendidos sin seguir un procedimiento formal, la mayoría de veces los cambios se hacen de esta manera.

Por ejemplo se hizo cambios en el sistema SOCODO para que se permita visualizar únicamente los procesos y documentos de la coordinación a la que el usuario pertenece. Dicho cambio nunca fue registrado ni documentado, solo se realizó en base a las sugerencias de un usuario por el desarrollador responsable del sistema.

- **Inspeccione una muestra de los cambios de emergencia y determine si una revisión posterior ha sido realizada después de que los cambios fueron aplicados. Considere las implicaciones para futuras aplicaciones en administración del sistema, impacto en el desarrollo y ambiente de pruebas.**

  Considerando el caso propuesto para el ítem anterior sobre el sistema SOCODO, no se mostró evidencia que el dicho caso haya tenido un seguimiento posterior a su implementación.

- **Revise a través del sistema de seguimiento y reportes, y verifique que se mantiene la documentación para los cambios rechazados, la situación de los cambios aprobados, cambios en proceso, y cambios cerrados, y confirme con los usuarios para garantizar cual es el estado actual.**

  No se mantiene la administración de los cambios automatizados por lo que es casi imposible definir reportes de los mismos.

- **Inspeccione los reportes de estado para una muestra de cambios para determinar si una pista de auditoría es utilizada para seguir el estado de los cambios desde su inicio hasta la culminación.**

  No se realiza un seguimiento de los cambios efectuados y no existe reporte alguno relacionado a los cambios.

- **Inspeccione los reportes de estado de una muestra de cambios para determinar si los parámetros de rendimiento son utilizados para la revisión y monitoreo del administrador.**

  Los cambios solo se expresan con una solicitud y especificación de cambios y luego con su cierre. No se evidencia estados en los cambios y los cambios no se revisan más que por el solicitante a manera de aceptación.

- **Inspeccione una muestra de los cambios para determinar si la documentación del cambio ha sido conservada de conformidad con el correspondiente período de retención.**

  Se comprueba la existencia de documentos físicos dentro del periodo de retención, de acuerdo a lo que dice el Sistema de Gestión de la Calidad del CEC-EPN.

- **Inspeccione los manuales de proceso del negocio para determinar si han sido actualizados de acuerdo con los cambios de funcionalidad nuevos o de mejora en hardware y software.**

  Se revisa los manuales y se determina que estos no han sido actualizados cuando se han producido cambios en la infraestructura tecnológica.

- **Seleccione una muestra de los cambios y evalúe la calidad de la coordinación con terceros.**

  Los cambios realizados a sistemas por terceros no se registran en el formulario.

- **Confirme el procedimiento de evaluación del rendimiento del proceso de administración de cambios. Evalúe las posibles mejoras identificadas que resulten en recomendaciones para la administración de TI.**

  No se define un procedimiento para la evaluación de este proceso, de hecho el proceso de administración de cambios es casi inexistente, pues el formulario de cambios pertenece al proceso de desarrollo de software específicamente.

  Para hardware no existe un procedimiento de cambio y los errores por falta de documentación en el cambio son comunes.

  Además el seguimiento posterior al cambio es nulo y la documentación es insuficiente.

Análisis del Nivel de Madurez

La Coordinación de Gestión Tecnológica del CEC-EPN, está consciente de la importancia de manejar y administrar los cambios, más sin embargo por el momento el cambio solo es tratado a nivel de software mas no de hardware e incluso en el tema de software los cambios son muy poco documentados y registrados, lo que sin duda es una deficiencia en su proceso.

Además se detectó luego del análisis que no todos los cambios se registran y que el seguimiento posterior es nulo.

Por lo tanto para este proceso el nivel de madurez es 1(Inicial /Ad Hoc)

1 Inicial / Ad Hoc cuando

Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.

2.3.8 PO2 Definir la Arquitectura de la Información.

Siga los siguientes pasos para comprobar el resultado de los objetivos de control:

- **Revise la documentación del modelo de arquitectura de la información para determinar si se dirige a todas las aplicaciones importantes, sus interfaces y relaciones.**

Se pudo observar que no todos los sistemas de información poseen su modelo de arquitectura de información. Por ejemplo se pudo evidenciar que sistemas como KASAMA, SYSNOTE no tienen definido dicho modelo, mas, sistemas como **KASAMA** si lo tienen definido pero básicamente, a nivel de metadatos de la base de datos, donde se define el diccionario de datos de todos los campos de la base de datos, pero por ejemplo no existe una definición de seguridad o integridad de los datos, etc; que deberían definirse en un modelo de arquitectura de información.

No se ha establecido un modelo de arquitectura de información para los archivos planos, que se distribuyen en dos servidores independientes en cada una de las sedes.

Anexo 12: Diccionario de Datos Kasama.

- **Revisar la información de la documentación de arquitectura para verificar que es consistente con la estrategia de la organización y los planes estratégicos y tácticos de TI.**

  Los modelos son descritos de una manera sencilla y se refieren principalmente a los metadatos de la base de datos, No se pudieron evidenciar planes estratégicos y taticos de TI.

- **Asegúrese de que los cambios realizados en el modelo de arquitectura de la información reflejan aquellos realizados en los planes estratégicos y tácticos de TI, y que los costos y riesgos asociados se identifican.**

El modelo de arquitectura de información no se integra o actualiza a ningún plan estratégico y táctico pues la Coordinación de Gestión Tecnológica no tiene definido estos planes, así como tampoco realiza una administración de sus riesgos.

- **Preguntar, y confirmar que la gestión del negocio y de TI comprenden las partes relevantes del modelo de arquitectura de la información (por ejemplo, propiedad de los datos, la rendición de cuentas, el gobierno de datos).**

  Aspectos como propiedad de los datos, la rendición de cuentas, el gobierno de datos, no se han definido en los actuales modelos de arquitectura expuestos.

- **Preguntar, y confirmar que el modelo de arquitectura de la información se verifica con regularidad para verificar su ajuste, flexibilidad, integridad y seguridad; y que está sujeto a revisiones frecuentes de los usuarios (por ejemplo, el impacto de cambios en el sistema de información).**

  No se pudieron identificar registros de las revisiones en el modelo de arquitectura, por lo general los cambios realizados no se documentan.

- **Revisar el diccionario de datos y verificar que todos los datos importantes se describen adecuadamente de acuerdo con el proceso definido.**

  Se pudo evidenciar que se definen todos los datos del sistema de una manera consistente.

Anexo 12: Diccionario de Datos

- **Verifique que se definen las reglas de sintaxis de datos, reglas de validación de datos y reglas de negocio mediante un proceso definido.**

  No se pudo evidenciar un procedimiento que norme la sintaxis de los datos, reglas de validación de datos, etc.

- **Preguntar, y confirmar que los metadatos en los diccionarios de datos son lo suficientemente detallados para comunicar la sintaxis de una manera integra en todas las aplicaciones y que incluyen los atributos de datos y niveles de seguridad para cada elemento de datos.**

  Como se puede evidenciar los metadatos son descritos con amplitud, como se dijo anteriormente no todos los sistemas poseen esta descripción. También se pudieron observar los atributos de los datos, pero no se pudo evidenciar que se establezca información sobre la seguridad de cada dato.

  Anexo 12: Diccionario de Datos.

- **Preguntar, y confirmar que la gestión de diccionario de datos se implementa, mantiene y revisa periódicamente para gestionar la organización del diccionario de datos y las reglas de sintaxis.**

  Se evidencio que no existe cambios entro lo que se puede ver en la base de datos y lo que está en el diccionario de datos del sistema tomado con referencia KASAMA.

- **Compruebe si el sistema cubre todos los elementos de datos relevantes mediante la comparación de una lista de datos con la aplicación efectiva de la herramienta.**

  Se analizó el sistema KASAMA y no se pudo notar diferencia entre el diccionario y el sistema o su base de datos.

- **Preguntar, y confirmar que un programa de calidad de datos se lleva a cabo para aumentar la integridad de los datos, la normalización, la coherencia, de una sola vez la entrada de datos y el almacenamiento (por ejemplo, el uso automatizado de recolección de pruebas cuando sea posible para poner a prueba la integridad de datos, la normalización, la coherencia, de una sola vez los datos de entrada y almacenamiento de datos de ejemplo, los módulos integrados de auditoría, análisis de datos utilizando el software de auditoría u otras herramientas de integración). Utilizar herramientas automatizadas (por ejemplo, con ayuda de computadora las técnicas de auditoría [TAACs]) para verificar la integridad de los datos**.

  No se ha encontrado evidencia de un procedimiento que establezca un programa para asegurar la calidad de los datos. Tampoco se hace este proceso de manera informal.

- **Preguntar, y confirmar que un esquema de clasificación de datos está definido y aprobado (por ejemplo, los niveles de seguridad, niveles de acceso y los valores predeterminados son apropiados).**

  No se pudo comprobar que exista un esquema de clasificación de los datos.

- **Preguntar, y confirmar que los niveles de clasificación de datos se definen en función de las necesidades de la organización para la protección de la información y el impacto en el negocio de la información sin protección.**

  No se ha definido formalmente una clasificación de la información únicamente se ha definido la información y se la separado, en información en base de datos o información en archivos planos, ambos contenidos en distintos servidores en las dos sedes.

- **Verifique que los dueños de los procesos del negocio revisan la clasificación actual de la información y son conscientes de sus roles, responsabilidades y rendición de cuentas para los datos.**

  No se logra validar lo expuesto, no existen documentos sobre el tema.

- **Preguntar, y confirmar que los componentes se heredan de la clasificación de los activos originales.**

  No se pudo evidenciar si los componentes se heredan de la clasificación de activos originales.

- **Verifique que todas las desviaciones de la política heredada de clasificación de datos han sido aprobados por el titular de los datos.**

  No se pudo evidenciar pues no existe dicha política.

- **Preguntar, y confirmar que la información y los datos (incluidas copias impresas de los mismos) están etiquetados, manejados, protegidos y sino están asegurados en una manera consistente con las categorías de clasificación de datos.**

  Los archivos o datos impresos están etiquetados y se llevan de acuerdo a los procedimientos debidos. Las seguridades son típicas de cada oficina aunque se trabaja en un ambiente abierto.

  No existen procedimientos que definan la seguridad delos documentos impresos.
  En lo que respecta a los datos en digital se encuentran en servidores específicos con seguridades intermedias con procedimientos de backup constante.
  El backup se lo realiza con la herramienta DataProtector de HP, la cual realiza un respaldo de bases de datos y de servidor de archivos
  Anexo 20: Herramienta de Backup.

- **Inspeccionar la evidencia de que la integridad y los criterios requeridos de consistencia de los datos se definen e implementan (por ejemplo, los datos almacenados en bases de datos y almacenes de datos son compatibles).**

  La realidad es intuitiva y no se demuestra evidencia de que se haya planeado dicha integración.

- **Preguntar si, y confirmar que un programa de calidad de los datos se lleva a cabo para validar y garantizar la integridad de los datos y la coherencia sobre una base regular.**

No se ha definido ningún programa de calidad de los datos.

Análisis Nivel de Madurez

Por lo que se pudo observar algunos proyectos y procesos hacen un levantamiento de arquitectura de información, sobre todo basada en datos no en información. La arquitectura de información es casi inexistente y la poca que existe se da por acciones individuales dentro de TI.

Por lo que se corresponde con el nivel de madurez 0 (No Existente)

0 No Existente cuando

No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en la organización.

2.3.9 Análisis Resumen de Niveles de Madurez

Proceso COBIT	Nivel de Madurez					
	0	1	2	3	4	5
PO10		X				
AI2	X					
AI3		X				
PO1	X					
AI6		X				
PO9	X					
DS8		X				
PO2	X					

Tabla 3: Resumen de Análisis de Madurez

Según lo que se puede apreciar el CEC-EPN, y en particular su Coordinación de Gestión Tecnológica se manejan de una manera intuitiva sin ninguna planificación en muchos casos y en otros peor aún sin observar estándares mínimos de gestión.

La mitad de los procesos se encuentran en nivel 0 de madurez, lo que refleja la nula importancia que tanto la Coordinación, como la alta dirección le están brindando a estos procesos.

La otra mitad de los 8 procesos de COBIT escogidos está en un nivel de madurez 1 que refleja esfuerzos de la organización por organizar dichos procesos, pero que aún falta la ejecución y repetición de los mismos por el personal de TI, y su formalización.

En lo que respecta a la solución planteada en este trabajo de tesis, sería tratar de equiparar todos los procesos en un nivel de madurez 2 con el fin de que al menos la organización tengo un proceso repetitivo e intente documentar y formalizar sus procesos. En otras razones se considera esto porque existen muchos procesos de planificación que sin duda influyen en el resto de procesos que se necesitarían estructurar.

CAPÍTULO III

3. PROPUESTAS PARA LA MEJORA DE LA GOBERNABILIDAD DE TI

3.1 Planteamiento de metas para cada proceso.

Basado en los modelos de madurez y pensando en un avance equitativo de todos los procesos evaluados, se propenderá a conseguir un nivel 2 de madurez, en todos los procesos que se escogieron para el CEC-EPN. Por lo tanto a continuación se detallara las metas de cada proceso, en base a citas textuales de los niveles de madurez 2 de los 8 procesos de COBIT 4.1.[2]

3.1.1 PO1 Definir Plan Estratégico de TI

"La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva."

3.1.2 PO2 Definir la Arquitectura de la Información

"Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro

[2] Libro Cobit 4.1
IT Governance Institute

de la organización. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas. Los requerimientos tácticos impulsan el desarrollo de los componentes de la arquitectura de la información por parte de los individuos".

3.1.3 PO9 Evaluar y Administrar los Riesgos de TI

"Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos."

3.1.4 PO10 Administración de Proyectos.

"La alta dirección ha obtenido y comunicado la conciencia de la necesidad de la administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos proyecto por proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI.

Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción de cada gerente de proyecto."

3.1.5 AI2 Adquisición e implementación software.

“Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro de la operación de TI. El mantenimiento es a menudo problemático y se resiente cuando se pierde el conocimiento interno de la organización. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.”

3.1.6 AI3 Adquirir y Mantener infraestructura Tecnológica.

“No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe un ambiente de prueba por separado.”

3.1.7 AI6 Administración de Cambios

“Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio.”

3.1.8 DS8 Administrar la Mesa de Servicio y los Incidentes

"Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo."

3.2 Análisis de posibles soluciones

La metodología para el análisis de posibles soluciones estará basado en el reporte generado por el Instituto de Gobernabilidad de TI(ITGI), "Alineando COBIT 4.1, ITIL V3 e ISO /IEC 27002 en beneficio del negocio"; del mismo que se tomará las comparaciones entre los estándares y se destacará los más importantes puntos de vista de cada uno de ellos(COBIT 4.1[3], ITIL V3[4] e ISO /IEC 27002[5]), para luego compaginarlos con las metas propuestas para cada proceso y ver que se puede aplicar para que el CEC-EPN convierta todos los 8 procesos en un nivel de madurez 2, según COBIT.

[3] Libro COBIT 4.1 –IT Governance Institute

[4] http://wiki.es.it-processmaps.com
ITIL Service Manager- Miguel Guapaz(New Horizonts)
Tesis: "Desarrollo de un plan para el mejoramiento de la empresa SMARTWAVE S.A basado en el Marco de Referencia ITIL V3 en la prestación del servicio drive test(mediciones de campo) a operadoras móviles con redes GSM"- Jorge Cueva y Pablo Tipan

[5] Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información(ISO 27002)

3.2.1 Solución para PO1 (Definir Plan Estratégico de TI)

En este proceso de COBIT el PO1, se alinea con el proceso de Estrategia de Servicio de ITIL V3, a continuación se expondrá, a manera de resumen, que sugiere cada estándar y luego se intentará brindar una solución que demuestre un compendio de COBIT e ITIL.

COBIT dice:

- Establecer una evaluación de los casos de negocio que sea justa, transparente, repetible y comparable, incluyendo el valor financiero, el riesgo de no cumplir con una capacidad y el riesgo de no materializar los beneficios esperados.
- Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Asegurarse de que el rumbo del negocio al cual está alineado TI está bien entendido. Identificar las áreas en que el negocio (estrategia) depende de forma crítica de TI.
- Evaluación del Desempeño y la Capacidad Actual.
- Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe

ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

- Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos.

ITIL dice:

- Definir todo lo que tenga que ver con presupuestos, planificar costo beneficio de cada uno de los proyectos o acciones de TI.
- Evaluar la situación actual del proveedor de servicios en su sector del mercado. Como la evaluación de los servicios actualmente ofrecidos, las necesidades del cliente y la oferta de competidores.
- Definir las metas generales a las que aspira el proveedor de servicios durante su desarrollo e identificar qué servicios se ofrecen y a que clientes o sectores, partiendo de los resultados de la evaluación estratégica del servicio.
- Modificar el contenido del portafolio de servicios de modo que refleje cambios en la estrategia del servicio o en el estatus de los mismos.
- Definir, iniciar y controlar programas y proyectos requeridos para implantar la Estrategia del Servicio.
- Funcionar bajo el consejo de dirección de TI que establece la dirección y la estrategia de Servicios de TI. Incluye a miembros de la alta dirección de la

empresa y de TI. Este consejo revisa las estrategias de la empresa y de TI para asegurar que estén en concordancia.

Analizando lo que cada uno de los estándares que rigen sobre la planificación estratégica de TI, coinciden en que lo importante no está desarrollar el plan estratégico como tal sino más bien en desarrollar todas las actividades preliminares a la estrategia, por lo tanto a continuación se describen los productos o soluciones para este proceso, considerando siempre la meta planteada con anterioridad en este trabajo de tesis para este proceso.

1. Evaluar los servicios que actualmente se vienen brindando en la Coordinación de Gestión Tecnológica del CEC-EPN. Además analizar las necesidades empresariales y de los clientes potenciales. Un método de análisis podría ser a través de matrices FODA por ejemplo.

2. Definir el portafolio de servicios de la Coordinación de Gestión Tecnológica del CEC-EPN, donde además se definan las metas de la coordinación, tratando de alinear las mismas con la metas del negocio.

3. Involucrar a la alta gerencia en la planificación estratégica de TI, socializando los beneficios y oportunidades que se puede obtener de TI, a través de comunicaciones formales e informales o reuniones de promoción del proyecto.

Además de solicitar de la alta gerencia la asignación de autoridad para realizar y cumplir el plan.

4. Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.

5. Definir, iniciar y establecer métodos de control para programas y proyectos (planes tácticos de TI) que permitan cumplir el plan estratégico de TI. Para este ítem podría desarrollarse un pequeño sistema que realice un seguimiento de los proyectos y brinde alertas a los interesados, o podría mantenerse el control como hasta el momento con una hoja de Excel que incluya algunos campos como tiempos exactos, diferencia entre lo planeado y ejecutado, observaciones, etc.

3.2.2 Solución propuesta para PO2 (Definir la Arquitectura de la Información)

Sobre este proceso tiene bastante preponderancia lo que dice COBIT, lo que dice ITIL es escueto sobre este tema, de la misma forma ISO 2700 hace muy poca referencia a este proceso por lo que en su mayoría se tomara recomendaciones de COBIT.

Ahora se verá cuáles son las recomendaciones de COBIT:

COBIT dice:

- La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información
- Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte. El modelo debe garantizar que la información mantenga su integridad, sea flexible, funcional, rentable, oportuna, segura y tolerante a fallos.
- Mantener un diccionario de datos empresarial que incluya las reglas de sintaxis de datos de la organización.
- Establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y

destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o cifrado.

- Definir e Implementar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.

Analizando la información y considerando las metas planteadas para este proceso las posibles soluciones son:

1. Concientizar al personal de TI y a la alta gerencia sobre la importancia de plantear un modelo arquitectónico de la información.
2. Los datos tendrán que ser procesados y buscar que cualquier persona de TI puede usar dicha información.
3. Generar un proyecto a nivel táctico que tenga como objetivo el generar la arquitectura de la información del negocio.

3.2.3 Solución propuesta para PO9 Evaluar y Administrar los Riesgos de TI

En este proceso existen aspectos a tomar de COBIT, ITIL e incluso de ISO 27002. A continuación se expondrá (en síntesis) que recomienda cada uno de los estándares para este proceso.

COBIT dice:*

- Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders).
- Establecer un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.
- Identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Registrar y mantener los riesgos relevantes en un registro de riesgos.
- Evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.
- Desarrollar y mantener un proceso de respuesta. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.
- Priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

ITIL dice:

El proceso de Gestión de Riesgo abarca los siguientes subprocesos:

- Análisis del impacto y riesgo al negocio: Cuantificar el impacto de la pérdida de servicios y activos en una empresa y determinar la probabilidad de una amenaza o la vulnerabilidad ante la misma. El resultado es un registro de riesgos que deben atenderse según su prioridad.
- Evaluación de mitigación de riesgo requerida: Determinar donde se necesitan medidas de mitigación de riesgo e identificar a los responsables del riesgo, quienes están a cargo de la implementación el mantenimiento continúo.
- Monitorización de riesgo: Monitorear el progreso de la implementación de contramedidas, y tomar acción correctiva de ser necesario.

ISO 27002-2005 dice:

Relacionado con la seguridad de la información:

- Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización.
- La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).
- Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo.

- Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:
    - aplicar los controles apropiados para reducir los riesgos.
    - aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización.
    - evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.
    - transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Analizando la información y considerando las metas planteadas para este proceso las posibles soluciones son:

1. Desarrollar un procedimiento documentado que norme la elaboración del análisis, evaluación, tratamiento y planes de mitigación de los riesgos de TI, por supuesto con el aval de Dirección y la Coordinación de Calidad.
    - En lo que respecta al análisis se deberá cuantificar el riesgo en base a los servicios que podrían verse afectados. Como resultado se obtendrá una lista de riesgos.
    - En lo que respecta a la evaluación se deberá comparar la lista de riesgos que deberán validarse con los niveles de tolerancia al riesgo previamente definidos por la organización o TI, para así clasificarlos y ordenarlos por su

importancia, además deberá asignarse responsables de la implementación de los controles y seguimiento de los mismos.

- Y para finalizar el tratamiento y mitigación del riesgo deberá desarrollarse y mantenerse un proceso de respuesta a los riesgos. El proceso de respuesta a riesgos debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

2. Además a nivel de ejercicio inicial para probar el procedimiento TI, debería poder hacer una evaluación de todos los riesgos del área en general, es decir infraestructura, información, etc.
3. Es clave indicar que basados en las metas los proyectos que tendrán obligatoriedad de seguir el procedimiento a definir son los proyectos más importantes.

3.2.4 Solución propuesta para PO10 Administración de Proyectos.

Sobre este proceso se obtiene referencia en COBIT, alguna información indirecta se puede encontrar en ITIL pero es muy es queta.

COBIT dice:

- Mantener el programa de los proyectos. Coordinar las actividades e interdependencias de múltiples proyectos, administrar la contribución de todos los proyectos dentro del programa hasta obtener los resultados esperados.

- Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas en cada proyecto emprendido.
- La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores de proyectos, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa).
- Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global.
- Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto dentro del contexto del programa global de inversiones facilitadas por TI.
- Solicitar que al finalizar cada proyecto, los interesados del proyecto se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados.
- Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto (Ej.costos, cronograma, alcance y calidad) se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto
- Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común
- Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado del alcance del proyecto y cómo se

relaciona con otros proyectos dentro del programa global de inversiones facilitadas por TI.

Analizando la información y considerando las metas planteadas para este proceso las posibles soluciones son:

1. Generar un compromiso directo de la Dirección del CEC-EPN, que genere y administre los proyectos no solo de TI sino en un marco mas general, para ello se necesitará:
2. Capacitar al personal pertinente, en la administración y desarrollo de proyectos de cualquier tipo.
3. Crear un comité que sea el encargado de administrar los proyectos.
4. Establecer un marco para el manejo de proyectos dentro de TI.
5. Documentar en primera fase la administración de proyectos con el fin de tratar de que al menos los proyectos más importantes se rijan por la misma.
6. Propender que cada proyecto tenga un patrocinador definido y que cada proyecto se alinea con los objetivos de TI y del negocio.

3.2.5 Soluciones para AI2 Adquisición e implementación software.

En este proceso existen aspectos a tomar de COBIT, ITIL e incluso de ISO 27002. A continuación se expondrá (en síntesis) que recomienda cada uno de los estándares para este proceso.

COBIT dice:

- Tener aprobadas las especificaciones de diseño por gerencia para garantizar que el diseño de alto nivel responde a los requerimientos. Reevaluar cuando sucedan discrepancias significativas técnicas o lógicas durante el desarrollo o mantenimiento.
- Definir el criterio de aceptación de los requerimientos.
- Abordar la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados y en línea con la clasificación de datos, la arquitectura de la información, la arquitectura de seguridad de la información y la tolerancia a riesgos de la organización.
- En caso de cambios importantes a los sistemas existentes que resulten en cambios significativos al diseño actual y/o funcionalidad, seguir un proceso de desarrollo similar al empleado para el desarrollo de sistemas nuevos.
- Garantizar que la funcionalidad de automatización se desarrolla de acuerdo con las especificaciones de diseño, los estándares de desarrollo y documentación, los requerimientos de calidad y estándares de aprobación. Asegurar que todos los aspectos legales y contractuales se identifican y direccionan para el software aplicativo desarrollado por terceros.
- Desarrollar, Implementar los recursos y ejecutar un plan de aseguramiento de calidad del software
- Seguir el estado de los requerimientos individuales (incluyendo todos los requerimientos rechazados) durante el diseño, desarrollo e implementación, y aprobar los cambios a los requerimientos a través de un proceso de gestión de cambios establecido

- Desarrollar una estrategia y un plan para el mantenimiento de aplicaciones de software.

ITIL V3 dice:

- Planificar y coordinar los recursos para implementar una edición dentro de los parámetros de costo, tiempo y calidad estimados.
- Es importante evaluar y planificar los cambios y asegurar su implementación de forma eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio de TI
- Asegurar que las ediciones implementadas y los servicios resultantes cumplan las expectativas de los clientes, y verificar que las operaciones de TI sirvan de soporte a los servicios nuevos.
- Hacer que todas las aplicaciones y sistemas que proveen la funcionalidad necesaria para la prestación de servicios de TI estén disponibles. Este proceso incluye el desarrollo y mantenimiento de aplicaciones personalizadas, y la personalización de productos de vendedores de programados.
- Asegurarse que la integridad del ambiente de producción se encuentre protegido de las versiones que son puestas en libertad.
- Específicamente al respecto del software realiza actividades preventivas, de consistencia, de disponibilidad, seguridad y de legalidad (licencias).
- Estar seguros de que se pone en marcha únicamente aquellos “Releases” que son correctos, consistentes y autorizados
- Planificar y ejecutar un proyecto estructurado de la validación y el proceso de prueba.

- Identificar, evaluar y abordar los problemas, errores y riesgos a lo largo de la transición de los servicios

ISO 27002-2005 dice:

- Se debieran producir y mantener registros de auditoría de las actividades para ayudar en investigaciones futuras y monitorear el control de acceso.
- Donde sea necesario, el hardware y el software debiera de ser chequeado para asegurar que son compatibles con otros componentes del sistema.
- Llevar un registro de fallas y correcciones., en el desarrollo de software.
- El diseño e implementación de las aplicaciones debiera asegurar que se minimicen los riesgos de fallas en el procesamiento que lleven a la pérdida de la integridad.
- En general, la clasificación dada a la información es una manera rápida para determinar cómo se está manejando y protegiendo la información.
- Los gerentes debieran asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas debieran migrar a producción después de obtener la aceptación formal.
- Para los desarrollos nuevos importantes, la función de las operaciones y los usuarios debieran ser consultados en todas las etapas del proceso del desarrollo para asegurar la eficiencia operacional del diseño del sistema propuesto

- El acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debieran controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados. Para el código fuente del programa, esto se puede lograr controlando el almacenaje central de dicho código, preferiblemente en las bibliotecas de fuentes del programa.
- No se debieran fomentar modificaciones a los paquetes de software, se debieran limitar a los cambios necesarios y todos los cambios debieran ser estrictamente controlados.
- Se debiera controlar la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio.
- Cuando el software es abastecido externamente, se debieran considerar los siguientes puntos contratos de licencias, propiedad de códigos, derechos de propiedad intelectual.

En base a las metas planteadas con anterioridad para este proceso se podrían definir algunas soluciones:

1. Se necesita definir una metodología de desarrollo común para TI que sea implementada en todos los proyectos que involucren la adquisición o mantenimiento de software.
2. Es necesario no solo definir los temas que competen al proyecto o aplicación sino definir si las condiciones existentes en hardware y software se acoplan a cada uno de los módulos a implementar.

3. Si se adquiere la solución es importante que se defina claramente que aspectos deben ser revisados y que nivel de injerencia en la empresa proveedora tendrá el CEC-EPN.
4. Se debe definir las condiciones pos implementación en referencia a las seguridades que tendrá la aplicación y la información contenida en ella. Además crear ambientes apropiados para pruebas, desarrollo o producción y especificar cuál es el proceso de aceptación para cambiar de ambiente en ambiente, aparte de asegurar que nadie pueda por equivocación cambiar de ambiente.
5. Los niveles de aceptación o barreras de seguridad para las aplicaciones deben estar bien definidos en la organización deben en todo momento propender la protección de la información de la institución.
6. El mantenimiento de las aplicaciones debe ser formal al menos en los casos más importantes y con el tiempo debe proyectarse a desarrollar un procedimiento que rija el mantenimiento de las aplicaciones.
7. Los cambios realizados en los sistemas deben ser realizados de acuerdo a un procedimiento que norme los mismos asegurando en todo momento la calidad y continuidad del servicio de TI.

3.2.6 Soluciones propuestas para AI3 Adquirir y Mantener infraestructura Tecnológica.

Para este proceso se puede encontrar información en COBIT e ITIL, aunque ISO 27002-2005 también puede hallarse algunas recomendaciones que pueden ser importantes.

COBIT dice:

- Generar un plan para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión.
- Implementar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad.
- Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.
- Establecer el ambiente de desarrollo y pruebas para soportar la efectividad y eficiencia de las pruebas de factibilidad e integración de aplicaciones e infraestructura, en las primeras fases del proceso de adquisición y desarrollo.

ITIL dice:

- Trazar un plan para el desarrollo futuro del panorama tecnológico, tomando en consideración la Estrategia del Servicio.
- Ejecuta día a día las tareas rutinarias relacionadas con el funcionamiento de componentes de la infraestructura y aplicaciones. Este trabajo incluye la programación, backup y restore de actividades, impresión y administración así como el mantenimiento de rutina.
- Gestionar el medio ambiente físico donde la infraestructura de IT se encuentra. Gestión de Instalaciones o Facilidades incluye todos los aspectos de la gestión del medio ambiente físico, por ejemplo de energía y enfriamiento, el acceso al edificio y vigilancia del medio ambiente tanto físico como lógico.
- Asegurar que las ediciones implementadas y los servicios resultantes cumplan las expectativas de los clientes, y verificar que las operaciones de TI sirvan de soporte a los servicios nuevos.
- Planificar, programar y controlar el despliegue de las versiones de prueba en vivo y en ambientes. Asegurar que la integridad del ambiente de producción se encuentre protegido de las versiones que son puestas en libertad.

ISO 27002-2005

- Se debieran mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo.

- Se debiera diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas, sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo.

- Se debieran cumplir con todos los requerimientos impuestos por las pólizas de seguros.
- La organización debiera definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida.
- Se debieran definir y documentar las reglas para la transferencia de software del estado de desarrollo al operacional. El ambiente del sistema de prueba debiera emular el ambiente del sistema operacional lo más estrechamente posible.

Basado en las metas propuestas, de acuerdo a los modelos de madurez y lo que dicen los distintos estándares se pueden obtener las siguientes soluciones:

1. Fundamentar y socializar con la dirección la importancia de la infraestructura de TI e intentar promover.
2. Realizar un estudio y determinación de los riesgos en la infraestructura de TI, y procurar generar una planificación de las futuras adquisiciones de infraestructura basada en el estudio de riesgos.
3. Promover la creación de ambientes de pruebas no solo para software sino para hardware que puedan ser usados por la mayoría de proyectos de TI.

4. Elaborar un procedimiento documentado para el mantenimiento de la infraestructura que incluya pasos a seguir para reposición de partes y piezas, histórico de mantenimientos, y por último la evaluación y seguimiento de los mantenimientos.

3.2.7 Soluciones propuestas para AI6 Administración de Cambios

Este proceso tiene mucha referencia en COBIT, ITIL y la ISO 27002:2005, a continuación las referencias más relevantes:

COBIT dice:

- Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales.
- Garantizar que todas las solicitudes de cambio se evalúan de una estructurada manera en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios. Previo a la migración hacia producción, los interesados correspondientes autorizan los cambios.
- Establecer un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes, acerca del estatus del cambio

- Siempre que se implantan cambios al sistema, actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes. Establecer un proceso de revisión para garantizar la implantación completa de los cambios.

ITIL dice:

- El objetivo principal de Gestión del Cambio es permitir cambios beneficiosos que deben introducirse, con un mínimo de interrupción de servicios de IT.
- Además, se debe asegurar que los cambios están justificados, que se llevan a cabo sin interferir en la calidad del servicio TI, que están registrados, clasificados y documentados.
- Los cambios en la infraestructura TI se originan siempre por las siguientes fuentes: solución de errores conocidos, desarrollo de nuevos servicios, mejora de los servicios existentes y de imperativo legal.
- Las principales actividades de la Gestión de Cambios se resume en:
  - Monitorización y dirección del proceso de cambio.
  - Registro, evaluación y aceptación o rechazo de las RFCs (solicitudes de cambio) recibidas.
  - Convocar reuniones del CAB(consejo asesor de cambios), excepto en el caso de cambios menores, para la aprobación de las RFCs y la elaboración del FSC(lista de cambios planificados).
  - Coordinación del desarrollo e implementación del cambio.
  - Evaluación de los resultados del cambio y cierre en caso de éxito.

- Una vez aceptado el cambio se debe asignar una prioridad y categoría dependiendo de la urgencia y el impacto de la misma.

ISO 27002:2005 dice:

- En particular, se debieran considerar los siguientes ítems:

  - Identificación y registro de cambios significativos;
  - Planeación y prueba de cambios;
  - Evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad,
  - Procedimiento de aprobación formal para los cambios propuestos;
  - Comunicación de los detalles del cambio para todos las personas relevantes:
  - Procedimientos de emergencia y respaldo, incluyendo los procedimientos y responsabilidades para abortar y recuperarse de cambios fallidos y eventos inesperados.

- Se debieran documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información. Este proceso debiera incluir una evaluación del riesgo, análisis de los impactos del cambio y la especificación de los controles de seguridad necesarios asegurar que la notificación de los cambios en el sistema de operación sea provista con tiempo para permitir realizar las pruebas y revisiones apropiadas antes de la implementación.

- Cuando se cambian los sistemas de operación, se debieran revisar y probar las aplicaciones comerciales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad
- No se debieran fomentar modificaciones a los paquetes de software.

Basado en lo que mencionan los tres estándares y en las metas propuestas de acuerdo al modelo de madurez 2 Repetible pero Intuitivo de COBIT, se puede brindar las siguientes sugerencias:

1. Desarrollar una metodología para la gestión de cambios y la gestión de las configuraciones. Tomando en cuenta para ello:
2. Identificación y registro de cambios relevantes.
3. Monitorización y dirección del proceso de cambio.
4. Evaluación y aceptación o rechazo de las RFCs (solicitudes de cambio) recibidas.
5. Categorización y priorización del cambio.
6. Convocar reuniones del CAB(consejo asesor de cambios), excepto en el caso de cambios menores, para la aprobación de las RFCs y la elaboración del FSC(lista de cambios planificados).
7. Coordinación del desarrollo e implementación del cambio.
8. Evaluación de los resultados del cambio y cierre en caso de éxito.
9. Desarrollar métodos de evaluación para dicha metodología que permitan medir su grado de cumplimiento y ejecución. Hay que tener en cuenta que la

evaluación que se plantea no es a los cambios como tal sino al funcionamiento y aplicabilidad de la metodología a crearse en el ítem anterior.

3.2.8 Soluciones propuestas para DS8 Administrar la Mesa de Servicio y los Incidentes.

Si bien COBIT posee algunas mejores prácticas acerca de este proceso, sin duda ITIL es la principal referencia para el mismo. A continuación la información más relevante de estos dos manuales de mejores prácticas respecto del proceso DS8 Administrar la Mesa de Servicio y los Incidentes.

COBIT dice:

- Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI.
- Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información. Los incidentes deben clasificarse de acuerdo al negocio y a la prioridad del servicio y se debe mantener informados a los clientes sobre el estatus de sus consultas.

- Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el SLA.
- Cuando se resuelve el incidente la mesa de servicios debe registrar la causa raíz, si la conoce, y confirmar que la acción tomada fue acordada con el cliente.
- Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta

ITIL dice:

- El service desk está compuesto por personas que recogen todo tipo de peticiones e incidencias y que tienen la destreza técnica para contestar a prácticamente cualquier pregunta o queja.
- Centralizar todos los procesos de la Gestión de TI, mediante la recepción y control de peticiones de servicio, incidentes, consultas y solicitudes de cambio.

- Uno de los Service Desk más usados es el Service Desk local que se define con el objetivo de cumplir las necesidades locales del negocio. Las consideraciones principales para la implementación de un Service Desk local incluyen:
    - Procesos y procedimientos comunes
    - Asegurar la compatibilidad de hardware, software e infraestructura de red.

- Procesos de escalado comunes y uso de códigos de impacto, severidad, prioridad y estado; iguales en todas las localidades.
- Usar medidas de informes de gestión común.
- Usar una base de datos compartida.

- El objetivo de la Gestión de Incidentes es resolver cualquier incidente que provoque una interrupción en el servicio restaurando el servicio de la forma más rápida y eficaz posible. La Gestión de incidentes se focaliza únicamente en restaurar el servicio.
- La clasificación del registro debe realizarse por impacto y urgencia.
- El escalado puede ser de dos tipos: funcional(a un especialista de mas alto nivel y jerárquico(a una autoridad con mayor rango).
- La Gestión de Problemas tiene como objetivo identificar las causas subyacentes de fallos y recomendar cambios. Con esto intenta prevenir la recurrencia de incidencias.

Basado en la meta propuesta y las observaciones recogidas en los manuales de mejores prácticas se pueden plantear las siguientes sugerencias:

1. Desarrollar un proceso de gestión de mesa de ayuda, incidentes y problemas del CEC-EPN basado en Service Desk local propuesto en ITIL.
2. Definir niveles de soporte de acuerdo a la realidad del CEC-EPN.
3. Gestionar la capacitación de equipo de Tecnología para mejorar el nivel de expertis en temas específicos.

4. Evaluar adquisición de herramientas que soporten a la mesa de ayuda, como herramientas de acceso remoto, administración de incidentes y/o problemas, etc.
5. Socializar proyecto de mesa de ayuda con alta gerencia del CEC-EPN y con el personal que usa directamente los servicios de la Coordinación de Gestión Tecnológica.

3.3 Planteamiento de Proyectos

En el planteamiento de proyectos no se determinará un valor al trabajo que lo realicen los empleados del CEC-EPN, pues se considera que los mismos ya obtiene su remuneración, que no está relacionada estrictamente con el desarrollo de los proyectos, y solo se establecerá valores para otros rubros donde exista un egreso adicional.

Los tiempos en los que se incluyan los empleados del CEC-EPN se estimarán como jornadas a medio tiempo.

Además se entenderá que todos proyectos, como es obvio que se necesitaría computadores con software de ofimática, acceso a la información necesaria, etc.

3.3.1 Proyecto 1

Nombre Proyecto:

Desarrollo del plan estratégico de TI del CEC-EPN

Antecedentes:

La Coordinación de Gestión Tecnológica no tiene un plan estratégico de TI, nunca se ha desarrollado y apenas se cuenta con el plan estratégico de la organización.

Problemas percibidos:

Las metas de la Coordinación de Tecnológica no están claras, no se ven alineadas a las de la organización. El trabajo de TI se basa en planes tácticos, lo que muestra la poca planeación a largo plazo que se realiza en el área. Además el poco interés que la alta gerencia le ha brindado a estos temas es una de las principales razones para la situación antes mencionada.

Objetivos:

- Concientizar a la alta gerencia la importancia de una planificación a largo plazo de la Coordinación de Gestión Tecnológica.
- Interrelacionar objetivos organizacionales con los de TI.
- Analizar los factores directos e indirectos que inciden en el entorno de la Coordinación de Gestión Tecnológica.
- Determinar necesidades que los clientes internos principalmente.
- Generar objetivos para la Coordinación de Gestión Tecnológica con metas medibles, a largo plazo.
- Generar proyectos a corto plazo que apuntalen los objetivos antes mencionados.
- Definir mecanismo para medición de objetivos y planes.

Entregables:

- Planificación Estratégica de TI.

- Planes tácticos para los objetivos estratégicos de TI
- Plan de socialización del plan estratégico con la alta gerencia.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo (USD)**
Jornada de Socialización Inicial con alta gerencia	1	Coordinador de TI	S/V
Interrelacionar objetivos organizacionales objetivos TI	4	Coordinador de TI, Jefe de Calidad	S/V
Matriz FODA de TI	2	Coordinador de TI, Subcoordinador de: Hardware, Software y Telecomunicaciones	S/V
Levantamiento de información con áreas clientes	15	Subcoordinador de: Hardware, Software y Telecomunicaciones	S/V
Taller generación cuadro de mando integral	4	Coordinador de TI, Subcoordinador de: Hardware, Software y Telecomunicaciones	S/V
Generar planificación estratégica de TI	4	Coordinador de TI, Subcoordinador de: Hardware, Software y Telecomunicaciones	S/V
Generar planes tácticos	5	Coordinador de TI	S/V
Talleres de socialización del plan estratégico de TI con la alta gerencia.	2	Coordinador de TI	S/V
Definir mecanismo de seguimiento y medición.	3	Coordinador de TI, Jefe de Calidad	S/V
Tiempo Total	40	**Costo Total**	S/V

Tabla 4: Proyecto Planificación Estratégica

3.3.2 Proyecto 2

Nombre Proyecto:

Desarrollo de la Arquitectura de la Información

Antecedentes:

La Coordinación de Gestión Tecnológica no ha definido la arquitectura de la información del CEC-EPN, hay pequeños esfuerzos para realizar por ejemplo diccionarios de datos de algunos sistemas, pero no se han definido esquemas de información, niveles de acceso, clasificación de la información, etc, por lo que la arquitectura de la información es un tema que se le ha dado poca importancia y trascendencia en el CEC-EPN.

Problemas percibidos:

- Arquitectura de la información inexistente.
- Poca conciencia de lo importante de definir el manejo de la información, tanto del personal de TI como de la alta gerencia que no tiene conocimiento alguno sobre el tema.

Objetivos:

- Concientizar a la alta gerencia la importancia de la correcta clasificación de la información de toda la organización.
- Proponer una arquitectura de la información acorde a las necesidades del CEC-EPN.
- Definir proceso para elaborar la arquitectura de información para los sistemas y demás información futura.

Entregables:

- Plan de socialización de la arquitectura de la información.

- Modelo de arquitectura de información del CEC-EPN.
- Proceso para generar arquitectura de la información.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo (USD)**
Jornada de Socialización Inicial con alta gerencia	1	Coordinador de TI	S/V
Análisis de situación actual referente al manejo de la información.	2	Coordinador de TI, Subcoordinador de: Software y Hardware	S/V
Establecer esquema de clasificación de información.	4	Coordinador de TI, Subcoordinador de: Software y Hardware	S/V
Definir niveles de seguridad e integridad necesaria para la información.	3	Coordinador de TI y Subcoordinador de Hardware	S/V
Plantear arquitectura de la información.	5	Coordinador de TI, Subcoordinador de: Software, Hardware y Telecomunicaciones	S/V
Diseñar proceso para generar arquitectura de información.	7	Coordinador de TI, Subcoordinador de: Software, Hardware y Telecomunicaciones	S/V
Tiempo Total	22	**Costo Total**	S/V

Tabla 5: Proyecto Arquitectura

3.3.3 Proyecto 3

Nombre Proyecto:

Diseñar cultura de riesgo para el CEC-EPN

Antecedentes:

La Coordinación de Gestión Tecnológica primeramente, no ha realizado nunca una evaluación e identificación de sus riesgos, por lo que en pocas palabras no conoce a ciencia cierta su situación. La alta gerencia tampoco evidencia haber tenido el interés de instaurar una cultura definida de riesgo aun a nivel organizacional, que permita al CEC-EPN conocer que problemas podrían originarse y como podrían contrarrestarse para minimizar o desaparecer su impacto.

Problemas percibidos:

- Falta de conciencia de alta dirección sobre el tratamiento de riesgos incluso a nivel organizacional.
- No se ha evaluado, ni identificado los riesgos relacionados con TI.
- No existen planes de contingencia que busquen minimizar o eliminar los riesgos.
- No se ha definido un proceso que norme la administración del riesgo.

Objetivos:

- Concientizar a la alta gerencia sobre la importancia de instaurar una cultura de riesgo de la organización, sus beneficios y acciones a seguir.
- Realizar una identificación y evaluación de los riesgos de TI, que incluya una lista detallada de los riesgos, su clasificación, controles, responsables, niveles de tolerancia. Además deberá definirse medidas de mitigación para los riesgos encontrados.
- Definir un proceso que permite normar la administración del riesgo en TI, en proyectos, infraestructura, software, etc, y que al menos sea de obligatoriedad de los principales proyectos y acciones de TI.

Entregables:

- Plan de socialización de la cultura de riesgos.
- Evaluación de riesgos actuales de TI.
- Plan de mitigación de riesgos actuales.
- Proceso que norme la administración del riesgo en TI.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo (USD)**
Jornada de Socialización con alta gerencia	1	Coordinador de TI	S/V
Obtener lista de riesgos actuales y su clasificación.	5	Subcoordinador de: Hardware, Software, Telecomunicaciones	S/V
Definir controles, responsables y tolerancia de los riesgos actuales.	7	Coordinador de TI y Subcoordinador de Hardware	S/V
Estructurar medidas de mitigación para riesgos actuales.	15	Coordinador de TI, Subcoordinador de: Hardware, Software y Telecomunicaciones	S/V
Definir proceso para la administración del riesgo de TI. Que incluya la identificación, evaluación, respuesta y monitoreo del riesgo.	22	Subcoordinador de: Infraestructura y Software	S/V
Tiempo Total	49	**Costo Total**	S/V

Tabla 6: Proyecto Riesgos

3.3.4 Proyecto 4

Nombre Proyecto:

Administración de Proyectos

Antecedentes:

El CEC-EPN no cuenta con una política formal en el manejo de proyectos, por lo que los proyectos son llevados según la iniciativa de cada encargado. En la gran mayoría de casos no se usa una estrategia definida ni tampoco existe documentación sobre el desarrollo del proyectos, los proyectos solo se ejecutan en las distintas coordinaciones del CEC-EPN. La realidad en la Coordinación de Gestión Tecnológica no es la excepción y el manejo es muy similar aunque se ha dado ciertos pasos hacia la mejora, generando formularios de descripción de proyectos, entrega de productos, etc; pero sin duda aun eso no es suficiente por la desorganización que se observa en la planeación y ejecución de proyectos

Problemas percibidos:

- Falta de compromiso de la alta gerencia para generar políticas, o procesos para el manejo de proyectos a nivel institucional.
- Poca o ninguna capacitación en el manejo de proyectos o estándares que normen los mismos, por los empleados del CEC-EPN.
- Inexistencia de un proceso formal que norme el desarrollo de proyectos en el CEC-EPN.

- Deficiencias en la asignación de autoridad, dirección y ejecución en los proyectos generados por el CEC-EPN, poniendo énfasis en los relaciones con la Coordinación de Gestión Tecnológica.

Objetivos:

- Capacitar al personal en un estándar o metodología internacional para el manejo y administración de proyectos, por ejemplo PMBOK.
- Concientizar a la alta gerencia sobre la importancia de manejar una política o procedimiento común para el manejo y administración de proyectos.
- Generar proceso para la administración de proyectos en el CEC-EPN, con sus respectivos procedimientos, registros, formularios, etc; e intentar implementar con los principales proyectos de TI.

Entregables:

- 2 personas al menos, por Coordinación capacitados en PMBOK.
- Plan de sociabilización con alta gerencia sobre la necesidad de normar los proyectos en el CEC-EPN y específicamente en la Coordinación de Gestión Tecnológica.
- Generar un proceso común que norme el desarrollo de proyectos dentro del CEC-EPN, que incluya procedimientos, registros, formularios, y que topen temas importantes como asignación de autoridad, dirección y ejecución de los proyectos.

Tiempo, Responsable y Costo Estimado:

Actividad	Tiempo Estimado (días)	Responsable	Costo (USD)
Capacitación al personal en PMBOK	10	Empresa especializada – Coordinador de Talento Humano	2400
Jornada de Socialización con alta gerencia	1	Coordinador de TI	S/V
Foro con Coordinadores de todas las áreas del CEC-EPN, para determinar necesidades	2	Coordinador: Tecnología, Marketing, Lingüística, Talento Humano y Calidad, Capacitación, Virtual	S/V
Definir proceso que norme el desarrollo de proyectos en el CEC-EPN	20	Jefe: Calidad, Tecnología, Lingüística y Capacitación	S/V
Estructurar los formularios, registros	3	Jefe: Calidad, Capacitación y Lingüística.	S/V
Tiempo Total	36	**Costo Total**	2400

Tabla 7: Proyecto desarrollo proyectos

3.3.5 Proyecto 5

Nombre Proyecto:

Adquisición y Desarrollo de Software

Antecedentes:

El CEC-EPN desarrolla gran parte del software que utiliza, siendo muy pocas las soluciones que son adquiridas a terceros. Pero el desarrollo se basa netamente en el conocimiento e iniciativa de los desarrolladores, es decir no hay una metodología y/o proceso que norme el desarrollo de software por lo que el ciclo de desarrollo es un misterio y los productos por lo general no se acoplan a las necesidades de los clientes, ya sea porque no se hizo un correcto levantamiento de requerimientos, o porque al no

tener los requerimientos formalmente validados los clientes pueden cambiar en cualquier momento de parecer y modificar el producto final.

Los cambios efectuados en la mayoría de sistemas no son registrados, lo que deriva en sistemas totalmente parchados sin ningún orden ni seguimiento, por lo que se depende mucho del personal para saber que se hizo o no en los sistemas.

La planeación como tal del proyecto no existe, por ejemplo compatibilidad con software vs hardware, niveles de aceptación, seguridades, posteriores mantenimiento, etc, son aristas que no se toman en cuenta a la hora de plantear un proyecto de desarrollo.

Problemas percibidos:

- No existe proceso de diseño del software.
- No existe una verdadera planificación del software que analice tema como seguridad, rentabilidad, adaptabilidad, futuros requerimientos, etc.
- El poco manejo del proceso de cambios genera aplicaciones parchadas y poco funcionales.
- No se ha definido una metodología estándar que rija el desenvolvimiento de los desarrollos.
- En lo que respecta a la adquisición no existe nada documentado, por lo que la momento de la compra de un nuevo software los lineamientos surgen de iniciativas del Coordinador de TI de turno.

- El proceso o procedimiento que norme el desarrollo o adquisición es pobre o inexistente.
- El personal técnico está muy poco capacitado en el uso de metodologías, estándares, que diferencien realmente entre lo que es un desarrollo de software y lo que es simplemente programar.

Objetivos:

- Obtener asesoramiento sobre el uso de metodologías y estándares de desarrollo de software por parte de una empresa con experiencia en el ramo.
- Capacitar al personal en un estándar o metodología internacional para desarrollo y mantenimiento de software.
- Obtener asesoramiento en la implementación y construcción del proceso o procedimiento que norme el desarrollo y adquisición del software en el CEC-EPN.
- Apoyar al proceso de administración de cambios desde la perspectiva del desarrollo y mantenimiento de aplicaciones.
- Definir claramente ambiente de pruebas, y políticas claras que determinen cuando moverse de dicho ambiente a uno de producción.
- Establecer organizacionalmente niveles de aceptación, niveles de seguridad, procedimientos para el mantenimiento o actualización del software,etc.

Entregables:

- Propuesta de metodología y estándar a ser usado por la Coordinación de Gestión Tecnológica del CEC-EPN para el desarrollo de software, por parte de la empresa experta.
- 50% del personal de TI capacitado en una metodología para el desarrollo de software, adecuada a las necesidades del CEC-EPN.
- Definición de políticas de seguridad básicas, niveles de aceptación mínimos, y normativa para el mantenimiento de software.
- Definición de lineamientos básicos para realizar cambios en las aplicaciones.
- Creación de ambiente de pruebas y lineamientos que lo normen.
- Propuesta de proceso de adquisición y desarrollo de software, que incluya formularios, políticas, registros, manuales, procedimientos, y demás.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo (USD)**
Análisis y propuesta de metodología y estándar a ser usado	5	Empresa especializada – Subcoordinador de Software	300
Capacitar en metodología seleccionada al personal pertinente.	2	Instructor afin-Coordinador de TI	600
Foro para definir políticas de seguridad básicas, niveles de aceptación mínimos, y normativa para el mantenimiento de software	2	Coordinador de TI, Subcoordinador de: Software y Hardware	S/V
Definición de lineamientos básicos para realizar cambios en las aplicaciones.	1	Coordinador de TI, Subcoordinador de Software.	S/V
Creación de ambiente de pruebas y lineamientos que lo normen. Que incluya la compra de hardware apropiado y capacitación o compra de herramienta para el manejo de	6	Coordinador de TI, Subcoordinador de: Software y Hardware	3000

código.			
Consultoría para generar el proceso de adquisición y desarrollo de software, que incluya formularios, políticas, registros, manuales, procedimientos, y además de asesoramiento en temas varios.	20	Empresa Especializada-Coordinador de TI y Subcoordinador de Software	2000
Tiempo Total	36	**Costo Total**	5900

Tabla 8: Proyecto Software

3.3.6 Proyecto 6

Nombre Proyecto:

Adquisición y Mantenimiento de Infraestructura.

Antecedentes:

El CEC-EPN dispone de infraestructura en términos generales en buenas condiciones y trata en la medida de su posibilidades, tenerla actualizada constantemente, sin embargo la adquisición es desordenada, sin un plan visible o basada en metas estratégicas propuestas por la Coordinación de Gestión Tecnológica.

La infraestructura está divida en distintas sedes y en algunos de los casos en equipos críticos como servidores, no se almacenan en los lugares apropiados, poniendo en riesgo la disponibilidad de los servicios en el CEC-EPN.

Nunca se ha realizado un levantamiento de riesgos de infraestructura con el fin de determinar qué puntos críticos existen y proponer medidas de mitigación para contrarrestar los mismos.

Problemas percibidos:

- No existe un plan de adquisición de infraestructura.
- No existe una evaluación de riesgos a nivel de infraestructura.
- No existe un procedimiento que norme la adquisición de la infraestructura tecnológica del CEC-EPN.
- Falta de ambientes de pruebas dedicados ya sea para el desarrollo de aplicaciones como para la inclusión de nueva hardware en los equipos de cómputo o cualquier otra infraestructura tecnológica.
- Falta de procedimientos especificados para el mantenimiento de la infraestructura.

Objetivos:

- Generar un proceso que rija la adquisición y mantenimiento de la infraestructura.
- Generar planes estratégicos y tácticos para la adquisición y mantenimiento de la infraestructura.
- Realizar una evaluación de riesgos a nivel de infraestructura en el CEC-EPN.
- Crear ambiente de pruebas, y políticas claras que determinen el modo de uso de los mismos.

Entregables:

- Proceso que norme la adquisición y mantenimiento de infraestructura que incluya: formularios, políticas, registros, manuales, procedimientos, y demás.
- Plan estratégico y plan táctico referente a la adquisición de infraestructura, basado en un plan estratégico de la Coordinación de Gestión Tecnológica.

- Documentos que incluya la evaluación de riesgos relacionados con la infraestructura, además de medidas de mitigación claras para los riegos más importantes.
- Procedimiento documentado que norme el mantenimiento diario de la infraestructura del CEC-EPN.
- Ambiente físico de pruebas implementado y funcionado, además de un manual que norme su uso.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo (USD)**
Desarrollo de proceso de adquisición de infraestructura.	15	Coordinador de TI, Subcoordinador de Hardware y Subcoordinador de Telecomunicaciones.	S/V
Creación de plan estratégico de adquisición.	3	Coordinador de TI y Subcoordinador de Hardware	S/V
Creación de plan táctico de que ejecute el plan estratégico de adquisición.	2	Coordinador de TI, Subcoordinador de Hardware	S/V
Determinación de riesgos referentes a la infraestructura y definición de medidas de mitigación.	3	Coordinador de TI, Subcoordinador de Hardware y Subcoordinador de Telecomunicaciones.	S/V
Creación de ambiente de pruebas y lineamientos que lo normen. Que incluya servidores y software necesario.	7	Coordinador de TI, Subcoordinador de: Software y Hardware	4000
Generar procedimiento documentado que norme el mantenimiento y reparación de la infraestructura.	4	Coordinador de TI, Subcoordinador de Hardware y Subcoordinador de Telecomunicaciones.	S/V
Tiempo Total	34	**Costo Total**	4000

Tabla 9: Proyecto Infraestructura

3.3.7 Proyecto 7

Nombre Proyecto:

Gestión del Cambio

Antecedentes:

El CEC-EPN dispone de iniciativas relevantes en el manejo del cambio sobre todo a nivel de software en la institución con la inclusión de algunos formularios y registros que en teoría permiten organizar de mejor manera los cambios en las aplicaciones. La realidad es que muchos de los cambios no se registran o se documentan formalmente y los que se documentan se les da muy poco seguimiento posterior a su entrega. Además la documentación es muy pobre, y la cultura de cambio es inexistente, por lo que es muy difícil controlar la aplicación de los formularios o registros existentes

En lo que respecta a infraestructura no existe ningún proceso que norme el cambio por lo que cualquier cambio realizado no lleva ningún control o registro.

Problemas percibidos:

- No se registran la gran mayoría de cambios relacionados con software.
- Falta un proceso o procedimiento que norme la realización de cambio en lo referente a hardware.
- El proceso o procedimiento de gestión del cambio está constituido de un par de formularios y registros por lo que se hace prudente la reformulación del mismo,

además lo poco que existe esta muy poco difundido y entendido por el personal de TI.

- No existe un adecuado procedimiento de planeación, aprobación, implementación y seguimiento del cambio.
- No existen esfuerzos para normar la configuración de los equipos y demás sistemas informáticos.

Objetivos:

- Generar un proceso más completo que incluya todas las áreas que efectúan cambios en TI, para así normarlas y generar una verdadera cultura de cambio, este proceso deberá contemplar el ciclo de vida de todo el cambio, es decir planeación, aprobación, implementación y seguimiento.
- Generar un procedimiento que norme la configuración de los equipos y sistemas informáticos.
- Socializar el procedimiento dentro de los integrantes de la Coordinación de Gestión Tecnológica.

Entregables:

- Proceso que norme la administración del cambio en la Coordinación de Gestión Tecnológica, que considere para aquello el ciclo de vida del cambio y busque integrar todos los componentes de TI.
- Procedimiento que norme la configuración de los equipos y sistemas informáticos.

- Socialización de proceso global para la administración del cambio.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo**
Analizar documentación existente referente a la gestión del cambio.	3	Coordinador de Ti, Coordinador de Calidad	S/V
Foro para definir metodología de cambio que tome en cuenta por ejemplo identificación y registro del cambio, monitorización, evaluación y aceptación, categorización y priorización, creación de comité de cambio, cierre.	3	Coordinador de TI, Subcoordinador de: Hardware, Telecomunicaciones y Software.	S/V
Reformulación de proceso de cambio	12	Coordinador de Ti, Coordinador de Calidad	S/V
Creación de procedimiento de configuración.	3	Coordinador de Ti, Coordinador de Calidad	S/V
Socialización de proceso de administración del cambio.	2	Coordinador de TI	S/V
Tiempo Total	23	**Costo Total**	S/V

Tabla 10: Proyectos Administración Cambio

3.3.8 Proyecto 8

Nombre Proyecto:

Administración de Mesa de Ayuda

Antecedentes:

El CEC-EPN realiza labores de soporte técnico tanto a clientes internos (personal administrativo) y el cliente externo (participantes de cursos de capacitación). En ninguno de los casos, el soporte técnico es guiado por algún procedimiento que

permita estandarizar el servicio. En todos los casos el soporte se brinda por iniciativa propia del personal de la Coordinación de Gestión Tecnológica.

Las funciones de soporte no están segregadas a determinado personal dentro de TI, ni se dispone de una mesa de ayuda que administre el soporte inicial. Tampoco se cuenta con un sistema informático que permita a agilizar el registro de los casos de soporte o tener una estadística de los mismos.

Problemas percibidos:

- No existe ningún proceso que norme el soporte técnico en el CEC-EPN.
- No se ha definido una área específica de brinde el soporte dentro de la Coordinación de Gestión Tecnológica, así como tampoco niveles de soporte ajustados a su realidad.
- El personal de TI está muy poco capacitado en temas como mesa de ayuda, gestión de incidentes, gestión de problemas, etc, por lo que su desempeño es netamente empírico.
- Todo el manejo del soporte no se ha sistematizado por lo que el manejo de la información causa muchos inconvenientes.
- El soporte que brinda la Coordinación de Gestión Tecnológica está muy poco socializado, hay muy poca retroalimentación de los clientes.

Objetivos:

- Generar un proceso más completo que incluya todas las áreas que efectúan cambios en TI, para así normarlas y generar una verdadera cultura de cambio.

- Generar un procedimiento que contemple el ciclo de vida de todo el cambio, es decir planeación, aprobación, implementación y seguimiento.
- Generar un procedimiento que norme la configuración de los equipos y sistemas informáticos.
- Socializar el procedimiento dentro de los integrantes de la Coordinación de Gestión Tecnológica.

Entregables:

- Proceso que norme la administración del cambio en la Coordinación de Gestión Tecnológica, que considere para aquello el ciclo de vida del cambio y busque integrar todos los componentes de TI.
- Procedimiento que norme la configuración de los equipos y sistemas informáticos.
- Socialización de proceso global para la administración del cambio.

Tiempo, Responsable y Costo Estimado:

Actividad	**Tiempo Estimado (días)**	**Responsable**	**Costo (USD)**
Foro para determinar necesidades de cada una de las áreas del CEC-EPN con respeto al soporte técnico	2	Director y Subdirector, Coordinador de: TI, Marketing, Lingüística, Capacitación, Virtual, Financiero, Calidad Talento Humano	S/V
Capacitación al personal en temas relacionados con soporte técnico y mesa de ayuda,	20	Empresa Especializada-Coordinador de TI	3000

Determinar organización interna de TI y niveles de soporte a brindarse.	3	Coordinador de TI, Subcoordinador de: Hardware, Telecomunicaciones y Software.	S/V
Generación del proceso de Soporte Técnico y mesa de ayuda	15	Coordinador de Ti, Coordinador de Calidad, Subcoordinador de: Hardware, Telecomunicaciones y Software.	S/V
Analizar factibilidad e implementación de sistema de administración de mesa de ayuda	5	Coordinador de Ti, Subcoordinador de Hardware	3000
Socialización de proceso de soporte técnico y mesa de ayuda con los involucrados	1	Coordinador de TI	S/V
Tiempo Total	46	**Costo Total**	6000

Tabla 11: Proyecto Mesa de Ayuda

CAPITULO IV

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El CEC-EPN y específicamente Coordinación de Gestión Tecnológica, tienen perspectivas de crecimiento importantes, buscando guiar su desarrollo en lo que manda el estándar de calidad ISO 9001, mas sin embargo dicha Coordinación ha dejado de un lado el mejorar específicamente el gobierno de TI al no regirse por un estándar de mejores prácticas. Esto ha hecho que un área tan importante para la organización se maneja de una manera informal.

- Se pudo determinar que los procesos que en mayor medida usan los servicios de la Coordinación de Gestión Tecnológica son: *Publicidad y Ventas* y *Prestación y Evaluación del Servicio*. Estos procesos abarcan algunas coordinaciones como las de Marketing, Lingüística e Intercambios de Culturales y Capacitación y Consultoría. Los servicios que se requieren son desarrollo de sistemas, adquisición y mantenimiento de infraestructura, soporte técnico a usuarios internos y sobre todo externos, etc.

- Los procesos donde la Coordinación de Gestión Tecnológica brinda sus servicios de mayor criticidad son también los procesos productivos y que se incluyen en las actividades principales de la organización, por lo que sin duda el

mejoramiento y la estandarización de los procesos de TI, se verá reflejados directa o indirectamente en el producto final.

- A través de un proceso de análisis que partió de la cadena de valor del CEC-EPN, prueba expresa de que se ajusta sus necesidades organizacionales, y que incluyo el procesamiento de entrevistas, análisis de riesgos, métodos deductivos, entre otros; se determinó que la mayor parte de actividades o procesos críticos que maneja la Coordinación de Gestión Tecnológica, se acoplan a estos 8 proceso de COBIT, que son:

    - DS8 Administrar la Mesa de Servicio y los Incidentes
    - AI2 Adquirir y mantener software aplicativo
    - PO1 Definir un Plan Estratégico de TI
    - AI3 Adquirir y mantener infraestructura tecnológica.
    - PO10 Administrar los proyectos de TI
    - PO9 Evaluar y Administrar los Riesgos de TI
    - AI6 Administrar Cambios
    - PO2 Definir la Arquitectura de la Información.

- Como meta principal de este trabajo de tesis se consideró, el poder plantear al CEC-EPN, un conjunto de proyectos que le ayuden a mejorar su gobernabilidad de TI, a través del crecimiento de la madurez de sus procesos. Estos proyectos nacieron de un análisis de lo que proponían estándares como COBIT 4.1, ITIL V3 e ISO 27002 versus lo que se podía acoplar a la realidad de la institución y

sobre todo a las metas planteadas, que significaron plantear un escenario donde todos los 8 procesos puedan llegar a un nivel de madurez 2, según COBIT.

4.2 RECOMENDACIONES

- La alta gerencia del CEC-EPN debería motivar la acogida de manuales de mejores prácticas de TI, con el fin de consolidar un área en la que hoy por hoy está basando su desarrollo y crecimiento, y que luego del análisis se ha visto muy poco organizada.

- La Coordinación de Gestión Tecnológica debería implementar los proyectos planteados con la finalidad de mejor su gobernabilidad. En muchos casos no se necesita de grandes inversiones, como se puede notar en cada uno de los 8 proyectos, sino más bien una iniciativa organizacional que busque el mejoramiento y la estandarización. Los proyectos planteados tendrían una duración de 286 días, con un costo total de $ 18.300.

- La alta gerencia del CEC-EPN y la Coordinación de Gestión Tecnológica, deberían promover activamente la difusión de procesos, con el fin de que toda la organización se involucre y entienda el verdadero valor de las iniciativas.

- La alta gerencia del CEC-EPN y la Coordinación de Gestión Tecnológica deberían promover la capacitación continua sobre estos temas, buscando así

obtener personal calificado que sea un verdadero apoyo al momento de promover iniciativas de mejora.

- Si bien primero debería comenzarse con la mejora en los 8 procesos de COBIT donde se involucran las actividades más críticas de la Coordinación de Gestión Tecnológica, quedaría pendiente analizar todos los procesos que plantea COBIT y verificar que grado de cumplimiento le está dando el CEC-EPN a sus mejores prácticas.

BIBLIOGRAFÍA

IT Governance Institute. (2007). *COBIT 4.1*. Recuperado de http://www.isaca.org/knowledge-center/cobit/documents/cobit4.1spanish.pdf

Cueva J. W. Tipán P. A. (2010). *Desarrollo de un Plan para el Mejoramiento de la Empresa Smartwave S.A basado en el Marco de Referencia Itil V3 en la Prestación del Servicio Drive Test(Mediciones de Campo) a Operadoras Móviles con Redes GSM*. Tesis de Pregrado no publicada. Facultad de Electrónica y Telecomunicaciones, Escuela Politécnica Nacional, Quito, Ecuador.

IT Governance Institute. (2007). *IT Assurance Guide using COBIT*. Recuperado de http://www.isaca.org/Knowledge-Center/cobit/Documents/IT-Assurance-Guide-Research.pdf

Zavala S. (2009). *Guía a la redacción en el estilo APA, 6ta edición.*

Talledo M. J. (2008). *Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK) Cuarta Edición*. EEUU.

Universidad de Piura. (2011). *Guía para la elaboración y presentación de trabajos de investigación, según el estilo APA (American Psychological Association).*

Recuperado de http://www.biblioteca.udep.edu.pe/wp-content/uploads/2011/02/Guia-ElabCitas-y-Ref-Estilo-APA.pdf

Guapas M., (2008), *ITIL Service Manager & ITIL Foundation V3*, Presentada en el Curso ITIL V3, New Horizonts, Quito, Ecuador.

Procesos ITIL (2011). Recuperado de http://wiki.es.it-processmaps.com

OSI. (2005). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información (ISO 27002)*. Recuperado de http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

ABREVIATURAS Y ACRÓNIMOS

TI: Tecnologías de la Información

TIC: Tecnologías de la información y comunicación.

CEC-EPN: Centro de Educación Continua de la Politécnica Nacional.