UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 9

IMPLEMENTACIÓN DEL MODELO COBIT EN EL PROCESO PRODUCTIVO DE LA CASA DE AUTORÍA DVD DE LA UCI

Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas

Autores: Ariesky Sotolongo Expósito

Sandro Cruz Pupo

Tutor(es): MSc. Isabel María Martínez García

Lic. Yaria Aguilera Matos

Ciudad de La Habana / julio de 2007 / Año 49 de la Revolución

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Ariesky Sotolongo Expósito
_____

Isabel M. Martínez García
_____

Sandro Cruz Pupo
_____

Yaria Aguilera Matos
_____

DEDICATORIA

Es difícil dedicar tan poco a los que han dado tanto por mi futuro:

A mi madre, por todo su amor y a quien va dedicado todo mi esfuerzo.

A mi padre, por su apoyo incondicional.

A mis hermanos, que son los mejores del mundo.

A mis abuelos, que han sido como mis padres.

A mi Lisy, que ha sido lo mejor que me ha podido ocurrir en la vida.

A Mercy y Armando, por saber ganarse un lugar en mi corazón.

A toda mi familia, que me ha apoyado siempre y ha hecho tanto por mí.

A mi amigo Yoanky, que me ha ayudado a pilotear esta nave como el mejor de los navegantes.

A mi amigo Jose, quién es para mí como un hermano.

A mis padres de afecto, Ofelia, Israel, Yanet, Alexis, Damaris, Vilma y Xenia.

A mi tutora Isa, que me ha soportado tanto pero a quién quiero mucho.

A mi maestra Yaria, por todos los 3 en Administración de Empresa.

A mi tropa de UCITeVe, que extrañaré siempre.

A todos aquellos que forman parte de este logro.

Ariesky Sotolongo Expósito

DEDICATORIA

A mis abuelos, Eremilda y Manuel.

A mis padres, Mirtha y César.

A mis tías, Marta y Martha, a Asalia y a Mandy.

A mis amigos Liskeny, Alberto, Frank y a Yaser por su apoyo.

Sandro Cruz Pupo

AGRADECIMIENTOS

Nancy Vandama (ETECSA)

Manuel Rodríguez Pantoja (UCI)

Yaylén Carrazana Del Llano (UCI)

Adrian Enrique De Huelbes Ocaña (UCI)

Alina Ruiz Jhones (UCI)

Roberto Francisco Peña Ronda (Funcionario C.E)

Jorge Angel Marimón Martínez (UCI)

DATOS DE CONTACTO

MSc. Isabel M. Martínez García

Centro de Trabajo: Ministerio de la Informática y las Comunicaciones

Cargo: Jefe de Seguridad y Auditoría Informática MIC

Categoría Docente: Asistente

Asignatura que imparte: Teleinformática.

Grado Científico: Máster en Sistemas de Radiocomunicaciones Máster en Administración de Negocios

Participación en eventos: UCiencia 2005, Uciencia 2006, Informática 2005, Informática 2007, Cursos optativos

Lic. Yaria Aguilera Matos.

Centro de trabajo: Universidad de Ciencias Informáticas

Categoría docente: Instructora.

Asignatura que imparte: Administración de Empresas y Comercio Electrónico.

Aspirante al grado científico de máster en Administración de Empresas.

Línea de investigación: Finanzas, Recursos Humanos.

Participación en eventos: UCIENCIA 2005, UCIENCIA 2006, Universidad 06, Fórum de Ciencia y Técnica 2005 y 2006, Eventos convocados por la ANEC (Evento de la Mujer Economista , Talleres de Liderazgo y Recursos Humanos), Jornada Científica de la Escuela de Altos Estudios de Hotelería y Turismo.

OPINIONES

Teniendo en cuenta la creciente vulnerabilidad y el amplio espectro de amenazas, relacionadas con la seguridad informática, el incremento y los costos de las inversiones en las tecnologías y el potencial que tienen las tecnologías de la información para cambiar radicalmente las practicas del negocio de las organizaciones, crear nuevas oportunidades y reducir costos. Además el empeño de la administración en lograr que todos los individuos involucrados en el uso, explotación de la tecnología tengan bien definidos sus roles y estén orientados hacia el negocio. Se ha podido constatar en la práctica la utilidad de la implementación del método Cobit en las Casas de Autoría DVD de la UCI, entidad de nueva creación que ha requerido de herramientas como las brindadas por este método para orientar estratégicamente el negocio, establecer las metodologías de trabajo correspondientes, identificar los procesos fundamentales, diseñar los roles, establecer los flujos de información y los procedimientos en las aéreas de trabajo, dotando a la Dirección de los medios necesarios para garantizar el éxito y las buenas prácticas del negocio.

Los diplomantes han tenido el mérito de ser fundadores del proyecto de las Casas de Autoría DVD, lo cual ha sido un ejercicio práctico, donde han puesto a prueba su talento, tesón y empeño en llevar a cabo esta tarea, desde la selección de la tecnología instalada hasta el diseño del flujo productivo y los roles, de una entidad que hoy ya brinda sus frutos, poniendo las mejores tecnologías de la Informática en función de los más pobres y desposeídos del mundo, dando a la luz el Programa de alfabetización Yo, si puedo a varios países hermanos como Brasil, Uruguay, Panamá y Colombia.

Manuel Rodríguez Pantoja
Director Autoría DVD UCI

OPINIÓN DE LAS TUTORAS

Las tutoras del presente Trabajo de Diploma consideran que durante su ejecución los estudiantes mostraron las cualidades que a continuación se detallan.

Muy alta independencia así como originalidad, creatividad y laboriosidad en la confección de su trabajo de diploma el cual asumieron con un alto nivel de responsabilidad cumpliendo sus objetivos y tareas necesarias en tiempo y con calidad.

Muy alta laboriosidad que dio como resultado la posibilidad de adquirir y aplicar conocimientos de buenas prácticas internacionales en el trabajo con las Tecnologías de la Información, tema que da sus primeros pasos en Cuba y que pudiera tomarse a la Casa de Autoría de DVD como referencia nacional. Además el resultado final permitirá que una entidad del estado dedicada al apoyo de obras de la Batalla de Ideas que desarrolla nuestro país, a pesar de ser un negocio nuevo, se lleve a cabo un proceso productivo optimizando el uso de la tecnología y bajo los estándares y normas internacionales que le proporcionan un valor agregado al producto final.

Durante la etapa de desarrollo muchos fueron los obstáculos a sortear pero el empeño puesto por los autores, así como la capacidad de escuchar, reflexionar, rectificar y dialogar, permitieron llevar a feliz término este trabajo que es solo el inicio de una continua superación y perfeccionamiento.

Por todo lo anteriormente expresado consideramos que los estudiantes están aptos para ejercer como Ingenieros Informáticos; y proponemos que se le otorgue al Trabajo de Diploma la calificación de 5 puntos.

RESUMEN

La Casa de Autoría DVD de la UCI, puesta en funcionamiento recientemente, cuenta con un gran número de recursos tecnológicos muy costosos. El personal que allí labora tiene muy poca experiencia en el uso de estas tecnologías. Sin embargo, entre sus misiones está el abastecer de material audiovisual a la planta de multicopiado de CD/DVD Luz Producciones Marianao en su etapa de puesta a punto, que precisa de materia prima de calidad óptima. El flujo productivo diseñado no incluye totalmente las mejores prácticas para el uso de las tecnologías de la información (TI), y adolece de un marco de controles bien organizado que permita medir el desempeño de los procesos y asegurar un máximo rendimiento de la tecnología que conlleve al cumplimiento de los objetivos y metas de la entidad. Por tanto es necesario dotar al proceso productivo de la Casa de Autoría DVD de un buen gobierno de TI, que permita a la dirección asegurarse de que las TI agregan valor al negocio y sostienen las estrategias y objetivos de la Casa. Esto se puede lograr mediante una implementación, ajustada a las necesidades de la Casa, del estándar COBIT (Objetivos de Control para la Información y las Tecnologías relacionadas), ya que el mismo se enfoca en el cumplimiento de los objetivos del negocio, observándolo como un todo, estableciendo un puente con las necesidades de control y los aspectos técnicos, y administrando los riesgos asociados a TI. Para la Universidad, podría ser un primer paso para la implementación de COBIT a un nivel más abarcador, ya que el mismo se está comenzando a utilizar en nuestro país con excelentes resultados.

PALABRAS CLAVE

Casa de Autoría DVD, Gobierno de TI, Buenas prácticas de TI, Cobit.

TABLAS Y FIGURAS

TABLAS:

FIGURAS:

ÍNDICE

INTRODUCCIÓN

Desde que en los años 80 la compañía norteamericana IBM lanzara al mundo su modelo PC, el uso de las computadoras para la gestión de la información se ha generalizado a un nivel inimaginable. En el mundo de hoy, casi la totalidad de las empresas y organizaciones, dependen de las tecnologías de la información (TI) para realizar sus funciones. Se hace necesario entonces el manejo correcto de la información y las tecnologías, de forma que éstas no se conviertan en un obstáculo para los usuarios y en cambio contribuyan al avance y cumplimiento de los objetivos y metas.

Tal es así, que en la actualidad los datos y las tecnologías de la información son considerados por muchas empresas como sus activos más valiosos. La administración efectiva de la información y de las tecnologías relacionadas, así como de los riesgos que acarrea, son elementos críticos para el éxito y la supervivencia de las organizaciones.

Este trabajo consiste en un análisis de las diversas soluciones que existen en el mundo para el control y gobierno de tecnologías de la información, y el desarrollo de estrategias acordes con los estándares internacionales a implementar en el proceso productivo de la Casa de Autoría de DVD de la Universidad de las Ciencias Informáticas, (en lo adelante “la Casa”).

La Casa, enfrenta un gran volumen de producción, por la necesidad que existe de difusión de materiales audiovisuales para los programas educativos.

Los subprocesos que se deben realizar para concretar un proyecto DVD son complejos, altamente interdependientes y además muy ligados a la tecnología.

Por la importancia que representa para el país y para los millones de personas que se beneficiarán de los programas audiovisuales y otros contenidos estratégicos, la Casa debe funcionar con eficiencia y alcanzar un nivel de competitividad que permita obtener productos de alta calidad.

Definición del problema:

De la situación problemática antes enunciada se define el siguiente **problema**: Ausencia de buenas prácticas y gobierno de TI en el proceso productivo de la Casa de Autoría de DVD.

Se define como **Objeto de estudio:**

La implementación del modelo CobiT en pequeñas y medianas empresas (PyME).

Del objeto de estudio analizado se ha definido como **Campo de acción:**

El proceso productivo de la Casa de Autoría de DVD de la UCI.

Objetivo general

Implementar el estándar internacional para las tecnologías de la información Cobit, en el flujo de proceso de la Casa de Autoría de DVD.

Objetivos específicos

- Diseñar y describir la metodología para la implementación del marco de controles de TI.
- Definir el nivel de madurez del proceso productivo en cuanto a los controles de TI.
- Elaborar un conjunto de políticas y guías para el correcto uso de las TI en el proceso productivo de la Casa de Autoría de DVD de la UCI.

Idea a defender:

La implementación del estándar internacional para las TI COBIT en el proceso productivo de la Casa de Autoría asegurará las mejores prácticas y buen Gobierno de TI que permitirá alcanzar los objetivos de la organización, añadiendo competitividad, eficiencia y seguridad.

Métodos científicos empleados

Se utiliza como estrategia de investigación la Investigación explicativa o experimental. Se hace uso de los métodos teóricos: histórico-lógico, hipotético-deductivo, analítico-sintético, de los métodos empíricos: la observación y de los métodos particulares: la entrevista.

Aportes prácticos esperados del trabajo

Los posibles resultados que se esperan obtener con este trabajo son un correcto uso de los recursos informáticos en el proceso productivo de la Casa, a tono con las mejores prácticas internacionales, mediante la acertada aplicación de controles, que permita llevar a cabo las misiones y el cumplimiento de sus objetivos.

1. CAPÍTULO I. LOS ESTÁNDARES INTERNACIONALES PARA LAS TI. EL PROCESO DE AUTORÍA DE DVD

1.1 Introducción

En este capítulo se hace una descripción de la Casa, su surgimiento y organización interna, y de las tecnologías instaladas. Además se detalla la situación problemática existente y se hace un recorrido por los principales estándares internacionales para las tecnologías de la información.

1.2. Conceptos fundamentales

A continuación se relacionan los elementos conceptuales que son necesarios conocer para el entendimiento del dominio.

Definición de DVD

(Digital Versatile/Video Disc) Disco Versátil/Video Digital. Formato de almacenamiento digital de datos. Tienen el mismo tamaño físico que un CD, 12 cm de diámetro, u 8 cm para los mini; aunque almacenan mucha más información. Los DVD guardan los datos utilizando un sistema de archivos denominado UDF, el cual es una extensión del estándar ISO 9660, usado para CD de datos.

Un DVD de capa simple puede guardar hasta 4,7 gigabytes (se le conoce como DVD-5).

Discos DVD±R DL (DVD-9): una cara, capa doble. 8.5 GB.

Discos DVD±R/RW (DVD-10): dos caras, capa simple en ambas. 9.4 GB.

Discos DVD+R (DVD-18): dos caras, capa doble en ambas. 17.1 GB.

Según el contenido, los DVD pueden clasificarse en:

DVD-Video: Películas (vídeo y audio).

DVD-Audio: Audio de alta definición.

DVD-Data: Datos cualesquiera.

Según su capacidad de regrabado:

DVD-ROM: Sólo lectura, manufacturado con prensa.

DVD R: Grabable una sola vez.

DVD RW: Regrabable.

DVD R DL: Grabable una sola vez de doble capa

DVD RW DL: Regrabable de doble capa.

La velocidad de transferencia de datos de una unidad DVD está dada en múltiplos de 1.350 kB/s, lo que significa que una unidad lectora de 16x, permite una transferencia de datos de 16 x 1.350 = 21.600 kB/s (21,09 MB/s). Como las velocidades de las unidades de CD se dan en múltiplos de 150 kB/s, cada múltiplo de velocidad en DVD equivale a nueve múltiplos de velocidad en CD. En términos de rotación física (revoluciones por minuto), un múltiplo de velocidad en DVD equivale a tres múltiplos de velocidad en CD, así que la cantidad de datos leída durante una rotación es tres veces mayor para el DVD que para el CD, y la unidad de DVD 8x tiene la misma velocidad rotacional que la unidad de CD 24x.

Autoría de DVD

Serie de procesos por los que debe pasar un material audiovisual para finalmente llegar al soporte DVD. Es la etapa posterior al telecinado y digitalización. Informáticamente, se procesan el conjunto de archivos de imagen (MPEG-2) y de audio (Dolby Digital, DTS o LPCM), se crean los menús, se añaden los extras, animaciones, se programan y prueban todas las interacciones del usuario. El resultado es una "imagen" en el disco duro de una computadora, de lo que finalmente se grabará en el disco editado.

Consejo de Dirección:

Lo constituye el primer nivel de la célula organizativa, Director, Subdirector, Jefes de Grupos y Coordinadores de Producción. Esto se muestra en el Anexo 1.

1.3. La Casa de Autoría de DVD de la UCI

Desde el mismo triunfo de la Revolución cubana, nuestro país se encuentra bajo un férreo bloqueo por parte del gobierno de Estados Unidos. En medio de esta guerra mediática, y dada la necesidad e importancia de potenciar el uso y difusión de materiales audiovisuales, como soporte de los principales Programas de la Batalla de Ideas, no sólo en Cuba, sino también en otros países, se creó en la Universidad de las Ciencias Informáticas la Casa de Autoría de DVD, como soporte inicial de la planta de multicopiado de DVD “Luz Producciones”, Marianao.

1.3.1. Surgimiento y descripción general

Cuba, máximo exponente de la solidaridad mundial en los campos de la salud y la educación, lleva a cabo disímiles programas educativos en aras de reducir los niveles de analfabetismo en el mundo. A raíz del desarrollo de estos programas se decide crear una planta de multicopiado de VHS, la indicación que se dio por la dirección del país, era buscar personas que no estaban familiarizadas con esta actividad, que no conocían nada de este sistema, y que no tenían vicios laborales, entonces se decidió buscar 4 ingenieros por especialidad, automática, telecomunicaciones, industrial y mecánica, 4 futuros ingenieros que todavía no se habían graduado pero con especialidades afines al VHS.

Para la replicación de contenidos audiovisuales se debe pasar por un proceso normal de desarrollo, primero el VHS, se recupera la inversión, se adquiere experiencia y comienza la migración a soportes más eficientes y de mayor calidad como es el CD y el DVD. Por este desarrollo natural se decide la creación en el país de una planta de multicopiado de CD y DVD, se realizaron los estudios de factibilidad a partir de los compromisos que tenía Cuba en VHS y se dio la posibilidad de pensar en la cantidad de tecnología a adquirir para asumir ciertas producciones en este nuevo soporte audiovisual.

Para completar esta idea se necesitaba de la materia prima fundamental del proceso, la autoría de materiales para replicarlos a gran escala en la planta, la mayoría de las empresas de replicado en el mundo no tiene asociada a si la autoría del DVD, en muchos casos es un servicio contratado que no necesariamente tiene que replicarse la autoría que se realice, por lo que son dos industrias completamente independientes. Pero el caso de Cuba es distinto, contratar la autoría en el exterior sería una millonaria carrera, compitiendo con las grandes productoras de películas del mundo. Sobre esta base surge Autoría de DVD no como un proceso natural del VHS, si no como una necesidad de que el país pudiese realizar el proceso completo sin obstáculos.

Por lo referido anteriormente, se toma la decisión de fundar la Casa de Autoría de DVD, situada en la infraestructura productiva de la UCI, dada la posibilidad de contar con compañeros jóvenes con deseos de trabajar y la experiencia que la universidad tenía en este campo, a la cual se le plantearon las siguientes **Misiones:**

- Satisfacer la demanda de productos audiovisuales de valor educativo y cultural, para soporte de DVD, que contribuyan al desarrollo de los Programas de la Revolución, en el marco de la Batalla de Ideas.

- Lograr autorías, afines con los estándares internacionales, con tecnología de punta y personal altamente calificado, garantizando la calidad de las producciones.

Y contando con los siguientes **Objetivos:**

1. Lograr el funcionamiento óptimo de la tecnología instalada.
2. Hacer los diseños de flujo productivo, que especifiquen las variantes posibles, acorde con la tecnología instalada.
3. Capacitar al personal en el domino de la tecnología, en cada puesto de trabajo.
4. Establecer un sistema de control de la calidad, que garantice la excelencia en sus productos.
5. Certificar a través de las normas ISO 9000, la calidad de sus producciones.
6. Establecer un sistema de mantenimiento que garantice un adecuado funcionamiento de la tecnología instalada.
7. Montar un sistema de vigilancia tecnológica, que les permita mantener actualizada la tecnología, acorde con los estándares internacionales.
8. Establecer los contratos de trabajo con el Canal Educativo, el Complejo Industrial de multicopiado Luz Producciones Marianao, y otras entidades, para garantizar un marco apropiado en su desempeño empresarial.
9. Aportar la autoría de materiales audiovisuales a la Planta de CD, DVD del Complejo Industrial de multicopiado Luz Producciones Marianao, logrando un rol destacado en las producciones de esta industria.
10. Establecer las bases legales para el tratamiento de la propiedad intelectual, con vistas a proteger sus productos y cumplir las legislaciones vigentes.

1.3.2. Descripción actual

1.3.2.1. Resumen del flujo productivo

El proceso de Autoría de DVD es el nombre que se le ha definido a la serie de procesos por los que debe pasar un material audiovisual para finalmente llegar al soporte DVD. Estos procesos son: Planificación, Revisión de medias, Diseño, Codificación, Edición de Sonido, Subtitulaje, Autoría y Visionaje (revisión de calidad), que se han agrupado en 4 departamentos: Producción, Diseño, Subtitulaje, Calidad y Archivo.

Al departamento de Producción están asociados los procesos de planificación, revisión de medias, codificación, edición de sonido y autoría. Este departamento a su vez es el iniciador del flujo productivo en su primer paso, realizándose una planificación del proyecto que se va a ejecutar, la misma es realizada por el Coordinador de Producción responsable, que es quien guiará el trabajo y las relaciones con los demás departamentos.

El material cultural traído por el cliente (materia prima fundamental para la actividad que se realiza) debe de ser revisado por la Casa. El Coordinador de Producción en conjunto con el Operador de Video Tape hace una revisión parcial de cada material para evaluar la calidad del mismo. Si es aceptado es necesario hacer una propuesta de proyecto, de ocurrir lo contrario se rechaza el proyecto y se le comunica al cliente.

Aceptado el proyecto, se hace el estudio de factibilidad económica, donde el Coordinador debe presentarle varias propuestas, y una maqueta de navegabilidad del proyecto al Subdirector; se define además la complejidad del proyecto y basado en esto se elige el software de autoría a utilizar.

En una segunda entrevista con el cliente, este debe aprobar la maqueta y el estudio de factibilidad que le sea más conveniente de acuerdo a sus posibilidades económicas. Si acepta el proyecto, se elabora un guión de producción, de lo contrario se suspende el proyecto.

A partir de este punto se da puesta en marcha al proyecto y comienza la interacción con los demás departamentos, se elabora el guión de realización donde el Coordinador distribuye el trabajo y los recursos a las diferentes áreas que intervendrán en el desarrollo del proyecto. En el guión se relacionan las diferentes actividades a realizar por Video Tape, Diseño, Subtitulaje, Codificación, Edición de Audio, Autoría, Calidad y Archivo.

El departamento de Diseño procesa y elabora todo el material gráfico necesario para cada proyecto, las pantallas de los menús, las etiquetas de disco, cubiertas de la caja y las animaciones que sean necesarias insertar en cada material, concluyendo así una propuesta que se presenta al cliente para su aprobación. Esta es transformada hasta lograr una variante en la que el cliente quede satisfecho.

Video Tape se encarga de copiar los materiales traídos por el cliente y la conversión de normas (si fuese necesaria esta última). La copia es utilizada en la Casa, pues el original se entrega al cliente para evitar accidentes donde pueda ser dañado el material. Las facilidades instaladas para este proceso permiten procesar fuentes de vídeo en los formatos más importantes difundidos en el mundo de hoy como son: Betacam digital, Betacam SX, Betacam SP, IMX, DVCPro 50, DVCPro 25, DVCAM y DV.

Al concluir video tape con la copia de la cinta, comienza el proceso de codificación a MPEG-2, formato certificado para la producción de DVD donde el vídeo y el audio se almacenan por separado, esto se realizará con los parámetros que anteriormente el coordinador calculó para el proyecto. La codificación se realiza en tiempo real, por lo que el codificador (persona responsable del proceso) es capaz de hacer una revisión 100% del material y detectar cualquier deficiencia. En caso de existir alguna se procede a evaluar de conjunto con el coordinador y el Editor de Vídeo, si el problema es solucionable, decidiéndose la herramienta que se usará para corregir dicho problema. De no encontrar defectos, el material queda listo para pasar al proceso siguiente. Las facilidades instaladas para la codificación pueden ser configuradas en correspondencia con las necesidades del producto.

El área de Edición de Sonido se encarga de procesar todo el audio necesario, efectos para las animaciones y menús, pistas en formatos DTS, Dolby o LPCM que podrán ser en ambiente 5.1 o estéreo según se halla concebido en el proyecto.

En el departamento de Subtitulaje se llevan a cabo los procesos de transcripción, traducción y sincronización de texto, pasos necesarios para generar las pistas de subtítulos de un proyecto, teniendo en cuenta que un DVD puede ser subtitulado en 32 idiomas diferentes a la vez. Para la transcripción es necesario usar un casete DV con un código de tiempo continuo, el video que contiene es capturado con un código de tiempo exacto al original, logrando minimizar el desfase con respecto al que fue codificado en MPEG-2, luego son escritos los parlamentos en el idioma nativo del video (transcripción) y enviados a las entidades contratadas para la traducción. Los parlamentos traducidos regresan a la Casa y es cuando se procede a la sincronización final del nuevo subtítulo con el video original. Terminado este proceso se exportan en un formato compatible con el software que se usará para la autoría.

Autoría también se le denomina al proceso final de la producción. En este sitio toma forma el cuerpo del DVD, se ensamblan todos los materiales que han sido tratados de una u otra forma por las diferentes áreas a lo largo del proceso productivo con un orden lógico (según el guión de realización). Aquí se genera el pre-máster que se envía al Departamento de Calidad para su revisión.

El área de Visionaje (calidad) es la encargada de examinar el pre-máster con el objetivo de comprobar la correspondencia con el guión de realización y detectar cualquier defecto que atente contra la calidad del DVD. Este proceso se realiza en tiempo real y es preciso determinar a qué parte del flujo productivo pertenecen cada uno de los posibles errores.

El departamento de Calidad entrega el DVD al Coordinador con el resumen de la revisión. Si es satisfactorio el resultado, se ordena a Autoría grabar el DLT que será entregado al cliente. De ser rechazado entonces se le enviará la orientación de corregir el error al área involucrada con el mismo, repitiéndose entonces el proceso hasta llegar a un producto conforme a lo planificado.

Los departamentos de Archivo y Gestión de Medias trabajan en conjunto. Este último hace las salvas de seguridad según la orientación del especialista de archivo. Salva todos los recursos mediales (portables o no), proyectos, ediciones, material gráfico, audio nativo, capturas y máster. Aunque puede asumir tareas de Sonido, Autoría y Edición si fuese necesario. A lo largo del proceso de fabricación del DVD pueden existir interacciones entre el área de Archivo y las de Autoría, Codificación, Diseño, Edición, Sonido y Subtitulaje, si el proyecto lo requiere, éstas pueden necesitar información en un momento dado.

El flujo de todos los procesos descritos se muestra en el Anexo 2.

1.3.2.2. Tecnologías de la información utilizadas en el proceso productivo

La Casa adquirió la tecnología a través de AudioMax, empresa con capacidad de importación perteneciente a Copextel, lográndose que la misma fuese manufacturada en el año 2006.

La instalación llevó alrededor de un mes, en ella participaron especialistas extranjeros provenientes de Canadá. Los cuatro departamentos recibieron tecnología de altas prestaciones para los procesos que realizan. El sistema instalado es compatible con las tecnologías informáticas y los formatos digitales de todos tipos existentes en el país o provenientes del exterior. Esto incluye el campo del video y el audio digital y los materiales generados por cualquiera de las aplicaciones en plataforma Microsoft Windows que puedan ser utilizados en el proceso de autoría, pudiéndose asimilar formatos en cinta del tipo Betacam digital, Betacam SX, Betacam SP, IMX, DVCPro 50, DVCPro 25, DVCAM y DV, hacer conversiones de norma y cambios de formato.

Se adquirió un sistema de edición no lineal, así como dos sistemas de codificación MPEG-2 certificados para autoría de DVD, herramientas de diseño gráfico, posibilidades de subtitulaje en 32 idiomas, procesamiento de audio con formatos Dolby, DTS y PCM, software de autoría de clase mundial como es Sonic Scenarist y capacidades de impresión en cinta DLT. Todo el sistema opera sobre ambiente de almacenamiento distribuido y basado en plataforma Microsoft Windows, procesadores Intel y arquitectura IBM PC.

1.3.3. Situación problemática

La Casa, por varias razones, enfrenta un gran volumen de producción. Una de ellas es la necesidad que existe de difusión de materiales audiovisuales para los programas educativos. En la actualidad, cada vez más convenios en materia de educación se consuman entre Cuba y otros países, lo que supone que en el futuro la cantidad de proyectos a realizar por la Casa tienda a aumentar. El formato DVD-Video ofrece grandes prestaciones frente al formato VHS para la distribución de medias, por lo que cada vez tiene más auge en nuestro país, sin embargo hasta ahora muy pocas entidades realizan la autoría de DVD ya que esta actividad requiere de tecnología de punta muy costosa.

Los subprocesos que se deben realizar para concretar un proyecto DVD son complejos, altamente interdependientes y además muy ligados a la tecnología. Entre los diferentes grupos de trabajo debe existir un continuo y bien estructurado flujo de información, de lo contrario los proyectos se retrasan, con las consecuencias que esto puede traer. En la concepción de la Casa se tuvieron en cuenta las experiencias adquiridas en visitas a empresas foráneas, pero no fue posible conocer las especificidades del proceso productivo de cada una, ya que esto es información confidencial que no se da a conocer.

Por tanto, con los elementos reunidos se construyó un flujo de proceso propio que intenta satisfacer las necesidades de la producción, sin contar con una vasta experiencia en materia de autoría de DVD, que asegure que es totalmente acertado. Es crucial entonces disponer de algún mecanismo que permita comprobar hasta qué punto el proceso diseñado es correcto y está acorde a lo que se realiza en el mundo.

Muchos de los proyectos que se llevan a cabo en la Casa tienen un alto nivel de confidencialidad, por lo que resulta indispensable mantener la seguridad de la información que se maneja. Sin embargo, a pesar de que se han tomado algunas medidas por parte de la administración en este sentido, no hay nada que certifique que el nivel de seguridad alcanzado sea el requerido.

Como toda tecnología informática, el equipamiento con que cuenta la Casa, cuyo costo supera los 700 mil dólares, corre el riesgo de quedar obsoleto en poco tiempo. Incluso la concepción y puesta en marcha del proyecto se desarrollaron en medio del surgimiento de nuevos formatos superiores al DVD tradicional, como el HD y el Blu-ray. Es preciso dotar a los propietarios del proceso productivo de herramientas que permitan adquirir e implementar nuevas tecnologías y saber manejar los riesgos que esto conlleva.

Por la importancia que representa para el país y para los millones de personas que se beneficiarán de los programas audiovisuales y otros contenidos estratégicos, la Casa debe funcionar con eficiencia y alcanzar un nivel de competitividad que permita obtener productos de alta calidad.

1.4. Principales normas internacionales para el gobierno de TI.

En los últimos años, se ha observado un incremento en la necesidad de aplicación de auditorías informáticas. Principalmente los auditores, han tomado la iniciativa en los esfuerzos de estandarización internacional, ya que son frecuentemente consultados por las gerencias acerca de los controles internos, y sin un marco referencial esta tarea les resulta demasiado compleja. (COBIT, 2000). Este fenómeno ha motivado el surgimiento de una variedad de estándares y normas para el control, con mayor o menor orientación a las tecnologías de la información.

El uso de estándares y prácticas internacionales está sujeto a los requerimientos de cada empresa en particular. En sentido general, con la aplicación de los mismos normalmente se pretende:

- Apoyar el gobierno de TI, proporcionando políticas de administración y marcos de control, permitiendo tomar propiedad de los procesos, responsabilidades claras y contabilidad de las actividades de TI, alinear los objetivos de TI con los del negocio, definir las prioridades y asignar recursos, asegurar el retorno de la inversión y optimizar costos, asegurar que los riesgos se han identificado y son claros para la administración, que se han asignado las responsabilidades para el manejo de los riesgos, organizando los recursos de manera eficiente y con suficiente capacidad para ejecutar la estrategia de TI, y asegurando que las tareas críticas de TI pueden ser monitoreadas y medidas, de forma que se puedan identificar problemas y tomar medidas correctivas.
- Definir requerimientos de servicios y proyectos, internamente o con proveedores externos, precisando métricas y objetivos claros y relacionados con el negocio, hablando en términos de usuarios finales, creando acuerdos a nivel de servicios y contratos que los clientes puedan monitorear, asegurando que los requerimientos de los clientes son reflejados en los requisitos técnicos operacionales de TI, y considerando los servicios y los proyectos colectivamente de manera que se puedan establecer prioridades y los recursos sean asignados en una base equitativa y alcanzable.
- Verificar la capacidad de proveer, o demostrar competencia en el mercado, mediante auditorías y asesoramiento de terceros, compromisos contractuales, certificaciones y atestiguaciones.
- Facilitar constantemente el mejoramiento mediante evaluaciones de madurez, análisis de requerimientos no cubiertos, comparaciones, planeamiento de mejoras y prevención de la reinvención de modelos ya probados.
- Obtener un marco de referencia para la auditoría o evaluación externa a través de objetivos y criterios mutuamente aceptados, contrastes para justificar debilidades y agujeros de control, e incrementando la profundidad y valor de las recomendaciones al tomar como guía las prácticas generalmente aceptadas.

A continuación se contrastan los estándares y mejores prácticas más utilizados en el mundo.

1.4.1. Normas ISO

La Organización Internacional para la Normalización (ISO, International Organization for Standardization) es una federación mundial de entidades nacionales de normalización de 130 países, establecida en 1947. Su misión es promocionar el desarrollo de la normalización y actividades relacionadas en el mundo, con vista a facilitar el intercambio internacional de productos y servicios, y aumentar la cooperación en las esferas intelectuales, científicas, tecnológicas y la actividad económica. Existe un gran número de normas ISO, destinadas a casi todas las ramas de la industria, que son reconocidas y aplicadas por una gran cantidad de empresas y organizaciones de todo el mundo.

1.4.1.1. ISO 20000

La norma ISO/IEC 20000 de diciembre de 2005 (Information technology -- Service management) es la primera aceptada a nivel mundial que tiene como objetivo específico la gestión de los servicios de TI. Describe un conjunto integrado de procesos de gestión para la prestación en forma eficaz de servicios a los negocios y a sus clientes. Esta norma está alineada y se complementa con el enfoque por procesos definido dentro de la biblioteca de infraestructura de TI ITIL *(Véase 1.4.2)* de la Oficina Gubernamental de Comercio del Reino Unido (OGC, Office of Government Commerce). Este estándar es aplicable a pequeñas y grandes empresas, y establece procesos de administración de servicios que permiten entregar éstos con calidad y ajustándose a las necesidades del cliente, asegurándose de que se analizan y administran los riesgos.

Esta norma consiste de dos partes. La primera, ISO/IEC 20000-1:2005, está basada en la norma británica BS 15000-2, es la especificación formal y define los requisitos para que una organización preste servicios de una calidad aceptable a sus clientes. El costo actual de esta parte del estándar es de CHF 84.00 (aproximadamente 68 USD), y puede ser usado por negocios que pretenden ofertar servicios, para proporcionar una aproximación consistente de todos los proveedores de servicios de una cadena de suministros, para referenciar la administración de servicios de TI, como base para la auditoría externa, para demostrar la habilidad de cumplir los requisitos del cliente y/o para mejorar los servicios. Esta primera parte representa el estándar certificable. (ISO/IEC 20000-1:2005).

El alcance de esta norma según (IRCA, 2006) incluye:

- Requisitos para los servicios de gestión de TI.

- Planificación e implementación de servicios de gestión de TI.
- Planificación e implementación de servicios nuevos o modificados.
- Procesos de prestación de los servicios.
- Procesos de comunicación entre los clientes y el prestador de servicio de TI.
- Procesos de resolución de temas presentados por los clientes.
- Procesos de control.
- Procesos de liberación.

La segunda parte, ISO/IEC 20000-2:2005, es el código de prácticas y representa el conjunto de mejores prácticas adoptadas y aceptadas por la industria en materia de gestión de servicios de TI. Se basa en la norma británica BS 15000-2, está alineada con la biblioteca ITIL y sirve como guía y soporte en el establecimiento de acciones de mejora en el servicio o en la preparación de auditorías contra el ISO/IEC 20000-1. (ISO/IEC 20000-2:2005).

1.4.1.2. ISO 17799

La ISO/IEC 17799 (Information technology -- Security techniques -- Code of practice for information security management) se desarrolló en el año 2000 a partir de las anteriores BS 15000 y BS 7799 publicadas por el Instituto Británico de Normalización (BSI, British Standards Institution) y constituye el primer estándar internacional para la administración de la seguridad de la información. Esta norma, cuya última revisión fue publicada en 2005, provee información a los responsables de implementar la seguridad de la información en las organizaciones y constituye una base para el desarrollo de prácticas de administración y de otros estándares para la seguridad de la información, permitiendo mejorar la fiabilidad en la seguridad de la información en las relaciones inter-empresariales. (ISO/IEC 17799, 2005).

ISO/IEC 17799:2005 contiene las mejores prácticas en cuanto a objetivos de control y controles en las siguientes áreas de la administración de seguridad de la información:

- Políticas de Seguridad.
- Organización de la seguridad de la información.
- Administración de activos.
- Seguridad de recursos humanos.
- Seguridad física y ambiental.

- Administración de operaciones y comunicaciones.
- Control de acceso.
- Adquisición de sistemas informáticos, desarrollo y mantenimiento.
- Administración de incidentes de Seguridad de la información.
- Administración de la continuidad del negocio.

Según esta norma, el punto inicial para implementar la seguridad de la información depende de requisitos legales y de buenas prácticas generalmente aceptadas. Entre los requisitos legales se encuentran la protección y no revelación de los datos personales, la información interna y los derechos de propiedad intelectual. En resumidas cuentas es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado para este documento. Actualmente se encuentra en fase de revisión y saldrá con el nombre ISO 27002 en el presente año.

1.4.1.3. ISO 27000

La serie ISO 27000 es un conjunto o familia de normas relacionadas con la gestión de la seguridad de la información. Su principal estándar es el ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*), aprobado y publicado en octubre de 2005, y que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) (ISO/IEC 27001, 2005). Según el ciclo de Deming: PDCA, acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799, es certificable y tiene su origen en la revisión de la norma BS 7799-2:2002. (ESTRADA, 2007).

El estándar 27001 está diseñado para asegurar la selección de controles de seguridad adecuados y debidamente proporcionados, que permitan la protección de los recursos de información y den confianza a las partes interesadas. Es posible utilizarlo de muchas formas, entre ellas para formular requerimientos y objetivos de seguridad, como guía para asegurar que los riesgos en seguridad son administrados y costeables, para asegurar el cumplimiento de leyes y regulaciones legales, como un marco de trabajo de procesos para la implementación y manejo de controles que hagan cumplir los objetivos específicos de seguridad de una organización, para la definición y esclarecimiento de procesos de administración de la seguridad de la información existentes, para determinar el estado de las actividades de administración de seguridad de la información, para proveer información de seguridad a los clientes, entre otros. (ISO/IEC 27001, 2005).

Los demás estándares de la serie 27000 complementarán a la 27001, por ejemplo, la ISO 27000 contiene los conceptos utilizados en toda la serie, la ISO 27002 contendrá la guía de buenas prácticas, la ISO 27003 contiene una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. La ISO 27004 le sigue en importancia a 27001 ya que especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados. La ISO 27005 consistirá en una guía para la gestión del riesgo de la seguridad de la información (ESTRADA, 2007).

Finalmente, las ISO 27006-27009 están sin concretar aún aunque ya se contempla actualmente incluir directrices para gestión de la recuperación de desastres en las áreas de tecnologías de la información y comunicaciones de las organizaciones, así como la adaptación de la guía Europea de Acreditación EA-3/07 (ESTRADA, 2007).

La principal diferencia de esta norma respecto a la 17799 (ya que en ambas se habla prácticamente lo mismo) radica en que aquí se trata la gestión de la seguridad de la información como un sistema dinámico e incremental, mientras en la 17799 se plantean solamente un conjunto de medidas técnicas, controles, y reglas estáticas. Este estándar está aceptado en todo el mundo y según (ESTRADA, 2007) en el corto plazo se convertirá en una necesidad para cualquier PyME.

1.4.2. ITIL

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL, IT Infrastructure Library) es el marco de referencia más aceptado y utilizado en el mundo, enfocado a la entrega, soporte y administración de servicios de TI. Este estándar fue desarrollado por la Oficina Gubernamental de Comercio del Reino Unido (OGC) y propone una terminología estándar e independiente de la industria y la tecnología, para definir "qué hacer" y "qué no hacer" al aplicar en una organización la administración de servicios de TI.

El marco de ITIL apoya, pero no dicta los procesos de negocios en una organización, por lo que sus mejores prácticas adquieren distintas formas y matices, adaptándose a las necesidades individuales de cada entidad (ORTIZ, 2005). Los procesos de entrega de servicios descritos en ITIL son los siguientes:

- Administración de capacidad
- Administración de disponibilidad
- Administración financiera para los servicios de TI
- Administración de nivel de servicios
- Administración de continuidad de servicios de TI

Entre las ventajas que brinda la aplicación de este estándar se encuentran las siguientes:

- Aumentar la satisfacción de los clientes.
- Reducir el costo de desarrollo de prácticas y procedimientos.
- Mejorar los flujos de comunicación entre el personal de informática y los clientes o usuarios.
- Aumentar la productividad, las capacidades y la experiencia de los colaboradores.
- Incrementar la calidad del servicio y apoyar la operación de la organización.
- Obtener una visión clara de la capacidad de las TI y sus ventajas para la organización.
- Obtener información acerca de los cambios que proporcionarán un mayor beneficio para la organización.
- Permitir la implantación efectiva de las TI.

- Favorecer una acertada toma de decisiones con base en indicadores de TI y organizacionales.
- Conocer los procesos de las TI y la forma en que apoyan a los procesos estratégicos.

Las buenas prácticas descritas en ITIL se pueden aplicar a la administración de los servicios de TI de forma interna al proceso productivo de la Casa de Autoría de DVD, sin embargo este estándar no abarca todos los problemas que es preciso resolver, pues por ejemplo, no define un marco de control, no trata el tema de la gestión de riesgos, hace muy poca alusión a la estrategia y no presenta un modelo de madurez que permita evaluar la implementación. En adición, es posible extrapolar los conceptos que brinda ITIL al modelo CobiT, el cómo hacerlo está fuera del alcance de este trabajo y está bien expresado en el documento publicado por la ISACA (Aligning COBIT, 2007).

1.4.3. CobiT

Objetivos de Control para la Información y las Tecnologías relacionadas (Control Objectives for Information and related Technology, COBIT) es una herramienta de gobierno de TI lanzada en 1996 por el IT Governance Institute (ITGI) de la Information Systems Audit and Control Association (ISACA), ambos con sede en Illinois, Estados Unidos. El ITGI "se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. (...) El ITGI ofrece investigación original, recursos electrónicos y casos de estudio para ayudar a los líderes de las empresas y a sus consejos directivos en sus responsabilidades de Gobierno de TI." (COBIT, 2005)

La ISACA es "...una organización global líder de profesionales que representa a individuos en más de 100 países y comprende todos los niveles de la TI –Dirección ejecutiva, gerencia media y practicantes, (...) únicamente posesionada para cubrir el papel de generador central que armoniza los estándares de las prácticas de control de TI a nivel mundial." (COBIT, 2000). La ISACA es una asociación sin ánimo de lucro, de más de 35,000 profesionales en Sistemas Informáticos dedicados a la auditoría, el control y la seguridad de sistemas informáticos, a través de un compromiso de educación, certificación y estandarización.

La misión de CobiT es: "Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores."(COBIT, 2000). Esta norma se aplica a los sistemas de información de toda la empresa, y está basado

en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

"El objetivo principal del proyecto COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. Esto concuerda con la perspectiva COSO, que constituye el primer y mejor marco referencial para la administración en cuanto a controles internos. Posteriormente, los objetivos de control fueron desarrollados a partir de la perspectiva de los objetivos de auditoría (certificación de información financiera, certificación de medidas de control interno, eficiencia y efectividad, etc.)" (Cobit 3: Marco Referencial, p4)

Desde su primera publicación en 1996, este producto ha evolucionado hasta la versión 4.1 de marzo de 2007, que estará disponible en mayo. La cuarta edición, disponible en formato electrónico en el sitio Web de la ISACA y traducida al español, representa el mayor cambio realizado al estándar en el proceso de actualización. Las características a resaltar de este modelo son su enfoque al negocio, que está orientado a los procesos, basado en controles y conducido por mediciones, de forma que establece un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. COBIT está dirigido a tres tipos de audiencias: la administración, los auditores, y los usuarios de TI.

Los beneficios que brinda COBIT son: (COBIT, 2000).

- Mejor alineación de los objetivos de TI con los objetivos de la organización, basados en un enfoque de negocio
- Una vista, comprensible por la administración, de lo que la tecnología de información hace
- Posesión y responsabilidades claros, basados en la orientación a procesos.
- Aceptación general por terceros y reguladores
- Entendimiento compartido entre todos los stakeholders, basado en un lenguaje común
- Cumplimiento de los requerimientos de COSO para el entorno de control de TI

1.4.4. Otros estándares

La tendencia actual que están tomando las empresas que se aventuran en la implementación de estándares, va siendo tomar de cada uno la parte que necesitan, en lugar de decidirse sólo por uno de ellos.

ISM3, SOX, PRINCE2, AS 8015-2005: Corporate Governance of ICT,

1.5. Experiencias en CobiT

Según Sergio Hernando Westerheide, Consultor y Auditor Certificado de Tecnologías de la Información (CISA) del Banco Bilbao Vizcaya Argentaria (BBVA), encontrar empresas de autoría de DVD que utilicen CobiT es difícil, ya que "...según han ido publicándose versiones del mismo, se ha ido tornando *más pro SOX*, y por tanto, más *pro grandes organizaciones...*". Sin embargo, los Objetivos de Control no han sido desarrollados específicamente para un tipo o tamaño de entidad, sino que son de carácter genérico.

1.5.1. Experiencias foráneas

COBIT es utilizado en los más de 100 países miembros de la ISACA, por una gran variedad de empresas. En el sitio Web de la asociación, se puede acceder a 38 casos de estudio de empresas que han utilizado el estándar, agrupados en los dominios Consultoría de TI, Educación, Servicios Financieros, Aseguradoras, Gobierno, Salud, Manufactureras, Transporte, e Industrias Básicas. Esto da la idea de la variedad de implementaciones que ha tenido, habiendo sido adaptado a las necesidades de cada una.

En todos los casos que aparecen en la web como casos de estudio se trata de grandes empresas que poseen gran cantidad de recursos tecnológicos y que se han visto en la necesidad de evaluar y optimizar su gobernabilidad de TI, entre las más conocidas están Sun Microsystems (Estados Unidos), Universidad Tecnológica Curtin (Australia Occidental), Allstate (Estados Unidos), Harley-Davidson (Estados Unidos), Provincia de Mendoza (Argentina), la Society for Worldwide Interbank Financial Telecommunication (SWIFT, Bélgica), Organización Gubernamental Australiana (Canberra), Departamento de Defensa de los Estados Unidos, Royal Philips Electronics (Holanda), y el gobierno de Uruguay, entre otros.

A la luz de la legislación Sarbanes-Oxley (SOX), el departamento de TI de Sun Microsystems buscó un marco común para ver y medir el grado de alineación y contribución de las TI a la estrategia general del negocio. Se decidieron por COBIT, ya que soporta las actividades de control de TI en un ambiente de recursos restringidos, además les permitió utilizar un lenguaje común entre los diferentes procesos. Con esto fabricaron un Listado de Actividades de TI de Sun mapeadas a CobiT, que cubre todos los procesos, así como un proceso de evaluación CobiT/SOX que optimizó el cumplimiento de sus actividades.

Con más de 31 000 estudiantes, la Universidad Tecnológica Curtin es la más grande del occidente de Australia, con alrededor de 850 cursos de pregrado y posgrado en Negocios, Ingenierías, Ciencias Médicas, Humanidades, Ciencias, Minería y Agricultura. En busca de una metodología detallada para el gobierno de TI, introdujeron COBIT mediante su grupo de auditoría interna y rápidamente se convirtió en un estándar de la universidad. Esto les permitió aumentar los niveles de aceptación de TI, utilizar las auditorías como oportunidad para planificar las mejoras, y como resultado hubo una transformación de las prácticas organizacionales y perfeccionamiento económico continuo.

El gobierno de Uruguay, conjuntamente con el Banco Interamericano de Desarrollo, financió un Programa de Desarrollo Tecnológico que permitió el desarrollo de herramientas de software para el gobierno de TI, basadas en COBIT, con el propósito de maximizar las ventajas de las habilidades de sus profesionales en el campo de la ciencia y la tecnología. La firma Datasec S.R.L., encargada de llevar a cabo el proyecto, implementó el sistema MEYCOR COBIT Control Self Assessment, que ha sido utilizado por varias compañías y organizaciones uruguayas y de otros países, como el Banco Hipotecario del Uruguay (BROU), la empresa estatal Administración Nacional de Combustibles (ANCAP), el Tribunal de Cuentas, entre otros.

1.5.2. Entidades cubanas

En nuestro país, las experiencias en COBIT son pocas, comenzándose a utilizar en las Auditorías a las Tecnologías de la Información, por el Ministerio de Auditoría y Control (MAC), el Ministerio de la Informática y las Comunicaciones (MIC) y la Corporación CIMEX S.A. La implementación más profunda de COBIT se realizó en la Empresa de Telecomunicaciones de Cuba S.A. (ETECSA), en el ejercicio de las Auditorías Informáticas, desarrollándose soluciones para esta actividad; y más recientemente fue utilizado como marco de referencia en la revisión de las medidas de control para el uso de las redes de datos de dicha empresa.

Mediante la implementación de COBIT en la auditoría informática realizada a la Dirección de Telefonía Pública Inteligente de ETECSA, se pudieron observar los siguientes beneficios:

- El modelo permite observar al auditado como un único proceso, y obtener una visión general del flujo informativo y de control asociado a los eventos y procesos que se desarrollan en el negocio, automatizados o no.
- Es aplicable a cualquier tecnología: Para este modelo resulta transparente la implementación tecnológica que se encuentre en el Auditado, por ejemplo Redes Windows, Redes Unix, etc., por cuanto la guía de controles mínimos que posee es válida para todos.
- Permitió analizar los estadíos de la información así como su consistencia. La integridad de la información al aplicar COBIT no se circunscribe a los procesos internos de la Dirección de Telefonía Pública Inteligente, sino además, a aquellos que se encuentren relacionados con el mismo fuera de esta, por cuanto el modelo está orientado al negocio en general y a la adecuada toma de decisiones de la máxima dirección.
- Permitió elaborar programas de Auditorías a partir de la conformación de Análisis de Riesgos en busca de eficiencia y focalización de las criticidades: En la Auditoría que se plantearon se logró con la evaluación de riesgos detectar las áreas vulnerables dentro del sistema del auditado y dentro de estas los focos de posibles amenazas intentando direccionar la auditoría hacia los puntos realmente neurálgicos, ganando en eficiencia y operatividad con la consiguiente reducción de costos.
- Mediante el empleo de la guía de controles mínimos, se ajustan los dominios y controles definidos por COBIT a los objetivos empresariales, a tono con el empleo adecuado de las tecnologías de información.
- Permite verificar la debida correspondencia entre los objetivos de la entidad y la implementación de los procesos automatizados: Se pudo comprobar que se había realizado una inversión en tecnologías de información (equipos antifraudes) que funcionalmente no resolvían la amplia gama de deficiencias que en este sentido se estaban presentando. Se detectó, entre otras cosas, que el objetivo o misión fundamental de la Dirección de Telefonía Pública Inteligente presentaba fisuras en su realización ya que los reparadores no tenían la ruta crítica adecuada para trabajar encareciendo el gasto de los mismos. Se realizó una inversión elevada en la compra de estos equipos los cuales como resultado se obtuvo que los mismos no resolvían el problema fundamental, ya que se comprobó su

ineficiencia en el análisis del Sistema, a través de experiencias propiamente técnicas y la realización final de pruebas de Campo para la verificación final de su funcionalidad. (1)

1.6 Conclusiones

A pesar de no ser el único en el mundo, COBIT es utilizado ampliamente por una gran variedad de empresas y organizaciones de más de 100 países. Desde hace unos años en nuestro país se vienen dando los primeros pasos y muchos aseguran que la generalización en su uso se producirá inevitablemente. Ello se debe en parte a que no excluye el uso de otras herramientas, estándares, información, procedimientos y pruebas que estén dirigidas a la obtención de los mismos resultados (COBIT, 2000), y además, se basa en otros 41 estándares de seguridad, auditoría y control.

Una de las fortalezas de este modelo es su novedoso enfoque al negocio y sus objetivos, contemplando los procesos que están informatizados y los que no, de forma global. La documentación existente en el sitio Web de ISACA, tanto casos de estudio como guías de alineación con otros estándares, así como el propio estándar traducido al español, facilitan su uso.

Sin embargo, una completa implementación se hace un tanto engorrosa y complicada, en dependencia del nivel de madurez que se pretenda alcanzar, y su éxito dependerá del entendimiento y la cooperación de cada uno de los trabajadores en cada puesto laboral.

2. CAPÍTULO II. ANÁLISIS E IMPLEMENTACIÓN DE COBIT

2.1 Introducción

En este capítulo se hace referencia a los conceptos relacionados con CobiT que son necesarios para el entendimiento del lector, se describe la metodología diseñada para la implementación del marco de controles, se da una idea de la madurez del proceso productivo en cuanto a los controles de TI y se mencionan los requerimientos del negocio y metas de TI de la Casa, se destacan además, los procesos clave de TI y se mencionan los controles a implementar por cada actividad de TI.

2.2. Marco conceptual

A continuación se relacionan algunos conceptos fundamentales que son necesarios conocer para el entendimiento del marco de trabajo de TI.

Control: Se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Objetivo de Control: Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de TI.

Nivel de Madurez: Los niveles de madurez están diseñados como perfiles de procesos de TI, que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior.

2.3. Marco de trabajo de Cobit

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y

Monitorear y Evaluar. Los dominios se equiparán a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa, visualiza y administra las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iníciales más importantes hacia un buen gobierno. También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

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

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

• ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?
• ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?

• ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
• ¿Los cambios afectarán las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia:

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

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

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

2.4. Metodología a utilizar

CobiT no es un marco de referencia estricto con una serie de pasos a seguir, sino que se debe ajustar a las necesidades de control de cada empresa donde se desee utilizar. Por esta razón se diseñó una metodología basada en el marco de trabajo de CobiT que permite implementar controles objetivos y enfocarlos hacia el cumplimiento de los requerimientos del negocio, así como medir hasta qué punto se llegó con la implantación de estos. La metodología diseñada es la siguiente:

1. Definir los Requerimientos del negocio

Una de las mayores ventajas de CobiT es que está enfocado al cumplimiento de los requerimientos del negocio, por tanto el primer paso para la implementación del marco de controles tiene que ser la determinación clara de los objetivos y metas del negocio. Esto le corresponde a la Dirección del negocio, en combinación con la alta gerencia.

2. Definir las Metas del negocio para TI

Una vez determinados los requerimientos del negocio, corresponde a la Dirección en combinación con el Subdirector de producción definir qué es lo que el negocio espera que TI le proporcione, en correspondencia con los requerimientos del negocio. Este paso es clave para asegurar la alineación de TI con los requerimientos del negocio.

3. Definir las Metas de TI alineadas

Las metas de TI constituyen la forma que se tiene de medir el desempeño de los procesos de TI de la organización, y se deben definir en concordancia con las metas del negocio para TI. Las metas de TI se deben definir por el Consejo de Dirección por el método de expertos.

4. Aplicar modelo de madurez de controles

El modelo de madurez de controles se aplica para conocer el estado inicial de la situación de los controles en el área de TI, y realizar una proyección del resultado que se desea obtener (al nivel que se desea llegar) con la implementación del marco de control. También permite obtener una idea de lo que se necesita hacer para llegar al nivel proyectado.

5. Definir la arquitectura empresarial de TI

La arquitectura empresarial de TI está formada por los procesos clave de TI, su responsable, así como el flujo de información (sus entradas y salidas de información). También se encuentran dentro de la arquitectura las aplicaciones, ya sean manuales o automatizadas, que procesan la información de entrada y generan las salidas, así como el personal y la infraestructura necesarias para su ejecución.

a. Definir los procesos clave que soportan al negocio

Los procesos clave que soportan al negocio se determinan mediante técnicas de trabajo en grupo por el Consejo de Dirección, a partir de los procesos genéricos que presenta CobiT, teniendo en cuenta los que ya se llevan a cabo en la empresa y desechando los que no se

realizan o no son afines. A cada proceso se le debe asignar una importancia alta, media o baja.

b. Definir el responsable del proceso

El responsable del proceso se determina por parte del Consejo de Dirección mediante el método de expertos. Debe existir una correcta segregación de funciones entre el responsable y las personas que ejecutan las aplicaciones.

c. Aplicar modelo de madurez de proceso

El modelo de madurez de proceso se realiza para cada proceso definido como clave para determinar el nivel inicial que presenta este proceso en la organización, para estimar al nivel que se pretende llegar con la implementación de los controles y para tener una idea de lo que se debe hacer para llegar a ese nivel.

d. Identificar actividades más importantes (Objetivos de Control detallados)

Las actividades de TI más significativas que se deben desarrollar en la empresa para el cumplimiento de los objetivos y metas del negocio, se identifican mediante el método de expertos por parte del Consejo de Dirección.

e. Definir controles

En concordancia con el nivel que se desea obtener en el proceso, se deben definir controles (políticas, procedimientos, prácticas y estructuras organizacionales) que contribuyan al cumplimiento de los requisitos del negocio a los cuales responde el proceso de TI.

6. Aplicar modelo de madurez de controles

Cuando se hayan implementado todos los controles necesarios, se aplica nuevamente el modelo de madurez del control interno para verificar si se ha llegado al nivel que se esperaba, definido en el paso 4.

2.5. Requerimientos del negocio

Los requerimientos del negocio los constituyen tanto los objetivos de la Casa como las metas. A continuación se relacionan los objetivos y metas así como el nivel (**P**rimario, **S**ecundario o ninguno) en que tributan hacia las Metas de TI.

	Objetivos	Metas de TI*
ON1	Lograr el funcionamiento óptimo de la tecnología instalada.	P
ON2	Hacer los diseños de flujo productivo, que especifiquen las variantes posibles, acorde con la tecnología instalada.	P
ON3	Capacitar al personal en el domino de la tecnología, en cada puesto de trabajo.	P
ON4	Establecer un sistema de control de la calidad, que garantice la excelencia en nuestros productos.	S
ON5	Certificar a través de las normas ISO 9000, la calidad de nuestras producciones.	
ON6	Establecer un sistema de mantenimiento que garantice un adecuado funcionamiento de la tecnología instalada.	P
ON7	Montar un sistema de vigilancia tecnológica, que nos permita mantener actualizada nuestra tecnología acorde con los estándares internacionales.	S
ON8	Establecer los contratos de trabajo con el Canal Educativo, el Complejo Industrial de multicopiado, Luz Producciones Marianao, y otras entidades, para garantizar un marco apropiado en nuestro desempeño empresarial.	
ON9	Establecer las bases legales para el tratamiento de la propiedad intelectual, con vistas a proteger nuestros productos y cumplir las legislaciones vigentes.	S
ON10	Disminuir el consumo energético.	P
ON11	Desarrollar productos propios.	S
ON12	Contar con los datos necesarios para realizar una planeación estratégica efectiva.	P
	Metas	Metas de TI
MN1	Poseer una tecnología de punta y estandarizada.	P
MN2	Contar con un personal altamente calificado y comprometido.	P
MN3	Lograr la excelencia en la calidad y aceptación de nuestros productos*.	P
MN4	Satisfacer a plenitud a nuestros clientes*.	P
MN5	Gozar de un prestigio nacional e internacional*.	P
MN6	Jugar un rol importante en el desarrollo de los Programas de la Revolución, en el marco de la Batalla de Ideas	P
MN7	Tener los procesos certificados por la norma ISO 9001:2000.	
MN8	Alcanzar altos niveles de organización empresarial en todas las operaciones y procesos que se generan en nuestra actividad económica.	P

Tabla 2-1: Objetivos y metas de TI

* Requerimientos facilitados por TI (Metas del Negocio para TI)

2.6. Metas de TI

A continuación se relacionan las Metas específicas de TI, así como la prioridad que representa cada una para la Casa de Autoría. Se tomaron como referencia las metas genéricas de Cobit y el nivel de prioridad se definió por el consejo de dirección.

№	Metas de TI	Prioridad
1	Responder a los requisitos del negocio de acuerdo a la estrategia del negocio.	P
2	Responder a los requisitos de gobierno de acuerdo a la dirección del consejo de dirección.	P
3	Garantizar la satisfacción de los usuarios finales con ofertas.	P
4	Optimizar el uso de la información.	P
5	Crear agilidad de TI.	P
6	Definir cómo los requisitos funcionales y de control se traducen a soluciones automatizadas efectivas y eficientes.	S
7	Adquirir y mantener sistemas aplicativos integrados y estandarizados.	P
8	Adquirir y mantener infraestructura de TI integradas y estandarizada.	P
9	Adquirir y mantener habilidades de TI que respondan a la estrategia de TI.	P
10	Integrar las soluciones aplicativas y tecnológicas de forma transparente.	P
11	Garantizar la transparencia y el entendimiento de los costos, beneficios, estrategias, políticas y niveles de servicio de TI.	S
12	Garantizar el uso y el desempeño apropiado de las soluciones aplicativas y tecnológicas.	P
13	Responder por todos los activos de TI y protegerlos.	P
14	Optimizar la infraestructura, recursos y capacidades de TI.	P
15	Reducir los defectos y trabajar en las soluciones y en la prestación del servicio.	S
16	Proteger el logro de los objetivos de TI.	P
17	Establecer claridad del impacto al negocio de los riesgos de los objetivos y recursos de TI.	P
18	Asegurar que la información crítica y confidencial se mantenga resguardada de aquellos que no deben tener acceso a ella.	P
19	Asegurarse de que se puede confiar en los intercambios de información.	S
20	Asegurarse de que los servicios y la infraestructura de TI pueden resistir y recuperarse adecuadamente de las fallas debidas a errores, ataques deliberados o desastres.	P
21	Garantizar un impacto mínimo al negocio en caso de una interrupción o cambio en el servicio de TI.	P
22	Garantizar que los servicios de TI estén disponibles según se requieran.	P
23	Entregar los proyectos a tiempo satisfaciendo los estándares de calidad.	P
24	Mantener la integridad de la infraestructura de la información y del procesamiento.	P
25	Asegurar que TI cumple las leyes y reglamentos.	P
26	Asegurar que TI demuestra una calidad de servicio, mejora continua, presteza para cambios futuros.	P

Tabla 2-2: Metas específicas de TI

2.7. Análisis actual del flujo productivo a la luz del modelo de madurez de CobiT

Atendiendo al modelo de madurez genérico para el control interno que presenta Cobit se determinó que el proceso productivo de la Casa se encuentra en nivel 1 (Inicial / ad hoc) ya que: se reconoce algo de la necesidad del control interno, el enfoque hacia los requerimientos de riesgo y control es ad hoc y desorganizado, sin comunicación o supervisión, no se identifican las deficiencias. En cuanto al establecimiento de controles internos no existe la conciencia de la necesidad de evaluar lo que se necesita en términos de controles de TI, cuando se llevan a cabo, son solamente de forma ad hoc, a alto nivel y como reacción a incidentes significativos, la evaluación sólo se enfoca al incidente presente.

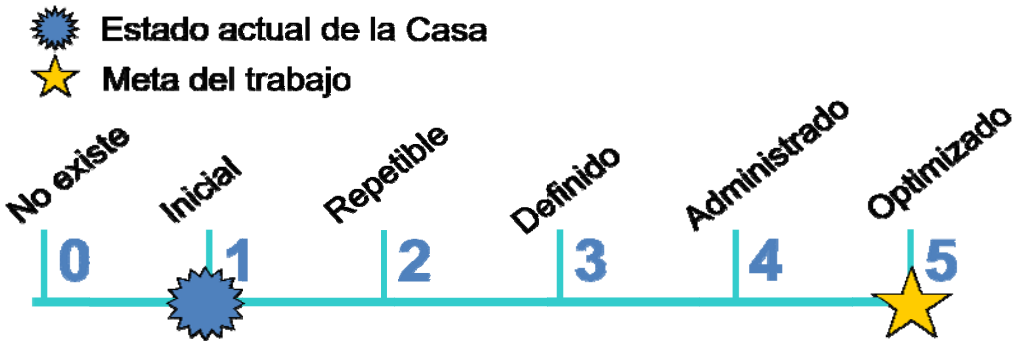


Figura 2-1: Nivel de madurez de los controles internos.

2.8. Procesos de TI identificados

Tomando como base los procesos genéricos de Cobit se identificaron 29 procesos y el consejo de dirección definió la importancia (**A**lta, **M**edia o **B**aja) de cada uno para la Casa.

		Importancia
Planeación y Organización		
PO1	Definir un plan estratégico de TI	A
PO2	Definir la arquitectura de la información	B
PO3	Definir la dirección tecnológica	M
PO4	Definir los procesos, organización y relaciones de TI	B
PO5	Comunicar las metas y la dirección de la gerencia	M
PO6	Administrar la calidad	M
PO7	Evaluar y administrar los riesgos de TI	A
PO8	Administrar los proyectos	A

Tabla 2-3: Nivel de importancia de los Procesos del Dominio **P**lanear y **O**rganizar.

		Importancia
Adquirir e Implantar		
AI1	Identificar las soluciones automatizadas	M
AI2	Adquirir y mantener software aplicativo	M
AI3	Adquirir y mantener la infraestructura tecnológica	B
AI4	Facilitar la operación y el uso	B
AI5	Procurar recursos de TI	M
AI6	Administrar los cambios	A
AI7	Instalar y acreditar soluciones y cambios	M

Tabla 2-4: Nivel de importancia de los Procesos del Dominio **A**dquirir e **I**mplementar.

		Importancia
Entregar y dar soporte		
DS1	Definir y administrar los niveles de servicio	M
DS2	Administrar el desempeño y la capacidad	B
DS3	Asegurar el servicio continúo	M
DS4	Garantizar la seguridad de los sistemas	A
DS5	Educar y entrenar a los usuarios	B
DS6	Administrar la mesa de servicio y los incidentes	B
DS7	Administrar la configuración	M
DS8	Administrar los problemas	M
DS9	Administrar los datos	A
DS10	Administrar las operaciones	B

Tabla 2-5: Nivel de importancia de los Procesos del Dominio Entregar y **D**ar **S**oporte.

		Importancia
Monitorear y Evaluar		
ME1	Monitorear y evaluar el desempeño de TI	A
ME2	Monitorear y evaluar el control interno	M
ME3	Garantizar el cumplimiento regulatorio	B
ME4	Proporcionar gobierno de TI	B

Tabla 2-6: Nivel de importancia de los Procesos del Dominio Monitorear y Evaluar.

3. CAPÍTULO III. ARQUITECTURA EMPRESARIAL DE TI Y MARCO DE CONTROLES OBTENIDOS

3.1. Introducción

En este capítulo se muestran en forma de tablas la arquitectura empresarial obtenida por cada proceso definido, estructurados en los cuatro dominios de Cobit, así como los controles propuestos a implementar. También se relacionan los niveles de madurez obtenidos para cada proceso de TI.

3.2. Planeación y organización

Elementos de la arquitectura:

Proceso:	**Definir un plan estratégico de TI**		**PO1**
Responsable(S):	Director		
Importancia:	Alta	Nivel de Madurez:	Inicial/Ad hoc (1)*
Entrada:			
• Reportes de costo / beneficio. • Evaluación de riesgos. • Requerimientos de servicio nuevos/actualizados; portafolio de servicios actualizado. • Estrategia y prioridades del negocio. • Portafolio de programas. • Entrada de desempeño a planeación de TI. • Reporte del estado del gobierno de TI; dirección estratégica de la empresa para TI.			
Salida:			
• Plan estratégico de TI. • Plan táctico de TI. • Portafolio de servicios de TI. • Estrategia de adquisición de TI.			
Aplicaciones:		Personal e Infraestructura:	
Determinación un plan estratégico para TI.		Subdirector Jefes de Grupo	
Actividades:			
1. Alineación de TI con el negocio. 2. Evaluación del desempeño actual. 3. Realización del plan estratégico de TI. 4. Realización de los planes tácticos de TI. 5. Administración del portafolio de TI.			

Tabla 3-1: Elementos de la arquitectura, Definir un plan estratégico de TI (PO1)

** La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requisito de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.*

Controles propuestos:

Controles:
• **Política para la definición del plan estratégico de TI**: Debe contemplar la participación de la alta gerencia y la gerencia del negocio, para alinear la planeación estratégica de TI con las necesidades del negocio actuales. El plan debe referir cómo la TI contribuirá al logro de las metas de la empresa y se deben describir claramente los riesgos relacionados. • **Procedimiento para la determinación de las capacidades actuales de TI:** Debe contribuir al entendimiento de las capacidades actuales de TI. • **Procedimiento para la priorización de los objetivos del negocio:** Debe permitir la aplicación de un esquema de prioridades que cuantifique los requerimientos del negocio.

Tabla 3-2: Controles propuestos, Definir un plan estratégico de TI (PO1).

Elementos de la arquitectura:

Proceso:	**Definir la arquitectura de la información**		**PO2**
Responsable(S):	Subdirector		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Planes estratégicos y tácticos de TI. • Estudio de factibilidad de requerimientos del negocio. • Revisión post-implantación. • Información de desempeño y capacidad. • Entrada de desempeño a planeación de TI.			
Salida:			
• Esquema de clasificación de datos. • Plan de sistemas de negocio optimizado. • Arquitectura de información. • Clasificaciones asignadas de datos. • Procedimientos y herramientas de clasificación.			
Aplicaciones:		Personal e Infraestructura:	
Establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.		Consejo de Dirección	
Actividades:			
1. Crear y mantener modelo de información corporativo / empresarial. 2. Establecer y mantener esquema de clasificación de datos. 3. Brindar a los propietarios procedimientos y herramientas para clasificar sistemas de información. 4. Usar el modelo de información y el esquema de clasificación para planear los sistemas optimizados de negocio.			

Tabla 3-3: Elementos de la arquitectura, Definir la arquitectura de la información (PO2).

**La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.*

Controles propuestos:

Controles:
• **Procedimiento para el aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos:** Debe contemplar el modelo de arquitectura de información empresarial que establecerá y mantendrá un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, oportuna, segura y tolerante a fallas. • **Política de clasificación de la información:** Debe 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 encriptación.

Tabla 3-4: Controles propuestos, Definir la arquitectura de la información (PO2).

Elementos de la arquitectura:

Proceso:	**Definir la dirección tecnológica**		**PO3**
Responsable(S):	Subdirector		
Importancia:	Media	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Planes estratégicos y tácticos de TI. • Plan optimizado de sistemas del negocio y arquitectura de información. • Actualizaciones de los estándares tecnológicos. • Información sobre el desempeño y la capacidad.			
Salida:			
• Oportunidades tecnológicas. • Estándares tecnológicos. • Actualizaciones rutinarias del “estado de la tecnología”. • Plan de infraestructura tecnológica. • Requerimientos de infraestructura.			
Aplicaciones:		Personal e Infraestructura:	
Definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.		Jefes de Grupos	
Actividades:			
1. Crear y mantener un plan de infraestructura tecnológica. 2. Crear y mantener estándares tecnológicos. 3. Publicar estándares tecnológicos. 4. Monitorear la evolución tecnológica. 5. Definir el uso (futuro) (estratégico) de la nueva tecnología.			

Tabla 3-5: Elementos de la arquitectura, Definir la dirección tecnológica (PO3).

** La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implantación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.*

Controles propuestos:

Controles:
• **Política para dirigir la arquitectura y verificar el cumplimiento:** Debe establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos. • **Procedimiento para establecer un plan de infraestructura tecnológica equilibrado versus costos, riesgos y requerimientos:** Debe crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones. • **Procediendo para la definición de estándares de infraestructura tecnológica:** Debe proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, manteniendo las regulaciones establecidas en los estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información.

Tabla 3-6: Controles propuestos, Definir la dirección tecnológica (PO3).

Elementos de la arquitectura:

Proceso:	**Definir los procesos, organización y relaciones de TI**		**PO4**
Responsable(S):	Subdirector		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Planes estratégicos y tácticos de TI. • Políticas y procedimientos de TI y. • Actividades de mejoramiento de calidad. • Planes de actividades para corregir riesgos relacionados con TI. • Reportar la efectividad de los controles de TI. • Catálogo de requerimientos legales y regulatorios relacionados con los servicios de TI. • Mejoras al marco de procesos.			
Salida:			
• Marco de trabajo para el proceso de TI. • Propietarios de sistemas documentados. • Organización y relaciones de TI. • Marco de procesos, roles documentados y responsabilidades de TI. • Roles y responsabilidades documentados.			
Aplicaciones:		Personal e Infraestructura:	
Establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implantación de procesos de TI con los propietarios, y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión.		Consejo de Dirección	
Actividades:			
1. Establecer estructura organizacional e TI. 2. Diseñar marco de trabajo para el proceso de TI. 3. Identificar propietarios de sistemas. 4. Identificar propietarios de datos. 5. Establecer e implantar roles y responsabilidades de TI.			

Tabla 3-7: Elementos de la arquitectura, Definir los procesos, organización y relaciones de TI (PO4).

**La dirección reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implantación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.*

Controles propuestos:

Controles:
• **Procedimiento para la definición del marco de trabajo de procesos de TI:** Debe contribuir a ejecutar el plan estratégico de TI. Incluyendo la estructura y relación de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporcionará integración entre los procesos que son específicos para TI, administración del portafolio de TI, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno. • **Procedimiento para el establecimiento de un cuerpo y una estructura organizacional apropiada:** Debe establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implantar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes. • **Política de definición de roles y responsabilidades:** Debe definir y comunicar los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad. Crear y actualizar periódicamente la descripción de roles. Estas descripciones deben estar alineadas con la responsabilidad y la autoridad incluyendo definiciones de habilidades y experiencia necesarias en cada posición y que serán aplicables en el uso y evaluación del desempeño.

Tabla 3-8: Controles propuestos, Definir los procesos, organización y relaciones de TI (PO4).

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Comunicar las metas y la dirección de la gerencia</td><td>PO5</td></tr>
<tr><td>Responsable(S):</td><td colspan="3">Director</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de Madurez:</td><td>1 Inicial/Ad Hoc*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Planes estratégicos y tácticos de TI, portafolios de proyectos y servicios.
• Directrices de administración de riesgos relativos a la TI.
• Reportes sobre la efectividad de los controles de TI.</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Marco de control empresarial para TI.
• Políticas para TI.</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e Infraestructura:</td></tr>
<tr><td colspan="2">Proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de TI a los interesados.</td><td colspan="2">Jefes de Grupos</td></tr>
<tr><td colspan="4">Actividades:</td></tr>
<tr><td colspan="4">1. Elaborar y mantener un ambiente y marco de control de TI
2. Elaborar y mantener políticas de TI
3. Comunicar el marco de control y los objetivos y dirección de TI</td></tr>
</table>

Tabla 3-9: Elementos de la arquitectura, Comunicar las metas y la dirección de la gerencia (PO5).

** La dirección es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.*

Controles propuestos:

Controles:
• **Procedimiento de definición del marco de trabajo de control para TI**: Debe estar integrado por el marco de procesos de TI y el sistema de administración de calidad, y debe cumplir los objetivos generales de la empresa. Debe tener como meta maximizar el éxito de la entrega de valor mientras minimiza los riesgos para los activos de información por medio de medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la oportuna recuperación de activos del negocio. • **Procedimiento para la elaboración e implantación de políticas para TI:** Debe permitir la elaboración de un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular. La implantación debe contribuir a que las políticas de TI se implanten y se comuniquen a todo el personal relevante, y se refuercen, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales. Los métodos de implantación deben resolver necesidades e implicaciones de recursos y concientización.

Tabla 3-10: Controles propuestos, Comunicar las metas y la dirección de la gerencia (PO5).

Elementos de la arquitectura:

Proceso:	**Administrar la calidad**		**PO6**
Responsable(S):	Jefe de Grupo de Calidad		
Importancia:	Media	Nivel de Madurez:	2 Repetible pero intuitiva*
Entrada:			
• Plan estratégico de TI. • Planes detallados de proyectos. • Planes de acciones correctivas.			
Salida:			
• Estándares de adquisición. • Estándares de desarrollo. • Requerimientos de estándares y métricas de calidad. • Medidas para la mejora de la calidad.			
Aplicaciones:		Personal e Infraestructura:	
Definición de un sistema de administración de calidad (QMS, por sus siglas en inglés), el monitoreo continuo del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI.		Revisores de Calidad	
Actividades:			
1. Definir un sistema de administración de calidad. 2. Establecer y mantener un sistema de administración de calidad. 3. Crear y comunicar estándares de calidad a toda la organización. 4. Crear y administrar el plan de calidad para la mejora continua. 5. Medir, monitorear y revisar el cumplimiento de las metas de calidad.			

Tabla 3-11: Elementos de la arquitectura, Administrar la calidad (PO6).

**Se establece un programa para definir y monitorear las actividades de QMS dentro de TI. Las actividades de QMS que ocurren están enfocadas en iniciativas orientadas a procesos, no a procesos de toda la organización.*

Controles propuestos:

Controles:
• **Procedimiento de definición de estándares y prácticas de calidad:** Debe contribuir a identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización. • **Procedimiento para el monitoreo y revisión interna y externa del desempeño contra los estándares y prácticas de calidad definidas:** Debe definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

Tabla 3-12: Controles propuestos, Administrar la calidad (PO6).

Elementos de la arquitectura:

Proceso:	**Evaluar y administrar los riesgos de TI**		**PO7**
Responsable(S):	Subdirector		
Importancia:	Alta	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Planes estratégicos y tácticos de TI, portafolio de servicios de TI. • Plan de administración de riesgos de proyectos. • Riesgos de proveedores. • Resultados de pruebas de contingencia. • Amenazas y vulnerabilidades de seguridad. • Tendencias y eventos de riesgos históricos.			
Salida:			
• Evaluación de riesgos. • Reporte de riesgos. • Directrices de administración de riesgos relacionados con TI. • Planes de acciones correctivas para riesgos relacionados con TI.			
Aplicaciones:		Personal e Infraestructura:	
Elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.		Jefes de Grupos	
Actividades:			
1. Determinar la alineación de la administración de riesgos (ej. Evaluar riesgo). 2. Entender los objetivos de negocio estratégicos relevantes. 3. Entender los objetivos de los procesos de negocio relevantes. 4. Evaluar los riesgos asociados con los eventos. 5. Evaluar las respuestas a los riesgos. 6. Priorizar y planear las actividades de control. 7. Aprobar y garantizar el financiamiento de los planes de acción de riesgos. 8. Mantener y monitorear un plan de acción de riesgos.			

Tabla 3-13: Elementos de la arquitectura, Evaluar y administrar los riesgos de TI (PO7).

** Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.*

Controles propuestos:

Controles:
• **Procedimiento para la alineación de la administración de riesgos de TI y del negocio:** Debe integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización. • **Política de evaluaciones de riesgo:** Debe evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio. • **Procedimiento para el mantenimiento y monitoreo de un plan de acción de riesgos:** Debe permitir y asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección**.**

Tabla 3-14: Controles propuestos, Evaluar y administrar los riesgos de TI (PO7).

Elementos de la arquitectura:

Proceso:	**Administrar los proyectos**		**PO8**
Responsable(S):	Consejo de Dirección		
Importancia:	Alta	Nivel de Madurez:	2 Repetible pero intuitiva*
Entrada:			
• Portafolio de proyectos. • Portafolio de proyectos de TI actualizado. • Matriz de habilidades de TI. • Estándares de desarrollo. • Revisión post-implantación.			
Salida:			
• Reportes de desempeño del proyecto. • Plan de administración de riesgos del proyecto. • Directrices administrativas del proyecto. • Planes detallados del proyecto. • Portafolio actualizado de proyectos de TI.			
Aplicaciones:		Personal e Infraestructura:	
Programa y enfoque de administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los interesados y el monitoreo de los riesgos y los avances de los proyectos.		Consejo de Dirección	
Actividades:			
1. Definir un marco administrativo de programas/portafolio para inversiones en TI. 2. Establecer y mantener un marco de trabajo para la administración de proyectos de TI. 3. Establecer y mantener un sistema de monitoreo, medición y administración de sistemas. 4. Elaborar, estatutos, calendarios, planes de calidad, presupuestos, y planes de comunicación y de administración de riesgos. 5. Asegurar el control efectivo de los proyectos y de los cambios a proyectos. 6. Definir e implantar métodos de aseguramiento y revisión de proyectos.			

Tabla 3-15: Elementos de la arquitectura, Administrar los proyectos (PO8).

** La alta dirección ha obtenido y comunicado la conciencia de la necesidad de una administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos de proyecto a proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iníciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción del gerente de proyecto.*

Controles propuestos:

Controles:
• **Política de administración de proyectos:** Debe establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores del proyecto, 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. • **Procedimiento para la administración de riesgos del proyecto:** Debe eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central. • **Política de planeación del proyecto y métodos de aseguramiento:** Debe identificar las tares de aseguramiento requerido para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

Tabla 3-16: Controles propuestos, Administrar los proyectos (PO8).

2.7.2. Adquirir e implanta

Elementos de la arquitectura:

Proceso:	**Identificar soluciones automatizadas**		**AI1**
Responsable(S):	Director		
Importancia:	Media	Nivel de Madurez:	3 Proceso definido*
Entrada:			
• Planes estratégicos y tácticos de TI. • Actualizaciones periódicas del "estado de la tecnología"; estándares tecnológicos. • Estándares de adquisición y desarrollo. • Directrices administrativas del proyecto y planes detallados del proyecto. • Descripción del proceso de cambio. • Plan de desempeño y capacidad (requerimientos).			
Salida:			
• Estudio de factibilidad de los requerimientos del negocio.			
Aplicaciones:		Personal e Infraestructura:	
Identificación de soluciones técnicamente factibles y rentables.		Subdirector Jefes de Grupos. Administrador de Redes	
Actividades:			
6. Definir los requerimientos funcionales y técnicos del negocio. 7. Identificar, documentar y analizar el riesgo del proceso de negocio. 8. Evaluar los beneficios operativos de TI para las soluciones propuestas. 9. Elaborar un proceso de aprobación de requerimientos.			

Tabla 3-17: Elementos de la arquitectura, Identificar las soluciones automatizadas (AI1)

**Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.*

Controles propuestos:

Controles:
• **Procedimiento para la definición y mantenimiento de los requerimientos técnicos y funcionales del negocio:** Debe contemplar que los requerimientos toman en cuenta las necesidades funcionales, la dirección tecnológica, el desempeño, el costo, la confiabilidad, la compatibilidad, la auditoría, la seguridad, la disponibilidad y continuidad, la funcionalidad, la seguridad y la legislación de la empresa. Se deben establecer procesos para garantizar y administrar la integridad, exactitud y la validez de los requerimientos del negocio, como base para el control de la adquisición y el desarrollo continuo de sistemas. • **Procedimiento para la elaboración de reporte de análisis de riesgos:** Se debe identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos. Los riesgos incluyen las amenazas a la integridad, seguridad, disponibilidad y privacidad de los datos, así como el cumplimiento de las leyes y reglamentos. • **Procedimiento para la formulación de cursos de acción alternativos y estudio de factibilidad:** Debe identificar los cursos alternativos de acción para el software, hardware, servicios y habilidades que satisfagan los requerimientos establecidos, tanto funcionales como técnicos, y evaluar la factibilidad tecnológica y económica (costo potencial y análisis de beneficios) de cada uno de los cursos de acción identificados en el contexto de inversión en TI.

Tabla 3-18: Controles propuestos, Identificar las soluciones automatizadas (AI1).

Elementos de la arquitectura:

Proceso:	**Adquirir y mantener software aplicativo**		**AI2**
Responsable(S):	Director		
Importancia:	Media	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Actualizaciones periódicas del “estado de la tecnología”. • Reporte de costo/beneficio. • Estándares de adquisición y desarrollo. • Directrices administrativas del proyecto y planes detallados del proyecto. • Estudio de factibilidad de los requerimientos del negocio. • Descripción del proceso de cambio.			
Salida:			
• Especificación de los controles de seguridad de la aplicación. • Conocimientos de la aplicación y del paquete de software. • Decisiones de adquisición. • Especificación de disponibilidad, continuidad y recuperación.			
Aplicaciones:		Personal e Infraestructura:	
Garantizar que exista un proceso de desarrollo oportuno y confiable.		Consejo de Dirección	
Actividades:			
1. Traducir los requerimientos del negocio en especificaciones de diseño de alto nivel. 2. Preparar diseño detallado y los requerimientos técnicos del software aplicativo. 3. Especificar los controles de aplicación dentro del diseño. 4. Personalizar e implementar la funcionalidad automatizada adquirida. 5. Desarrollar un plan para el mantenimiento de aplicaciones de software.			

Tabla 3-19: Elementos de la arquitectura, Adquirir y mantener software aplicativo (AI2).

** Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición y mantenimientos de software aplicativo varían. Se ha adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.*

Controles propuestos:

Controles:
• **Procedimiento para la traducción de requerimientos de negocio a especificaciones de diseño:** Traducir los requerimientos del negocio a una especificación de diseño de alto nivel para desarrollo de software, tomando en cuenta las directivas tecnológicas y la arquitectura de información dentro de la organización, y aprobar las especificaciones de diseño para garantizar que el diseño de alto nivel responde a los requerimientos. • **Política de adhesión a los estándares de desarrollo para todas las modificaciones:** Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema. • **Procedimiento de separación de las actividades de desarrollo, de pruebas y operativas:** Se debe asegurar que las actividades de desarrollo concernientes a la fase de prueba se realicen de forma independiste a la operativa, siendo documentadas y ordenadas.

Tabla 3-20: Controles propuestos, Adquirir y mantener software aplicativo (AI2).

Elementos de la arquitectura:

Proceso:	**Adquirir y mantener infraestructura tecnológica**		**AI3**
Responsable(S):	Director		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Plan de infraestructura de tecnología; estándares y oportunidades, actualizaciones periódicas del 'estado de tecnología'. • Estándares de adquisición y desarrollo. • Descripción del proceso de cambio. • Plan de desempeño y capacidad (requerimientos).			
Salida:			
• Decisiones de adquisición. • Sistema configurado para realizar prueba / instalación. • Requerimientos de ambiente físico. • Actualizaciones de estándares de tecnología. • Requerimientos de monitoreo del sistema.			
Aplicaciones:		Personal e Infraestructura:	
Proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.		Consejo de Dirección	
Actividades:			
1. Definir el procedimiento/proceso de adquisición. 2. Negociar la compra y adquirir la infraestructura requerida con proveedores (aprobados). 3. Definir estrategia y planear el mantenimiento de infraestructura. 4. Configurar componentes de la infraestructura.			

Tabla 3-21: Elementos de la arquitectura, Adquirir y mantener la infraestructura tecnológica (AI3).

** 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.*

Controles propuestos:

Controles:
• **Procedimiento para el establecimiento de un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica:** Se debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica. • **Políticas de mantenimiento de la infraestructura:** Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlen 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. • **Políticas para la implantación de medidas de control interno, seguridad y auditabilidad:** Se debe implantar 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.

Tabla 3-22: Controles propuestos, Adquirir y mantener la infraestructura tecnológica (AI3).

Elementos de la arquitectura:

Proceso:	**Facilitar la operación y el uso**		**AI4**
Responsable(S):	Subdirector		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Directrices de administración del proyecto y planes detallados de proyecto. • Conocimientos de la aplicación y de software. • Conocimiento de la infraestructura. • Errores conocidos y admitidos. • Actualizaciones de documentación requeridas.			
Salida:			
• Manuales de usuario, de operación, de soporte, técnicos y de administración. • Requerimientos de transferencia de conocimiento para implantación de soluciones. • Materiales de entrenamiento.			
Aplicaciones:		Personal e Infraestructura:	
Proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitosos del sistema.		Jefes de Grupo	
Actividades:			
1. Desarrollar estrategia para que la solución sea operativa. 2. Desarrollar metodología de transferencia de conocimiento. 3. Desarrolla manuales de procedimiento del usuario final. 4. Desarrollar documentación de soporte técnica para operaciones y personal de soporte. 5. Desarrollar y dar entrenamiento. 6. Evaluar los resultados del entrenamiento y ampliar la documentación como se requiera.			

Tabla 3-23: Elementos de la arquitectura, Facilitar la operación y el uso (AI4).

** Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.*

Controles propuestos:

Controles:
• **Procedimiento de desarrollo y disponibilidad de documentación para transferir el conocimiento:** Se debe considerar que la transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente. • **Comunicación y entrenamiento a usuarios y a la gerencia del negocio, al personal de apoyo y al personal de operación:** Se temará en cuenta el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario. • **La generación de materiales de entrenamiento:** Se desarrollará un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.

Tabla 3-24: Controles propuestos, Facilitar la operación y el uso (AI4).

Elementos de la arquitectura:

Proceso:	**Procurar recursos de TI**		**AI5**
Responsable(S):	Subdirector		
Importancia:	Media	Nivel de Madurez:	Inicial/Ad Hoc*
Entrada:			
• Estrategia de adquisición de TI • Estándares de adquisición. • Directrices de administración de proyecto y planes detallados de proyecto. • Estudio de factibilidad de requerimientos del negocio. • Decisiones de adquisición. • Catálogo de proveedores.			
Salida:			
• Requerimientos de administración de la relación con terceros. • Artículos provistos. • Arreglos contractuales.			
Aplicaciones:		Personal e Infraestructura:	
Adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI.		Consejo de Dirección	
Actividades:			
1. Desarrollar políticas y procedimientos de adquisición de TI de acuerdo con las políticas de adquisiciones a nivel corporativo. 2. Establecer/mantener una lista de proveedores acreditados. 3. Evaluar y seleccionar proveedores a través de un proceso de solicitud de propuesta. 4. Desarrollar contratos que protejan los intereses de la organización. 5. Realizar adquisiciones de conformidad con los procedimientos establecidos.			

Tabla 3-25: Elementos de la arquitectura, Procurar recursos de TI (AI5).

** La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe un relación ad hoc entre los procesos de administración de adquisiciones y contratos corporativos y TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.*

Controles propuestos:

Controles:
• **Política de asesoría profesional legal y contractual:** Se garantizará la asesoría necesaria garantizando procedimientos que cubran, el mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad de propiedad intelectual y de conclusión, así como términos legales (que incluyan cláusulas de penalización). • **Política de definición de procedimientos y estándares de adquisición:** Se debe desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio. • **Procedimiento para la adquisición de hardware, software y servicios requeridos:** Se debe garantizar que se protejan los intereses de la organización en todos los acuerdos contractuales de adquisición. Incluir y reforzar los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de hardware, software y servicios requeridos involucrados en el suministro y uso continuo. Estos derechos y obligaciones pueden incluir la propiedad y licencia de propiedad intelectual, mantenimiento, garantías, procedimientos de arbitraje, condiciones para la actualización y aspectos de conveniencia que incluyen seguridad, custodia y derechos de acceso.

Tabla 3-26: Controles propuestos, Procurar recursos de TI (AI5).

Elementos de la arquitectura:

Proceso:	**Administrar los cambios**		**AI6**
Responsable(S):	Director		
Importancia:	Alta	Nivel de Madurez:	0 No existente*
Entrada:			
• Portafolio de proyectos TI. • Acciones de mejora de la calidad. • Planes de acción para solución de riesgos relacionados con TI. • Directrices de administración de proyecto y plan de proyecto detallado. • Cambios requeridos. • Cambios de seguridad requeridos. • Solicitudes de servicio / solicitudes de cambio. • Solicitudes de cambio (dónde y cómo aplicar la solución). • Registros de problemas.			
Salida:			
• Descripción de proceso de cambio. • Reportes de estatus de cambio. • Autorización de cambio.			
Aplicaciones:		Personal e Infraestructura:	
Controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados.		Consejo de Dirección	
Actividades:			
1. Desarrollar e implementar un proceso para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio. 2. Evaluar impacto y dar prioridad a cambios en base a las necesidades del negocio. 3. Garantizar que cualquier cambio crítico y de emergencia sigue el proceso aprobado. 4. Autorizar cambios. 5. Administrar y diseminar la información relevante referente a cambios.			

Tabla 3-27: Elementos de la arquitectura, Administrar los cambios (AI6).

** No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio.*

Controles propuestos:

Controles:
• **Política de definición y comunicación de los procedimientos de cambio, que incluyen cambios de emergencia:** Se establecerán 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. Se establecerá un proceso para definir, plantear, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido. La documentación y pruebas se realizan, posiblemente, después de la implantación del cambio de emergencia. • **Procedimiento para la evaluación, la asignación de prioridad y autorización de cambios:** Se 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. • **Política de seguimiento del estatus y reporte de los cambios:** Se deberá 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 a las aplicaciones, a los procedimientos, a los procesos, parámetros del sistema y del servicio y las plataformas fundamentales.

Tabla 3-28: Controles propuestos, Administrar los cambios (AI6).

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Instalar y acreditar soluciones y cambios</td><td>AI7</td></tr>
<tr><td>Responsable(S):</td><td colspan="3">Subdirector</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de Madurez:</td><td>1 Inicial/Ad Hoc*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Estándares de tecnología.
• Propietarios de sistema documentado.
• Estándares de desarrollo.
• Directrices de administración de proyecto y plan de proyecto detallado.
• Sistema configurado a ser probado/instalado.
• Manuales de usuario, operacionales, de soporte, técnicos y de administración.
• Adquisición de productos.
• Autorización de cambio.</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Componentes de configuración liberados.
• Errores conocidos y aceptados.
• Liberación a producción.
• Liberación de software y plan de distribución.
• Revisión posterior a la implantación.</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e Infraestructura:</td></tr>
<tr><td colspan="2">Probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libres de errores, y planear las liberaciones a producción.</td><td colspan="2">Consejo de Dirección</td></tr>
<tr><td colspan="4">Actividades:</td></tr>
<tr><td colspan="4">1. Construir y revisar planes de implantación.
2. Definir y revisar una estrategia de prueba (criterio de entrada y salida) y una metodología de plan de prueba operacional.
3. Construir y mantener un repositorio de requerimientos de negocio y técnicos y casos de prueba para sistemas acreditados.
4. Ejecutar la conversión del sistema y las pruebas de integración en ambiente de prueba.
5. Establecer ambiente de prueba y conducir pruebas de aceptación finales.</td></tr>
</table>

Tabla 3-29: Elementos de la arquitectura, Instalar y acreditar soluciones y cambios (AI7).

** Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares y los enfoques que se toman varían. La acreditación formal y la autorización son raras o no existentes.*

Controles propuestos:

Controles:
• **Procedimiento para el establecimiento de una metodología de prueba:** Se basará en los estándares de toda la organización y definirá roles, responsabilidades y criterios de éxito. Se considerará la preparación de pruebas (incluye la preparación del sitio), requerimientos de entrenamiento, instalación o actualización de un ambiente de pruebas definido, planear / ejecutar / documentar / retener casos de prueba, manejo y corrección de errores y aprobación formal. Con base en la evaluación de riesgos de fallas en el sistema y en la implantación, la metodología deberá incluir los requerimientos de prueba de desempeño, stress, de usabilidad, piloto y de seguridad. • **Política de evaluación y aprobación de los resultados de las pruebas por parte de la gerencia del negocio:** Se garantizará que los procedimientos proporcionen, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI. Las pruebas deberán cubrir todos los componentes del sistema de información (ejemplo, software aplicativo, instalaciones, procedimientos de tecnología y usuario) y garantizar que los requerimientos de seguridad de la información se satisfacen para todos los componentes. Los datos de prueba se deben salvar para propósitos de pistas de auditoría y para pruebas futuras. • **Procedimiento de ejecución de revisiones posteriores a la implantación:** Se establecerán procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.

Tabla 3-30: Controles propuestos, Instalar y acreditar soluciones y cambios (AI7).

2.7.3. Entregar y dar soporte.

Elementos de la arquitectura:

Proceso:	Definir y administrar los niveles de servicio		**DS1**
Responsable(S):	Consejo de Dirección		
Importancia:	Media	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Planes de TI tácticos y estratégicos, portafolio de servicios de TI. • Clasificaciones de datos asignados. • Portafolio de servicios de TI actualizado. • Requerimientos de servicio en caso de desastre incluyendo roles y responsabilidades. • Entrada de desempeño hacia la planeación de TI.			
Salida:			
• Reporte de revisión de contrato. • Reportes de desempeño de los procesos. • Requerimientos de servicio nuevos / actualizados. • Portafolio de servicios actualizado.			
Aplicaciones:		Personal e Infraestructura:	
Identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.		Jefes de Grupos	
Actividades:			
1. Crear un marco de trabajo para los definir servicios de TI. 2. Construir un catálogo de servicios de TI. 3. Monitorear y reportar el desempeño del servicio de punta a punta. 4. Revisar y actualizar el catálogo de servicios de TI. 5. Crear un plan de mejora de servicios.			

Tabla 3-31: Elementos de la arquitectura, Definir y administrar los niveles de servicio (DS1).

** Hay conciencia de la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas sobre para la definición y la administración de servicios no está definida. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa. La notificación es informal, infrecuente e inconsistente.*

Controles propuestos:

Controles:
• **Procedimiento para la definición de un marco de trabajo de la administración de los niveles de servicio:** Debe permitir la definición de un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio. El marco de trabajo mantiene una alineación continua con los requerimientos y las prioridades de negocio y facilita el entendimiento común entre el cliente y el(los) prestador(es) de servicio. El marco de trabajo incluye procesos para la creación de requerimientos de servicio, definiciones de servicio, acuerdos de niveles de servicio, acuerdos de niveles de operación y las fuentes de financiamiento. Estos atributos están organizados en un catálogo de servicios. El marco de trabajo define la estructura organizacional para la administración del nivel de servicio, incluyendo los roles, tareas y responsabilidades de los proveedores externos e internos y de los clientes. • **Procedimiento para el monitoreo y reporte del cumplimento de los niveles de servicio:** Debe permitir monitorear continuamente los criterios de desempeño especificados para el nivel de servicio. Los reportes sobre el cumplimiento de los niveles de servicio deben emitirse en un formato que sea entendible para los interesados. Las estadísticas de monitoreo son analizadas para identificar tendencias positivas y negativas tanto de servicios individuales como de los servicios en conjunto. • **Política de acuerdos de niveles de servicio y de los contratos:** Debe permitir revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

Tabla 3-32: Controles propuestos, Definir y administrar los niveles de servicio (DS1).

Elementos de la arquitectura:

Proceso:	Administrar el desempeño y la capacidad		**DS2**
Responsable(S):	Subdirector		
Importancia:		Nivel de Madurez:	2 Repetible pero intuitivo*
Entrada:			
• Especificaciones de disponibilidad, continuidad y de recuperación. • Requerimientos de monitoreo del sistema.			
Salida:			
• Información sobre desempeño y capacidad. • Plan de desempeño y capacidad (requerimientos). • Cambios requeridos. • Reportes de desempeño del proceso.			
Aplicaciones:		Personal e Infraestructura:	
Cumplir con los requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición.		Consejo de Dirección	
Actividades:			
1. Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI. 2. Revisar el desempeño y la capacidad actual de los recursos de TI. 3. Realizar pronósticos de desempeño y capacidad de los recursos de TI. 4. Realizar análisis de brecha para identificar incompatibilidad de los recursos de TI. 5. Realizar un plan de contingencia respecto a una potencial falta de disponibilidad de recursos de TI. 6. Monitorear y reportar continuamente la disponibilidad, el desempeño y la capacidad de los recursos de TI.			

Tabla 3-33: Elementos de la arquitectura, Administrar el desempeño y la capacidad (DS2).

** Los responsables del negocio y la gerencia de TI están consientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.*

Controles propuestos:

Controles:
• **Procedimiento para la planeación del desempeño y la capacidad:** Debe permitir establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, logrando procesar las cargas de trabajo acordadas. Los planes de capacidad y desempeño deben hacer uso de técnicas de modelado apropiadas para producir un modelo de desempeño, de capacidad y de rendimiento de los recursos de TI, tanto actual como pronosticado. • **Procedimiento para el monitoreando y reporte del desempeño del sistema:** De contribuir a monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida servirá para mantener y poner a punto el desempeño actual dentro de TI y atender temas como contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos y para reportar la disponibilidad hacia el negocio del servicio. Acompañar todos los reportes de excepción con recomendaciones para llevar a cabo acciones correctivas.

Tabla 3-34: Controles propuestos, Administrar el desempeño y la capacidad (DS2).

Elementos de la arquitectura:

Proceso:	Asegurar el servicio continúo		**DS3**
Responsable(S):	Subdirector		
Importancia:	Media	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Clasificaciones de datos asignados. • Valoración de riesgo. • Especificación de disponibilidad, continuidad y recuperación. • Manuales, de usuario, técnicos, operativos, de soporte y de administración.			
Salida:			
• Resultados de las prueba de contingencia. • Criticidad de puntos de configuración de TI. • Plan de almacenamiento de respaldos y de protección. • Umbrales de incidente/desastre. • Requerimientos de servicios contra desastres incluyendo roles y responsabilidades. • Reportes de desempeño de los procesos.			
Aplicaciones:		Personal e Infraestructura:	
Desarrollo de resistencia en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI.		Jefes de Grupos Administrador de Red	
Actividades:			
1. Desarrollar un marco de trabajo de continuidad de TI. 2. Realizar un análisis de impacto al negocio y valoración de riesgo. 3. Desarrollar y mantener planes de continuidad de TI. 4. Identificar y categorizar los recursos de TI con base en los objetivos de recuperación. 5. Definir y ejecutar procedimientos de control de cambios para asegurar que el plan de continuidad sea vigente. 6. Probar regularmente el plan de continuidad de TI. 7. Desarrollar un plan de acción a seguir con base en los resultados de las pruebas. 8. Planear y llevar a cabo capacitación sobre los planes de continuidad de TI. 9. Planear la recuperación y reanudación de los servicios de TI. 10. Planear e implementar el almacenamiento y la protección de respaldos. 11. Establecer los procedimientos para llevar a cabo revisiones post-reanudación.			

Tabla 3-35: Elementos de la arquitectura, Asegurar el servicio continúo (DS3).

** Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.*

Controles propuestos:

Controles:
• **Política de desarrollando de planes de continuidad de TI:** Debe permitir el desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas. • **Política de prueba del plan de continuidad de TI:** Debe permitir la comprobación del plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor. • **Procedimiento para guardando copias de los planes de contingencia y de los datos fuera de las instalaciones:** Debe permitir almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

Tabla 3-36: Controles propuestos, Asegurar el servicio continúo (DS3).

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Garantizar la seguridad de los sistemas</td><td>DS4</td></tr>
<tr><td>Responsable(S):</td><td colspan="3">Subdirector</td></tr>
<tr><td>Importancia:</td><td>Alta</td><td>Nivel de Madurez:</td><td>3 Proceso definido*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Arquitectura de Información; clasificación de datos asignados.
• Estándares de tecnología.
• Evaluación de riesgo.
• Especificaciones de controles de seguridad en las aplicaciones.</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Definición de incidentes de seguridad.
• Requerimientos específicos de entrenamiento sobre conciencia de seguridad.
• Reportes de desempeño del proceso.
• Cambios de seguridad requeridos.
• Amenazas y vulnerabilidades de seguridad.</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e Infraestructura:</td></tr>
<tr><td colspan="2">Definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.</td><td colspan="2">Jefes de Grupos
Administrador de Red</td></tr>
<tr><td colspan="4">Actividades:</td></tr>
<tr><td colspan="4">1. Definir y mantener un plan de seguridad de TI.
2. Definir, establecer y operar un proceso de administración de identidad (cuentas).
3. Monitorear incidentes de seguridad, reales y potenciales.
4. Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios.
5. Establecer y mantener procedimientos para mantener y salvaguardar las llaves criptográficas.
6. Implementar y mantener controles técnicos y de procedimiento para proteger el flujo de información a través de las redes.
7. Realizar evaluaciones de vulnerabilidad de manera regular.</td></tr>
</table>

Tabla 3-37: Elementos de la arquitectura, Garantizar la seguridad de los sistemas (DS4).

** Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.*

Controles propuestos:

Controles:
• **Procedimiento para la elaboración del plan de seguridad de TI:** Debe contribuir a trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios. • **Política de administración de identidades y autorizaciones:** Debe permitir que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deban ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo. Los derechos de acceso del usuario son solicitados por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se implementan y se mantienen actualizadas medidas técnicas y procedimientos rentables, para establecer la identificación del usuario, realizar la autenticación y habilitar los derechos de acceso. • **Procedimiento de pruebas, vigilancia y monitoreo de la seguridad:** Debe garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser re acreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención. El acceso a la información de ingreso al sistema está alineado con los requerimientos del negocio en términos de requerimientos de retención y de derechos de acceso.

Tabla 3-38: Controles propuestos, Garantizar la seguridad de los sistemas (DS4).

Elementos de la arquitectura:

Proceso:	Educar y entrenar a los usuarios		**DS5**
Responsable(S):	Subdirector		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Habilidades y competencias de los usuarios, incluyendo el entrenamiento individual y los requerimientos específicos de entrenamiento. • Materiales de entrenamiento; requerimientos de transferencia del conocimiento para implementación de soluciones. • Requerimientos específicos de entrenamiento sobre conocimientos de seguridad. • Reportes de satisfacción de usuario.			
Salida:			
• Reportes de desempeño de procesos. • Actualizaciones de documentación requeridas.			
Aplicaciones:		Personal e Infraestructura:	
Entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados.		Consejo de Dirección	
Actividades:			
1. Identificar y categorizar las necesidades de capacitación de los usuarios. 2. Construir un programa de capacitación. 3. Realizar actividades de capacitación, instrucción y concientización. 4. Llevar a cabo evaluaciones de la capacitación. 5. Identificar y evaluar los mejores métodos y herramientas para impartir la capacitación.			

Tabla 3-39: Elementos de la arquitectura, Educar y entrenar a los usuarios (DS5).

** Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos de entrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre la seguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.*

Controles propuestos:

Controles:
• **Política de entrenamiento y educación:** Debe permitir el establecimiento y actualización de forma regular un programa de entrenamiento para cada grupo objetivo de empleados, que incluya: Estrategias y requerimientos actuales y futuros del negocio. Valores corporativos (valores éticos, cultura de control y seguridad, etc.) Implementación de nuevo software e infraestructura de TI (paquetes y aplicaciones). Habilidades, perfiles de competencias y certificaciones actuales y/o credenciales necesarias. Métodos de impartición (por ejemplo, aula, web), tamaño del grupo objetivo, accesibilidad y tiempo. • **Procedimiento para la impartición de entrenamiento y educación:** Con base en las necesidades de entrenamiento identificadas, identificar: a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros. Designar instructores y organizar el entrenamiento con tiempo suficiente. Debe tomarse nota del registro (incluyendo los prerrequisitos), la asistencia, y de las evaluaciones de desempeño. • **Procedimiento para la evaluación del entrenamiento**: Debe posibilitar que al finalizar del entrenamiento, evaluar el contenido del entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor. Los resultados de esta evaluación deben contribuir en la definición futura de los planes de estudio y de las sesiones de entrenamiento.

Tabla 3-40: Controles propuestos, Educar y entrenar a los usuarios (DS5).

Elementos de la arquitectura:

Proceso:	Administrar la mesa de servicio y los incidentes		**DS6**
Responsable(S):	Director		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Manuales de usuario, de operación, técnicos y de administración. • Autorización de cambios. • Puntos de configuración liberados. • Umbrales de incidente/ desastre. • Definición de incidente de seguridad. • Detalles de configuración/activos de TI. • Problemas conocidos, errores conocidos y soluciones alternas. • Tiquetes de incidente.			
Salida:			
• Solicitud de servicio / solicitud de cambio. • Reportes de incidentes. • Reportes de desempeño de procesos. • Reportes de satisfacción de usuarios.			
Aplicaciones:		Personal e Infraestructura:	
Una función profesional de mesa de servicio, con tiempo de respuesta rápido, procedimientos de escalamiento claros y análisis de tendencias y de resolución.		Consejo de Dirección	
Actividades:			
1. Crear procedimientos de clasificación (severidad e impacto) y de escalamiento (funcional y jerárquico) 2. Detectar y registrar incidentes / solicitudes de servicio / solicitudes de información 3. Clasificar, investigar y diagnosticar consultas 4. Resolver, recuperar y cerrar incidentes 5. Informar a usuarios (por ejemplo, actualizaciones de estatus) 6. Hacer reportes para la gerencia			

Tabla 3-41: Elementos de la arquitectura, Administrar la mesa de servicio y los incidentes (DS6).

** 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 dirección 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.*

Controles propuestos:

Controles:
• **Procedimiento para la instalación y operación de la mesa de servicios:** Debe contribuir a 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. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados, que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI. • **Política de monitoreo y análisis de tendencias:** Debe permitir la emisión de reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

Tabla 3-42: Controles propuestos, Administrar la mesa de servicio y los incidentes (DS6).

Elementos de la arquitectura:

Proceso:	Administrar la configuración		**DS7**
Responsable(S):	Subdirector		
Importancia:	Media	Nivel de Madurez:	2 Repetible pero intuitivo*
Entrada:			
• Manuales, de usuario, técnicos, de soporte y de administración. • Elementos de configuración liberados. • Criticidad de los elementos de configuración de TI.			
Salida:			
• Configuración de TI / detalles de activos. • Solicitud de cambio (donde y como aplicar el parche). • Reportes de desempeño del proceso.			
Aplicaciones:		Personal e Infraestructura:	
Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.		Jefes de Grupos Administrador de Red	
Actividades:			
1. Desarrollar procedimientos de planeación de administración de la configuración. 2. Recopilar información sobre la configuración inicial y establecer líneas base. 3. Verificar y auditar la información de la configuración (incluye la detección de software no autorizado). 4. Actualizar el repositorio de configuración.			

Tabla 3-43: Elementos de la arquitectura, Administrar la configuración (DS7).

** La dirección esta consiente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales como administración de cambios y administración de problemas.*

Controles propuestos:

Controles:
• **Política para el establecimiento de un repositorio central de todos los elementos de la configuración:** Debe establecer un repositorio central que contenga toda la información referente a los elementos de configuración. Este repositorio incluye hardware, software aplicativo, middleware, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas y los servicios. La información importante a considerar es el nombre, números de versión y detalles de licenciamiento. Una línea base de elementos de configuración debe mantenerse para cada sistema y servicio, como un punto de control al cual regresar después de realizar cambios. • **Procedimiento para la identificación de los elementos de configuración y su mantenimiento: Debe contar con procedimientos en orden para:** Identificar elementos de configuración y sus atributos. Registrar elementos de configuración nuevos, modificados y eliminados. Identificar y mantener las relaciones entre los elementos de configuración y el repositorio de configuraciones. Actualizar los elementos de configuración existentes en el repositorio de configuraciones. Prevenir la inclusión de software no-autorizado. • **Procedimiento de revisión de la integridad de los datos de configuración**: Debe permitir revisar y verificar de manera regular, utilizando cuando sea necesario herramientas apropiadas, el estatus de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica y para comparar con la situación actual. Revisar periódicamente contra la política de uso de software, la existencia de cualquier software personal o no autorizado de cualquier instancia de software por encima de los acuerdos de licenciamiento actuales. Los errores y las desviaciones deben reportarse, atenderse y corregirse.

Tabla 3-44: Controles propuestos, Administrar la configuración (DS7).

Elementos de la arquitectura:

Proceso:	Administrar los problemas		**DS8**
Responsable(S):	Director		
Importancia:	Media	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Autorización de cambio. • Reportes de incidentes. • Detalles de activos / configuración de TI. • Bitácoras de errores.			
Salida:			
• Solicitud de cambio. • Registros de problemas. • Reportes de desempeño del proceso. • Problemas conocidos, errores conocidos y soluciones alternas.			
Aplicaciones:		Personal e Infraestructura:	
Registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados.		Consejo de Dirección	
Actividades:			
1. Identificar y clasificar problemas 2. Realizar análisis de causa raíz 3. Resolver problemas 4. Revisar el estatus de problemas 5. Emitir recomendaciones para mejorar y crear una solicitud de cambio relacionada 6. Mantener registros de los problemas			

Tabla 3-45: Elementos de la arquitectura, Administrar los problemas (DS8).

** Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.*

Controles propuestos:

Controles:
• **Procedimiento para la identificación y clasificación de problemas:** Debe permitir la implementación de procesos para reportar y clasificar problemas que hayan sido identificados como parte de la administración de incidentes. Los pasos involucrados son: determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte. • **Política de rastreo y resolución de problemas:** Debe contribuir a que el sistema de administración de problemas mantenga pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando: todos los elementos de configuración asociados, problemas e incidentes sobresalientes, errores conocidos y sospechados.

Tabla 3-46: Controles propuestos, Administrar los problemas (DS8).

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="3">Administrar los datos</td><td>DS9</td></tr>
<tr><td>Responsable(S):</td><td colspan="4">Subdirector</td></tr>
<tr><td>Importancia:</td><td>Alta</td><td>Nivel de Madurez:</td><td colspan="2">1 Inicial/Ad Hoc*</td></tr>
<tr><td colspan="5">Entrada:</td></tr>
<tr><td colspan="5">• Clasificaciones de datos asignados.
• Manuales de usuario, de operación, de soporte, técnicos y de administración.
• Plan de protección y de almacenamiento de respaldos.</td></tr>
<tr><td colspan="5">Salida:</td></tr>
<tr><td colspan="5">• Reportes de desempeño del proceso.
• Instrucciones del operador para administración de datos.</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="3">Personal e Infraestructura:</td></tr>
<tr><td colspan="2">Mantener la integridad, exactitud, disponibilidad y protección de los datos.</td><td colspan="3">Jefes de Grupos
Administrador de Red</td></tr>
<tr><td colspan="5">Actividades:</td></tr>
<tr><td colspan="5">1. Traducir los requerimientos de almacenamiento y conservación a procedimientos.
2. Definir, mantener e implementar procedimientos para administrar librerías de medios.
3. Definir, mantener e implementar procedimientos para desechar de forma segura medios y equipo.
4. Respaldar los datos de acuerdo al esquema.
5. Definir, mantener e implementar procedimientos para restauración de datos.</td></tr>
</table>

Tabla 3-47: Elementos de la arquitectura, Administrar los datos (DS9).

** La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal. No se lleva a cabo capacitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Los procedimientos de respaldo y recuperación y los acuerdos sobre desechos están en orden.*

Controles propuestos:

Controles:
• **Procedimiento para el respaldo de datos y comprobación de restauración**: Debe contribuir a definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad. Verificar el cumplimiento de los procedimientos de respaldo y verificar la capacidad y el tiempo requerido para tener una restauración completa y exitosa. Probar los medios de respaldo y el proceso de restauración. • **Política de almacenamiento y conservación de datos**: Debe permitir la aplicación de procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encriptación y autenticación.

Tabla 3-48: Controles propuestos, Administrar los datos (DS9).

Elementos de la arquitectura:

Proceso:	Administrar las operaciones		**DS10**
Responsable(S):	Subdirector		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Manuales de usuario, técnicos, operación y administración. • Plan de almacenamiento y protección de respaldos. • Configuración de TI / detalle de los activos de TI. • Instrucciones del operador para administración de datos.			
Salida:			
• Tiquetes de incidentes. • Bitácoras de errores. • Reportes de desempeño de los procesos.			
Aplicaciones:		Personal e Infraestructura:	
Cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura.		Jefes de Grupos Administrador de Red	
Actividades:			
1. Crear / modificar procedimientos de operación (incluyendo manuales, planes de cambios, procedimientos de escalamiento, etc.) 2. Programación de cargas de trabajo y de programas en lote. 3. Monitorear la infraestructura y procesar y resolver problemas 4. Administrar y asegurar la salida física de información (reportes, medios, etc.) 5. Aplicar cambios o arreglos al programa y la infraestructura 6. Implementar / establecer un proceso para salvaguardar los dispositivos de autenticación contra interferencia, perdida o robo. 7. Programar y llevar a cabo mantenimiento preventivo.			

Tabla 3-49: Elementos de la arquitectura, Administrar las operaciones (DS10).

** La organización reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen.*

Controles propuestos:

Controles:
• **Procedimiento para la operación del ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas:** Debe definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones. • **Política de manteniendo de la infraestructura de TI:** Debe contribuir a definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizando que en los registros de operación se almacene suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

Tabla 3-50: Controles propuestos, Administrar las operaciones (DS10).

2.7.4. Monitorear y evaluar.

Elementos de la arquitectura:

Proceso:	Monitorear y evaluar el desempeño de TI		**ME1**
Responsable(S):	Subdirector		
Importancia:	Alta	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Reportes de desempeño del proyecto. • Reportes del estatus de los cambios. • Reportes de desempeño del proceso. • Reportes de satisfacción del usuario. • Reportes de la efectividad de los controles de TI. • Reportes sobre el cumplimiento de las actividades de TI respecto a requerimientos legales y regulatorios externos. • Reportes sobre el estatus del gobierno de TI.			
Salida:			
• Retro-alimentación de desempeño para la planeación de TI. • Planes de acciones correctivas. • Tendencias y eventos de riesgos históricos. • Reporte de desempeño del proceso.			
Aplicaciones:		Personal e Infraestructura:	
Monitorear y reportar las métricas del proceso e identificar e implantar acciones de mejoramiento del desempeño.		Jefes de Grupos	
Actividades:			
7. Establecer el enfoque de monitoreo. 8. Identificar y recolectar objetivos medibles que apoyen a los objetivos del negocio. 9. Evaluar el desempeño. 10. Reportar el desempeño. 11. Identificar y monitorear las medidas de mejora del desempeño.			

Tabla 3-51: Elementos de la arquitectura, Monitorear y evaluar el desempeño de TI (ME1)

** La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.*

Controles propuestos:

Controles:
• **Procedimiento para la definición y recolección de datos de monitoreo:** Debe garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes. Los indicadores de desempeño deberán incluir: 1. Desempeño contra el plan estratégico del negocio y de TI 2. Riesgo y cumplimiento de las regulaciones 3. Satisfacción del usuario interno y externo 4. Procesos clave de TI que incluyan desarrollo y entrega del servicio 5. Actividades orientadas a futuro, por ejemplo, la tecnología emergente, la infraestructura re-utilizable, habilidades del personal de TI y del negocio. • **Política de realización de medidas correctivas:** Debe permitir identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con: 1. Revisión, negociación y establecimiento de respuestas administrativas 2. Asignación de responsabilidades por la corrección 3. Rastreo de los resultados de las acciones comprometidas

Tabla 3-52: Controles propuestos, Monitorear y evaluar el desempeño de TI (ME1)

Elementos de la arquitectura:

Proceso:	Monitorear y evaluar el control interno		**ME2**
Responsable(S):	Subdirector		
Importancia:	Media	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Reporte de desempeño de procesos.			
Salida:			
• Reporte sobre la efectividad de los controles de TI.			
Aplicaciones:		Personal e Infraestructura:	
El monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento.		Jefes de Grupos	
Actividades:			
1. Monitorear y controlar las actividades de control interno de TI. 2. Monitorear el proceso de auto-evaluación. 3. Monitorear el desempeño de las revisiones, auditorías y exámenes independientes. 4. Monitorear el proceso para identificar y evaluar las excepciones de control. 5. Monitorear el proceso para identificar y evaluar y remediar las excepciones de control. 6. Reportar a los terceras partes interesadas.			

Tabla 3-53: Elementos de la arquitectura, Monitorear y evaluar el control interno (ME2)

**La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.*

Controles propuestos:

Controles:
• **Procedimiento para el monitoreo del marco de trabajo de control interno:** Debe monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se deberá utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI. • **Procedimiento para reportar las excepciones de control a la gerencia:** Debe registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones se deberían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas. • **Procedimiento para la realización de acciones correctivas:** Debe identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con: 1. La revisión, negociación y establecimiento de respuestas administrativas. 2. La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos). 3. El rastreo de los resultados de las acciones comprometidas.

Tabla 3-54: Controles propuestos, Monitorear y evaluar el control interno (ME2)

Elementos de la arquitectura:

Proceso:	Garantizar el cumplimiento regulatorio		**ME3**
Responsable(S):	Director		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Requerimientos de cumplimiento legal y regulatorio.			
Salida:			
• Catálogo de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI. • Reporte sobre el cumplimiento de las actividades de TI con los requerimientos externos legales y regulatorios.			
Aplicaciones:		Personal e Infraestructura:	
Identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.		Consejo de Dirección	
Actividades:			
1. Definir y ejecutar un proceso para identificar los requerimientos legales, contractuales, de políticas y regulatorios. 2. Evaluar cumplimiento de actividades de TI con políticas, estándares y procedimientos de TI 3. Reportar el aseguramiento del cumplimiento de las actividades de TI con las políticas, estándares y procedimientos de TI. 4. Brindar retroalimentación para alinear las políticas, estándares y procedimientos de TI con los requerimientos de cumplimiento. 5. Integrar los reportes de TI sobre requerimientos regulatorios con similares provenientes de otras funciones del negocio.			

Tabla 3-55: Elementos de la arquitectura, Garantizar el cumplimiento regulatorio (ME3).

** Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorías o revisiones.*

Controles propuestos:

Controles:
• **Procedimiento para la identificación de los requisitos legales y regulatorios relacionados con la TI:** Debe definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI. Tomar en cuenta las leyes y reglamentos de comercio electrónico, flujo de datos, privacidad, controles internos, reportes financieros, reglamentos específicos de la industria, propiedad intelectual y derechos de autor, además de salud y seguridad. • **Procedimiento para la evaluación del impacto de los requisitos regulatorios:** Debe permitir la evaluación de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.

Tabla 3-56: Controles propuestos, Garantizar el cumplimiento regulatorio (ME3).

Elementos de la arquitectura:

Proceso:	Proporcionar gobierno de TI		**ME4**
Responsable(S):	Director		
Importancia:	Baja	Nivel de Madurez:	1 Inicial/Ad Hoc*
Entrada:			
• Marco de trabajo del proceso de TI. • Evaluación y reportes de riesgo. • Reportar la efectividad de los controles de TI. • Catálogo de requisitos legales y regulatorios relacionados con la prestación de servicios de TI.			
Salida:			
• Mejoras al marco de trabajo de los procesos. • Reportar el estatus del gobierno de TI. • Resultados de negocio esperados de las inversiones en TI. • Dirección estratégica empresarial para TI. • Apetito empresarial de riesgos de TI.			
Aplicaciones:		Personal e Infraestructura:	
Elaboración de informes para el consejo de dirección sobre la estrategia, el desempeño y los riesgos de TI y responder a los requerimientos de gobierno de acuerdo a las directrices del consejo de dirección.		Subdirector	
Actividades:			
1. Establecer visibilidad y facilitación del consejo y de los ejecutivos hacia las actividades de TI 2. Revisar, avalar, alinear y comunicar el desempeño de TI, la estrategia de TI, el manejo de recursos y riesgos de TI con respecto a la estrategia empresarial. 3. Obtener evaluaciones independientes periódicas del desempeño, y del cumplimiento con las políticas, estándares y procedimientos. 4. Resolver los hallazgos de las evaluaciones independientes y garantizar la implantación por parte de la gerencia de las recomendaciones acordadas. 5. Generar un reporte de gobierno de TI.			

Tabla 3-57: Elementos de la arquitectura, Proporcionar gobierno de TI (ME4).

** Se reconoce que el tema del gobierno de TI existe y que debe ser resuelto. Existen enfoques ad hoc aplicados individualmente o caso por caso. El enfoque de la gerencia es reactivo y solamente existe una comunicación esporádica e inconsistente sobre los temas y los enfoques para resolverlos. La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio. La gerencia solo responde de forma reactiva a los incidentes que hayan causado pérdidas o vergüenza a la organización.*

Controles propuestos:

Controles:
• **Procedimiento para establecer un marco de trabajo de gobierno para TI:** Debe permitir el trabajo con el consejo de dirección para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales. El marco de trabajo debería proporcionar vínculos claros entre la estrategia empresarial, el portafolio de programas de inversiones habilitadas por TI que ejecutan la estrategia, los programas de inversión individual y los proyectos de negocio y de TI que forman los programas. El marco de trabajo debería definir una rendición de cuentas y prácticas incontrovertibles para evitar fallas de control interno y de supervisión. El marco de trabajo debería ser consistente con el ambiente completo de control empresarial y con los principios de control generalmente aceptados y estar basado en el proceso y en el marco de control de TI. • **Política de aseguramiento independiente**: Debe garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo– esto ocurrirá probablemente a través de un comité de auditoría – aseguramiento independiente y oportuno sobre el cumplimiento que tiene TI respecto a sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas.

Tabla 3-58: Controles propuestos, Proporcionar gobierno de TI (ME4).

Conclusiones

Con la realización de esta investigación se logró dar respuesta a las interrogantes y objetivos propuestos inicialmente, ya que se diseñó una metodología basada en el marco de trabajo de Cobit, que guía la implementación adecuada de un marco de controles de TI.

Se definió que la Casa de Autoría DVD se encuentra en un nivel 1 en cuanto a los controles de TI, y se propone alcanzar el nivel 5 en la escala de madurez.

Se diseñó la arquitectura empresarial de TI y se elaboraron los controles necesarios para que el proceso productivo de la Casa esté acorde con las mejores Prácticas Internacionales y brinde un adecuado Gobierno de TI que permita cumplir con los objetivos del negocio.

Recomendaciones

Estudiar la posible implementación de otros estándares mas específicos como ITIL e ISO 27001en la Casa de Autoría DVD.

El estudio de Cobit y su posible implementación en los diferentes procesos de la Universidad de las Ciencias Informáticas.

Incluir el estudio de los estándares internacionales de Gobierno de TI en el plan de estudio de la carrera de Ingeniería en Ciencias informáticas.

BIBLIOGRAFÍA

Aligning COBIT, ITIL and ISO 17799 for Business Benefit. ISACA, 2007]. Disponible en: http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/AligningCOBIT,ITIL.pdf

COBIT. 4ta edición. ITGI, 2005. p. ISBN 1-933284-37-4

COBIT Objetivos de Control. 3a edición. ISACA, 2000. p. ISBN 1-893209-99-7

COBIT Edición 4.0. ISACA. [En línea] 2005.

http://www.isaca.org/Template.cfm?Section=Downloads5&CONTENTID=31413. ISBN 1-933284-37-4.

ESTRADA, A. C. El standard ISO 27001 y su aplicación en las PyMEs. VIII Seminario Iberoamericano de Seguridad en Tecnologías de la Información. La Habana, 2007.

IRCA. ¿Qué es la norma ISO 20000:2005?: Inform, IRCA, Registro Internacional de Auditores Certificados, 2006. 12.

Implementación del modelo COBIT en el desarrollo de las Auditorías Informáticas. Vandama, Nancy y Lescay, Milagros. La Habana : s.n., 2002. Simposio Latinoamericano y del Caribe, La Educación, La Ciencia y la Cultura en la Sociedad de la Información, SimpLAC 2002.

ISO/IEC 17799. 2005. [2007]. Disponible en:

http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612

ISO/IEC 20000-1:2005. ISO/IEC, 2007]. Disponible en:

http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41332

ISO/IEC 20000-2:2005. ISO/IEC, 2007]. Disponible en:

http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41333

ISO/IEC 27001. ISO, 2005. [2007]. Disponible en:

http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42103

ORTÍZ, S. G. C. and D. F. J. P. MARTÍNEZ. ITIL: servicios de tecnologías de información, 2005. [2007]. Disponible en: http://www.enterate.unam.mx/Articulos/2005/noviem/itil.htm

VANDAMA, N. and M. LESCAY. Implementación del modelo COBIT en el desarrollo de las Auditorías Informáticas. Simposio Latinoamericano y del Caribe, La Educación, La Ciencia y la Cultura en la Sociedad de la Información, SimpLAC 2002 La Habana, Cuba, UNESCO, 2002.

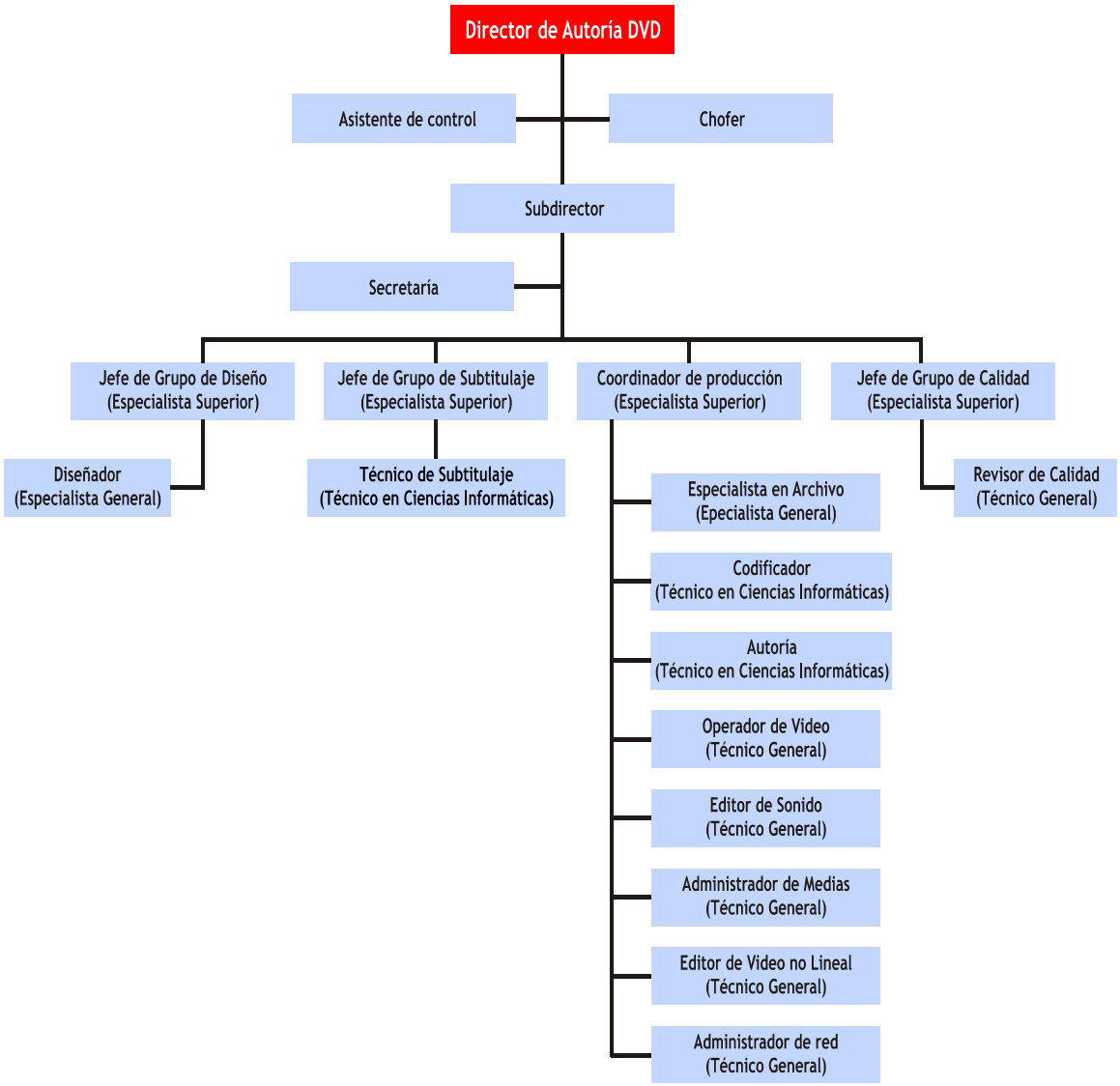
Sitios Web Visitados

www.isaca.org

www.iso.org

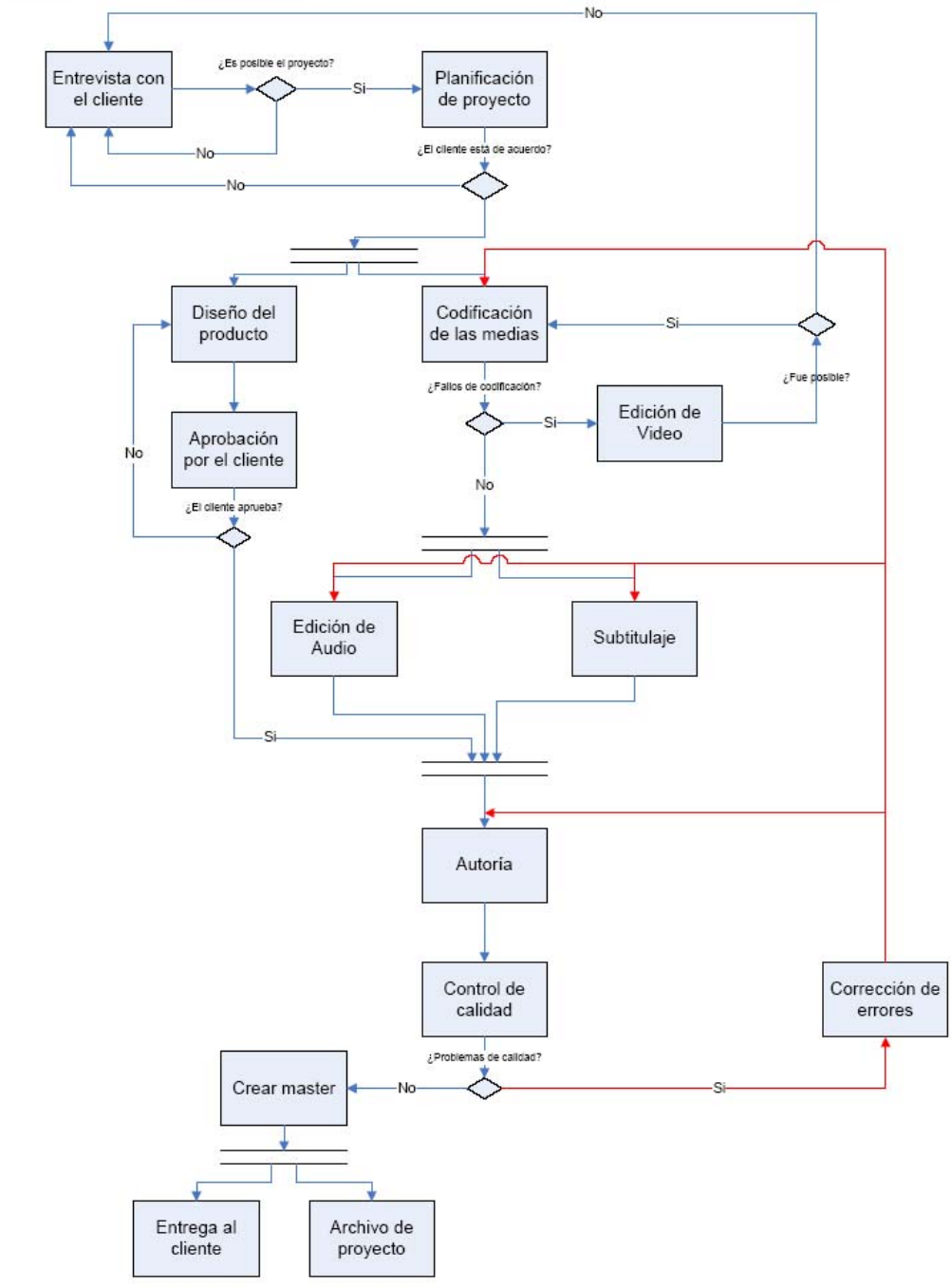
ANEXOS

Anexo 1



Anexo 2

Flujo productivo. Casa de Autoría DVD de la UCI



GLOSARIO DE TÉRMINOS Y SIGLAS

Términos:

Ad hoc: es una locución latina que significa literalmente «para esto». Generalmente se refiere a una solución elaborada específicamente para un problema o fin preciso y, por tanto, no es generalizable ni utilizable para otros propósitos. Se usa pues para referirse a algo que es adecuado sólo para un determinado fin. En sentido amplio, ad hoc puede traducirse como «específico» o «específicamente».

Ambiente 5.1: ambiente acústico que cuenta con 6 canales de audio cubriendo un área de 360 grados sobre el centro.

Audio nativo: pista de audio en formato LPCM.

Backup: (Copia de seguridad) Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento. Esta copia de respaldo debe ser guardada en algún otro sistema de almacenamiento masivo, como ser discos duros, CDs, DVDs o cintas magnéticas (DDS, Travan, AIT, SLR,DLT y VXA).

Betacam digital: graba usando una señal de vídeo por componentes comprimida con el algoritmo DCT (el ratio de compresión es variable, normalmente alrededor de 2:1). Su profundidad de color es de 10 bit y su frecuencia de muestreo es 4:2:2 en PAL (720x576) y NTSC (720x486), con el resultado de un bitrate de 90 Mb/s. En cuanto a sonido proporciona 4 canales de audio PCM a 48 KHz y 20 bits. Incluye dos pistas longitudinales para control track y código de tiempo.

Betacam SP: sistema analógico de vídeo por componentes, que almacena la luminancia (Y) en una pista y la crominancia (Y-R, Y-B) en otra distinta. La separación de las señales proporciona una calidad suficiente para un entorno broadcast y 340 líneas verticales de resolución.

Betacam SX: es un formato digital creado en 1996, con la idea de ser una alternativa más barata al Betacam Digital, especialmente para trabajos ENG. Comprime la señal por componentes usando MPEG-2 4:2:2 Profile@ML (MPEG-2 4:2:2P@ML), con 4 canales de audio PCM a 48 KHz y 16 bits. Betacam SX es compatible con cintas de Betacam SP. El tamaño S guarda hasta 64 minutos y el tamaño L, hasta 194.

Bitrate: "Tasa de bits": Velocidad de transferencia de información (audio, vídeo y subtítulos) de un disco a la computadora o al reproductor. Se expresa en Kbps (kilobit = 1,000 bits por

segundo) o en Mbps (megabit = 1,000,000 bits por segundo). Como es sabido (suponemos), un byte son 8 bits.

Codificación: almacenamiento de audio y video para un DVD empleando un sistema de compresión con pérdida.

Código de tiempo continúo: contador de tiempo interno usado en las cintas de video tape.

Desfase: Cuando no coinciden la imagen y el sonido.

Digitalización: proceso donde se codifican señales de audio y video.

Dolby Digital: formato de compresión de audio (también conocido como "AC-3"), desarrollado por Dolby Laboratories. Es un formato digital, multi-canal, que usa una tecnología de codificación "con pérdidas" (se elimina la parte de la información sobre el sonido que supuestamente es más difícil de percibir por el oído humano).

DVCAM: es el nombre de la versión propia de Sony. Tiene las mismas características que el DV, pero Sony amplió el ancho de pista a 15 µm y aumentó en un 50 por ciento la velocidad de cinta. Esto repercute en mayor calidad, pero también en que las cintas duren un tercio que las del formato original. DVCAM puede grabar en cintas DVCAM y Mini DV y reproduce DV y DVCPRO -no desde el principio del formato.

DVCPro 25: es la variante del DVC desarrollada por Panasonic. Al contrario que Sony, se apostó fuerte por este formato y se ha convertido en una importante franquicia con tres versiones desarrolladas hasta el año 2006. Su principal diferencia es que usa cinta con pistas de ancho de 18 µm y con otro tipo de emulsión, partículas de metal en lugar de metal evaporado -usado en DVC y DVCAM-. Además, cuenta con una pista longitudinal de audio y otra también longitudinal de control track para ayudar en edición, especialmente edición lineal. Otra característica respecto al audio es que sólo permite la opción de 2 pistas a 48 KHz y 16 bit.

DVCPro 50: es una versión de mayor calidad que creó JVC en cinta de 1/2" pulgada llamada D9 (Digital S) con muestreo 4:2:2 a 50Mbps y compresión 3.3:1 utilizando dos codificadores de DV en paralelo con 4 pistas de audio PCM, y que posteriormente adoptó Panasonic como mejora de su DVCpro, pensando no sólo en cometidos ENG, sino en poder ofrecer aplicaciones de estudio. Lógicamente la capacidad de las cintas es la mitad de la proporcionada por DVCPRO 25.

Estéreo: pista de audio con dos canales L (izquierdo), R (derecho).

Máster: es el producto final de la autoría y que fue certificado por calidad.

MPEG: (Moving Pictures Expert Group - Grupo de expertos en imágenes en movimiento). Grupo de trabajo de ISO/IEC encargado del desarrollo de estándares de codificación de video y audio. Su primer encuentro fue en Mayo de 1988 en Ottawa (Canadá) con unos pocos miembros. Actualmente incluye más de 350 miembros por reunión provenientes de industrias, universidades e institutos de investigación. El nombre oficial de MPEG es ISO/IEC JTC1/SC29 WG11.

Algunos de los formatos de compresión que ha estandarizado MPEG son:

* MPEG-1: Estándar inicial para la compresión de video y audio. Usado como estándar en Video CD e incluido en el formato de audio MP3 (Layer 3).

* MPEG-2: Estándar para la transmisión de televisión. Usado para la televisión digital ATSC, DVS y ISDB, señales digitales de televisión por cable, y (con pequeñas modificaciones) para DVD.

* MPEG-3: Originalmente fue diseñado para la televisión de alta definición (HDTV), fue abandonado cuando descubrieron que el MPEG-2 (con extensiones) era suficiente para la HDTV.

* MPEG-4: Expande el MPEG-1 para soportar objetos video/audio, contenido 3D, soporte para Digital Rights Management, y codificación de bajo bitrate. Existen varias versiones, la más importante es la MPEG-4 Part 10 (o Advanced Video Coding o H.264). Es usado en HD-DVD y discos Blu-ray.

Multicopiado: proceso donde se hacen varias copias de un DVD.

Parlamentos: párrafos.

Pre-máster: Es el primer DVD correspondiente a un proyecto generado en el proceso de Autoría.

Sonic Scenarist: Software para la Autoría de DVD.

Stakeholders: es un interesado en que el proyecto resulte, es alguien a quien beneficiará el éxito del proyecto, y el fracaso del proyecto perjudicará. Cualquier persona o grupo que se verá, directa o indirectamente, afectado por el proyecto a ser desarrollado.

Subtitulaje: proceso en el cual se le incorpora texto a un video.

Telecinado: proceso que consiste en la transformación de la película desde su formato cinematográfico (en soporte de celuloide - negativos o copias positivas) a vídeo (en soporte electrónico), como paso previo a su digitalización.

Transcripción: escribir parlamentos en el idioma nativo del video.

Visionaje: proceso de control de calidad realizado a los DVD.

Siglas:

ANCAP: Administración Nacional de Combustibles.

Blu-ray: rayo azul, es un nuevo formato físico de alta densidad, capaz de almacenar entre 23 y 27 GB por capa.

BROU: Banco Hipotecario del Uruguay.

CISA: Consultor y Auditor Certificado de Tecnologías de la Información.

DLT: (Digital Linear Tape o DLT). Tecnología de almacenamiento de datos por cintas magnéticas. Es utilizado especialmente para las copias de seguridad (backup). DLT fue desarrollado por DEC en 1984. En 1994 fue comprado por Quantum Corporation, quien actualmente fabrica unidades y licencias de tecnologías y marcas.

DTS: Digital Theater Systems, es un formato de codificación de audio multi-canal (hasta 7 canales), similar al Dolby Digital. Para disfrutarlo, necesitas un reproductor y / o un receptor / amplificador preparado para decodificar DTS.

DV: DVC DIGITAL VIDEO CASSETE es la versión genérica del formato. Existen 2 tamaños de cinta: DV y MiniDV, la segunda más pequeña permite hacer los camcorders más compactos y ligeros de forma que se impone en el mercado. Las características del DVC: muestreo 4:2:0 con color a 8 bit, compresión 5:1 tipo DCT intraframe , flujo de vídeo de 25 Mb/s, 2 ó 4 canales de audio PCM a 32 ó 48 KHz y a 12 ó 16 bit. Es la versión no propietaria, el estándar acordado por la IEC. Todos los fabricantes distribuyen DVC con cinta pequeña MiniDV, quedando este nombre como la versión que se comercializa para uso doméstico.

ETECSA: Empresa de Telecomunicaciones de Cuba S.A.

HDTV: Televisión de Alta Definición. Proporcionará una calidad de imagen cercana al cine de 35mm con sonido multicanal. La imagen de televisión estándar SD (Standard Definition) se

transmite con una resolución de 720 x 576 pixels (PAL), la imagen de alta definición HD (High Definition) tiene una tamaño de hasta 1920 x 1080 pixels. Por tanto, el número de elementos de la imagen por segundo se multiplica por un factor de 5. El resultado es una imagen con mucha claridad, nitidez y detalle que para aprovecharlas al máximo, es preciso visionarlas en pantallas o monitores HDTV de alta calidad o a través de proyectores.

ISACA: Information Systems Audit and Control Association

ISO: International Organization for Standardization.

LPCM: track de audio sin comprimir.

MAC: Ministerio de Auditoría y Control.

MIC: Ministerio de la Informática y las Comunicaciones.

MPEG IMX: formato basado en el estándar de compresión MPEG2 4:2:2 P&ML a 50 Mbps permite la edición con precisión de cuadro. Este formato está diseñado para adecuarse a las actuales infraestructuras de distribución, conexión y redes.

OGC: Oficina Gubernamental de Comercio del Reino Unido.

PyME: acrónimo de pequeñas y medianas empresas.

SOX: legislación Sarbanes-Oxley.

TI: Tecnologías de la Información.

UDF: Universal Disc Format (Formato de Disco Universal), estándar de Sistema de Archivo, que permite agregar archivos y carpetas, es por ello que es usado por la mayoría de el software existente de Escritura por Paquetes. Este Sistema de Archivo es obligatorio en los DVD's, pero también se admite en CD's. Es reconocido por Win98 si se trata de la versión 1.02, reconocido por Win2K si se trata de la versión 1.5, y reconocido por WinXP si se trata de la versión 2.01 (en el caso de que la sesión del CD/DVD/BD/HD DVD esté cerrada).

VHS: casete de video analógico.